Time Reversal Precoding with Artificial Noise Injection for Physical Layer Security

Sidney Golstein

▶ **To cite this version:**

Sidney Golstein. Time Reversal Precoding with Artificial Noise Injection for Physical Layer Security. Information Theory [cs.IT]. Sorbonne Universite; Université Libre de Bruxelles, 2022. English. ⟨NNT : ⟩. ⟨tel-04995129⟩

HAL Id: tel-04995129

https://hal.science/tel-04995129v1

Submitted on 18 Mar 2025

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons CC BY 4.0 - Attribution - International License

ECOLE POLYTECHNIQUE DE BRUXELLES

Université Libre de Bruxelles
Ecole Polytechnique de Bruxelles
OPERA
Wireless Communication Group

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

Sorbonne Université
Faculté d'Ingénierie
CNRS, Laboratoire de Génie
Electrique et Electronique de Paris

Time Reversal Precoding with Artificial Noise Injection for Physical Layer Security

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor in Electronics - Sorbonne Université
&
Doctor in Engineering and Technology - Université Libre de Bruxelles

Presented by
Sidney GOLSTEIN

under the supervision of
Dr. Julien Sarrazin and Pr. Dr. Philippe De Doncker

Defence on February 15^{th}*, 2022*
Members of the jury:

Ms. Michèle Wigger	Professor at Telecom ParisTech	Reviewer
Mr. Jérome Louveaux	Professor at Université Catholique Louvain	Reviewer
Mr. François Rottenberg	Assistant Professor at Katholieke Universiteit Leuven	Examining Board
Ms. Mireille Sarkiss	Associate Professor at Telecom SudParis	Examining Board
Mr. François Horlin	Professor at Université Libre de Bruxelles	Examining Board
Mr. Sébastien Tixeuil	Professor at Sorbonne Université	Examining Board
Mr. Julien Sarrazin	Associate Professor at Sorbonne Université	Supervisor
Mr. Philippe De Doncker	Professor at Université Libre de Bruxelles	Supervisor

Acknowledgements

At the end of this work, I would like to express my deep gratefulness to my supervisor from Paris, Pr. Dr. Ir. Julien Sarrazin for his unfailing availability, his continuous support, his great patience, his brilliant advices, his enthusiasm as well as his impressive knowledge. He was my internship supervisor and gave me the opportunity to join his team as intern in the L2E laboratory (now GeePs laboratory) back in summer 2017. He then closely supervised my research work during my master thesis and encouraged me to start a PhD journey. He inspired me and gave me the interest to fundamental research. I want to thank him for the enormous amount of time he spent for more than 4 years on the successful operation of my work and for encouraging my research. I couldn't hope for a better supervisor.

I would also like to express gratitude to my supervisor from Brussels, Pr. Dr. Ir. Philippe De Doncker. He trusted me and encouraged me to undertake a 3 months research internship at the L2E laboratory (now GeePs laboratory) at Sorbonne Université in Paris, back in summer 2017. He supervised my master thesis work, and then welcomed me at the Wireless Communication Group laboratory during the first year of my PhD at Université Libre de Bruxelles. His availability and warned advices motivated me throughout my entire research work.

Beside my supervisors, I also address my deep gratefulness to the members of my jury for their careful reading of the manuscript, the time they gave me, their insightful comments, suggestions, and their relevant questions.

My sincere thanks also goes to Pr. Dr. Ir. François Horlin. His 3 classes I followed during my university background were very exciting and inspiring. His availability and his knowledge helped me a lot during my PhD.

I would like to offer my special thanks to Asst. Pr. Dr. Ir. François Rottenberg. He gave me a lot of time answering my questions. His kindness, patience, and impressive scientific, technical, and mathematical knowledge were of great help during my PhD journey.

I am also grateful to all of the members of the Wireless Communication Group and the GeePs laboratories with whom I have had the pleasure to work with during more than three years. They welcomed me in Brussels and Paris, and I felt like a real member of the labs.

In addition, I particularly want to thank my parents and my sister Sophie for their permanent support and guidance. Without them, none of this would have been possible.

Finally, I would like to thank my grandfather. He was an electrical engineer and was the one who encouraged me to start my engineering studies. I will always remember the interest in science he gave me. I'm sure he would have been proud of the work I achieved. Thank you for that, Simi.

Abstract

An increasing number of devices exchanges data via the wireless medium into large scale, decentralized, and heterogeneous networks, leading to the concept of Internet of Things (IoT). This PhD work proposes a new practical scheme to perform physical layer security (PLS) in this IoT context.

Wireless communications in IoT networks are prone to passive eavesdropping. Therefore, this work introduces a scheme that guarantees the reliability of a communication from a transmitter (Alice) towards a legitimate user (Bob), while preventing multiple passive eavesdroppers (Eve) to correctly decode the data in a worst-cases scenario, thereby considering i) Eve to be noiseless, ii) Eve equipped with an arbitrarily large number of antennas, iii) Alice imperfectly estimating Bob's channel state information (CSI).

To do so, a frequency domain time-reversal (TR) precoder is proposed using orthogonal frequency-division multiplexing (OFDM) and artificial noise (AN) injection. The scheme exploits the frequency diversity selective behaviour in multipath channels, and can be incorporated into existing standards, such as in LTE or 5G networks. Different configurations are investigated, namely, single-input single-output (SISO), multiple-input single-output (MISO), and single-input multiple-output (SIMO) systems.

The handshake procedures between Alice and Bob are described, both in time-division duplexing (TDD) and frequency-division duplexing (FDD) systems, highlighting the amount of CSI acquisition at Eve, which influences the secrecy performances.

Depending on the handshake procedures, different decoding structures are investigated at Eve for each system configuration, considering a block-fading environment. Closed-form approximations of the signal-to-noise ratio required at Bob and the maximal CSI error that can be made at Alice, in order to guarantee a communication ergodic secrecy rate (ESR), are derived. Furthermore, the optimal amount of AN energy to inject, as well as the maximal number of eavesdropper's antennas allowed, considering imperfect CSI, are also given as closed-form expressions. A trade-off on the choice of the spreading factor of the TR precoder is established between maximizing the ESR and decreasing the percentage of outage, leading to information leaked to Eve. Finally, thanks to these results, Alice can be a-priori aware of the ESR over which she can establish a secure communication, assuming worst-case assumptions regarding the eavesdroppers. The PLS scheme presented in this PhD work therefore emerges as a promising solution to secure wireless communications in IoT networks.

Keywords— Physical layer security, IoT, artificial noise, time reversal, OFDM, SISO, MISO, SIMO, block-fading, passive eavesdropping, TDD, FDD, ergodic secrecy rate, outage.

Contents

List of Acronyms

Acronym	Description
ADC	analog-to-digital
AFF	artificial fast fading
AN	artificial noise
AoA	angle-of-arrival
ASM	antenna subset modulation
AWGN	additive white Gaussian noise
BAN	body area network
BCC	broadcast channel with confidential message
BER	bit error rate
BF	block fading
BOR	back-of-rate
BS	base station
CFO	carrier frequency offset
CP	cyclic prefix
CSI	channel state information
D2D	device-to-device
DAC	digital-to-analog
DL	downlink
DM	directional modulation
DMC	discrete memoryless channel
DoS	denial of service
DPS	Doppler power spectrum
DSSS	direct-sequence spread spectrum
DWTC	degraded wiretap channel
EC	ergodic capacity
ESC	ergodic secrecy capacity
ESINR	ergodic signal-to-interference-plus-noise ratio
ESR	ergodic secrecy rate
FD	frequency domain
FDD	frequency division duplex
FFT	fast Fourier transform
FHSS	frequency-hopping spread spectrum
GBCC	Gaussian broadcast channel with confidential message

Acronym	Description
GSOP	generalized secrecy outage probability
GSVD	generalized singular value decomposition
GWTC	Gaussian wiretap channel
i.i.d.	independent and identically distributed
ICI	inter-carrier interference
IFFT	inverse fast Fourier transform
iif.	if and only if
IoT	Internet of Things
ISI	inter-symbol interference
LDPC	low density parity check
LMMSE	linear minimum mean square error
LOS	line-of-sight
LTE	Long Term Evolution
LTE-A	Long Term Evolution-Advanced
MAC	medium access control
MF	matched filter
MIMO	multiple-input multiple-output
MIMOME	multiple-input multiple-output multi-eavesdropper
MISO	multiple-input single-output
MISO-ME	multiple-input single-output muti-eavesdropper
MISO-SE	multiple-input single-output single-eavesdropper
MRC	maximal-ratio combining
MSE	mean square error
MTC	machine-type communication
NFDAM	near-field direct antennal modulation
NLOS	non line-of-sight
NMSE	normalized mean square error
OC	own channel
OFDM	orthogonal frequency-division multiplexing
OSI	open systems interconnection
OTDM	orthogonal transform division multiplexing
PAPR	peak-to-average power ratio
pdf	probability density function
PDP	power delay profile
PLS	physical layer security
pmf	probability mass function
PSK	phase shift keying
QAM	quadrature amplitude modulation
QoS	Quality of Service
RF	radio frequency
RFF	radio frequency fingerprint

Acronym	**Description**
RV	random variable
SC	secrecy capacity
SDMA	spatial division multiple access
SDS	same decoding structure
SF	slow fading
SIC	successive interference cancellation
SIMO	single-input multiple-output
SIMO-ME	single-input multiple-output muti-eavesdropper
SIMO-SE	single-input multiple-output single-eavesdropper
SINR	signal-to-interference-plus-noise ratio
SISO	single-input single-output
SISO-ME	single-input single-output muti-eavesdropper
SISO-SE	single-input single-output single-eavesdropper
SNR	signal to noise ratio
SPER	secure packet error rate
SR	secrecy rate
STO	symbol time offset
SVD	singular value decomposition
TD	time domain
TDD	time division duplex
TR	time reversal
TSOP	tight secrecy outage probability
UE	user equipment
UL	uplink
VLC	visible light communication
w.r.t.	with respect to
Wi-Fi	Wireless Fidelity
WTC	wiretap channel
ZMCSCG	zero mean circularly symmetric complex Gaussian

List of Symbols

Sign	Description	Unit
$\mathbf{H_{BE}}$	Bob-to-Eve channel	Dimensionless
$\mathbf{H_{B},}_{k}$	Bob's k^{th} subchannel	Dimensionless
$\mathbf{H_B}$	Alice-to-Bob (i.e., main) channel	Dimensionless
$\mathbf{H_{E,k,l}}$	Alice's k^{th} antenna-to-Eve's l^{th} antenna channel	Dimensionless
$\mathbf{H_{E,k}}$	Eve's k^{th} subchannel	Dimensionless
$\mathbf{H_E}$	Alice-to-Eve (i.e., eavesdropper) channel	Dimensionless
δ_B	Bob's SNR	Dimensionless
δ_E	Eve's SNR	Dimensionless
$\gamma_{B,n}$	Bob's instantaneous SINR for a particular symbol n	Dimensionless
γ_B	Bob's instantaneous SINR	Dimensionless
$\gamma_{E,n}$	Eve's instantaneous SINR for a particular symbol n	Dimensionless
γ_E	Eve's instantaneous SINR	Dimensionless
σ_{AN}	Artificial noise variance	Dimensionless
σ_{B}	Bob's noise variance	Dimensionless
σ_{E}	Eve's noise variance	Dimensionless
N_A	Number of antennas at Alice	Dimensionless
N_B	Number of antennas at Bob	Dimensionless
N_E	Number of antennas at Eve	Dimensionless
N	Number of symbols per OFDM block	Dimensionless
Q	Number of subcarriers per OFDM block	Dimensionless
U	Back-of-rate, spreading factor	Dimensionless
α^D_{opt}	Optimal ratio between useful and the total signal power to inject, depending on the scenario	Dimensionless
α	Ratio between useful and the total signal power	Dimensionless
ϵ	Fraction of outage	Dimensionless
σ^D_{max}	Maximal allowed estimation error variance, depending on the scenario	Dimensionless
σ_{dB}	Estimation error variance in dB	dB
σ	Estimation error variance	Dimensionless
B_d	Doppler spread of the channel	Hz
$(\Delta f)_c$	Coherence bandwidth of the channel	Hz
f_{DL}	Downlink frequency	Hz
f_{UL}	Uplink frequency	Hz
Δ	Targeted ergodic secrecy rate	bit/channel use
C_B	Bob's ergodic capacity per OFDM block	bit/channel use
C_E	Eve's ergodic capacity per OFDM block	bit/channel use
$C_{B,n}$	Bob's ergodic capacity per symbol	bit/channel use

Sign	Description	Unit
$C_{E,n}$	Eve's ergodic capacity per symbol	bit/channel use
R_s	Ergodic secrecy rate per OFDM block	bit/channel use
$R_{s,n}$	Ergodic secrecy rate per symbol	bit/channel use
$(\Delta t)_c$	Coherence time of the channel	s
T_m	Multipath spread of the channel	s

List of Figures

List of Tables

1 | Introduction

Contents

1.1 General context

As networks flourish worldwide, the problems of transmission, routing, resource allocation, end-to-end reliability, authentication, and congestion are assigned to different layers of the open systems interconnection (OSI) protocol. When considering securing communications, the physical layer, lying at the bottom of the protocol architecture and converting bits of information into modulated signals, has remained almost ignored. However, randomness, a key element in secrecy systems, is intrinsically part of noise and propagation channel. Therefore, the physical layer emerges as a promising solution to provide secure wireless communication schemes, [1].

In addition, the wireless medium has become the dominant access to Internet-based services. According to the Cisco annual Internet Report (2018-2021), the number of global mobile subscribers will grow from 5.1 billion in 2018 (66 % of global population) to 5.7 billions by 2023 (71 % of global population). Internet users will grow from 3.9 billion in 2018 (51 % of global population) to 5.3 billion by 2023 (66% of global population), [2]. New access technologies, such as in 5G networks, have been deployed to guarantee customers Quality of Service (QoS), and offer a huge amount of beneficial applications for mobile users. These new generations of wireless networks are large-scale heterogeneous and decentralized, as depicted in Figure 1.1.

However, due to the broadcast nature of radio propagation, the wireless air interface is inherently unsecure, since it is unbounded and accessible to both authorized and illegitimate receivers. It is therefore of paramount importance to improve the security of wireless networks which are carrying and exchanging an increasing amount of sensitive and valuable data, e.g., banking or health data. New security requirements consequently need to be implemented, without just relying on cryptographic key-based security schemes, [3, 4]. Classical cryptography systems use public-key cryptography for authentication, and secret-key distribution and symmetric encryption for data protection. The technology is widely employed and mature, few assumptions are made about the messages to be encrypted and trusted. Nevertheless, it suffers from several main drawbacks, [3, 5–7]:

- The key management process, distribution, and maintenance for the legitimate parties become a real issue with the deployment of large-scale heterogeneous and decentralized networks involving different access technologies, such as in 5G networks. It requires a trusted third party as well as complex protocols and system architectures. It necessitates additional computational power and therefore causes latency.

- Longer keys are needed to increase the level of security, which results in more waste of resources.
- The illegitimate parties are assumed to have limited computational capabilities. Indeed, cryptography-based systems implement one-way functions that are supposed *hard to invert*. However, with the fast development in high-computing-power devices, secret keys that were secure decades ago are nowadays more subject to successful brut-force attacks.
- Cryptographic schemes are based on semantic secrecy and security is measured by the fact that a given protocol resists or not to attacks. No precise metric is available to quantify the degree of secrecy.

To circumvent the aforementioned issues, physical layer security (PLS) has emerged as an effective way to enhance security of wireless communications, [8–11]. No computational limitation is given to the illegitimate parties, and the information that is leaked can be precisely quantified with information-theoretic metrics as a function of the channel quality. Nevertheless, PLS also suffers from several demerits:

- Security relies on average information measures, such that it can be impossible to guarantee a secure communication with probability one.
- In order to provide security, assumptions are undertaken regarding the communication channel, which can be inaccurate in practice.

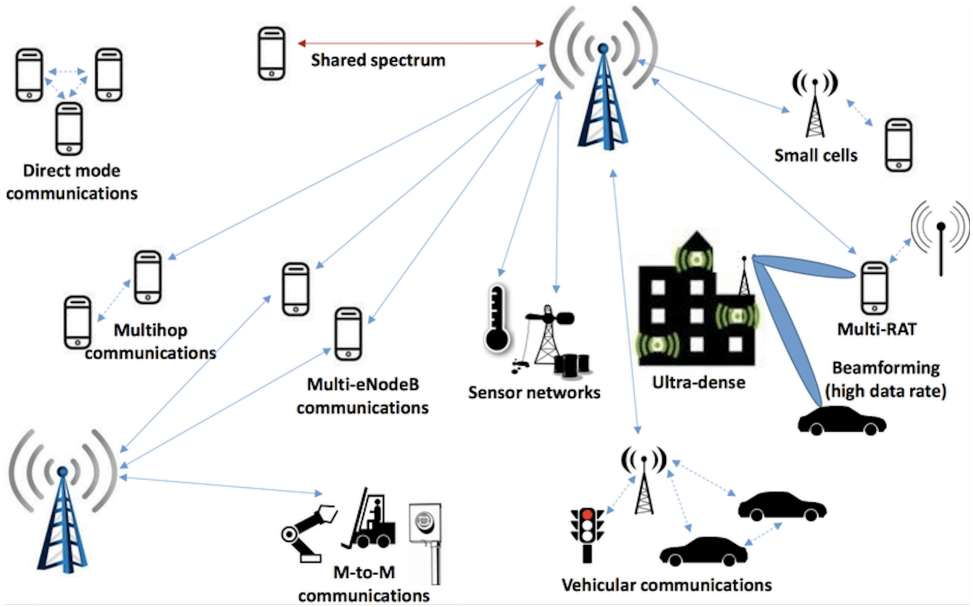

Figure 1.1: 5G network architecture, [12, Figure 1]

As seen, PLS and cryptographic systems have their own merits and demerits. In order to benefit from higher secrecy performances, PLS schemes can be incorporated into existing security systems. That is, security at the physical layer should be implemented as part of a layered protocol to perform ***cross-layer security***. It allows one to exploit the degrees of freedom at different layers, which therefore increases the robustness of practical systems against potential attacks, while meeting the requirements of new wireless technologies.

Security in heterogeneous and distributed networks

As explained, a larger number of objects are being connected to the Internet at an unprecedented rate, leading to the concept of Internet of Things (IoT), [13]. According to the Ericsson Mobility Report of June 2021, the number of connected IoT devices around the world will rise from 12.4 billion in 2020, to an expected 26.4 billion by 2026, [14, Figure 11]. IoT systems allow physical objects to communicate,

monitor, access, and collect valuable data without human-to-human or human-to-computer intervention, [15]. New emergent services are provided in IoT, such as vehicular communications for autonomous driving, massive machine-type communications (MTCs), device-to-device (D2D) communications, or body area network (BAN) communications for instance, with their own constraints and requirements.

In IoT, various networks must interoperate and coexist, and different types of objects access and exchange data in the networks. From that, IoT devices can benefit from the decentralized, heterogeneous, and flexible architecture offered in public 5G networks. Fog/Edge computing appears as a suitable solution to provide efficient and secure services for IoT. Fog/Edge computing is an architecture organized by the networking edge devices where the massive amount of data can be processed at the network edges instead of being transmitted to the centralized cloud infrastructures. Therefore, this distributed architecture allows one to provide services with faster response and greater quality in comparison with cloud computing, [16].

IoT devices are composed of objects of compact sizes, power limited, hardware complexity limited, signal processing restricted, and data rate limited, [3, 15, 17, 18]. These different objects require low signal overhead, sporadic low data rate, are typically equipped with single antenna sensors. They exchange data with a multi-antenna controller, or base station (BS), as seen in Figure 1.2. Consequently, security in IoT networks is unsuitable for classical encryption-based security methods, [3, 15, 17, 18].

From the above discussion, security in decentralized, large scale, and heterogeneous public networks (such as in 5G networks) appears to be a challenging task that can be addressed thanks to well designed PLS schemes. Indeed, having everything densely connected, these networks are prone to a wide range of attacks, as explained in section 1.2. Furthermore, different secure system configurations need to be considered, i.e., communications between single-antenna user equipments (UEs) (single-input single-output (SISO) system), downlink (DL) between multi-antenna BS and single-antenna UE (multiple-input single-output (MISO) system), as well as uplink (UL) between single-antenna UE and multi-antenna BS (single-input multiple-output (SIMO) system). The security schemes that can be implemented in the UL (respectively the DL) might indeed become unsuited for the DL (respectively the UL), [3].

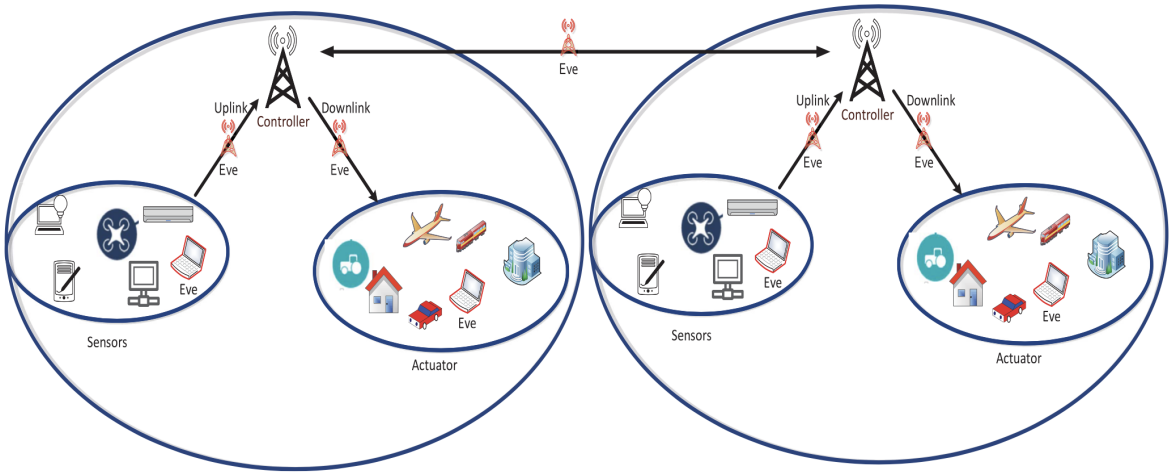

Figure 1.2: Internet of Things network with eavesdropper, [3, Figure 23]

1.2 Security requirements in wireless networks

When considering a secure system, it is assumed that a transmitter (Alice) and a legitimate receiver (Bob) aim to "***securely***" communicate over a wireless medium, where an illegitimate receiver (Eve) can intercept the transmitted data. It is of prime importance to understand the fundamental security

requirements in wireless networks. Indeed, different desirable properties can be identified, namely data integrity, availability, authenticity, and confidentiality and reliability, [5], [19, Chapter 8].

Data integrity
Data integrity refers to the fact that Alice and Bob aim to ensure that the content of the transmitted data is not falsified in transit. A node that is compromised and altered by an adversary is termed as a compromised node. It is challenging to detect the attacks by compromised nodes since these are nodes that have valid identities, [15].

Availability
Availability implies that the authorized users can access the wireless network anytime and anywhere upon request. Denial of service (DoS) refers to the violation of availability, i.e., users are unable to access the wireless network resulting in unsatisfactory user experience.

Authenticity
Authenticity means that both the transmitter and the legitimate receiver should be able to confirm their identity, and distinguish authorized users from unauthorized users. At the physical layer, data authentication can be performed using either the hardware properties of radio frequency (RF) devices, or the propagation characteristics of wireless channels. As an example, one can implement radio frequency fingerprint (RFF) authentication schemes, [18]. It is based on the fact that hardware imperfections in analog circuits result from manufacturing processes, and are permanent and unique for every device. RFF can therefore be used to authenticate the device. In addition, the channel properties at the transmitter and the receiver can be compared to provide authentication, by exploiting the uniqueness of the channel state information (CSI), or by exploiting the angle-of-arrival (AoA) information, for instance, [5].

Confidentiality and reliability
Confidentiality and reliability suggests that the data is only accessible and understandable by the transmitter and the legitimate receiver, i.e., reliability, while the leakage of information is prevented from the illegitimate receiver, i.e., confidentiality. There is a wide range of PLS schemes implemented in the literature aiming to provide reliability at the legitimate receiver, while preventing the eavesdropper to accurately decode the data. As it will be explained in next chapters, the idea is to give a physical advantage to Bob compared to Eve in order to provide positive information-theoretic security performances.

Conclusion
The confidentiality and reliability requirement is by far the most investigated security requirement at the physical layer and yet, there is a lack of realistic schemes whereby confidentiality and reliability can be guaranteed. There is therefore a need to design practical PLS schemes that can be incorporated into existing communications standards, while being able to guarantee QoS to the different users.

1.3 Physical layer attack models

In addition to requiring different security services, wireless communications are subject to multiple types of attacks. These can be classified into four categories, namely, impersonation, message falsification, jamming, and eavesdropping, [6].

Impersonation
Impersonation attempts to the message integrity requirement. In that situation, the attacker is active and sends a fake message while the source is idle. At the physical layer, to counteract an impersonation attack, one can implement authentication PLS schemes, [4].

Message falsification
Message falsification suggests that an internal or an external attacker has the ability to modify some part of the message during transmission process. It therefore affects the trust of the received message, [6]. As for the impersonation attack, message falsification destroys the integrity requirement.

Jamming
Jamming attacks aim from preventing authorized users to access the wireless medium by sending unwanted radio signals that introduce interference and disrupt the communications. Jamming attacks are also known as DoS attacks. It therefore corrupts the availability requirement. In [5], authors subdivided the jamming attacks into five categories, namely, constant, intermittent, reactive, adaptive, and intelligent jamming attacks. These strategies correspond to different trade-off between jamming efficiency and risks for the jammer to be detected.

Eavesdropping
Eavesdropping it the act of secretly listening to a private communication. Wireless communications can be overheard by unauthorized users as long as they are located in the transmit area coverage of the source node, which results to information leakage, [5]. The broadcast nature of wireless communications makes it prone to eavesdropping attacks. It can be classified into active and passive eavesdropping. An active eavesdropper is registered in the network as a subscribed user and exchanges messages with the BS. The transmitter can therefore estimate the active eavesdropper's propagation channel characteristics and take it into account to design a PLS scheme. It is often assumed that the objective of an active eavesdropper is to decode private messages of any legitimate users, [20]. In a passive eavesdropping scenario, the attacker only listens to the transmission between Alice and Bob, while remaining silent. He passively eavesdrops the data and Alice cannot have the knowledge of his propagation channel characteristics. Eavesdropping therefore aims to deny the confidentiality requirement of security.

Conclusion
Eavesdropping is an important attack model that needs to be investigated in the context of IoT. Indeed, due to the large and increasing number of connected IoT devices in large scale, heterogeneous and decentralized networks, wireless communications are very prone to be overheard by unauthorized devices, i.e., there are subject to passive or active eavesdropping. In addition, a passive eavesdropping scenario reflects the malicious behaviour of an attacker which is not considered as a subscribed user of the network, which remains silent, undetectable, and unknown to the legitimate communication's ends. The issue of designing practical and robust PLS schemes against passive eavesdroppers therefore needs to be addressed.

1.4 Challenges and objectives of the manuscript

Secure wireless communications need to meet multiple requirements and are subject to various types of attacks. In addition, secure wireless systems have to be deployed for an increasing number of different applications with their own constraints in terms of security level, delay, power efficiency, spectral efficiency, and complexity. To optimize the security performances, wireless communications have to integrate multi-layered security protocols taking advantage of the various merits and demerits at each layer of the OSI protocol. In other words, PLS schemes must jointly be designed alongside classical cryptography-based schemes.

PLS has emerged as a promising solution to enhance the security of communications in the context of IoT, where a growing number of interconnected devices communicate within decentralized, heterogeneous, and large scale public infrastructures, such as in 5G networks. PLS schemes in IoT networks need to consider different system configurations, namely, SISO, MISO, and SIMO systems. Indeed, security has to be provided for communications between UEs (SISO system), in the DL between a BS and an UE (MISO system), as well as in the UL between an UE and a BS (SIMO system). In addition,

having everything densely connected, communications in IoT networks are prone to be intercepted and miscellaneously treated by unauthorized and unknown users. Therefore, the design of PLS schemes against passive eavesdropping in IoT networks has to be handled.

The theoretical limits of physical layer secrecy performances are provided with information theory. However, practical design of PLS schemes that achieve these theoretical performances are lacking.

The objective of this PhD work is therefore to design and study a practical PLS scheme that can be incorporated into large scale, heterogeneous and decentralized networks, such as in 5G networks. The proposed scheme aims to deliver reliable data at the legitimate receiver, while preventing the illegitimate passive receiver(s) to correctly decode the data. A passive eavesdropping scenario is considered since it reflects many practical attacking situations encountered in IoT networks. In addition, the PLS scheme can be implemented for SISO, MISO, and SIMO systems. It is therefore suitable for the different system configurations present in IoT networks. As it will be seen, designs of PLS schemes that provide reliability at the legitimate user and confidentiality from the passive eavesdropper(s) are well studied in the literature. However, there is a lack of studies that allow the transmitter to guarantee a desired secure QoS. Consequently, analytic models of the secrecy performances are derived in this PhD work. The goal is to design the communication parameters in order for the transmitter to be a-priori aware of the secrecy performances of the communication. In doing so, the transmitter is able to guarantee a desired QoS at the legitimate receiver's end, while preventing the illegitimate receiver(s) to eavesdrop the data.

The manuscript is organized as follows.
Chapter 2 introduces the fundamentals of information theory. It allows one to present the two conventional approaches to implement PLS systems, namely the complexity-based (key-based) and signal-to-interference-plus-noise ratio (SINR)-based (key-less) approaches. The chapter motivates the study of a SINR-based PLS scheme. It is shown that a positive secrecy capacity, which quantifies from an information-theoretic perspective the maximal achievable secure communication's rate, can be obtained if a physical advantage is given at Bob compared to Eve. The goal of the thesis is therefore to ensure giving a physical advantage to Bob's channel. The chapter ends by highlighting different metrics that are classically used in PLS. The choice of the metrics that are considered throughout this manuscript is also justified.

Chapter 3 draws a state-of-the-art of the SINR-based PLS techniques. The chapter highlights the fact that some channel state information (CSI) knowledge is needed at the transmitter to design a secure communication scheme, and that the amount of CSI knowledge at the communication's ends, i.e., at Alice, Bob, and Eve, strongly impacts the secrecy performances. It is shown that, in practical scenarios, the transmitter is not able to perfectly estimate the main CSI. The physical reasons of imperfect CSI estimation are described and a state-of-the-art of PLS techniques that take into account this imperfect main CSI knowledge is outlined.

Chapter 4 presents the PLS scheme that is considered throughout this study. In particular, different system configurations are investigated depending on whether Alice or Bob and/or Eve possess one or multiple antennas. For each configuration, it is shown that, depending on the handshake procedure between Alice and Bob, Eve can obtain different amount of CSI knowledge. She therefore implements the most suitable practical decoding structures which leads to different secrecy performances.

Chapters 5 and 6 respectively analyse the secrecy performances of the single antenna system, i.e., both Alice and Bob possess one antenna, and the multi-antenna system, i.e., either Alice or Bob possess multiple antennas, in the presence of passive eavesdroppers. For each investigated practical scenario, analytic models of the secure communication rate are derived. It allows Alice to design the communication parameters to know a-priori the secure rate over which she can communicate

with the legitimate receiver, while preventing the eavesdropper to correctly decode the transmitted data. Outage constraints are also considered. The worst case assumptions regarding the eavesdropper are undertaken. By doing so, the transmitter is able to guarantee a desired QoS to the legitimate receiver.

Chapter 7 concludes the manuscript. It gives the main contributions of the work and suggests the challenges and the perspectives for future research directions.

Remark 1.1: Use of *security* term

With a slight abuse of language, security refers to ***confidentiality from Eve and reliability at Bob*** in the following of this manuscript. Authentication, integrity and availability schemes are not investigated in this work. It is considered that these requirements are beforehand fulfilled and are implemented at the upper layers of the protocol stack.

2 | Introduction to Physical Layer Security

Contents

2.1 Introduction

Cryptography-based security techniques, implemented at the upper layers of the OSI protocol, can be unsuitable for new wireless technologies involved in 5G networks. To circumvent these issues, this manuscript investigates security techniques that are implemented at the physical layer to ensure reliability at the legitimate receiver and confidentiality from the illegitimate receiver. While the work presented in the next chapters introduces coding techniques from a communication perspective, foundation of PLS lies in information theory.

Indeed, secure communication performances can be precisely quantified with information theory metrics and that is why the objective of this chapter is to introduce PLS from an information-theoretic perspective. First, the fundamentals of information theory are presented. Then, using these fundamentals, the notion of information-theoretic channel capacity is defined, and a mathematical presentation of the

secrecy capacity is then given. This important information-theoretic concept is used in the following of this manuscript to model and quantify the secure communication rate of the PLS scheme. Finally, different PLS metrics are presented with their merits and demerits. It allows to motivate and justify the metrics that are considered throughout this manuscript to evaluate the level of security of the proposed PLS scheme.

This chapter consequently introduces the necessary background for the following chapters. It is mainly based on the reference book from Bloch and Barros, [1].

Notation 2.1

In the reminder of this manuscript, the italic lower-case letter denotes a scalar number. Greek letter corresponds to a real scalar, the bold lower-case letter denotes a column vector. Bold upper-case letter corresponds to a matrix; $\mathbf{I}_N$ is the $N \times N$ identity matrix; $(.)^{-1}$, $(.)^*$, $(.)^H$, $(.)^T$ are respectively the inverse, the complex conjugate, the Hermitian transpose, and the transpose operators; $\mathbb{E}[.]$ is the expectation operator; $||.||$ is the Frobenius norm of a matrix, $|.|$ is the modulus operator of a scalar; $\mathbf{0}_N$ and $\mathbf{1}_N$ are respectively all-zero and all-one column vector of dimension $N \times 1$.

2.2 Information theory metrics

This section defines some information-theoretic tools that are useful for the reader's understanding for rest of the manuscript.

Entropy
Let $X \in \mathcal{X}$ be a discrete random variable (RV) with probability mass function (pmf) $p_X(x)$, i.e., $X \sim p_X(x)$. The entropy of X is defined as:

$$\mathbb{H}(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x) \tag{2.1}$$

It gives the uncertainty about the outcome X, or the measure of the average amount of information contained in X. The unit for entropy is called a bit, and all logarithms are taken to the base two.

Conditional entropy
Let $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ be two discrete RVs with joint distribution $p_{XY}(x,y)$. The conditional entropy (equivocation) of Y given X is defined as:

$$\mathbb{H}(Y|X) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p_{XY}(x,y) \log p_{Y|X}(y|x) \tag{2.2}$$

It gives a measure of the remaining uncertainty about the outcome Y given the observation X.

Joint entropy
Let $(X,Y) \sim p_{XY}(x,y)$ be a pair of discrete RVs. The joint entropy of X and Y is defined as:

$$\begin{aligned} \mathbb{H}(X,Y) &= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p_{XY}(x,y) \log p_{XY}(x,y) \\ &= \mathbb{H}(X) + \mathbb{H}(Y|X) \\ &= \mathbb{H}(Y) + \mathbb{H}(X|Y) \end{aligned} \tag{2.3}$$

it gives a measure of the uncertainty associated with the set of variables (X,Y).

Mutual information

Let $(X,Y) \sim p_{XY}(x,y)$ be a pair of discrete RVs. The mutual information between X and Y is defined as:

$$\begin{aligned} \mathbb{I}(X;Y) &= \mathbb{H}(X) - \mathbb{H}(X|Y) \\ &= \mathbb{H}(Y) - \mathbb{H}(Y|X) \\ &= \mathbb{H}(X) + \mathbb{H}(Y) - \mathbb{H}(X,Y) \end{aligned} \tag{2.4}$$

It gives a measure of the information about X obtained from the observation Y. The mutual information is a non-negative function and equals zero if and only if (iif.) X and Y are statistically independent.

Conditional mutual information

Let $(X,Y,Z) \sim p_{XYZ}(x,y,z)$ be a triplet of discrete RVs. The conditional mutual information between X and Y given Z is defined as:

$$\begin{aligned} \mathbb{I}(X;Y|Z) &= \mathbb{H}(X|Z) - \mathbb{H}(X|Y,Z) \\ &= \mathbb{H}(Y|Z) + \mathbb{H}(Y|X,Z) \\ &= \mathbb{H}(X|Z) + \mathbb{H}(Y|Z) - \mathbb{H}(X,Y|Z) \end{aligned} \tag{2.5}$$

Figure 2.1 shows the relationships between the different information-theory quantities defined above.

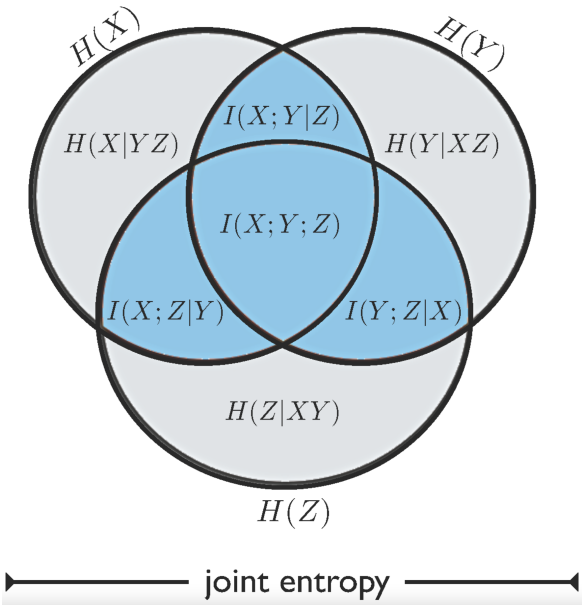

Figure 2.1: Relationship between information-theory metrics

Data-processing inequality

Le $X \in \mathcal{X}$, $Y \in \mathcal{Y}$, and $Z \in \mathcal{Z}$ be three discrete RVs such that $X \to Y \to Z$ forms a Markov chain. Then:

$$\mathbb{I}(X;Z) \leq \mathbb{I}(X;Y) \Leftrightarrow \mathbb{H}(X|Z) \geq \mathbb{H}(X|Y) \tag{2.6}$$

The data processing inequality means that, on average, processing Y can only decrease the mutual information with X. In other words, processing Y increases on average the uncertainty about X.

Remark 2.1: Continuous random variables

For continuous random variables, the notion of entropy is replaced with differential entropy, the pmf is replaced with the probability density function (pdf), the sum are replaced by integrals. All the above definitions can be adapted to continuous random variables.

2.3 Channel capacity

2.3.1 Introduction to the point-to-point communication

The point-to-point communication model is of prime importance since it allows to define the fundamental notion of ***channel capacity*** . This notion is then used to define the ***secrecy capacity*** in the following of this chapter.
This communication model introduces the definitions of a discrete memoryless channel (DMC), channel code for a DMC, achievable transmission rate for a DMC, and capacity of a DMC. A block diagram of a DMC is depicted in Figure 2.2.

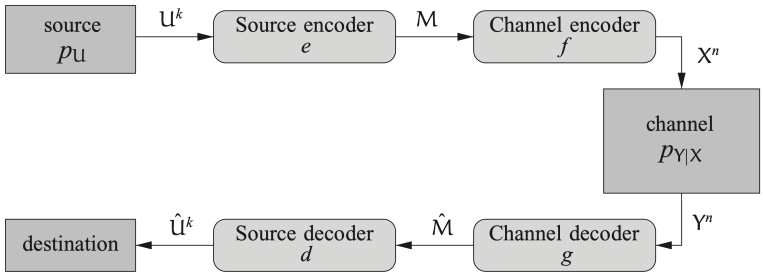

Figure 2.2: Point-to-point communication model, [1, Figure 2.3].

It shows a two-stage communication scheme where it is assumed that the *source* and the *channel* are described by discrete-time random processes. The transmitter and the receiver agree on a common *code*, specified by an *encoder* and *decoder* pair. The source $(\mathcal{U}, p_U)$ is compressed before being encoded for transmission through a DMC. At the receiving side, the channel output is decoded and decompressed. In what follows, the source $(\mathcal{U}, p_U)$ is considered uniform over $\mathcal{U}$, i.e., there is no need to encode the source since its entropy is maximal. The rest of the chapter only focuses on the channel encoding and decoding processes.

2.3.2 The discrete memoryless channel

A DMC is denoted as $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$. It consists in a finite input alphabet $\mathcal{X}$ with channel inputs X, a finite output alphabet $\mathcal{Y}$ with channel outputs Y, and a conditional probability distribution $p_{Y|X}$, i.e., the channel.

2.3.2.1 Channel code for a discrete memoryless channel

A $(2^{nR}, n)$ channel code C_n for a DMC $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ consists of:

- A message set $\mathcal{M} = \left[1, 2^{nR}\right]$, where R is an achievable transmission rate for the DMC and is defined below, and n is the number of symbols.
- An encoding function $f : \mathcal{M} \to \mathcal{X}^n$, that maps a message m to a codeword x^n with n symbols.
- A decoding function $g : \mathcal{Y}^n \to M \cup \{e\}$, that maps a block of n channel outputs y^n to a message $\hat{m} \in \mathcal{M}$ or an error message e.

The *codebook* of C_n is the set of all possible codewords $\{f(m) : m \in \left[1, 2^{nR}\right]\}$. It is assumed that codebook and the conditional probability distribution $p_{Y|X}$ are known to the receiver.

2.3.2.2 Achievable transmission rate for a discrete memoryless channel

The average probability of error is defined as:

$$\mathbf{P}_e(C_n) = \mathbb{P}\left[\hat{M} \neq M | C_n\right]. \tag{2.7}$$

From (2.7), a rate R is an *achievable transmission rate* for the DMC $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$, if there exists a sequence of $(2^{nR}, n)$ channel codes $\{C_n\}_{n\geq 1}$ such that:

$$\lim_{n\to\infty} \mathbf{P}_e(C_n) = 0. \tag{2.8}$$

Equation (2.8) states that messages can be transmitted at rates arbitrarily close to R and decoded with arbitrarily small probability of error.

2.3.2.3 The channel coding theorem

The capacity of a DMC $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ is given by:

$$C = \max_{p_X} \mathbb{I}(X;Y). \tag{2.9}$$

In other words, if a rate R is such that $R < C$, R is an achievable transmission rate. In addition, an achievable transmission rate R must respect $R \leq C$. The channel coding theorem shows that it is possible to design channel codes C_n allowing achievable transmission rate, upper bounded by the channel capacity C. The channel capacity is defined as the maximum mutual information between the channel input X and the channel output Y.

2.4 Types of secrecy

Section 2.3 presents the capacity of a point-to-point communication. The key idea of a capacity-achieving communication is to ensure reliability at the receiver side. This section introduces the notion of information-theoretic security, where secrecy from the eavesdropper has to be provided in addition to reliability at the legitimate receiver. Different notions of secrecy are presented with their implications, which are useful to characterize the secrecy capacity of the system considered in this manuscript.

2.4.1 Shannon's perfect secrecy

Shannon first formalized the notion of information-theoretic perfect secrecy in [21]. In his model, a transmitter (Alice) encodes a message $M \in \mathcal{M}$ into codewords $X \in \mathcal{X}$ thanks to a secret key $K \in \mathcal{K}$, unknown to an eavesdropper (Eve), and transmits it over the legitimate receiver (Bob) and the eavesdropper channels. The scheme is presented in Figure 2.3. The use of a shared secret-key is motivated by the fact that the main and the eavesdropper's channels are noise-free. From that, the codeword is overheard by Eve whose channel is error-free, which corresponds to the worst case scenario in terms of security. To possess an advantage over Eve in order to recover the message M, Bob agrees with Alice over a *secure channel* on a secret-key that is used to encode and decode the transmitted message. The codeword is then generated with a function of the message M and the key K. A *coding scheme* is a pair (e, d) of encoding and decoding functions such that $X = e(M, K)$ and $M = d(X, K)$. The key and the message are assumed to be statistically independent.

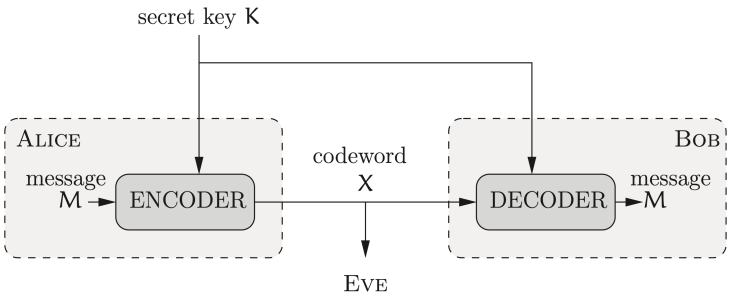

Figure 2.3: Shannon's model of perfect secrecy, [1, Figure 1.1].

Security is quantified by a measure of the average uncertainty at the eavesdropper. It is given by the conditional entropy of the message given the codeword, called eavesdropper's equivocation. A coding scheme is said to achieve *perfect secrecy* iif.:

$$\mathbb{H}(M|X) = \mathbb{H}(M) \Leftrightarrow \mathbb{I}(M;X) = 0 \Leftrightarrow \mathbb{H}(K) \geq \mathbb{H}(M), \tag{2.10}$$

i.e., messages and codewords are statistically independent. The absence of correlation ensures the there is no algorithm allowing the eavesdropper to retrieve the message. Equation (2.10) ensures no information leakage to Eve. It has to be pointed out that, in real systems, noise is always present. Therefore, the theoretical assumption of a noise-free eavesdropper channel corresponds to the existence of powerful error-correction mechanisms.

The issue with Shannon's notion of perfect secrecy is that it can only be achieved if the uncertainty about the key is larger than the uncertainty about the message, i.e., $\mathbb{H}(K) \geq \mathbb{H}(M)$. In other words, the secret key must contain at least one bit for every information bit. The drawbacks of the perfect secrecy requirement are listed below:

- Alice must generate and store long keys.
- A key can only be used once.
- The key must be shared over a secure channel.

The notion of perfect secrecy is therefore not applicable in practical scenarios. Nevertheless, one can affirm that requiring perfect secrecy is much stricter than preventing Eve to decode correctly, such that relaxed secrecy definitions can be introduced.

2.4.2 Wyner's asymptotic perfect secrecy

Shannon's model does not include the noise which is inherent to physical channels. By taking the noise into account, Wyner introduced the *Wyner's wiretap channel model* where there is no more the need to share a secret key, [22]. The model is depicted in Figure 2.4.

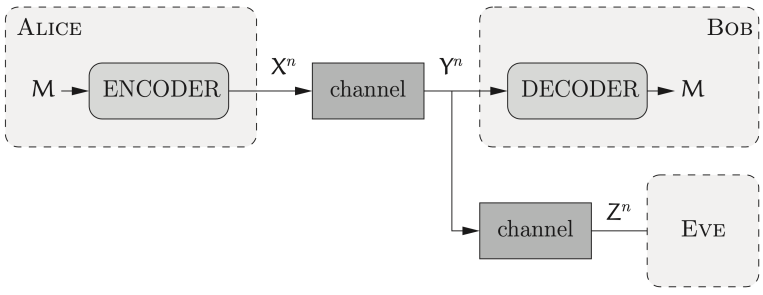

Figure 2.4: Wyner's model of asymptotic perfect secrecy, [1, Figure 1.2].

From Figure 2.4, Alice encodes a message M into a codeword X^n composed of n symbols, which is sent over a noisy channel to the legitimate receiver, called the ***main channel***. Bob observes Y^n, and Eve observes Z^n, which is a noisy version of Y^n. The channel between Alice and Eve is the ***eavesdropper's channel***.

Wyner proposed a less stringent definition of secrecy. Instead of imposing ***exact*** statistical independence between the message M and the eavesdropper's observations Z^n, he requires ***asymptotic*** statistical independence, as the codeword length n goes to infinity. With this new secrecy definition, known as ***asymptotic perfect secrecy***, the equivocation ***rate*** $\frac{1}{n}\mathbb{H}(M|Z^n)$ must be arbitrarily close to the entropy ***rate*** of the message $\frac{1}{n}\mathbb{H}(M)$, for sufficiently large codeword length n.

With this relaxed security constraint, it can be shown that it exists codes, called ***wiretap codes***, that asymptotically ensure both reliability, i.e., arbitrarily small decoding probability error at Bob, and secrecy, i.e., the amount of (or the rate of) information leakage at Eve vanishes. However, the practical construction of these codes is arduous as mentioned in section 2.6.

The ***secrecy capacity*** is the supremum of the transmission rates that respect the above conditions. It is positive whenever Eve's observation is ***noisier*** than Bob's one. In other words, if Bob's channel induces less errors than Eve's channel, Bob should still be able to recover messages using a channel code. On the opposite, Eve should be left with a list of possible codewords and messages. Asymptotic perfect secrecy is achieved if this list covers the entire set of messages and their probability given that the received codeword is roughly uniform.

In the following, two definitions of secrecy, that use the concept of equivocation rate instead of the exact equivocation, are given.

Strong secrecy
Strong secrecy was introduced by Csiszar and implies asymptotic statistical independence between the message M and Eve's observation Z^n, when the codeword length n goes to infinity, i.e.,:

$$\lim_{n\to\infty} \mathbb{I}(M;Z^n) = 0. \tag{2.11}$$

Equation (2.11) imposes the amount of information leaked to Eve to vanish for sufficiently long codeword's length n. This definition of secrecy is less stringent than the perfect secrecy notion where it is imposed that the information leaked to Eve is strictly zero.

Weak secrecy
Weak secrecy, introduced by Wyner, only requires the rate of information leaked to Eve to vanish for sufficiently long codeword length n, i.e.,:

$$\lim_{n\to\infty} \frac{1}{n}\mathbb{I}(M;Z^n) = 0. \tag{2.12}$$

In particular, the weak secrecy condition is less stringent that the strong secrecy condition, since it is satisfied as soon as $\mathbb{I}(M;Z^n)$ grows sub-linearly with n. However, the amount of leaked information may go to infinity with a scheme that respects weak secrecy only.

Whether a strong or a wear secrecy criteria is assumed, Wyner's approach requires Eve's channel being *noisier* than Bob's channel. To meet this assumption, channel coding techniques can be applied as presented in next chapters.

2.5 Secrecy capacity characterization of the wiretap channel

Previous sections 2.2, 2.3, and 2.4 respectively present the information-theoretic mathematical tools, the notion of channel capacity, and different definitions of secrecy. The aim of this section is to provide

the necessary characterization of the secrecy capacity for the system studied in next chapters. As it will be explained, a block-fading communication in the presence of passive eavesdropper(s) is considered. First, this section presents the secrecy capacity of the general wiretap channel. Then, the more specific Gaussian wiretap channel is introduced, which allows one to discuss the secrecy capacity of the even more specific wireless channel.

2.5.1 Characterization of a secure communication in a wiretap channel

A discrete memoryless wiretap channel (WTC) $(\mathcal{X}, p_{YZ|X}, \mathcal{Y}, \mathcal{Z})$ consists of a finite input alphabet $\mathcal{X}$, two finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, and transition probabilities $p_{YZ|X}$. The marginal probabilities $p_{Y|X}$ and $p_{Z|X}$ define two DMCs, i.e., the DMC $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ being the main channel, and the DMC $(\mathcal{X}, p_{Z|X}, \mathcal{Z})$ being the eavesdropper channel.

A very important result was found in [23] by Liang *et. al.* They showed that a secure communication in a WTC can be characterized only by comparing the main channel $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ with the eavesdropper's channel $(\mathcal{X}, p_{Z|X}, \mathcal{Z})$. This is useful since it allows to define the secrecy capacity of Wyner's wiretap channel by comparing the two DMCs composing it, as explained below.

2.5.1.1 Wyner's wiretap channel is a physically degraded channel

A DMC $(\mathcal{X}, p_{Z|X}, \mathcal{Z})$ is physically degraded with respect to (w.r.t.) another DMC $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ if:

$$\forall (x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} : p_{YZ|X}(y, z|x) = p_{Z|Y}(z|y) p_{Y|X}(y|x), \tag{2.13}$$

for some transition probabilities $p_{Z|X}$. In other words, $(\mathcal{X}, p_{Z|X}, \mathcal{Z})$ is physically degraded with respect to $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ if $X \to Y \to Z$ forms a Markov chain.

From that, Wyner's WTC shown in Figure 2.4, also termed as degraded wiretap channel (DWTC), is simply a WTC where the eavesdropper's channel is physically degraded w.r.t. the main channel. As a consequence from Liang *et. al.* [23], one can directly compare the main and the eavesdropper channels of a DWTC to obtain a characterization of its secrecy capacity.

2.5.1.2 Channel code for the DWTC

The wiretap code is defined in this section. A $(2^{nR}, n)$ code C_n for a DWTC consists in:

- A message set $\mathcal{M} = \left[1, 2^{nR}\right]$, where R is an achievable transmission rate for the DMC, and is defined below, and n is the number of symbols.
- A source of local randomness at the encoder.
- An encoding function $f : \mathcal{M} \to \mathcal{X}^n$, that maps a message m and a realization of the local randomness r to a codeword x^n with n symbols.
- A decoding function $g : \mathcal{Y}^n \to M \cup \{e\}$, that maps each channel outputs y^n to a message $\hat{m} \in \mathcal{M}$ or an error message e.

It is assumed that a $(2^{nR}, n)$ code C_n for a DWTC is known at Alice, Bob, and Eve. However, the realizations of the source of randomness, used for encoding, are only known at Alice.
The reliability performance of the code C_n is measured in terms of average probability of error:

$$\mathbf{P}_e(C_n) = \mathbb{P}\left[\hat{M} \neq M | C_n\right]. \tag{2.14}$$

The secrecy performance of the code C_n is measured in terms of information leakage to the eavesdropper:

$$\mathbf{L}(C_n) = \mathbb{I}(M; Z^n | C_n), \tag{2.15}$$

or equivalently, in terms of the equivocation, i.e., the uncertainty at Eve:

$$\mathbf{E}(C_n) = \mathbb{H}(M|Z^n, C_n)\,. \tag{2.16}$$

Equation (2.15) measures the information leaked to Eve, while (2.16) measures the uncertainty at Eve.

2.5.1.3 Rate-equivocation pair for the DWTC

The rate-equivocation pair's definition allows to find an expression of the secrecy capacity of a DWTC. A rate R is an achievable transmission rate, i.e., it allows one to provide reliability at the legitimate receiver. An equivocation rate R_e is a rate allowing to provide secrecy from the eavesdropper. There are two definitions of rate-equivocation pair depending on whether a weak or a strong secrecy constraint is considered.

Weak rate-equivocation pair
A weak rate-equivocation pair (R, R_e) is achievable for a DWTC $(\mathcal{X}, p_{YZ|X}, \mathcal{Y}, \mathcal{Z})$ if there exists a sequence of $(2^{nR}, n)$ codes $\{C_n\}_{n\geq 1}$, such that:

$$\lim_{n\to\infty} \mathbf{P}_e(C_n) = 0 \qquad \Rightarrow \qquad \text{reliability condition} \tag{2.17a}$$

$$\lim_{n\to\infty} \frac{1}{n}\mathbf{E}(C_n) \geq R_e \qquad \Rightarrow \qquad \text{weak secrecy condition} \tag{2.17b}$$

From that, the weak rate-equivocation region of a DWTC is defined as the set of weak rate-equivocation pairs that are achievable, i.e.,:

$$\mathcal{R}^{\mathrm{DWTC}} = \{(R, R_e) : (R, R_e) \text{ is achievable}\}. \tag{2.18}$$

The weak secrecy capacity of a DWTC is defined as the supremum of the rates achieving simultaneously reliability and secrecy, i.e.,:

$$C_s^{\mathrm{DWTC}} = \sup_R \{R : (R, R) \in \mathcal{R}^{\mathrm{DWTC}}\}. \tag{2.19}$$

Strong rate-equivocation pair
A strong rate-equivocation pair (R, R_e) is achievable for a DWTC $(\mathcal{X}, p_{YZ|X}, \mathcal{Y}, \mathcal{Z})$ if there exists a sequence of $(2^{nR}, n)$ codes $\{C_n\}_{n\geq 1}$, such that:

$$\lim_{n\to\infty} \mathbf{P}_e(C_n) = 0 \qquad \Rightarrow \qquad \text{reliability condition} \tag{2.20a}$$

$$\lim_{n\to\infty} (\mathbf{E}(C_n) - nR_e) \geq 0 \qquad \Rightarrow \qquad \text{strong secrecy condition} \tag{2.20b}$$

From that, the strong rate-equivocation region of a DWTC is defined as:

$$\bar{\mathcal{R}}^{\mathrm{DWTC}} = \{(R, R_e) : (R, R_e) \text{ is achievable}\}. \tag{2.21}$$

The strong secrecy capacity of a DWTC is defined as:

$$\bar{C}_s^{\mathrm{DWTC}} = \sup_R \{R : (R, R) \in \bar{\mathcal{R}}^{\mathrm{DWTC}}\}. \tag{2.22}$$

Condition (2.20b) is more stringent than (2.17b) and would be preferable to be used to define the secrecy capacity of a DWTC. However, it is more difficult to design channel codes achieving the strong secrecy condition rather than weak secrecy condition.
Nevertheless, it can be shown that:

$$\mathcal{R}^{\mathrm{DWTC}} = \bar{\mathcal{R}}^{\mathrm{DWTC}}$$
$$C_s^{\mathrm{DWTC}} = \bar{C}_s^{\mathrm{DWTC}}.$$

It outlines that, even if it is more convenient (but more arduous) to design channel codes achieving strong secrecy rather than weak secrecy, only the weak secrecy condition can be used to characterize the secrecy capacity of a DWTC.
$\Rightarrow$ From the rate-equivocation pair definition (weak or strong), it follows:

- If the pair (R, R_e) is achievable, any pair (R, R'_e) with $R'_e \leq R_e$ is achievable as well. In particular, $(R, 0)$ is always achievable.
- If a pair (R, R_e) with $R_e = R$ is achievable, then R is said to be a ***full secrecy rate***.

From now, it can be stated that the reliability and the secrecy conditions must be simultaneously satisfied, which is not obvious. Indeed, reliability at the legitimate receiver is met if some redundancy is introduced. However, introducing too much redundancy is likely to affect secrecy. Nevertheless, Wyner's theorem shows that, with appropriate coding schemes, it is possible to control the balance between reliability and secrecy, and the equivocation-pair region of a DWTC $(\mathcal{X}, p_{Z|Y}p_{Y|X}, \mathcal{Y}, \mathcal{Z})$ can be exactly characterized with information-theoretic quantities. It follows:

$$\begin{aligned} 0 \leq R_e \leq R \leq \mathbb{I}(X;Y) \\ 0 \leq R_e \leq \mathbb{I}(X;Y|Z), \end{aligned} \tag{2.23}$$

where the first line of (2.23) is the reliability condition, and the second line of (2.23) is the secrecy condition.
A typical rate-equivocation region of a DWTC is shown in Figure 2.5.

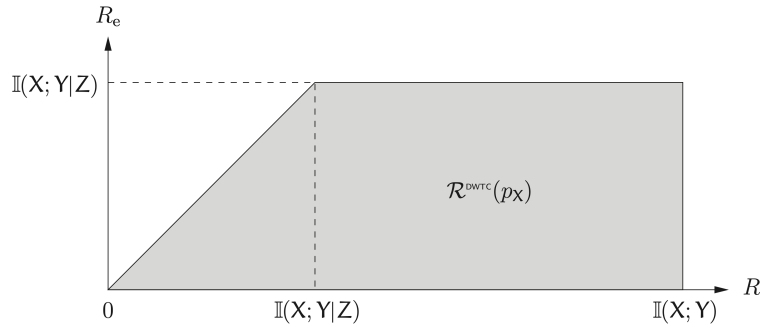

Figure 2.5: Rate-equivocation region of degraded wiretap channel, [1, Figure 3.5].

From Wyner's theorem, and looking at Figure 2.5, ***at rates $R \leq \mathbb{I}(X;Y|Z)$, it is possible to find channel codes ensuring full secrecy rates.*** At rates $R > \mathbb{I}(X;Y|Z)$, it is possible to transmit but the equivocation rate saturates, i.e., no more secrecy can be guaranteed above $R_e = \mathbb{I}(X;Y|Z)$. At full secrecy rate $R_e = R$, one obtains the secrecy capacity of the DWTC.

Remark 2.2: Full secrecy and secrecy capacity

The secrecy capacity rate is achieved when the equivocation rate is maximal. In other words, the secrecy capacity is the maximal transmission rate that achieves full secrecy.

From the above remark, the secrecy capacity of a DWTC $(\mathcal{X}, p_{Z|Y}p_{Y|X}, \mathcal{Y}, \mathcal{Z})$ is given by:

$$C_s^{\text{DWTC}} = \max_{p_X} \mathbb{I}(X;Y|Z) = \max_{p_X} \left(\mathbb{I}(X;Y) - \mathbb{I}(X;Z)\right) \tag{2.24}$$

By denoting Bob's channel capacity as $C_B = \max_{p_X} \mathbb{I}(X;Y)$, and Eve's channel capacity as $C_E = \max_{p_X} \mathbb{I}(X;Z)$, it follows:

$$\begin{aligned} C_s^{\text{DWTC}} &= \max_{p_X} \left(\mathbb{I}(X;Y) - \mathbb{I}(X;Z)\right) \\ &\geq \max_{p_X} \mathbb{I}(X;Y) - \max_{p_X} \mathbb{I}(X;Z) = C_B - C_E \end{aligned} \tag{2.25}$$

From (2.25), ***the secrecy capacity is at least as large as the difference between the main channel capacity and the eavesdropper's channel capacity.*** In other words, the secrecy capacity of a DWTC is at least as large as the difference between the rate of information conveyed to Bob and

the rate of information leaked at Eve. The inequality is strict if both the main and the eavesdropper channels are weakly symmetric. In that situation, it is shown in [24] that the secrecy capacity (2.25) becomes:

$$C_s^{\mathrm{DWTC}} = C_B - C_E \tag{2.26}$$

A DMC $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ is weakly symmetric if the rows of $p_{Y|X}$ are permutations of each other, and the columns of $\sum_{x\in\mathcal{X}} p_{Y|X}$ are independent of each other. Equation (2.26) is useful because many channels of interest are weakly symmetric.

2.5.2 Gaussian wiretap channel

In a Gaussian wiretap channel, the secrecy capacity admits an easily computable expression. In addition, Gaussian channels provide reasonable approximations of the physical layer encountered in many systems, and are therefore of great interest. It also builds the foundations to study the wireless channel model, which is of interest for this PhD work.

2.5.2.1 Single antenna system

The Gaussian wiretap channel (GWTC) is a channel model where the codewords transmitted by Alice are corrupted by additive white Gaussian noise (AWGN). The input-output relationship of the GWTC for a particular realization i, is given by:

$$\begin{aligned} y_i &= x_i + n_{B,i} \\ z_i &= x_i + n_{E,i}, \end{aligned} \tag{2.27}$$

where x_i is the i^{th} channel input coefficient, the noise at Bob and Eve is $n_{B,i}$ and $n_{E,i}$, respectively. The noise sources follow a normal distribution, i.e., $n_{B,i} \sim \mathbb{N}(0, \sigma_B^2)$ and $n_{E,i} \sim \mathbb{N}(0, \sigma_E^2)$. The input channel is subject to an average power constraint P:

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[x_i^2\right] \leq P,$$

where n is the codeword length. One key property of the GWTC compared to the more general WTC, is that either the eavesdropper's channel is physically degraded w.r.t. the legitimate receiver, if $\sigma_E^2 > \sigma_B^2$, or the legitimate receiver is physically degraded w.r.t. the eavesdropper, if $\sigma_B^2 > \sigma_E^2$. Consequently, the secrecy capacity of such a system is the difference between the main channel capacity and the eavesdropper channel capacity, i.e., equation (2.26) holds.

It has to be pointed out that the GWTC model presented in equation (2.27), considers real noise sources but can be extended to the complex GWTC. That is, the noises sources follow a zero mean circularly symmetric complex Gaussian (ZMCSCG) distribution, i.e., $n_{B,i} \sim \mathbb{CN}(0, \sigma_B^2)$ and $n_{E,i} \sim \mathbb{CN}(0, \sigma_E^2)$. In addition, one has to introduce the complex channel coefficients $h_B \in \mathbb{C}$ and $h_E \in \mathbb{C}$, respectively being the main and the eavesdropper's channel coefficients.

In [25], Leung-Yan-Cheong and Hellman showed that the secrecy capacity of the complex GWTC is found to be:

$$C_s = (C_B - C_E)^+ = \left(\log_2\left(1 + \frac{|h_B|^2 P}{\sigma_B^2}\right) - \log_2\left(1 + \frac{|h_E|^2 P}{\sigma_E^2}\right)\right)^+ \tag{2.28}$$

where $(x)^+ = \max(x, 0)$, $\frac{|h_B|^2 P}{\sigma_B^2}$ and $\frac{|h_E|^2 P}{\sigma_E^2}$ are the signal to noise ratios (SNRs) at Bob and Eve, respectively. From (2.28), secure communication is only possible if Bob's SNR is higher than Eve's SNR, i.e., Bob has a physical advantage compared to Eve.

2.5.2.2 Multiple-input multiple-output Gaussian wiretap channel

The secrecy capacity derived in section 2.5.2.1 and characterized by (2.28), can be extended to the multiple-input multiple-output (MIMO) GWTC system. In that situation, Alice, Bob, and Eve respectively possess N_A, N_B, and N_E antennas, as depicted in Figure 2.6.

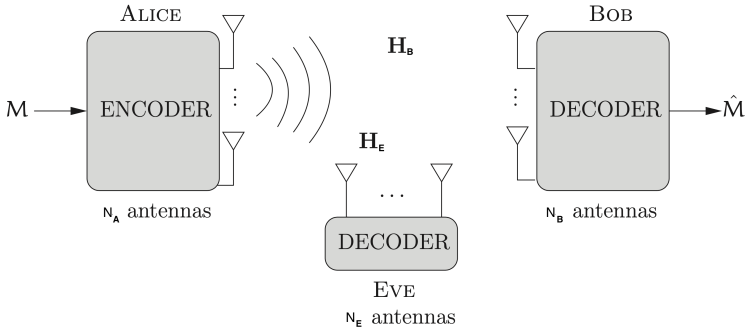

Figure 2.6: Communication scheme over MIMO Gaussian wiretap channel, [1, Figure 5.3].

This scenario also refers to a multiple-input multiple-output multi-eavesdropper (MIMOME) GWTC. In particular, Eve can be considered as a single eavesdropper with multiple colluding antennas, or as multiple cooperative eavesdroppers with one or multiple antenna(s).
The relationships between the inputs and outputs of the channels at time i are:

$$\begin{aligned} \mathbf{y}_i^{N_B} &= \mathbf{H_B}\mathbf{x}_i^{N_A} + \mathbf{n}_{B,i} \\ \mathbf{z}_i^{N_E} &= \mathbf{H_E}\mathbf{x}_i^{N_A} + \mathbf{n}_{E,i}, \end{aligned} \tag{2.29}$$

where $\mathbf{x}_i^{N_A} \in \mathbb{C}^{N_A \times 1}$ is the i^{th} channel input vector. $\mathbf{H_B} \in \mathbb{C}^{N_B \times N_A}$ and $\mathbf{H_E} \in \mathbb{C}^{N_E \times N_A}$ are respectively the main and the eavesdropper's channels, that are considered fixed during the transmission and known to both terminals. $\mathbf{y}_i^{N_B} \in \mathbb{C}^{N_B \times 1}$ is the i^{th} observation vector at Bob, and $\mathbf{z}_i^{N_E} \in \mathbb{C}^{N_E \times 1}$ is the i^{th} observation vector at Eve. The noise vectors $\mathbf{n}_{B,i} \in \mathbb{C}^{N_B \times 1}$ and $\mathbf{n}_{E,i} \in \mathbb{C}^{N_E \times 1}$ are ZMCSCG random vectors with covariance matrices $\mathbf{K}_B = \sigma_B^2 \mathbf{I}_{N_B}$ and $\mathbf{K}_E = \sigma_E^2 \mathbf{I}_{N_E}$, respectively. The noise processes $\{\mathbf{n}_{B,i}\}_{i\geq 1}$ and $\{\mathbf{n}_{E,i}\}_{i\geq 1}$ are independent and identically distributed (i.i.d.). The input channel is subject to an average power constraint P:

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[\left|\left|\mathbf{x}_i^{N_A}\right|\right|^2\right] \leq P.$$

In [26–28], the secrecy capacity of the Gaussian MIMO GWTC is found to be:

$$C_s^{\text{MIMO}} = \max\left(\log_2\left|\mathbf{I}_{N_B} + \frac{1}{\sigma_B^2}\mathbf{H_B}\mathbf{K}_X\mathbf{H_B}^H\right| - \log_2\left|\mathbf{I}_{N_E} + \frac{1}{\sigma_E^2}\mathbf{H_E}\mathbf{K}_X\mathbf{H_E}^H\right|\right). \tag{2.30}$$

The maximization in (2.30) is performed over all positive semi-definite input covariance matrices $\mathbf{K}_X$, such that $tr(\mathbf{K}_X) \leq P$.

2.5.3 Wireless channel

With all the above considerations taken into account, it is now possible to characterize the secrecy capacity of the scenario that is considered in this PhD work, namely, a wireless channel in the presence of a passive eavesdropper. The situation is depicted in Figure 2.7.

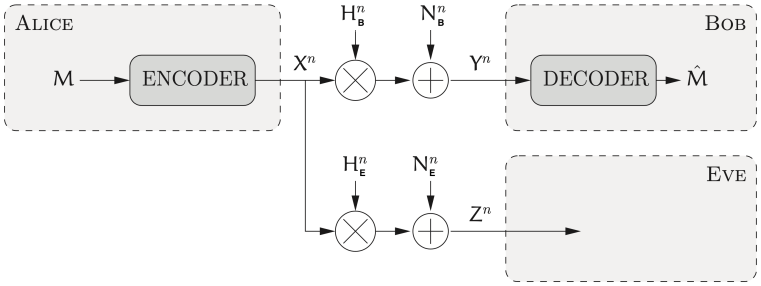

Figure 2.7: Communication scheme over a wireless channel, [1, Figure 5.5].

The relationships between the inputs and outputs of the channels at time i are:

$$\begin{aligned} y_i &= h_{\mathrm{B},i} x_i + n_{B,i} \\ z_i &= h_{\mathrm{E},i} x_i + n_{E,i}. \end{aligned} \tag{2.31}$$

The input of the channel is also subject to the power constraint P:

$$\frac{1}{n} \sum_{i=1}^{n} \mathbb{E}\left[|x_i|^2 \right] \leq P.$$

In this model, the channel between Alice and Bob (resp. between Alice and Eve) is the main *fading* channel (resp. eavesdropper *fading* channel). h_B and h_E are the complex coefficients at Bob and Eve, respectively. The gain at Bob (resp. at Eve) is $G_B = |h_B|^2$ (resp. $G_E = |h_E|^2$). n_B and n_E are the AWGNs at Bob and Eve, respectively. The noise processes $\{n_{B,i}\}_{i\geq 1}$ and $\{n_{E,i}\}_{i\geq 1}$ are i.i.d. complex Gaussian, with $n_{B,i} \sim \mathbb{CN}(0, \sigma_B^2)$ and $n_{E,i} \sim \mathbb{CN}(0, \sigma_E^2)$. It is assumed that $h_{B,i}$, $h_{E,i}$, $n_{B,i}$, $n_{E,i}$ are mutually independent.

In a wireless communication, *fading* changes over time due to variations in the structure of the medium or due to the relative movement of the transmitter to the receiver. The *coherence time* of the channel is the time interval over which the channel coefficients remain almost constant. The coherence time allows one to characterize fading.

Two parameters influence the secrecy capacity of a wireless channel:

- The fading model of the channel, related to the coherence time of the channel w.r.t. the duration of any single symbol from the codeword.
- The CSI knowledge at the transmitter side.

2.5.3.1 Fading models

Fast-fading
In this situation, the coherence time is of the order of the time required to send a single symbol. The fading coefficients change every $N = 1$ channel use and a codeword experiences many fading realizations since $N << n$. The transmitter is allowed a single channel use per coherence interval, and the information leaked to the eavesdropper can be consequently arbitrarily large.

Block-fading
In this situation, the time required to send a single symbol is much smaller than the coherence time. Nevertheless, a codeword of length n is assumed to experience many fading coefficients since the channel fading coefficients change every N channel uses, and $1 << N << n$.
This model is fundamentally different from the fast-fading channel. Indeed, in a block-fading environment, the coherence interval N is sufficiently large such that asymptotic coding results hold within each coherence interval.

The processes $\{h_{B,i}\}_{i\geq 1}$ and $\{h_{E,i}\}_{i\geq 1}$ are i.i.d., but for each realization $(h_{B,i}, h_{E,i})$, the relationships between the inputs and outputs of the channels are:

$$\begin{aligned} y_{i,j} &= h_{B,i}x_{i,j} + n_{B,i} \\ z_{i,j} &= h_{E,i}x_{i,j} + n_{E,i}, \end{aligned} \tag{2.32}$$

for $j \in [1, N] << n$, where N is assumed sufficiently large.

Quasi-static fading
The fading coefficients remain constant during the transmission of an entire codeword, i.e., $N = n$, but changes from one codeword to another. The coherence time is of the order of the time needed to send an entire codeword.

Throughout this manuscript, a block-fading channel model is adopted, as explained and motivated in chapter 4.

2.5.3.2 Secrecy capacity of block fading channels with passive eavesdroppers

The expression of the secrecy capacity differs depending on the CSI knowledge at the transmitter side. Indeed, if Alice knows the CSIs at Bob and Eve, i.e., full CSI knowledge, she can access to the instantaneous fading coefficients and therefore adapt the transmission rate accordingly, thanks to a power allocation procedure. However, if the eavesdropper is passive, as considered in this study, Alice does not have access to Eve's instantaneous fading gains, i.e., she only knows Bob's instantaneous fading gains. As a consequence, she is bounded to adopt a power allocation strategy that takes into account Bob's instantaneous fading coefficients only, in order to provide positive secrecy performances.

As a reminder, for the block-fading model, the transmitter can code within a coherence interval of length $N << n$, since N is assumed sufficiently large for coding results to hold. Therefore, the information leaked to the eavesdropper cannot exceed the information communicated to the legitimate receiver. Otherwise, no secrecy can be provided.
Let X^N be a coded sequence chosen randomly in the transmitter's codebook (of length $n >> N$) and sent during a coherence interval, and Z^N be the observation at Eve. In a block-fading environment, it holds:

$$\mathbb{I}\left(X^N; Z^N\right) \leq \mathbb{H}\left(X^N\right) < +\infty, \tag{2.33}$$

since X^N takes a finite number of values, which bounds the information that leaked at Eve.

In [29], Gopala *et. al.* demonstrate that the secrecy capacity of a block-fading WTC, with CSI at the transmitter about the legitimate receiver but no CSI about the eavesdropper, is given by, :

$$C_s = \max_{\gamma} \mathbb{E}_{G_B, G_E}\left[\left(\log_2\left(1 + \frac{\gamma(G_B)G_B}{\sigma_B^2}\right) - \log_2\left(1 + \frac{\gamma(G_B)G_E}{\sigma_E^2}\right)\right)^+\right], \tag{2.34}$$

where the power allocation function $\gamma : \mathbb{R}^+ \to \mathbb{R}^+$ is subject to $\mathbb{E}[\gamma(G_B)] \leq P$.
As expected, the power allocation function in (2.34) is applied on Bob's fading gains only. Equation (2.34) also shows that an optimization procedure is needed to achieve the secrecy capacity transmission rate. In addition, (2.34) is called the ***ergodic secrecy capacity.*** In order to construct a wiretap code, the key ideas are to code within each coherence interval in order to bound the information leaked to the eavesdropper, and to spread the codewords over many realizations of the eavesdropper's fading gains. It is interesting to note that the $(.)^+$ operator in (2.34) appears because the information leaked to the eavesdropper within each coherence interval is bounded. Equation (2.34) indicates that a positive secrecy capacity may not always be achieved if $\sigma_E^2 << \sigma_B^2$ and/or if G_B is too correlated with G_E. This therefore suggests that, if nothing is done on the channel, secure communications might not be possible.

2.6 Coding for secrecy

Section 2.5 presents mathematical expressions of the secrecy capacity of wiretap channels, which is defined as the maximal transmission rate that ensures simultaneously secrecy and reliability. In particular, Wyner's theorem proves that it is always possible to achieve the secrecy capacity rate by using appropriate codes, called channel codes or wiretap codes. Thanks to this theory, it is not necessary to first design the actual code in order to know the maximal rate. However, in practice, to communicate in a secure and reliable way, such codes need to be designed, which appears to be a challenging task. Indeed, wiretap codes should jointly provide reliability at the legitimate receiver and secrecy, preferably strong over weak, from the eavesdropper. On one hand, reliability is provided by the introduction of redundancy to mitigate the stochastic effect of the noise and the propagation medium. On the other hand, if too much redundancy is introduced, the secrecy is affected. In addition, since there is no restriction on Eve's computational abilities, there is no simple metric to evaluate the performance of a wiretap code. On the opposite, for capacity-achieving-only codes, where no secrecy condition is imposed, the bit error rate (BER) can be used to assess the code's performances. This considerably eases the design of secret-key distillation strategies, used in Shannon's model of perfect secrecy, since reliability and secrecy can be handled separately.

To summarize, two properties are desirable for the wiretap codes.
First, several codewords should represent the same message in order to provide reliability at Bob. In order to do so, the encoder should select a codeword from a set of codewords, i.e., from a ***bin*** of codewords, representing the same message. That is, a wiretap code should have a ***binning structure***, also termed as a ***nested structure***.
Second, in order to confuse the eavesdropper, i.e., to provide secrecy, the encoder should introduce local randomness. In other words, the encoder should randomly select the codeword from the bin to represent the message. The situation is depicted in Figure 2.8.

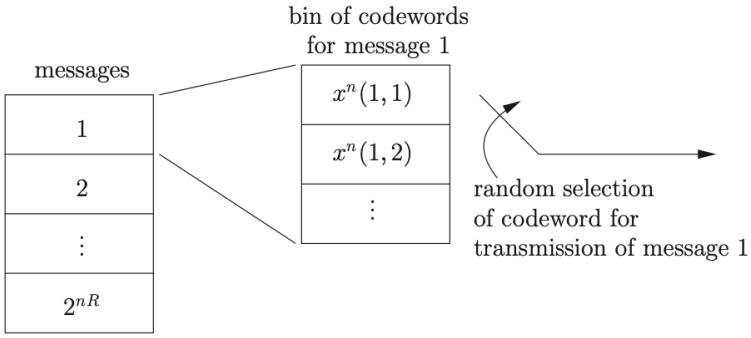

Figure 2.8: Binning structure and encoding of a wiretap code, [1, Figure 3.8].

Practically, for a WTC $(\mathcal{X}, p_{YZ|X}, \mathcal{Y}, \mathcal{Z})$, one has to partition the codebook containing 2^{nR+nR_d} codewords into 2^{nR} bins of 2^{nR_d} codewords each. The sub-codes are chosen to ensure reliability at Bob. In addition, it can be proven that each sub-code is implicitly a capacity-achieving code for the eavesdropper's channel since its rate R_d respects:

$$R_d = \mathbb{I}(X;Z) - \delta(\epsilon),\ \forall \epsilon > 0. \tag{2.35}$$

In [30], a sufficient condition for a coding scheme that guarantees secrecy w.r.t. an eavesdropper is provided. Authors show that, if each sub-code in the set $\{C_i\}_{2^{nR}}$ stems for a sequence of capacity-achieving codes over the eavesdropper's channel as n goes to infinity, then:

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{I}(M; Z^n) = 0. \tag{2.36}$$

Equation (2.36) is a weak-secrecy condition, but suggests that one needs to design channel codes based on nested codes and capacity-achieving codes over Eve's channel. However, practical wiretap code

constructions are only known for few channels.

In [31], polar wiretap codes are proposed for binary input channels. Authors show that these codes are secrecy-achieving for long codeword lengths. Authors in [30] provide the construction of low density parity check (LDPC) codes for binary erasure and symmetric channels, and for Gaussian channels with binary inputs. Study [32] proposes to design lattice codes for the Gaussian channel with input power constraint. In addition, authors in [32] prove that their codes achieve strong secrecy for any message, [33].

The research on wiretap codes is still on-going and while it is out-of-the scope of the study presented in this manuscript, it is interesting to note that, to design a suitable wiretap code, the system needs to know the secrecy rate. So, any physical technique that aims to ensure Eve's channel being *noisier* than Bob's channel, should also allow Alice to estimate the secrecy rate for which the wiretap code should be designed.

2.7 Metrics for physical layer security

One key element when designing a secure communication is the determination of a suitable metric that accurately reflects the security performance of the scheme, [3, 34]. As a reminder, Wyner's model of secrecy, also known as key-less approach or SINR-based approach, is considered in this manuscript. Several SINR-based metrics are thus presented below.

2.7.1 Secrecy capacity

The notion of secrecy capacity is defined in section 2.5. As a reminder, the secrecy capacity is the maximum achievable secrecy rate over every input distributions of the transmitted signal X. For wireless channel, the secrecy capacity is defined as:

$$C_s = C_B - C_E, \tag{2.37}$$

where C_B and C_E are respectively the main and the eavesdropper's channel capacities. Depending on the fading environment, the secrecy capacity can be ergodic or not. Indeed, in fast-fading or block-fading environments, an ergodic secrecy capacity is more likely to be characterized. In quasi-static fading environments, the instantaneous secrecy capacity is adopted. The secrecy capacity only gives achievable bounds on the secure transmission rate. It does not necessarily reflect the actual level of secrecy in practical transceiver designs, [34].

2.7.2 Secrecy outage probability

The secrecy capacity is extended to secrecy outage probability in [35]. The secrecy outage probability is a random variable that takes into account the fading in wireless environments. It gives the probability that the instantaneous secrecy capacity becomes lower than a given secrecy rate threshold R_s^t:

$$P_{\text{out}}(R_s^t) = P(C_s < R_s^t). \tag{2.38}$$

In a classical communication with a fixed rate, if the channel capacity drops below the rate, errors occur and reliability of the communication thus decreases. In a PLS scheme with a communication operating at a fixed secrecy rate, both errors and leakage can occur. While the secrecy outage probability reflects those effects, it has three main drawbacks, [3]:

- When outage occurs, it does not quantify the amount of leakage to Eve.
- It does not provide any insight on Eve's capability to decode the message successfully.
- It cannot be linked to QoS requirements of applications and services.

2.7.3 Tight secrecy outage probability

The secrecy outage probability definition (2.38) mainly focuses on evaluating the probability that the secrecy capacity drops below a given secrecy rate. It does not always guarantee secrecy, especially when the CSI is not known at the transmitter side, [3]. To address this issue, the tight secrecy outage probability (TSOP) is proposed in [36]. It constraints the information leakage to Eve while guaranteeing a certain amount of information to Bob.

$$P_{\text{out}}(R_s) = 1 - P\left(\{C_B \geq R_B\} \bigcap \{C_E < R_E\}\right), \tag{2.39}$$

where R_B and R_E are the rate constraints at Bob and Eve, respectively.

2.7.4 ϵ-achievable secrecy rate

Another metric that can characterize the outage is the ϵ-achievable secrecy rate. For any $0 \leq \epsilon \leq 1$, the ϵ-achievable secrecy rate corresponds to the rate that is achievable securely while keeping an outage probability under ϵ, i.e., $100\epsilon\%$ of the realizations lead to lower secrecy values, [37]. Consequently, high ϵ-achievable secrecy rates are desired for low ϵ values if one aims to restrict the leakage at the eavesdropper while guaranteeing a certain amount of information rate conveyed to Bob.

2.7.5 Secrecy throughput

It gives a measure of the average confidential transmission rate:

$$ST = R_s(1 - P_{\text{out}}(R_s)). \tag{2.40}$$

2.7.6 Practical metrics

The secrecy capacity is a common metric to provide security estimation in a communication. However, it is difficult to measure in practical communication scenarios where non-Gaussian codes and finite block length are used. To have more insight on the practical secrecy performance, several practical metrics are introduced.

Security gap
The security gap is defined in [38, 39]. It does not address the information-theoretic measure, but quantifies the gap between Bob's SNR to achieve reliable decoding for a given service, and Eve's SNR that is not sufficient to achieve reliable decoding for the same service:

$$\mathrm{S}_g = \mathrm{SNR}^B_{min} - \mathrm{SNR}^E_{max}. \tag{2.41}$$

This metric depends is unpractical in passive eavesdropping scenario since Eve's SNR as well as her decoding capabilities need to be known.

Bit error rate
A cost function depending on the BER can be minimized. If the BER at Bob and Eve is respectively denoted as BER_B and BER_E, it comes:

$$\text{cost} = \frac{BER_B}{\min(BER_E)}. \tag{2.42}$$

The issue with BER-based metrics is that it does not satisfy the secrecy condition (weak or strong). Indeed, weak (resp. strong) secrecy requires that the rate of information leaked (resp. amount of information leaked) to Eve must asymptotically vanish to zero as the length of the codeword goes to infinity. This implies that the asymptotic decoding error probability at Eve must approach unity as the number of messages goes to infinity. However, the decoding error probability can never be greater than 0.5, i.e., there is at least half of the information that always leaks to Eve, [34]. In addition, as for the security gap metric, Eve's SNR as well as her decoding capabilities need to be known.

Secure packet error rate
The secure packet error rate (SPER) is introduced in [40]. It is equal to the ratio of erroneously received packets at Bob (respectively Eve) to the total number of packets sent to Bob (respectively to Eve). It is a cross-layer metric that allows to take into account the effects of upper layer functionalities, that is linked and related to QoS requirements, and that can be measured by wireless receivers. To idea is to make sure that Eve operates above a certain SPER level when her SNR is arbitrarily large, while maintaining Bob's SPER below a given threshold, [34].

Conclusion on practical metrics
Practical secrecy metrics can be measured to gain more insight on the actual level of secrecy in scenarios where non-Gaussian codes and finite block length are used. However, these metrics do not satisfy the secrecy condition (weak or strong). As an example, when the BER is considered as performance metric, there is at best half of the information that leaked to Eve. In addition, it requires the knowledge at the transmitter side of Eve's decoding capabilities as well as Eve's SNR, which is therefore unsuitable in passive eavesdropping situations, as considered in this PhD work.

2.8 Conclusion

In this chapter, the fundamentals of information-theoretic security are presented. It allows one to mathematically quantify the level of secrecy in a communication. In particular, it is shown that Wyner's model of secrecy is adopted since a secure communication between Alice and Bob without secret-key exchange is considered. The wiretap channel is therefore studied. It has to be pointed out that the information-theoretic approach of security aims to describe the fundamental limits of communication systems, without relying on practical limitations.

The notion of secrecy capacity for the wiretap channel is investigated. The secrecy capacity is defined as the maximal transmission rate that achieves full secrecy (in the weak or strong sense). In order to communicate at this rate, one needs to design channel codes, called wiretap codes, that simultaneously respect the reliability and the secrecy conditions. In other words, these codes must allow Bob to decode the data with an arbitrarily low probability of error, while preventing Eve to correctly decode the data. In his theorem, Wyner proves that, with a proper design, it is always possible to find wiretap codes that achieve the secrecy capacity. The secrecy capacity is then characterized as the difference between Bob and Eve channel's capacities. Consequently, a positive secure communication rate can be achieved by providing a physical advantage to the main channel over the eavesdropper's channel. From that, a mathematical formulation of the secrecy capacity of a wireless block-fading channel with main CSI knowledge at the transmitter but no eavesdropper's CSI knowledge is given in equation (2.34), which is the system model that is considered in the following of this manuscript. In particular, it shows that a power allocation optimization procedure needs to be resolved at the transmitter side to achieve the secrecy capacity rate in such a system.

Consequently, the following of this PhD work aims to design a PLS scheme (on top of which a wiretap code is to be designed) that ensures an advantage to Bob's channel over Eve's channel, while considering worst-case assumptions regarding the eavesdropper, such as an arbitrarily large SNR at Eve, for instance. Furthermore, from parameters assumed to be known at Alice, such as Bob's SNR for instance, Alice must be able to know the secrecy rate of the communication.

Section 2.7 presents several SINR-based PLS metrics. It is shown that the ergodic secrecy capacity is a suitable metric in a block-fading environment. This metric is therefore used to quantify the secrecy of the implemented PLS scheme in next chapters. In addition, outage is convenient to be considered since it occurs when the instantaneous secrecy capacity is lower than the rate at which Alice actually communicates, i.e., the ergodic secrecy capacity. Also, it is seen that, in a block-fading environment, the

transmitter can code within a channel coherence interval, which implies that the amount of information leaked to the eavesdropper is bounded. As a consequence, it is chosen to study the ϵ-achievable secrecy rate as outage metric.

Next chapter 3 draws a state-of-the-art of the SINR-based PLS techniques, i.e., the PLS techniques based on Wyner's model of secrecy, which aims to provide an advantage to Bob's channel w.r.t. Eve's channel. The system model considered in this study is presented in chapter 4. The performances of the communication scheme, in terms of ergodic secrecy capacity and ϵ-achievable secrecy rate, are assessed in chapters 5 and 6.

Figure 2.9 shows a visual abstract of this manuscript.

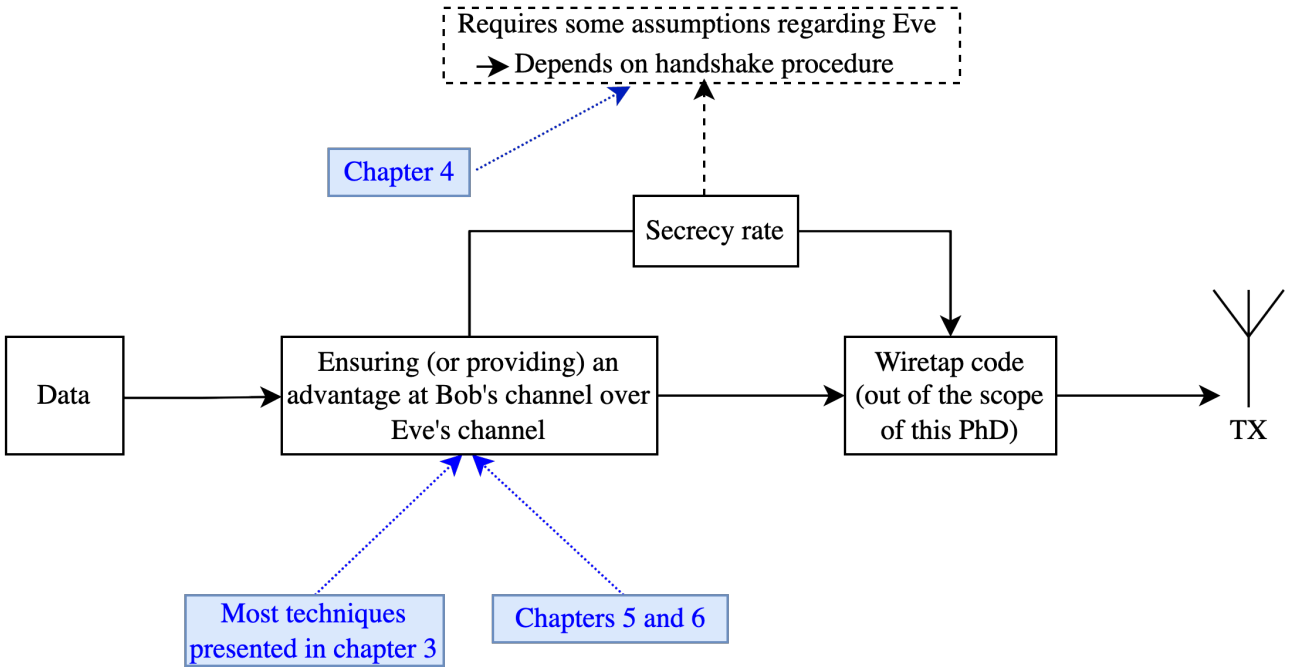

Figure 2.9: Visual abstract of the PhD work

3 | Physical Layer Security Techniques: a State-of-the-Art

Contents

3.1 Introduction

Chapter 2 has highlighted how a degraded wiretap channel can support a secret communication. So, to provide an advantage to Bob's channel over Eve's channel, two approaches can be conducted, namely, ***channel-based adaptation transmissions*** and ***artificial signals injection***. Each approach can be implemented in the time, frequency, or space domain, or any combination thereof, [3, 15, 41]. The aim of this chapter 3 is therefore to draw a state-of-the-art of existing techniques that introduce a physical advantage to Bob's channel over Eve's channel. As a reminder, the study focuses on a point-to-point secure communication. Therefore, the presented state-of-the-art only involves single-node communication PLS techniques. Furthermore, it is considered that Alice aims to communicate with a single legitimate user such that the state-of-the-art mainly presents single-users PLS techniques.

To implement these techniques, Alice must have some knowledge about the main CSI to provide secrecy. However, in practical scenarios, the transmitter can never obtain a perfect CSI estimation. This

motivates the study of a practical communication scheme where Alice misestimates Bob's CSI to some extent. The physical reasons of imperfect main CSI estimation are outlined in the following of this chapter, and a state-of-the-art of PLS techniques involving imperfect main CSI knowledge is also drawn.

Figure 3.1 shows a classification of the SINR-based PLS techniques against passive eavesdropping that are reviewed in this chapter. Choosing between channel-based adaptation and AN injection depends mainly whether or not Alice knows Eve's CSI, respectively. Then, the implementation in time/frequency/spatial domains is related to several factors including available hardware, modulation schemes of the chosen communication standard, available propagation channels...

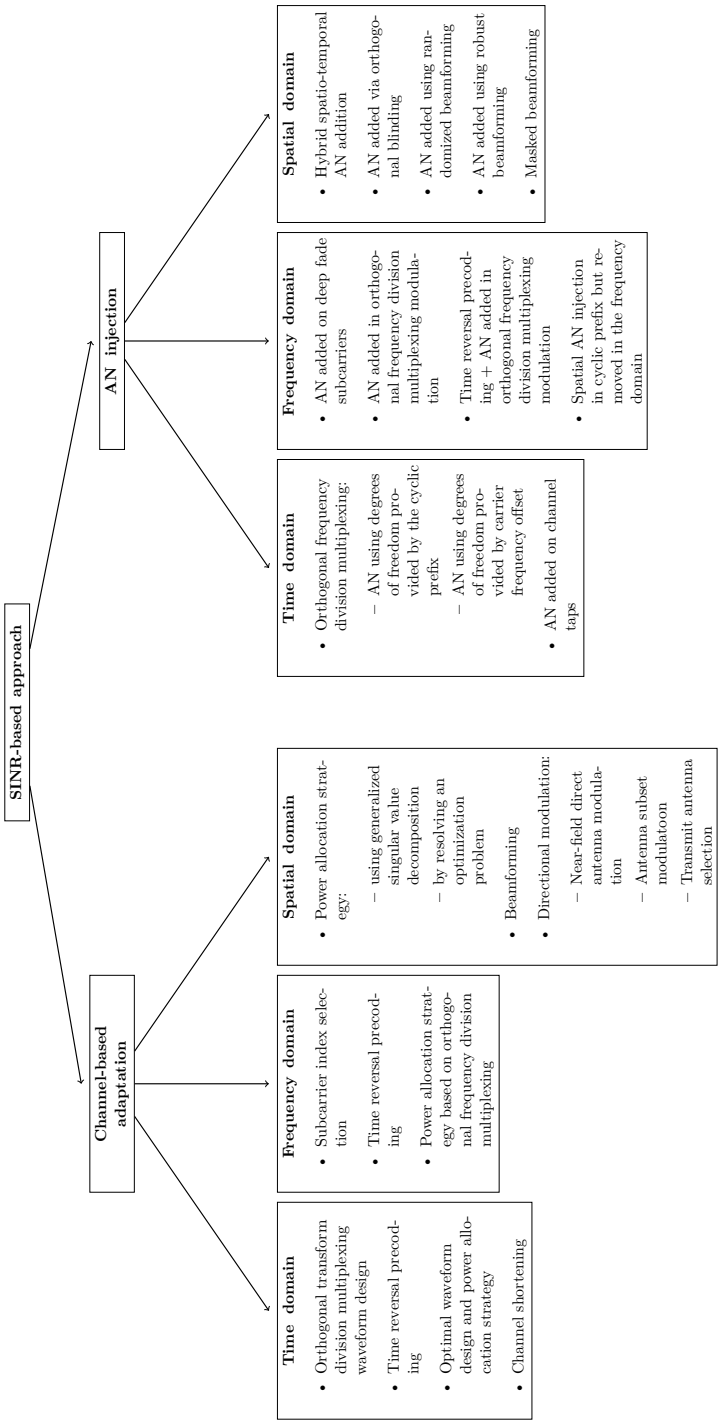

Figure 3.1: Classification of PLS techniques against passive eavesdropping

3.2 Channel-based adaptation techniques

3.2.1 Introduction

Channel-based adaptation secrecy schemes were first introduced from an information-theoretic perspective in [29, 35, 42]. In these works, it was proven that positive secrecy rate (SR) can be obtained even if, on average, the channel between Alice and Bob is a degraded version of the one between Alice and Eve, by optimizing or adapting at the transmitter side the communication parameters. Indeed, since Bob and Eve are assumed to experience different fading, there are always times where Bob's fading gains are larger than Eve's ones. In doing so, the precoded signal can be optimized for Bob's channel but not for Eve's one, according to the wireless fading conditions. Adaptive transmission-based techniques require at least some CSI knowledge at the transmitter. This is achieved by the exchange of feedbacks between Alice and Bob, e.g., pilots in time division duplex (TDD) systems, or explicit feedbacks in frequency division duplex (FDD) systems. Figure 3.2 shows a typical handshake procedure for the establishment of a secure channel-based adaption communication.

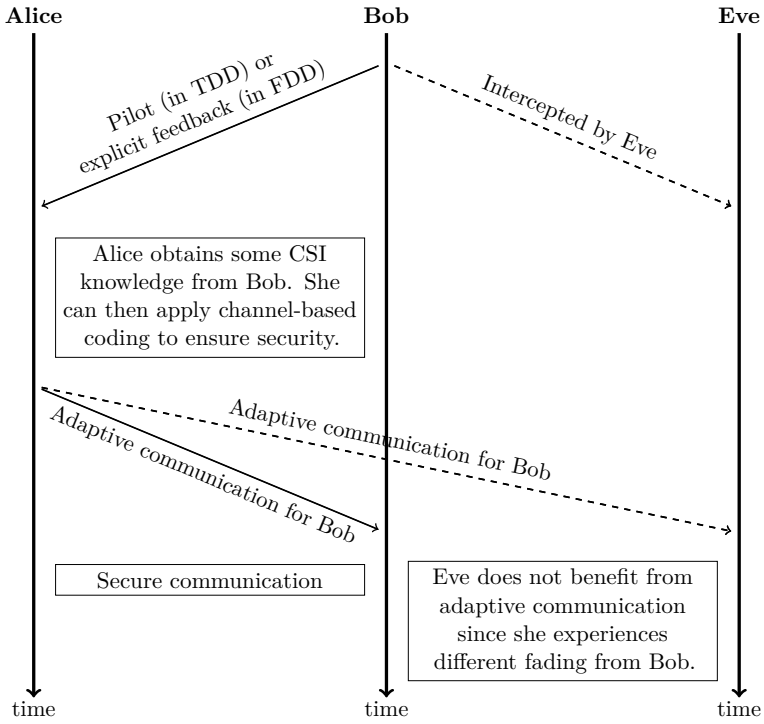

Figure 3.2: Typical handshake for channel-based adaptive transmission against eavesdropping, [3, Figure 5]

The merits of the channel-based adaptation techniques are the following, [3]:

- It is energy efficient, it increases Bob's reliability, and it enhances the secrecy of the communication.
- It can be deployed in FDD, TDD, or hybrid division duplex systems.
- Even if Eve is able to intercept the feedback, i.e., some CSI information leaks at Eve, it always exists designs that do not allow Eve to achieve Bob's performance. This ensures positive secrecy capacity, and therefore PLS.
- These techniques allow Bob to implement low-complexity receiving structures, which is suitable for devices with low capabilities, such as in IoT systems.

Channel-based adaptation transmission schemes can be implemented in time, frequency, or space domains, as explained below.

3.2.2 Time domain

In time domain (TD), the information is transmitted over one carrier frequency and at different time slots. Security is obtained by designing specific waveforms. Works [37, 42–44] show the power allocation strategies that achieve weak secrecy condition at a certain rate over wireless fading channels, by adapting the transmission to the channel condition, [3].

In [45], authors design a waveform that minimizes the likelihood that a message is eavesdropped. They find the optimum waveform and transmit energy to minimize Eve's SINR while maximizing Bob's SINR. In [46, 47], a secure orthogonal transform division multiplexing (OTDM) waveform design is presented. The idea is to determine Bob's channel basis functions via OTDM transform, and use them to modulate and demodulate the data symbols. This differs from classical exponential basis function, generated by inverse fast Fourier transform (IFFT) and fast Fourier transform (FFT) as in orthogonal frequency-division multiplexing (OFDM). Authors consider a SISO system with passive eavesdropper. By using OTDM basis functions, authors prove that the security gap between Bob and Eve, which is observed via differences in BERs, is significantly enhanced. It is also more robust against channel impairments. In [47], it is also shown that this waveform design reduces the peak-to-average power ratio (PAPR) compared to OFDM. In [48], a power adaptation scheme is proposed in SISO wireless fading environments. Authors formulate the security-driven power adaptation problem for throughput maximization over fading channels. The normalized average throughput is used as performance metric. The superiority of the scheme is compared over water-filling. In [49], a channel shortening design is proposed for TD OFDM systems, in the presence of an active or passive eavesdropper. The underlying idea is to make the length of the effective channel at Bob lower than the cyclic prefix (CP), while the length of the eavesdropper's channel is greater than the CP. This is achieved thanks to the design of filters at the transmitter side. It concentrates the energy of Bob's channel into a window of length being just one sample more than the length of the CP, while the energy of the tails of the filter is minimized outside the window to prevent Eve from correctly decoding. It is proven that the scheme is robust against channel imperfections and can provide reliability beside enhancing security. However, an optimization problem is proposed to design the filter and only the BER is used as a performance metric.

Another approach to increase the SINR at the intended position is to implement time reversal (TR) pre-filtering [50–53]. TR can be implemented in the time or frequency domains. In TD, TR is achieved by up/downsampling the signal and then applying a matched filter (MF). The up/down sampling factor is denoted as the back-of-rate (BOR) factor, [54–56]. The information signal is then filtered by the time-reversed version of the main channel before being transmitted. In doing so, thanks to the TR precoding, the transmitted data benefits from a focusing gain at the intended receiver position only, thereby naturally offering intrinsic anti-eavesdropping capabilities, [52]. The issue is that the received signal quality is improved at the expense of spectral efficiency, [50].

The techniques presented in this section either propose optimization procedures to provide Bob with a physical advantage over Eve, or use security gap metrics to quantify the secrecy of the scheme. Because of that, the transmitter cannot be a priori aware of the secure rate over which securely communicating with the legitimate receiver. In addition, security gap metrics do not respect the secrecy conditions (weak or strong) since, in the worst case scenario, Eve's BER is equal to 0.5, i.e., half of the information leaked to the eavesdropper.

3.2.3 Frequency domain

In the frequency domain (FD), the signal is sent in one time slot but over multiple subcarrier frequencies. In this situation, the PLS techniques are mainly related to adaptation of the communication parameters in multi-carrier systems, such as in OFDM for instance, [3].

OFDM modulation is first introduced in [57, 58]. It is a modulation scheme that is used in current technologies, such as in Long Term Evolution (LTE) or in 5G networks, [15]. The principle is to divide the bandwidth of a signal that suffers from frequency selective channel into multiple sub-bands. The sub-bands are designed in such a way that their bandwidths are strictly lower than the channel coherence bandwidth. In doing so, the sub-channels experience flat fading. From that, the problem of having a frequency selective channel is replaced to having multiple parallel flat-fading sub-channels, which eases the mitigation and equalization processes. The sub-channels are transmitted in parallel, therefore increasing the spectral efficiency of the system. To avoid inter-symbol interference (ISI) and inter-carrier interference (ICI), a CP, i.e., an extension of the signal, is inserted in TD between successive OFDM symbols, whose length must be at least equal to the delay spread of the channel, [59–61]. Figure 3.3 represents an OFDM signal in time and frequency domains.

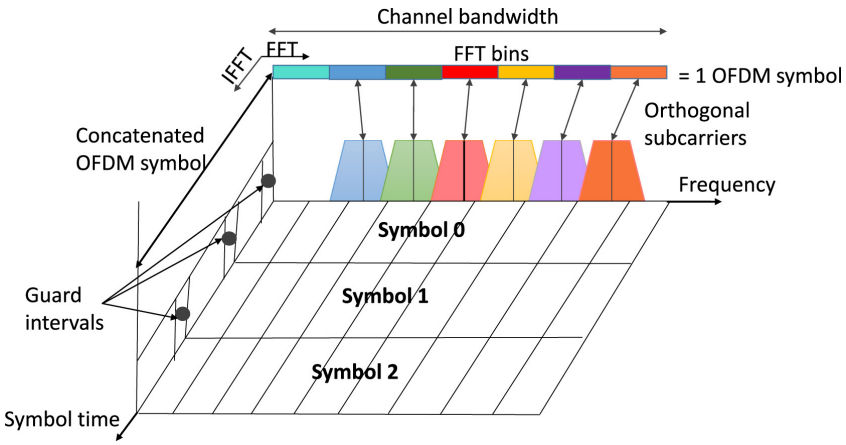

Figure 3.3: Time-frequency representation of an OFDM signal, [15, Figure 7]

First, Liu and Trappe studied the capacity of an OFDM channel. They demonstrate that, when the sub-channels are corrupted by AWGN, the optimal power allocation strategy that maximizes the secrecy rate of the communication is similar to the water-filling strategy, [62, Chapter 1]. In the following, several PLS techniques using channel-based adaptation strategies in the FD are described.

In [63], the achievable information-theoretic secrecy rate of several precoding techniques is studied, such as inputs using water-filling, generalized singular value decomposition (GSVD), or optimal power allocation with independent inputs. Authors allow Eve to use sophisticated decoding structure compared to Bob. However, a full CSI knowledge is assumed at Alice, i.e., she knows Bob and Eve instantaneous CSIs. In addition, the secrecy capacity is formulated as a maximization problem, but adopts a simple expression in the high SNR region. In [64], power and rates optimization schemes are considered to achieve security in K parallel channels. In the power optimization scheme, the message is encoded and is then split over the K subchannels. In the rate optimization scheme, the secret message is split in K sub-messages that are transmitted onto different sub-channels. The latter scheme requires multiple encoder/decoders pairs, while the first scheme only requires one encoder/decoder pair. Authors use the secrecy outage probability as performance metric to determine the optimal power/rate allocation strategy over the different sub-channels. Authors compare the optimal strategy performances, obtained via optimization procedure, with the water-filling, equal power, and single channel power allocation strategies. The technique requires full main CSI and partial eavesdropper's CSI at the transmitter side. In [65, 66], subcarrier index selection techniques are presented. The underlying idea is to use only the strongest fading gains to convey the transmitted data. The main issue is that it reduces the spectral efficiency of the scheme since several subcarriers are unused. Both schemes use the secrecy gap in terms of BER differences between Bob and Eve as performance metric. In [65], an approximated average BER expression at Bob, and an exact averaged BER expression at Eve are obtained. No closed-form expressions of the BERs are derived in [66]. Authors in [67] independently transmit, over uncorrelated fading sub-channels, the in-phase and quadrature components of phase shift keying

(PSK) or quadrature amplitude modulation (QAM) modulated signals. They adopt a channel-based interleaving pattern to introduce more frequency diversity gain at Bob than at Eve, therefore leading to security enhancement. The difference between Bob and Eve's BERs is also used as performance metric, and is shown via simulation only. Study [68] presents a PLS technique where the main channel is pre-compensated before data transmission according to the main CSI. Authors use the difference of BERs as a performance metric.

In [69], the equivalence between TD TR precoding and FD TR precoding is assessed. The FD TR precoding is implemented thanks to an OFDM modulation. In order to benefit from TR focusing effect, each modulated symbol is duplicated (or spread) and transmitted over BOR sub-channels, introducing frequency diversity. The BOR factor in the FD is equivalent to the up/downsampling factor in the TD. In the FD, the transmitted signal is filtered with the hermitian transpose of the main channel frequency response. That is, Alice needs to be aware of Bob's instantaneous CSI to pre-compensate the transmitted signal. Considering a perfect main CSI knowledge at Alice, when the transmitted signal passes through Bob's channel, each sub-channel component will be affected by a real gain thanks to the precoding. Since Eve experiences different fading from Bob, she will not benefit from the focusing gain, as illustrated by the example of two transmitted symbols spread by a factor BOR=4 in Figure 3.4. Anti-eavesdropping capability is therefore inherent to the FD implementation of the TR scheme. Authors evaluate the secrecy performance of the scheme by comparing the TR focusing gains at Bob and Eve via the normalized mean square error (NMSE) of the estimated received symbols. They demonstrate that, increasing the BOR enhances the focusing gain at Bob, while it does not improve the focusing gain at the unintended position. While this technique is promising, its assessment in terms of secrecy has not been carried out.

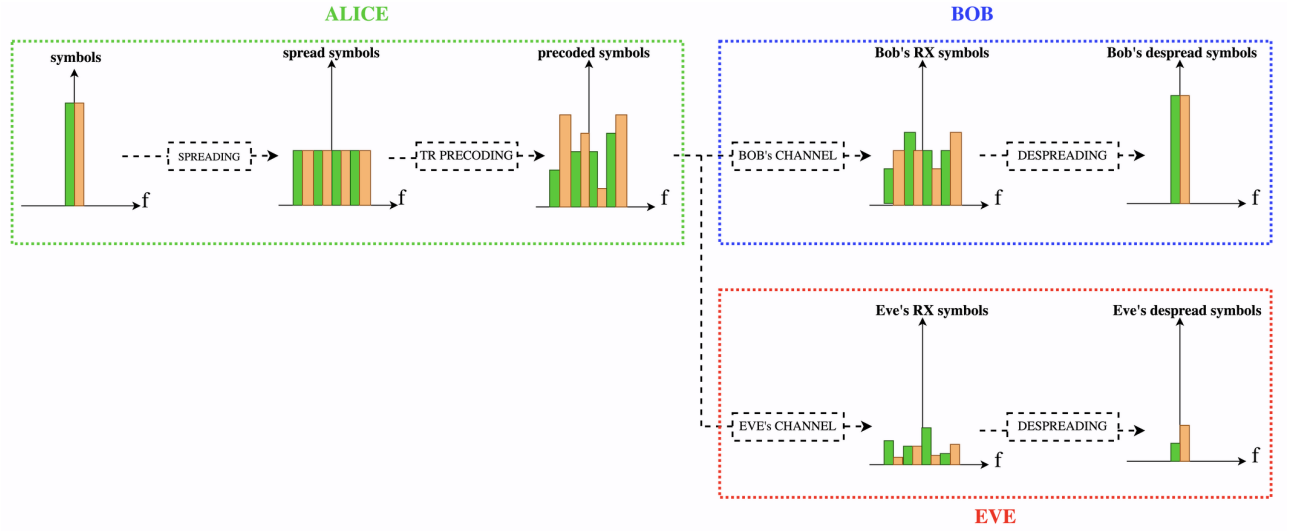

Figure 3.4: Frequency domain time reversal scheme

3.2.4 Space domain

In that scenario, using multiple antennas, the signal is transmitted in one time slot, with one frequency carrier. Architectures taking advantage of space domain are SIMO, MISO, and MIMO systems. Information-theoretic studies in [26, 27, 70] characterize the theoretical bounds on the achievable secrecy capacity of multi-antenna systems. Several space domain channel-based adaptation PLS techniques are presented below.

In [26], authors propose a power allocation strategy consisting in a GSVD precoding. It allows to separate the main and the eavesdropper's channels into two subspaces, i.e., one for the legitimate receiver, and the other for the eavesdropper. Most of the transmitted energy is dedicated to the first subspace. In doing so, the secrecy capacity of the MIMO system is improved. However, it requires

perfect CSI knowledge of both the main and the eavesdropper. Study in [71] designs a beamforming precoding matrix to minimize the mean square error (MSE) between Alice and Bob, while keeping the MSE between Alice and Eve above a given threshold. In [72], authors design a linear precoder, including an optimal regularization parameter and a power allocation scheme, that maximizes Bob's SINR while minimizing Eve's one. Another beamforming approach for MISO systems, when Eve's CSI is known at Alice, is termed as orthogonalization-based beamforming, [73, 74]. It allows to find the optimal beamforming directions for any SNR value, and therefore transmit in these directions. All these studies consider that Alice has the knowledge of Eve's CSI, and are therefore not well suited when Eve is passive.

Another kind of space-domain PLS techniques is directional modulation (DM), and is depicted in Figure 3.5.

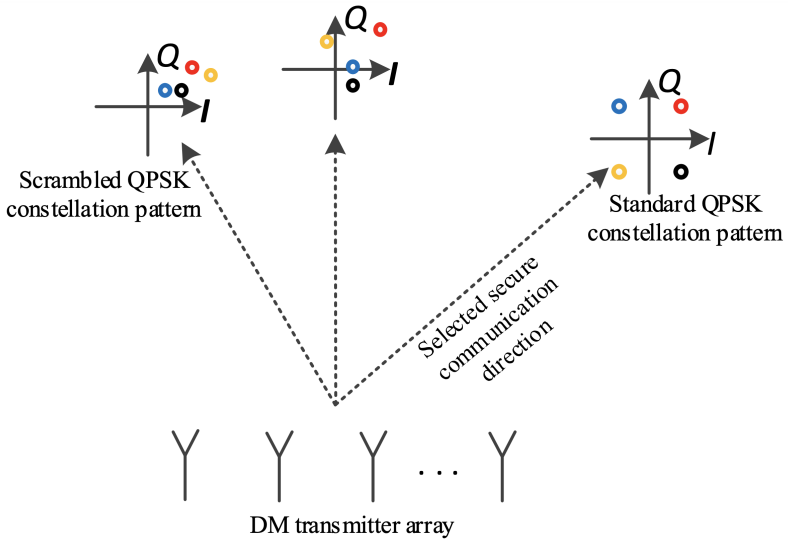

Figure 3.5: Illustration of a directional modulation transmitter, [75, Figure 1]

The underlying idea is that a DM transmitter has the capability to project an undistorted signal into a specified direction to a legitimate receiver, while simultaneously scrambling the constellation in all other unwanted directions. In such a fashion, only receivers located in the direction(s) of secure communication are able to successfully recover the data. It was first presented by Daly and Bernhard in [76]. Another DM transmitter is near-field direct antennal modulation (NFDAM), and is described in [77, 78]. It consists in integrating reflectors with switches in the near-field of a center-driven dipole antenna. By opening or closing the switch, the reflector effective length and scattering properties are modified, which causes the reflected signal to have a different phase and amplitude. Therefore, each set of switch state combinations on the near field passive reflectors results to an unique far-field radiation pattern (i.e., of complex amplitude) that can be seen as a constellation point. From that, it is possible to determine, for each symbol to be transmitted, a switch state combination leading to a quasi standard constellation symbol in the pre-specified direction of secure communication. Another DM scheme is antenna subset modulation (ASM), [79, 80]. For each transmitted symbol, a random subset of antennas are selected to radiate the symbol in a given direction. In doing so, since the subset always changes, the constellation appears to be scrambled in the other directions than the desired one. Transmit antenna selection schemes are presented in [81–83] where only a subset of antennas is used to beam-form the signal to the legitimate receiver. This scheme appears to provide secrecy in MIMO and massive MIMO systems, even when a passive eavesdropping scenario is considered. However, spatial resources are waisted since only a subset of antennas is used. No closed-form expression of the achievable secrecy is derived. In [81], authors show that the scheme achieved weak secrecy when the total available transmit antennas grows arbitrarily large, regardless of the number of active antennas.

The issue with DM systems is that, if an eavesdropper is located in the same angular direction as the

legitimate receiver, he has access to the standard constellation pattern. He can therefore demodulate the signal with a relative low probability of error. Therefore, DM systems cannot achieve secrecy in range, but only angular secrecy can be achieved. In addition, most studies consider a line-of-sight (LOS) scenario. Furthermore, the performance metric is the angular BER which does not respect any secrecy condition since leakage to the eavesdropper occurs.

3.2.5 Conclusion on channel-based adaptation techniques

The channel-based adaptation techniques presented in this section typically provide a physical advantage to Bob compare to Eve. However, some of the information always leaks at Eve. In addition, it is possible that no secrecy can be achieved in the case of multiple cooperative eavesdroppers. That is, in some system configurations, little can be done against an eavesdropper with high capabilities. Indeed, by observing multiple replicas of the signal sent by Alice that have experienced different fading, Eves could retrieve the data perfectly. Furthermore, none of the above techniques allow the transmitter to ensure a priori a desired communication secrecy rate. Indeed, either a noisy eavesdropper is considered, or optimization procedure are required to characterize the secrecy capacity of the scheme. Moreover, some techniques use the difference in BERs to quantify the secrecy of the communication schemes, which therefore do not respect the weak or strong secrecy definitions. Also, most of the power allocation techniques consider that Alice is aware of Eve's CSI, which does not reflect the practicality of real scheme where the eavesdropper is often considered as passive. Eve decoding capabilities are not justified based on the amount of CSI she may potentially extract from practical handshake procedures between Alice and Bob. Finally, the DM techniques only provide angular-based secrecy, which is a major flaw since any eavesdropper located in the angular direction of the legitimate receiver is able to correctly decode the received data.

To circumvent the main limitation of channel-based adaptation techniques which is necessary for Alice to know Eve's CSI, the concept of artificial noise injection has been introduced in the literature and is discussed in the next section.

3.3 Addition of artificial noise to the data

3.3.1 Introduction

The concept of AN addition was first established in [84–86]. The idea is that a trusted node intentionally degrades Eve's received signal by adding an artificial signal (which is called an AN signal throughout this manuscript) to the transmitted signal. This artificial signal is designed in such a way not to degrade Bob's communication, i.e., to provide reliability at Bob, therefore leading to security enhancement. In order to do so, the null space of the main channel is often used to transmit the artificial signal. It means that the AN component of the signal transmitted by Alice (which also includes data component) vanishes once having propagated through Bob's channel. It implies that Bob must have some degrees of freedom.
The merits of this category of PLS techniques are the following, [3]:

- It is possible to properly design the AN such that one obtains no information leaked to Eve.
- It does not require Bob to implement complex receiving structures, which is suitable for devices with low capabilities, such as in IoT systems for instance.
- It can be applied in TDD, FDD, or hybrid duplexing systems.
- The AN signal can provide additional benefits alongside secrecy such as reducing the PAPR, mitigating adjacent channel interference and out-off-band emission, as explained in [87].

PLS techniques that consist in injecting an AN signal to the data can be implemented in the time, frequency, or space domains, or any combination thereof, as described below.

3.3.2 Time domain

In this situation, it is considered that the information signal and the AN are sent over one frequency slot but multiple time slots.

Authors in [88] design a secure TD OFDM precoding technique. They propose an AN injection which exploits temporal degrees of freedom provided by the CP of OFDM systems to corrupt the eavesdropper. The idea is that the AN is designed to be function of Bob's channel by exploiting the redundancy introduced by the CP. From that, the AN signal gets collected over the CP when it passes through Bob's frequency selective channel and is removed when Bob removes the CP. On the other hand, since Eve's channel's response is different, she suffers from interference. Authors jointly optimize the subcarrier power allocation as well as the covariance matrix of the time-domain AN signal to study the secrecy rate performances. This scheme is not limited to scenarios where the number of transmit antennas is larger than the number of receive antennas. An extension of the technique to multi-users is presented in [89]. The study in [90] uses the approach adopted in [88] but optimizes the transmit filter which is implemented just before the CP addition process. In doing so, authors maximize the secrecy of the scheme while maintaining a level of reliability at Bob. In [91], authors design a TD AN signal that exploits the degrees of freedom inherent to the CP of OFDM modulation for visible light communication (VLC) wiretap systems. They propose a convex optimization method to restrict the PAPR increase due to the AN insertion, and to maximize the secrecy rates. Another PLS technique that use TD OFDM modulation is proposed in [92]. Authors use the degree of freedom provided by the carrier frequency offset (CFO) in order to secure the communication. CFO is the difference between the transmitter local oscillator frequency and the receiver local oscillator frequency. In OFDM systems, CFO introduces ICI, therefore leading to a signal degradation. The idea of the proposed scheme is to introduce self ICI to pre-compensate the CFO only for the legitimate user. Since Eve experiences an uncorrelated channel, her performance is expected to be degraded. However, this PLS technique requires a precise CFO estimation at Alice before transmission.

In [93], an AN signal is introduced after pulse shaping, i.e., after up-sampling, that lies in Bob's null space at the output of the matched filter, i.e., after down-sampling. This scheme assumes that Bob perfectly knows his instantaneous CSI, which is fed back to Alice. No discussion on whether this feedback can be intercepted or not by Eve is provided. In doing so, Bob's SINR is maintained above a certain threshold, while Eve's performance is strongly degraded. However, it is assumed that Bob and Eve AWGN levels are similar. Furthermore, no closed-form expression of the secrecy performance is derived. Study in [94] aims to secure a SISO communication with a single eavesdropper in quasi-static fading channels. It is assumed that Bob knows his instantaneous CSI. The AN injection process is a two-phase scheme. First, Bob broadcasts a pseudo-random artificial noise sequence. In this first phase, Bob does not send any pilot symbols for the channel estimation, such that Alice and Eve do not know the instantaneous CSI. Then, Alice broadcasts over the medium the information signal along the pseudo random artificial noise sequence received from Bob. Since Bob knows his instantaneous CSI and the pseudo-random artificial noise sequence he transmitted in the first phase, he can recover the data sent by Alice, while Eve is unable to do so. The secrecy rate, the reliability and the throughput performances of the system are analysed. However, it is considered that, prior to the two-phase transmission, Alice sends pilots to Bob allowing channel estimation. Consequently, Eve can intercept these pilots and also know her own CSI, which can potentially strongly degrade the secrecy performances. Finally, the above system is limited to a single antenna eavesdropper scenario.

In [95–97], TD TR precoders are presented where the AN is added either on all the channel taps or on a set of selected taps. While the condition for AN generation is given, its derivation is however not detailed. In [98], a TD TR multi-users single-eavesdropper precoder with AN injection is presented when the eavesdropper CSI is known or not. A convex optimization problem is solved numerically. It ensures a minimal signal power transmitted to the legitimate users under a SINR target constraint, while maximizing the amount of AN energy reaching the eavesdropper by designing the pre-filter and the AN signal.

The above techniques require optimization procedure to be solved in order to characterize the secrecy of the schemes. The transmitter is not aware a-priori of the secure communication rate over which he can communicate with Bob. It also assumes perfect CSI estimation to inject the AN in legitimate user's null space. Finally, several PLS techniques require high up-sampling factors to efficiently introduce the AN.

3.3.3 Frequency domain

In this scenario, the artificial signal is added on top of the information signal over multiple subcarriers and during a single time slot.

In [99], a fade-avoiding scheme in a passive eavesdropping scenario is presented. The idea is to transmit the signal only over Bob's sub-channels that are not in deep fade, while the deep-fade sub-channels are used to send an AN signal. Since only the deep-fade sub-channels are not used to send information signal, the main channel capacity is not strongly impacted. However, because Bob and Eve fading is independent, Eve's capacity proportionally decreases w.r.t. the number of unused sub-channels, i.e., w.r.t. the number of sub-channels filled with AN. The scenario assumes that Eve is not able to obtain any CSI knowledge about the main channel, which is restrictive. A closed-form expression of the outage probability is derived, considering a noisy eavesdropper. In the case of noise-free eavesdropper, i.e., worst case scenario in terms of secrecy, the outage probability is equal to 1, such that no secrecy can be guaranteed, see [99, Equation 21]. In [100], an AN signal is inserted in the TD in MIMO-OFDM systems. However, the AN is removed in the FD at the legitimate receiver. That is, the technique can generate the AN signal irrespective of the number of transmit antennas and the length of the CP. The study shows that the implementation achieves a higher secrecy rate when a MIMO-OFDM system is employed with the number of legitimate receiver's antennas is higher than the number of transmitter's antenna. The eavesdropper is assumed to have the same decoding structure as Bob. The performances of the scheme are only shown via simulation results.

In [56, 101, 102], FD precoders using OFDM and AN injection are presented. [101, 102] use several OFDM subcarriers for dummy data transmission. However, the encryption information must be shared between the transmitter and the legitimate receiver, leading to more processing needed at the receiver. In addition, the security is enhanced when more subcarriers are used for data obfuscation, at the expense of the data rate. Furthermore, it is assumed that Eve has no knowledge about the legitimate link. In [56], a FD TR precoder with AN injection is presented. The AN is transmitted in the null space of Bob but only limited decoding capabilities are attributed to Eve.

The techniques that introduce an AN signal in the frequency domain alongside data, do not consider higher decoding capabilities at Eve w.r.t. to Bob's decoding capabilities. In addition, Eve is assumed to have no knowledge about the legitimate link, which in turns is not always the case, depending on the handshake procedure between Alice and Bob. The worst case scenario regarding the eavesdropper is not always investigated. Indeed, Eve is usually assumed to be corrupted by AWGN. Since in a passive eavesdropping scenario Alice cannot be aware on Eve's SNR, the presented techniques can therefore not guarantee a given secrecy performance.

3.3.4 Space domain

In this situation, the signal and the AN are transmitted via multiple antennas, over one frequency slot and one time slot. The concept of AN in multi-antenna systems is introduced in the information-theoretic work [86]. In that paper, authors state two conditions for the technique to work:

- The number of antennas at the transmitter must be greater than the one at the legitimate receiver. This ensures that the main channel has a non trivial null-space, allowing the transmitter to introduce the AN in the main channel null space.

- The number of antennas at the transmitter must be greater than the one at the eavesdropper. This ensures that Eve is not able to align the AN is the null space of the legitimate receiver.

In [103], authors revisit the study performed in [86] where the effect of the number of eavesdropping antennas is detailed. They derive a closed-form expression of the average secrecy rate as a function of the communication parameters, and provide an asymptotic analysis of the instantaneous secrecy rate. However, it is assumed that Eve's channel is degraded w.r.t. Bob's channel, i.e., Eve is noisier than Bob. The scheme does not bound Eve's number of antennas, but imposes that Alice possesses more antennas than Bob. No practical decoding structure is considered at Bob and Eve. Works in [104, 105] use orthogonal blinding to precode the AN signal for MIMO systems, and achieve positive secrecy. Alice must have at least two antennas to send the AN into an orthogonal channel of the main channel. The orthogonal channel is obtained by performing a Gram-Schmidt decomposition of the main channel. The difference in SNRs at Bob and Eve is used as metric. Study in [70] proposes an AN transmission scheme, termed as masked-beamforming, in a multi-eavesdroppers MISO scenario when only Bob's CSI is known at Alice. The message is sent (assuming it is encoded via wiretap codes) in the direction of the legitimate receiver, while the AN is sent in Bob's null space. Eve is therefore impacted by the AN. Authors achieve near-optimal secrecy rate performances in the high SNR regime, but do not derive a closed-form approximation of the secrecy rate. An hybrid AN injection, both in the spatial and temporal dimensions, is presented in [106], for a MISO system with a single-antenna passive eavesdropper. They investigate the power allocation between the data and the AN, and between the temporal AN and the spatial AN. They derive a closed form expression of the ergodic secrecy rate in the limit of large number of transmit antennas. Authors extended their scheme in [107] by considering a multi eavesdroppers scenario in MIMO systems. Randomized beamforming in MISO wiretap channels with single antenna passive eavesdropper is described in [108]. If Alice possesses N_A antennas, the first $N_A - 1$ elements of the beamforming vector are generated randomly. The last beamforming vector element is generated in such a way that the added multiplicative noise is cancelled at Bob. Since Eve experiences different fading, her received signal is corrupted by the multiplicative noise. The BER is taken as performance metric. Authors in [109, 110] study the secrecy rate performance of the randomized beamforming scheme presented in [108], by considering a main AWGN channel while that of the multi-eavesdroppers are fast fading channels. It prevents the eavesdroppers obtaining the CSI, which is limiting. The multiplicative noise is called artificial fast fading (AFF). They compare the secrecy rate of the classical MISO AN injection with multi-eavesdroppers, with their AFF scheme. The eavesdropper is considered passive. When the number of transmitting antennas is higher than the number of eavesdropper antennas, the classical AN scheme outperforms the AFF scheme. However, when the number of eavesdropper antennas is higher than the number of transmitting antennas, the secrecy rate of the AFF scheme is much higher than for the classical AN scheme. Motivated by this conclusion, they implement an hybrid AN-AFF scheme that further improves the secrecy rate of the communication. Authors assume that Eve has the knowledge of her instantaneous CSI, as well as Bob's CSI, while Alice and Bob only know Bob's instantaneous CSI. No closed-form expression of the communication secrecy rate is derived. In [111], a multi-antenna robust beamforming technique is presented. Authors ensure a predefined SINR at Bob while maximizing the AN transmitted power to degrade Eve's conditions.

Several PLS techniques involving different AN injection in the spatial domain are presented. The main issue with these techniques is that the transmitter needs to possess more antennas than the legitimate receiver which makes them not suitable for an UL between a single-antenna node towards a multiple antennas BS, as encountered in IoT for instance. The majority of these techniques use power allocation strategies alongside AN injection to achieve secrecy. None of the above works allow the transmitter to know a priori the secrecy rate of the communication. In addition, Eve decoding capabilities are not discussed.

3.3.5 Conclusion on artificial noise injection techniques

The AN injection scheme allows to achieve secrecy even if Alice does not know Eve's CSI. This approach is therefore well-suited to address the passive Eve scenario that is considered in this manuscript. It is

to be noted that AN injection requires additional resources (power, time, frequency, and/or space) which makes this technique more suited to applications requiring high level of security (e.g., wireless transmissions of medical data, highly personal data, military communications,...). In these scenarios, it is required to guarantee the secrecy offered by the system, which is one of the main bottleneck identified in the literature. Indeed, if information theory proves a weak or strong secrecy, as mentioned in chapter 2, thanks to wiretap codes, it necessitates the a-priori knowledge of the SR to build a code that ensures reliability and secrecy.
The analysis of the state-of-the-art of AN-injection-based techniques highlights a number of shortcomings that motivates the work presented in the following chapters. Those shortcomings includes:

- The AN design is done with a complex optimization procedure which is power consuming, especially for IoT nodes.
- Assumptions are undertaken on Eve which are not suited for all applications:
  - Eve has the same decoder as Bob, while she could do better.
  - Eve has no CSI knowledge at all, while it actually depends on the handshake procedure which is not discussed in the literature.
- There is no guarantee of a positive SR if Eve is less noisy than Bob and/or if she is equipped with an arbitrary large number of antennas.
- The worst-case scenario is not considered in terms of SNR at Eve: if a noise is assumed to exist at Eve, then Alice needs to know Eve's SNR in order to determine the SR.
- The multi-antenna-based techniques that used the spatial domain only face limitations:
  - Since N_A should be greater than N_B, SIMO configuration for IoT node to base station-UL cannot be secured.
  - N_A should be greater than N_E, this cannot be guaranteed unless Alice knows Eve's number of antennas.
- Finally, since the AN must lie in Bob's channel null space, Alice must know accurately $\mathbf{H_B}$. In practice, the estimation is prone to errors. The influence of CSI errors on the SR must be thus studied. Therefore, next section draws a state-of-the-art of PLS schemes that assess the influence of CSI errors.

3.4 Imperfect main channel state information

3.4.1 Introduction

As seen, channel-based adaptation and AN injection schemes artificially provide a physical advantage to Bob's channel w.r.t. Eve's channel. In order to design PLS techniques, Alice and/or Bob must have some CSI knowledge about the main link. Indeed, for channel-based adaptation PLS techniques, Alice must adapt the communication parameters to the main channel conditions to provide an advantage at Bob as compared to Eve. This is only possible if she fully or partially knows Bob's CSI. In addition, the legitimate receiver may be required to know his own CSI to implement a decoding structure that matches his channel conditions. Furthermore, for AN injection schemes, Alice must also have the knowledge of Bob's CSI.

Another important feature to consider when designing a PLS scheme, is the availability of the eavesdropper's CSI at the transmitter side, which in turns influences the secrecy performance of the communication. Indeed, if Alice perfectly knows the instantaneous CSIs of both Bob and Eve, she can benefit from this knowledge to completely hide the transmitted information from Eve, while maximizing the reliability at Bob. If she is not aware of Eve's instantaneous CSI, but only has the knowledge of

Bob's condition, she is bounded to transmit an AN signal in Bob's null space. In the first situation, Eve is an active eavesdropper. However it does not capture the practicality of a wide range of real-life schemes where the eavesdropper remains silent and only listens to the medium. For this reason, it is generally assumed a passive eavesdropping scenario where Alice cannot access to Eve's instantaneous CSI, but fully or partially accesses to Bob's CSI.

3.4.2 Feedback mechanisms

CSI is acquired at the transmitter (respectively at the legitimate receiver) via feedback signaling from the legitimate receiver (respectively from the transmitter), which results in an overhead. The process of CSI acquisition via feedback signaling is called a ***training phase***, and usually occurs during the handshake procedure, and at the beginning of each channel coherence interval, [17].

Different transmission schemes allowing the communication ends to know their CSIs can be considered, depending on whether Alice or Bob first send pilots. As explained below, these schemes lead to different secrecy implications. It is also usually assumed that the pilot sequences are known to everyone, i.e., Alice, Bob, and Eve.

If Alice first sends pilots to Bob, Bob is then able to estimate his CSI. This phase, called ***forward training***, also allows Eve from obtaining her DL CSI. Bob can then feedback his CSI to Alice. This pilot signaling scheme is used in FDD systems where Bob broadcasts a compressed version of his DL CSI in the UL to Alice. This ***explicit feedback*** is also subject to be intercepted by Eve, allowing her to know Bob's DL CSI too. Thereafter, Alice can adopt channel-based adaptation and/or AN-based PLS techniques to provide secrecy, as depicted in Figure 3.6, [112].

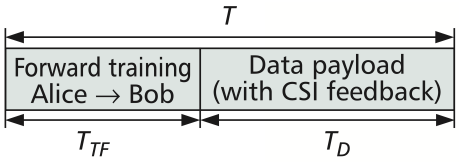

Figure 3.6: CSI transmission and feedback over a coherence block: forward training, [112, Figure 1]

Consequently, this feedback signaling scheme does not prevent Eve from obtaining CSI knowledge.

The second situation occurs when Bob first sends pilots to Alice, which is called a ***reverse training*** phase. This enables channel estimation directly at the transmitter. This ***implicit feedback*** transmission is followed by a forward training phase, i.e., Alice sends pilots to Bob corrupted by artificial noise. The AN injected alongside pilots is motivated since it allows Bob to estimate his CSI, while preventing Eve to do so. Finally, Alice adopts a PLS technique to provide secrecy in the communication. However, one needs to use reverse training alongside AN injection, which may not be suitable for all scenarios. Indeed, it implies that the UL and DL channels are reciprocal. This requirement can be met in TDD systems with calibrated RF chains, but not in FDD systems requiring explicit feedbacks sent by Bob to Alice in the UL.

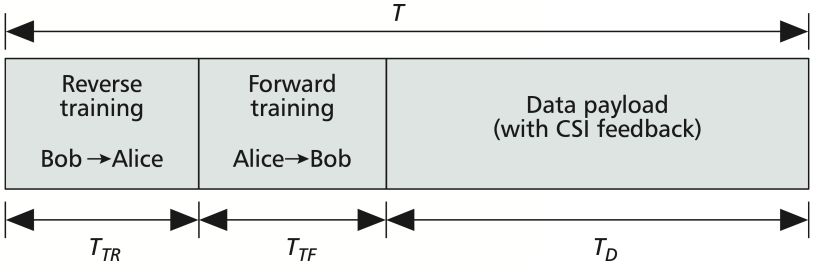

Figure 3.7: CSI transmission and feedback over a coherence block: reverse and forward trainings, [112, Figure 4]

CSI leakage to Eve can be avoided with this feedback signaling procedure.

It has to be noted that explicit feedbacks introduce larger overhead in terms of time and feedback control bits than implicit feedbacks, at the expense of CSI leakage, [113].

3.4.3 Causes of imperfect main channel state information

Most of the studies presented in sections 3.2 and 3.3 assume perfect main CSI knowledge at Alice. However, in real-life scenarios, feedbacks, whether implicit or explicit, can never provide perfect CSI. In practice, the transmitter only receives partial CSI from explicit feedback in FDD systems, [114, 115], or directly using channel reciprocity in TDD systems, [116–118]. Therefore, in order to design practical PLS schemes, one has to take into account the effects of Bob's CSI misestimation at the transmitter side. The accuracy of the main CSI at the transmitter side strongly impacts the secrecy performance of the communication. If a transmitter has imperfect CSI, there is high probability of information leakage to Eve, therefore leading to non-perfect secrecy scheme, [119]. In addition, in a passive eavesdropping scenario with imperfect main CSI knowledge, Alice is bounded to design an AN signal that lies in Bob's estimated null space. As a consequence, some AN energy may leak at Bob after reception. It is worth mentioning that, from the discussion in section 3.4.2, the accuracy of the CSI estimation can be improved if more resources are allocated to training. However, this implies less resources available for secret data transmission, such that a trade-off exists between allocating resources for CSI estimation and for secure data transmission, [112].

Some causes of imperfect main CSI estimation are outlined below:

One of the main reasons of CSI misestimation at Alice comes from the fact that she ***suffers from noise***, such as thermal noise for instance. Therefore, she only obtains a noisy version of the main CSI coming from Bob's feedback. This is directly related to Alice's SNR. Indeed, at poor SNR values, she is more prone to CSI estimation errors.

Another cause of CSI misestimate is the use of ***finite-rate links*** to transmit the feedback information. Indeed, the process of procuring CSI with feedbacks is resource consuming in time-varying fading channels. FDD systems use lower transmission rates on the reverse side of the link to provide information, via explicit feedbacks, to the transmitter of the forward side of the link. This information conveys some notion of the forward link condition such as channel state, received power, interference level, for instance, and the transmitter uses the information to adapt forward link transmission, [114]. In these systems, the CSI is first quantized before being fed-back, such that Alice receives only partial CSI from Bob, [112, 120]. As an example, Long Term Evolution-Advanced (LTE-A) systems use quantized feedbacks, [112]. Nevertheless, the use of quantized feedbacks allows to reduce the overhead, [121].

A common source of CSI errors is due to ***delayed feedback***. Time variation of a wireless channel is characterized by its coherence time, which is defined as the time duration over which its impulse response is considered to not change. Since the exchange of feedback between the receiver and the transmitter is time consuming, the transmitter only receives partially or fully outdated CSI. So, Alice bases her transmission strategy on time-delayed channel coefficients, which consequently degrades the secrecy performance of PLS techniques, [120, 122]. Channel estimation error introduced by devices movements is another source of imperfect main CSI at the transmitter side, [17]. In moderate mobility scenarios, channels have relatively high coherence time, and channel reciprocity can be assumed, [123]. However, in high mobility scenario, phase distortion and severe mismatches are observed with channel feedback, [113]. Device mobility needs to be taken into account to implement robust PLS techniques.

Hardware impairments occur during transmission and are source of imperfect CSI estimation. These impairments degrade the security of the transmitted data, [15]. Hardware impairments create a mismatch between the intended transmit signal and the actual transmit signal, and distort the received

signal in the reception processing, [124]. For example, when the transmit and the received chains are not perfectly synchronized, CFO and symbol time offset (STO) degrade the communication performances. Other hardware impairments such as IQ imbalance, phase noise, high power amplifier non-linearities at the transmitter, or low noise amplifier filter at the receiver need to be considered. Indeed these impairments introduces signal distortion and therefore decrease the secrecy of the communication, [125]. In addition, the transmit and receive RF chains in transceivers (hardware from digital-to-analog (DAC) to antenna at the transmit path, and hardware from antenna to analog-to-digital (ADC) at the receive path) are not reciprocal. To assume reciprocity, inherent to TDD communication schemes, one needs to compensate the hardware asymmetry by implementing some kind of calibrations (e.g., measuring transfer functions via feedbacks in the transceiver hardware) which are naturally not perfect, [126].

3.4.4 PLS techniques considering imperfect main CSI

This section presents a state-of-the-art of PLS schemes that include a study of the influence of the imperfect main CSI.

Estimation error of the main CSI

In every scenario, the main CSI error is modeled as a ZMCSCG variable independent from the main CSI, with an error variance bounded between 0 and 1.

Study [43] focuses on the secrecy capacity of the wiretap channel with imperfect main CSI. Authors derive lower and upper bounds of the achievable secrecy capacity in SISO fast fading channel via optimization, by considering the secrecy loss due to imperfect main CSI estimation. The gap between the upper and lower bounds is numerically characterized. In this scenario, Alice knows the statistics of Eve's channel. In [127], a robust MIMO precoding and decoding scheme is proposed when imperfect main CSI is available at the transmitter side. Authors implement a precoder and a decoder thanks to an optimization procedure to compensate for SNR loss due to imperfect CSI. In doing so, they can achieve full recovering rate and perfect secrecy. In [128], a robust beamforming optimization is solved for MISO channels when imperfect main and eavesdropper CSIs are available. Authors address the problem of secrecy rate maximization, which is solved numerically. They illustrate the secrecy rate performance gains of the scheme compared to suboptimal transmit design strategies. In [129], an optimization problem is resolved in order to maximize the secrecy throughput under secrecy outage probability and reliability output probability constraints when imperfect main CSI is available. In [130], a secure on-off single-antenna wiretap transmission scheme is adopted subject to constraints on secrecy outage probability, under quasi-static fading channel, with imperfect main CSI, and when the eavesdropper CSI is known or partially known at the transmitter. Authors in [131] study a robust beamforming scheme with AN injection to secure MISO multi-eavesdroppers systems. They ensure QoS, i.e., they provide a minimum SINR at Bob while minimizing Eve's SINR when imperfect main CSI is available.

Limited main CSI feedback

Authors in [121] characterize an upper bound of the rate loss in MIMO wiretap channels due to quantized feedback in FDD systems. They quantify the impact of channel estimation errors, quantization errors, and outdated quantized CSI on the rate loss. In [132, 133], the impact of having imperfect main CSI via a limited rate feedback on the secrecy rate of multi-antenna systems is studied. Authors consider MISO and MIMO systems with AN injection. They show that, due to partial available CSI at the transmitter side, the AN leaks at Bob and strongly degrades the performance of the scheme. In [134], an FDD MIMO wiretap system with AN injection and imperfect main CSI due to quantized feedback is considered. Authors provide the optimal power allocation and training overhead that maximize the ergodic secrecy rate of the communication. Authors in [135] study the ergodic secrecy capacity in block-fading wiretap channels when the CSI information is sent over an error-free public channel with limited capacity.

Outdated main CSI

In [136], authors derived the connection outage probability, the secrecy outage probability, and the reliable and secure transmission probability when outdated main CSI is available. The connection outage probability is defined as the probability that Bob is unable to decode the received signal correctly. The reliable and secure transmission probability jointly evaluate the connection outage probability and the secrecy outage probability. They then determined the optimal secrecy rates maximizing the secrecy throughput under dual connection and secrecy outage constraints. The outdated CSI is modeled as a correlated random variable from the exact CSI. The autocorrelation coefficient is obtained according Jake's autocorrelation model. In [137], a transmit antenna selection beamforming scheme is addressed when Alice accesses to an outdated version of Bob's CSI, and when she has no information about Eve's CSI. It shows that it is preferable for Alice to use a statistical CSI instead of an outdated CSI for beamforming design when a fast-fading channel model is considered. Reference [138] studies the effect of feedback delay to minimize the performance losses of a multi-antenna scheme with AN injection. In [139], a new secure transmit antenna selection strategy is presented for MIMO systems with outdated main CSI. Bob and Eve are supposed to possess the same decoding capabilities. That is, they both implement a maximal-ratio combining (MRC) decoder. Authors derive closed-form expressions for the exact secrecy outage probability and the probability of non-zero secrecy capacity. They also characterize the decrease of secrecy diversity order due to the outdated CSI. The scheme requires the receiver to feed back the index of the optimal transmit antenna and the associated instantaneous CSI in different time slots. This ensures that the CSI associated with the selected transmit antenna is used for secure transmission. Authors in [140] focus on the secrecy performance of MIMO multi-eavesdroppers scheme. A transmit antenna selection strategy and outdated main CSI are considered. Authors study the scenarios where Alice is or not aware of Eve's instantaneous CSI. The outdated CSI is modeled as in [136]. For passive eavesdropping system, they derive an exact and an asymptotic closed-form expressions of the secrecy outage probability in Nakagami-m fading channels. They also derive the probability of non-zero secrecy capacity and the ϵ-outage secrecy rate. The main issue with the presented work is that authors assume no cooperation between eavesdroppers, and an MRC decoding structure at Bob. That is, secure data transmission can take place between Alice and Bob as soon as the quality of the main channel is larger than that of any eavesdropper's channel. In addition, authors consider the scenario where Eve is not equipped with a noise-free hardware, i.e., the worst case scenario is not investigated. Studies [141, 142] particularly show that the secrecy performance of a communication system is strongly degraded when the CSI is imperfectly known because of mobility of the transmitter relative to the receiver.

Channel and hardware impairments

Studies in [125, 143] consider the secrecy outage probability of a full-duplex system affected by hardware impairments. Results show a significant performance degradation due to transceiver impairments. In [124], the capacity of a massive MIMO under imperfect CSI due to the aggregate impact of different hardware impairments is studied. It is shown that the large number of degrees of freedom offered by massive MIMO can be used to mitigate the impairments. The hardware impairments are modelled thanks to two additive distortion noise terms. That is, an ergodic stochastic process that describes the residual transceiver impairments of the transmitter hardware, and an ergodic stochastic process that describes the residual transceiver impairments of the legitimate receiver hardware. These are assumed to be dependent on the channel, i.e., the noise terms are stationary within a coherence interval, and are proportional to the signal power at the considered antenna. In [144], authors quantify the secrecy rate loss of a wiretap system due to IQ imbalance at Bob and Eve, in the case of an ideal transmitter. In [145], the impact of phase noise on the secrecy performance of downlink massive MIMO systems in the presence of a passive multiple-antenna eavesdropper is assessed. A MF precoding at the base station with AN injection is implemented. It is assumed that Eve possesses an ideal phase noise-free hardware, but Alice and Bob are impacted by phase noise. Phase noise is the inherent noise present in real oscillators that spreads the power of a signal to adjacent frequencies, leading to noise side-bands. It is shown in [124] that phase noise is the main contributor in degrading the quality of the CSI estimation,

needed at the transmitter to precode the data. A closed-form lower bound on the achievable ergodic secrecy rate of a given user is derived.

3.4.5 Conclusion on imperfect main CSI knowledge

The introduction of imperfect main CSI knowledge at the transmitter side allows to more realistically characterize the secrecy performances of a communication scheme. It is seen that the CSI misestimation has different origins. For noisy CSI, the error is modeled as an uncorrelated random variable following a ZMCSCG distribution, with error variance bounded between 0 and 1. For outdated CSI, the error is modeled as a correlated random variable from the exact CSI, with autocorrelation coefficient obtained according to Jake's autocorrelation model. To model hardware impairments, two noise terms are added, respectively to take into account the impairments of the transceiver's hardware's of the transmitter and the legitimate receiver. The noise terms depend on the channel and are assumed stationary during a coherence interval. These terms are also considered to be proportional to the signal power at the particular antenna.

While most techniques only assess the secrecy loss due to CSI misestimation, it is worth highlighting that some proposed PLS techniques are robust to CSI errors, i.e., that achieve secrecy. However, to be able to recover the secrecy loss due to imperfect CSI acquisition, complex optimization procedures need to be solved numerically, which is power consuming. It is therefore not suited for nodes with limited computational capabilities, such as encountered in IoT networks for instance. In addition, none of the PLS schemes allow the transmitter to a-priori guarantee a level of secrecy, depending on CSI errors, which motivates the work presented in next chapters.

3.5 Conclusions and implemented technique in this work

A state-of the-art of PLS techniques based on Wyner's model of security is drawn in this chapter. These SINR-based techniques are subdivided into channel-based adaptation schemes, presented in section 3.2, and addition of an AN signal alongside to the data, presented in section 3.3.

None of the presented PLS schemes allow the transmitter to a-priori guarantee a given amount of secrecy in the communication. Indeed, either bounds on the achievable secrecy performances are detailed, or optimization procedures that need to be numerically solved are characterized, or schemes that do not consider the worst-case scenario regarding the eavesdropper are investigated, i.e., eavesdroppers have few CSI knowledge, limited decoding capabilities, or limited number of antennas. In addition, the vast majority of the techniques presented in sections 3.2 and 3.3 assume at least a perfect CSI knowledge of the legitimate link at the transmitter side. In practical scenarios, imperfect main CSI knowledge is unavoidable and strongly impacts the secrecy performances. Consequently, a state-of-the-art of PLS techniques that take into account imperfect main CSI knowledge at the transmitter is outlined in section 3.4. While some of the presented PLS schemes are robust to imperfect CSI knowledge at the transmitter side, it requires complex optimization procedures that need to be solved in order to fully recover from the secrecy loss. These recovery schemes are therefore unsuited for devices with limited computing capabilities, such as encountered with IoT objects, for instance.

Consequently, the goal of this PhD is to provide a PLS technique based on channel adaptation and AN injection that overcomes some of the limitations identified in the state-of-the-art. In particular, the work presented in the next chapters investigates an approach to *guarantee* a positive SR with an outage below a desired threshold. To do so, a frequency domain precoder is designed and the undertaken approach does sacrifice frequency resources to guarantee a given set of security and reliability performance. So, the proposed scheme rather targets highly confidential data exchange. To guarantee PLS to some extent, reasonable assumptions must be considered regarding Eve. At the same time, the system has to be designed using whatever knowledge can be realistically acquired by Alice. In particular, chapters

5 and 6 investigate scenarios where PLS performances can be *guaranteed* when: i) Eve is assumed to be noiseless, ii) Eve is equipped with an arbitrarily large number of antennas, iii) Alice imperfectly estimates Bob's CSI. To achieve these goals, one has to identify what CSI knowledge can be possibly acquired by Eve and how she can efficiently benefit from this knowledge in her attempt to eavesdrop the data. This depends on the communication protocol, and specifically on the handshake procedure. Consequently, the next chapter 4 introduces the different handshake procedures considered in this manuscript, and highlights the amount of CSI acquisition at Eve which is assumed to be perfect. The procedures are reviewed in an IoT context and therefore cover different system configurations, namely, SISO (e.g., node-to-node communication), MISO (e.g., DL from multi-antenna BS to single-antenna node), and SIMO (e.g., UL from single-antenna node to multi-antenna BS) .

4 | System models, Scenarios, and Handshake Procedures

Contents

4.1 Introduction

Chapter 3 highlighted different PLS techniques that can be implemented in order to provide security, in the sense of reliability at the legitimate receiver and confidentiality from the eavesdropper, in a point-to-point wireless communication. Some flaws in the literature are outlined. In particular, the handshake procedure that determines the amount of CSI knowledge at the communication's ends, which in turns influences the communication secrecy performances, is overlooked in many studies.

The aim of this chapter is to present, motivate, and justify the PLS scheme that is considered throughout this study. It therefore establishes the foundations to assess the secrecy performances of the scheme in next chapters 5 and 6.

As a reminder, a passive eavesdropping scenario is studied to reflect the practicality of many real-life security schemes. A passive eavesdropper is not detected by the transmitter and silently eavesdrops the data. So, Alice cannot access to Eve's CSI.
The general communication scheme is presented in Figure 4.1. The wireless channel between Alice and Bob is called the ***main channel*** ($\mathbf{H_B}$). The wireless channel between Alice and Eve is called the ***eavesdropper channel*** ($\mathbf{H_E}$). The channel between Bob and Eve is denoted $\mathbf{H_{BE}}$. Different

system configurations are investigated depending on whether Alice or Bob and/or Eve is equipped with multiple antennas. In addition, when a DL communication is considered, Alice can be seen as a BS and Bob as an UE of the network. When an UL communication is considered, Alice can be seen as an UE of the network, and Bob as a BS. In this works, it is considered that the BS and Eve can be equipped with multiple antennas, whereas the UE is a single-antenna node. Therefore, the configurations of interest are SISO, MISO, and SIMO.

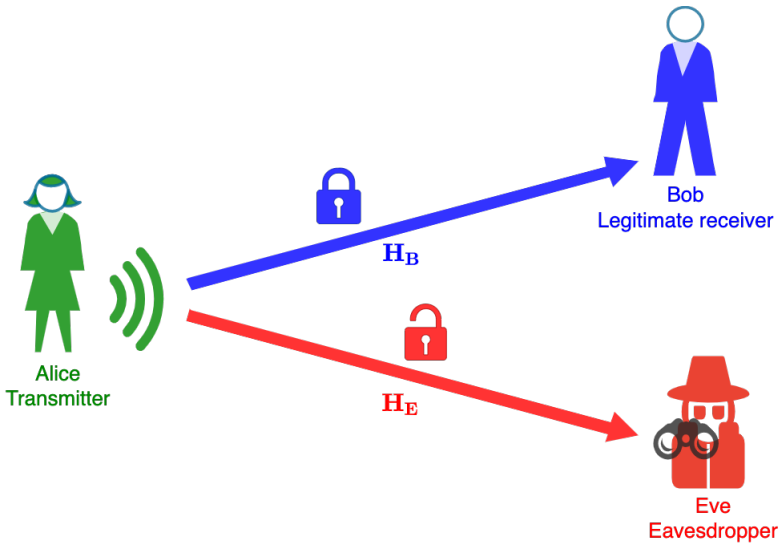

Figure 4.1: Security scheme

Section 4.2 justifies and outlines the assumptions undertaken to study the PLS scheme. Then, the global system model is presented in section 4.3. The modeling of the main CSI misestimation by Alice is given in section 4.4. Section 4.5 describes the different secrecy scenarios considered in this work, and section 4.6 highlights the practical handshake procedures.

4.2 General assumptions

Several main assumptions are undertaken for the system model under consideration. The aim of this section is to justify and motivate these assumptions.

4.2.1 Channel model

A ***block fading multipath*** channel is considered. The multiple propagation paths are assumed to come from multiple reflections in the medium. Each path is associated with a propagation delay and an attenuation factor that are time-varying. Such a channel belongs to time-varying multipath channels that present two main characteristics:

- The **delay spread** introduced in a signal transmitted through the channel, which is due to the multipath propagation. If an impulse is transmitted at *time 1* for instance, the received signal, i.e. the impulse response, is composed of several pulses, as observed in Figure 4.2.

- The **time variations** in the structure of the medium, resulting in variations in the structure of the multipath. If an impulse is transmitted at time different from *time 1*, say *time (i+1)* for instance, the received pulses change in phase, amplitude, delay, and number, as seen in Figure 4.2, [146, Chapter 13].

Figure 4.2 shows classical impulse responses of a time varying multipath channel.

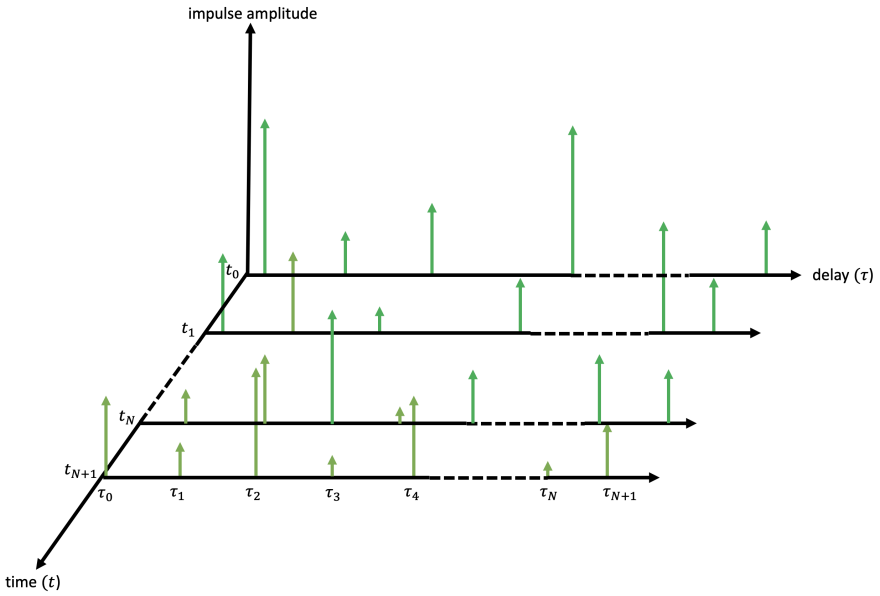

Figure 4.2: Impulse responses to a time-varying multipath channel

Throughout this work, the channel is considered as a ***Rayleigh fading channel***. These are channels where every tap of the impulse responses is modeled as zero-mean complex Gaussian RVs, which approximates the behaviour of rich multipath environments.

Delay spread characterization

One key parameter that characterizes a multipath channel is the ***delay spread*** of the channel, denoted as T_m, associated to the power delay profile (PDP). The PDP gives the power density (per-unit delay τ) incident onto a local area as a function of propagation delay (τ). It indicates that the signal arrives with some delay spread at the receiver. The delay spread of the channel characterizes the PDP duration. The Fourier transform of the PDP gives the ***coherence bandwidth*** of the channel $(\Delta f)_c$. It is defined as the bandwidth over which correlation is above a given threshold (typically 0.7). The precise relation between the delay spread and the coherence bandwidth depends on the PDP shape. Typically, it comes, [147, Chapter 3]:

$$(\Delta f)_c \approx \frac{1}{2\pi T_m}. \tag{4.1}$$

Therefore, if a signal with bandwidth W is transmitted through a channel such as $W < (\Delta f)_c$, the channel is said ***frequency non-selective***, i.e., flat-fading channel. In that situation, all the frequency components of the signal are affected similarly by the channel. On the opposite, if $W > (\Delta f)_c$, the channel is ***frequency selective***, [146, Chapter 13].

Time variation characterization

To characterize the time variations in the multipath propagation, the Doppler power spectrum (DPS) is often used. The spectral broadening caused by the time varying nature of the channel is defined as the ***Doppler spread*** of the channel, B_d. It is related to the ***coherence time*** of the channel $(\Delta t)_c$ as:

$$(\Delta t)_c \approx \frac{1}{B_d}. \tag{4.2}$$

A channel with large coherence time, i.e., low Doppler spread, slowly varies with time, [146, Chapter 13].

4.2.2 Channel related assumptions

Assumption 1: Frequency selective channel

In this work, an OFDM structure with Q subcarriers is considered. The OFDM block duration is T, i.e.,

the block bandwidth is $W = Q/T$. It is usual to have $T > T_m$, i.e., the channel is frequency-selective for the whole OFDM block. However, it is considered that $\frac{W}{Q} < (\Delta f)_c$, i.e., all subcarriers experience non-correlated fading, [146, Chapter 13].

Assumption 2: Block-fading channel
When considering the actual handshake procedure, one has to study the rate at which the channel changes compared to the transmission rate. It is considered in this work that the channel remains constant during the transmission of an OFDM burst, i.e., several successive OFDM blocks. Such a channel is called a ***block fading*** channel. From that, each burst experiences a single state of the channel and two different bursts experience two different states, [146, Chapter 14]. This assumption justifies that the channel remains constant during the handshake procedure and the transmission of a few OFDM blocks.

Discussion
It is to be noted that the flexibility in the communication parameters in current standards such as 5G, offers degrees of freedom that increases the chances that assumptions 1 and 2 are valid. For instance, flexible numerology in 5G allows for subcarrier spacings from 15KHz up to 240 KHz, which in turns allows for acting on slot durations to help meeting assumption 2. Also, using resource blocks in non-contiguous bands can help meeting assumption 1.

4.3 Global system model

This section aims to present the practical secure communication protocol that is investigated throughout this work, for all investigated scenarios, i.e., SISO, MISO, and SIMO systems.

The PLS techniques presented in chapter 3 particularly show that, in a passive eavesdropping scenario, Alice is bounded to exploit the null space of the main channel to inject an AN signal that degrades the performances of the eavesdropper. To do so, the main channel must have some degrees of freedom, which can be exploited with the help of diversity. Diversity methods are usually used to mitigate reception errors when the channel is in deep fade. The same information is sent onto different fading channels such that the probability of simultaneous fading is considerably reduced. Frequency diversity is a method that consists in sending the same information signal onto multiple carriers, at least separated by the coherence bandwidth of the channel, [146, Chapter 13].

It is also stated that TR precoding presents intrinsic anti-eavesdropping capabilities due to the focusing gain it offers at the legitimate receiver's position. Furthermore, it is seen that in the FD, TR can be implemented into an OFDM modulation, and can therefore be incorporated into existing standards, such as in 5G or LTE for instance. To benefit from the focusing effect, each modulated symbol is transmitted over BOR subchannels, introducing the frequency diversity needed for AN injection.

For the aforementioned reasons, an FD TR channel-based adaptation scheme with AN injection is considered in this study. The proposed scheme uses frequency diversity inherently present in any multipath environments, it can be incorporated into practical standards, and have the ability to offer reliability and secrecy.

Remark 4.1: Investigated scheme optimality

The scheme considered in this PhD work, i.e., FD TR channel-based adaptation scheme with AN injection, is not optimal but does not require any optimization procedure. In a block-fading scenario with passive eavesdropping, a power allocation strategy (2.34) maximizes the secrecy rate. Nevertheless, (2.34) requires a complex optimization procedure and is therefore not suited for devices with limited capabilities such as encountered in IoT networks.

The general communication block diagram of the PLS scheme of interest is depicted in Figure 4.3 and comprises three main blocks:

- The FD TR precoding at Alice,
- The AN injection at Alice,
- The decoding structures at Bob and Eve.

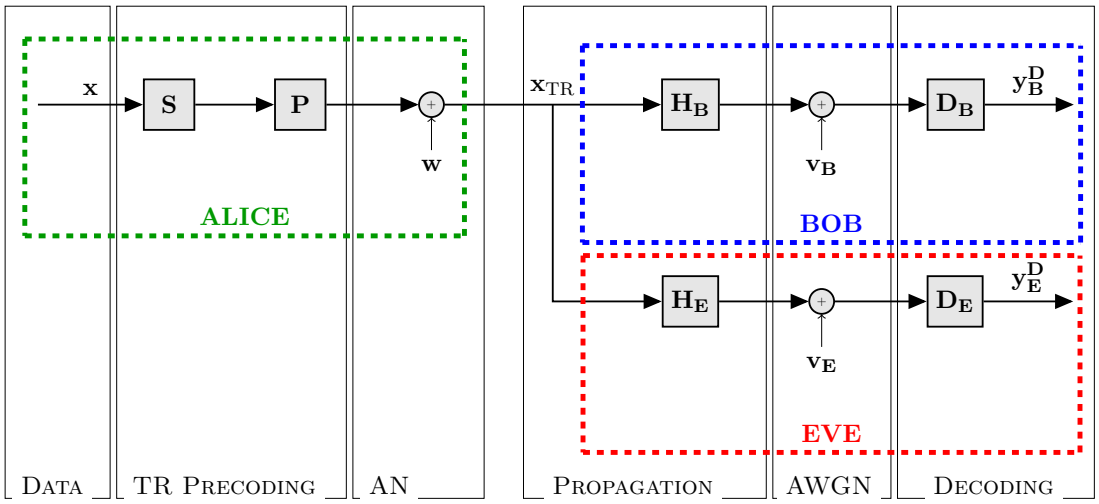

Figure 4.3: General communication block diagram

Alice aims to transmit secure data to Bob. To do so, without loss of generality, it is considered that she sends one block of useful data $\mathbf{x}$, composed of $N < Q$ symbols x_n (with $n = 0, ..., N-1$). A symbol x_n is a zero-mean RV with unit variance, i.e., $\mathbb{E}\left[|x_n|^2\right] = \sigma_x^2 = 1$. Alice first precodes the useful data block. It consists in a ***spreading*** operation followed by the application of a ***precoding matrix***, as seen in Figure 4.3. As stated in chapter 3, the spreading/despreading operation in the FD is equivalent to upsampling/downsampling in the TD, [69].

The useful data block is spread in the FD by a BOR factor $U = Q/N$ thanks to a spreading matrix $\mathbf{S}$ of size $Q \times N$. $\mathbf{S}$ is an unitary matrix, i.e., $\mathbf{S}^H\mathbf{S} = \mathbf{I}_N$. It is the concatenation of U independent $N \times N$ diagonal matrices, whose diagonal values are randomly distributed and taken from the set $\{\pm 1\}$ in order not to increase the peak-to-average power ratio, as suggested in [54, 148].

$$\mathbf{S} = \frac{1}{\sqrt{UN_A}} \begin{pmatrix} \pm 1 & 0 & \dots & 0 \\ 0 & \pm 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \pm 1 \\ & \vdots & \vdots & \\ \pm 1 & 0 & \dots & 0 \\ 0 & \pm 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \pm 1 \end{pmatrix}. \tag{4.3}$$

In doing so, each data symbol is transmitted onto U different subcarriers with a spacing of N subcarriers, thereby introducing frequency diversity. In MISO configurations, the spread sequence is replicated onto Alice's N_A antennas.

Then, a precoding matrix $\mathbf{P}$ is applied to the spread sequence. Finally, an AN signal $\mathbf{w}$ is added before transmission. The AN signal is composed of Q components w_q ($q = 1, ..., Q$), such that

$\mathbb{E}\left[|w_q|^2\right] = \sigma^2_{\text{AN}} = \frac{1}{N_A U}$.

Consequently, the transmitted signal $\mathbf{x}_{\text{TR}}$ can be expressed as:

$$\mathbf{x}_{\text{TR}} = \underbrace{\sqrt{\alpha}\,\mathbf{P}\mathbf{S}\,\mathbf{x}}_{\text{useful signal}} + \underbrace{\sqrt{1-\alpha}\,\mathbf{w}}_{\text{AN signal}} \tag{4.4}$$

where $\alpha \in [0,1]$ defines the ratio between the useful and the total signal power. The spreading matrix $\mathbf{S}$, the precoding matrix $\mathbf{P}$, and the AN signal are designed such that the transmitted energy remains constant, whatever the value of α, and equals 1 per transmitted symbol. Equivalently, the transmitted energy per OFDM block is equal to N.

Remark 4.2: AN injection

Equation (4.4) highlights the fact that the inclusion of the AN signal does not affect the total transmitted power of the system, which is distributed between the useful signal and the AN signal. Injecting more AN decreases the useful data energy transmitted but increases the interference at the eavesdropper's position. In addition, the AN signal shares the same resources (i.e., spectral content and time slots) as the useful signal. Therefore, the introduction of an AN signal does not cause more interference to a separate network than classical information data. For example, if different legitimate users with their own resources aim to securely communicate with a BS, each user will communicate at different time and/or frequency slots. The AN from one user will not leak to another since it is injected on the resources of this particular legitimate link.

At the receiver ends, the transmitted signal propagates through Bob and Eve's channels respectively. $\mathbf{v}_{\text{B}}$ (resp. $\mathbf{v}_{\text{E}}$) is the FD complex AWGN at Bob (resp. Eve), with noise's variance $\mathbb{E}\left[|v_{\text{B},n}|^2\right] = \sigma^2_{\text{B}}$ (resp. $\mathbb{E}\left[|v_{\text{E},n}|^2\right] = \sigma^2_{\text{E}}$). The received signal at Bob is expressed as:

$$\mathbf{y}_{\text{B}} = \mathbf{H_B}\mathbf{x}_{\text{TR}} + \mathbf{v}_{\text{B}} = \begin{pmatrix} h_{\text{B},1} & 0 & \dots & 0 \\ 0 & h_{\text{B},2} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & h_{\text{B},Q} \end{pmatrix} \begin{pmatrix} x_{\text{TR},1} \\ x_{\text{TR},2} \\ \vdots \\ x_{\text{TR},Q} \end{pmatrix} + \begin{pmatrix} v_{\text{B},1} \\ v_{\text{B},2} \\ \vdots \\ v_{\text{B},Q} \end{pmatrix}. \tag{4.5}$$

The received signal at Eve is given by:

$$\mathbf{y}_{\text{E}} = \mathbf{H_E}\mathbf{x}_{\text{TR}} + \mathbf{v}_{\text{E}} = \begin{pmatrix} h_{\text{E},1} & 0 & \dots & 0 \\ 0 & h_{\text{E},2} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & h_{\text{E},Q} \end{pmatrix} \begin{pmatrix} x_{\text{TR},1} \\ x_{\text{TR},2} \\ \vdots \\ x_{\text{TR},Q} \end{pmatrix} + \begin{pmatrix} v_{\text{E},1} \\ v_{\text{E},2} \\ \vdots \\ v_{\text{E},Q} \end{pmatrix}. \tag{4.6}$$

At the legitimate receiver's end, a linear decoding matrix $\mathbf{D_B}$ is applied to the received sequence, which depends on the system configuration. From that, Bob obtains an estimate $\mathbf{y}^{\mathbf{D}}_{\mathbf{B}}$ of the transmitted symbol sequence $\mathbf{x}$, of dimension $N \times 1$. It is assumed that both Bob and Eve know the spreading matrix $\mathbf{S}$. The amount of CSI Eve can estimate depends on the handshake procedure. Consequently, depending on the available CSI, she uses the most suitable decoding structure $\mathbf{D_E}$ to obtain an estimate $\mathbf{y}^{\mathbf{D}}_{\mathbf{E}}$ of the transmitted symbol sequence $\mathbf{x}$, of dimension $N \times 1$, as explained in section 4.6. A perfect synchronization at Bob and Eve is finally assumed.

Remark 4.3: Spreading factor

The design of the spreading factor U is of prime importance for securing the communication, as described in next chapters 5 and 6, but results in an overhead, since additional frequency resources are required. For an OFDM block with a fixed number of subcarriers, i.e., fixed bandwidth, only $N = Q/U$ useful data symbols are transmitted. If the spreading factor increases, the number of useful data symbol per block decreases. Security is here obtained at the expense of the data rate. On the other hand, one can fix the transmission rate, i.e., N useful data symbols sent per OFDM block with a spreading factor U. Increasing the BOR factor therefore requires more bandwidth in the system. In the latter, security is obtained at the expense of the total spectral occupancy. In this manuscript, it is considered that the total bandwidth is fixed as well as the transmitted energy, and the spreading factor is made variable, i.e., the effective data rate is affected.

4.4 Imperfect channel state information

The amount of available CSI at the communication ends strongly impacts the security performance of the communication, as explained in chapter 3.

In this work, it is considered that the main CSI Alice estimates from Bob's pilots is not perfect. The imperfections arise from noisy preamble estimations, and are modelled as a ZMCSCG distribution with variance σ. Alice estimation of Bob's CSI is therefore expressed as [43, 111, 130]:

$$\widehat{\mathbf{H}}_{\mathbf{B}} = \sqrt{1-\sigma}\mathbf{H}_{\mathbf{B}} + \sqrt{\sigma}\Delta\mathbf{H}_{\mathbf{B}} \tag{4.7}$$

where $\widehat{\mathbf{H}}_{\mathbf{B}}$ is Bob's CSI estimation made by Alice, $\Delta\mathbf{H}_{\mathbf{B}}$ is the related CSI error, and $\sigma \in [0,1]$ is the estimation error variance.
Finally, in order to study the worst case scenario in terms of security, it is assumed that the CSI obtained by Eve is perfect (i.e., no error).

4.5 Considered secrecy scenarios

This section presents the secrecy scenarios that are investigated. In particular, the AN generation and the expressions of the received signals at Bob and Eve are described.

In the following, three system configurations are considered depending on whether Alice or Bob and/or Eve possess one or multiple antennas. A single-antenna eavesdropper is denoted by *SE*, and a multi-antenna eavesdropper by *ME*. A multi-antenna eavesdropper can either represent multiple colluding eavesdropper with one or multiple antennas, or a single eavesdropper that is equipped with multiple antennas. Since no spatial nor frequency correlations are considered in this manuscript, both configurations are similarly treated.

Common to all configurations, Alice transmits an FD OFDM block of Q subcarriers. That is, each SISO subchannel, i.e., a propagation channel between a particular antenna at Alice and a receiving antenna at Bob or Eve, is considered as a $Q \times Q$ diagonal matrix whose diagonal elements are the subcarrier channel coefficients. It is considered that the channel coefficients are ***Rayleigh distributed*** and follow a ZMCSCG distribution. This corresponds to urban or indoor environments with rich multipath components. The system dimensions are discussed below. Note that only the multi-eavesdropper(s), i.e., multiple-antenna eavesdropper or multi-eavesdroppers, scenarios are investigated. The reader can set the number of eavesdropper's antennas to one in order to obtain the corresponding single-antenna eavesdropper situation.

Remark 4.4: Frequency selectivity impact

Rich multipath environments are considered in this work. However, if frequency non-selective channels are considered, i.e., flat fading channels, no frequency diversity is introduced by the FD implementation of TR precoding. Bob and Eve's channels are then strongly correlated, and positive secrecy rate may not be achieved, as anticipated from (2.34).

4.5.1 SISO system

If both communication ends possess one antenna ($N_A = N_B = 1$), the system is referred as SISO. SISO systems can be further classified into single-input single-output single-eavesdropper (SISO-SE) systems if the eavesdropper only has one antenna ($N_E = 1$), and single-input single-output muti-eavesdropper (SISO-ME) systems if the eavesdropper(s) dispose of multiple antennas ($N_E > 1$). In a SISO-ME configuration, the channel between Alice and Eve's k^{th} antenna ($k = 1, ..., N_E$) is denoted $\mathbf{H}_{\mathbf{E},k}$. This situation illustrates the secure wireless data transmission between two UEs with limited capabilities, e.g., two IoT nodes in a network, in the presence of single or multi-antenna eavesdropper(s). The different SISO system configurations are depicted in Figure 4.4.

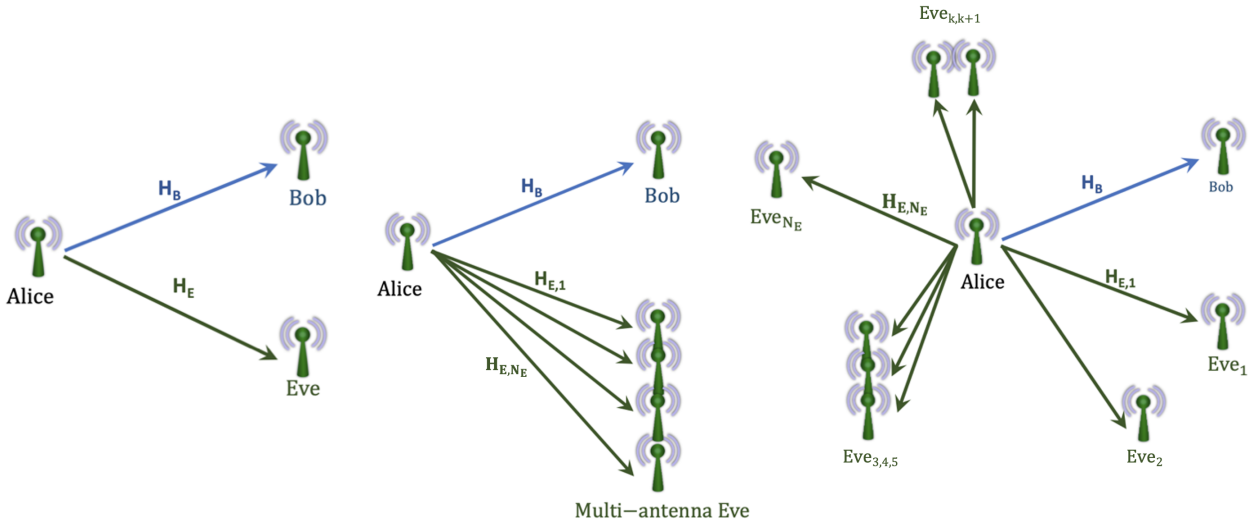

Figure 4.4: SISO configurations: single-antenna eavesdropper (left), multi-antenna eavesdropper (centre), multi-eavesdroppers (right).

4.5.1.1 System presentation

The block diagram of a SISO-ME system is shown in Figure 4.5. In this configuration, Bob receives a signal coming from Alice's single transmitting antenna. Eve receives N_E signals, one at each antenna.

- $\mathbf{S}$ is a $Q \times N$ spreading matrix defined in (4.3) with $N_A = 1$.
- $\mathbf{H_B}$ is a $Q \times Q$ diagonal matrix, whose elements are $h_{\text{B},q}$, $q = 1, ..., Q$, and follow a ZMCSCG distribution with unit variance, i.e., $h_{\text{B},q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\text{B},q}$ represents the q^{th} Alice-to-Bob channel coefficient.
- $\mathbf{H_E} = \left[\mathbf{H}_{\mathbf{E},1}, ..., \mathbf{H}_{\mathbf{E},N_E}\right]^T$ is a $(Q \times N_E) \times Q$ SIMO channel, where each SISO subchannel $\mathbf{H}_{\mathbf{E},k}$, $k = 1, ..., N_E$ is a $Q \times Q$ diagonal matrix whose elements are $h_{\text{E},k,q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\text{E},k,q}$ represents the q^{th} channel coefficient between Alice and Eve k^{th} antenna.
- The precoding matrix $\mathbf{P} = \widehat{\mathbf{H}}_{\mathbf{B}}^{H}$ in Figure 4.3 is a $Q \times Q$ diagonal matrix whose elements are $\tilde{h}^{*}_{\text{B},q} \sim \mathbb{CN}(0,1)$. The precoding matrix allows to implement a MRC at the transmitter side, equivalent to the FD implementation of a TR precoder.

- The channel error matrix $\Delta\mathbf{H_B}$ is a $Q \times Q$ in (4.7) diagonal matrix with elements $\Delta h_{\mathrm{B},q} \sim \mathbb{CN}(0,1)$.
- The decoding matrix at Bob is $\mathbf{D_B} = \mathbf{S}^H$, which is the despreading matrix of dimension $N \times Q$.
- The decoding matrix at Eve is $\mathbf{D_E} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}$, whose nature depends on the handshake procedure between Alice and Bob. $\mathbf{D}_{\mathbf{E},k}$, $k = 1, ..., N_E$, is a $Q \times Q$ diagonal matrix whose elements are $d_{\mathbf{E},k,q}$, $q = 1, ..., Q$.

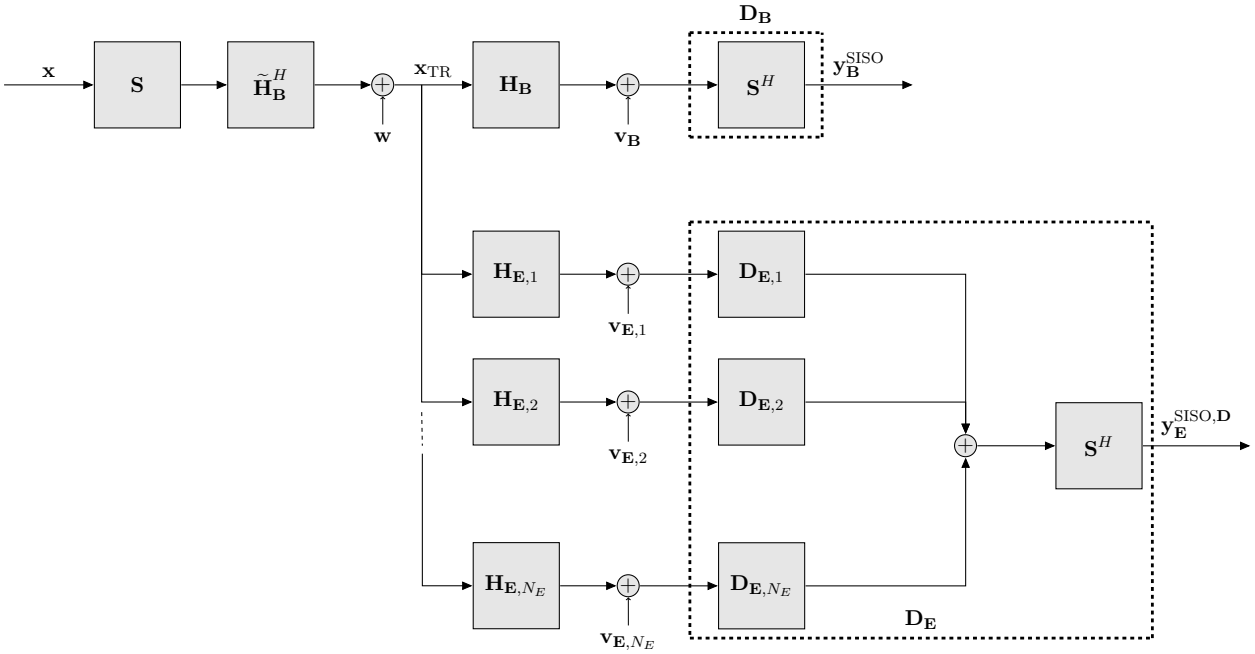

Figure 4.5: SISO-ME block diagram

4.5.1.2 Artificial noise generation

From Figure 4.5, Alice designs the AN signal to lie in Bob's null space as:

$$\mathbf{S}^H \widehat{\mathbf{H}}_\mathbf{B} \mathbf{w} = \mathbf{A}\mathbf{w} = \mathbf{0}_N, \tag{4.8}$$

where $\widehat{\mathbf{H}}_\mathbf{B}$ is the estimate of $\mathbf{H_B}$ available at Alice. From (4.8), it can be observed that the AN signal lies in Bob's estimated null space. To design an AN signal that meets equation (4.8), a singular value decomposition (SVD) of A is performed:

$$\mathbf{A} = \mathbf{S}^H \widehat{\mathbf{H}}_\mathbf{B} = \mathbf{U} \left(\Sigma \, \mathbf{0}_{Q-N \times Q} \right) \begin{pmatrix} \mathbf{V}_1^H \\ \mathbf{V}_2^H \end{pmatrix}, \tag{4.9}$$

where $\mathbf{U} \in \mathbb{C}^{N \times N}$ contains left singular vectors, $\Sigma \in \mathbb{C}^{N \times N}$ is a diagonal matrix containing non-zero singular values, $\mathbf{V}_1 \in \mathbb{C}^{Q \times N}$ contains right singular vectors associated to non-zero singular values, and $\mathbf{V}_2 \in \mathbb{C}^{Q \times Q-N}$ contains right singular vectors that span the right null space of $\mathbf{A}$. The AN signal can finally be expressed as:

$$\mathbf{w} = \frac{\mathbf{V}_2}{\sqrt{U-1}} \tilde{\mathbf{w}}. \tag{4.10}$$

Equation (4.10) ensures that (4.8) is satisfied for any arbitrary vector $\tilde{\mathbf{w}} \in \mathbb{C}^{Q-N \times 1}$. Since $Q = NU$, as soon as $U \geq 2$, there is an infinite set of solutions to generate $\tilde{\mathbf{w}}$ and therefore the AN signal. In the following, it is assumed that $\tilde{\mathbf{w}} \sim \mathbb{CN}(\mathbf{0}_{Q-N}, \mathbf{I}_{Q-N})$. The AN signal is then generated thanks to (4.10) with a normalization factor ensuring a total energy per symbol of 1.

4.5.1.3 Received signal expressions

Received signal at Bob

From Figure 4.5 and equation (4.4), the received sequence at the intended position can be written as:

$$\begin{aligned}\mathbf{y}_{\mathrm{B}}^{\mathrm{SISO}} =& \sqrt{\alpha}\mathbf{S}^H\mathbf{H_B}\widehat{\mathbf{H}}_{\mathbf{B}}^H\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H_B}\mathbf{w} + \mathbf{S}^H\mathbf{v}_{\mathrm{B}} \\ =& \underbrace{\sqrt{\alpha(1-\sigma)}\mathbf{S}^H||\mathbf{H_B}||^2\mathbf{S}\mathbf{x} + \sqrt{\alpha\sigma}\mathbf{S}^H\mathbf{H_B}\Delta\mathbf{H}_{\mathbf{B}}^H\mathbf{S}\mathbf{x}}_{\text{data}} + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H_B}\mathbf{w}}_{\text{AN interference}} + \underbrace{\mathbf{S}^H\mathbf{v}_{\mathrm{B}}}_{\text{noise}},\end{aligned} \tag{4.11}$$

where the AN has been designed such that $\mathbf{S}^H\widehat{\mathbf{H}}_{\mathbf{B}}\mathbf{w} = \mathbf{0}_N$

Equation (4.11) shows that each transmitted data symbol x_n is affected by a complex gain

$$\frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^2 + \frac{\sqrt{\alpha\sigma}}{U}\sum_{i=0}^{U-1}h_{\mathrm{B},n+iN}\Delta h_{\mathrm{B},n+iN}^*$$

at the legitimate receiver position. If Alice perfectly estimates Bob's CSI (σ=0), the received useful signal power at Bob benefits from a real gain due to frequency diversity and increases with the BOR value. Considering a fixed bandwidth, the TR focusing effect is enhanced for higher BORs at the expense of the data rate. It can be pointed out that the summation over the index i represents the addition of the U replicas of the n^{th} symbol.

From equation (4.11), some AN leaks at Bob in case of imperfect main channel state information. Indeed, the AN interference term is given by:

$$\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H_B}\mathbf{w}. \tag{4.12}$$

However, when Alice perfectly estimates Bob's CSI, i.e., $\sigma = 0$, the AN interference term cancels out. Indeed, when $\sigma = 0$, it comes $\widehat{\mathbf{H}}_{\mathbf{B}} = \mathbf{H_B}$. Therefore, the AN interference term (4.12) becomes:

$$\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H_B}\mathbf{w} = \sqrt{1-\alpha}\mathbf{S}^H\widehat{\mathbf{H}}_{\mathbf{B}}\mathbf{w} = \mathbf{0}_N, \tag{4.13}$$

thanks to (4.8).

Notation 4.1

The subscript $n+iN$ highlights the fact that two subsequent components of a symbol are separated by N subcarriers. However, to compact the notations, the subscript $n+iN$ will be written i. Every subscript referring to a symbol component will be written in its compact form in the following of this manuscript.

Received signal at Eve(s)

At Eve(s), the received signal is given by:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{SISO},\mathbf{D}} = \underbrace{\sqrt{\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\widehat{\mathbf{H}}_{\mathbf{B}}^*\mathbf{S}\mathbf{x}}_{\text{data}} + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\mathbf{w}}_{\text{AN interference}} + \underbrace{\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{D}_{\mathbf{E},k}\mathbf{v}_{\mathrm{E},k}}_{\text{noise}}, \tag{4.14}$$

where the superscript $\mathbf{D}$ stands for the particular decoder used in a given handshake procedure. The nature of the decoding matrix $\mathbf{D_E}$ depends on handshake procedures detailed in section 4.6. The gain of the data component in (4.14) is given by:

$$\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_E}d_{\mathbf{E},k,i}h_{\mathbf{E},k,i}\tilde{h}_{\mathbf{B},i}^*,$$

and depends on $\mathbf{D_E}$ and does not generally provide an SNR enhancement. Similarly, the AN component does not generally cancel out, depending on $\mathbf{D_E}$. It is to be noted that, since $\mathbf{w}$ is generated from an infinite and random set of possibilities, even if Eve knows $\sum_{k=1}^{N_E}\mathbf{H}_{\mathbf{E},k}\widehat{\mathbf{H}}_{\mathbf{B}}^H$ and $\mathbf{S}$, she cannot estimate the AN signal to try retrieving the data.

4.5.2 MISO system

If Alice has a multi-antenna transmitter ($N_A > 1$) and Bob is a single-antenna legitimate receiver ($N_B = 1$), the system is said to be MISO. In this scheme, the channel between Alice's k^{th} antenna ($k = 1, ..., N_A$) and Bob is $\mathbf{H}_{\mathbf{B},k}$. MISO systems can be subdivided into multiple-input single-output single-eavesdropper (MISO-SE) and multiple-input single-output muti-eavesdropper (MISO-ME) if the eavesdropper structure has one or multiple antennas, respectively. The channel between Alice's k^{th} antenna ($k = 1, ..., N_A$) and Eve's l^{th} antenna ($l = 1, ..., N_E$) is $\mathbf{H}_{\mathbf{E},lk}$. The study of the MISO scheme may correspond to a DL communication between a BS (multiple-antenna Alice) and a UE with limited capabilities (single-antenna Bob), in the presence of single or multi-antenna eavesdropper(s). The different MISO system configurations are depicted in Figure 4.6.

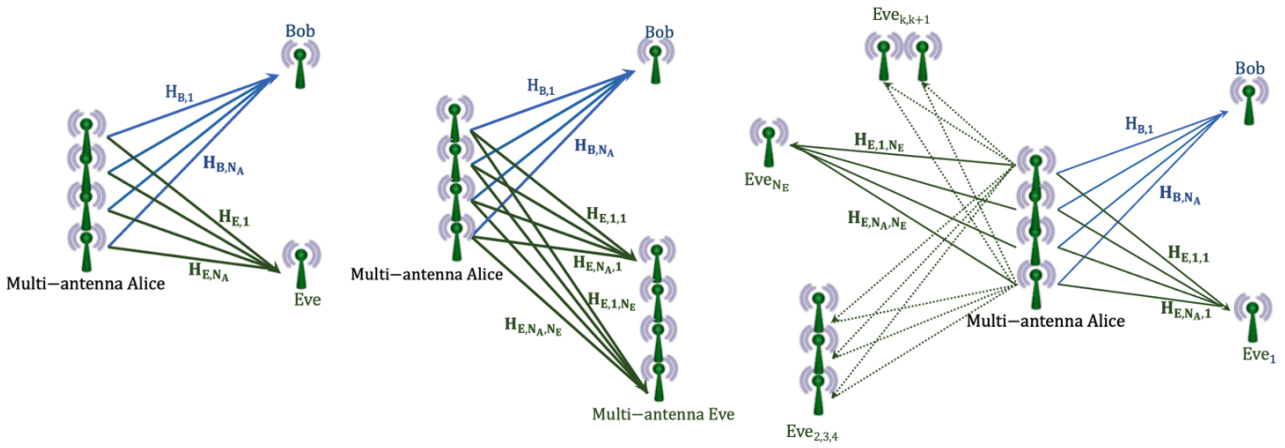

Figure 4.6: MISO configurations: single-antenna eavesdropper (left), multi-antenna eavesdropper (centre), multi-eavesdroppers (right).

4.5.2.1 System presentation

In a MISO-ME system, N_A signals are transmitted at Alice towards Bob's single antenna. The N_A signals are eavesdropped by N_E receiving antennas at Eve(s).

- $\mathbf{S}$ is a $Q \times N$ spreading matrix defined in (4.3).
- $\mathbf{H_B} = \left[\mathbf{H}_{\mathbf{B},1}, ..., \mathbf{H}_{\mathbf{B},N_A}\right]^T$ is a $Q \times (Q \times N_A)$ MISO channel, where each SISO subchannel $\mathbf{H}_{\mathbf{B},k}$, $k = 1, ..., N_A$ is a $Q \times Q$ diagonal matrix whose elements are $h_{\mathrm{B},k,q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\mathrm{B},k,q}$ represents the q^{th} channel coefficient between Alice k^{th} antenna and Bob's single antenna.
- $\mathbf{H_E} = \left[\mathbf{H}_{\mathbf{E},1}, ..., \mathbf{H}_{\mathbf{E},N_E}\right]^T$ is a $(Q \times N_E) \times (Q \times N_A)$ MIMO channel, where each MISO subchannel $\mathbf{H}_{\mathbf{E},l} = \left[\mathbf{H}_{\mathbf{E},l1}, ..., \mathbf{H}_{\mathbf{B},lN_A}\right]^T$, $l = 1, ..., N_E$, is a $Q \times (Q \times N_A)$ matrix. Each SISO subchannel $\mathbf{H}_{\mathbf{E},lk}$, $k = 1, ..., N_A$, $l = 1, ..., N_E$, is a $Q \times Q$ diagonal matrix whose elements are $h_{\mathrm{E},lk,q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\mathrm{E},lk,q}$ represents the q^{th} channel coefficient between Alice k^{th} antenna and Eve l^{th} antenna.
- The precoding matrix $\mathbf{P} = \left[\widetilde{\mathbf{H}}^H_{\mathbf{B},1}, ..., \widetilde{\mathbf{H}}^H_{\mathbf{B},N_A}\right]^T$ in Figure 4.3 is a $(Q \times N_A) \times Q$ matrix where $\widehat{\mathbf{H}}_{\mathbf{B},k}$ ($k = 1, ..N_A$) is diagonal matrix whose elements are $\tilde{h}^*_{\mathrm{B},k,q} \sim \mathbb{CN}(0,1)$.
- The channel error matrix $\Delta\mathbf{H_B} = \left[\Delta\mathbf{H}_{\mathbf{B},1}, ..., \Delta\mathbf{H}_{\mathbf{B},N_A}\right]^T$ in (4.7) is a $(Q \times N_A) \times Q$ matrix where $\Delta\mathbf{H}_{\mathbf{B},k}$ ($k = 1, ..N_A$) is diagonal matrix whose elements are $\Delta h_{\mathrm{B},k,q} \sim \mathbb{CN}(0,1)$.
- The decoding matrix at Bob is $\mathbf{D_B} = \mathbf{S}^H$, which is the despreading matrix of dimension $N \times Q$.

- The decoding matrix at Eve is $\mathbf{D_E} = \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}$, whose nature depends on the handshake procedure between Alice and Bob. $\mathbf{D}_{\mathbf{E},k}$, $k = 1, ..., N_E$, is a $Q \times Q$ diagonal matrix whose elements are $d_{\mathbf{E},k,q}$, $q = 1, ..., Q$.

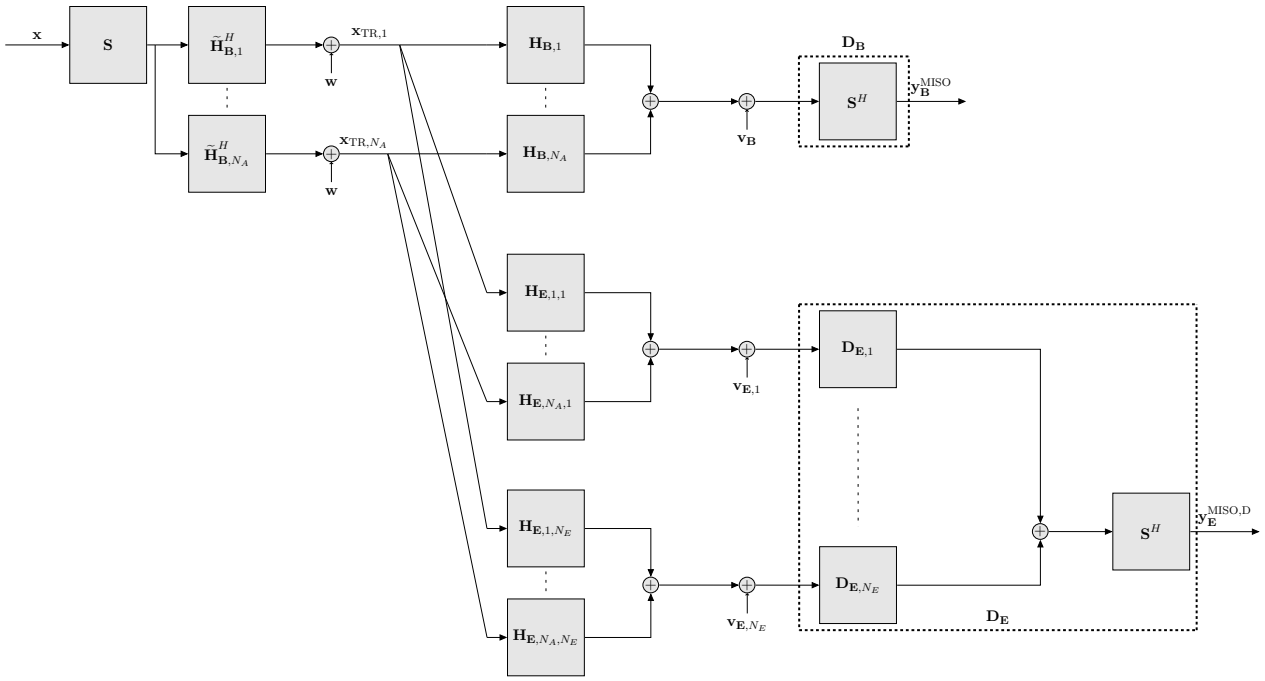

Figure 4.7: MISO-ME block diagram

4.5.2.2 Artificial noise generation

Figure 4.7 shows the block diagram of the considered MISO scenario. To ensure the AN lies in Bob's null-space, Alice must design the AN based on the available CSI, such as:

$$\mathbf{S}^H \sum_{k=1}^{N_A} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{w} = \mathbf{A}\mathbf{w} = \mathbf{0}_N. \tag{4.15}$$

To design an AN signal that satisfies equation (4.15), an SVD of A is performed, leading to:

$$\mathbf{A} = \mathbf{S}^H \sum_{k=1}^{N_A} \widehat{\mathbf{H}}_{\mathbf{B},k} = \mathbf{U} \left(\Sigma \, \mathbf{0}_{Q-N \times Q} \right) \begin{pmatrix} \mathbf{V}_1^H \\ \mathbf{V}_2^H \end{pmatrix}, \tag{4.16}$$

where $\mathbf{U}$, Σ, $\mathbf{V}_1$, and $\mathbf{V}_2$ are defined in Section 4.5.1.2. Finally, the AN signal can be expressed as:

$$\mathbf{w} = \frac{\mathbf{V}_2}{\sqrt{N_A(U-1)}} \tilde{\mathbf{w}}, \tag{4.17}$$

where the normalization factor ensures a total energy per transmitted symbol of 1.

4.5.2.3 Received signal expressions

Received signal at Bob

From Figure 4.7 and equation (4.4), the received signal at Bob is therefore given by:

$$\begin{aligned}\mathbf{y}_{\mathbf{B}}^{\text{MISO}} =& \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{H}_{\mathbf{B},k}\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\mathbf{w} + \mathbf{S}^H\mathbf{v}_{\text{B}} \\ =& \underbrace{\sqrt{\alpha(1-\sigma)}\mathbf{S}^H \sum_{k=1}^{N_A} ||\mathbf{H}_{\mathbf{B},k}||^2 \mathbf{S}\mathbf{x} + \sqrt{\alpha\sigma}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x}}_{\text{data}} \\ &+ \underbrace{\sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\mathbf{w}}_{\text{AN interference}} + \underbrace{\mathbf{S}^H\mathbf{v}_{\text{B}}}_{\text{noise}},\end{aligned} \tag{4.18}$$

where the AN has been designed such that $\mathbf{S}^H \sum_{k=1}^{N_A} \widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{w} = \mathbf{0}_N$.

As for the SISO configuration, equation (4.18) shows that each transmitted data symbol is affected by a complex gain

$$\frac{\sqrt{\alpha(1-\sigma)}}{UN_A} \sum_{i=0}^{U-1}\sum_{k=1}^{N_A} |h_{\text{B},k,i}|^2 + \frac{\sqrt{\alpha\sigma}}{UN_A} \sum_{i=0}^{U-1}\sum_{k=1}^{N_A} h_{\text{B},k,i}\Delta h_{\text{B},k,i}^H$$

at the legitimate receiver position. If Alice perfectly estimates Bob's CSI ($\sigma = 0$), the received useful signal power at Bob benefits from a real gain due to frequency diversity which increases with the BOR value, and an array gain increasing with N_A. Considering a fixed bandwidth, the TR focusing effect is enhanced for higher BORs at the expense of the data rate.

From equation (4.18), some AN leaks at Bob in case of imperfect main channel state information. Indeed, the AN interference term is given by:

$$\sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\mathbf{w}. \tag{4.19}$$

However, when Alice perfectly estimates Bob's CSI, i.e., $\sigma = 0$, the AN interference term cancels out. Indeed, when $\sigma = 0$, it comes $\widehat{\mathbf{H}}_{\mathbf{B},k} = \mathbf{H}_{\mathbf{B},k}$. Therefore, the AN interference term (4.19) becomes:

$$\sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\mathbf{w} = \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{w} = \mathbf{0}_N, \tag{4.20}$$

thanks to (4.15).

Received signal at Eve(s)

At the eavesdropper's position(s), the received signal is given by:

$$\mathbf{y}_{\text{E}}^{\text{MISO},\mathbf{D}} = \underbrace{\sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{D}_{\mathbf{E},l}\mathbf{H}_{\mathbf{E},lk}\widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x}}_{\text{data}} + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{D}_{\mathbf{E},l}\mathbf{H}_{\mathbf{E},lk}\mathbf{w}}_{\text{AN interference}} + \underbrace{\mathbf{S}^H \sum_{l=1}^{N_E} \mathbf{D}_{\mathbf{E},l}\mathbf{v}_{\text{E},l}}_{\text{noise}}, \tag{4.21}$$

where the superscript $\mathbf{D}$ stands for the particular decoder used in a given handshake procedure.

The gain of the data component in (4.21) is given by:

$$\frac{\sqrt{\alpha}}{U} \sum_{i=0}^{U-1}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E} d_{\mathbf{E},l,i} h_{\mathbf{E},lk,i} \tilde{h}_{\mathbf{B},k,i}^*,$$

and depends on $\mathbf{D}_{\mathbf{E}}$, which does not generally provide an SNR enhancement. Similar to the SISO system, the AN component does not generally cancel out, depending on $\mathbf{D}_{\mathbf{E}}$. Again, since $\mathbf{w}$ is generated from an infinite and random set of possibilities, even if Eve knows $\sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}\widehat{\mathbf{H}}_{\mathbf{B},k}^H$ and $\mathbf{S}$, she cannot estimate the AN signal to try retrieving the data.

4.5.3 SIMO system

In a SIMO system, the transmitter has only one antenna ($N_A = 1$), the legitimate receiver is equipped with multiple antennas ($N_B > 1$), and the eavesdropper possesses one or multiple antennas: single-input multiple-output single-eavesdropper (SIMO-SE) or single-input multiple-output muti-eavesdropper (SIMO-ME) systems, respectively. $\mathbf{H_{B},}_k$ is the channel between Alice and Bob's k^{th} antenna ($k = 1, ..., N_B$), and $\mathbf{H_{E},}_k$ is the channel between Alice and Eve's k^{th} antenna ($k = 1, ..., N_E$). This configuration may illustrate an UL communication between an UE with limited capabilities (here, a single-antenna Alice) and a BS (here, a multi-antenna Bob), in the presence of a single or multi-antenna eavesdropper(s). The different SIMO configurations are depicted in Figure 4.8.

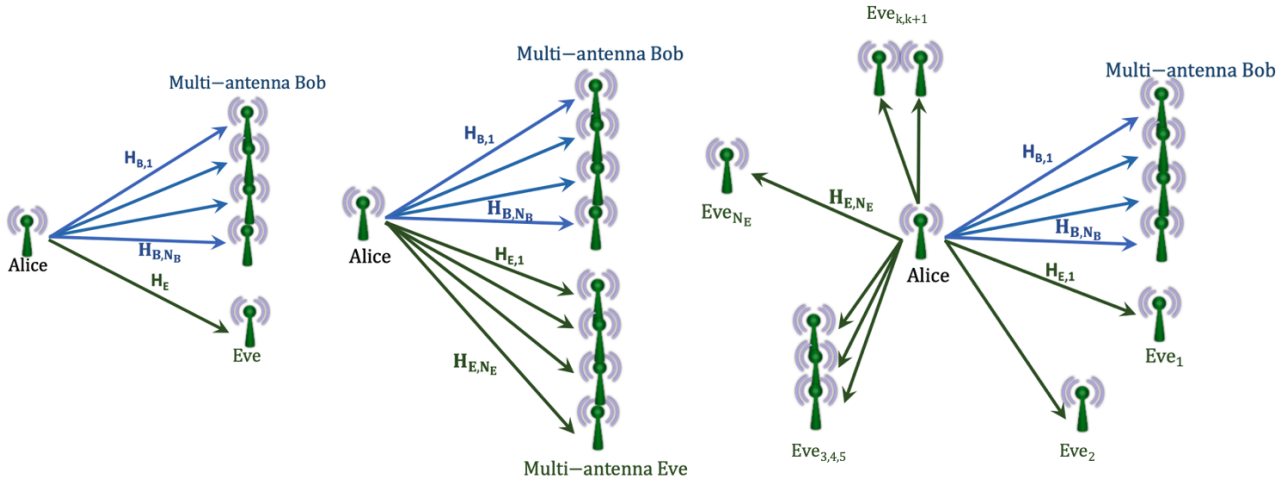

Figure 4.8: SIMO configurations: single-antenna eavesdropper (left), multi-antenna eavesdropper (centre), multi-eavesdroppers (right).

In a SIMO configuration, the signal is transmitted towards N_B and N_E antennas, at the legitimate receiver and the eavesdropper positions, respectively. In what follows, two SIMO schemes are introduced and motivated, depending on the precoding at the transmitter side.

4.5.3.1 Scheme 1: SIMO no precoding

4.5.3.1.1 System presentation

In that situation, Alice only spreads the useful data block and adds AN before transmission. At the receiving side, Bob recombines the N_B received signals with an MRC decoding structure. The MRC structure that was usually implemented at the transmitter side, thanks to a TR precoding at Alice in SISO or MISO configurations, is here implemented at the receiving side. The block diagram of the SIMO scheme without precoding is depicted in Figure 4.9.

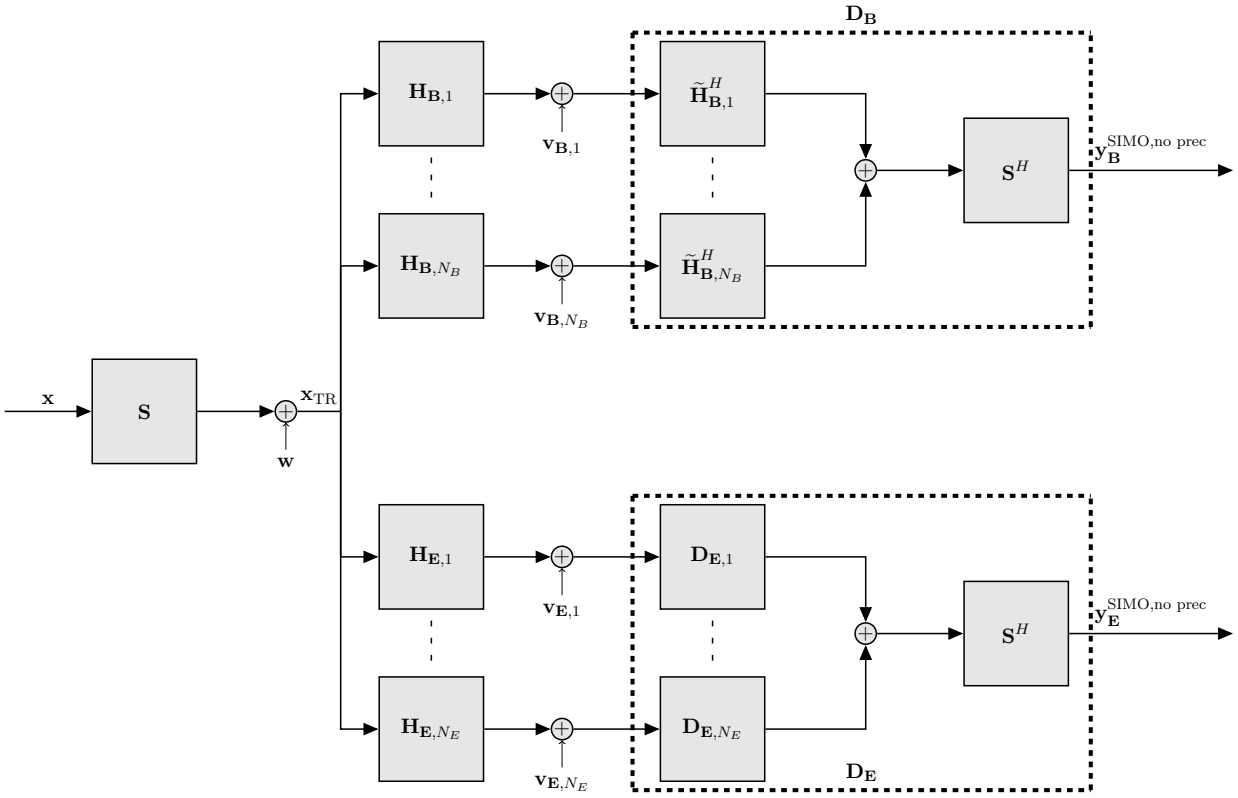

Figure 4.9: SIMO-ME without precoding block diagram

In this scenario, the system is described as follow:

- $\mathbf{S}$ is a $Q \times N$ spreading matrix defined in (4.3) with $N_A = 1$.
- $\mathbf{H_B} = \left[\mathbf{H_{B}},_1, ..., \mathbf{H_{B},}_{N_B}\right]^T$ is a $(Q \times N_B) \times Q$ SIMO channel, where each SISO subchannel $\mathbf{H_{B},}_k$, $k = 1, ..., N_B$ is a $Q \times Q$ diagonal matrix whose elements are $h_{\text{B},k,q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\text{B},k,q}$ represents the q^{th} channel coefficient between Alice single-antenna and Bob's k^{th} antenna.
- $\mathbf{H_E} = \left[\mathbf{H_{E}},_1, ..., \mathbf{H_{E},}_{N_E}\right]^T$ is a $(Q \times N_E) \times Q$ SIMO channel, where each SISO subchannel $\mathbf{H_{E},}_k$, $k = 1, ..., N_E$ is a $Q \times Q$ diagonal matrix whose elements are $h_{\text{E},k,q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\text{E},k,q}$ represents the q^{th} channel coefficient between Alice single-antenna and Eve's k^{th} antenna.
- The precoding matrix $\mathbf{P}$ in Figure 4.3 is an identity matrix $\mathbf{P} = \mathbf{I}_Q$, i.e., Alice does not precode the transmitted data (so $\mathbf{P}$ does not appear in Figure 4.9).
- The channel error matrix $\Delta\mathbf{H_B} = \left[\Delta\mathbf{H_{B}},_1, ..., \Delta\mathbf{H_{B},}_{N_B}\right]^T$ in (4.7) is a $(Q \times N_B) \times Q$ matrix where $\Delta\mathbf{H_{B},}_k$ $(k = 1, ..N_B)$ is diagonal matrix whose elements are $\Delta h_{\text{B},k,q} \sim \mathbb{CN}(0,1)$.
- The decoding matrix at Bob is $\mathbf{D_B} = \mathbf{S}^H \sum_{k=1}^{N_B} \widehat{\mathbf{H}}^H_{\mathbf{B},k}$, which allows him to implement an MRC receiver.
- The decoding matrix at Eve is $\mathbf{D_E} = \sum_{k=1}^{N_E} \mathbf{D_{E},}_k$, whose nature depends on the handshake procedure between Alice and Bob. $\mathbf{D_{E},}_k$, $k = 1, ..., N_E$, is a $Q \times Q$ diagonal matrix whose elements are $d_{\mathbf{E},k,q}$, $q = 1, ..., Q$.

4.5.3.1.2 Artificial noise generation

From Figure 4.9, Alice attempts to design the AN signal such that it lies in Bob's estimated null space:

$$\mathbf{S}^H \sum_{k=1}^{N_B} \left|\left|\widehat{\mathbf{H}}_{\mathbf{B},k}\right|\right|^2 \mathbf{w} = \mathbf{A}\mathbf{w} = \mathbf{0}_N. \tag{4.22}$$

To do so, an SVD of $\mathbf{A}$ is performed, leading to:

$$\mathbf{A} = \mathbf{S}^H \sum_{k=1}^{N_B} \left|\left|\widehat{\mathbf{H}}_{\mathbf{B},k}\right|\right|^2 = \mathbf{U}\left(\Sigma\ \mathbf{0}_{Q-N\times Q}\right)\begin{pmatrix}\mathbf{V}_1^H \\ \mathbf{V}_2^H\end{pmatrix}, \tag{4.23}$$

where $\mathbf{U}$, Σ, $\mathbf{V}_1$, and $\mathbf{V}_2$ are defined in Section 4.5.1.2. Finally, the AN signal can be expressed as:

$$\mathbf{w} = \frac{\mathbf{V}_2}{\sqrt{U-1}}\tilde{\mathbf{w}}, \tag{4.24}$$

where the normalization factor ensures a total energy per transmitted symbol of 1.

Remark 4.5: SIMO without precoding

Unlike the other communication schemes, the above SIMO scenario requires that Bob knows his own CSI in order to implement an MRC decoder, as explained in section 4.6.3.4.

4.5.3.1.3 Received signal expressions

Received signal at Bob

From Figure 4.9 and equation (4.4), the received signal at Bob can be expressed as:

$$\begin{aligned}\mathbf{y}_{\mathbf{B}}^{\text{SIMO, no precod}} =& \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{H}_{\mathbf{B},k}\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_B} \mathbf{H}_{\mathbf{B},k}\widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{w} + \mathbf{S}^H \sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{v}_{\mathrm{B},k} \\ =& \underbrace{\sqrt{\alpha(1-\sigma)}\mathbf{S}^H \sum_{k=1}^{N_B} \left|\left|\mathbf{H}_{\mathbf{B},k}\right|\right|^2 \mathbf{S}\mathbf{x} + \sqrt{\alpha\sigma}\mathbf{S}^H \sum_{k=1}^{N_B} \mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x}}_{\text{data}} \\ &+ \underbrace{\sqrt{(1-\alpha)(1-\sigma)}\mathbf{S}^H \sum_{k=1}^{N_B} \left|\left|\mathbf{H}_{\mathbf{B},k}\right|\right|^2 \mathbf{w} + \sqrt{(1-\alpha)\sigma}\mathbf{S}^H \sum_{k=1}^{N_B} \mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}_{\mathbf{B},k}^H \mathbf{w}}_{\text{AN interference}} \\ &+ \underbrace{\mathbf{S}^H \sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{v}_{\mathrm{B},k}}_{\text{noise}}.\end{aligned} \tag{4.25}$$

Similar to the SISO and MISO configurations, equation (4.25) shows that each transmitted data symbol is affected by a complex gain

$$\frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_B}|h_{\mathrm{B},k,i}|^2 + \frac{\sqrt{\alpha\sigma}}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_B} h_{\mathrm{B},k,i}\Delta h_{\mathrm{B},k,i}^H$$

at the legitimate receiver position. If Alice perfectly estimates Bob's CSI ($\sigma = 0$), the received useful signal power at Bob benefits from a real gain due to frequency diversity which increases with the BOR value, and an array gain increasing with N_B. Considering a fixed bandwidth, the TR focusing effect is enhanced for higher BORs at the expense of the data rate.

From equation (4.25), some AN leaks at Bob in case of imperfect main channel state information. Indeed, the AN interference term is given by:

$$\sqrt{(1-\alpha)(1-\sigma)}\mathbf{S}^H \sum_{k=1}^{N_B} \left|\left|\mathbf{H}_{\mathbf{B},k}\right|\right|^2 \mathbf{w} + \sqrt{(1-\alpha)\sigma}\mathbf{S}^H \sum_{k=1}^{N_B} \mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}_{\mathbf{B},k}^H \mathbf{w}. \tag{4.26}$$

However, when Alice perfectly estimates Bob's CSI, i.e., $\sigma = 0$, the AN interference term cancels out. Indeed, when $\sigma = 0$, it comes $\widehat{\mathbf{H}}_{\mathbf{B},k} = \mathbf{H}_{\mathbf{B},k}$. Therefore, the AN interference term (4.26) becomes:

$$\sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{\mathbf{B},k}||^2 \mathbf{w} = \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_B} \left|\left|\widehat{\mathbf{H}}_{\mathbf{B},k}\right|\right|^2 \mathbf{w} = \mathbf{0}_N, \tag{4.27}$$

thanks to (4.22).

Received signal at Eve(s)
At Eve(s), the received signal takes the following form:

$$\mathbf{y}_{\mathrm{E}}^{\text{SIMO, no precod,}\mathbf{D}} = \underbrace{\sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\mathbf{S}\mathbf{x}}_{\text{data}} + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\mathbf{w}}_{\text{AN interference}} + \underbrace{\mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}\mathbf{v}_{\mathrm{E},k}}_{\text{noise}}, \tag{4.28}$$

where the superscript $\mathbf{D}$ stands for the particular decoder used in a given handshake procedure.
The gain of the data component in (4.28) is given by:

$$\frac{\sqrt{\alpha}}{U} \sum_{i=0}^{U-1} \sum_{k=1}^{N_E} d_{\mathbf{E},k,i} h_{\mathbf{E},k,i},$$

and depends on $\mathbf{D}_{\mathbf{E}}$, which does not generally provide an SNR enhancement. Similar to the SISO and MISO systems, the AN component does not generally cancel out, depending on $\mathbf{D}_{\mathbf{E}}$. Again, since $\mathbf{w}$ is generated from an infinite and random set of possibilities, even if Eve knows $\sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}$ and $\mathbf{S}$, she cannot estimate the AN signal to try retrieving the data.

4.5.3.2 Scheme 2: SIMO precoding

4.5.3.2.1 System presentation

The block diagram of the SIMO scheme with precoding is depicted in Figure 4.10.

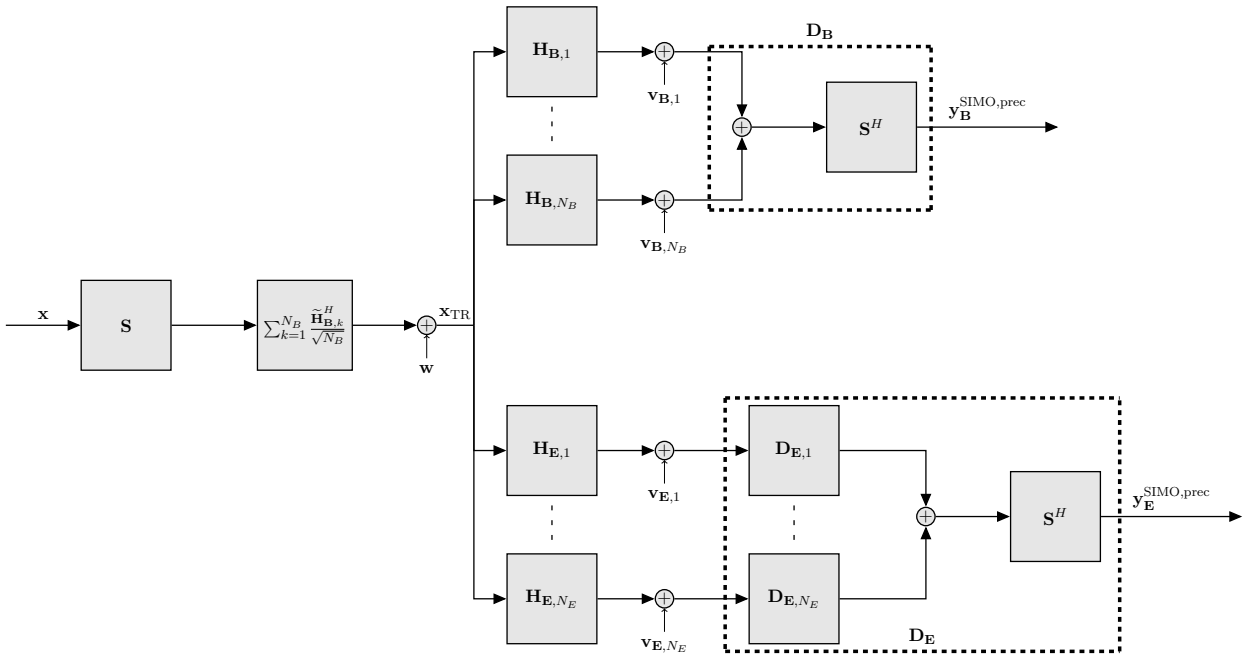

Figure 4.10: SIMO-ME with precoding block diagram

In a SIMO configuration, it can be interesting to somehow precode the data at the transmitter side to further jeopardize data retrieval at Eve, as explained in chapter 6. Since Alice possesses only

one antenna, she can estimate the sum of the subchannel components between her antenna and the legitimate receiver's antennas, thanks to a prior pilot sent by Bob. Therefore, she can precode the useful data with the sum of the complex conjugate of the subchannel estimates.

The system is described as follow:

- $\mathbf{H_B} = \left[\mathbf{H}_{\mathbf{B},1}, ..., \mathbf{H}_{\mathbf{B},N_B}\right]^T$ is a $Q \times (Q \times N_B)$ SIMO channel, where each SISO subchannel $\mathbf{H}_{\mathbf{B},k}$, $k = 1, ..., N_B$ is a $Q \times Q$ diagonal matrix whose elements are $h_{\mathrm{B},k,q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\mathrm{B},k,q}$ represents the q^{th} channel coefficient between Alice single-antenna and Bob's k^{th}.
- $\mathbf{H_E} = \left[\mathbf{H}_{\mathbf{E},1}, ..., \mathbf{H}_{\mathbf{E},N_E}\right]^T$ is a $Q \times (Q \times N_E)$ SIMO channel, where each SISO subchannel $\mathbf{H}_{\mathbf{E},k}$, $k = 1, ..., N_E$ is a $Q \times Q$ diagonal matrix whose elements are $h_{\mathrm{E},k,q} \sim \mathbb{CN}(0,1)$, $q = 1, ..., Q$. $h_{\mathrm{E},k,q}$ represents the q^{th} channel coefficient between Alice single-antenna and Eve's k^{th} antenna.
- The precoding matrix $\mathbf{P} = \frac{1}{\sqrt{N_B}} \sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k}^H$ in Figure 4.3 is a $Q \times Q$ diagonal matrix. The scaling factor $\frac{1}{\sqrt{N_B}}$ ensures energy normalization at the transmitter side, i.e., it ensures a total transmitted energy of 1 per symbol.
- The channel error matrix $\Delta\mathbf{H_B} = \left[\Delta\mathbf{H}_{\mathbf{B},1}, ..., \Delta\mathbf{H}_{\mathbf{B},N_B}\right]^T$ in (4.7) is a $Q \times (Q \times N_B)$ matrix where $\Delta\mathbf{H}_{\mathbf{B},k}$ $(k = 1, ..N_B)$ is diagonal matrix whose elements are $\Delta h_{\mathrm{B},k,q} \sim \mathbb{CN}(0,1)$.
- The decoding matrix at Bob is $\mathbf{D_B} = \mathbf{S}^H$, which is the despreading of dimension $N \times Q$.
- The decoding matrix at Eve is $\mathbf{D_E} = \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}$, whose nature depends on the handshake procedure between Alice and Bob as detailed later on. $\mathbf{D}_{\mathbf{E},k}$, $k = 1, ..., N_E$, is a $Q \times Q$ diagonal matrix whose elements are $d_{\mathbf{E},k,q}$, $q = 1, ..., Q$.

4.5.3.2.2 Artificial noise generation

From Figure 4.10, Alice intends to design an AN signal that lies in Bob's null space as:

$$\mathbf{S}^H \sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{w} = \mathbf{A}\mathbf{w} = \mathbf{0}_N. \tag{4.29}$$

To do so, an SVD of $\mathbf{A}$ is performed, leading to:

$$\mathbf{A} = \mathbf{S}^H \sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k} = \mathbf{U} \left(\Sigma \; \mathbf{0}_{Q-N \times Q}\right) \begin{pmatrix} \mathbf{V}_1^H \\ \mathbf{V}_2^H \end{pmatrix}, \tag{4.30}$$

where $\mathbf{U}$, Σ, $\mathbf{V}_1$, and $\mathbf{V}_2$ are defined in Section 4.5.1.2. Finally, the AN signal can be written as:

$$\mathbf{w} = \frac{\mathbf{V}_2}{\sqrt{U-1}} \tilde{\mathbf{w}}, \tag{4.31}$$

where the normalization factor ensures a total energy per transmitted symbol of 1.

4.5.3.2.3 Received signal expressions

Received signal at Bob

From Figure 4.10 and equation (4.4), the received signal at Bob is therefore given by:

$$\mathbf{y}_{\mathbf{B}}^{\text{SIMO, precod}} = \underbrace{\sqrt{\frac{\alpha}{N_B}} \mathbf{S}^H \sum_{k=1}^{N_B} \sum_{k'=1}^{N_B} \mathbf{H}_{\mathbf{B},k} \widetilde{\mathbf{H}}_{\mathbf{B},k'} \mathbf{S}\mathbf{x}}_{\text{data}} + \underbrace{\sqrt{1-\alpha} \mathbf{S}^H \sum_{k=1}^{N_B} \mathbf{H}_{\mathbf{B},k} \mathbf{w}}_{\text{AN interference}} + \underbrace{\mathbf{S}^H \sum_{k=1}^{N_B} \mathbf{v}_{\mathrm{B},k}}_{\text{noise}}. \tag{4.32}$$

Similar to the SISO and MISO configurations, equation (4.32) shows that each transmitted data symbol is affected by a complex gain

$$\frac{\alpha}{U}\left[\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}\left(\sqrt{1-\sigma}\,|h_{\mathrm{B},k,i}|^2+\sqrt{\sigma}h_{\mathrm{B},k,i}\Delta h^*_{\mathrm{B},k,i}\right)+\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{i=0}^{U-1}\left(\sqrt{1-\sigma}h_{\mathrm{B},k,i}h_{\mathrm{B},k',i}+\sqrt{\sigma}h_{\mathrm{B},k,i}h^*_{\mathrm{B},k',i}\right)\right]$$

at the legitimate receiver position. In addition, Bob's k^{th} antenna intercepts other subchannel signal components, which is highlighted by the sum over the k' index.
From equation (4.32), some AN leaks at Bob in case of imperfect main channel state information. Indeed, the AN interference term is given by:

$$\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_B}\mathbf{H}_{\mathbf{B},k}\mathbf{w}. \tag{4.33}$$

However, when Alice perfectly estimates Bob's CSI, i.e., $\sigma=0$, the AN interference term cancels out. Indeed, when $\sigma=0$, it comes $\widehat{\mathbf{H}}_{\mathbf{B},k}=\mathbf{H}_{\mathbf{B},k}$. Therefore, the AN interference term (4.33) becomes:

$$\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_B}\mathbf{H}_{\mathbf{B},k}\mathbf{w}=\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_B}\widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{w}=\mathbf{0}_N, \tag{4.34}$$

thanks to (4.29).

Received signal at Eve(s)
At Eve(s), the received signal is:

$$\mathbf{y}_{\mathrm{E}}^{\text{SIMO, precod,}\mathbf{D}}=\underbrace{\sqrt{\frac{\alpha}{N_B}}\mathbf{S}^H\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\widehat{\mathbf{H}}^H_{\mathbf{B},k}\mathbf{D}_{\mathbf{E},l}\mathbf{H}_{\mathbf{E},l}\mathbf{S}\mathbf{x}}_{\text{data}}+\underbrace{\sqrt{\frac{(1-\alpha)}{N_B}}\mathbf{S}^H\sum_{l=1}^{N_E}\mathbf{D}_{\mathbf{E},l}\mathbf{w}}_{\text{AN interference}}+\underbrace{\mathbf{S}^H\sum_{l=1}^{N_E}\mathbf{D}_{\mathbf{E},l}\mathbf{v}_{\mathrm{E},l}}_{\text{noise}}, \tag{4.35}$$

where the superscript $\mathbf{D}$ stands for the particular decoder used in a given handshake procedure.
The gain of the data component in (4.35) is given by:

$$\frac{\sqrt{\alpha}}{UN_B}\sum_{i=0}^{U-1}\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}d_{\mathbf{E},l,i}h_{\mathbf{E},l,i}\tilde{h}^*_{\mathbf{B},ki},,$$

and depends on $\mathbf{D}_{\mathbf{E}}$ and does not generally provide an SNR enhancement due to a TR effect. Similarly, the AN component does not generally cancel out, depending on $\mathbf{D}_{\mathbf{E}}$. It is to be noted that, since $\mathbf{w}$ is generated from an infinite and random set of possibilities, even if Eve knows $\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\mathbf{H}_{\mathbf{E},l}\widehat{\mathbf{H}}^H_{\mathbf{B},k}$ and $\mathbf{S}$, she cannot estimate the AN signal to try retrieving the data.

4.6 Handshake procedures

4.6.1 Time division duplexing and frequency division duplexing

The system that is considered in this study is a duplex communication system, i.e., a point-to-point system where the different parties can communicate in both directions. In particular, time-division duplex (TDD) and FDD communications are investigated. In a TDD communication, the users can communicate using the whole available spectrum but at different times slots. On the opposite, an FDD system allows users to communicate at the same time on different frequency slots, i.e., at the DL frequency (f_{DL}) and the UL frequency (f_{UL}), respectively, as seen in Figure 4.11.

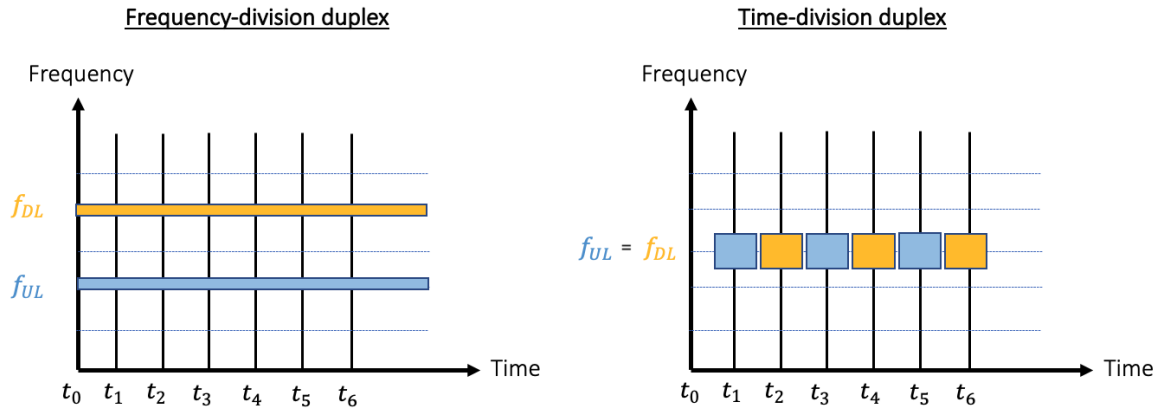

Figure 4.11: TDD and FDD communication scheme

With TDD, since the channel is reciprocal, Alice can estimate Bob's CSI with a simple pilot sent by Bob. That is, Bob does not need to feedback his CSI to Alice. On the opposite, in FDD system, the transmitter and the legitimate receiver communicate at different frequencies, and the UL and DL channels are therefore different. Consequently, the legitimate receiver has to feedback his CSI to the transmitter. In doing so, Alice obtains Bob's CSI and implements a suitable precoder. However, at the same time, an eavesdropper can also intercept Bob's CSI and benefits from this knowledge. It is worth mentioning that the pilots exchanged during handshake are sequences a priori known from Alice, Bob, and Eve.

4.6.2 Handshake preliminaries

Before the secure data transmission begins, a handshake procedure between Alice and Bob must take place. A handshake is a process between two nodes aiming to communicate, that generally occurs before the actual communication starts. During handshake, both devices exchange signals in order to agree to several rules, such as the communication protocol that will be used, or the transmission rate, for instance. Consequently, depending on the protocol and the synchronization of the communication, different handshake procedures between Alice and Bob may take place.

The handshake processes described below influence the amount of CSI Eve can estimate. In doing so, Eve can adopt different decoding strategies, which therefore leads to different secrecy performance, according to the amount of CSI she obtains. Common to all handshake procedures, Alice imperfectly estimates Bob's instantaneous CSI. This process depends on the division duplexing, as explained in Sections 4.6.3 and 4.6.4. On the opposite, the worst case scenario is considered regarding Eve. That is, it is assumed that the CSI the eavesdropper can estimate is error-free. It is also considered that the transmitter is not aware of Eve instantaneous CSI who is considered as an external passive node of the network that tries to eavesdrop the data.

As a reminder, the precoding matrices implemented by Alice may take the following forms:

- SISO system: $\mathbf{P} = \widehat{\mathbf{H}}_{\mathbf{B}}^{H}$.
- MISO system : $\mathbf{P} = \left[\widetilde{\mathbf{H}}_{\mathbf{B},1}^{H}, ..., \widetilde{\mathbf{H}}_{\mathbf{B},N_A}^{H}\right]^{T}$.
- SIMO without precoding system: $\mathbf{P} = \mathbf{I}_Q$.
- SIMO with precoding system: $\mathbf{P} = \frac{1}{\sqrt{N_B}} \sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k}^{H}$.

4.6.3 TDD handshakes

All the TDD handshake procedures described below consider a block fading (BF) channel model. That is, the main and the eavesdropper channels remain constant over a coherence interval and are independent from one interval to another. During a coherence interval, Alice transmits a burst that is composed of several OFDM blocks preceded or not by some pilots. Under BF assumption, two bursts experience different fading. In other words, Alice waits a coherence interval before performing a new channel estimation and sending a new burst, [1]. It results in an impossibility for Eve to learn some parameters from the communication, such as the AN variance, since Bob's channel varies between each sent burst. It has to be noted that, since the AN signal only depends on the main channel, it can generated at each new transmitted burst or at each new OFDM block. Generating the AN at each new burst is more power efficient compared to each new OFDM block, but it introduces less randomness.

Common to all procedures in TDD considered in this section, Bob first sends to Alice an unprecoded pilot. Therefore, Alice is able to estimate Bob's channel. The unprecoded pilot sent by Bob also allows Eve to perfectly estimate $\mathbf{H_{BE}}$, which is of no help for her. Indeed, the received signal expressions at Eve, depending on the system configuration, and given by (4.14), (4.21), (4.28), and (4.35), do not depend on the channel between Bob and Eve. Then, Alice has four ways to initiate the communication. The fourth handshake procedure is specific to the SIMO *without precoding* system as explained in section 4.6.3.4.

4.6.3.1 Handshake procedure 1: SDS decoder

In this scenario, Alice sends an OFDM burst only composed of precoded data. Eve therefore cannot estimate any communication parameter. Indeed, since no unprecoded (resp. precoded) pilot is transmitted by Alice, Eve is not able to ***estimate*** her channel (resp. her equivalent channel due to the precoding performed by Alice). In addition, under BF assumption, the channel changes between two subsequent transmitted OFDM bursts. This prevents Eve from ***learning*** her own channel, or her equivalent channel, as well as the AN variance. The scenario is shown in Figure 4.12.

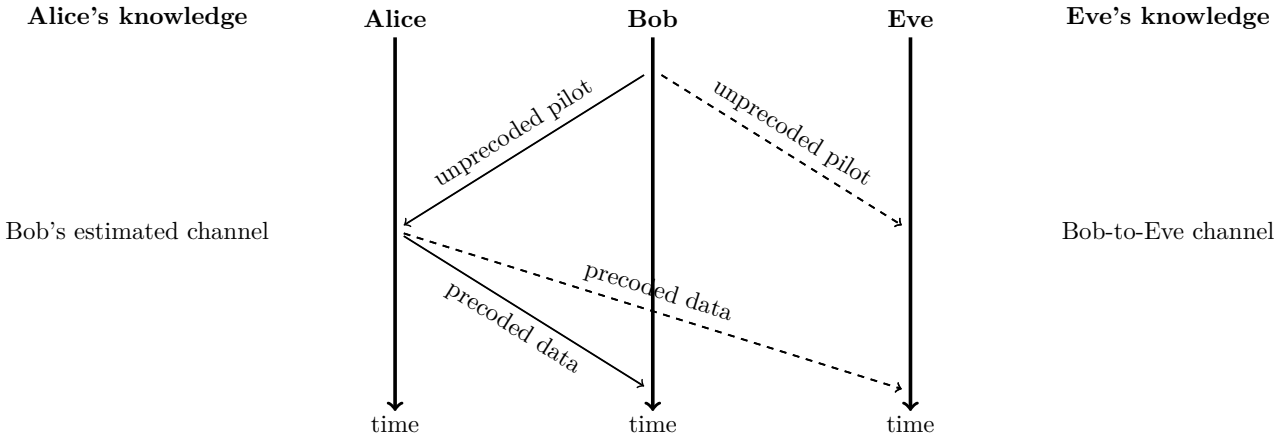

Figure 4.12: BF TDD communication, handshake procedure 1 (SDS decoder)

Having no useful information about the communication between Alice and Bob, Eve is bound to perform the same decoding structure (SDS) as Bob. The decoding matrix implemented by Eve is thus given by:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{SDS}} = \mathbf{S}^{H} \sum_{k=1}^{N_E} \mathbf{I}_Q. \tag{4.36}$$

It is to be noted that, even if different handshake procedures are used where Eve can acquire useful CSI as seen in the following sections, she might still be bound to use the simple decoder in equation (4.36). Indeed, this situation can occur if Eve is a node of the same network as the legitimate receiver,

i.e., she has the same capabilities as Bob. She therefore may not have the resources to reconfigure her physical layer features, and is bound to perform (4.36).

4.6.3.2 Handshake procedure 2: OC decoder

If Alice sends an OFDM burst composed of an unprecoded pilot prior to precoded data, as shown in Figure 4.13, Eve is then able to perfectly ***estimate*** her own channel. However, since a BF channel model is considered, Eve cannot ***learn*** some communication parameters such as her equivalent channel, or the AN variance. She therefore cannot do better but to implement a decoding structure that takes benefit of her own channel (OC) knowledge.

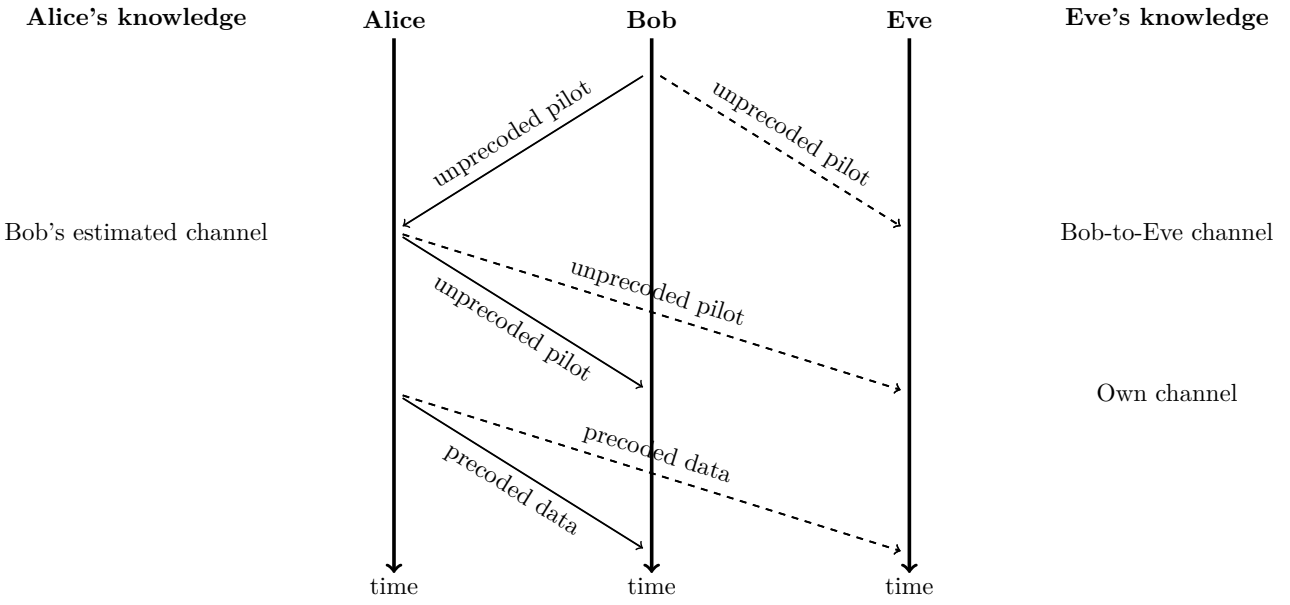

Figure 4.13: BF TDD communication, handshake procedure 2 (OC decoder)

Eve's OC decoder takes the following form depending on the system configuration.

- In a SISO system (see Figure 4.5), Eve decodes the data thanks to:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{OC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}^H. \tag{4.37}$$

- In a MISO system (see Figure 4.7), Eve decodes the data thanks to:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{OC}} = \mathbf{S}^H \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}^H. \tag{4.38}$$

- In a SIMO with precoding system (see Figure 4.10), Eve decodes the data thanks to:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{OC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}^H. \tag{4.39}$$

4.6.3.3 Handshake procedure 3: MRC decoder

If Alice sends an OFDM burst composed of a precoded pilot prior to precoded data, as depicted in Figure 4.14, Eve is then able to perfectly ***estimate*** her equivalent channel due to the precoding at Alice. Since a BF channel model is assumed, Eve cannot ***learn*** the AN variance. However, the eavesdropper is able to implement an MRC decoding structure. This decoding structure fully benefits

from Eve's equivalent channel knowledge, which is a term that arises in the expressions of the received sequences (4.14), (4.21), and (4.35).

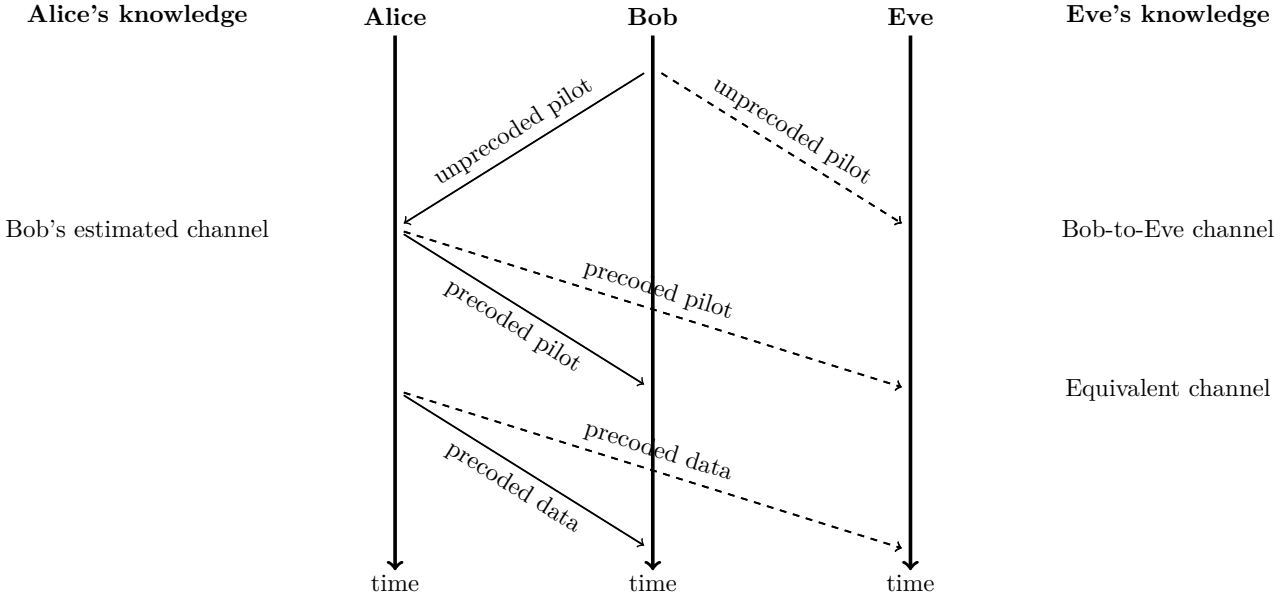

Figure 4.14: BF TDD communication, handshake procedure 3 (MRC decoder)

Eve's MRC decoder takes the following form depending on the system configuration:

- In a SISO system (see Figure 4.5), Eve decodes the data thanks to:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B}} \mathbf{H}_{\mathbf{E},k}^H. \tag{4.40}$$

- In a MISO system (see Figure 4.7), Eve decodes the data thanks to:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{H}_{\mathbf{E},lk}^H. \tag{4.41}$$

- In a SIMO with precoding system system (see Figure 4.10), Eve decodes the data thanks to:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MRC}} = \mathbf{S}^H \frac{1}{\sqrt{N_B}} \sum_{k=1}^{N_B} \sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{H}_{\mathbf{E},l}^H. \tag{4.42}$$

4.6.3.4 Handshake procedure 4: SIMO without precoding

This scenario considers a SIMO without precoding configuration, and is presented in Figure 4.15. The unprecoded pilot sent by Bob to Alice allows her to estimate $\sum_{k=1}^{N_B} \widehat{\mathbf{H}}_{\mathbf{B},k}$, which is useful to design the AN signal. It also allows Eve to perfectly estimate the channel between her and Bob, which is of no help. However, since Alice does not implement a precoding of the useful data, Bob must have the knowledge of his own CSI in order to implement an MRC receiver. This is possible only if Alice sends an unprecoded pilot to Bob, which also allows Eve to perfectly ***estimate*** her own CSI. Finally, Alice sends unprecoded data to Bob. Since a BF channel model is assumed, Eve cannot ***learn*** the AN variance. From that, she only takes benefits of her own CSI knowledge to implement an MRC decoding structure. She therefore decodes the data thanks to (see Figure 4.9) :

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}^H. \tag{4.43}$$

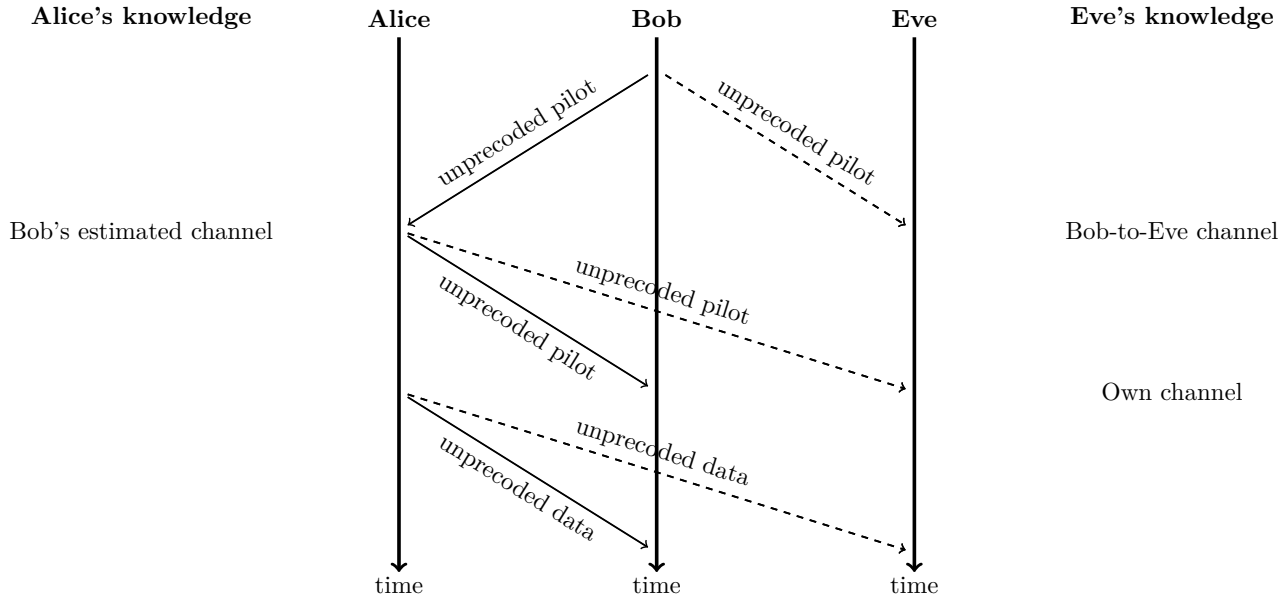

Figure 4.15: BF TDD communication, handshake procedure 4 (SIMO without precoding)

Notation 4.2

To lighten the notations, the subscripts *SISO*, *MISO*, *SIMO precod*, and *SIMO no precod* are voluntarily omitted when considering Eve's decoding matrix $\mathbf{D_E}$. For example, Eve's decoding matrix when a MRC decoder is implemented in a MISO-ME system should have been written $\mathbf{D}^{\text{MRC}}_{\mathbf{E},\text{MISO}}$ but is instead written $\mathbf{D}^{\text{MRC}}_{\mathbf{E}}$. For clarity, the system configuration (SISO, MISO, SIMO with or without precoding) is always stated so that there is no ambiguity for the reader.

4.6.4 FDD handshakes

Two handshake procedures are presented in FDD configurations depending on whether a BF channel model, or a slow fading (SF) channel model is considered. In an SF environment, Eve acquires sufficient statistics from different communications parameters, and could therefore ***learn*** these parameters, such as the AN variance for instance.

Common to both FDD protocols, Alice has to know Bob's DL CSI in order to design the AN signal and the FD TR precoder. The handshake procedures, shown in Figure 4.16 and 4.17, can be described as follows:

- Alice first initiates the communication by transmitting an unprecoded pilot, at $f = f_{\text{DL}}$.
    1. It allows Bob to estimate his DL CSI ($\widehat{\mathbf{H}}_{\mathbf{B}}$).
    2. It allows Eve to perfectly know of her DL CSI ($\mathbf{H_E}$).
- Knowing his estimated DL CSI, Bob feedbacks it to Alice, at $f = f_{\text{UL}}$.
    1. Alice therefore knows Bob's DL CSI and is able to implement the TR precoder, at $f = f_{\text{DL}}$.
    2. However, because Bob feedbacks his estimated DL CSI, Eve intercepts it and can therefore perfectly know $\widehat{\mathbf{H}}_{\mathbf{B}}$. With $\widehat{\mathbf{H}}_{\mathbf{B}}$ and $\mathbf{H_E}$, Eve has the knowledge of $\widehat{\mathbf{H}}^{H}_{\mathbf{B}}\mathbf{H_E}$.
- Alice finally sends precoded data to Bob at $f = f_{\text{DL}}$.

1. In a BF configuration, Eve cannot learn the AN variance and is limited to the knowledge of $\widehat{\mathbf{H}}_{\mathbf{B}}$, $\mathbf{H}_{\mathbf{E}}$, and $\widehat{\mathbf{H}}_{\mathbf{B}}^{H}\mathbf{H}_{\mathbf{E}}$, as depicted in Figure 4.16. She then can implement the following AN killer decoder:

$$\mathbf{D}_{\mathbf{E}}^{\text{AN killer}} = \widehat{\mathbf{H}}_{\mathbf{B}}\mathbf{H}_{\mathbf{E}}^{-1}. \tag{4.44}$$

Replacing (4.44) in the expression of the received signal in a SISO configuration, i.e., in equation (4.14), shows that the AN killer allows Eve to put the AN component in her null space. In doing so, the received signal at Eve is no more impacted by the AN. However, it also shows that the decoder amplifies the AWGN, especially when Eve is in deep fade. These effects are detailed in chapter 5.

2. Furthermore, in an SF configuration, since Alice sends multiple precoded data blocks without performing a new channel estimation, Eve could learn the AN variance σ_{AN}^2, as depicted in Figure 4.17. She can therefore implement a linear minimum mean square error (LMMSE) decoder as:

$$\mathbf{D}_{\mathbf{E}}^{\text{LMMSE}} = \sqrt{\alpha}\Gamma_{\text{E}}^{H}\left(\alpha\Gamma_{\text{E}}\Gamma_{\text{E}}^{H} + (1-\alpha)\,||\mathbf{H}_{\mathbf{E}}||^2\sigma_{\text{AN}}^2\mathbf{I}_Q + \sigma_{\text{E}}^2\mathbf{I}_Q\right)^{-1}, \tag{4.45}$$

where $\Gamma_{\text{E}} = \widehat{\mathbf{H}}_{\mathbf{B}}^{H}\mathbf{H}_{\mathbf{E}}\mathbf{S}$. The LMMSE decoder implements a trade-off between suppressing the AN and amplifying the AWGN at Eve.

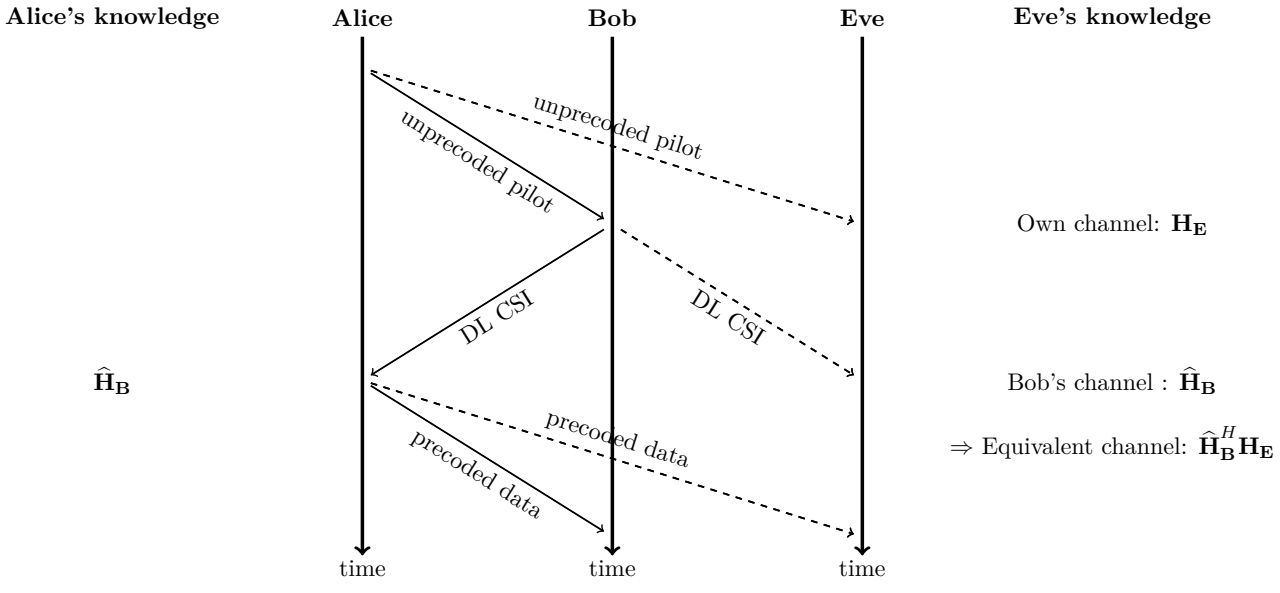

Figure 4.16: FDD handshake procedure: Block-fading (AN killer)

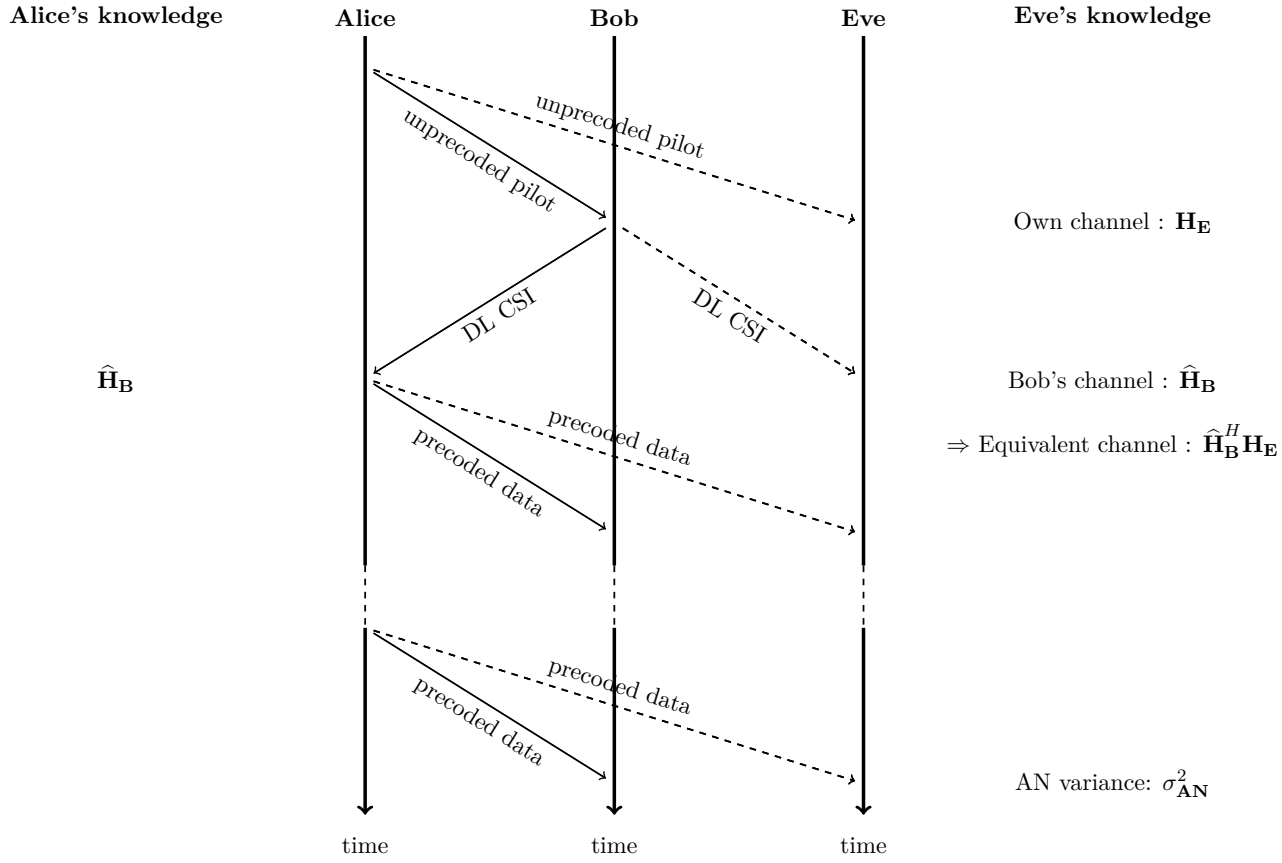

Figure 4.17: FDD handshake procedure: Slow-fading (LMMSE)

4.6.5 Handshake summary

Tables 4.1 and 4.2 summarize the different handshake procedures as a function of the system configurations in TDD and FDD environments, respectively.

Scenarios		SISO	MISO	SIMO no precoding	SIMO precoding
TDD : SDS decoder	**Figure**	Figure 4.12	Figure 4.12	/	Figure 4.12
	Fading	block fading	block fading	/	block fading
	OFDM burst	precoded data	precoded data	/	precoded data
	Decoding matrix	$\mathbf{D}_{\mathbf{E}}^{\text{SDS}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{I}_Q$	$\mathbf{D}_{\mathbf{E}}^{\text{SDS}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{I}_Q$	/	$\mathbf{D}_{\mathbf{E}}^{\text{SDS}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{I}_Q$
TDD : OC decoder	**Figure**	Figure 4.13	Figure 4.13	/	Figure 4.13
	Fading	block fading	block fading	/	block fading
	OFDM burst	unprecoded pilot + precoded data	unprecoded pilot + precoded data	/	unprecoded pilot + precoded data
	Decoding matrix	$\mathbf{D}_{\mathbf{E}}^{\text{OC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}^H$	$\mathbf{D}_{\mathbf{E}}^{\text{OC}} = \mathbf{S}^H \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}^H$	/	$\mathbf{D}_{\mathbf{E}}^{\text{OC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}^H$
TDD : MRC decoder	**Figure**	Figure 4.14	Figure 4.14	Figure 4.15	Figure 4.14
	Fading	block fading	block fading	block fading	block fading
	OFDM burst	precoded pilot + precoded data	precoded pilot + precoded data	unprecoded pilot + unprecoded data	precoded pilot + precoded data
	Decoding matrix	$\mathbf{D}_{\mathbf{E}}^{\text{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B}} \mathbf{H}_{\mathbf{E},k}^H$	$\mathbf{D}_{\mathbf{E}}^{\text{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{H}_{\mathbf{E},lk}^H$	$\mathbf{D}_{\mathbf{E}}^{\text{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}^H$	$\mathbf{D}_{\mathbf{E}}^{\text{MRC}} = \mathbf{S}^H \frac{1}{\sqrt{N_B}} \sum_{k=1}^{N_B} \sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{H}_{\mathbf{E},l}^H$

Table 4.1: TDD handshake protocols summary

Scenarios		SISO
FDD : AN killer decoder	**Figure**	Figure 4.16
	Fading	block fading
	OFDM burst	unprecoded pilot + precoded data
	Decoding matrix	$\mathbf{D}_{\mathbf{E}}^{\text{AN killer}} = \widehat{\mathbf{H}}_{\mathbf{B}} \mathbf{H}_{\mathbf{E}}^{-1}$
FDD : LMMSE decoder	**Figure**	Figure 4.17
	Fading	slow fading
	OFDM burst	unprecoded pilot + multiple precoded data
	Decoding matrix	$\mathbf{D}_{\mathbf{E}}^{\text{LMMSE}} = \sqrt{\alpha} \Gamma_{\text{E}}^H \left(\alpha \Gamma_{\text{E}} \Gamma_{\text{E}}^H + (1-\alpha) \lvert\lvert \mathbf{H}_{\mathbf{E}} \rvert\rvert^2 \sigma_{\text{AN}}^2 \mathbf{I}_Q + \sigma_{\text{E}}^2 \mathbf{I}_Q \right)^{-1}$

Table 4.2: FDD handshake protocols summary

4.7 Conclusions

This chapter presents the different system models that are studied throughout this work.

The design of the investigated PLS scheme is first motivated. In particular, the FD TR channel-based adaptation scheme is justified by the fact the TR precoding offers intrinsic anti-eavesdropping abilities. In addition, the FD implementation of TR makes this scheme compatible with existing standards, such as in 5G or LTE networks. Moreover, this implementation introduces frequency diversity, which is therefore suitable for AN injection.

It has been stated in chapter 3 that a perfect knowledge of the main CSI at the transmitter cannot be obtained in practical scenarios. Consequently, an imperfect main CSI is considered and it is assumed that the misestimate arises from noisy pilots estimation at the transmitter side. This chapter 4 introduces the model of CSI error.

Furthermore, chapter 3 outlined that the eavesdropper's capabilities to decode the data are not well discussed in the literature. Eve's capabilities depend on the amount of knowledge she can acquire from the communication, which is influenced by the handshake procedures between Alice and Bob. For that reason, practical handshake procedures are considered in this study, leading to different decoding structures that can be implemented by Eve. The handshake procedures, both in TDD and FDD configurations, are detailed in this chapter 4. In addition, several system's configurations are investigated, namely, SISO, MISO, and SIMO systems. Eve's decoding matrices for all scenarios are given allowing chapters 5 and 6 to derive closed-form approximations of the communication's ergodic secrecy rate for all investigated system configurations. Therefore, the advantages and limitations of the different handshake procedures can be assessed in these chapters.

5 | Single-Antenna System

Contents

The first part of this chapter (single-eavesdropper) is based on the results derived from the Journal Article [149] under minor reviewing in IEEE Access, and from the Conference paper [56]. The second part of this chapter (multi-eavesdropper) is based on the Letter [150] in preparation.

5.1 Introduction

This chapter presents the security performance of the SISO system, i.e., both Alice and Bob are equipped with a single antenna. Throughout this chapter, this SISO configuration is considered in the presence of a single-antenna passive eavesdropper, i.e., SISO-SE system (section 5.3), or a multi-antenna passive eavesdropper(s), i.e., SISO-ME system (section 5.4).

Chapter 4 has highlighted that, depending on the handshake procedure between Alice and Bob, Eve may acquire different amount of CSI knowledge, leading to different security performances. The implication of the handshake procedure is not well studied in the literature, as observed in chapter 3. In this work, it is considered that Eve perfectly estimates the CSI she obtains from the handshake. From that, depending on the handshake procedures in TDD systems, described in section 4.6.3, a closed-form expression of the communication ergodic secrecy rate (ESR) is derived. It allows the transmitter to design its communication parameters in order to a-priori know the secure rate over which communicate with the legitimate receiver. The data leakage is also investigated. In addition, the ESR performances of the FDD handshake procedures, described in section 4.6.4, are also assessed.

5.2 Assumptions

As a reminder, the dimensions and the nature of the matrices in a SISO system are given in section 4.5.1. The block diagram of a SISO-ME communication is shown in Figure 4.5. Throughout this chapter 5, several assumptions are undertaken:

- There are Q subcarriers per OFDM block, with a BOR of U, and $N = Q/U$ data symbols are transmitted per OFDM block.
- Alice possesses $N_A = 1$ antenna.
- Bob possesses $N_B = 1$ antenna.
- Eve possesses $N_E = 1$ antenna in a SISO-SE configuration, or $N_E > 1$ antennas in a SISO-ME configuration.
- No frequency correlation amongst Bob's subcarriers is assumed, i.e., $h_{B,i} \perp\!\!\!\perp h_{B,j}\ \forall i \neq j$, $i = 1...Q$, $j = 1...Q$.
- In a SISO-SE configuration, no frequency correlation amongst Eve's subcarriers is assumed, i.e., $h_{E,i} \perp\!\!\!\perp h_{E,j}\ \forall i \neq j$, $i = 1...Q$, $j = 1...Q$.
- In a SISO-ME configuration, no frequency correlation amongst Eve's subcarriers nor spatial correlation between Eve's antennas is assumed, i.e., $h_{E,ki} \perp\!\!\!\perp h_{E,lj}\ \forall (i,k) \neq (j,l)$, $i,j = 1...Q, \forall k,l = 1...N_E$.
- No spatial correlation between Bob's antenna and Eve's antenna(s) is assumed, i.e., $h_{B,i} \perp\!\!\!\perp h_{E,kj}\ \forall i,j$, $\forall k = 1...N_E$.
- No frequency correlation amongst the estimated error's subcarriers made by Alice and Bob's subcarriers is assumed, i.e., $h_{B,i} \perp\!\!\!\perp \Delta h_{B,j}\ \forall i,j = 1...Q$.
- No frequency correlation amongst the estimated error's subcarriers made by Alice is assumed, i.e., $\Delta h_{B,i} \perp\!\!\!\perp \Delta h_{B,j}\ \forall i \neq j$, $i = 1...Q$, $j = 1...Q$.

The uncorrelated frequency assumption is justify by the fact that, thanks to the design of the spreading matrix, the U subcarriers composing one symbol are spaced by $N = Q/U$ subcarriers. If this distance is larger than the coherence bandwidth of the channel, two components of a transmitted symbol experience uncorrelated fading, which usually occurs in rich multipath environments, or thanks to flexible numerology, for instance. The uncorrelated spatial assumption between Bob and Eve holds as soon as Bob and Eve are spaced by more than a few wavelengths, depending on the environment. The same holds in what concern the uncorrelated spatial assumption between Eve's antennas. The uncorrelated channel errors assumption holds if the subcarriers are not correlated. It is finally assumed that the noise is white in the frequency domain.

The communication parameters used to study the SISO system are given in Table 5.1:

Symbol	Description	Value
α	Ratio between the useful and the total signal power.	$\alpha \in [0,1]$
σ	CSI estimation error variance.	$\sigma \in [0,1]$
σ_{dB}	CSI estimation error variance in dB.	$\sigma_{\text{dB}} \in \mathbb{R}^-$
ϵ	Fraction of outage.	$\epsilon \in [0,1]$
Δ	Targeted ergodic secrecy rate in bit/channel use.	$\Delta \in \mathbb{R}^+$
Q	# of OFDM subcarriers.	$Q = 256$
U	Spreading factor.	$U = 2^n$, $n \in \{2,4,8,16,32\}$
N	# of symbols per OFDM block.	$N = Q/U$
N_A	# of antenna at Alice.	$N_A = 1$
N_B	# of antenna at Bob.	$N_B = 1$
N_E	# of antenna(s) at Eve.	$N_E \geq 1$

Table 5.1: SISO communication parameters

5.3 Single-Input Single-Output Single-Eavesdropper

5.3.1 Preliminaries

The expressions of the received signals at Bob and Eve's positions, the decoding structures implemented at Eve, as well as the AN generation condition, were given in chapter 4 and are also given in this section to facilitate the reader's understanding.

Received signal expressions
From Chapter 4, in a SISO-SE situation, the received signal at Bob is given by (see equation (4.11)):

$$\mathbf{y}_{\text{B}}^{\text{SISOSE}} = \sqrt{\alpha(1-\sigma)}\mathbf{S}^H ||\mathbf{H_B}||^2 \mathbf{Sx} + \sqrt{\alpha\sigma}\mathbf{S}^H \mathbf{H_B} \Delta \mathbf{H_B}^H \mathbf{Sx} + \sqrt{1-\alpha}\mathbf{S}^H \mathbf{H_B w} + \mathbf{S}^H \mathbf{v}_{\text{B}}, \tag{5.1}$$

where $\mathbf{S}$ (respectively ($\mathbf{S}^H$) is the spreading (respectively) the despreading matrix, $\mathbf{H_B}$ is Bob's channel, $\mathbf{\Delta H_B}$ is Bob's error matrix, $\mathbf{x}$ is the data vector, $\mathbf{w}$ is the AN vector, and $\mathbf{v}_{\text{B}}$ is the noise vector at Bob. At Eve, replacing $N_E = 1$ in equation (4.14) to obtain the correspond the single-eavesdropper scenario, the received signal is expressed as:

$$\mathbf{y}_{\text{E}}^{\text{SISOSE,D}} = \sqrt{\alpha}\mathbf{S}^H \mathbf{D_E} \mathbf{H_E} \widehat{\mathbf{H}}_{\mathbf{B}}^* \mathbf{Sx} + \sqrt{1-\alpha}\mathbf{S}^H \mathbf{D_E} \mathbf{H_E w} + \mathbf{S}^H \mathbf{D_E} \mathbf{v}_{\text{E}}, \tag{5.2}$$

where $\mathbf{D_E}$ is a $Q \times Q$ decoding matrix performed at Eve whose nature depends on the handshake protocol between the transmitter and the legitimate receiver, $\widehat{\mathbf{H}}_{\mathbf{B}} = \sqrt{\sigma}\mathbf{H_B} + \sqrt{1-\sigma}\mathbf{\Delta H_B}$ is Bob's channel estimated by Alice, $\mathbf{H_E}$ is Eve's channel, and $\mathbf{v}_{\text{E}}$ is the noise vector at Eve.

Decoding structures at Eve
To obtain the expressions of the decoding structures at Eve when a SISO-SE configuration is considered, one has to set the number of Eve's antenna to $N_E = 1$ in the decoder's expressions given in Sections 4.6.3 and 4.6.4.

TDD handshake procedure 1: same decoding structure (SDS) decoder.
Eve is only able to know $\mathbf{H_{BE}}$ which is of no help. She implements the same decoding structure as Bob:

$$\mathbf{D}_{\mathbf{E}}^{\text{SDS}} = \mathbf{S}^H. \tag{5.3}$$

TDD handshake procedure 2: own channel (OC) decoder.
Eve implements a decoding structure that takes benefit from her own channel knowledge:

$$\mathbf{D}_{\mathbf{E}}^{\text{OC}} = \mathbf{S}^H \mathbf{H}_{\mathbf{E}}^H. \tag{5.4}$$

TDD handshake procedure 3: matched filter (MF) decoder.
Eve can access to the knowledge of her equivalent channel. She implements a MF decoding structure, which is equivalent to the MRC decoder in the case of single-antenna receiver:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MF}} = \mathbf{S}^H \widehat{\mathbf{H}}_{\mathbf{B}} \mathbf{H}_{\mathbf{E}}^H. \tag{5.5}$$

FDD handshake procedure, block-fading channel: AN killer decoder.
Eve has the knowledge of $\widehat{\mathbf{H}}_{\mathbf{B}}$, $\mathbf{H}_{\mathbf{E}}$, and $\widehat{\mathbf{H}}_{\mathbf{B}}^H \mathbf{H}_{\mathbf{E}}$. She implements a decoder that aligns the AN in her null space:

$$\mathbf{D}_{\mathbf{E}}^{\text{AN killer}} = \widehat{\mathbf{H}}_{\mathbf{B}} \mathbf{H}_{\mathbf{E}}^{-1}. \tag{5.6}$$

FDD handshake procedure, slow-fading channel: LMMSE decoder.
Eve has the knowledge of $\widehat{\mathbf{H}}_{\mathbf{B}}$, $\mathbf{H}_{\mathbf{E}}$, $\widehat{\mathbf{H}}_{\mathbf{B}}^H \mathbf{H}_{\mathbf{E}}$, and the AN variance σ_{AN}^2. She implements a LMMSE decoder (see Appendix B.1 for the derivation):

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}} = \sqrt{\alpha} \Gamma_{\mathrm{E}}^H \left(\alpha \Gamma_{\mathrm{E}} \Gamma_{\mathrm{E}}^H + (1-\alpha) ||\mathbf{H}_{\mathbf{E}}||^2 \sigma_{\mathrm{AN}}^2 \mathbf{I}_Q + \sigma_{\mathrm{E}}^2 \mathbf{I}_Q \right)^{-1}, \tag{5.7}$$

where $\Gamma_{\mathrm{E}} = \widehat{\mathbf{H}}_{\mathbf{B}}^H \mathbf{H}_{\mathbf{E}} \mathbf{S}$.

AN generation
In a SISO-SE configuration, the AN is generated such that:

$$\mathbf{S}^H \widehat{\mathbf{H}}_{\mathbf{B}} \mathbf{w} = \mathbf{0}_N. \tag{5.8}$$

5.3.2 Ergodic secrecy rate modeling

To evaluate the degree of secrecy in a PLS communication, the ergodic secrecy capacity (ESC) is often considered, defined as the expectation of the secrecy capacity (SC). As explained in chapter 2, the SC is the maximum achievable transmission rate that can be supported by the main channel, i.e., reliability at Bob, while ensuring the impossibility for the eavesdropper to retrieve the data, i.e., secrecy against Eve, [151]. The ESC is given by:

$$C_S = \mathbb{E}\left[\left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E) \right]^+ \right], \tag{5.9}$$

where $[x]^+ = \max(x, 0)$, γ_B and γ_E being respectively the instantaneous SINRs at Bob and Eve's positions. In this work, the ESR is used as a metric. It was shown in [152], Lemma 1, that an achievable ESR, i.e., a positive rate smaller than or equal to the ESC, is given by:

$$R_S = \left[\mathbb{E}\left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E) \right] \right]^+ \tag{5.10a}$$

$$\Leftrightarrow R_S \approx \left[\log_2(1+\mathbb{E}[\gamma_B]) - \log_2(1+\mathbb{E}[\gamma_E]) \right]^+. \tag{5.10b}$$

Expression (5.10b) is the ESR for the whole OFDM block. Keeping into account the spreading effect, the ESR per transmitted symbol x_n is derived by defining $\gamma_{B,n}$ (resp. $\gamma_{E,n}$) as Bob (resp. Eve) instantaneous SINR for a particular transmitted symbol n:

$$R_{S,n} \approx \frac{1}{U} \left[\log_2(1+\mathbb{E}[\gamma_{B,n}]) - \log_2(1+\mathbb{E}[\gamma_{E,n}]) \right]^+, \tag{5.11}$$

where $\frac{1}{U}$ represents the rate decrease due to the spreading. As a reminder, to implement a TR precoder in the FD, N data symbols are first spread by a factor U and then sent over one OFDM block of $Q = NU$ subcarriers. Each data symbol is transmitted via U different subcarriers. At the receiver, the symbol components are despread, i.e., the U components of each symbol are summed together. Therefore, only $N = Q/U$ different data symbols are transmitted within one OFDM block, such that it is convenient to take the spreading effect into account via the $\frac{1}{U}$ factor.

Remark 5.1: Rough estimation of effective secrecy rate

The secrecy rate is defined in bit per channel use in this manuscript, i.e., in bit per input symbol into the channel. It is interesting to compute the effective secrecy rate in bit per second.

In this work, it is considered that, between two successive channel uses, the channel is uncorrelated in time/frequency. Alice can only use the channel in time/frequency at intervals longer than the channel coherence time/channel coherence bandwidth. Otherwise, Eve could be able to estimate some communication parameters based on large statistics. This very stringent condition strongly decreases the effective secrecy rate.

As an example, in LTE-A, the channel bandwidth can be up to 100MHz.
A typical delay spread in suburban area is about $T_m = 0.5\mu$s, which corresponds to a coherence bandwidth of:

$$(\Delta f)_c \approx \frac{1}{2\pi T_m} \approx 320\,\text{kHz}.$$

Therefore, approximatively $\frac{100\,.\,10^6}{320\,.\,10^3} \approx 300$ channel uses can be supported at a time.
If the channel coherence time is 100ms, Alice can access the channel 10 times per second.

Consequently, a secrecy rate of 1 bit per channel use corresponds to an effective secrecy rate of roughly:

$$R_s \approx 1 \times 300 \times 10 = 3\,\text{kbit/s}.$$

This example shows that the investigated scheme is suited for ultra low data rate ultra secure communications.

From equation (5.11), one can state that analytic expressions of Bob and Eve's ergodic signal-to-interference-plus-noise ratios (ESINRs) must be derived in order to obtain a closed-form approximation of the communication ESR, which is the aim of next sections 5.3.2.1 and 5.3.2.2 for TDD handshake procedures.

Remark 5.2: ESINR definition

In this manuscript, the ESINR at Bob/Eve, for a particular investigated scenario, is defined as the expected value of the ratio between the energy of the data component of the received signal at Bob/Eve, and the energy of the noise plus the interference components of the received signal at Bob/Eve.

5.3.2.1 Bob's ergodic SINR

At Bob, a despreading operation is performed. From (5.1), the ESINR is given by:

$$\mathbb{E}\left[\gamma_B^{\text{SISOSE}}\right] = \mathbb{E}\left[\frac{\left|B_1^{\text{SISOSE}}\right|^2}{\left|B_2^{\text{SISOSE}} + B_3^{\text{SISOSE}}\right|^2}\right], \tag{5.12}$$

with:

$$\begin{aligned} B_1^{\text{SISOSE}} &= \sqrt{\alpha(1-\sigma)}\mathbf{S}^H ||\mathbf{H_B}||^2 \mathbf{Sx} + \sqrt{\alpha\sigma}\mathbf{S}^H \mathbf{H_B} \Delta \mathbf{H_B}^H \mathbf{Sx}, \\ B_2^{\text{SISOSE}} &= \mathbf{S}^H \mathbf{v}_{\text{B}}, \\ B_3^{\text{SISOSE}} &= \sqrt{1-\alpha}\mathbf{S}^H \mathbf{H_B w}, \end{aligned} \tag{5.13}$$

being respectively the data, noise, and AN components of the received signal at Bob. From 5.12, an approximation of the ESINR of the n^{th} symbol is:

$$\begin{aligned}\mathbb{E}\left[\gamma_{B,n}^{\text{SISOSE}}\right] &= \mathbb{E}\left[\frac{\left|B_{1,n}^{\text{SISOSE}}\right|^2}{\left|B_{2,n}^{\text{SISOSE}}+B_{3,n}^{\text{SISOSE}}\right|^2}\right] \approx \mathbb{E}\left[\left|B_{1,n}^{\text{SISOSE}}\right|^2\right]\mathbb{E}\left[\frac{1}{\left|B_{2,n}^{\text{SISOSE}}+B_{3,n}^{\text{SISOSE}}\right|^2}\right] \\ &\approx \frac{\mathbb{E}\left[\left|B_{1,n}^{\text{SISOSE}}\right|^2\right]}{\mathbb{E}\left[\left|B_{2,n}^{\text{SISOSE}}+B_{3,n}^{\text{SISOSE}}\right|^2\right]} = \frac{\mathbb{E}\left[\left|B_{1,n}^{\text{SISOSE}}\right|^2\right]}{\mathbb{E}\left[\left|B_{2,n}^{\text{SISOSE}}\right|^2\right]+\mathbb{E}\left[\left|B_{3,n}^{\text{SISOSE}}\right|^2\right]},\end{aligned} \tag{5.14}$$

where $B_{1,n}^{\text{SISOSE}}$, $B_{2,n}^{\text{SISOSE}}$, and $B_{3,n}^{\text{SISOSE}}$ are respectively the data, noise, and AN (i.e., interference) n^{th} symbol components of the received signal at Bob's position, when a SISO-SE system is considered. It is assumed that the data, noise, and AN symbol components are mutually independent.

Notation 5.1

To lighten the notations, the superscripts *SISOSE* and *SISOME* are omitted in the following of this chapter. For clarity, the system configuration (SISO-SE or SISO-ME) will always be stated so that there is no ambiguity for the reader. If needed, the superscripts will be denoted.

From (5.13), the received components at Bob are:

$$B_{1,n} = \frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{i=0}^{U-1}|h_{\text{B},i}|^2 + \frac{\sqrt{\alpha\sigma}}{U}\sum_{i=0}^{U-1}h_{\text{B},i}\Delta h_{\text{B},i}^* \tag{5.15a}$$

$$B_{2,n} = \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1}v_{\text{B},i} \tag{5.15b}$$

$$B_{3,n} = \sqrt{\frac{1-\alpha}{U}}\sum_{i=0}^{U-1}h_{\text{B},i}w_i. \tag{5.15c}$$

As detailed in Appendices B.2.1, B.2.2, and B.2.3, the components can respectively be derived as:

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U} \tag{5.16a}$$

$$\mathbb{E}\left[|B_{2,n}|^2\right] = \sigma_{\text{B}}^2 \tag{5.16b}$$

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)\sigma}{U}, \tag{5.16c}$$

where Bob's noise variance is defined as:

$$\sigma_{\text{B}}^2 = \frac{1}{U\delta_B}, \tag{5.17}$$

where δ_B is the SNR at Bob in linear scale, and $1/U$ is the received energy per symbol component.

Remark 5.3: SNR definition

In this manuscript, the SNR at Bob/Eve is defined as the ratio between the energy of the received symbol component at Bob/Eve, i.e., data component plus AN component (equal to $1/U$), and the energy of the noise component at Bob (respectively, Eve), which equals to σ_{B}^2 (respectively, σ_{E}^2).

Introducing (5.16a), (5.16b), and (5.16c) into (5.14), the per-symbol approximated ESINR at Bob in a SISO-SE system configuration is given by:

$$\mathbb{E}[\gamma_{B,n}] \approx \frac{\alpha[(U+1)(1-\sigma)+\sigma]}{U\sigma_{\mathrm{B}}^2+(1-\alpha)\sigma}. \tag{5.18}$$

The approximated ergodic capacity (EC) at Bob is therefore expressed as:

$$C_B \approx \log_2(1+\mathbb{E}[\gamma_{B,n}]) = \log_2\left(1+\frac{\alpha[(U+1)(1-\sigma)+\sigma]}{U\sigma_{\mathrm{B}}^2+(1-\alpha)\sigma}\right) \tag{5.19}$$

Figure 5.1 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_B$) with the approximated EC at Bob (C_B) given in (5.19), for different spreading factor values and CSI estimation errors made at Alice, and at SNR $\delta_B = 10$dB. The exact EC is found by Monte Carlo simulations (100.000 realizations of the instantaneous capacity), and is given by:

$$\widehat{C}_B = \mathbb{E}[\log_2(1+\gamma_{B,n})] \tag{5.20}$$

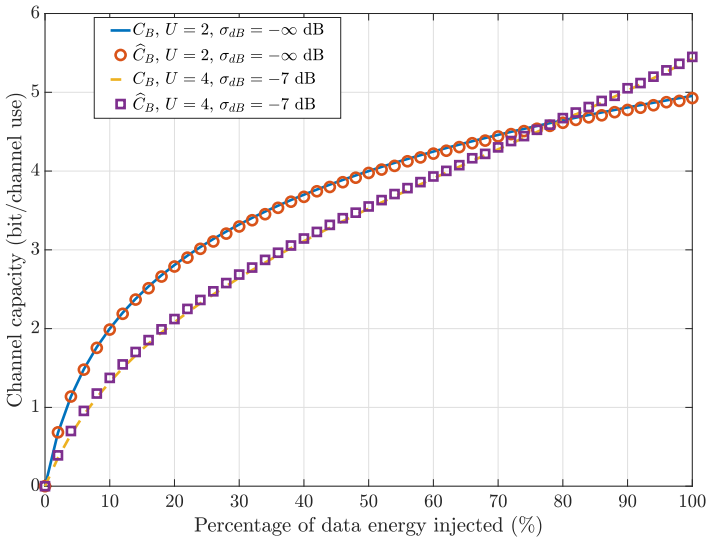

Figure 5.1: Comparison between approximated EC and exact EC at Bob, $\delta_B = 10$dB, 100.000 realizations

From Figure 5.1, it can be observed that the approximated EC (5.19) is very close to the exact EC (5.20). It is therefore used as a closed-form expression for the rest of this study.

5.3.2.2 Eve's ergodic SINR

The derivation of the ESINR at the eavesdropper is conducted in this section for the three investigated decoding structures, coming from the TDD handshakes. Depending on the decoder, the ESINR is given by:

$$\mathbb{E}\left[\gamma_E^{\mathrm{D}}\right] = \mathbb{E}\left[\frac{\left|E_1^{\mathrm{D}}\right|^2}{\left|E_2^{\mathrm{D}}+E_3^{\mathrm{D}}\right|^2}\right], \tag{5.21}$$

with E_1^{D}, E_2^{D}, and E_3^{D} respectively being the data, noise, and AN components of the received signal at Eve. From 5.21, an approximation of the ESINR of the n^{th} symbol is:

$$\begin{aligned}\mathbb{E}\left[\gamma_{E,n}^{\mathrm{D}}\right] &= \mathbb{E}\left[\frac{\left|E_{1,n}^{\mathrm{D}}\right|^2}{\left|E_{2,n}^{\mathrm{D}}+E_{3,n}^{\mathrm{D}}\right|^2}\right] \approx \mathbb{E}\left[\left|E_{1,n}^{\mathrm{D}}\right|^2\right]\mathbb{E}\left[\frac{1}{\left|E_{2,n}^{\mathrm{D}}+E_{3,n}^{\mathrm{D}}\right|^2}\right] \\ &\approx \frac{\mathbb{E}\left[\left|E_{1,n}^{\mathrm{D}}\right|^2\right]}{\mathbb{E}\left[\left|E_{2,n}^{\mathrm{D}}+E_{3,n}^{\mathrm{D}}\right|^2\right]} = \frac{\mathbb{E}\left[\left|E_{1,n}^{\mathrm{D}}\right|^2\right]}{\mathbb{E}\left[\left|E_{2,n}^{\mathrm{D}}\right|^2\right]+\mathbb{E}\left[\left|E_{3,n}^{\mathrm{D}}\right|^2\right]},\end{aligned} \tag{5.22}$$

where $E_{1,n}^{\mathrm{D}}$, $E_{2,n}^{\mathrm{D}}$, and $E_{3,n}^{\mathrm{D}}$ are respectively the data, noise, and AN (i.e., interference) n^{th} symbol components of the received signal at Eve's position, depending on the investigated scenario, when a SISO-SE system is considered. It is assumed that the data, noise, and AN symbol components are mutually independent.

TDD handshake procedure 1: same decoding structure decoder

When Eve implements the SDS decoder, by replacing (5.3) in (5.2), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{SDS}} = \sqrt{\alpha}\mathbf{S}^H\mathbf{H_E}\widehat{\mathbf{H}}_{\mathbf{B}}^H\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\mathbf{H_E}\mathbf{w} + \mathbf{S}^H\mathbf{v}_{\mathrm{E}}. \tag{5.23}$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\mathrm{SDS}} = \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1} h_{\mathrm{E},i}\hat{h}_{\mathrm{B},i}^* \tag{5.24a}$$

$$E_{2,n}^{\mathrm{SDS}} = \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} v_{\mathrm{E},i} \tag{5.24b}$$

$$E_{3,n}^{\mathrm{SDS}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},i}w_i. \tag{5.24c}$$

As detailed in B.3.1.1, B.3.1.2, and B.3.1.3, the expected energy of the components are respectively given by:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{SDS}}|^2\right] = \frac{\alpha}{U} \tag{5.25a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{SDS}}|^2\right] = \sigma_{\mathrm{E}}^2 \tag{5.25b}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{SDS}}|^2\right] = \frac{1-\alpha}{U}. \tag{5.25c}$$

Eve's noise variance is defined as:

$$\sigma_{\mathrm{E}}^2 = \frac{1}{U\delta_E}, \tag{5.26}$$

where δ_E is the SNR at Eve in linear scale, and $1/U$ is the received energy per symbol component.
Since it is assumed that Eve perfectly estimates the amount of CSI she can obtain from the handshake procedure, she is not impacted by the precoding error made by Alice, i.e., there is no dependency in σ in (5.25a), (5.25b), and (5.25c).
Introducing (5.25a), (5.25b), and (5.25c) into (5.22), the per-symbol approximated ESINR when Eve implements a SDS decoder, in a SISO-SE system configuration, is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{SDS}}\right] \approx \frac{\alpha}{U\sigma_{\mathrm{E}}^2+(1-\alpha)}. \tag{5.27}$$

The approximated EC at Eve when a SDS decoder is implemented is therefore expressed as:

$$C_E^{\mathrm{SDS}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{SDS}}\right]\right) = \log_2\left(1+\frac{\alpha}{U\sigma_{\mathrm{E}}^2+(1-\alpha)}\right) \tag{5.28}$$

Figure 5.2 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_E^{\mathrm{SDS}}$) obtained by simulation, with the approximated EC at Eve (C_E^{SDS}) given in (5.28), for different spreading factor values and CSI estimation errors made at Alice, and at SNR $\delta_E = 10$dB. The exact EC is obtained by Monte Carlo simulations (100.000 realizations) as:

$$\widehat{C}_E^{\mathrm{SDS}} = \mathbb{E}\left[\log_2\left(1+\gamma_{E,n}^{\mathrm{SDS}}\right)\right] \tag{5.29}$$

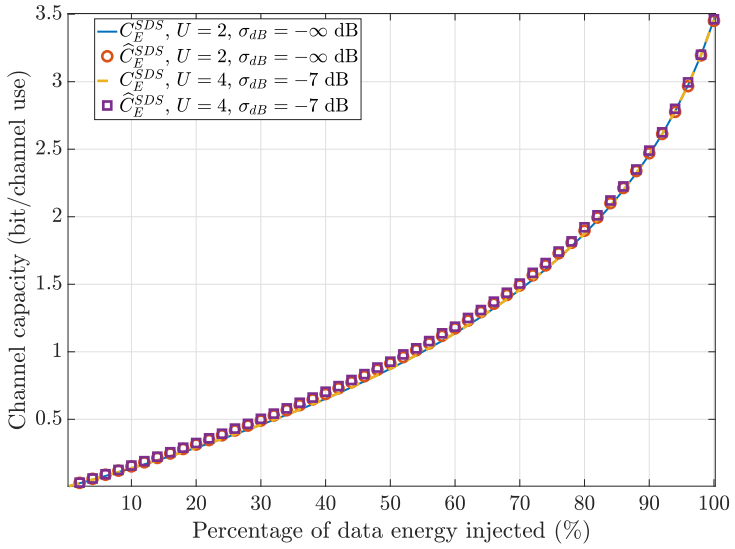

Figure 5.2: Comparison between approximated EC and exact EC at Eve, SDS decoder, $\delta_E = 10$dB, 100.000 realizations

From Figure 5.2, it can be observed that the approximated EC (5.28) is very close to the exact EC (5.29). It is therefore used as a closed-form expression for the rest of this study. As anticipated, the EC is not impacted by the main channel misestimate made by Alice. In addition, one can observe the little impact the BOR has on the value of the capacity. This can be understood from (5.28) where the BOR only influences the AWGN variance, which is generally a small quantity.

TDD handshake procedure 2: own channel decoder

When Eve implements the OC decoder, by replacing (5.4) in (5.2), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{OC}} = \sqrt{\alpha}\mathbf{S}^H ||\mathbf{H_E}||^2 \widehat{\mathbf{H}}_{\mathbf{B}}^H \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H ||\mathbf{H_E}||^2 \mathbf{w} + \mathbf{S}^H \mathbf{H}_{\mathbf{E}}^H \mathbf{v}_{\mathrm{E}}. \tag{5.30}$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\mathrm{OC}} = \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1} |h_{\mathrm{E},i}|^2 \hat{h}_{\mathrm{B},i}^* \tag{5.31a}$$

$$E_{2,n}^{\mathrm{OC}} = \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},i}^* v_{\mathrm{E},i} \tag{5.31b}$$

$$E_{3,n}^{\mathrm{OC}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1} |h_{\mathrm{E},i}|^2 w_i. \tag{5.31c}$$

As detailed in B.3.2.1, B.3.2.2, and B.3.2.3, the expected energy of the components can respectively be expressed as:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{OC}}|^2\right] = \frac{2\alpha}{U} \tag{5.32a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{OC}}|^2\right] = \sigma_{\mathrm{E}}^2 \tag{5.32b}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{OC}}|^2\right] = \frac{2(1-\alpha)}{U}. \tag{5.32c}$$

As for the SDS decoder, Eve is not impacted by the CSI estimation error made by Alice.
Introducing (5.32a), (5.32b), and (5.32c) into (5.22), the per-symbol approximated ESINR when Eve implements an OC decoder, in a SISO-SE system configuration, is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right] \approx \frac{\alpha}{\frac{U\sigma_{\mathrm{E}}^2}{2}+(1-\alpha)}. \tag{5.33}$$

The approximated EC at Eve when a SDS decoder is implemented is therefore expressed as:

$$C_E^{\mathrm{OC}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right]\right) = \log_2\left(1+\frac{\alpha}{\frac{U\sigma_{\mathrm{E}}^2}{2}+(1-\alpha)}\right) \tag{5.34}$$

Figure 5.3 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_E^{\mathrm{OC}}$) obtained by simulation, with the approximated EC at Eve (C_E^{OC}) given in (5.34), for different spreading factor values and CSI estimation errors made at Alice, and at SNR $\delta_E = 10$dB.

From Figure 5.3, it can be observed that the approximated EC (5.34) is very close to the exact EC obtained by Monte Carlo simulations (100.000 realizations). It is therefore used as a closed-form expression for the rest of this study. Similarly to the SDS scenario, the EC is not impacted by the main channel misestimate made by Alice, and the BOR value does not influence much the capacity. In addition, one can observe that (5.34) is very similar to (5.28). In particular, (5.34) leads to slightly higher SINR values at Eve than (5.28), especially at high σ_{E}^2 and when $\alpha \to 1$, i.e., when Eve is equipped with a low-noise hardware, and when the majority of the energy sent is dedicated for data transmission. Relatively low performances at Eve are expected with these decoding structures since these decoders do not allow to coherently sum up the received symbol components when despreading. No frequency diversity gain is consequently achieved, leading to sub-optimal decoding performances.

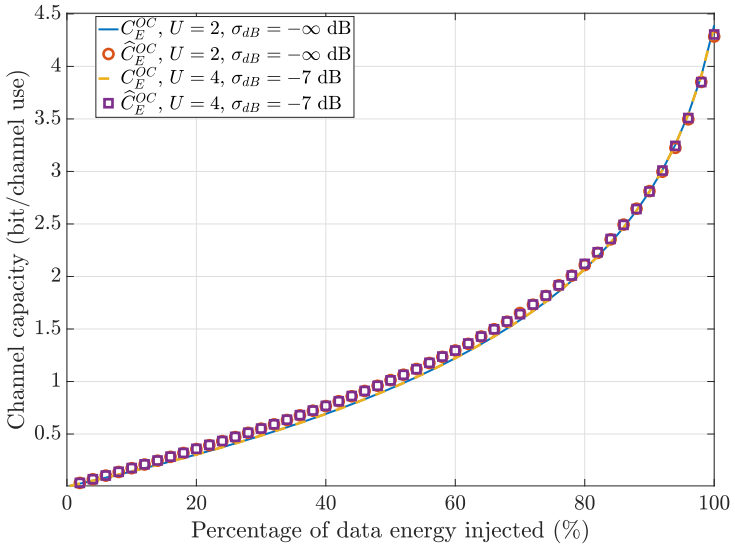

Figure 5.3: Comparison between approximated EC and exact EC at Eve, OC decoder, $\delta_E = 10$dB, 100.000 realizations

TDD handshake procedure 3: matched filter decoder

When Eve implements the MF decoder, by replacing (5.5) in (5.2), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{MF}} = \sqrt{\alpha}\mathbf{S}^H ||\mathbf{H_E}||^2 \left|\left|\widehat{\mathbf{H}}_{\mathbf{B}}\right|\right|^2 \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\widehat{\mathbf{H}}_{\mathbf{B}} ||\mathbf{H_E}||^2 \mathbf{w} + \mathbf{S}^H\mathbf{H_E}\widehat{\mathbf{H}}_{\mathbf{B}}\mathbf{v}_{\mathrm{E}}. \tag{5.35}$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\text{MF}} = \frac{\sqrt{\alpha}}{U} \sum_{i=0}^{U-1} |h_{\text{E},i}|^2 \left|\hat{h}_{\text{B},i}\right|^2 \tag{5.36a}$$

$$E_{2,n}^{\text{MF}} = \frac{1}{\sqrt{U}} \sum_{i=0}^{U-1} h_{\text{E},i}^* \hat{h}_{\text{B},i} v_{\text{E},i} \tag{5.36b}$$

$$E_{3,n}^{\text{MF}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}} \sum_{i=0}^{U-1} \hat{h}_{\text{B},i} |h_{\text{E},i}|^2 w_i. \tag{5.36c}$$

As detailed in B.3.3.1, B.3.3.2, and B.3.3.3, the expected energy of the components can respectively be expressed as:

$$\mathbb{E}\left[|E_{1,n}^{\text{MF}}|^2\right] = \frac{\alpha(U+3)}{U} \tag{5.37a}$$

$$\mathbb{E}\left[|E_{2,n}^{\text{MF}}|^2\right] = \sigma_{\text{E}}^2 \tag{5.37b}$$

$$\mathbb{E}\left[|E_{3,n}^{\text{MF}}|^2\right] = \frac{1-\alpha}{U+1}. \tag{5.37c}$$

As for the the other decoding structures, Eve is not impacted by the CSI estimation error made by Alice.
Introducing (5.37a), (5.37b), and (5.37c) into (5.22), the per-symbol approximated ESINR when Eve implements a MF decoder, in a SISO-SE system configuration, is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\text{MF}}\right] \approx \frac{\alpha \frac{U+3}{U}}{\sigma_{\text{E}}^2 + \frac{1-\alpha}{U+1}}. \tag{5.38}$$

It can be outlined that the numerator in (5.38) is about U times larger than in (5.27) and (5.33). This is due to the fact that, when Eve implements an MF decoder, she benefits from a frequency diversity gain U. The approximated EC at Eve when an MF decoder is implemented is therefore expressed as:

$$C_E^{\text{MF}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\text{MF}}\right]\right) = \log_2\left(1+\frac{\alpha \frac{U+3}{U}}{\sigma_{\text{E}}^2 + \frac{1-\alpha}{U+1}}\right) \tag{5.39}$$

Figure 5.4 shows the accuracy of the approximation on the EC, by comparing the exact obtained by Monte Carlo simulations (100.000 realizations), with the approximated EC at Eve (C_E^{MF}) given in (5.39), for different spreading factor values and CSI estimation errors made at Alice, and at SNR $\delta_E = 10\text{dB}$.

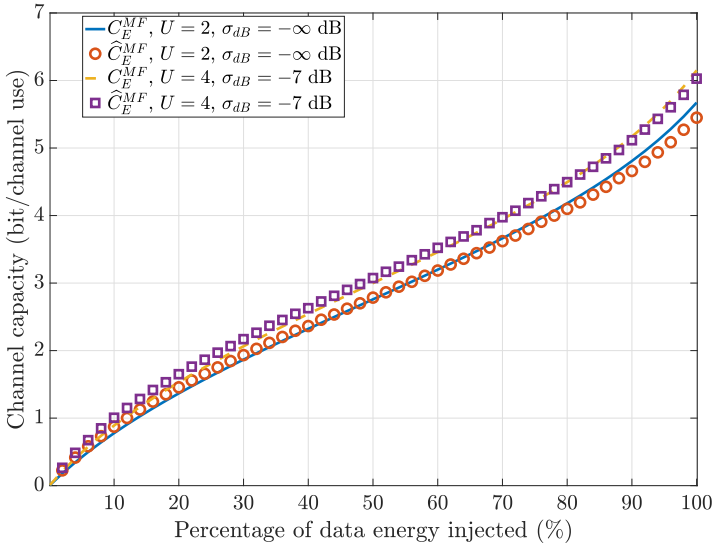

Figure 5.4: Comparison between approximated EC and exact EC at Eve, MF decoder, $\delta_E = 10\text{dB}$, 100.000 realizations

As anticipated, it can be observed from Figure 5.4 that the implementation of an MF decoder at Eve increases the EC compared to when she uses the SDS or the OC decoders. From that, higher decoding performances are expected at Eve, i.e., lower secrecy performances, when she decodes the data with a MF decoder.

5.3.3 Guaranteeing secrecy rate

In a practical scenario, Alice needs to a-priori know the per-symbol communication ESR over which she can securely communicate with Bob. In other words, she must determine the achievable ergodic secrecy rate that **guarantees** reliability at Bob and secrecy from Eve. In order to do so, Alice must design the communication parameters, depending on the investigated scenario, i.e., on the handshake procedure she establishes with Bob at the beginning of each coherence time. In this Section, derivations of the required SNR at Bob $\delta_{\mathrm{B}}^{\mathrm{D}}$ (Section 5.3.3.1), the maximal main CSI estimation error $\sigma_{\max}^{\mathrm{D}}$ (Section 5.3.3.2), as well as the optimal amount of data energy to inject $\alpha_{\mathrm{opt}}^{\mathrm{D}}$ (Section 5.3.3.3), are conducted depending on the investigated scenario, to guarantee a targeted ESR $= \Delta$ (in bit/channel use). Three scenarios are considered:

- Scenario 1: Eve implements the SDS decoder.
- Scenario 2: Eve implements the OC decoder.
- Scenario 3: Eve implements the MF decoder.

Since Eve is a passive eavesdropper, Alice cannot access to her SNR. Therefore, the worst-case scenario in terms of security is considered. That is, it is assumed that Eve's SNR $\to \infty$, which is obtained with $\sigma_{\mathrm{E}}^2 \to 0$ in the expressions of Eve's capacity. This may correspond to the case where Eve is close to Alice and/or her hardware is low-noise. From that, Alice is able to a-priori guarantee a targeted per-symbol communication ESR.

5.3.3.1 Required SNR at Bob

As a reminder, the transmitted energy per symbol is 1, i.e., the transmitted energy per symbol component is $1/U$. Since normalized channel realizations are considered, the received energy per symbol component is also $1/U$. From that, Bob's SNR per symbol component is defined as:

$$\delta_{\mathrm{B}}^{\mathrm{D}} = \frac{1}{U\sigma_{\mathrm{B}}^2}. \tag{5.40}$$

It is assumed that Alice aims to guarantee a per-symbol ESR $= \Delta$ bit/channel use.

Scenario 1: SDS decoder
Introducing (5.19) and (5.28) in (5.11), and considering $\sigma_{\mathrm{E}}^2 \to 0$, the guaranteed ESR in this scenario becomes:

$$R_{s,n}^{\mathrm{SDS}} = \Delta = \frac{1}{U}\left[\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U\sigma_{\mathrm{B}}^2+(1-\alpha)\sigma}\right) - \log_2\left(1+\frac{\alpha}{1-\alpha}\right)\right]. \tag{5.41}$$

Figure 5.5 represents the guaranteed ESR as a function of the percentage of injected energy dedicated for information data, i.e., as a function of α, for different BOR values, and for different CSI estimation errors made by Alice, i.e., no CSI error ($\sigma_{\mathrm{dB}} = -\infty$ dB) and 10% of CSI error ($\sigma_{\mathrm{dB}} = -10$dB), when Eve implements the SDS decoder.

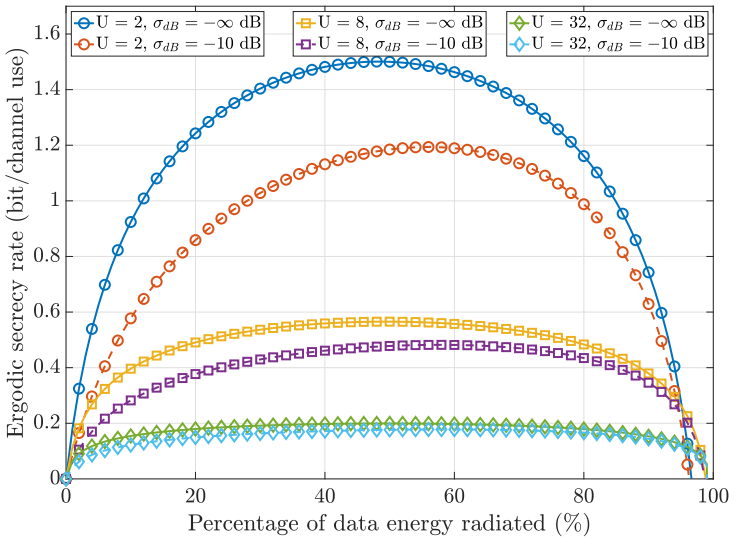

Figure 5.5: Guaranteed ergodic secrecy rate, SDS decoder, $\delta_B = 10$dB

First, one can notice the importance of AN injection on the ESR value. It is observed an ESR enhancement with the addition of AN except for very high ($\alpha \to 0$) or very low ($\alpha \to 1$) percentages of injected AN. Second, it can be seen that the maximal ESR strongly decreases when the BOR increases. For example, for the error-free scenario, the maximal ESR is equal to 1.5 bit/channel use when $U = 2$, i.e., low diversity gain, and decreases to 0.57 bit/channel use when $U = 8$, i.e., moderate diversity gain, and to 0.2 bit/channel use when $U = 32$, i.e., high diversity gain. Indeed, when the BOR increases, the TR focusing gain increases at the expense of the data rate since less symbols are sent per OFDM block. This leads to a per-symbol ESR decrease. Third, for all BOR values, the ESR performance decreases with a CSI misestimate. However, when the diversity gain increases, the PLS scheme is more robust to the imperfect main CSI estimation made at the transmitter side. In fact, with $U = 2$, the ESR decreases by 20.67% (from 1.5 to 1.19 bit/channel use when Alice misestimates Bob's CSI with 10% of error), it decreases by 15.79% with $U = 8$ (from 0.57 to 0.48 bit/channel use), and only by 12.5% with $U = 32$ (from 0.2 to 0.175 bit/channel use).

After manipulating equation (5.41), one obtains the required SNR at Bob to guarantee ESR $= \Delta$, when Eve implements the SDS decoder:

$$\delta_{\mathrm{B}}^{\mathrm{SDS}} = \frac{\alpha + T_1^{\mathrm{SDS}}}{\alpha^2 T_2^{\mathrm{SDS}} + \alpha T_3^{SDS\mathrm{SDS}} + T_4^{\mathrm{SDS}}}, \tag{5.42}$$

where:

$$\begin{aligned} T_1^{\mathrm{SDS}} &= 2^{\Delta U} - 1 \\ T_2^{\mathrm{SDS}} &= (U+1)(\sigma - 1) \\ T_3^{\mathrm{SDS}} &= (U+1)(1-\sigma) + \sigma(2^{\Delta U} - 1) \\ T_4^{\mathrm{SDS}} &= \sigma\left(1 - 2^{\Delta U}\right). \end{aligned}$$

Scenario 2: OC decoder

Introducing (5.19) and (5.34) in (5.11), and considering $\sigma_{\mathrm{E}}^2 \to 0$, the guaranteed ESR in this scenario becomes:

$$R_{s,n}^{\mathrm{OC}} = \Delta = \frac{1}{U}\left[\log_2\left(1 + \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U\sigma_{\mathrm{B}}^2 + (1-\alpha)\sigma}\right) - \log_2\left(1 + \frac{\alpha}{1-\alpha}\right)\right] = R_{s,n}^{\mathrm{SDS}}. \tag{5.43}$$

It can be seen that the guaranteed ESR when Eve implements the OC decoder is identical to the one when she implements the SDS. This can be understood from the capacity expressions (5.28) and (5.34) which are identical when Eve is assumed to have infinite SNR. From that, the results derived for the SDS decoder also hold for the OC decoder for the rest of Section 5.3.3. The required SNR at Bob to guarantee ESR=Δ is thus:

$$\delta_{\mathrm{B}}^{\mathrm{OC}} = \delta_{\mathrm{B}}^{\mathrm{SDS}}. \tag{5.44}$$

Scenario 3: MF decoder

Introducing (5.19) and (5.39) in (5.11), and considering $\sigma_{\mathrm{E}}^2 \to 0$, the guaranteed ESR when Eve implements the MF decoder is:

$$R_{s,n}^{\mathrm{MF}} = \frac{1}{U}\left[\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right|}{U\sigma_{\mathrm{B}}^2+(1-\alpha)\sigma}\right)-\log_2\left(1+\frac{\alpha\frac{U+3}{U}}{\frac{1-\alpha}{U+1}}\right)\right]. \tag{5.45}$$

Figure 5.6 represents the guaranteed ESR as a function of the percentage injected energy dedicated for information data, when Eve implements the MF. The figure is obtained with the same configurations as in the SDS scenario.

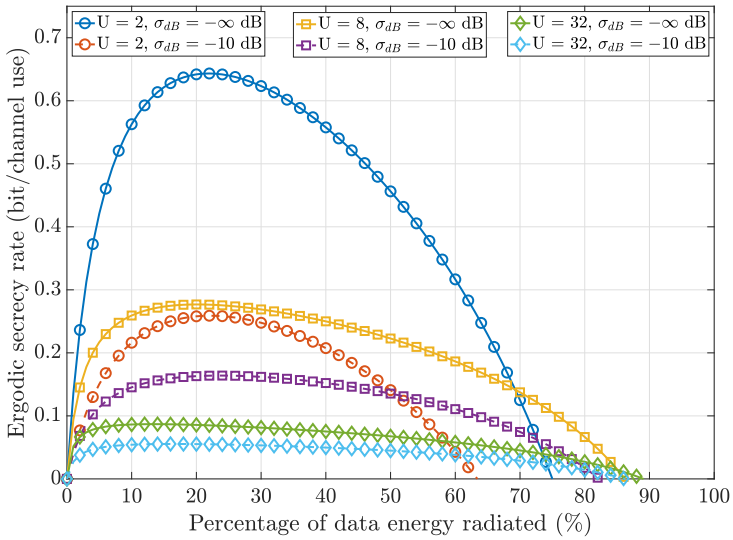

Figure 5.6: Guaranteed ergodic secrecy rate, MF decoder, $\delta_B = 10$dB

The same observations can be made regarding the ESR increase with AN injection, the ESR decrease due to an increase of the diversity gain, and the robustness of the scheme due to imperfect main CSI estimation. However, it is observed that the scheme requires more AN injection, i.e., smaller α, in order to provide a maximal security compared to the SDS scenario. As an example, when $U = 2$ and Alice estimates Bob's CSI with 10% of error, the maximal ESR is attained when $\approx 78\%$ of AN is injected for the MF situation. For the same configuration, Alice must inject $\approx 44\%$ of AN to maximize the ESR if Eve implements the SDS decoder. Furthermore, more AN needs to be injected in order to maximize the ESR performance, when the BOR increases. As seen in Figure 5.6, for the noise-free scenario, the ESR is maximized for 78%, 82%, and 90% of injected AN, when $U = 2, 8$, and 32, respectively. In addition, as expected, the MF scenario exhibits lower secrecy performances than the SDS scenario. It is due to the fact that, in this situation, Eve benefits from a frequency diversity gain due to the MF implementation. This can be seen in (5.35) where each transmitted data symbol is affected by a frequency diversity gain at Eve. Eve's SINR is consequently about U times larger compared to the SDS and OC decoders. As a consequence, Eve has higher decoding performances and the secrecy is therefore degraded.

After manipulating equation (5.45), one obtains the required SNR at Bob to guarantee ESR $= \Delta$, when Eve implements the MF decoder:

$$\delta_{\mathrm{B}}^{\mathrm{MF}} = \frac{\alpha T_0^{\mathrm{MF}} + T_1^{\mathrm{MF}}}{\alpha^2 T_2^{\mathrm{MF}} + \alpha T_3^{\mathrm{MF}} + T_4^{\mathrm{MF}}}, \tag{5.46}$$

where:

$$\begin{aligned}
T_0^{\mathrm{MF}} &= U + 2^{\Delta U} A \\
T_1^{\mathrm{MF}} &= U\left(2^{\Delta U} - 1\right) \\
T_2^{\mathrm{MF}} &= 2^{\Delta U} A\sigma - U(U+1)(1-\sigma) \\
T_3^{\mathrm{MF}} &= 2^{\Delta U} U\sigma - 2^{\Delta U}\sigma A + U(U+1)(1-\sigma) - \sigma U \\
T_4^{\mathrm{MF}} &= \sigma U\left(1 - 2^{\Delta U}\right),
\end{aligned}$$

with $A = U^3 + 3U + 3$.

5.3.3.2 Maximal CSI error allowed

Expressions (5.42), (5.44), and (5.46) give the required SNR at Bob (in linear scale) to guarantee a per-symbol communication ESR $= \Delta$, when Eve respectively implements the SDS decoder, the OC decoder, and the MF decoder, as a function of the communication parameters in a SISO-SE configuration. For a solution to exist, expressions (5.42), (5.44), and (5.46) must be positive, which in turns imposes a maximal CSI error $\sigma_{\max}^{\mathrm{D}}$ that can be made by Alice to possibly reach the targeted ESR. Determining the maximal CSI error allows to find the domain of validity of the SNR expressions, i.e., it allows to find an upper bound on Alice's CSI accuracy to be able to guarantee ESR=Δ bit/channel use. In other words, when $\sigma < \sigma_{\max}^{\mathrm{D}}$, Alice can determine a finite SNR at Bob that enables a guaranteed communication ESR $= \Delta$. When $\sigma = \sigma_{\max}^{\mathrm{D}}$, Bob's SNR has to be infinite to allow Alice to target ESR=Δ. When $\sigma > \sigma_{\max}^{\mathrm{D}}$, Alice is unable to ensure a secure rate Δ.

Scenario 1: SDS decoder

The numerator of (5.46) is always positive, such that one has to focus on the denominator to find the domain of validity of (5.46). In particular, to obtain possible roots in α, one has to determine the maximal allowed CSI error that cannot be exceeded by Alice, denoted by $\sigma_{\max}^{\mathrm{SDS}}$. After some manipulations, it can be found that:

$$\sigma_{\max}^{\mathrm{SDS}} = 1 - \frac{2^{\Delta U} - 1}{(U+1) + \left(2^{\Delta U} - 1\right)}. \tag{5.47}$$

From (5.47), in order to guarantee a targeted per-symbol ESR $\Delta \to \infty$, Alice must perfectly estimate Bob's CSI. Indeed, in this situation, the maximal estimation error she is allowed to is: $\sigma_{\max}^{\mathrm{SDS}} \to 0$. In addition, when $\Delta \to 0^+$, $\sigma_{\max}^{\mathrm{SDS}} \to 1$, i.e., it is always possible to ensure a positive ESR when Eve implements the SDS decoder, whatever the CSI misestimate performed at Alice. Figure 5.7 represents equation (5.47) as a function of the maximal ESR= Δ that can be theoretically guaranteed. That is, if Alice aims to target a communication ESR= Δ, with an error variance $\sigma = \sigma_{\max}^{\mathrm{SDS}}$ in (5.47), Bob's SNR has to be infinite. From that, it can be observed that lower CSI errors are allowed to target a particular ESR when the BOR increases. For example, when 0.3 bit/channel use is targeted, Alice can make an error of at most $\sigma \approx -14$ dB when $U = 32$ (corresponding to 4% of CSI error) but is allowed to misestimate Bob's CSI with an error up to ≈ -0.7 dB when $U = 2$ (corresponding to $\approx 85\%$ of CSI error). There are two reasons. First, lower ESR values can be achieved when the BOR increases, as anticipated from Figure 5.5. It leads to lower allowed CSI errors to target the same ESR for higher BORs than for lower ones. Second, when the BOR increases, the TR focusing gain increases at Bob as well. Therefore, a CSI estimation error has a greater impact for higher BOR values, leading to more ESR decrease. As expected, it can be observed that $\sigma_{\mathrm{dB,max}}^{\mathrm{SDS}}\Big|_{\Delta \to 0^+} = 0\mathrm{dB}$.

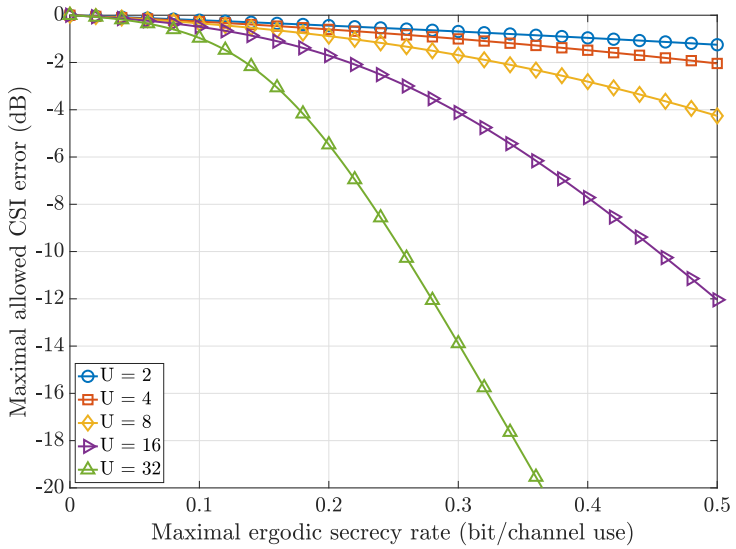

Figure 5.7: Maximal allowed CSI as a function of the maximal ESR that can be guaranteed, SDS decoder

Scenario 2: OC decoder
Since the guaranteed ESR formula for the OC scenario is identical to the SDS scenario, it follows:

$$\sigma_{\max}^{\mathrm{OC}} = \sigma_{\max}^{\mathrm{SDS}}, \tag{5.48}$$

and all remarks made for SDS decoder still hold for OC decoder.

Scenario 3: MF decoder
The same process as in the SDS scenario is undertaken to determine an upper bound on Alice's CSI estimation error that cannot be excessed. Therefore, to ensure a plausible targeted ESR, the numerator in (5.46) has to be positive. One can show that the condition to meet is: $T_2^{MF} < 0$ in (5.46), which leads to:

$$\sigma_{\max}^{\mathrm{MF}} = 1 - \frac{2^{\Delta U}(U^2+3U+3)}{2^{\Delta U}(U^2+3U+3)+U(U+1)}. \tag{5.49}$$

As for the SDS and OC decoding structures, Alice has to perfectly estimate Bob's CSI if an arbitrarily large targeted ESR aims to be ensured. However, when $\Delta \to 0^+$, $\sigma_{\max}^{\mathrm{MF}} < 1$, i.e., a positive ESR can be ensured subject to a condition on Alice's accuracy on Bob's estimated CSI. Indeed, if a targeted ESR of $\Delta \to 0^+$ wants to be ensured, it comes:

$$\sigma_{\max}^{\mathrm{MF}}\Big|_{\Delta\to 0^+} = 1 - \frac{U^2+3U+3}{2U^2+4U+3} = \frac{U(U+1)}{2U^2+4U+3}. \tag{5.50}$$

From (5.50), if $U \to \infty$, Alice is allowed to misestimate Bob's CSI with an error up to 50%, which is equivalent to ≈ -3dB of error, to ensure a positive ESR. This behaviour is observed in Figure 5.8.

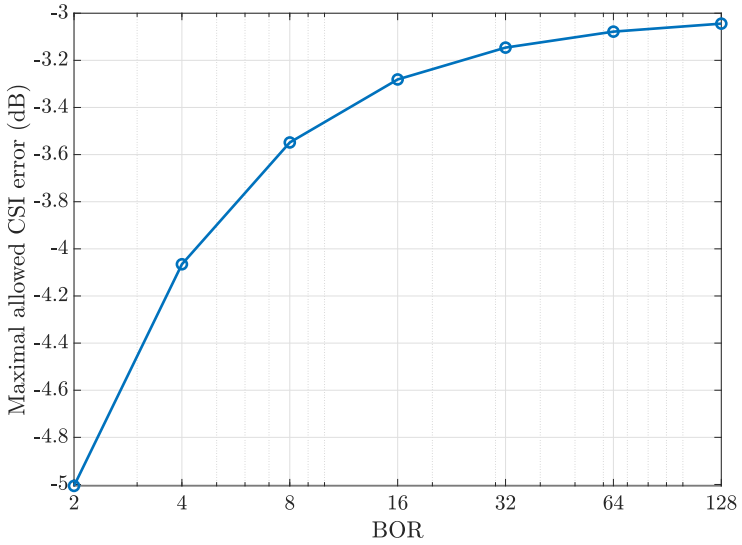

Figure 5.8: Maximal allowed CSI error to ensure a positive ESR $\Delta \to 0^+$ bit/channel use, MF decoder

Figure 5.9 shows the maximal allowed CSI estimation error as a function of the maximal per-symbol ESR that can be guaranteed by Alice, for different BOR values, and when Eve implements an MF decoder. In particular, it represents equation (5.49) as a function of Δ. The same conclusions as for the SDS and OC decoders can be drawn regarding the CSI estimation accuracy to target a given ESR w.r.t. the BOR value. However, compared to the SDS and OC decoders in Figure 5.7, when Eve implements a MF, Alice must be more precise on her main CSI estimation to ensure a given communication ESR. As an example, when the transmitter aims to communicate at a guaranteed rate of 0.2 bit/channel use with a diversity gain of $U = 32$, he can misestimate the main CSI up to ≈ -20dB of error ($\approx 1\%$ of CSI error) when the MF scenario is considered, but he is allowed to misestimate the main CSI up to ≈ -5.5dB of error ($\approx 28\%$ of CSI error) when the SDS scenario is assumed. Furthermore, for low ESRs, an increase of the BOR U relaxes the maximum allowed CSI error, as also observed in Figure 5.9 and as opposed to higher ESRs.

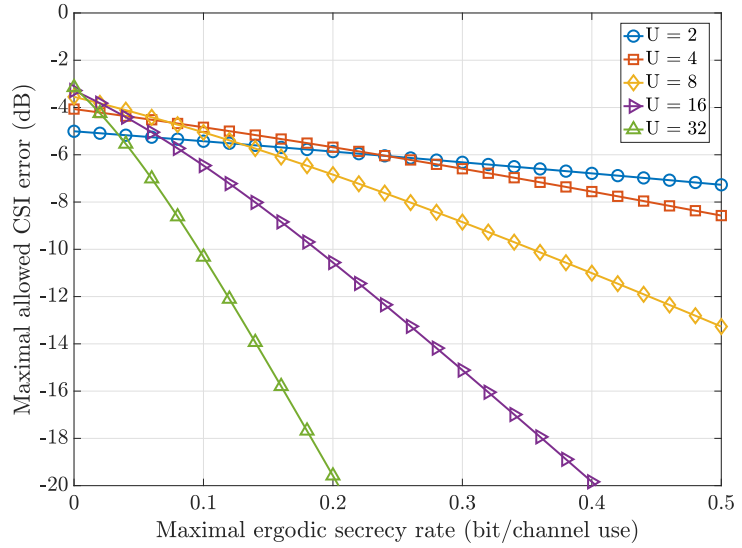

Figure 5.9: Maximal allowed CSI as a function of the maximal ESR that can be guaranteed, MF decoder

5.3.3.3 Optimal amount of data energy to inject

Expressions (5.42), (5.44), and (5.46) give the required SNR at Bob as a function of the communication parameters and the investigated scenarios. These are convex expressions in α. So, one can minimize these expressions to determine the optimal amount of data energy to inject. This corresponds to the amount of data energy that Alice has to inject, which minimizes the required SNR at Bob to ensure ESR $= \Delta$. It depends on the communication parameters, on the decoding structure implemented at Eve, and will be denoted as $\alpha_{\text{opt}}^{\text{D}}$. To find $\alpha_{\text{opt}}^{\text{D}}$, one has to calculate the derivative of SNR expressions as a function of α, and find the roots of it.

Scenario 1: SDS decoder
By denoting

$$\begin{aligned} A_1^{\text{SDS}} &= (U+1)(1-\sigma) \\ A_2^{\text{SDS}} &= \sigma\left(2^{\Delta U}-1\right) \\ A_3^{\text{SDS}} &= A_1^{\text{SDS}} + A_2^{\text{SDS}}, \end{aligned}$$

one can show that:

$$\alpha_{\text{opt}}^{\text{SDS}} = \left.\frac{-2A_1^{\text{SDS}}\left(2^{\Delta U}-1\right)+\sqrt{\Sigma^{SDS}}}{2A_1^{\text{SDS}}}\right|_{\sigma\leq\sigma_{\max}^{\text{SDS}},\alpha_{\text{opt}}^{\text{SDS}}\in[0,1]} \tag{5.51}$$

with $\Sigma^{\text{SDS}} = 4(A_1^{\text{SDS}})^2\left(2^{\Delta U}-1\right)^2 - 4A_1^{\text{SDS}}\left[-\left(2^{\Delta U}-1\right)A_3^{\text{SDS}} - A_2^{\text{SDS}}\right]$, and $\sigma_{\max}^{\text{SDS}}$ given by (5.47).
Equation (5.51) determines the amount of data that Alice has to inject, in order to minimize the required SNR at Bob that guarantees a per-symbol communication ESR$= \Delta$ bit/channel use, as a function of the BOR U, and the main CSI estimation error made at Alice σ, when Eve performs the SDS decoder. To obtain the corresponding SNR values, the parameter α in (5.42) is replaced with the values obtain in equation (5.51).

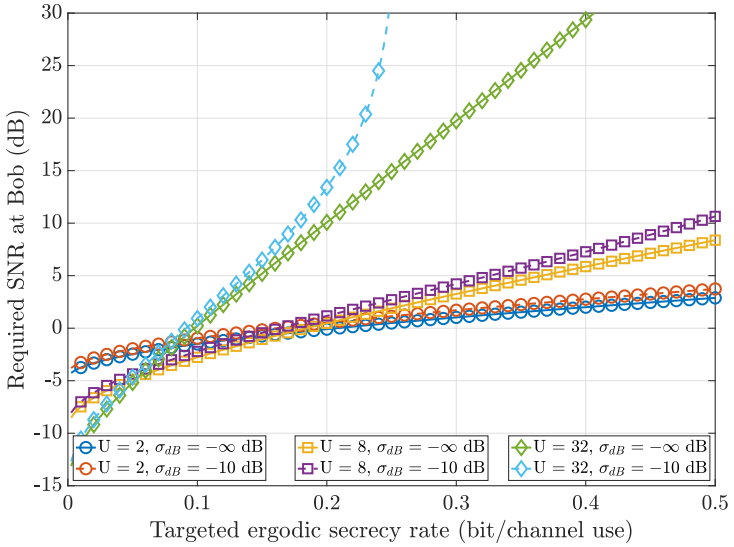

Figure 5.10: Required SNR at Bob as a function of the guaranteed ESR, with optimal AN injected, SDS decoder

Figure 5.10 represents the required SNR at Bob as a function of the targeted ESR, for different spreading factors, i.e., $U = 2$, 8, 32, and different main CSI errors, i.e. $\sigma_{\text{dB}} = -\infty$dB and $\sigma_{\text{dB}} = -10$dB, when Eve implements the SDS decoder.
First, one can observe that, a lower SNR at Bob is required to achieve a given ESR for low BORs.

However, lower SNRs are required with high BOR values when the targeted ESRs are low. The reason is that at these low rates, the secrecy of the communication is mainly influenced by the diversity gain, i.e., by the BOR value, instead of the rate decrease due to the diversity gain. As an example, when 0.05 bit/channel use is desired, $\delta_B = -4.65$dB for the error-free scenario with $U = 32$, and $\delta_B = -2.47$dB for the error-free scenario with $U = 2$. However, from a certain targeted ESR, the influence of the rate decrease exceeds that of the diversity gain, and lower BORs are desired to communicate at a given ESR. In fact, when Alice aims to safely communicate at $\Delta = 0.2$ bit/channel use, $\delta_B = 10.1$dB with $U = 32$ and $\sigma_{\text{dB}} = -\infty$dB, but only equals -0.1dB with $U = 2$ and $\sigma_{\text{dB}} = -\infty$dB. In addition, it can be outlined that the SNR loss due to imperfect main CSI estimation is higher for high BORs to maintain a desired ESR. In particular, when one wants to guarantee ESR $= 0.25$ bit/channel use when $U = 32$ and $\sigma = -10$ dB, the required SNR tends to be very large. This can be anticipated from Figure 5.7 where the maximal allowed CSI error is equal to -9.5 dB when $U = 32$ and $\Delta = 0.25$ bit/channel use. Therefore, a very high SNR at Bob is needed to communicate at this rate with $\sigma_{\text{dB}} = -10$dB.

Scenario 2: OC decoder
The optimal amount of data energy to inject when Eve implements the OC decoder is equivalent to the SDS decoder, i.e.:

$$\alpha_{\text{opt}}^{\text{OC}} = \alpha_{\text{opt}}^{\text{SDS}}\Big|_{\sigma \leq \sigma_{\max}^{\text{OC}},\, \alpha_{\text{opt}}^{\text{OC}} \in [0,1]}. \tag{5.52}$$

The optimal required SNR at Bob to guarantee ESR$= \Delta$ is therefore equivalent to the SDS scenario.

Scenario 3: MF decoder
Introducing:

$$\begin{aligned}
A_1^{\text{MF}} =& \sigma\left[2^{\Delta U}(U^2+3U+3)+U(U+1)\right]-U(U+1)\\
A_2^{\text{MF}} =& \sigma\left[2^{\Delta U}U-2^{\Delta U}(U^2+3U+3)-U(U+2)\right]+U(U+1)\\
A_3^{\text{MF}} =& U+2^{\Delta U}(U^2+3U+3)\\
A_4^{\text{MF}} =& U\left(1-2^{\Delta U}\right),
\end{aligned}$$

one finds:

$$\alpha_{\text{opt}}^{\text{MF}} = \frac{A_1^{\text{MF}}A_4^{\text{MF}} - \sqrt{\Sigma^{\text{MF}}}}{A_1^{\text{MF}}A_3^{\text{MF}}}\Big|_{\sigma \leq \sigma_{\max}^{\text{MF}},\, \alpha_{\text{opt}}^{\text{SDS}} \in [0,1]} \tag{5.53}$$

with $\Sigma^{\text{MF}} = \left(A_1^{\text{MF}}A_4^{\text{MF}}\right)^2 + A_1^{\text{MF}}A_3^{\text{MF}}A_4^{\text{MF}}\left(\sigma A_3^{\text{MF}} + A_2^{\text{MF}}\right)$, and $\sigma_{\max}^{\text{MF}}$ given in (5.49). As for the SDS scenario, equation (5.53) determines the amount of data that Alice has to inject, in order to minimize the required SNR at Bob that guarantees a per-symbol communication ESR$= \Delta$ bit/channel use, as a function of the frequency diversity gain U, and the main CSI estimation error made at Alice σ. To obtain the corresponding SNR values, the parameter α in (5.46) is replaced with the values obtained in equation (5.53).
The same remarks as for the SDS scenario can be drawn from Figure 5.11. However, when Eve implements an MF decoder, she experiences higher decoding capabilities, leading to poorer secrecy performances. From that, higher SNRs at Bob are required, compared to the SDS scenario, to guarantee a given communication ESR. As an example, when $\Delta = 0.2$ bit/channel use , $U = 8$ and $\sigma_{\text{dB}} = -10$dB, 20.48dB of SNR is required at Bob when Eve implements an MF decoder, but only 4.21dB is required when Eve implements the SDS decoder.

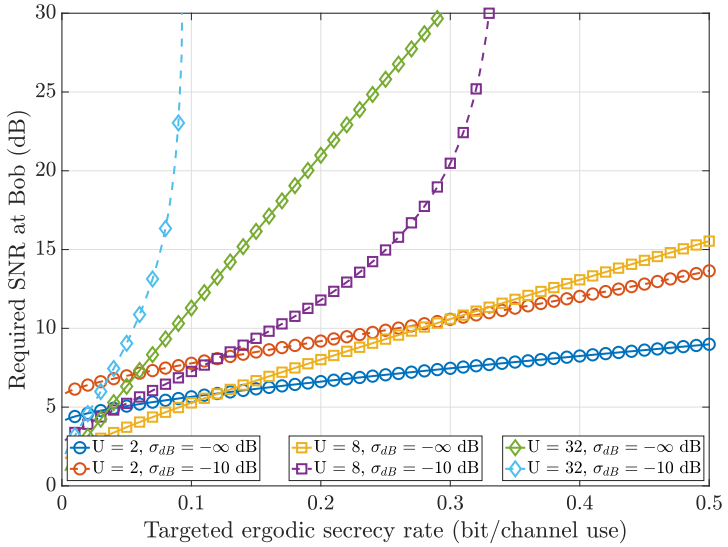

Figure 5.11: Required SNR at Bob as a function of the guaranteed ESR, with optimal AN energy injected, MF decoder

5.3.4 Secrecy outage consideration

Until now, one can state that it is preferable to communicate at low BOR values to guarantee higher communication ESRs. However, the analysis did not take into account that outages occur if the instantaneous secrecy rate that can be supported by the communication is lower than the actual ESR at which Bob and Alice communicate. This results to information that leaked to Eve. The precise amount of leaked information cannot be known since it depends on the wiretap codes, but outages can be characterized. As explained in chapter 2, an BF environment is assumed, allowing Alice to code within a coherence interval, and thus limiting the amount of leaked information at the eavesdropper to the amount of information transmitted at the legitimate receiver. As a reminder, it was chosen to study the ϵ-achievable secrecy rate (ϵ-achievable SR), which corresponds to the rate that is achievable securely while keeping an outage probability under ϵ. As always, the worst-case scenario in terms of security is assumed, i.e., Eve has a noise-free hardware. The following results are obtained via Monte Carlo simulation with Matlab, considering 100.000 realizations of the instantaneous secrecy rate, in order to observe very low outage percentages.

Scenarios 1: SDS decoder

The left part of Figure 5.12 represents the ϵ-achievable SR as a function of the fraction of outage, for different BOR values, and when Alice misestimates Bob's CSI with an error of 30%, i.e., $\sigma_{\text{dB}} \approx -5.2$dB. It can be observed that, when Eve implements an SDS decoder, for very low percentages of outage, it is preferable to communicate at higher BOR values. Indeed, the system exhibit higher ϵ-achievable secrecy rates with $U = 8$ compared to $U = 2$ when less than 0.13% of outage is allowed. For higher percentages of outage, lower BOR values are more likely to be used.
The right part represents the 0.2%-achievable SR, as a function of the CSI estimation error made by Alice, for different BOR values. It is seen that, when Alice well estimates Bob's CSI, i.e., low value of σ, low BORs enhance the secrecy performance. On the opposite, when Alice strongly misestimates Bob's CSI, it is more likely to communicate at higher BORs to enhance the outage performance.

From the above discussion, Alice's choice on the communication BOR factor results from a trade-off. When low outage percentages are required and Alice strongly misestimates Bob's CSI, higher BORs values are needed to increase the outage performances. However, it is more likely to communicate at lower BORs if Alice aims to increase the ESR. In fact, the trade-off on Alice's choice on the BOR factor is expected even when she estimates well Bob's CSI. However, it is expected to be seen for outage percentages that are several order lower than when Alice strongly misestimates Bob's CSI,

which cannot be observed in simulation.

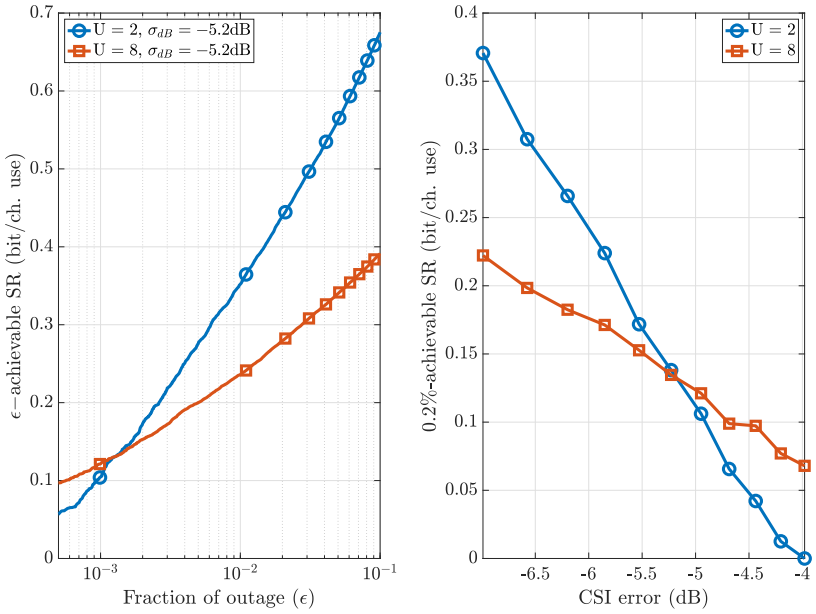

Figure 5.12: ϵ-achievable secrecy rate performances, $\delta_B = 10$dB, SDS decoder

Scenarios 2: OC decoder

The left part of Figure 5.13 represents the ϵ-achievable SR as a function of the fraction of outage, for different BOR values, and when Alice misestimates Bob's CSI with an error of 20%, i.e., $\sigma_{\text{dB}} \approx -7$dB. The same conclusions as for the SISO-SE SDS scenario can be drawn.

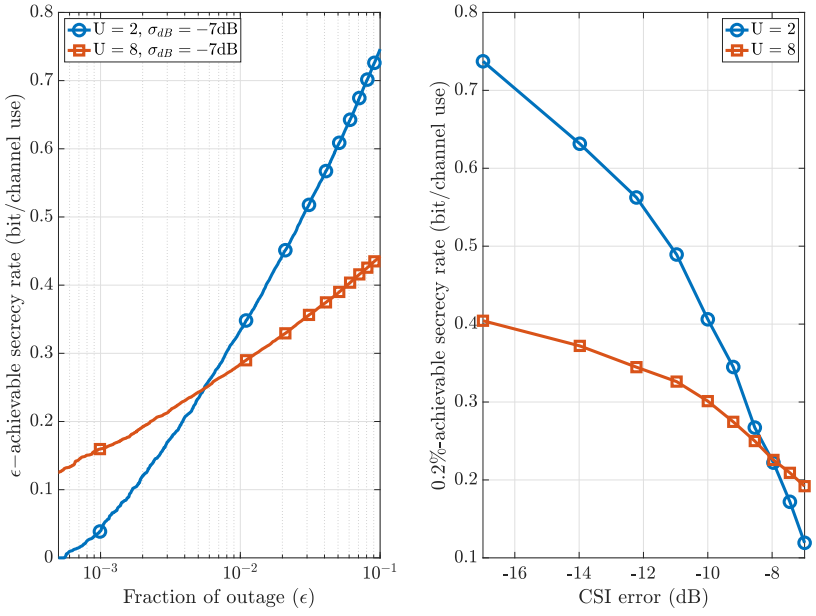

Figure 5.13: ϵ-achievable secrecy rate performances, $\delta_B = 10$dB, OC decoder

Scenarios 3: MF decoder

Figure 5.14 represents the same situations as Figure 5.12 but with no CSI error made at Alice. First,

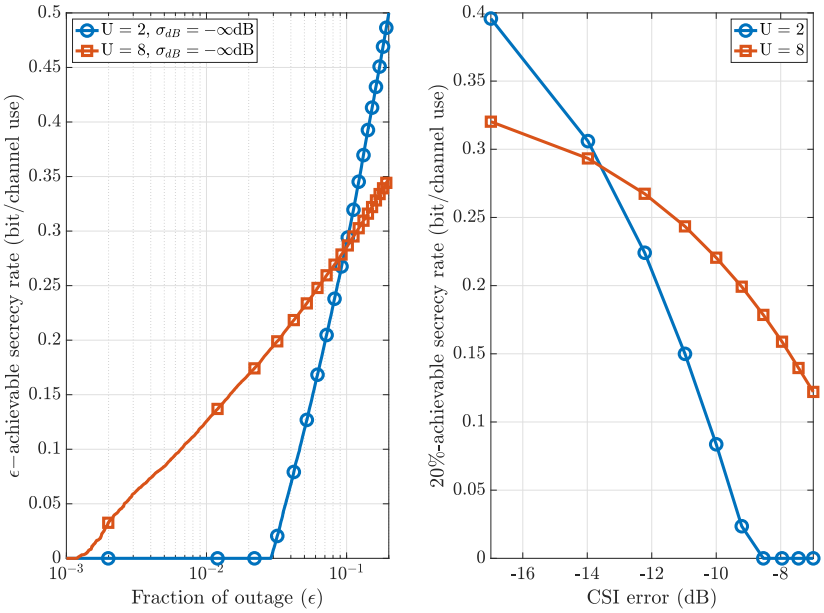

Figure 5.14: ϵ-achievable secrecy rate performances, $\delta_B = 10$dB, MF decoder

it is observed from the left part that, when $U = 8$, the ϵ-achievable secrecy rate outperforms lower BOR values until $\approx 9.7\%$ of outage. In addition, when 3% of outage is allowed, no secrecy can be ensured when $U = 2$, but 0.2 bit/channel can be provided at $U = 8$.

From the right part of Figure 5.14, it is observed that the 20%-achievable SR is very low and becomes zero, i.e., impossible to ensure a positive SR with less than 20% of outage, as soon as $\sigma_{\text{dB}} > -9$ dB (corresponding to $\approx 12.6\%$ of CSI error) with $U = 2$. Increasing the BOR value allows to keep higher 20%-achievable secrecy rate for poor channel estimates. In particular, if $\sigma_{\text{dB}} = -9$ dB, the 20%-achievable SR equals 0.18 bit/ channel use with $U = 8$. To achieve low outage, higher BOR values are therefore mandatory.

As a consequence, when Eve implements a MF, i.e., when she is able to benefit from high decoding capabilities, it is observed that Alice's choice on the BOR value results from a trade-off. Knowing, the CSI error variance and Bob's SNR, Alice can choose a BOR value either to maximize the ESR (by decreasing the BOR value), i.e., higher data rate transmission, or to ensure a given $\epsilon-$achievable secrecy rate (by increasing the BOR value), i.e., less data leakage. On the opposite, when Eve implements the SDS or the OC decoders, there is no trade-off on the choice on the spreading factor of the communication. It is preferable to communicate at low BOR to guarantee higher data rate transmission with lower outage, even when Alice strongly misestimates Bob's CSI.

5.3.5 Strong decoding structures performance

In Section 4.6.4, two handshake procedures considering a FDD communication are described. As a reminder, if a BF environment is assumed, Eve implements a decoding structure that aligns the AN signal in her null space, termed as the AN killer, and defined in equation (5.6). In a SF environment, Eve implements a LMMSE decoder which makes a trade-off between suppressing the AN and amplifying the AWGN. The LMMSE decoding structure is defined in equation (5.7).

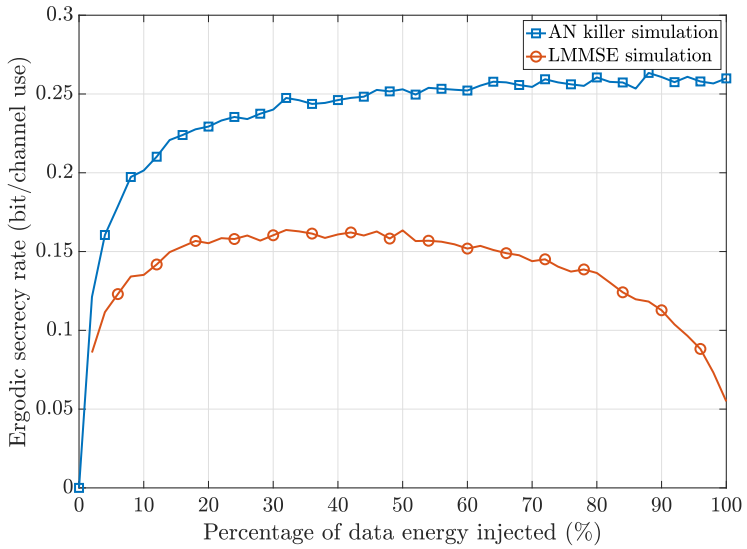

Figure 5.15: Ergodic secrecy rate as a function of α, $\delta_B = 10$dB, $\delta_E = 10$dB, $U = 8$, $\sigma_{\text{dB}} = -\infty$ dB, FDD decoders

The ESR performance of these two decoding is shown in Figure 5.15 via simulation only. It presents the ESR a function of the injected energy dedicated for information data. It is considered that Bob and Eve's SNRs both equal 10dB. It is seen that the LMMSE decoder outperforms the AN killer, which is expected. Indeed, the LMMSE implements a trade-off between amplifying the AWGN and reducing the AN. On the opposite, the AN killer strongly amplifies the AWGN, while suppressing the AN. In addition, both decoders outperform the classical linear decoders implemented in TDD communications, i.e., they lead to lower secrecy performances. As an example, for the error-free scenario, with $U = 8$ and $\delta_E = 10$dB, a maximal ESR of 0.26 and 0.16 bit/channel use is achieved for the AN killer and the LMMSE decoders, respectively. When Eve implements a MF decoder and considering $\delta_E = +\infty$dB, with $U = 8$ and $\sigma_{\text{dB}} = -\infty$dB, a maximal ESR of 0.28 bit/channel use can be guaranteed, as seen in Figure 5.6. Furthermore, if Eve is equipped with a noise-free hardware, the ESR becomes zero, i.e., it is not possible to guarantee a given secrecy performance with these decoding scenarios. Indeed, with the AN killer decoding structure, if $\sigma_{\text{E}}^2 = 0$, Eve's capacity becomes infinite since no AN remains. With the LMMSE decoder, the AN is suppressed when there is no AWGN.

From that, one can conclude that no secrecy can be ensured when FDD communications are considered. Indeed, even with only one antenna, Eve can implement decoding structures that considerably jeopardize any attempt to secure the communication. This motivates the fact that the secrecy performances in FDD scenarios, coming from two different FDD handshake procedures, are only assessed for the SISO-SE system's configuration.

5.4 Single-Input Single-Output Multi-Eavesdropper

5.4.1 Preliminaries

The expressions of the received signals at Bob and Eve(s)'s positions, the decoding structures implemented at Eve(s), as well as the AN generation condition, are first reminded in this section to facilitate the reader's understanding. As a reminder, only the three scenarios involving a TDD handshake procedure are investigated.

Remark 5.4: Multi-eavesdropper(s)

As already explained, the multi-antenna eavesdropper scenario can either represent one eavesdropper with multiple antennas, or multiple colluding eavesdroppers with one or multiple antenna(s). Both cases are treated similarly since no spatial correlation is considered. For the rest of this chapter, the multi-eavesdroppers are simply denoted as "Eve".

Received signal expressions
At Bob, nothing changes compared to the SISO-SE configuration. The received signal is therefore:

$$\mathbf{y}_{\mathrm{B}}^{\mathrm{SISOME}} = \sqrt{\alpha(1-\sigma)}\mathbf{S}^H ||\mathbf{H_B}||^2 \mathbf{S}\mathbf{x} + \sqrt{\alpha\sigma}\mathbf{S}^H \mathbf{H_B} \Delta \mathbf{H_B}^H \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \mathbf{H_B}\mathbf{w} + \mathbf{S}^H \mathbf{v}_{\mathrm{B}}, \tag{5.54}$$

At Eve, from equation (4.14), the received signal is expressed as:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{SISOME},\mathbf{D}} = \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\widehat{\mathbf{H}}_{\mathbf{B}}^{*}\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\mathbf{w} + \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{D}_{\mathbf{E},k}\mathbf{v}_{\mathrm{E},k} \tag{5.55}$$

where $\mathbf{D}_{\mathbf{E},k}$ is a $Q \times Q$ decoding matrix performed at Eve(s) whose nature depends on the handshake protocol between the transmitter and the legitimate receiver.

Decoding structures at Eve
The decoding structures at Eve are given in Sections 4.6.3.

TDD handshake procedure 1: same decoding structure decoder.
The handshake procedure is presented in Figure 4.12. Eve is only able to know $\mathbf{H_{BE}}$ which is of no help. She implements the same decoding structure as Bob:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{SDS}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{I}_Q. \tag{5.56}$$

TDD handshake procedure 2: own channel decoder.
The handshake procedure is presented in Figure 4.13. Eve implements a decoding structure that takes benefit from her own channel knowledge:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{OC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}^H. \tag{5.57}$$

TDD handshake procedure 3: maximum ration combining decoder.
The handshake procedure is presented in Figure 4.14. Eve can access to the knowledge of her equivalent channel. She implements a MRC decoding structure, which is equivalent to the a MF decoder in the case of multiple antennas:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B}}\mathbf{H}_{\mathbf{E},k}^H. \tag{5.58}$$

AN generation
In a SISO-ME configuration, the AN is generated similarly as for the SISO-SE configuration:

$$\mathbf{S}^H \widehat{\mathbf{H}}_{\mathbf{B}} \mathbf{w} = \mathbf{0}_N, \tag{5.59}$$

5.4.2 Ergodic secrecy rate modeling

As for the SISO-SE system, the metric of interest is the ESR, defined in (5.11). In order to obtain a model for the ESR, analytic expressions of the ESINRs are determined. Bob's ESINR is naturally not affected by the presence of passive Eve. Therefore, Bob's ESINR and channel capacity are respectively given by equations (5.18) and (5.19).

The derivation of the ESINR at Eve is conducted in this section for the three investigated decoding structures, coming from the TDD handshakes. Depending on the decoder Eve implements, an approximation of the ESINR of the n^{th} symbol is derived, which is identical to the SISO-SE configuration:

$$\mathbb{E}\left[\gamma_{E,n}^{\text{D}}\right] \approx \frac{\mathbb{E}\left[\left|E_{1,n}^{\text{D}}\right|^2\right]}{\mathbb{E}\left[\left|E_{2,n}^{\text{D}}\right|^2\right] + \mathbb{E}\left[\left|E_{3,n}^{\text{D}}\right|^2\right]}, \tag{5.60}$$

where $E_{1,n}^{\text{D}}$, $E_{2,n}^{\text{D}}$ and $E_{3,n}^{\text{D}}$ are respectively the data, noise, and AN (i.e., interference) n^{th} symbol components of the received signal at Eve's position, depending on the investigated scenario, when a SISO-ME system is considered.

TDD handshake procedure 1: same decoding structure decoder
When Eve implements the SDS decoder, by replacing (5.56) in (5.55), the received signal becomes:

$$\mathbf{y}_{\text{E}}^{\text{SDS}} = \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k} \widehat{\mathbf{H}}_{\mathbf{B}}^H \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}\mathbf{w} + \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{v}_{\text{E},k}. \tag{5.61}$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\text{SDS}} = \frac{\sqrt{\alpha}}{U} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} h_{\text{E},k,i} \hat{h}_{\text{B},i}^* \tag{5.62a}$$

$$E_{2,n}^{\text{SDS}} = \frac{1}{\sqrt{U}} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} v_{\text{E},k,i} \tag{5.62b}$$

$$E_{3,n}^{\text{SDS}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} h_{\text{E},k,i} w_i. \tag{5.62c}$$

As detailed in C.1.1, C.1.2, and C.1.3, the expected energy of the components can respectively be expressed as:

$$\mathbb{E}\left[|E_{1,n}^{\text{SDS}}|^2\right] = \frac{N_E \alpha}{U} \tag{5.63a}$$

$$\mathbb{E}\left[|E_{2,n}^{\text{SDS}}|^2\right] = N_E \sigma_{\text{E}}^2 \tag{5.63b}$$

$$\mathbb{E}\left[|E_{3,n}^{\text{SDS}}|^2\right] = \frac{(1-\alpha)N_E}{U}. \tag{5.63c}$$

As for the SISO-SE configuration, Eve is not impacted by the CSI estimation error from Alice, since she is able to perfectly estimates the amount of CSI she can obtain.

Introducing (5.63a), (5.63b), and (5.63c) into (5.60), the per-symbol approximated ESINR when Eve implements a SDS decoder, in a SISO-ME system configuration, is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{SDS}}\right] \approx \frac{N_E\alpha}{N_E U\sigma_{\mathrm{E}}^2 + N_E(1-\alpha)} = \frac{\alpha}{U\sigma_{\mathrm{E}}^2 + (1-\alpha)}. \tag{5.64}$$

Result (5.64) is very interesting. In particular, it shows that, when Eve implements an SDS decoder, her performance is not influenced by the number of antennas she is equipped with. Indeed, the array gain, equal to N_E, applies similarly to the data, the noise and the AN components as seen in (5.63). Thus, the expression (5.64) is identical to the SISO-SE ESINR expression (5.27), i.e., Eve's ESINR in a SISO-ME system is identical to Eve's ESINR in a SISO-SE system. From that, all the results from the single-antenna eavesdropper scenario hold for the multi-antenna eavesdropper scenario. The approximated EC at Eve with an SDS decoder is therefore given by (5.28):

$$C_E^{\mathrm{SDS}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{SDS}}\right]\right) = \log_2\left(1+\frac{\alpha}{U\sigma_{\mathrm{E}}^2+(1-\alpha)}\right) \tag{5.65}$$

The exact EC is by Monte Carlo simulations(100.000 realizations) as:

$$\widehat{C}_E^{\mathrm{SDS}} = \mathbb{E}\left[\log_2\left(1+\gamma_{E,n}^{\mathrm{SDS}}\right)\right]. \tag{5.66}$$

Figure 5.16 compares the approximated EC C_E^{SDS} given in (5.65) with the exact EC $\hat{C}_E^{\mathrm{SDS}}$, and given in (5.66), as a function of α, with $U=2$, when considering the error-free scenario, and for different number of Eve's antennas. It is first observed that the approximated and the exact capacities are very close, which validates the approximation in (5.28). In addition, it is seen that the number of eavesdropper's antennas does not influence the eavesdropper's capacity, as anticipated from equation (5.64). Consequently, when Eve implements an SDS decoder, she experiences the same performance regardless of the number of antennas she possesses.

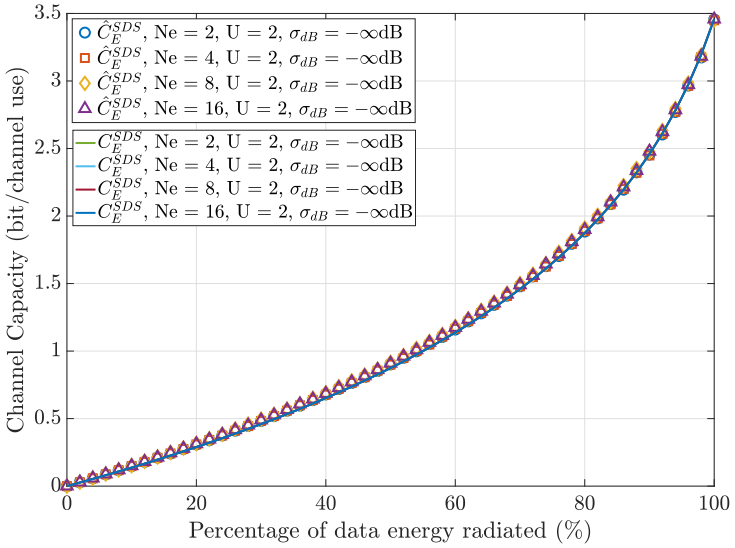

Figure 5.16: Comparison between approximated EC and exact EC at Eve, SDS decoder, $\delta_E = 10$dB, 100.000 realizations

TDD handshake procedure 2: own channel decoder

When Eve implements the OC decoder, by replacing (5.57) in (5.55), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{OC}} = \sqrt{\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}||\mathbf{H}_{\mathbf{E},k}||^2\widehat{\mathbf{H}}_{\mathbf{B}}^H\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}||\mathbf{H}_{\mathbf{E},k}||^2\mathbf{w} + \mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{H}_{\mathbf{E},k}^H\mathbf{v}_{\mathrm{E},k}. \tag{5.67}$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\text{OC}} = \frac{\sqrt{\alpha}}{U} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} |h_{\text{E},k,i}|^2 \hat{h}_{\text{B},i}^* \tag{5.68a}$$

$$E_{2,n}^{\text{OC}} = \frac{1}{\sqrt{U}} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} h_{\text{E},ki}^* v_{\text{E},k,i} \tag{5.68b}$$

$$E_{3,n}^{\text{OC}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} |h_{\text{E},k,i}|^2 w_i. \tag{5.68c}$$

As detailed in C.2.1, C.2.2, and C.2.3, the expected energy of the components can respectively be expressed as:

$$\mathbb{E}\left[|E_{1,n}^{\text{OC}}|^2\right] = \frac{\alpha N_E(N_E+1)}{U} \tag{5.69a}$$

$$\mathbb{E}\left[|E_{2,n}^{\text{OC}}|^2\right] = N_E \sigma_{\text{E}}^2 \tag{5.69b}$$

$$\mathbb{E}\left[|E_{3,n}^{\text{OC}}|^2\right] = \frac{(1-\alpha)N_E(N_E+1)}{U}. \tag{5.69c}$$

As always, Eve is not impacted by the main CSI misestimate. Introducing (5.69a), (5.69b), and (5.69c) into (5.60), the per-symbol approximated ESINR when Eve implements the OC decoding structure, in a SISO-ME system configuration, is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\text{OC}}\right] \approx \frac{\frac{\alpha N_E(N_E+1)}{U}}{N_E\sigma_{\text{E}}^2 + \frac{(1-\alpha)N_E(N_E+1)}{U}} = \frac{\alpha(N_E+1)}{U\sigma_{\text{E}}^2 + (1-\alpha)(N_E+1)}. \tag{5.70}$$

Eve's SINR in a SISO-ME OC scenario (5.70) is not identical to her SINR in a SISO-SE OC scenario (5.33). Indeed, one can observe the impact of N_E in (5.70). However, at large number of received antennas, i.e., $N_E \to \infty$, $\mathbb{E}\left[\gamma_{E,n}^{\text{OC}}\right] \to \frac{\alpha}{(1-\alpha)}$, i.e., Eve's performances are no more influenced by the number of antennas she possesses. In addition, when $N_E = 1$ in (5.70), one comes back to the single-antenna eavesdropper derivation (5.33).
The approximated EC at Eve when the OC decoder is implemented is therefore expressed as:

$$C_E^{\text{OC}} \approx \log_2\left(1 + \mathbb{E}\left[\gamma_{E,n}^{\text{OC}}\right]\right) = \log_2\left(1 + \frac{\alpha(N_E+1)}{U\sigma_{\text{E}}^2 + (1-\alpha)(N_E+1)}\right). \tag{5.71}$$

Figure 5.17 compares the approximated EC C_E^{OC} given in (5.71) with the exact EC $\hat{C}_E^{\text{OC}}$ obtained by Monte Carlo simulations (100.000 realizations) for the same set of parameters as in the SDS scenario.

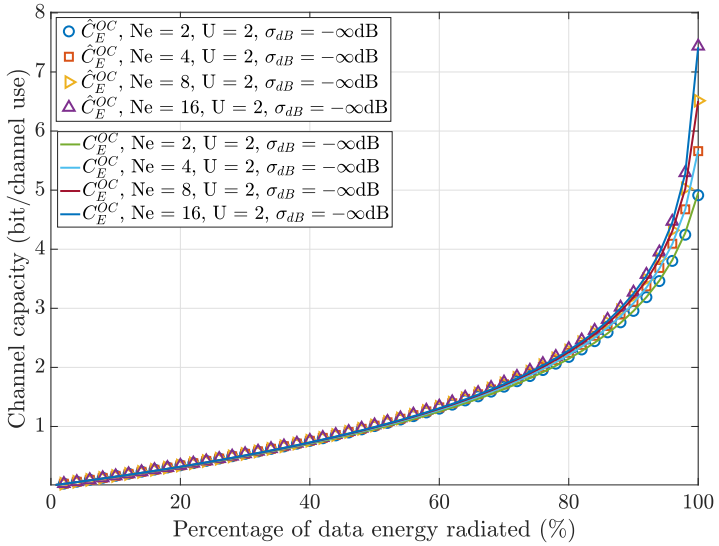

Figure 5.17: Comparison between approximated EC and exact EC at Eve, OC decoder, $\delta_E = 10$dB, 100.000 realizations

First, the EC approximation's curves given by (5.71) fit well the exact EC curves. Therefore, it can be used as a closed-form expression for the rest of the study. One can also observe a slight influence of the number of eavesdropping antennas on the capacity, especially at high percentages of data energy injected, i.e., when $\alpha \to 1$. Indeed, when $\alpha \to 1$, the numerator of Eve's SINR is equal to $N_E + 1$, and the denominator does not depend on N_E. The SINR consequently increases with an increase of the number of antennas. This shows the need of AN injection at the transmitter side, in order not to suffer from too high decoding capabilities at Eve when she is equipped with a large number of antennas.

TDD handshake procedure 3: maximum ratio combining decoder

When Eve implements the MRC decoder, by replacing (5.58) in (5.55), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{MRC}} = \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} ||\mathbf{H}_{\mathbf{E},k}||^2 \left|\left|\widehat{\mathbf{H}}_{\mathbf{B}}\right|\right|^2 \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B}} ||\mathbf{H}_{\mathbf{E},k}||^2 \mathbf{w} + \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{H}_{\mathbf{E},k}\widehat{\mathbf{H}}_{\mathbf{B}}\mathbf{v}_{\mathrm{E},k}. \quad (5.72)$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\mathrm{MRC}} = \frac{\sqrt{\alpha}}{U} \sum_{i=0}^{U-1} \sum_{k=1}^{N_E} |h_{\mathrm{E},k,i}|^2 \left|\hat{h}_{\mathrm{B},i}\right|^2 \quad (5.73a)$$

$$E_{2,n}^{\mathrm{MRC}} = \frac{1}{\sqrt{U}} \sum_{i=0}^{U-1} \sum_{k=1}^{N_E} h_{\mathrm{E},k,i}^* \hat{h}_{\mathrm{B},i} v_{\mathrm{E},k,i} \quad (5.73b)$$

$$E_{3,n}^{\mathrm{MRC}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}} \sum_{i=0}^{U-1} \sum_{k=1}^{N_E} \hat{h}_{\mathrm{B},i} |h_{\mathrm{E},ki}|^2 w_{k,i}. \quad (5.73c)$$

As detailed in C.3.1, C.3.2, and C.3.3, the expected energy of the components can respectively be expressed as:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{MRC}}|^2\right] = \frac{\alpha N_E}{U}\left[N_E(U+1)+2\right] \quad (5.74a)$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{MRC}}|^2\right] = N_E \sigma_{\mathrm{E}}^2 \quad (5.74b)$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{MRC}}|^2\right] = \frac{(1-\alpha)}{U+1} N_E. \quad (5.74c)$$

Introducing (5.74a), (5.74b), and (5.74c) into (5.60), the per-symbol approximated ESINR when Eve implements the MRC decoding structure, in a SISO-ME system configuration, is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right] \approx \frac{\frac{\alpha N_E}{U}\left[N_E(U+1)+2\right]}{N_E\sigma_{\mathrm{E}}^2+\frac{(1-\alpha)}{U+1}N_E} = \frac{\frac{\alpha}{U}\left[N_E(U+1)+2\right]}{\sigma_{\mathrm{E}}^2+\frac{(1-\alpha)}{U+1}}. \tag{5.75}$$

First, if one sets $N_E = 1$, one comes back to the single-antenna scenario (5.38). Also, it is observed that the numerator in (5.75) is about $N_E\,U$ times larger than in the SDS and OC scenarios given in (5.64) and (5.70), respectively. This results from the fact that, when Eve implements an MRC decoder, she benefits from a diversity gain U at each of her N_E antennas. In addition, it is observed an influence of the number of antennas on the SINR expression. Indeed, $\mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right] \propto N_E$, i.e., the SINR tends to be infinite when the number of eavesdropper's antennas becomes arbitrarily large thanks to the array gain. The approximated EC when Eve implements a MRC decoder in a SISO-ME configuration is given by:

$$C_E^{\mathrm{MRC}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right]\right) = \log_2\left(1+\frac{\frac{\alpha}{U}\left[N_E(U+1)+2\right]}{\sigma_{\mathrm{E}}^2+\frac{(1-\alpha)}{U+1}}\right). \tag{5.76}$$

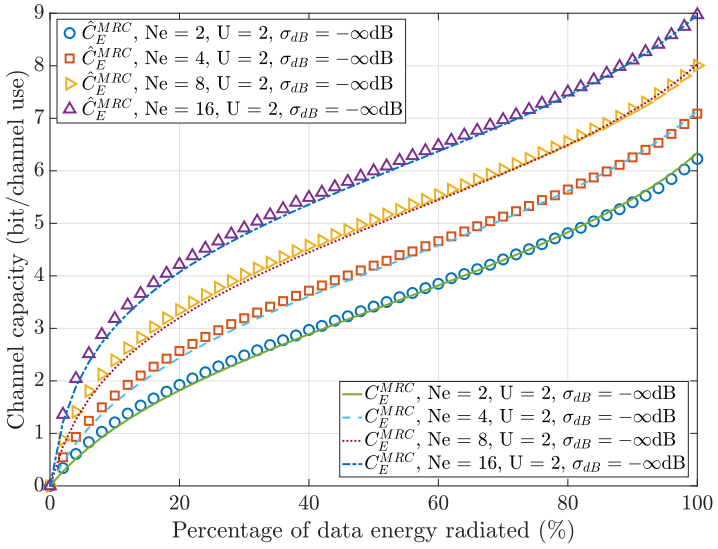

Figure 5.18: Comparison between approximated EC and exact EC at Eve, MRC decoder, $\delta_E = 10$dB, 100.000 realizations

Figure 5.18 compares the approximation (5.76) with the exact EC expression obtained by Monte Carlo simulations (100.000 realizations), for the same set of parameters as for the previous scenarios. It can be observed that (5.76) well approximates the exact EC, such that the approximation can be considered as a closed-form expression for the rest of the study. In addition, Eve's capacity increases when her number of antennas increases, which is expected from the discussion about (5.75).

5.4.3 Guaranteeing Secrecy Rate

As for the SISO-SE system configuration, Alice needs to a-priori know the per-symbol communication ESR over which she can securely communicate with Bob. In order to do so, Alice must design the communication parameters, depending on the investigated scenario. Similarly to the single-antenna eavesdropper scenario, derivations of the required SNR at Bob $\delta_{\mathrm{B}}^{\mathrm{D}}$ (Section 5.4.3.1), the maximal main CSI estimation error $\sigma_{\mathrm{max}}^{\mathrm{D}}$ (Section 5.4.3.3), and the optimal amount of data energy to inject $\alpha_{\mathrm{opt}}^{\mathrm{D}}$ (Section 5.4.3.4), are derived, for the three investigated scenarios. In addition, a study of the maximal number of Eve's antennas allowing to guarantee targeted communication ESR $= \Delta$ is conveyed in Section 5.4.3.2. To be able to guarantee a communication ESR, Eve is assumed to have a noise-free hardware, like previously.

5.4.3.1 Required SNR at Bob

As for the SISO-SE configuration, Bob's SNR is defined as $\delta_{\mathrm{B}}^{\mathrm{D}} = \frac{1}{U\sigma_{\mathrm{B}}^2}$, which is the ratio between the energy of the received symbol components (data and AN) and the noise components at Bob.

Scenario 1: same decoding structure decoder
Bob and Eve's SINRs in an SDS SISO-ME scenario are identical to the ones in a SDS SISO-SE configuration. Therefore, the required SNR at Bob to guarantee a communication ESR=Δ bit/channel is similar to the SISO-SE configuration, and can be found in Section 5.3.3.1. This is a remarkable result since a positive ESR can be guaranteed, regardless the number of antennas at Eve.

Scenario 2: own channel decoder
When $\sigma_{\mathrm{E}}^2 = 0$, Eve's SINR becomes:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right]\Big|_{\sigma_{\mathrm{E}}^2=0} = \frac{\alpha(N_E+1)}{(1-\alpha)(N_E+1)} = \frac{\alpha}{1-\alpha}, \tag{5.77}$$

which is equivalent to Eve's ESINR in the single eavesdropper case with $\sigma_{\mathrm{E}}^2 = 0$, given by (5.33). One can conclude that the study of the SISO-ME system can be reduced to the study of the SISO-SE system when Eve implements the OC decoder, which is also equivalent to the SDS decoder in terms of required Bob's SNR. The related discussion be found in section 5.3.3.1, and the secrecy performance does not depend on the number of Eve's antennas.

Scenario 3: maximum ratio combining decoder
Introducing (5.19) and (5.76) in (5.11), and considering $\sigma_{\mathrm{E}}^2 = 0$, the guaranteed ESR when Eve implements the MRC decoder is:

$$R_{s,n}^{\mathrm{MRC}} = \frac{1}{U}\left[\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right|}{U\sigma_{\mathrm{B}}^2+(1-\alpha)\sigma}\right) - \log_2\left(1+\frac{\frac{\alpha}{U}\left[N_E(U+1)+2\right]}{\frac{(1-\alpha)}{U+1}}\right)\right] \tag{5.78}$$

Figure 5.19 shows the maximal ESR that can be guaranteed as a function of the main CSI estimation error σ_{dB}, for different numbers of eavesdropping antennas. Between each sub-figure, the BOR value changes. First, it can be stated that, at low BOR values, the security scheme is less robust to an increase number of Eve's antennas. As an example, when $\sigma_{\mathrm{dB}} = -10$dB, i.e., Alice misestimates Bob's CSI with 10% or error, a positive ESR is only possible if Eve has $N_E \leq 2$ antennas with $U = 2$. However, when $U = 32$, Eve can have up to 4 antennas and yet, positive ESR is possible. In addition, when the BOR increases, for a particular number of eavesdropper's antennas, the ESR stays positive for larger CSI estimation errors. Indeed, if $N_E = 2$ and $U = 2$, one observes null secrecy, i.e., $\Delta = 0$, as soon as $\sigma_{\mathrm{dB}} > -9$dB, which corresponds to $\approx 12.5\%$ of CSI error. With $U = 32$, null secrecy is obtained as soon as $\sigma_{\mathrm{dB}} > -6$dB, which corresponds to $\approx 25\%$ of CSI error. Furthermore, when the number of eavesdropping antennas increases, Alice can provide less secrecy. This is clearly visible in the ESINR expression (5.75) where it is seen that it increases proportionally with N_E. The secrecy of the communication is then reduced.

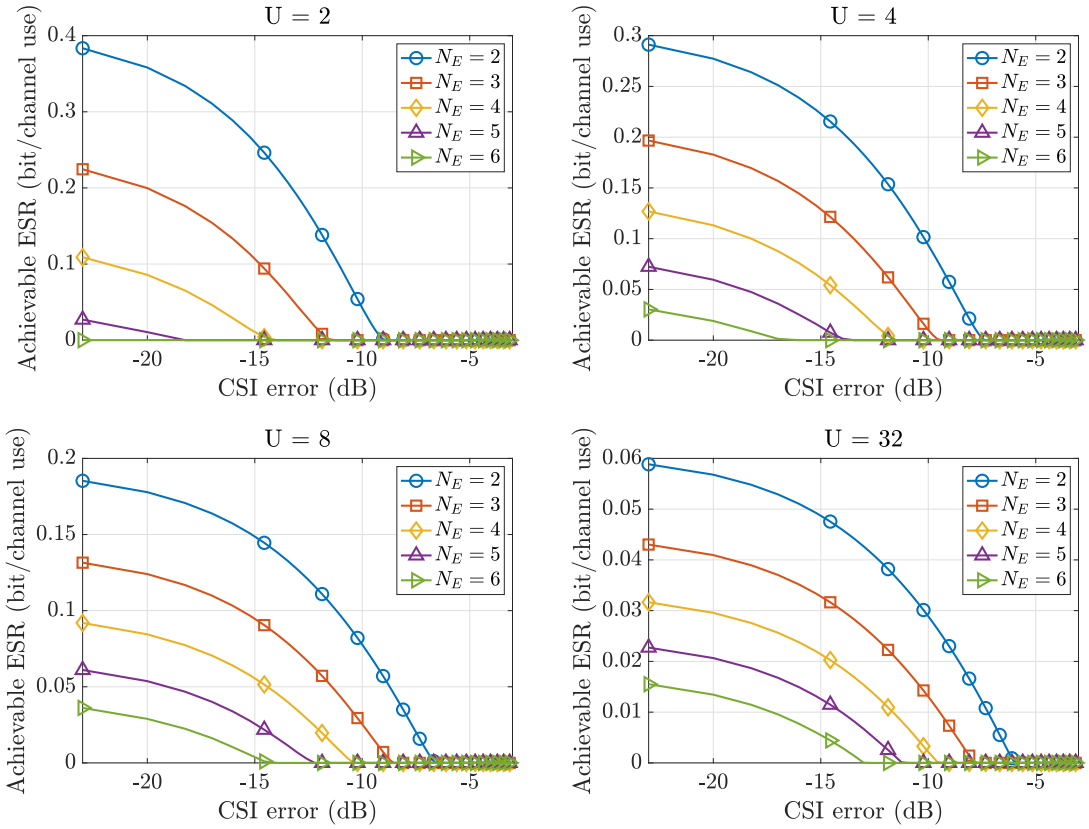

Figure 5.19: Maximal guaranteed ESR as a function of the main CSI error, MRC decoder.

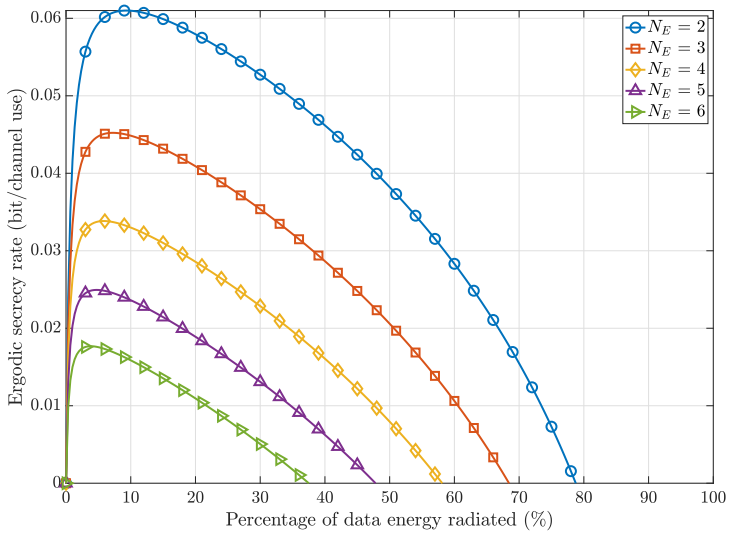

Figure 5.20: Guaranteed ergodic secrecy rate, MRC decoder, $U = 32$, $\sigma_{\text{dB}} = -\infty\text{dB}$, $\delta_B = 10\text{dB}$.

Figure 5.20 shows the achievable ergodic ESR as a function of the percentage of energy injected dedicated for information data, considering the error-free scenario, i.e., $\sigma_{\text{dB}} = -\infty\text{dB}$, and with $U = 32$. One observes an ESR decrease due to an increase number of Eve's antennas. In fact, when $N_E = 2$, a maximal ESR of 0.061 bit/channel use can be ensured. When $N_E = 6$, only 0.018 bit/channel use can be provided. In addition, it is seen that when N_E increases, more AN, i.e., lower percentage of data energy, needs to be injected to maximize the ESR. The maximal ESR is attained for $\approx 91.6\%$

of injected AN energy with $N_E = 2$, and for $\approx 96\%$ of AN energy with $N_E = 6$. Finally, when Eve implements the MRC decoder, one concludes that it is crucial to inject some AN since no secrecy can be provided when only information data is transmitted.

After manipulating equation (5.78), one obtains the required SNR at Bob to guarantee ESR $= \Delta$, when Eve implements the MRC decoder:

$$\delta_{\mathrm{B}}^{\mathrm{MRC}} = \frac{\alpha T_0^{\mathrm{MRC}} + T_1^{\mathrm{MRC}}}{\alpha^2 T_2^{\mathrm{MRC}} + \alpha T_3^{\mathrm{MRC}} + T_4^{\mathrm{MRC}}}, \tag{5.79}$$

where:

$$\begin{aligned}
T_0^{\mathrm{MRC}} &= 2^{\Delta U}\left[N_E(U+1)^2 + (U+2)\right] + U \\
T_1^{\mathrm{MRC}} &= U(2^{\Delta U} - 1) \\
T_2^{\mathrm{MRC}} &= 2^{\Delta U}\sigma\left[N_E(U+1)^2 + (U+2)\right] - U(U+1)(1-\sigma) \\
T_3^{\mathrm{MRC}} &= U\left[(U+1)(1-\sigma) - \sigma\right] - 2^{\Delta U}\sigma\left[N_E(U+1)^2 + 2\right] \\
T_4^{\mathrm{MRC}} &= U\sigma\left(1 - 2^{\Delta U}\right).
\end{aligned}$$

If one sets $N_E = 1$ in (5.79), one comes back to MF SISO-SE scenario (5.46).

5.4.3.2 Maximal eavesdropper antennas allowed

Scenario 1: same decoding structure decoder
There is no condition to determine for the maximal number of eavesdropping antennas allowed to ensure a per-symbol communication ESR. This arises from the fact that the SDS SISO-ME scenario is similar to the SDS SISO-SE scenario.

Scenario 2: own channel decoder
There is no condition to determine for the maximal number of eavesdropping antennas allowed to ensure a per-symbol communication ESR. This arises from the fact that the OC SISO-ME scenario is similar to the OC SISO-SE scenario when $\sigma_{\mathrm{E}}^2 = 0$.

Scenario 3: maximum ratio combining decoder
As for the SISO-SE system, (5.79) must be positive. This in turns imposes an upper bound on the maximal allowed number of eavesdropper's antennas $N_{E,\max}$ to be able to guarantee a given targeted ESR. That is, if $N_E < N_{E,\max}$, Alice can determine a finite Bob's SNR that is needed to target the desired ESR. If $N_E = N_{E,\max}$, Bob's SNR needs to be infinite to guarantee Δ bit/channel use of ESR. To find the upper bound on N_E, the condition $T_2^{\mathrm{MRC}} < 0$ needs to be met, leading to:

$$N_{E,\max} = \left\lfloor \frac{U(U+1)(1-\sigma) - (U+2)2^{\Delta U}\sigma}{(U+1)^2 2^{\Delta U}\sigma} \right\rfloor^+, \tag{5.80}$$

where $\lfloor x \rfloor^+$ is the maximum between 0 and the nearest integer lower or equal to x. From (5.80), if Alice perfectly estimates Bob's CSI, $N_{E,\max} \to +\infty$, whatever the value of the targeted ESR. That is, a positive ESR can be guaranteed if Alice perfectly estimates Bob's CSI, whatever the number of Eve's antennas. In addition, if $\sigma \neq 0$, equation (5.80) proves that it is not possible to ensure an arbitrarily large ESR. In fact, in that situation, $N_{E,\max} = 0$, which is not relevant. This behaviour can be observed in Figure 5.21, where the maximal number of Eve's antennas is plotted as a function of the maximal ESR that can be targeted, for different BORs. Between each sub-figure, the main CSI error changes.

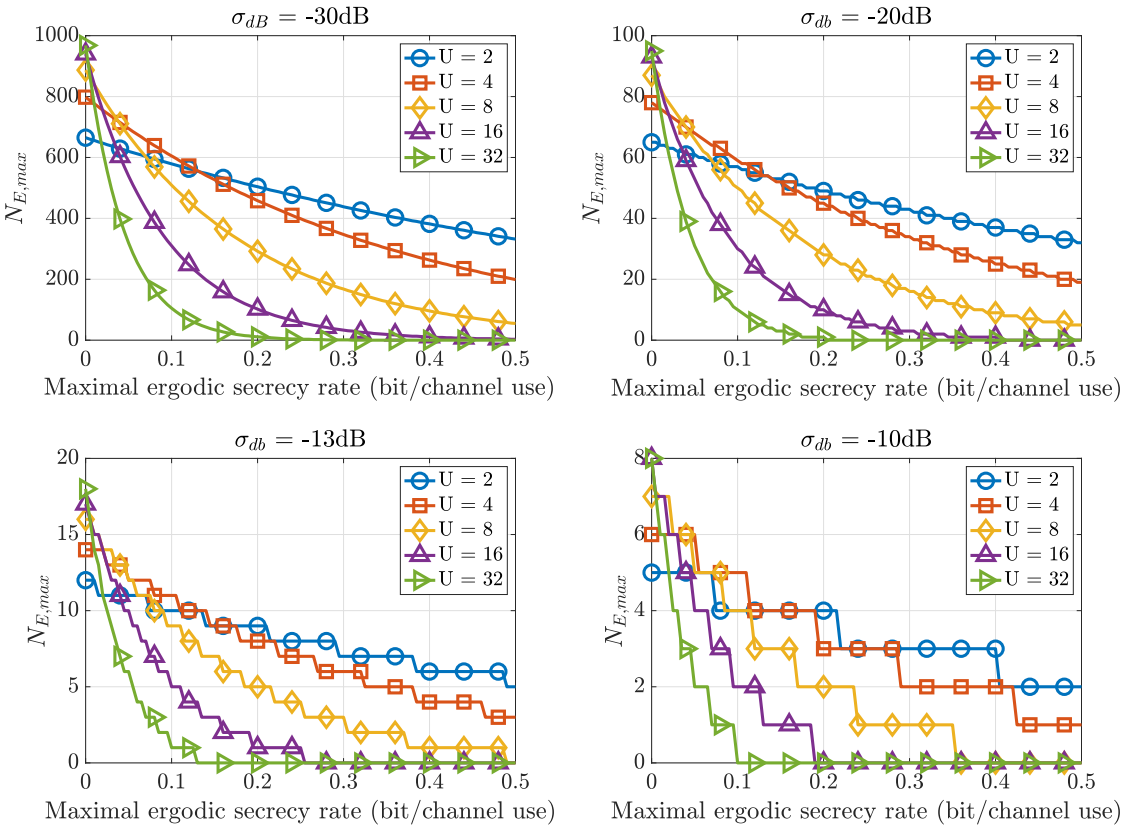

Figure 5.21: Maximal number of eavesdropping antennas as a function of the guaranteed ESR Δ, MRC decoder

From Figure 5.21, it is observed that the maximal number of Eve's antennas decreases with a decrease of Alice's accuracy on Bob's CSI estimation. Relatively low number of antennas are sufficient for Eve to jeopardize the secure communication if Alice strongly misestimates Bob's CSI. Indeed, if $U = 2$ and $\sigma_{\text{dB}} = -10$dB, i.e., Alice estimates Bob's CSI with 10% of error, Eve needs only 2 antennas to set a maximal bound on the ESR to 0.5 bit/channel use. However, if $\sigma_{\text{dB}} = -30$dB, i.e., 0.1% of estimation error on Bob's CSI, $N_{E,\max} = 332$ antennas. In addition, except at low ESRs, more antennas are required at Eve for lower BOR values. It also highlights that, except at low targeted ESRs, lower BOR values makes eavesdropping more difficult for a given targeted ESR since Eve needs more antennas (larger $N_{E,\max}$). An illustration of the robustness of the investigated PLS scheme to the number of antennas at Eve is shown in Figure 5.22. The maximal number of eavesdropping antennas is plotted as a function of the main CSI estimation error, for different diversity gains, and when Alice aims to ensure 0.2 bit/channel use of secrecy. It is observed that the PLS scheme is very sensible to Alice's accuracy on Bob's estimated CSI. For instance, when $U = 2$ and $\sigma_{\text{dB}} = -20$dB, i.e., 1% of CSI error, $N_{E,\max} = 49$ antennas. When Alice misestimates Bob's CSI with 2% or error, i.e., $\sigma_{\text{dB}} \approx -17$dB, and with $U = 2$, the maximal number of Eve's antennas drops to only 24.

5.4.3.3 Maximal CSI error allowed

Scenario 1: same decoding structure decoder
The maximum CSI estimation error at Alice is identical to the single-antenna eavesdropping scenario. That is, the condition is determined in (5.47).

Scenario procedure 2: own channel decoder
The maximum CSI estimation error at Alice is identical to the single-antenna eavesdropping scenario. That is, the condition is determined in (5.48).

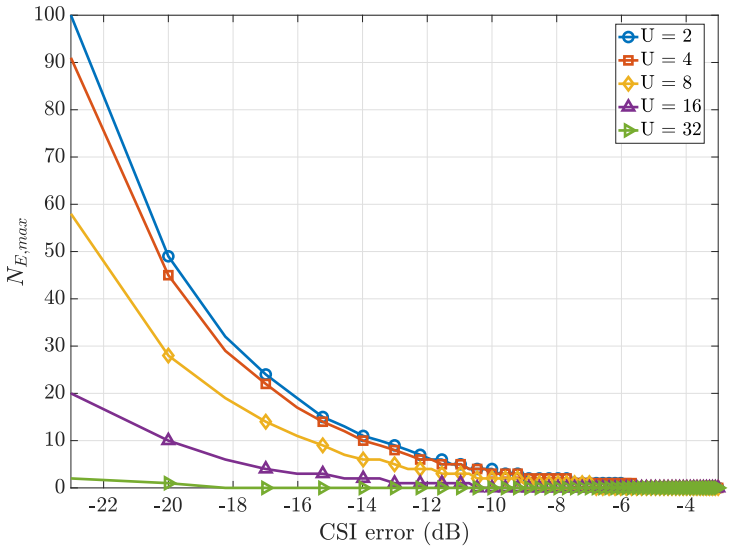

Figure 5.22: Maximal number of eavesdropping antennas as a function of the CSI estimation's error, $\Delta = 0.2$ bit/channel use, MRC decoder

Scenario 3: maximum ratio combining decoder

To be able to determine the maximal communication ESR that can be guaranteed, one can isolate σ in equation in (5.80). This in turns imposes a condition on the maximal CSI error $\sigma_{\max}^{\text{MRC}}$ that Alice is allowed to perform to ensure a maximal ESR $=\Delta$, as a function of U and N_E. In other words, if Alice aims to communicate at a maximal ESR$=\Delta$, with $\sigma < \sigma_{\max}^{\text{MRC}}$ and $N_E < N_{E,\max)}$, a finite SNR at Bob can be determined to be able to reach the desired rate. From (5.80), it comes:

$$\sigma_{\max}^{\text{MRC}} = 1 - \frac{2^{\Delta U}\left[N_E U^2 + N_E + 2 + U(1+2N_E)\right]}{2^{\Delta U}\left[N_E U^2 + N_E + 2U(1+2N_E)\right] + U(U+1)}\Bigg|_{N_E \leq N_{E,\max},\, \sigma_{\max}^{\text{MRC}} \in [0,1]}. \tag{5.81}$$

Setting $N_E = 1$ in (5.81), one comes back to the SISO-SE condition (5.49). As expected, (5.81) decreases when N_E increases, i.e., Alice must more accurately estimate Bob's CSI when Eve is equipped with a larger number of antennas. As for the single-antenna scenario, there is a condition on $\sigma_{\max}^{\text{MRC}}$ when $\Delta \to 0^+$, i.e., a positive ESR can be ensured subject to a condition on Alice's CSI estimation accuracy. In a multi-antenna eavesdropper scenario, the condition now depends on Eve's number of antennas. Indeed, if a argeted ESR of $\Delta \to 0^+$ is to be ensured, it comes:

$$\sigma_{\max}^{\text{MRC}}\Big|_{\Delta \to 0^+} = \frac{U(U+1)}{N_E U^2 + N_E + 2 + U(1+2N_E) + U(U+1)}. \tag{5.82}$$

Expression (5.82) is shown in Figure 5.23. It is seen from Figure 5.23 that higher CSI estimation errors are allowed with an increase of the spreading factor when $\Delta \to 0^+$. More, Alice must be more precise on Bob's CSI estimation, if Eve's number of antennas increases, which is expected. In addition, from equation (5.81), if $\Delta \to +\infty$, $\sigma_{\max}^{\text{MRC}} \to 0$, i.e., Alice needs to perfectly estimate Bob's CSI if she aims to ensure an arbitrarily large communication ESR. This behaviour is expected, and condition (5.81) is depicted in Figure 5.24.

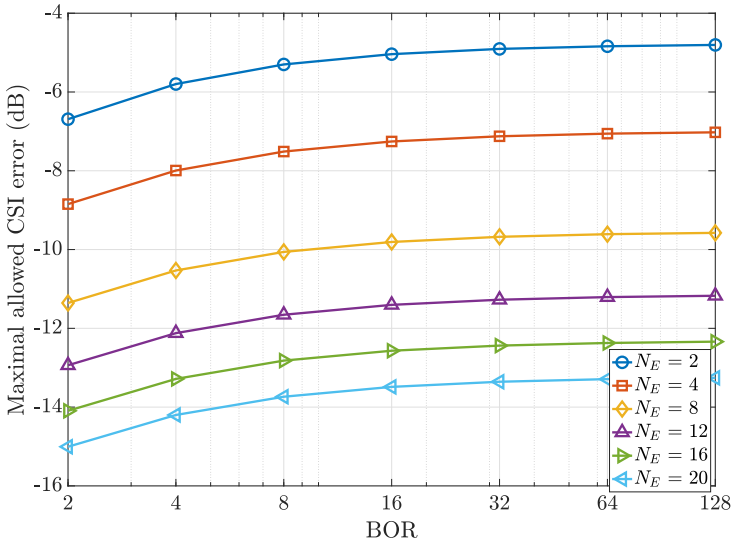

Figure 5.23: Maximal allowed CSI error to ensure a positive ESR $\Delta \to 0^+$ bit/channel use, MRC decoder

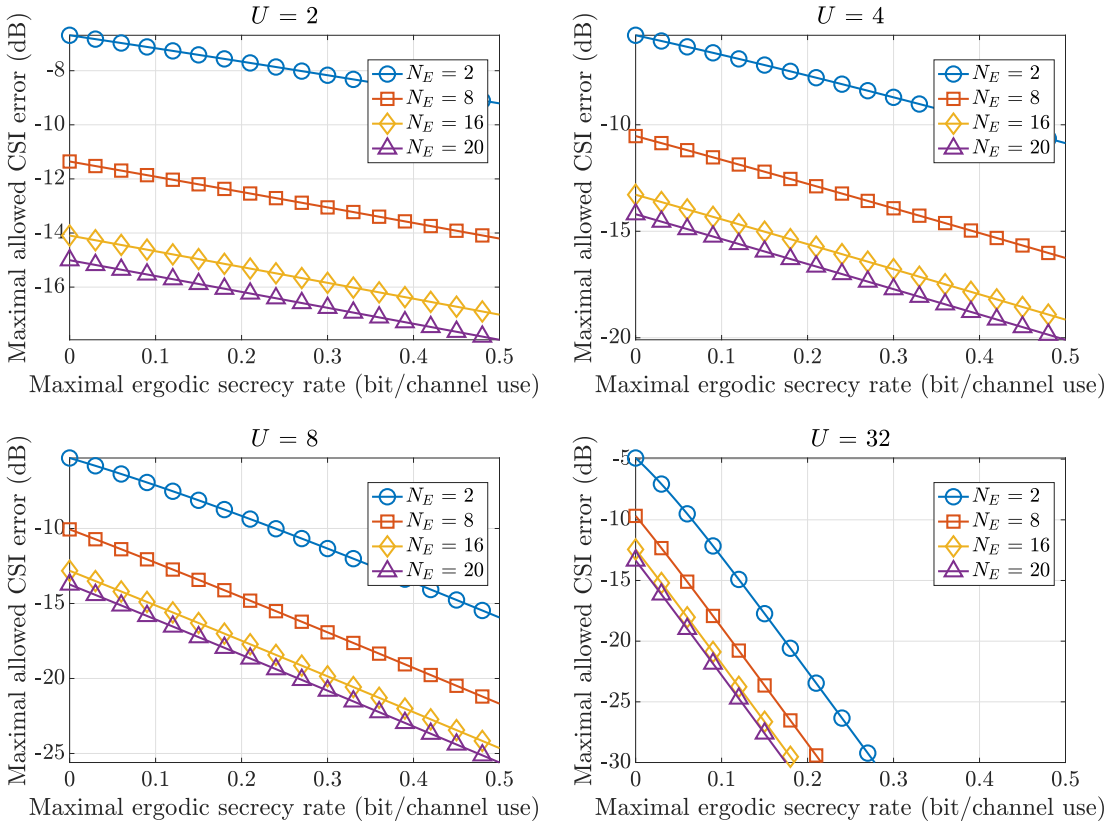

Figure 5.24: Maximal allowed CSI error as a function of the targeted ESR, MRC decoder

Between each sub-figure, the BOR changes. It is first observed that, lower BOR values are preferable to achieve higher targeted ESRs. Indeed, at low BORs, Alice is allowed to less precisely estimate Bob's CSI, at fixed N_E. As an example, when $U = 2$, Alice is allowed to misestimate Bob's CSI with an error up to ≈ -16dB, i.e., $\approx 2.5\%$ of error, when $\Delta = 0.2$ bit/channel use, if $N_E = 20$. With $U = 32$, for the same set of parameters, the maximal CSI error is ≈ -32dB, i.e., $\approx 0.08\%$ of error. In addition, as it is expected, Alice must more accurately estimate Bob's CSI to target a given ESR, if Eve is equipped

with an increase number of antennas.

5.4.3.4 Optimal amount of data energy to inject

Scenario 1: same decoding structure decoder The optimal amount of data to inject is identical to the SDS SISO-SE scenario, and is found in (5.51).

Scenario 2: own channel decoder
The optimal amount of data to inject is identical to the OC SISO-SE scenario, and is found in (5.52).

Scenario 3: maximum ratio combining decoder
In order to obtain the optimal amount of data energy to inject, one needs to find the roots of the derivative of (5.79) as a function of α. In doing so, the amount of AN determined corresponds to the one that minimizes the required SNR at Bob in order to guarantee ESR=Δ. By denoting:

$$\begin{aligned}
A_1^{\mathrm{MRC}} =& \left[2^{\Delta U}\left(N_E(U+1)^2+(U+2)\right)+U\right]\left[2^{\Delta U}\sigma\left(N_E(U+1)^2+(U+2)\right)-U(U+1)(1-\sigma)\right]\\
A_2^{\mathrm{MRC}} =& U(2^{\Delta U}-1)\left[2^{\Delta U}\sigma\left(N_E(U+1)^2+(U+2)\right)-U(U+1)(1-\sigma)\right]\\
A_3^{\mathrm{MRC}} =& U\sigma(1-2^{\Delta U})\left[2^{\Delta U}\left(N_E(U+1)^2+(U+2)\right)+U\right]\\
&+U(1-2^{\Delta U})\left[U(U+1)(1-\sigma)-U\sigma-2^{\Delta U}\sigma\left(N_E(U+1)^2+2\right)\right]
\end{aligned}$$

one can show that:

$$\alpha_{\mathrm{opt}}^{\mathrm{MRC}} = -\frac{A_2^{\mathrm{MRC}}+\sqrt{\left(A_2^{\mathrm{MRC}}\right)^2+A_1^{\mathrm{MRC}}A_3^{\mathrm{MRC}}}}{A_1^{\mathrm{MRC}}}\Bigg|_{\sigma\leq\sigma_{\max}^{\mathrm{MRC}},\, N_E\leq N_{E,\max},\, \alpha_{\mathrm{opt}}^{\mathrm{MRC}}\in[0,1]}. \tag{5.83}$$

Equation (5.83) determines the optimal amount of data that Alice has to inject when Eve performs an MRC decoder. It minimizes the required SNR at Bob that guarantees a per-symbol communication ESR= Δ bit/channel use, as a function of the BOR U, the main CSI estimation error made at Alice σ, the number of eavesdropping antennas. To obtain the corresponding SNR values, the parameter α in (5.79) is replaced with the values obtain in equation (5.83).

From Figure 5.25, one can state that, increasing the number of eavesdropper's antennas increases the required SNR at Bob to target a given ESR. Indeed, if $\sigma_{\mathrm{dB}} = -20$dB, i.e., 1% of CSI error, with $U = 8$ for instance, $\delta_{\mathrm{B}}^{\mathrm{MF}} = 9.2$dB is required to target 0.15 bit/channel use with $N_E = 2$. When Eve is equipped with $N_E = 20$ antennas, $\delta_{\mathrm{B}}^{\mathrm{MF}} = 21.13$dB is needed. Also, when the BOR decreases, the required SNR at Bob decreases as well to target a given ESR at fixed N_E. As an example, with $N_E = 6$ and $\sigma_{\mathrm{dB}} = -23$dB, i.e. $\approx 0.5\%$ of CSI error, $\delta_{\mathrm{B}}^{\mathrm{MF}} = 33.1$dB for $U = 32$, $\delta_{\mathrm{B}}^{\mathrm{MF}} = 13.27$dB for $U = 8$, $\delta_{\mathrm{B}}^{\mathrm{MF}} = 11.92$dB for $U = 4$, and $\delta_{\mathrm{B}}^{\mathrm{MF}} = 11.56$dB for $U = 2$. Also, when σ_{dB} increases, $\delta_{\mathrm{B}}^{\mathrm{MF}}$ increases as well, i.e., the required SNR at Bob increases when Alice estimates Bob's CSI with larger errors. Furthermore, when σ_{dB} increases, it becomes impossible to ensure 0.15 bit/channel of ESR when the BOR increases. For instance, when $U = 32$, it is impossible to ensure 0.15 bit/channel use if Eve is a multi-antenna eavesdropper and $\sigma_{\mathrm{dB}} = -13$dB, i.e., Alice misestimates Bob's CSI with $\approx 5\%$ of error. Finally, for a given number of eavesdropper antennas and a given BOR value, $\delta_{\mathrm{B}}^{\mathrm{MF}}$ increases when σ_{dB} increases. As an example, for $N_E = 8$ antennas and $U = 4$, $\delta_{\mathrm{B}}^{\mathrm{MRC}} = 12.69$dB for the noise-free scenario, $\delta_{\mathrm{B}}^{\mathrm{MRC}} = 13.01$dB when 0.5% of error is made on Bob's CSI estimation, $\delta_{\mathrm{B}}^{\mathrm{MRC}} = 13.54$dB when 1% of error is made on Bob's CSI estimation, and $\delta_{\mathrm{B}}^{\mathrm{MRC}} = 26.49$dB when 5% of error is made on Bob's CSI estimation.

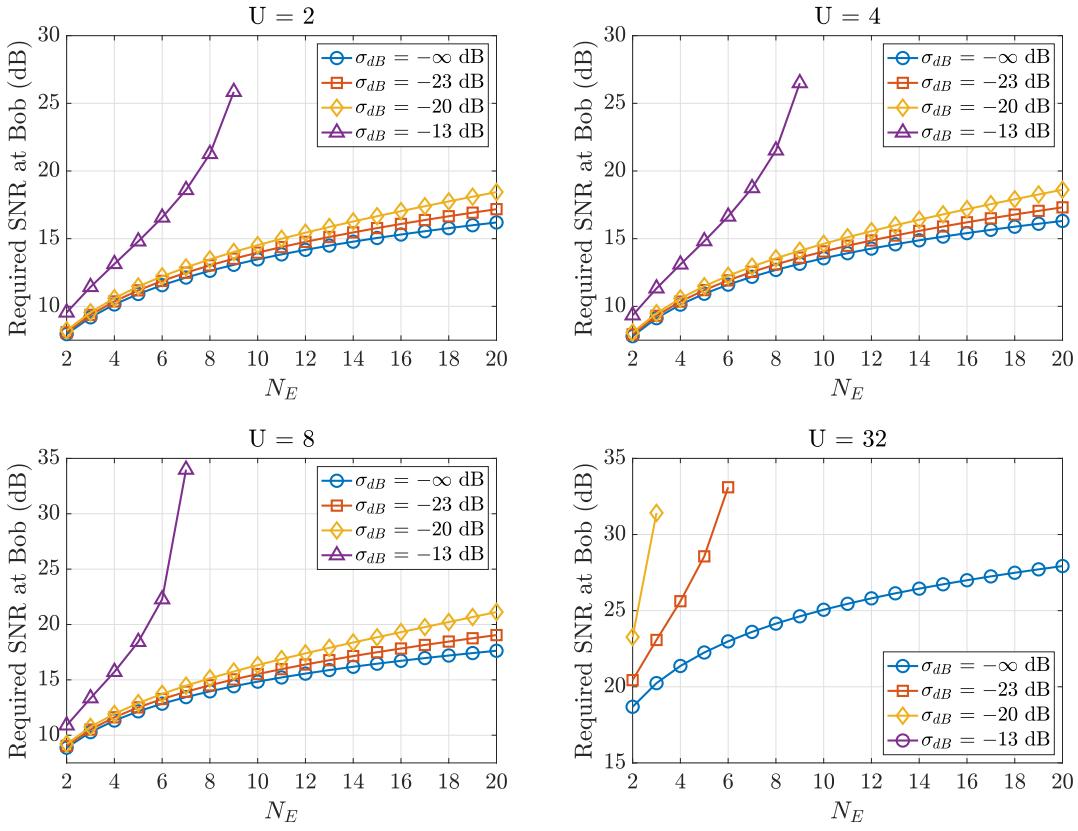

Figure 5.25: Required SNR at Bob as a function of N_E, $\Delta = 0.15$ bit/channel use, optimal amount of AN injected, MRC decoder

From the discussions in section 5.4.3, one can state that relatively poor secrecy performances can be provided in a SISO-ME system if Eve implements an MRC decoder. The reason is that worst case assumptions in terms of secrecy are considered for Eve. Indeed, it is assumed that Eve has a noise-free hardware, that a multiple colluding eavesdropper scenario is studied, and that Eve can perfectly estimate the amount of CSI she eavesdrops from the handshake procedure between Alice and Bob. Although these assumptions are not realistic, these parameters cannot be known by Alice who cannot do better but to assume the worst if she wants to securely communicate with a given ESR. Finally, when Eve implements an MRC decoder, her ESINR is proportional to the number of antennas she is equipped with. From that, little can be done against multiple colluding eavesdroppers. Regarding Alice, she does not perfectly estimates Bob's CSI. Consequently, she precodes the data with an estimate of Bob's CSI, which does not allow Bob to fully benefit from frequency diversity inherent from the FD TR PLS scheme. Furthermore, due to the wrong estimate, some AN energy leaks at Bob after decoding.

5.4.4 Secrecy outage consideration

As for the SISO-SE system, outage considerations are investigated via the ϵ-achievable SR in this section. It takes into account that outages occur if the instantaneous secrecy rate that can be supported by the communication is lower than the actual ESR at which Bob and Alice communicate, resulting to leakage to Eve. In order to observe low outage percentages, 100.000 realizations of the instantaneous SR are conducted for the three investigated scenarios. Eve is also considered as noiseless.

Scenarios 1: SDS decoder

Figure 5.26 presents the ϵ-achievable SR as a function of the fraction of outage, for different number of Eve's antennas, different BOR values and when Alice misestimates Bob's CSI with 30% of error. It can

be observed that the number of Eve's antennas does not influence the outage performance. In addition, the performances are identical to the single eavesdropper scenario, presented in Figure 5.12. The same conclusions as for the SISO-SE SDS scenario can therefore be drawn. That is, when Alice strongly misestimates Bob's CSI are low outage percentages are required, it is more likely to communicate at higher BOR values to maximize the outage performances.

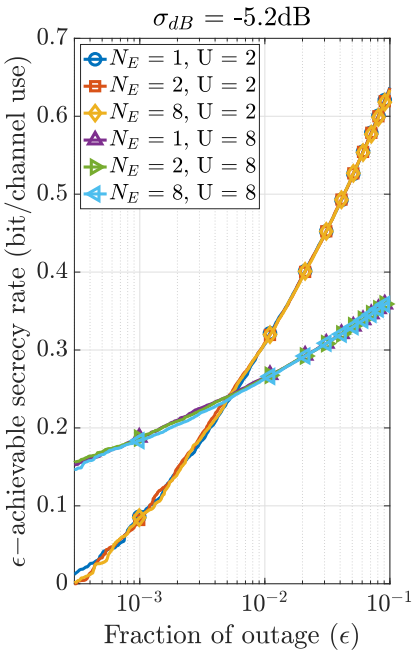

Figure 5.26: ϵ-achievable secrecy rate as a function of the fraction of outage, $\delta_B = 10$dB, SDS decoder

Scenarios 2: OC decoder

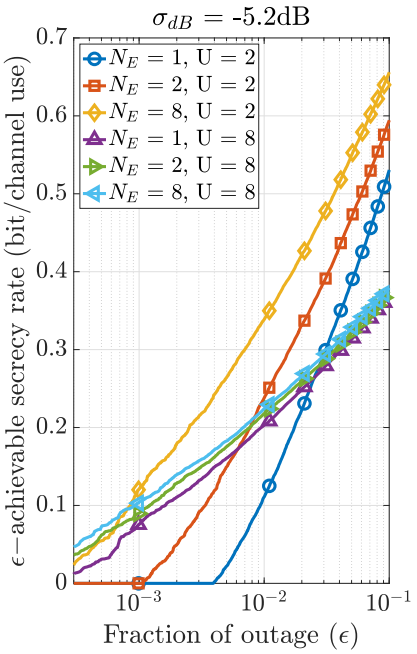

Figure 5.27: ϵ-achievable secrecy rate as a function of the fraction of outage, $\delta_B = 10$dB, OC decoder

Figure 5.27 presents the ϵ-achievable SR performances for the same set of parameters as for the SDS

scenario. It is seen that Eve's number of antennas influences the performances. In particular, when she is equipped with a larger number of antennas, the outage performances are enhanced such that it is preferable for Eve to possess less antennas when she implements a SISO-ME OC decoding structure. In addition, when Alice strongly misestimates Bob's CSI and low percentage of outages are allowed, one observes that higher BOR values are more likely to be used.

Figure 5.28 presents the 1%-achievable SR as a function of Alice's accuracy on Bob's CSI estimate, for different number of Eve's antennas. Between each sub-figure, the BOR factor changes. It can be observed that lower BORs are preferable to enhance the outage performances when the accuracy on the CSI estimation increases.

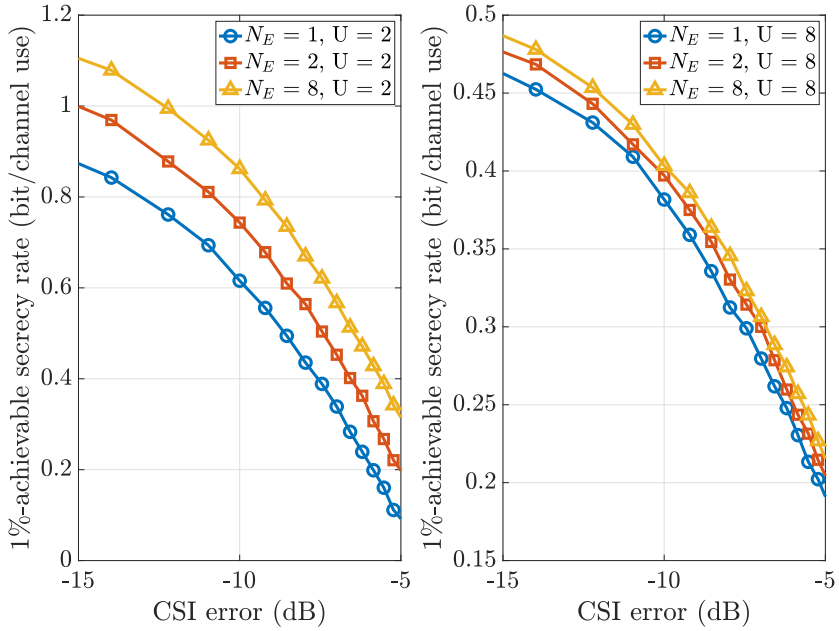

Figure 5.28: 1%-achievable secrecy rate as a function of the main CSI error, $\delta_B = 10$dB, OC decoder

The same conclusions as for the corresponding single-antenna eavesdropper scenario can be drawn regarding the trade-off on Alice's choice of the communication BOR.

Scenario 3: maximum ratio combining decoder

From section 5.4.3, it was seen that higher BORs are preferable to maximize the ESR when N_E increases. In addition, when Alice estimation error increases, higher BORs must also be used. However, if Alice estimates well Bob's CSI, it is more likely to use lower BORs to increase the ESR.

Figure 5.29 presents the $\epsilon-$achievable secrecy rate as a function of the fraction of outage, for different number of eavesdropping antennas and when Alice perfectly estimates Bob's. Between each sub-figure, the BOR factor changes. First, it is observed that it is more likely to communicate at higher BORs if one wants to constraint the leakage to Eve. Indeed, when $U = 2$, it is impossible to obtain non-null $\epsilon-$achievable SR as soon as less than 3% of outage occurs, whatever the number of eavesdropping antennas. On the opposite, if $U = 8$, a non-null $\epsilon-$achievable secrecy rate is attained for only 0.13% of outage, when $N_E = 1$. In addition, it is seen than lower $\epsilon-$achievable SRs are obtained if Eve is equipped with a larger number of antennas. This behaviour is expected since in that situations, Eve exhibits more decoding capabilities, leading to worse secrecy performances.

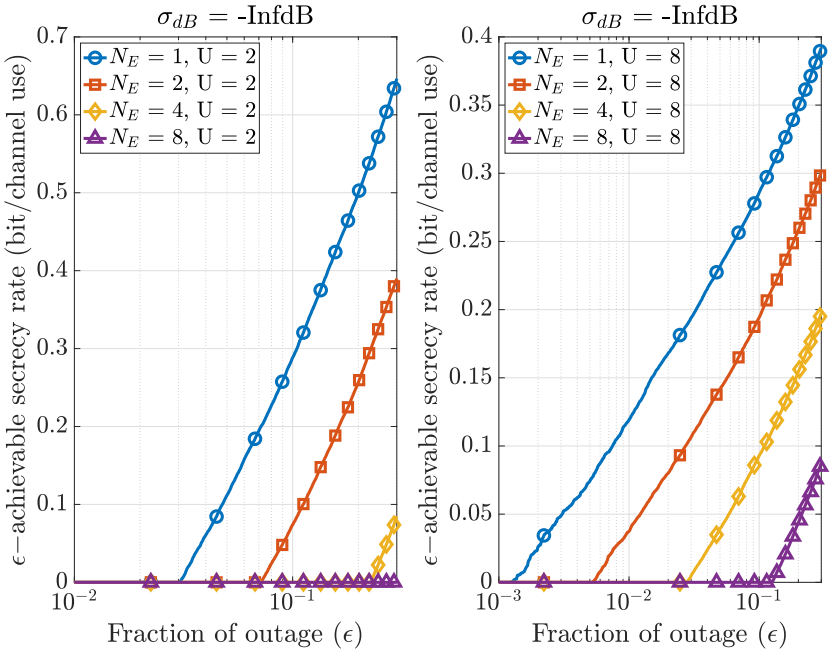

Figure 5.29: ϵ-achievable secrecy rate as a function of the fraction of outage, δ_B = 10dB, MRC decoder

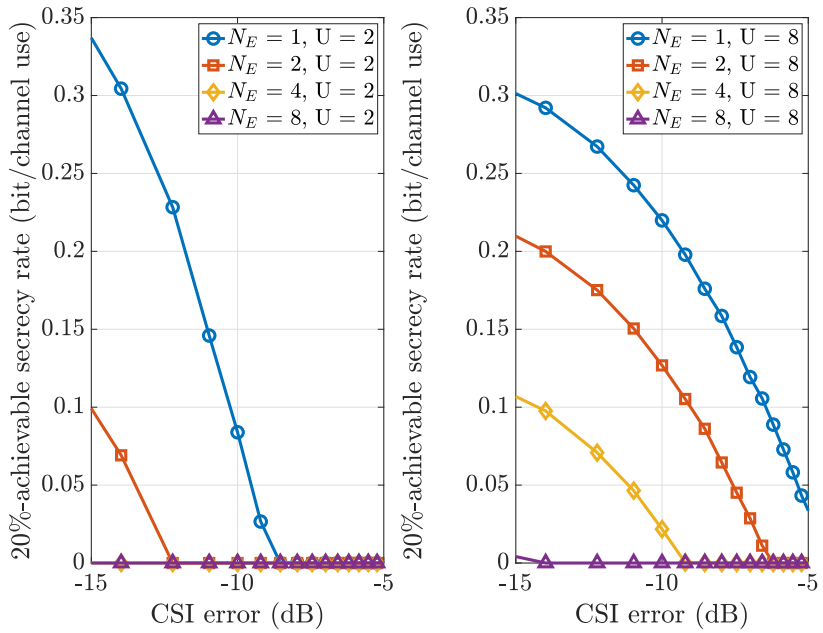

Figure 5.30: 20%-achievable secrecy rate as a function of the main CSI error, δ_B = 10dB, MRC decoder

The 20%$-$achievable secrecy rate as a function of the main CSI estimation error, for different number of Eve's antennas is presented in Figure 5.30. The BOR value is made variable between each sub-figure. As explained, low BOR values are preferred when Bob's CSI estimation error is low, and when Eve is equipped with a relatively low number of antennas. However, increasing the BOR allows to obtain positive 20%-achievable SRs for higher CSI estimation errors and larger number of eavesdropping antennas.

5.5 Conclusions

This chapter highlights the secrecy performances of the single-antenna system, in the presence of one or multiple cooperative and passive eavesdroppers.

FDD scenarios : Main results
Considering the FDD scenarios, the ESR performances of the AN killer and the LMMSE decoders are assessed via simulations and for a noisy eavesdropper. It is shown that these two decoding structures considerably outperform the linear TDD decoders and lead to poor secrecy performances. These schemes therefore jeopardize any attempt for Alice to guarantee a secure communication with Bob, even if Eve is equipped with only one antenna. No further study of the secrecy performances of the FDD schemes are consequently conducted in the rest of this manuscript.

TDD scenarios : Analytic derivation methodology
Six scenarios are presented depending on the TDD handshake procedures between Alice and Bob, and on whether Eve possesses one or more antennas. For each scenario, an approximation of the ergodic secrecy rate is derived. It is shown that the approximations fit well the exact ergodic secrecy rate performances obtained via simulations, and are therefore used as closed-form expressions throughout this chapter to derive a certain number of useful metrics.
The communication parameters are designed in order to **guarantee a targeted per-symbol ESR**. To do so, worst case assumptions in terms of secrecy are considered, such has Eve being equipped with a noise-free hardware and/or is situated close to Alice, i.e., Eve having an arbitrarily large SNR, or Eve being equipped with an arbitrarily large number of antennas.
The analytic model of the ESR, depending on the investigated scenario, allows Alice to determine an analytic expression of the required SNR at Bob to guarantee Δ bit per channel use of secure rate. Thanks to this expression, Alice is able to derive:

- the maximal allowed main CSI error she can perform,
- the maximal number of allowed eavesdropping antennas,
- the optimal amount of data energy to inject.

TDD scenarios : Main results
For each scenario, it is seen that Alice's choice on the BOR of the communication results from a **trade-off**. Knowing the CSI error variance and Bob's SNR, Alice can choose a BOR value either to maximize the ESR (by decreasing the BOR value), i.e., higher data rate transmission, or to ensure a communication with low outage percentages (by increasing the BOR value), i.e., less data leakage to Eve[1].
When the handshake procedure between Alice and Bob allows Eve to implement an SDS or an OC decoder, i.e., handshake procedures 1 or 2 (see sections 4.6.3.1 and 4.6.3.2 respectively), this trade-off arises when low percentages of outage are targeted (less than 0.1% of outage) and/or when Alice strongly misestimates Bob's CSI. When she better estimates Bob's CSI, it arises for even lower outage percentages (several orders lower), such that it is difficult to observe via simulations.
When the handshake procedure between Alice and Bob allows Eve to implement an MRC decoder, i.e., handshake procedure 3 (see section 4.6.3.3), this trade-off occurs for larger percentages of outage (typically more than 1%) and when Alice more accurately estimates Bob's CSI.

In addition, the analytic derivations prove that, when an SDS or an OC decoder is implemented, Eve's decoding capabilities, and so the secrecy performances, do not depend on the number of antennas she is equipped with. This outcome is of particular interest. Indeed, in the context of IoT, secure

[1] Alice can be a-priori aware of the variance of the error she performs when estimating Bob's CSI since it is related on her SNR and her channel estimator.

node-to-node communications can therefore be achieved by designing a communication using handshake procedures 1 & 2, regardless of the number of Eve's antennas. It makes these scenarios robust against passive eavesdropping.
However, when Eve is able to implement an MRC decoder, no secrecy can be guaranteed by Alice since the secrecy performance strongly decreases when Eve's number of antenna increases.

Table 5.2 summarizes the performances of the SISO system.

Table 5.2: SISO system: secrecy performance summary

	SISO-SE SDS	**SISO-SE OC**	**SISO-SE MF**	**SISO-ME SDS**	**SISO-ME OC**	**SISO-ME MRC**
Guaranteed ESR expression	Equation (5.41), Fig. 5.5.	Equation (5.43), Fig 5.5.	Equation (5.45), Fig. 5.6.	Identical to the SISO-SE SDS scenario.	Identical to the SISO-SE OC scenario.	Equation (5.78), Fig. 5.19 and 5.20.
Impact of imperfect CSI estimation	Equation (5.47), Fig. 5.7. Perfect estimation needed if an arbitrarily large ESR is to be targeted. Always possible to guarantee a positive ESR.	Identical to the SISO-SE SDS scenario.	Equation (5.49), Fig. 5.9. Perfect estimation needed if an arbitrarily large ESR is to be targeted. Not always possible to ensure a positive ESR, condition in (5.50), Fig. 5.8.	Identical to the SISO-SE SDS scenario.	Identical to the SISO-SE SDS scenario.	Equation (5.81), Fig. 5.24. Perfect estimation needed if an arbitrarily large ESR is to be targeted. Not always possible to ensure a positive ESR, condition in (5.82), Fig. 5.23.
Condition on maximal N_E	/	/	/	No condition since identical to the SISO-SE SDS scenario.	No condition since identical to the SISO-SE SDS scenario.	Equation (5.80), Fig. 5.21 and 5.22. Strongly depends on Alice's CSI estimation accuracy.
Required SNR at Bob	Equation (5.42), Fig. 5.10. Higher required SNR if σ_{dB} increases.	Identical to the SISO-SE SDS scenario.	Equation (5.46), Fig 5.11. Higher required SNR if σ_{dB} increases.	Identical to the SISO-SE SDS scenario.	Identical to the SISO-SE SDS scenario.	Equation (5.79), Fig. 5.25. Higher required SNR if N_E or σ_{dB} increases.
Outage consideration	Fig. 5.12. Higher BORs are desired when lower outage percentages are required ($\approx 0.1\%$) to maximize the $\epsilon-$achievable SR, at high σ. This trade-off is also expected for very low outage percentages (several order lower than 0.1%) at lower σ.	Figure 5.13. Same conclusions as for the SISO-SE SDS scenario. However, lower outage performances are observed compared to the SISO-SE SDS scenario	Fig. 5.14. Higher BORs are desired to keep positive $\epsilon-$achievable SR when σ increases.	Figure 5.26. The same conclusions as for the SISO-SE SDS scenario can be drawn.	Figure 5.28. The number of Eve's antennas impacts the performances. Lower number of antennas leads to lower outage performances. The same conclusions as for the SISO-SE OC scenario can be drawn.	Fig. 5.29 and 5.30. If Eve is equipped with a large number of antennas, she is more likely to communicate at higher BORs to keep positive $\epsilon-$achievable SRs.
Performance summary	Highest ESR values since very poor decoding performance at Eve. Eve does not benefit from frequency diversity. Lower BORs enhance the ESR. However, higher BOR values enhances the outage performances when low outage percentages are allowed. From that, a trade-off on the BOR design exists.	Same ESR performances but lower outage performances are obtained compared to the SISO-SE SDS scenario. The same conclusions regarding the trade-off on Alice's choice of the BOR can be drawn compared to the SISO-SE SDS scenario.	Low ESR values since matched filtering at Eve, leading to a frequency diversity gain. SINR about U times bigger compared to the SISO-SE SDS/OC scenarios. The choice on the BOR value results from a trade-off. Alice can choose a BOR value either to maximize the ESR by decreasing the BOR value, or to ensure a given $\epsilon-$achievable secrecy rate by increasing the BOR value.	Same performances (ESR and outage) compared to the SISO-SE SDS scenario. Eve's number of antennas does not influence the secrecy rate performances of the scheme since Eve's array gain is identical on all her received symbol components. It exists a trade-off on Alice choice's of the BOR.	Same ESR performances compared to the SISO-SE OC scenario. Eve's number of antennas does influence the outage performances of the scheme. Lower number of Eve's antennas result to lower outage performances. It exists a trade-off on Alice choice's of the BOR	Lowest ESR values since MRC at Eve, leading to a frequency diversity gain. SINR about $N_E U$ times bigger compared to the SISO-SE SDS/OC scenarios. Trade-off on the choice of the BOR value. If Alice well estimates Bob's CSI and Eve does not possess many antennas, low BORs are likely to be used to maximize the ESR and the $\epsilon-$achievable SR. Increasing the BOR is preferable to ensure a given $\epsilon-$achievable SR if σ_{dB} and/or N_E increase. No secrecy can be guaranteed by Alice since Eve's ESINR is proportional to N_E (see (5.75)).

6 | Multi-Antenna System

Contents

This chapter is based on the Journal Article [153] in preparation.

6.1 Introduction

Throughout this chapter, multiple antenna systems are investigated. That is, the secrecy performances of MISO (Section 6.2) and SIMO systems (Section 6.3) are assessed, in the presence of a single-antenna or multi-antenna passive eavesdroppers. The results derived in this chapter directly consider the multi-antenna eavesdropper scenario. The reader can set $N_E = 1$ in order to obtain the expressions of the corresponding single-antenna eavesdropping system.

As a reminder, depending on the handshake procedure between Alice and Bob, Eve may acquire different amount of CSI knowledge, leading to different security performances. It is considered that she can perfectly estimate the amount of CSI she obtains from the handshake. On the opposite, it is assumed that Alice is able to estimate Bob's CSI with an error, modeled by its variance σ. From that, depending on the handshake procedures in TDD systems, described in section 4.6.3, closed-form expressions of the communication ESR are derived. A data leakage consideration is also investigated for the different scenarios in MISO and SIMO systems.

6.2 Multi-Input Single-Output

6.2.1 Introduction

In this first part of the chapter, the secrecy performances of a MISO system are assessed. As a reminder, the implemented PLS technique is a channel-based adaptation technique with AN injection into Bob's estimated null space. Alice precodes the transmitted data with a FD TR precoder within an OFDM structure. She benefits from frequency diversity thanks to the spreading operation and can then inject an AN signal on top of the data signal. Due to the imperfect precoding, some AN energy leaks at Bob after decoding. Three decoding structures are considered at Eve, depending on the handshake procedures between Alice and Bob. A MISO secure communication may correspond to a secure DL communication between a BS (multi-antenna Alice) and a UE with limited capabilities (single-antenna Bob), in the presence of a single or multi-antenna eavesdropper, as depicted in Figure 4.6.

6.2.2 Assumptions

The dimensions and the natures of the matrices in a MISO system are given in Section 4.5.2. The block diagram of a MISO-ME communication is shown in Figure 4.7. To study the MISO system, several assumptions are undertaken:

- There are Q subcarriers per OFDM block, with a BOR of U, and $N = Q/U$ data symbols are transmitted per OFDM block.
- Alice possesses $N_A > 1$ antennas.
- Bob possesses $N_B = 1$ antenna.
- Eve possesses $N_E = 1$ antennas in a MISO-SE configuration, or $N_E > 1$ antenna in a MISO-ME configuration.
- No spatial correlation amongst Alice's antennas is assumed.
- No spatial correlation amongst Eve's antennas is assumed.
- No spatial correlation amongst Bob's antenna and Eve's antenna(s) is assumed.
- No frequency correlation amongst Bob's subcarriers is assumed, i.e., $h_{B,k,i} \perp\!\!\!\perp h_{B,k,j}$, $\forall k = 1...N_A$, $\forall i \neq j$, $i = 1...Q$, $j = 1...Q$.
- No frequency correlation amongst Eve's subcarriers is assumed, i.e., $h_{E,lki} \perp\!\!\!\perp h_{E,lk,j}$, $\forall l = 1...N_E$, $\forall k = 1...N_A$,$\forall i \neq j$, $i = 1...Q$, $j = 1...Q$.
- No frequency correlation amongst the estimated error's subcarriers made by Alice and Bob's subcarriers is assumed, i.e., $h_{B,k,i} \perp\!\!\!\perp \Delta h_{B,k,j}$, $\forall k = 1...N_A$, $\forall i,j = 1...Q$.
- No frequency correlation amongst the estimated error's subcarriers made by Alice is assumed, i.e., $\Delta h_{B,k,i} \perp\!\!\!\perp \Delta h_{B,k,j}$, $\forall k' = 1...N_A$, $\forall i \neq j$, $i = 1...Q$, $j = 1...Q$.

As for the SISO system, the uncorrelated frequency assumption is justify by the fact that it is possible to separate two symbol components by more than the coherence bandwidth of the channel. This is achieved thanks to the spreading operation and/or with flexible numerology in 5G modulation, for instance. From that, the BOR components of a symbol are spaced enough in frequency domain in order to experience non-correlated channels. The uncorrelated spatial assumption between Bob and Eve holds as soon as Bob and Eve are spaced by more than a few wavelengths, depending on the environment.

The communication parameters used to study the MISO system are given in Table 6.3:

Symbol	Description	Value
α	Ratio between the useful and the total signal power.	$\alpha \in [0,1]$
σ	CSI estimation error variance.	$\sigma \in [0,1]$
σ_{dB}	CSI estimation error variance in dB.	$\sigma_{\text{dB}} \in \mathbb{R}^-$
ϵ	Fraction of outage.	$\epsilon \in [0,1]$
Δ	Targeted ergodic secrecy rate in bit/channel use.	$\Delta \in \mathbb{R}^+$
Q	# of OFDM subcarriers.	$Q = 256$
U	Spreading factor.	$U = 2^n$, $n \in \{2,4,8,16,32\}$
N	# of symbols per OFDM block.	$N = Q/U$
N_A	# of antennas at Alice.	$N_A > 1$
N_B	# of antenna at Bob.	$N_B = 1$
N_E	# of antenna(s) at Eve.	$N_E \geq 1$

Table 6.1: MISO communication parameters

6.2.3 Preliminaries

The expressions of the received signals at Bob and Eve's positions, the decoding structures implemented at Eve, as well as the AN generation condition, are reminded, in this section to facilitate the reader's understanding.

Received signal expressions
From Chapter 4, in a MISO-ME situation, the received signal at Bob is given by (see equation (4.18)):

$$\begin{aligned}\mathbf{y}_{\mathbf{B}}^{\text{MISO}} =& \sqrt{\alpha(1-\sigma)}\mathbf{S}^H \sum_{k=1}^{N_A} ||\mathbf{H}_{\mathbf{B},k}||^2 \mathbf{S}\mathbf{x} + \sqrt{\alpha\sigma}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x} \\ &+ \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\mathbf{w} + \mathbf{S}^H \mathbf{v}_{\text{B}}.\end{aligned} \tag{6.1}$$

At the eavesdropper's position, the received sequence is given by:

$$\mathbf{y}_{\text{E}}^{\text{MISO},\mathbf{D}} = \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{D}_{\mathbf{E},l}\mathbf{H}_{\mathbf{E},lk}\widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{D}_{\mathbf{E},l}\mathbf{H}_{\mathbf{E},lk}\mathbf{w} + \mathbf{S}^H \sum_{l=1}^{N_E} \mathbf{D}_{\mathbf{E},l}\mathbf{v}_{\text{E},l}, \tag{6.2}$$

where $\mathbf{D}_{\mathbf{E},l}$ is a $Q \times Q$ decoding matrix whose nature depends on the investigated scenario, i.e., on the handshake procedure between Alice and Bob.

Decoding structures at Eve
Eve's decoding structures depend on the handshake procedures presented in section 4.6.3.

TDD handshake procedure 1: same decoding structure decoder.

The handshake procedure is presented in Figure 4.12. Eve is only able to know $\mathbf{H}_{\mathbf{BE}}$ which is of no help. She implements the same decoding structure as Bob:

$$\mathbf{D}_{\mathbf{E}}^{\text{SDS}} = \mathbf{S}^H \sum_{k=1}^{N_E} \mathbf{I}_Q. \tag{6.3}$$

TDD handshake procedure 2: own channel decoder.

The handshake procedure is presented in Figure 4.13. Eve implements a decoding structure that takes benefit from her own channel knowledge:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{OC}} = \mathbf{S}^H \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}^H. \tag{6.4}$$

TDD handshake procedure 3: maximum ratio combining decoder.

The handshake procedure is presented in Figure 4.14. Eve can access to the knowledge of her equivalent channel. She therefore implements an MRC decoding structure:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MRC}} = \mathbf{S}^H \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{H}_{\mathbf{E},lk}^H. \tag{6.5}$$

AN generation
In a MISO-ME configuration, the AN is generated such that:

$$\mathbf{S}^H \sum_{k=1}^{N_A} \widehat{\mathbf{H}}_{\mathbf{B},k} \mathbf{w} = \mathbf{0}_N. \tag{6.6}$$

6.2.4 Ergodic secrecy rate modeling

As for the SISO system investigated in chapter 5, the metric of interest is the ESR which is defined in (5.11). In order to obtain a model for the ESR, closed-form expressions of the ESINRs must be determined.

6.2.4.1 Bob's ergodic SINR

The approximation of Bob's ESINR is identical to the approximation defined in chapter 5:

$$\mathbb{E}\left[\gamma_B\right] = \mathbb{E}\left[\frac{|B_1|^2}{|B_2 + B_3|^2}\right], \tag{6.7}$$

with:

$$\begin{aligned} B_1 &= \sqrt{\alpha(1-\sigma)}\mathbf{S}^H \sum_{k=1}^{N_A} ||\mathbf{H}_{\mathbf{B},k}||^2 \mathbf{S}\mathbf{x} + \sqrt{\alpha\sigma}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k} \Delta\mathbf{H}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x}, \\ B_2 &= \mathbf{S}^H \mathbf{v}_{\mathrm{B}}, \\ B_3 &= \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A} \mathbf{H}_{\mathbf{B},k}\mathbf{w}, \end{aligned} \tag{6.8}$$

being respectively the data, noise, and AN components of the received signal at Bob, in a MISO system. From 6.7, an approximation of the ESINR of the n^{th} symbol is:

$$\mathbb{E}\left[\gamma_{B,n}\right] \approx \frac{\mathbb{E}\left[|B_{1,n}|^2\right]}{\mathbb{E}\left[|B_{2,n}|^2\right] + \mathbb{E}\left[|B_{3,n}|^2\right]}, \tag{6.9}$$

From (6.1), the received components at Bob are:

$$B_{1,n} = \frac{\sqrt{\alpha(1-\sigma)}}{N_A U} \sum_{k=1}^{N_A} \sum_{i=0}^{U-1} |h_{\mathrm{B},k,i}|^2 + \frac{\sqrt{\alpha\sigma}}{N_A U} \sum_{k=1}^{N_A} \sum_{i=0}^{U-1} h_{\mathrm{B},k,i} \Delta h^*_{\mathrm{B},k,i}, \tag{6.10a}$$

$$B_{2,n} = \frac{1}{\sqrt{N_A U}} \sum_{i=0}^{U-1} v_{\mathrm{B},i} \tag{6.10b}$$

$$B_{3,n} = \sqrt{\frac{1-\alpha}{N_A U}} \sum_{k=1}^{N_A} \sum_{i=0}^{U-1} h_{\mathrm{B},k,i} w_i. \tag{6.10c}$$

As detailed in Appendices D.1.1, D.1.2, and D.1.3, the components can respectively be derived as:

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \frac{\alpha\left[N_A U(1-\sigma)+1\right]}{N_A U} \tag{6.11a}$$

$$\mathbb{E}\left[|B_{2,n}|^2\right] = \frac{\sigma^2_{\mathrm{B}}}{N_A} \tag{6.11b}$$

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)\sigma}{N_A U}. \tag{6.11c}$$

Bob's noise variance is defined as:

$$\sigma^2_{\mathrm{B}} = \frac{1}{U\delta_B}, \tag{6.12}$$

where δ_B is the SNR at Bob in linear scale, and $1/U$ is the received energy per symbol component (data + AN).
Introducing (6.11a), (6.11b), and (6.11c) into (6.9), the per-symbol approximated ESINR at Bob in a MISO-ME system is given by:

$$\mathbb{E}[\gamma_{B,n}] \approx \frac{\frac{\alpha[N_A U(1-\sigma)+1]}{N_A U}}{\frac{\sigma^2_{\mathrm{B}}}{N_A} + \frac{(1-\alpha)\sigma}{N_A U}} = \frac{\alpha\left[N_A U(1-\sigma)+1\right]}{U\sigma^2_{\mathrm{B}} + (1-\alpha)\sigma}. \tag{6.13}$$

The approximated EC at Bob is therefore expressed as:

$$C_B \approx \log_2\left(1+\mathbb{E}[\gamma_{B,n}]\right) = \log_2\left(1+\frac{\alpha\left[N_A U(1-\sigma)+1\right]}{U\sigma^2_{\mathrm{B}} + (1-\alpha)\sigma}\right). \tag{6.14}$$

Figure 6.1 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_B$) with the approximated EC at Bob (C_B) given in (6.14), for different number of Alice's antennas, and at SNR $\delta_B = 10$dB. Between each sub-figure, $U = 2$ or $U = 8$, and the CSI estimation errors made at Alice change, i.e., 0% and 10% of error, respectively. The exact EC is found by Monte Carlo simulations (100.000 realizations), and is given by:

$$\widehat{C}_B = \mathbb{E}\left[\log_2\left(1+\gamma_{B,n}\right)\right]. \tag{6.15}$$

From Figure 6.1, it is first observed that the approximated EC, given in (6.14), fits perfectly the exact EC, given in (6.15). Equation (6.14) can therefore be used as a closed-form approximation for the rest of the study. Also, it is seen that the EC increases with an increase of the number of transmitter's antennas. This is expected since Bob benefits from a higher array gain when Alice's number of antennas increases, therefore leading to higher channel capacities. Indeed, he benefits from an array gain N_A, and a frequency diversity gain U, which can be observed on his ESINR expression (6.13) whose numerator is proportional to $N_A U$. Compared to the SISO ESINR (5.18), the MISO ESINR (6.13) is about N_A times higher. It can also be outlined that the capacity increases with an increase of the BOR factor.

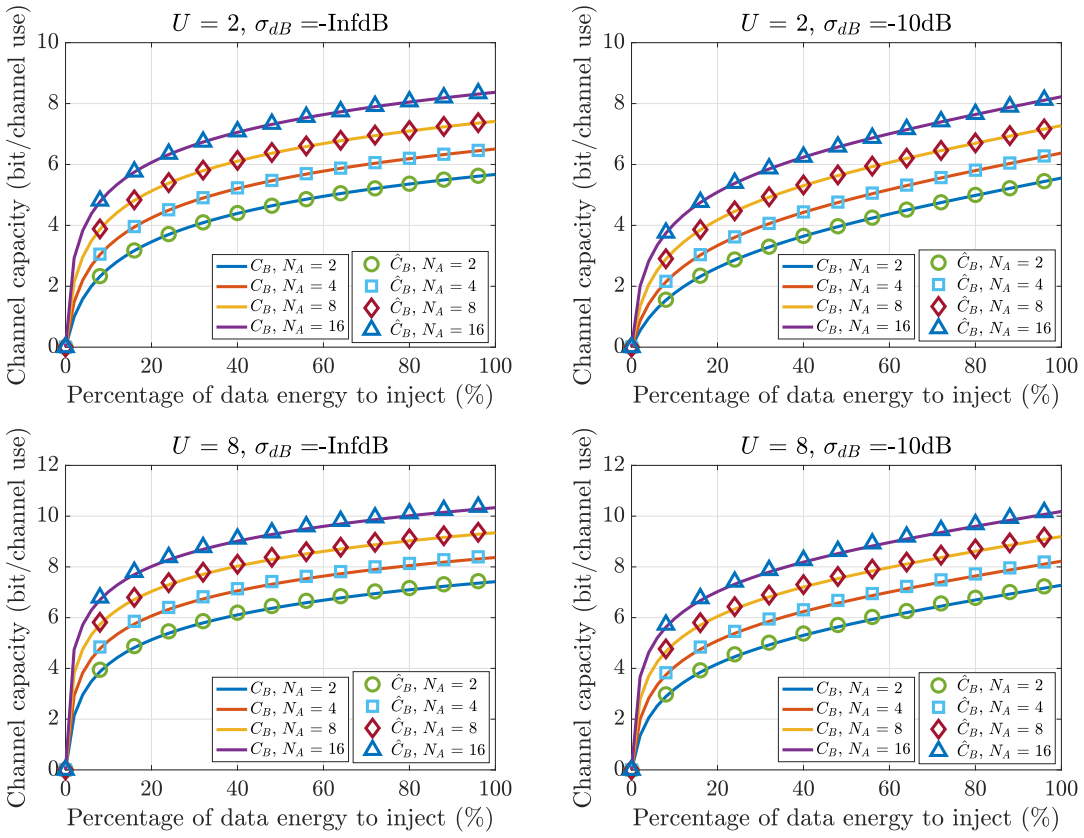

Figure 6.1: Comparison between approximated EC and exact EC at Bob, $\delta_B = 10$dB, 100.000 realizations

6.2.4.2 Eve's ergodic SINR

The derivation of Eve's ESINR is conducted in this section for the three investigated scenarios coming from the TDD handshake procedures. As for the SISO system, depending on the decoder, the ESINR is given by:

$$\mathbb{E}\left[\gamma_E^{\mathrm{D}}\right] = \mathbb{E}\left[\frac{\left|E_1^{\mathrm{D}}\right|^2}{\left|E_2^{\mathrm{D}} + E_3^{\mathrm{D}}\right|^2}\right], \tag{6.16}$$

with E_1^{D}, E_2^{D}, and E_3^{D} respectively being the data, noise, and AN components of the received signal at Eve. From 6.16, an approximation of the ESINR of the n^{th} symbol is:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{D}}\right] \approx \frac{\mathbb{E}\left[\left|E_{1,n}^{\mathrm{D}}\right|^2\right]}{\mathbb{E}\left[\left|E_{2,n}^{\mathrm{D}}\right|^2\right] + \mathbb{E}\left[\left|E_{3,n}^{\mathrm{D}}\right|^2\right]}, \tag{6.17}$$

where $E_{1,n}^{\mathrm{D}}$, $E_{2,n}^{\mathrm{D}}$, and $E_{3,n}^{\mathrm{D}}$ are respectively the data, noise, and AN (i.e., interference) n^{th} symbol components of the received signal at Eve's position, depending on the investigated scenario, when a MISO-ME system is considered.

TDD handshake procedure 1: same decoding structure decoder

When Eve implements the SDS decoder, by replacing (6.3) in (6.2), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{SDS}} = \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}\widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}\mathbf{w} + \mathbf{S}^H \sum_{l=1}^{N_E} \mathbf{v}_{\mathrm{E},l}. \tag{6.18}$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\text{SDS}} = \frac{\sqrt{\alpha}}{N_A U} \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \sum_{i=0}^{U-1} h_{\text{E},kl,i} \hat{h}_{\text{B},k,i}^{*} \tag{6.19a}$$

$$E_{2,n}^{\text{SDS}} = \frac{1}{\sqrt{N_A U}} \sum_{l=1}^{N_E} \sum_{i=0}^{U-1} v_{\text{E},l,i} \tag{6.19b}$$

$$E_{3,n}^{\text{SDS}} = \frac{\sqrt{1-\alpha}}{\sqrt{N_A U}} \sum_{k=1}^{N_A} \sum_{l=1}^{N_E} \sum_{i=0}^{U-1} h_{\text{E},kl,i} w_i. \tag{6.19c}$$

As detailed in D.2.1.1, D.2.1.2, and D.2.1.3, the expected energy of the components are respectively given by:

$$\mathbb{E}\left[|E_{1,n}^{\text{SDS}}|^2\right] = \frac{\alpha N_E}{U N_A} \tag{6.20a}$$

$$\mathbb{E}\left[|E_{2,n}^{\text{SDS}}|^2\right] = \frac{N_E}{N_A} \sigma_{\text{E}}^2 \tag{6.20b}$$

$$\mathbb{E}\left[|E_{3,n}^{\text{SDS}}|^2\right] = \frac{(1-\alpha) N_E}{U N_A}. \tag{6.20c}$$

Eve's noise variance is defined as:

$$\sigma_{\text{E}}^2 = \frac{1}{U \delta_E}, \tag{6.21}$$

where δ_E is the SNR at Eve in linear scale, and $1/U$ is the received energy per symbol component. Introducing (6.20a), (6.20b), and (6.20c) into (6.17), the per-symbol approximated ESINR at Eve is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\text{SDS}}\right] \approx \frac{\frac{\alpha N_E}{U N_A}}{\frac{N_E}{N_A}\sigma_{\text{E}}^2 + \frac{(1-\alpha) N_E}{N_A U}} = \frac{\alpha}{U\sigma_{\text{E}}^2 + (1-\alpha)}. \tag{6.22}$$

Result (6.22) is very interesting. In particular, it shows that, when Eve implements an SDS decoder in a MISO-ME configuration, the ESINR does not depend on N_E nor N_A. Therefore, (6.22) is similar to the corresponding SISO-SE ESINR expression (5.27). In a MISO-ME SDS scenario, Eve benefits from a gain N_E/N_A which identically impacts each of her received signal components. Consequently, this gain simplifies and one comes back to the SISO-SE situation. In addition, it is observed that Eve is not impacted by Alice's error on Bob's CSI estimation.
The approximated EC at Eve, when a SDS decoder is implemented, is therefore expressed as:

$$C_E^{\text{SDS}} \approx \log_2\left(1 + \mathbb{E}\left[\gamma_{E,n}^{\text{SDS}}\right]\right) = \log_2\left(1 + \frac{\alpha}{U\sigma_{\text{E}}^2 + (1-\alpha)}\right) \tag{6.23}$$

Figure 6.2 shows the accuracy of the EC approximation, by comparing the exact EC ($\widehat{C}_E^{\text{SDS}}$) obtained by Monte Carlo simulations (100.000 realizations), with the approximated EC at Eve (C_E^{SDS}) given in (6.23), as a function of the energy dedicated for information data. In each sub-figure, different number of Eve's antennas are considered. Between each-subplot, the number of antennas at Alice and/or the main CSI estimation error are made variable. It is assumed a spreading factor of $U = 2$, and $\delta_E = 10$dB. The exact EC is found as:

$$\widehat{C}_E^{\text{SDS}} = \mathbb{E}\left[\log_2\left(1 + \gamma_{E,n}^{\text{SDS}}\right)\right] \tag{6.24}$$

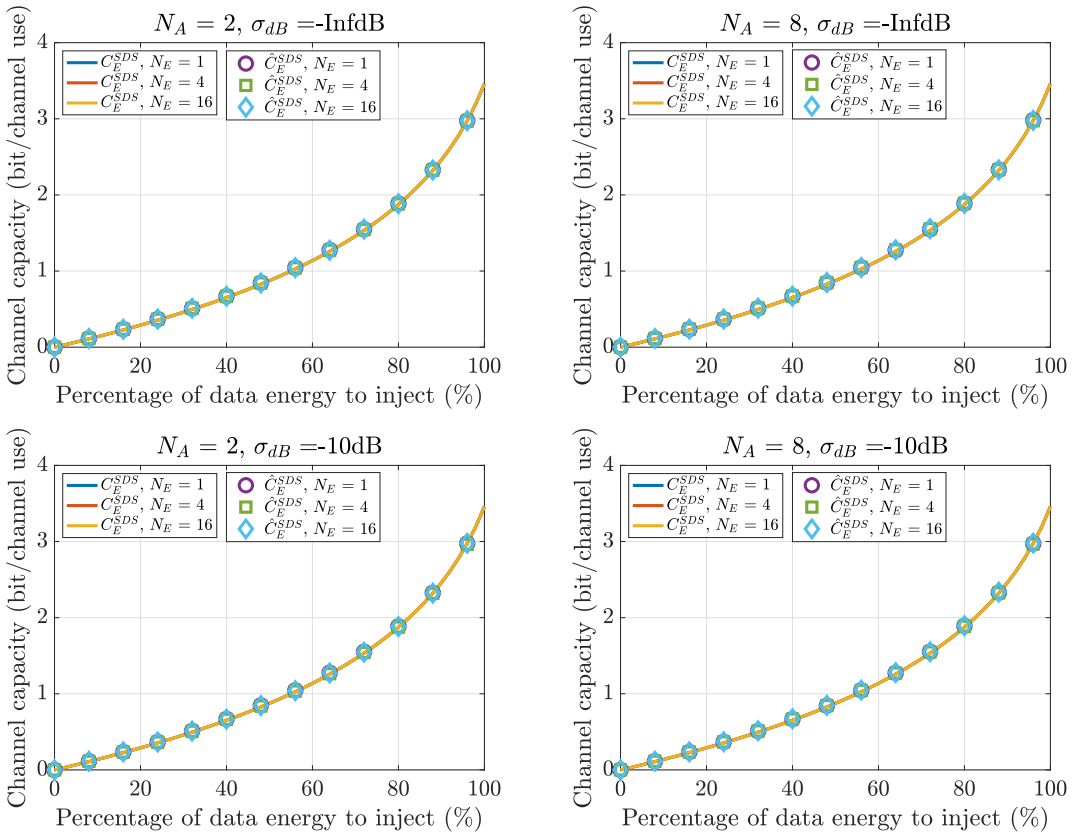

Figure 6.2: Comparison between approximated EC and exact EC at Eve, SDS decoder, $U = 2$, $\delta_E = 10$dB, 100.000 realizations

As anticipated from the above discussion, Eve's capacity does not depend on her number of antennas nor on Alice's number of antennas. Furthermore, one can observe that the approximated EC perfectly fits the exact EC, such that it can be used as a closed-form expression for the rest of the study. In addition, the EC values observed in Figure 6.2 are identical to the ones obtained in Figure 5.2, which shows the EC at Eve in a SISO-SE SDS scenario.

TDD handshake procedure 2: own channel decoder

When Eve implements the OC decoder, by replacing (6.4) in (6.2), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{OC}} = \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},lk}||^2 \widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},lk}||^2 \mathbf{w} + \mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}^H \mathbf{v}_{\mathrm{E},l}, \quad (6.25)$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\mathrm{OC}} = \frac{\sqrt{\alpha}}{N_A U} \sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},kl,i}|^2 \hat{h}_{\mathrm{B},k,i}^* \quad (6.26a)$$

$$E_{2,n}^{\mathrm{OC}} = \frac{1}{\sqrt{N_A U}} \sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},kl,i}^* v_{\mathrm{E},l,i} \quad (6.26b)$$

$$E_{3,n}^{\mathrm{OC}} = \frac{\sqrt{1-\alpha}}{\sqrt{N_A U}} \sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},kl,i}|^2 w_i. \quad (6.26c)$$

As detailed in D.2.2.1, D.2.2.2, and D.2.2.3, the expected energy of the components are respectively given by:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{OC}}|^2\right] = \frac{\alpha N_E(N_E+1)}{UN_A} \tag{6.27a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{OC}}|^2\right] = N_E\sigma_{\mathrm{E}}^2 \tag{6.27b}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{OC}}|^2\right] = \frac{(1-\alpha)N_E}{UN_A}(N_AN_E+1). \tag{6.27c}$$

Introducing (6.27a), (6.27b), and (6.27c) into (6.17), the per-symbol approximated ESINR at Eve in a MISO-ME system configuration is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right] \approx \frac{\frac{\alpha N_E(N_E+1)}{UN_A}}{N_E\sigma_{\mathrm{E}}^2 + \frac{(1-\alpha)N_E}{UN_A}(N_AN_E+1)} = \frac{\alpha(N_E+1)}{N_AU\sigma_{\mathrm{E}}^2 + (1-\alpha)(N_AN_E+1)}. \tag{6.28}$$

Equation (6.28) shows that Eve's ESINR depends on N_A and N_E. However, it is interesting to note that, when $N_E \to +\infty$, Eve's ESINR becomes independent of N_E. Furthermore, one can state that when $N_A \to +\infty$, $\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right] \to 0$. That is, Eve's ESINR decreases when Alice is equipped with a growing number of antennas. In addition, if one sets $N_A = 1$ in (6.28), one comes back to the SISO-ME OC scenario.
The approximated EC at Eve when an OC decoder is implemented is therefore expressed as:

$$C_E^{\mathrm{OC}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right]\right) = \log_2\left(1+\frac{\alpha(N_E+1)}{N_AU\sigma_{\mathrm{E}}^2 + (1-\alpha)(N_AN_E+1)}\right) \tag{6.29}$$

Figure 6.3 shows the accuracy of the EC, by comparing the exact EC ($\widehat{C}_E^{\mathrm{OC}}$) obtained by Monte Carlo simulations (100.000 realizations), with the approximated EC at Eve (C_E^{OC}) given in (6.29), as a function of the energy dedicated for information data. In each sub-figure, different number of Eve's antennas are considered. Between each-subplot, the number of antennas at Alice and/or the main CSI estimation error are made variable. It is assumed a spreading factor of $U = 2$, and $\delta_E = 10$dB.

From Figure 6.3, one observes that (6.29) fits perfectly the exact EC and is therefore used as a closed-form approximation for the rest of this study. In addition, it can be stated that there is no influence of Alice's CSI estimation error on Eve's EC, as anticipated from equation (6.29). Furthermore, the influence of Eve's number of antennas on the capacity value is minimal. Indeed, there is not much difference between the different capacity curves when N_E increases. Also, it is observed that, except when a large majority of the transmitted energy is dedicated for data, i.e., except when $\alpha \to 1$, increasing the number of Alice's antennas decreases Eve's capacity. As an example, when $N_A = 2$, $N_E = 16$, and $\alpha = 0.5$, i.e., 50% of the transmitted energy is dedicated for information data, Eve's capacity equals 0.59 bit/channel use. With the same set of parameters but $N_A = 8$, Eve's capacity equals 0.18 bit/channel use. This can be understood from (6.28) . In fact, except at large α, one obtains: $\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right] \propto 1/N_A$. Therefore, it can concluded that Alice can considerably decrease Eve's EC if she is equipped with a growing number of antennas.

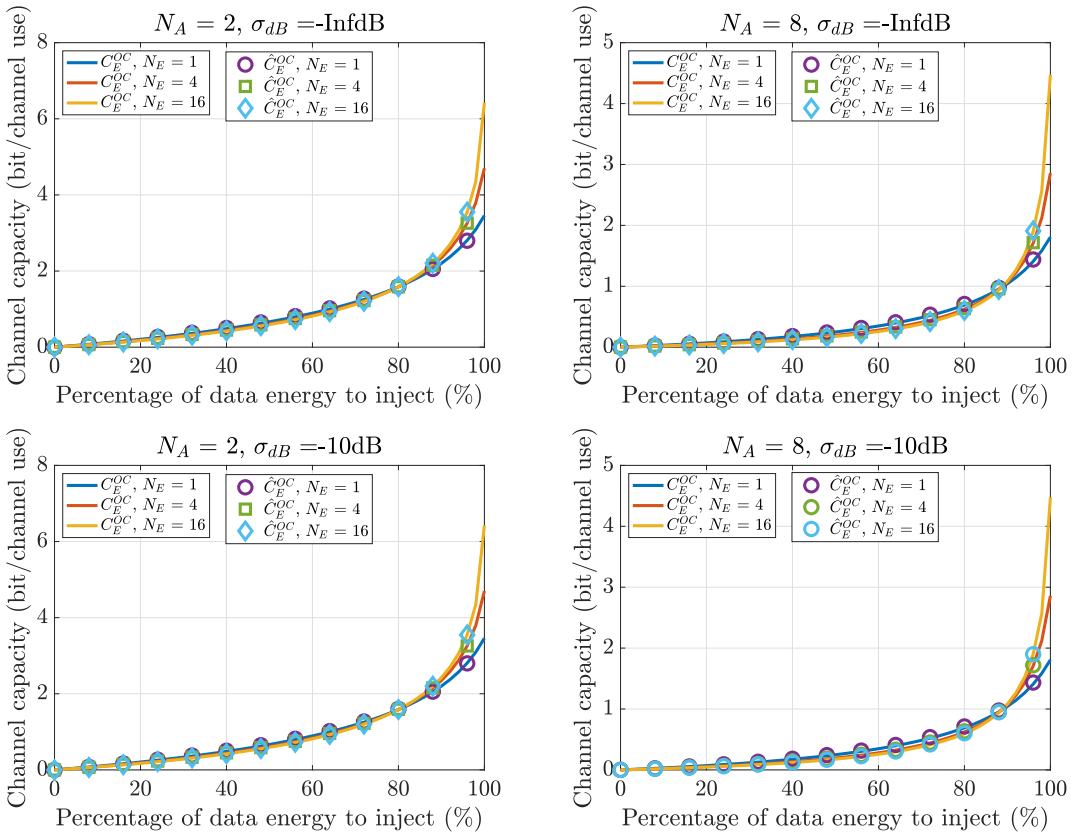

Figure 6.3: Comparison between approximated EC and exact EC at Eve, OC decoder, $U = 2$, $\delta_E = 10$dB, 100.000 realizations

TDD handshake procedure 3: maximum ratio combining decoder

When Eve implements the MRC decoder, by replacing (6.5) in (6.2), the received signal becomes:

$$\begin{aligned}\mathbf{y}_{\mathrm{E}}^{\mathrm{MRC}} =& \sqrt{\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},lk}||^2 \left|\left|\widehat{\mathbf{H}}_{\mathbf{B},k}\right|\right|^2 \mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},lk}||^2 \widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{w} \\ &+ \mathbf{S}^H \sum_{k=1}^{N_A}\sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}^H \widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{v}_{\mathrm{E},l},\end{aligned} \tag{6.30}$$

The received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\mathrm{MRC}} = \frac{\sqrt{\alpha}}{N_A U}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},kl,i}|^2 \left|\hat{h}_{\mathrm{B},k,i}\right|^2 \tag{6.31a}$$

$$E_{2,n}^{\mathrm{MRC}} = \frac{1}{\sqrt{N_A U}}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},kl,i}^{*}\hat{h}_{\mathrm{B},k,i}v_{\mathrm{E},l,i} \tag{6.31b}$$

$$E_{3,n}^{\mathrm{MRC}} = \frac{\sqrt{1-\alpha}}{\sqrt{N_A U}}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},kl,i}|^2 \hat{h}_{\mathrm{B},k,i}w_i. \tag{6.31c}$$

As detailed in D.2.3.1, D.2.3.2, and D.2.3.3, the expected energy of the components are respectively given by:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{MRC}}|^2\right] = \frac{\alpha N_E}{N_A U}\left[2 + N_E(N_A U + 1)\right] \tag{6.32a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{MRC}}|^2\right] = N_E \sigma_{\mathrm{E}}^2 \tag{6.32b}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{MRC}}|^2\right] = \frac{(1-\alpha)N_E}{N_A U + 1}. \tag{6.32c}$$

Introducing (6.32a), (6.32b), and (6.32c) into (6.17), the per-symbol approximated ESINR at Eve is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right] \approx \frac{\frac{\alpha N_E}{N_A U}\left[2 + N_E(N_A U + 1)\right]}{N_E \sigma_{\mathrm{E}}^2 + \frac{(1-\alpha)N_E}{N_A U + 1}} = \frac{\frac{\alpha}{N_A U}\left[2 + N_E(N_A U + 1)\right]}{\sigma_{\mathrm{E}}^2 + \frac{(1-\alpha)}{N_A U + 1}}. \tag{6.33}$$

From (6.33), it can be outlined that Eve's ESINR becomes arbitrarily large when Eve is equipped with an arbitrarily large number of antennas. One observes that it also increases when N_A increases. In particular, when $\alpha \neq 0$ or $\alpha \neq 1$, $\mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right] \propto N_E N_A U$. This arises from the fact that, when Eve implements a MRC decoder, she benefits from a diversity gain U at each of her N_E antennas, where each of her N_E antennas intercept N_A signals coming from Alice, which can be sum up coherently thanks to the MRC. That is, Eve benefits from an array gain $N_A N_E$ (i.e., TX and RX array gain), and a frequency diversity gain U.
The approximated EC at Eve, when an MRC decoder is implemented, is therefore expressed as:

$$C_E^{\mathrm{MRC}} \approx \log_2\left(1 + \mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right]\right) = \log_2\left(1 + \frac{\frac{\alpha}{N_A U}\left[2 + N_E(N_A U + 1)\right]}{\sigma_{\mathrm{E}}^2 + \frac{(1-\alpha)}{N_A U + 1}}\right) \tag{6.34}$$

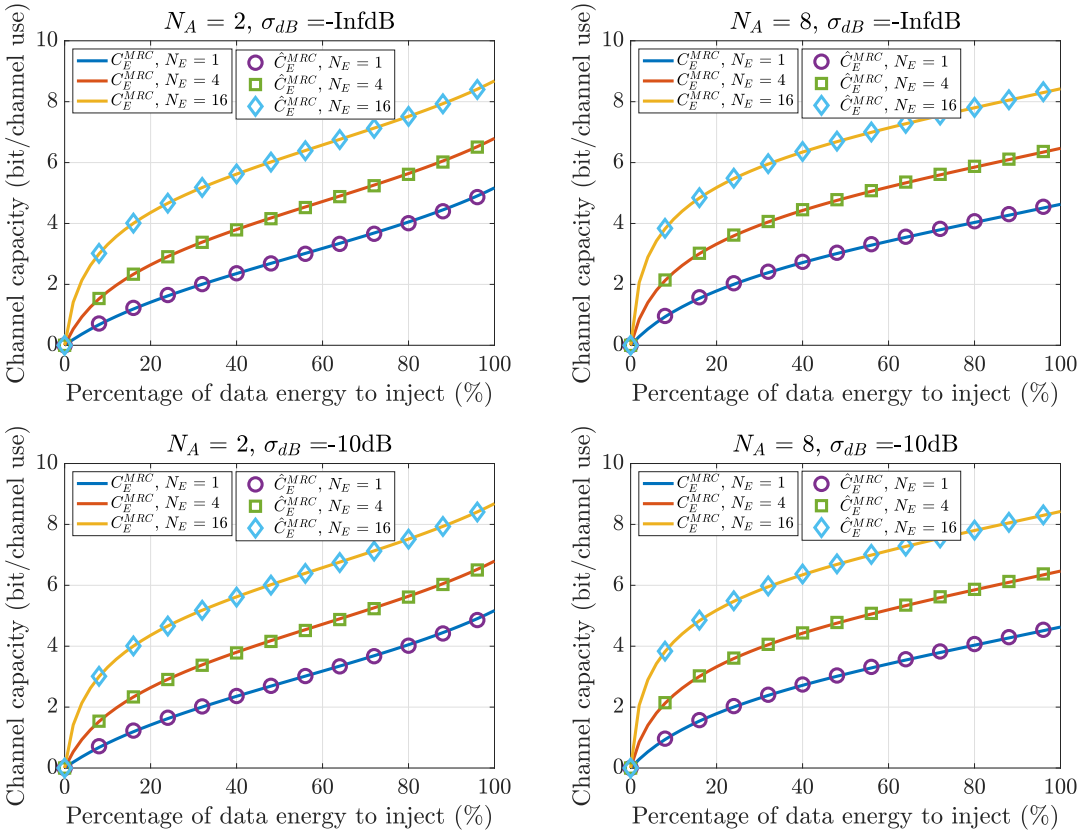

Figure 6.4: Comparison between approximated EC and exact EC at Eve, MRC decoder, $U = 2$, $\delta_E = 10$dB, 100.000 realizations

Figure 6.4 shows the accuracy of the EC, by comparing the exact EC ($\widehat{C}_E^{\mathrm{MRC}}$) obtained by Monte Carlo simulations (100.000 realizations), with the approximated EC at Eve (C_E^{MRC}) given in (6.34), as a function of the energy dedicated for information data. In each sub-figure, different number of Eve's antennas are considered. Between each-subplot, the number of antennas at Alice and/or the main CSI estimation error are made variable. It is assumed a spreading factor of $U = 2$, and $\delta_E = 10$dB.

It is observed from Figure 6.4 that (6.34) fits perfectly the exact EC, and is therefore used as a closed-form approximation for the rest of this study. One can also see the influence of Eve's number of antennas on the capacity value. Indeed C_E^{MRC} increases when N_E increases, as anticipated from the discussion about Eve's ESINR (6.33). It can also be outlined an increase of Eve's capacity when Alice is equipped with an increase number of antennas. Finally, it can be stated that Alice's error on Bob's CSI does not influence Eve's EC.

6.2.5 Guaranteeing secrecy rate

Similarly to the SISO system investigated in chapter 5, in a practical scenario, Alice needs to a priori know the per-symbol ESR over which she can securely communicate with Bob. In order to do so, Alice must design the communication parameters that guarantee a targeted communicated ESR, depending on the handshake procedures with Bob. Three scenarios are investigated:

- Scenario 1: Eve implements the SDS decoder.
- Scenario 2: Eve implements the OC decoder.
- Scenario 3: Eve implements the MRC decoder.

For each scenario, the required SNR at Bob that guarantees ESR$= \Delta$ is derived in Section 6.2.5.1. Upper bounds on Eve's number of antennas that are allowed, as well as on Alice's CSI estimation error, are derived in Section 6.2.5.2 and 6.2.5.3, respectively. The optimal amount of data energy to inject, i.e., the amount of data energy that minimizes Bob's required SNR to target ESR$= \Delta$, is expressed in Section 6.2.5.4. As usual, the worst case scenario in terms of secrecy is considered. That is, Eve's SNR $\rightarrow +\infty$, which is obtained by setting $\sigma_{\mathrm{E}}^2 = 0$ in Eve's capacity expressions. This corresponds to the situations where Eve is close to Alice, and/or Eve is equipped with a noise-free hardware.

6.2.5.1 Required SNR at Bob

As a reminder, the transmitted energy per symbol is 1. Since one symbol is spread over U subcarriers, the transmitted energy per symbol component is $1/U$. In addition, it is considered normalized channels, such that the received energy per symbol component is $1/U$. Therefore, Bob's SNR per symbol component is defined as :

$$\delta_{\mathrm{B}}^{\mathrm{D}} = \frac{1}{U\sigma_{\mathrm{B}}^2}. \tag{6.35}$$

It is also assumed that Alice aims to guarantee a per-symbol communication ESR $= \Delta$ bit/channel use.

Scenario 1: same decoding structure decoder
Introducing (6.14) and (6.23) into the per-symbol ESR expression (5.11), and considering $\sigma_{\mathrm{E}}^2 = 0$, the guaranteed ESR in a MISO-ME SDS configuration is given by:

$$R_{s,n}^{\mathrm{SDS}} = \Delta = \frac{1}{U}\left[\log_2\left(1 + \frac{\alpha\left[N_A U(1-\sigma)+1\right]}{U\sigma_{\mathrm{B}}^2 + (1-\alpha)\sigma}\right) - \log_2\left(1 + \frac{\alpha}{1-\alpha}\right)\right]. \tag{6.36}$$

The ESR being independent of N_E, the impact of Eve's number of antennas is therefore not investigated.

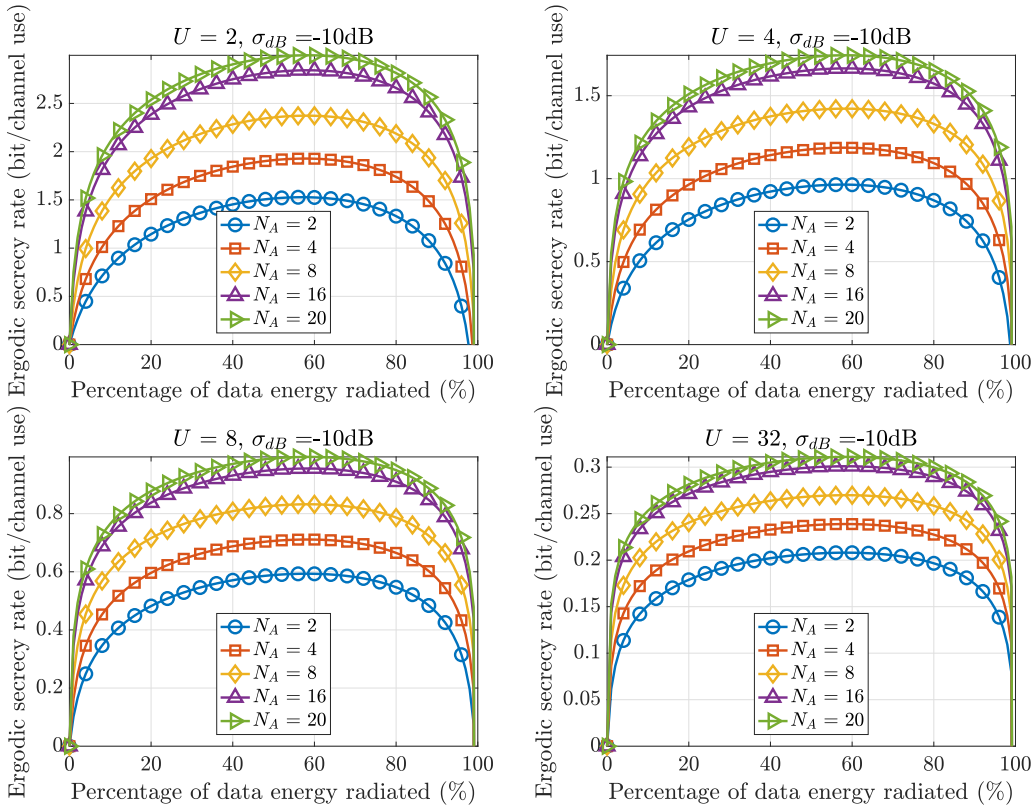

Figure 6.5: Guaranteed ergodic secrecy rate, SDS decoder, $\delta_B = 10$dB

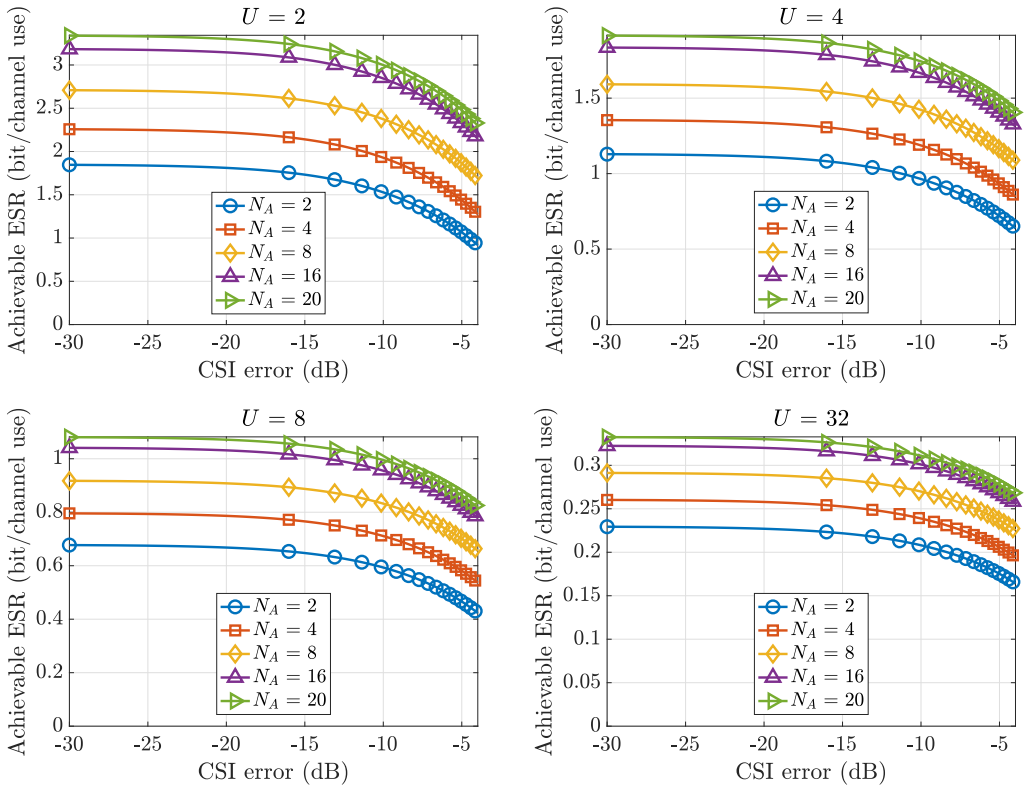

Figure 6.6: Maximal guaranteed ergodic secrecy rate as a function of the main CSI error, SDS decoder, $\delta_B = 10$dB

Figure 6.5 presents the ESR as a function of α, for different number of transmitter's antennas, at fixed CSI estimation error of 10%, and with different BOR values between each subplot.
First, it shows that the ESR increases with an increase of N_A. In that situation, Bob's capacity is enhanced but not Eve's one. In addition, when N_A increases, less AN energy, i.e., more data energy, has to be injected to maximize the communication ESR. As an example, when $U=4$, $\sigma_{\text{dB}}=-10\text{dB}$, the ESR is maximized for $\alpha=0.56$ when $N_A=2$, for $\alpha=0.6$ when $N_A=8$, and for $\alpha=0.62$ when $N_A=20$. The reason is that, when N_A increases, since Bob's decoding capabilities increase but not Eve's ones, one needs less AN to give Bob a physical advantage compared to Eve. Furthermore, due to the rate decrease factor, when the BOR increases, the ESR decreases.

Figure 6.6 shows the impact of Alice's main CSI estimation error on the achievable per-symbol communication ESR. As expected, when Alice more accurately estimates Bob's CSI, the achievable ESR increases. It is also observed that, whatever U and N_A, positive achievable ESRs can be obtained for low CSI estimation accuracies. Indeed, the achievable ESR remains positive, for $\sigma_{\text{dB}}\approx-4\text{dB}$, i.e., Alice misestimates Bob's CSI with $\approx 40\%$ of error, even for low N_A and high spreading factors.
After manipulating equation (6.36), one obtains the required SNR at Bob to guarantee ESR $=\Delta$, when Eve implements the SDS decoder:

$$\delta_{\text{B}}^{\text{SDS}}=\frac{\alpha+T_1^{\text{SDS}}}{\alpha^2T_2^{\text{SDS}}+\alpha T_3^{\text{SDS}}+T_4^{\text{SDS}}}, \tag{6.37}$$

where:

$$\begin{aligned}
T_1^{\text{SDS}}&=2^{\Delta U}-1\\
T_2^{\text{SDS}}&=(N_AU+1)(\sigma-1)\\
T_3^{\text{SDS}}&=(N_AU+1)(1-\sigma)+\sigma(2^{\Delta U}-1)\\
T_4^{\text{SDS}}&=\sigma\left(1-2^{\Delta U}\right).
\end{aligned}$$

Scenario 2: own channel decoder
Introducing (6.14) and (6.29) into the per-symbol ESR expression (5.11), and considering $\sigma_{\text{E}}^2=0$, the guaranteed ESR in a MISO-ME OC configuration is given by:

$$R_{s,n}^{\text{OC}}=\Delta=\frac{1}{U}\left[\log_2\left(1+\frac{\alpha\left[N_AU(1-\sigma)+1\right]}{U\sigma_{\text{B}}^2+(1-\alpha)\sigma}\right)-\log_2\left(1+\frac{\alpha(N_E+1)}{(1-\alpha)(N_AN_E+1)}\right)\right]. \tag{6.38}$$

Figure 6.7 shows the ESR as a function of α, for different N_E, with $U=4$, $\sigma_{\text{dB}}=-10\text{dB}$, and with variable N_A between each sub-figure. First, it is observed that, when N_E increases, the maximal ESR saturates. This can be understood from Eve's ergodic capacity (6.29) which is bounded when $N_E\to+\infty$. Second, it is seen that more data energy has to be injected to maximize the ESR when N_A increases. The justification is similar to the SDS situation since, when Alice is equipped with a growing number of antennas, Bob's capacity is enhanced but Eve's capacity is penalized. From that, it can also be concluded that the per-symbol communication ESR increases when N_A increases. Furthermore, one can see in Figure 6.7 that the maximal ESR slightly increases with an increase of N_E, whatever the value of N_A. This can be anticipated from Eve's ESINR expression (6.28). Indeed, Eve's ESINR is proportional to $\frac{N_E+1}{N_AN_E+1}$ when $\sigma_{\text{E}}^2=0$. Since $N_A\geq 2$, one obtains:

$$\left.\frac{1}{N_A}\right|_{N_E\to+\infty}\leq\mathbb{E}\left[\gamma_{E,n}^{\text{OC}}\right]\leq\left.\frac{2}{N_A+1}\right|_{N_E=1}. \tag{6.39}$$

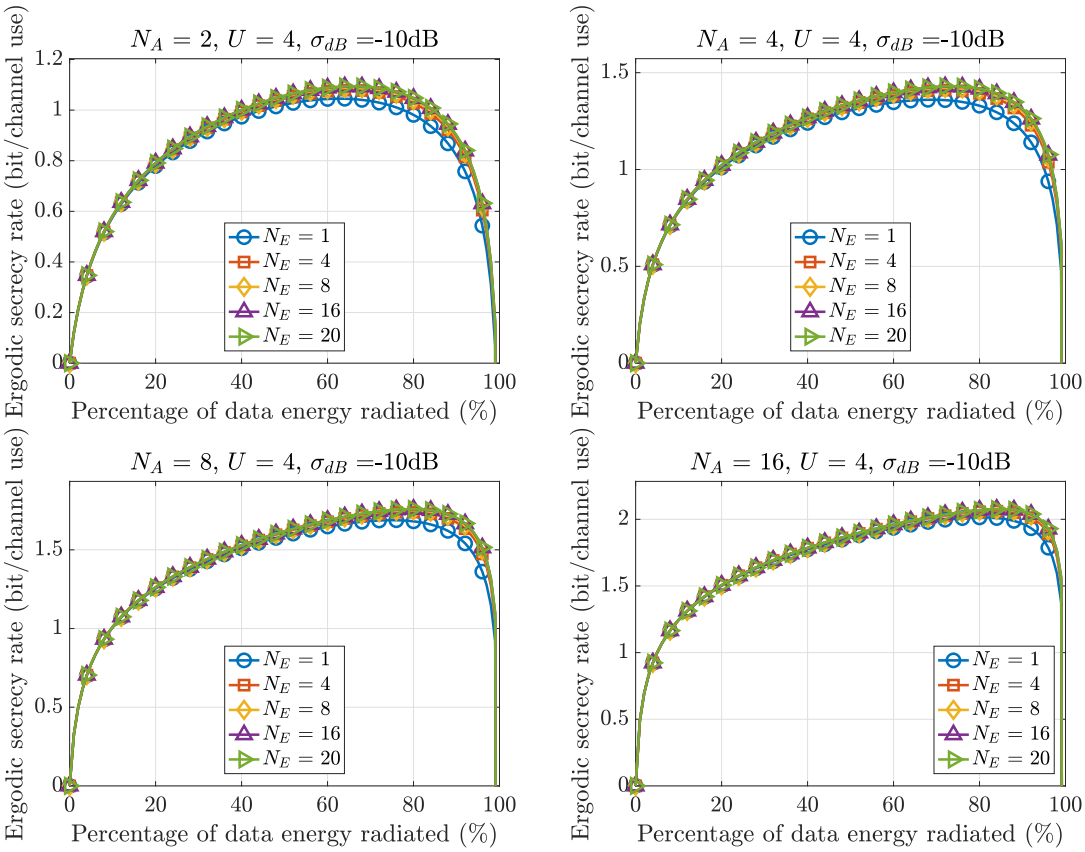

Figure 6.7: Guaranteed ergodic secrecy rate, OC decoder, $\delta_B = 10$dB

Consequently, in a MISO-ME OC system, the worst case scenario in terms of secrecy is obtained when $N_E = 1$, i.e., when Eve is a single-antenna eavesdropper. Only this configuration will be investigated for the rest of this chapter with this decoding structure. Finally, one can conclude that the OC scenario exhibits higher secrecy performances compared to the SDS scenario. As an example, when $U = 4$, $\sigma_{\text{dB}} = -10$dB, $N_A = 8$, and $N_E = 1$, a maximal ESR of $\Delta = 1.68$ bit/channel use is ensured for the OC scenario, but only 1.42 bit/channel use is ensured for the SDS scenario, as seen in Figure 6.5.

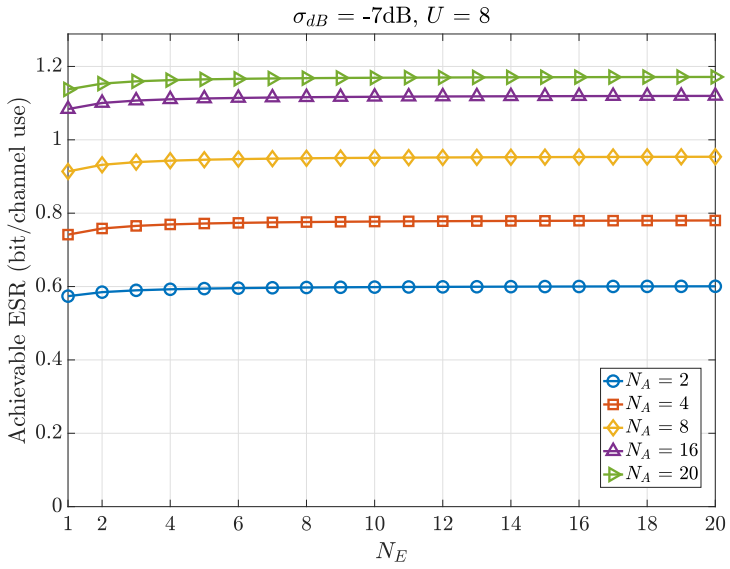

Figure 6.8: Maximal guaranteed ergodic secrecy rate as a function of N_E, OC decoder, $\delta_B = 10$dB

Figure 6.8 confirms that lower ESR values are obtained when $N_E = 1$, whatever the number of antennas at Alice. However, it is observed that, for fixed N_A, U, and σ_{dB} values, the ESR not much increases when N_E increases.

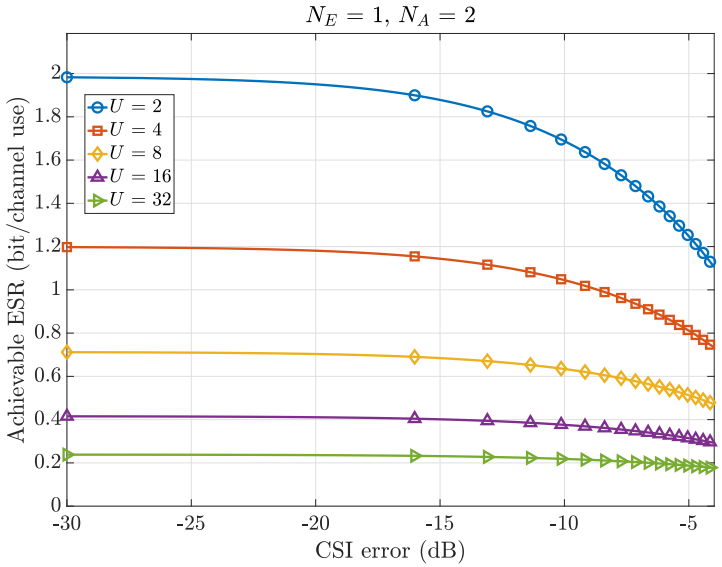

Figure 6.9: Maximal guaranteed ergodic secrecy rate as a function of the main CSI error, OC decoder, $\delta_B = 10$dB

Figures 6.7 and 6.8 show the impacts of α, N_A, and N_E on the ESR performances while Figure 6.9 presents the influence of the main CSI estimation error made by Alice, as well as the spreading factor. As expected, when U increases, the ESR decreases. In addition, when Alice more accurately estimates Bob's CSI, the achievable ESR increases. It is also observed that, whatever U, positive achievable ESRs can be obtained for low CSI estimation accuracies.
After setting $N_E = 1$ in equation (6.38), one obtains the required SNR at Bob to guarantee ESR $= \Delta$, when Eve implements the OC decoder. Indeed, $N_E = 1$ is the worst-case scenario for OC decoder. That is, the SNR is given by:

$$\delta_{\text{B}}^{\text{OC}} = \frac{\alpha T_0^{\text{OC}} + T_1^{\text{OC}}}{\alpha^2 T_2^{\text{OC}} + \alpha T_3^{\text{OC}} + T_4^{\text{OC}}}, \tag{6.40}$$

where:

$$\begin{aligned}
T_0^{\text{OC}} &= 2^{\Delta U}(1 - N_A) + (N_A + 1) \\
T_1^{\text{OC}} &= (N_A + 1)(2^{\Delta U} - 1) \\
T_2^{\text{OC}} &= 2^{\Delta U}\sigma(1 - N_A) - (N_A + 1)(N_A U + 1) \\
T_3^{\text{OC}} &= N_A + 1)\left((1 - \sigma)(N_A U + 1) + \sigma(2^{\Delta U} - 1)\right) - 2^{\Delta U}\sigma \\
T_4^{\text{OC}} &= (N_A + 1)\left(1 - 2^{\Delta U}\right).
\end{aligned}$$

Scenario 3: maximum ratio combining decoder
Introducing (6.14) and (6.34) into the per-symbol ESR expression (5.11), and considering $\sigma_{\text{E}}^2 = 0$, the guaranteed ESR in a MISO-ME MRC configuration is given by:

$$R_{s,n}^{\text{MRC}} = \Delta = \frac{1}{U}\left[\log_2\left(1 + \frac{\alpha\left[N_A U(1-\sigma) + 1\right]}{U\sigma_{\text{B}}^2 + (1-\alpha)\sigma}\right) - \log_2\left(1 + \frac{\frac{\alpha}{N_A U}\left[2 + N_E(N_A U + 1)\right]}{\frac{(1-\alpha)}{N_A U + 1}}\right)\right]. \tag{6.41}$$

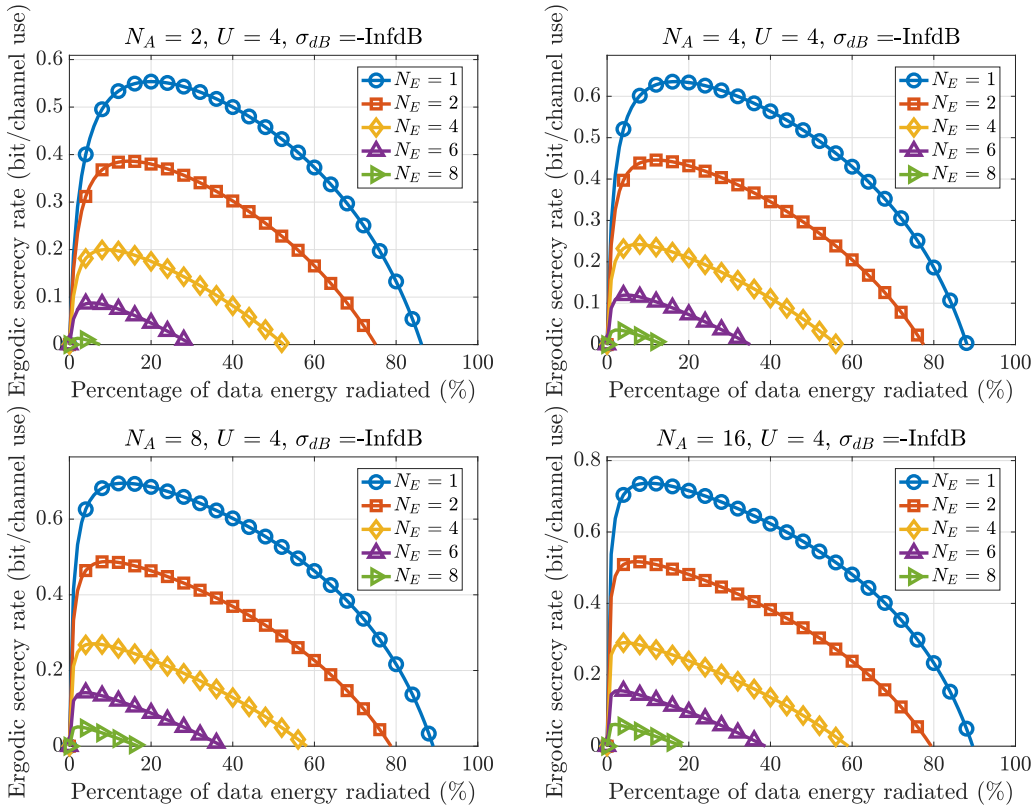

Figure 6.10: Guaranteed ergodic secrecy rate, MRC decoder, $\delta_B = 10$dB

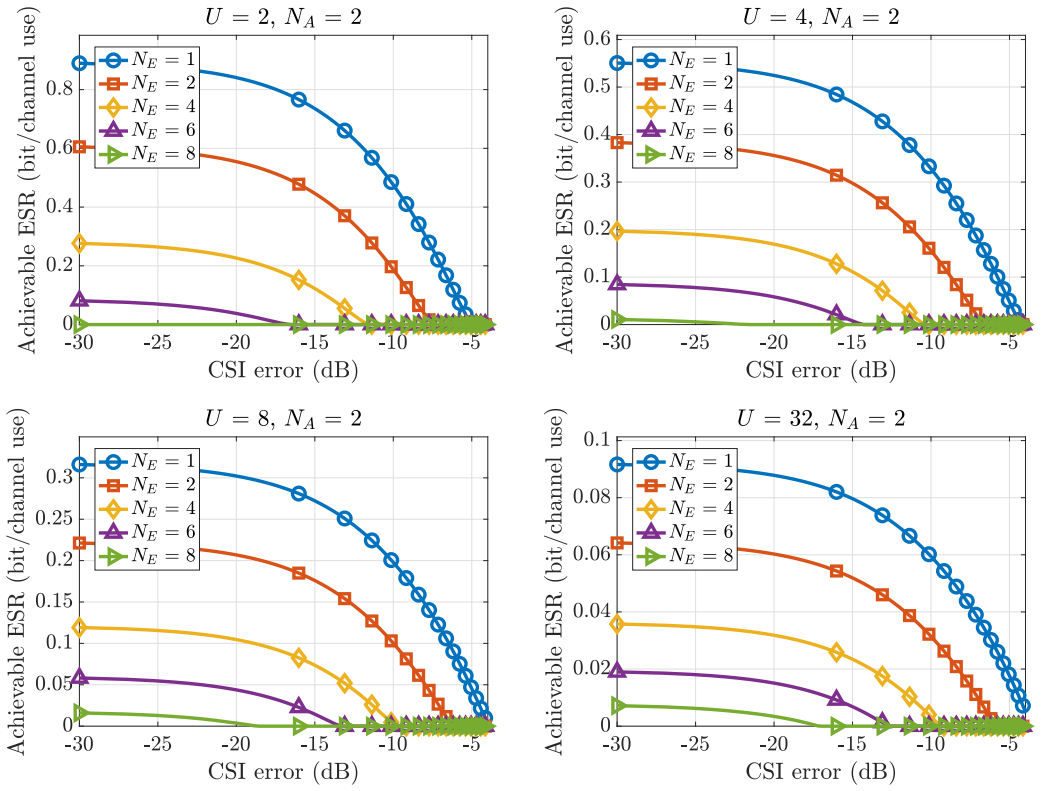

Figure 6.11: Maximal guaranteed ergodic secrecy rate as a function of the main CSI error, MRC decoder, $\delta_B = 10$dB

Figure 6.10 illustrates the ESR as a function of α, for different N_E, with fixed $U=4$ and $\sigma_{\text{dB}}=-\infty$dB, and with variable N_A between each sub-figure. First, it is observed that the ESR decreases when Eve is equipped with an increase number of antennas. This can be understood from Eve's ESINR expression (6.33), where it is seen that her decoding capabilities are enhanced when N_E increases. Second, one can also outline an ESR increase when N_A increases. Third, one can state that when N_E or N_A increases, more AN energy has to be injected to maximize the ESR. In particular, when N_E is large, the vast majority of the energy injected must be dedicated for AN. As an example, when $N_A=4$ and $N_E=8$, Alice has to inject 98% of AN to maximize the ESR performances, compared to 83% when $N_E=1$. Finally, compared to the SDS and OC scenarios, the MRC scenario presents the lowest ESR performances. This is expected since in that situation, Eve benefits from a frequency diversity gain due to the implementation of the MRC decoder. She is able to coherently sum up her received symbol components .

Figure 6.11 highlights the influence of σ_{dB} and U on the ESR performances, when Eve implements a MRC decoder. It is observed that, for lower number of Eve's antennas, Alice is allowed to less accurately estimate Bob's CSI in order to ensure positive achievable ESR. As an example, for $U=4$ and $N_A=2$, a positive ESR is achieved as soon as $\sigma_{\text{dB}}<-4$dB when $N_E=1$, i.e. $\approx 40\%$ of estimation error, as soon as $\sigma_{\text{dB}}<-6.61$dB when $N_E=2$, i.e. $\approx 21.8\%$ of estimation error, and as soon as $\sigma_{\text{dB}}<-10.65$dB when $N_E=4$, i.e., $\approx 8.6\%$ of estimation error. In addition, less accurate CSI estimation errors are allowed when U increases, if a positive achievable ESR is aimed. Indeed, for $U=2$ and $N_A=2$, Alice can make a CSI estimation error up to ≈ -16dB, i.e., $\approx 2.5\%$ of error, when Eve has 6 antennas. For the same set of parameters but $U=32$, Alice can misestimate Bob's CSI with an error up to ≈ -12.67dB, i.e., $\approx 5.4\%$ of error. Finally, lower ESR performances are obtained with higher spreading factors.
After manipulating equation (6.41), one obtains the required SNR at Bob to guarantee ESR $=\Delta$, when Eve implements the MRC decoder:

$$\delta_{\text{B}}^{\text{MRC}}=\frac{\alpha T_0^{\text{MRC}}+T_1^{\text{MRC}}}{\alpha^2 T_2^{\text{MRC}}+\alpha T_3^{\text{MRC}}+T_4^{\text{MRC}}}, \tag{6.42}$$

where:

$$\begin{aligned}
T_0^{\text{MRC}}&=2^{\Delta U}\left(N_E(N_AU+1)^2+2(N_AU+1)-N_AU\right)+N_AU\\
T_1^{\text{MRC}}&=N_AU(2^{\Delta U}-1)\\
T_2^{\text{MRC}}&=2^{\Delta U}\sigma\left[(N_AU+1)(2+N_E)(N_AU+1)-N_AU\right]-N_AU(N_AU+1)(1-\sigma)\\
T_3^{\text{MRC}}&=N_AU\left[(1-\sigma)(N_AU+1)-\sigma\right]-2^{\Delta U}\sigma\left[N_AU+(N_AU+1)(2+N_E(N_AU+1))\right]\\
T_4^{\text{MRC}}&=N_AU\sigma\left(1-2^{\Delta U}\right).
\end{aligned}$$

6.2.5.2 Maximal eavesdropper antennas allowed

Scenario 1: same decoding structure decoder
There is no condition to determine for the maximal number of eavesdropping antennas allowed to ensure a maximal per-symbol communication ESR, since Eve's capacity is independent of N_E.

Scenario 2: own channel decoder
There is no condition to determine for the maximal number of eavesdropping antennas allowed to ensure a maximal per-symbol communication ESR, since the worst-case scenario is obtained for $N_E=1$.

Scenario 3: maximum ratio combining decoder
Expression (6.42) gives the required SNR at Bob to guarantee a per-symbol communication ESR $=\Delta$, when Eve implements a MRC decoder, as a function of the communication parameters in a MISO-ME configuration. For a solution to exist, (6.42) must be positive. That is, one has to find a condition on σ in order to obtain plausible roots in α in (6.42). This imposes an upper bound on the allowed number of eavesdropper's antennas $N_{E,\max}$ to be able to guarantee a given targeted ESR. In other

words, if $N_E < N_{E,\max}$, a finite Bob's SNR is needed to target the desired ESR. If $N_E = N_{E,\max}$, Bob's SNR needs to be infinite to guarantee the ESR. If $N_E > N_{E,\max}$, it is impossible to target the desired communication ESR. To find the upper bound on N_E, the condition $T_2^{\mathrm{MRC}} < 0$ needs to be met, leading to:

$$N_{E,\max} = \left\lfloor \frac{N_A U(N_A U+1)(1-\sigma) + 2^{\Delta U}\sigma\left[N_A U - 2(N_A U+1)\right]}{(N_A U+1)^2 2^{\Delta U}\sigma} \right\rfloor^+, \tag{6.43}$$

where $\lfloor x \rfloor^+$ is the maximum between 0 and the nearest integer lower or equal to x. If $N_A = 1$, one comes back to the corresponding SISO-ME condition (5.80).
Figure 6.12 presents the maximal number of eavesdropper antennas that is allowed, as a function of the maximal ESR that can be targeted, for different BOR factors, at fixed $\sigma_{\mathrm{dB}} = -20$dB, i.e., 1% of CSI error, and with variable N_A between each sub-figure. As expected, $N_{E,\max}$ decreases when Δ increases. In addition, it is seen that $N_{E,\max}$ slightly increases when N_A increases, to target a given maximal ESR. As an example, when $\Delta = 0.2$ bit/channel use can at most be targeted and $U = 8$, $N_{E,\max} = 30$ when $N_A = 2$, and $N_{E,\max} = 32$ when $N_A = 16$. Furthermore, one can observe that, except at low ESRs, $N_{E,\max}$ increases when U decreases. The reason is that the rate decrease due to the spreading operation has a greater impact at higher BORs than at lower ones. It is therefore more stringent to communicate at a given ESR with higher BORs. However, at low targeted ESRs, the frequency diversity gain has a greater impact than the rate decrease. From that, higher BORs are preferable than lower ones if one wants to communicate at low rates, and Eve is allowed to be equipped with more antennas.

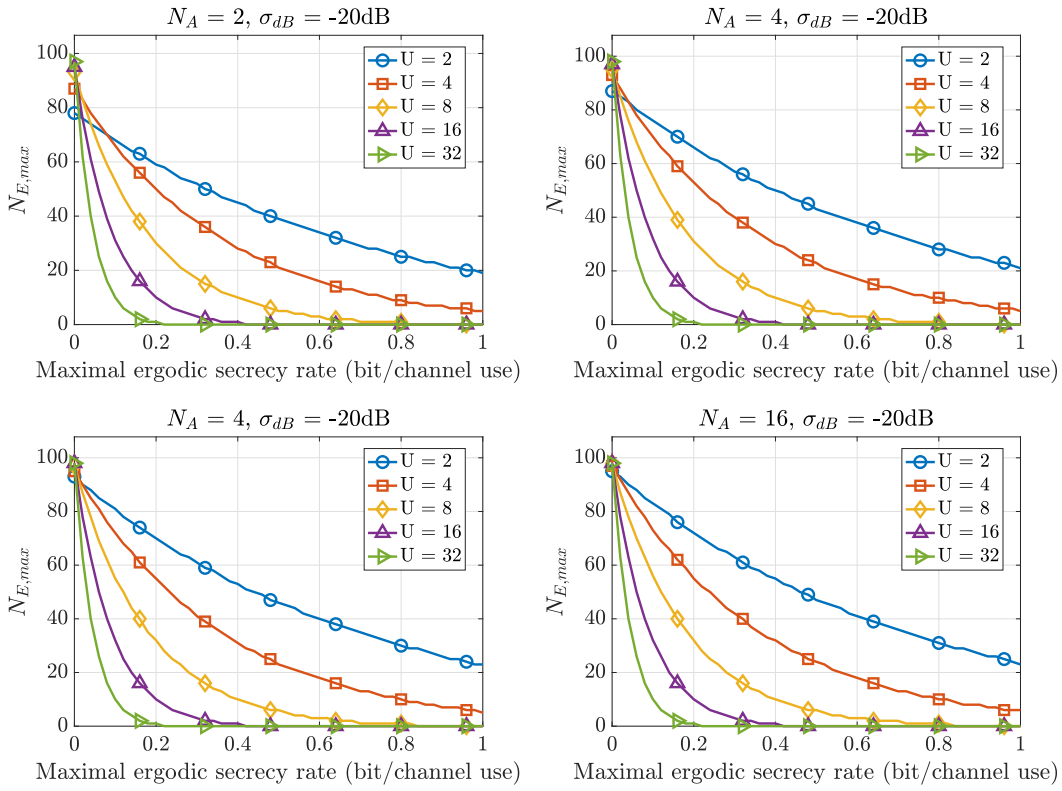

Figure 6.12: Maximal number of eavesdropping antennas as a function of the guaranteed ESR Δ, MRC decoder

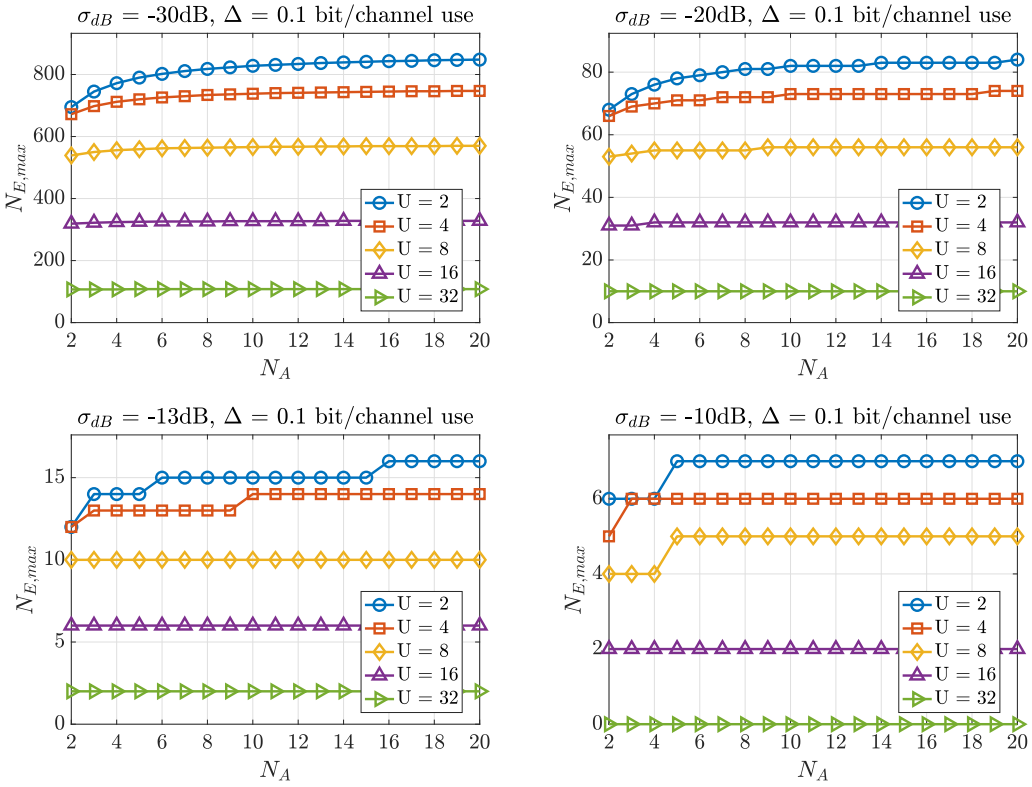

Figure 6.13: Maximal number of eavesdropping antennas as a function of N_A, MRC decoder

Figure 6.13 outlines the impact of N_A and σ_{dB} on $N_{E,\max}$, at fixed $\Delta = 0.1$bit/channel use. It first confirms that $N_{E,\max}$ does not increase much when Alice is equipped with a growing number of antennas. In addition, it is seen that $N_{E,\max}$ is very sensible to Alice main CSI estimation error. As an example, when $N_A = 8$, $U = 8$, and $\Delta = 0.1$bit/channel use, $N_{E,\max} = 564$ if $\sigma_{\text{dB}} = -30$dB, $N_{E,\max} = 55$ if $\sigma_{\text{dB}} = -20$dB, $N_{E,\max} = 10$ if $\sigma_{\text{dB}} = -13$dB, and $N_{E,\max} = 5$ if $\sigma_{\text{dB}} = -10$dB.

6.2.5.3 Maximal CSI error allowed

Expressions (6.37), (6.40), and (6.43) give the required SNR at Bob to guarantee a per-symbol communication ESR $= \Delta$ when Eve implements respectively an SDS, on OC, and an MRC decoder, as a function of the communication parameters in a MISO-ME configuration. For a solution to exist, SNR must be positive, which in turns imposes a maximal CSI error $\sigma^{\text{SDS}}_{\max}$ that can be made by Alice to possibly reach the targeted ESR. Determining the maximal CSI error allows to find the domain of validity of the SNR expression, i.e., it allows to find an upper bound on Alice's CSI misestimation to be able to guarantee ESR=Δ bit/channel use. In other words, when $\sigma < \sigma^{\text{SDS}}_{\max}$, Alice can determine a finite SNR at Bob that enables a guaranteed communication ESR $= \Delta$.

Scenario 1: same decoding structure decoder
From (6.37), it can be shown that:

$$\sigma^{\text{SDS}}_{\max} = 1 - \frac{2^{\Delta U} - 1}{2^{\Delta U} + N_A U}\bigg|_{\sigma^{\text{SDS}}_{\max} \in [0,1]}. \tag{6.44}$$

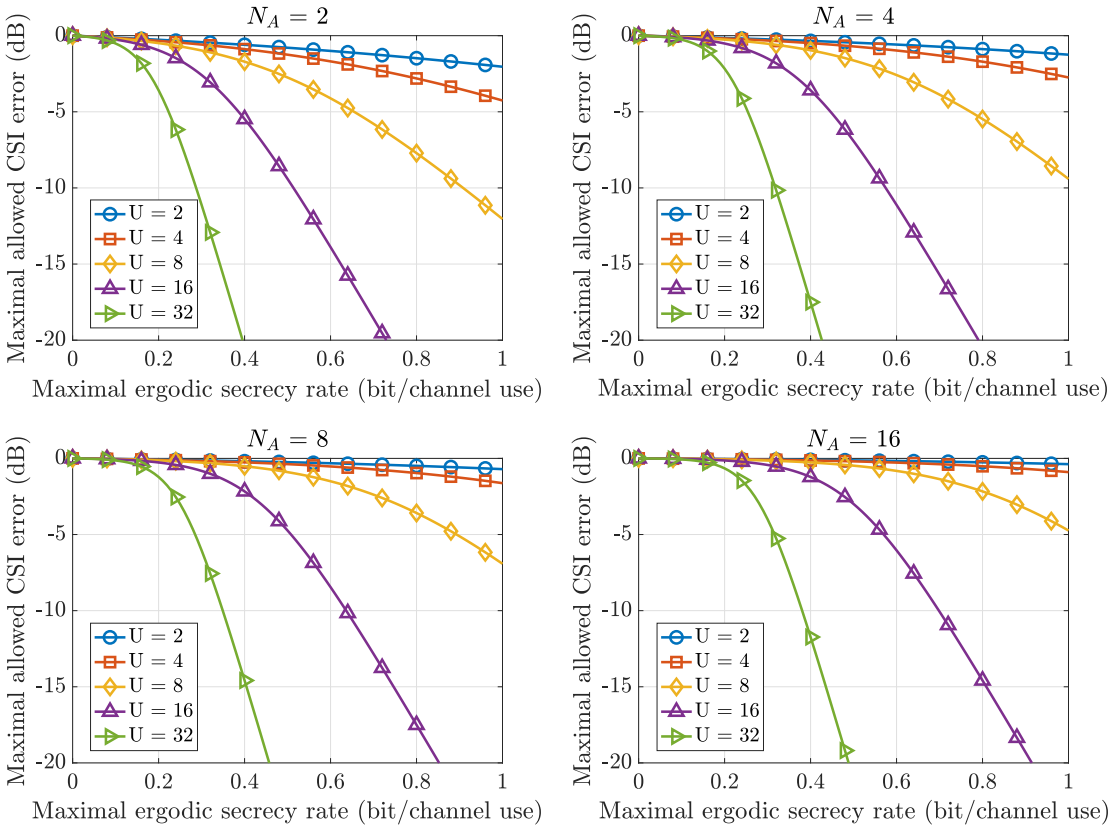

Figure 6.14: Maximal allowed CSI error as a function of the maximal ESR that can be guaranteed, SDS decoder

From condition (6.44), it is observed that $\sigma_{\max}^{\text{SDS}} \to 1$ if $N_A \to +\infty$. In addition, $\sigma_{\max}^{\text{SDS}} \to 1$ if $\Delta \to 0^+$. From these, Alice can a priori make any estimation error if she is equipped with an arbitrarily large number of antennas, or if she aims to ensure a positive ESR $\to 0^+$ bit/channel use. However, $\sigma_{\max}^{\text{SDS}} \to 0$ if $U \to +\infty$, or if $\Delta \to +\infty$. These behaviours are confirmed in Figure 6.14 where $\sigma_{\max}^{\text{SDS}}$ is plotted as a function of the maximal ESR that can be targeted, for different spreading factors, and with variable N_A between each sub-figure. It is observed that more accurate CSI estimations need to be performed at Alice if U increases to reach the same ESR performances. Also, Alice can make larger CSI estimation errors if she is equipped with more antennas.

Scenario 2: own channel decoder

As a reminder, only the situation when $N_E = 1$ is considered since it corresponds to the worst-case scenario. From (6.40), it can be shown that:

$$\sigma_{\max}^{\text{OC}} = 1 - \left. \frac{2^{\Delta U+1} - (N_A+1)}{2^{\Delta U+1} + N_A U(N_A+1)} \right|_{\sigma_{\max}^{\text{OC}} \in [0,1]}. \tag{6.45}$$

The behaviour of $\sigma_{\max}^{\text{OC}}$ is similar to $\sigma_{\max}^{\text{SDS}}$, and is presented in Figure 6.15. However, compared to the SDS scenario, Alice can be less stringent to estimate Bob's CSI in order to target a given ESR, with identical communication parameters. As explained, this scenario exhibits better secrecy performances than the SDS scenario. Therefore, less stricter conditions can be met at Alice to reach the same ESR performances.

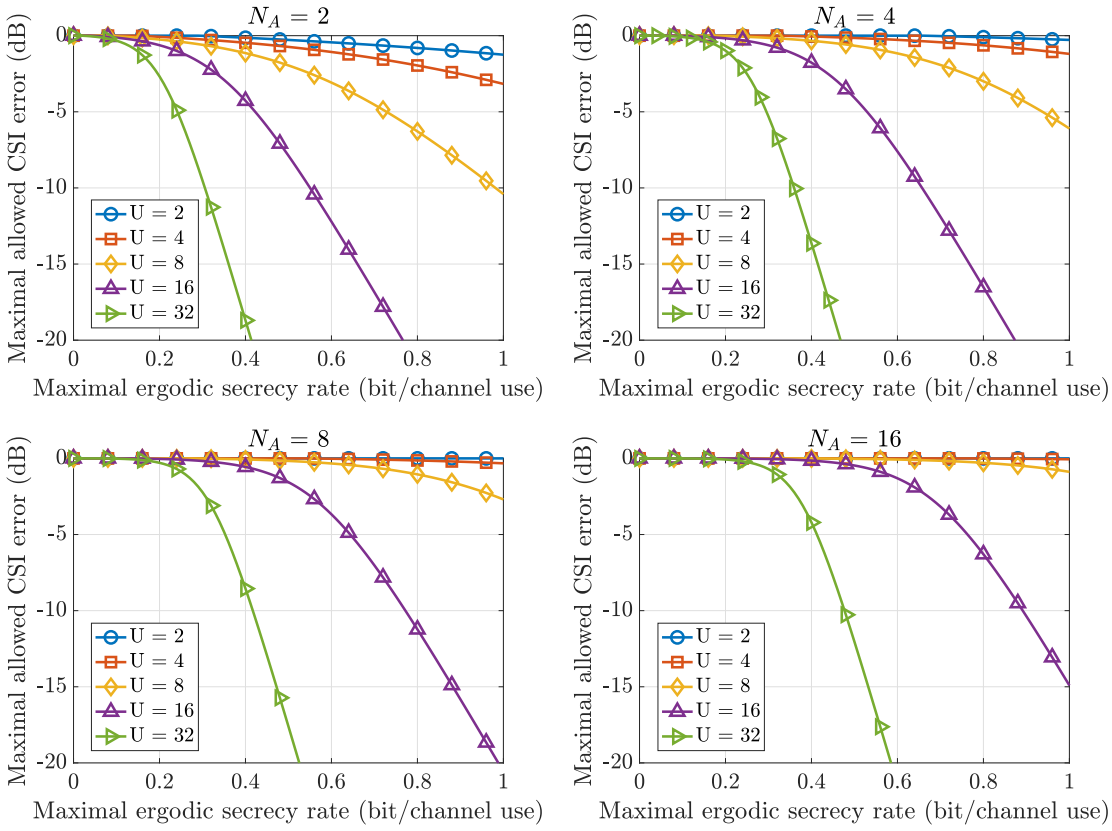

Figure 6.15: Maximal allowed CSI error as a function of the maximal ESR that can be guaranteed, OC decoder

Scenario 3: maximum ratio combining decoder

From equation (6.43), the upper bound on Alice's CSI estimation error to possibly reach a targeted ESR=Δ is:

$$\sigma_{\max}^{\mathrm{MRC}} = 1 - \left. \frac{2^{\Delta U}\left[N_E(N_AU+1)^2+(N_AU+1)+1\right]}{2^{\Delta U}\left[N_E(N_AU+1)^2+(N_AU+1)+1\right]+N_AU(N_AU+1)} \right|_{N_{\mathrm{E}} \leq N_{\mathrm{E,max}}\,, \sigma_{\max}^{\mathrm{MRC}} \in [0,1]} . \quad (6.46)$$

As for the SISO-ME MRC scenario, $\sigma_{\max}^{\mathrm{MRC}} < 1$ if $\Delta \to 0^+$. In addition, $\sigma_{\max}^{\mathrm{MRC}} \to 0$ if $\Delta \to +\infty$, or $N_E \to +\infty$, i.e., Alice must perfectly estimate Bob's CSI if Eve is equipped with an arbitrarily large number of antennas, and/or an arbitrarily large ESR aims to be reached.

Figure 6.16 shows the maximal allowed CSI error as a function of N_E. In each sub-figure, $N_A = 4$ or 16, and $\Delta = 0.1$ or 0.2 bit/channel use. The spreading factor differs between each sub-figure. It is first observed that $\sigma_{\max}^{\mathrm{MRC}}$ decreases when Δ increases, as expected. It also decreases when the BOR increases. Furthermore, Alice must be more accurate on Bob's CSI estimation if Eve has more antennas. In addition, it can be seen that $\sigma_{\max}^{\mathrm{MRC}}$ increases with an increase of N_A, but not significantly. Finally, compared to the SDS and OC scenarios, the MRC scenario exhibits significantly stricter conditions on the maximal allowed CSI error. As an illustration, when $N_A = 4$, $N_E = 10$, $U = 4$, and $\Delta = 0.2$ bit/channel use, $\sigma_{\max}^{\mathrm{SDS}} = -0.18$dB $\sigma_{\max}^{\mathrm{OC}} = -0.17$dB, and $\sigma_{\max}^{\mathrm{MRC}} = -12.9$dB.

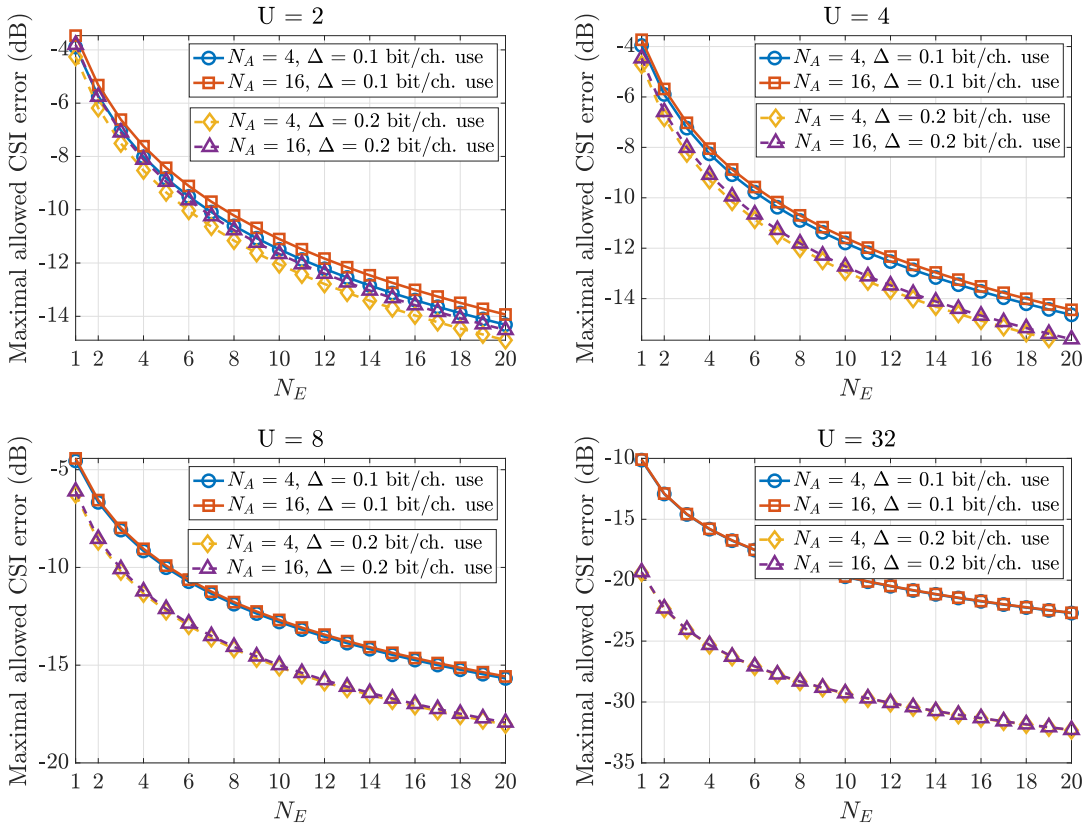

Figure 6.16: Maximal allowed CSI error as a function of N_E, MRC decoder

6.2.5.4 Optimal amount of data energy to inject

The SNR expressions (6.37), (6.40), and (6.42) are convex expressions in α. So, one can minimize these expressions to determine the optimal amount of data energy to inject. This corresponds to the amount of data energy that minimizes the required SNR at Bob to ensure ESR $= \Delta$, as a function of the communication parameters (U, σ, N_E, and N_A). It also depends on the decoding structure implemented at Eve, and will be denoted as $\alpha^{\mathrm{D}}_{\mathrm{opt}}$. To find $\alpha^{\mathrm{D}}_{\mathrm{opt}}$, one has to derive the SNR expressions as a function of α, and find to roots of it.

Scenario 1: same decoding structure decoder
By denoting

$$\begin{aligned} A_1^{\mathrm{SDS}} &= (N_A U + 1)(1-\sigma) \\ A_2^{\mathrm{SDS}} &= \sigma\left(2^{\Delta U} - 1\right) \\ A_3^{\mathrm{SDS}} &= A_1^{\mathrm{SDS}} + A_2^{\mathrm{SDS}}, \end{aligned}$$

one can show that:

$$\alpha_{\mathrm{opt}}^{\mathrm{SDS}} = \left.\frac{-2A_1^{\mathrm{SDS}}\left(2^{\Delta U}-1\right) + \sqrt{\Sigma^{SDS}}}{2A_1^{\mathrm{SDS}}}\right|_{\sigma \le \sigma_{\max}^{\mathrm{SDS}}, \alpha_{\mathrm{opt}}^{\mathrm{SDS}} \in [0,1]} \tag{6.47}$$

with $\Sigma^{\mathrm{SDS}} = 4(A_1^{\mathrm{SDS}})^2\left(2^{\Delta U}-1\right)^2 - 4A_1^{\mathrm{SDS}}\left[-\left(2^{\Delta U}-1\right)A_3^{\mathrm{SDS}} - A_2^{\mathrm{SDS}}\right]$. Equation (6.47) determines the amount of data that Alice has to inject in order to minimize the required SNR at Bob that guarantees a per-symbol communication ESR$= \Delta$ bit/channel use, when Eve performs the SDS decoder. To

obtain the corresponding SNR values, the parameter α in (6.37) is replaced with the values obtained in equation (6.47).

Figure 6.17 presents the required SNR at Bob as a function of the targeted ESR. For each sub-figure, $U = 2$ or 32, and $\sigma_{\text{dB}} = -10$ or -5dB, which corresponds to 10% and $\approx 30\%$ of CSI error. Between each sub-figure, N_A changes. First, the required SNR increases when Alice aims to target a larger ESR. Second, when the spreading factor increases, the required SNR increases as well, except for low targeted ESR values. This is expected since, when U increases, it becomes more difficult to target a given per-symbol communication ESR due to the rate decrease in $1/U$. However, at low ESRs, the diversity gain predominates the rate decrease, such that higher BORs are preferable. Third, when N_A increases, Bob's required SNR decreases to target a given communication ESR.

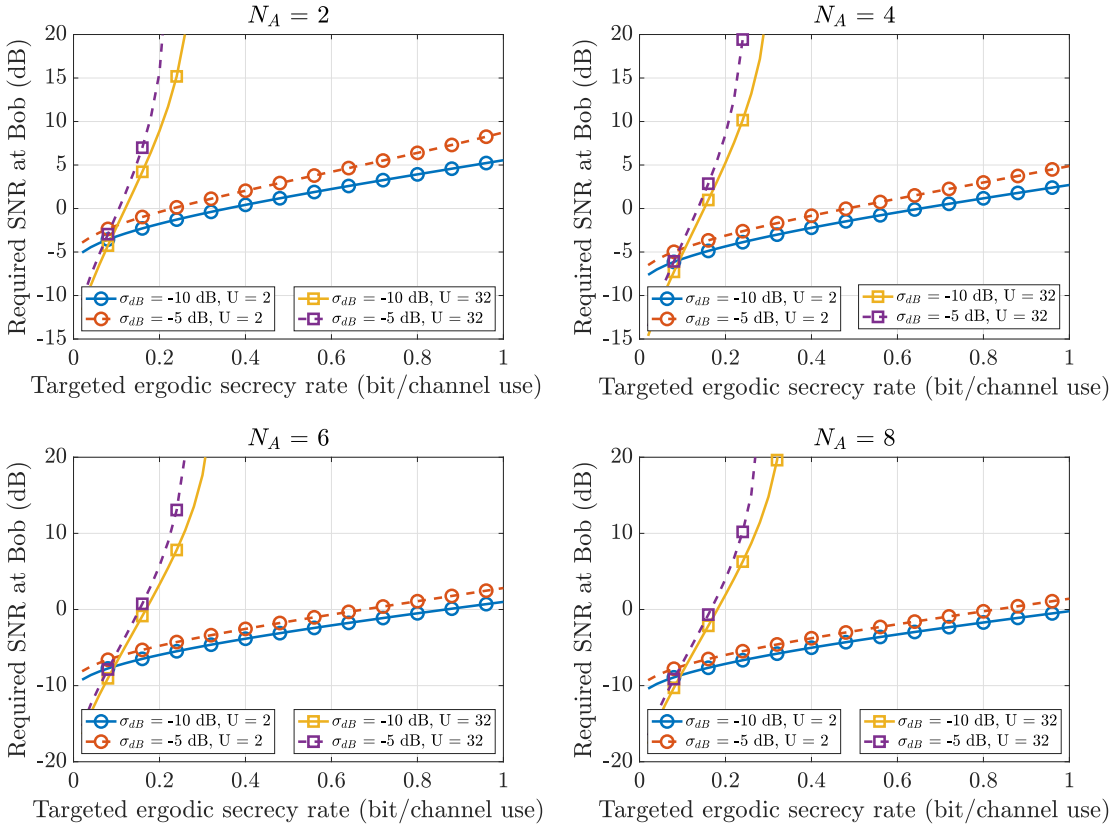

Figure 6.17: Required SNR at Bob as a function of the guaranteed ESR, SDS decoder

Scenario 2: own channel decoder

With the terms defined in (6.40), one can show that:

$$\alpha_{\text{opt}}^{\text{OC}} = \left. \frac{-T_1^{\text{OC}} T_2^{\text{OC}} - \sqrt{\left(T_1^{\text{OC}}\right)^2 \left(T_2^{\text{OC}}\right)^2 + T_0^{\text{OC}} T_2^{\text{OC}} \left(T_0^{\text{OC}} T_4^{\text{OC}} - T_2^{\text{OC}} T_3^{\text{OC}}\right)}}{T_0^{\text{OC}} T_2^{\text{OC}}} \right|_{\sigma \leq \sigma_{\max}^{\text{OC}}, \alpha_{\text{opt}}^{\text{OC}} \in [0,1]} \tag{6.48}$$

Equation (6.48) determines the amount of data that Alice has to inject, in order to minimize the required SNR at Bob that guarantees a per-symbol communication ESR$= \Delta$ bit/channel use, when Eve performs the OC decoder. Again, to obtain the corresponding SNR values, the parameter α in (6.40) is replaced with the values obtained in equation (6.48).

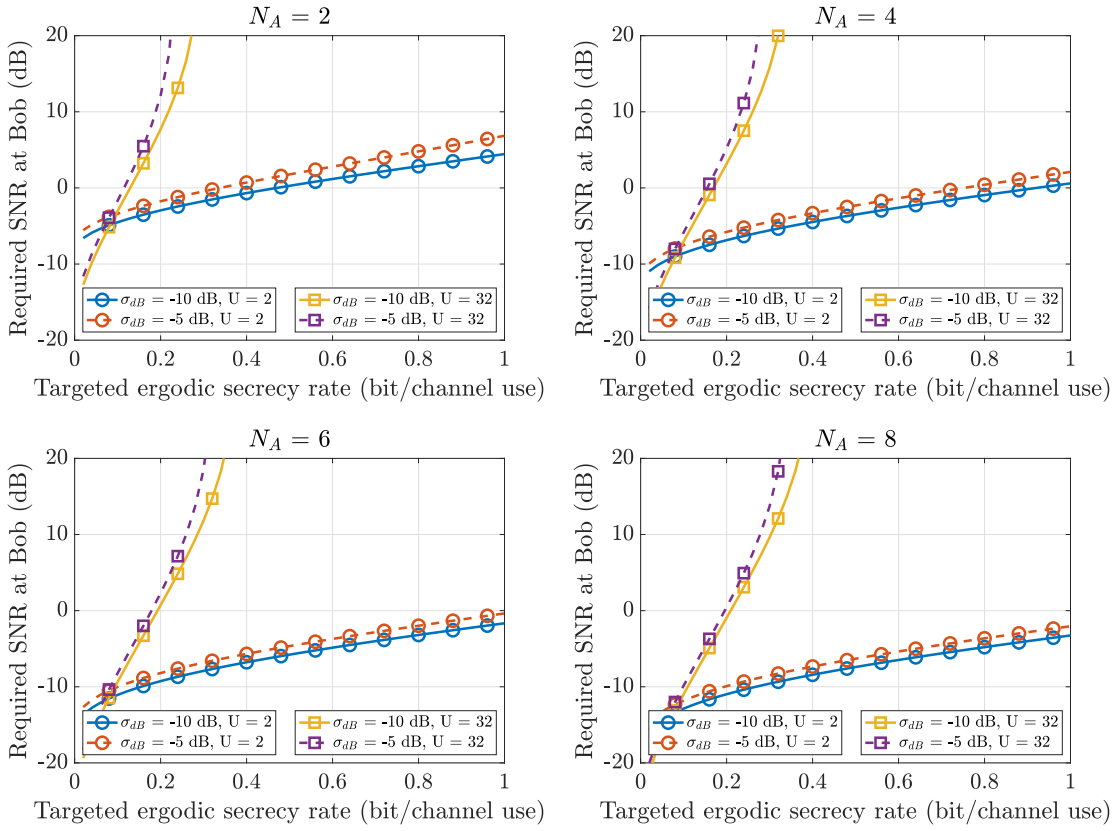

Figure 6.18: Required SNR at Bob as a function of the guaranteed ESR, OC decoder

Figure 6.18 presents the required SNR at Bob as a function of the targeted ESR for the same set of parameters as Figure 6.17. The same conclusions can be drawn. In addition, to reach similar performances, lower SNR are required in this scenario compared to the SDS scenario, which is expected.

Scenario 3: maximum ratio combining decoder
With the terms defined in (6.42), one can show that:

$$\alpha_{\text{opt}}^{\text{MRC}} = \left. \frac{-T_1^{\text{MRC}} T_2^{\text{MRC}} - \sqrt{\left(T_1^{\text{MRC}}\right)^2 \left(T_2^{\text{MRC}}\right)^2 + T_0^{\text{MRC}} T_2^{\text{MRC}} \left(T_0^{\text{MRC}} T_4^{\text{MRC}} - T_2^{\text{MRC}} T_3^{\text{MRC}}\right)}}{T_0^{\text{MRC}} T_2^{\text{MRC}}} \right|_{\substack{\sigma \leq \sigma_{\max}^{\text{MRC}}, \\ N_E \leq N_{E,\max}, \\ \alpha_{\text{opt}}^{\text{MRC}} \in [0,1]}} \tag{6.49}$$

Equation (6.49) determines the amount of data that Alice has to inject, in order to minimize the required SNR at Bob that guarantees a per-symbol communication ESR$= \Delta$ bit/channel use, when Eve performs the MRC decoder. To obtain the corresponding SNR values, the parameter α in (6.42) is replaced with the values obtained in equation (6.49).
Figure 6.19 presents the required SNR at Bob as a function of the targeted ESR. For each sub-figure, $N_E = 4$, $U = 2$ or 8, and $\sigma_{\text{dB}} = -\infty$dB or -10dB, which corresponds to 0% and 10% of CSI error. Between each sub-figure, N_A changes. The same conclusions as for the other scenarios can be drawn. However, as expected, higher SNRs are required at Bob to guarantee a similar ESR compared to the previously presented scenarios. As an example, to target $\Delta = 0.1$ bit/channel use, when $N_E = 4$, $N_A = 4$, $U = 8$, and $\sigma_{\text{dB}} = -10$dB, one needs $\delta_{\text{B}}^{\text{SDS}} = -5.18$dB, $\delta_{\text{B}}^{\text{OC}} = -7.03$dB, and $\delta_{\text{B}}^{\text{MRC}} = 17.29$dB. In addition, lower ESRs can be guaranteed when Eve implements the MRC decoder. Finally, the accuracy on Bob's CSI estimation strongly impacts the scenario performances.

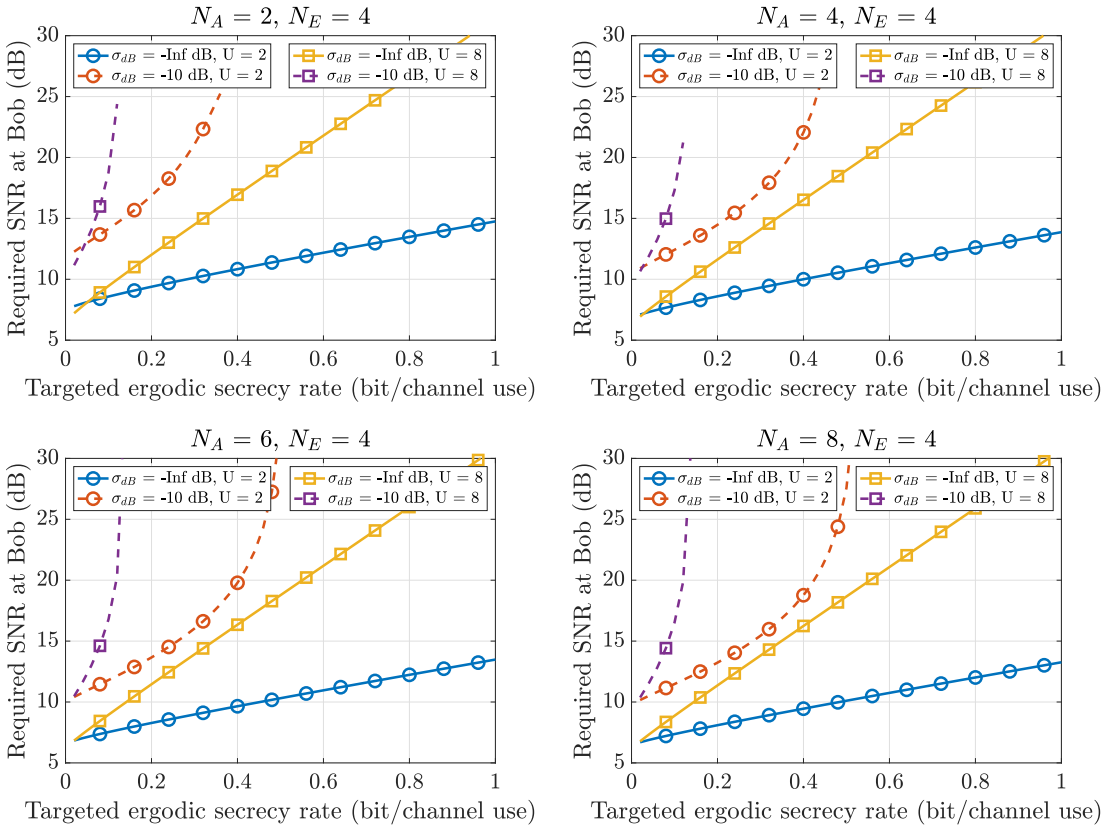

Figure 6.19: Required SNR at Bob as a function of the guaranteed ESR, MRC decoder

Figure 6.20 outlines the impact of N_E on the required SNR at Bob. As expected, when N_E increases, larger SNR at Bob is required to target a given ESR. It also confirms that the performances are strongly dependent on Alice's estimation accuracy. Indeed, when $U = 32$, with only 0.1% of CSI error, i.e., $\sigma_{\text{dB}} = -30\text{dB}$, it is impossible to ensure 0.2 bit/channel use if Eve is equipped with more than 11 antennas, when Alice has 8 antennas. In addition, to reach this level of secrecy, Bob's SNR needs to be equal to 42 dB. For the same set of parameters but with $\sigma = 0\%$ of CSI error, i.e., $\sigma_{\text{dB}} = -\infty\text{dB}$, Bob's required SNR is equal to 29.9dB (not shown in the plot).

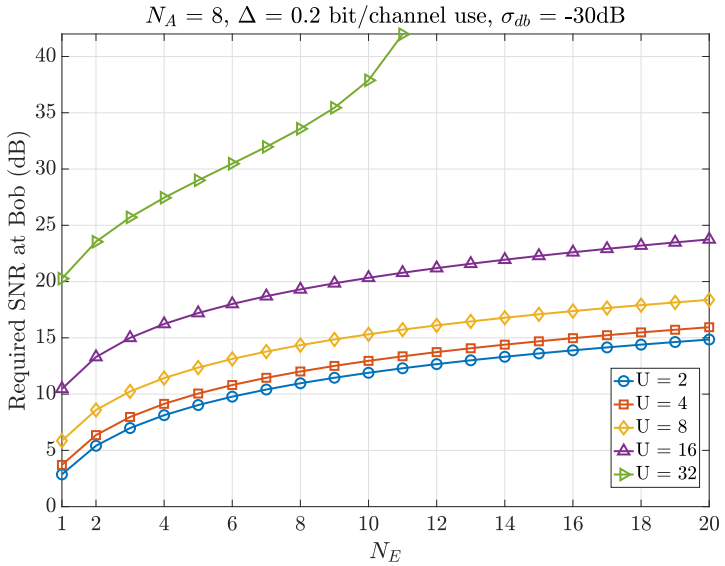

Figure 6.20: Required SNR at Bob as a function of N_E, MRC decoder

6.2.6 Secrecy outage consideration

Until now, one can state that it is preferable to communicate at low BOR values to guarantee higher communication ESRs when Eve implements a SDS or an OC decoder. When she is able to implement a MRC decoder, it was seen in Figure 6.11 that higher BORs are more likely to be used if Alice strongly misestimates Bob's CSI and if N_E increases. However, the analysis did not take into account that outages occur if the instantaneous secrecy rate that can be supported by the communication is lower than the actual ESR at which Bob and Alice communicate, resulting to leakage to Eve. As a reminder, the precise amount of leaked information cannot be known since it depends on the wiretap codes, but outages can be characterized. As for the SISO system, the $\epsilon-$achievable SR performances for the three investigated schemes are studied, considering 100.000 realizations of the instantaneous secrecy rate, in order to observe very low outage percentages. As always, it is assumed that Eve is noiseless. For the OC scenario, $N_E = 1$ is also considered since it corresponds to the worst case scenario in terms of secrecy.

Scenario 1: same decoding structure decoder

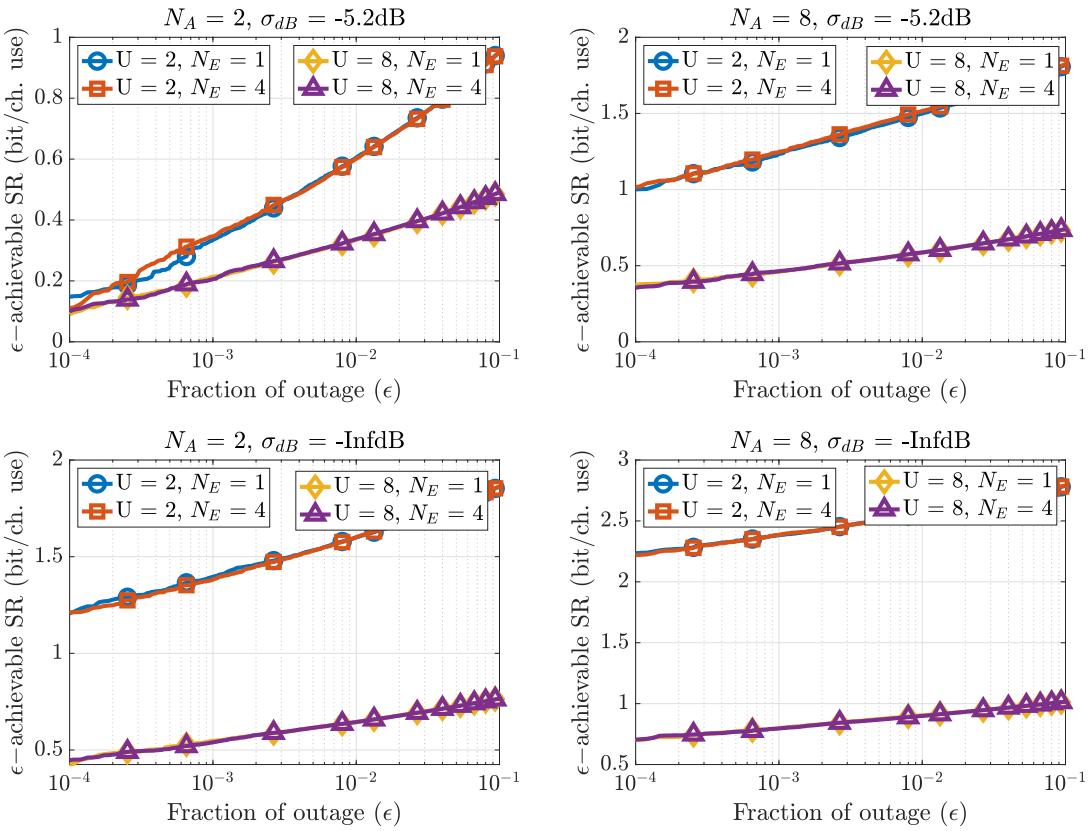

Figure 6.21: ϵ-achievable secrecy rate as a function of the fraction of outage, $\delta_B = 10$dB, SDS decoder

Figure 6.21 presents the $\epsilon-$achievable SR as a function of the faction of outage, for different number of Eve antennas, and different BOR factors. Between each sub-figure, the number of Alice's antennas and/or the CSI estimation error is made variable. First, it is observed that the number of Eve's antennas does not influence the outage performances. In addition, it is observed that higher BOR values are preferable when low outage percentage are required. The crossing point where higher BOR values are preferable to lower ones occurs for higher outage percentages when Alice is equipped with a low number of antennas and/or when she strongly misestimates Bob's CSI. As an example, Alice is more likely to communicate with $U = 8$ instead of $U = 2$, as soon as less than 0.01% of outage is

required, when $N_A = 2$ and $\sigma_{\text{dB}} = -5.2$dB, i.e., 30% of CSI error. With $N_A = 8$ and no CSI error, it is expected from Figure 6.21 that it is preferable to communicate with $U = 8$ instead of $U = 2$ for fractions of outage that are several orders lower than 10^{-4}, which cannot be observed in simulations. In addition, one can state that better outage performances are obtained when N_A increases and/or Alice's accuracy on Bob's CSI increases.

Scenario 2: own channel decoder

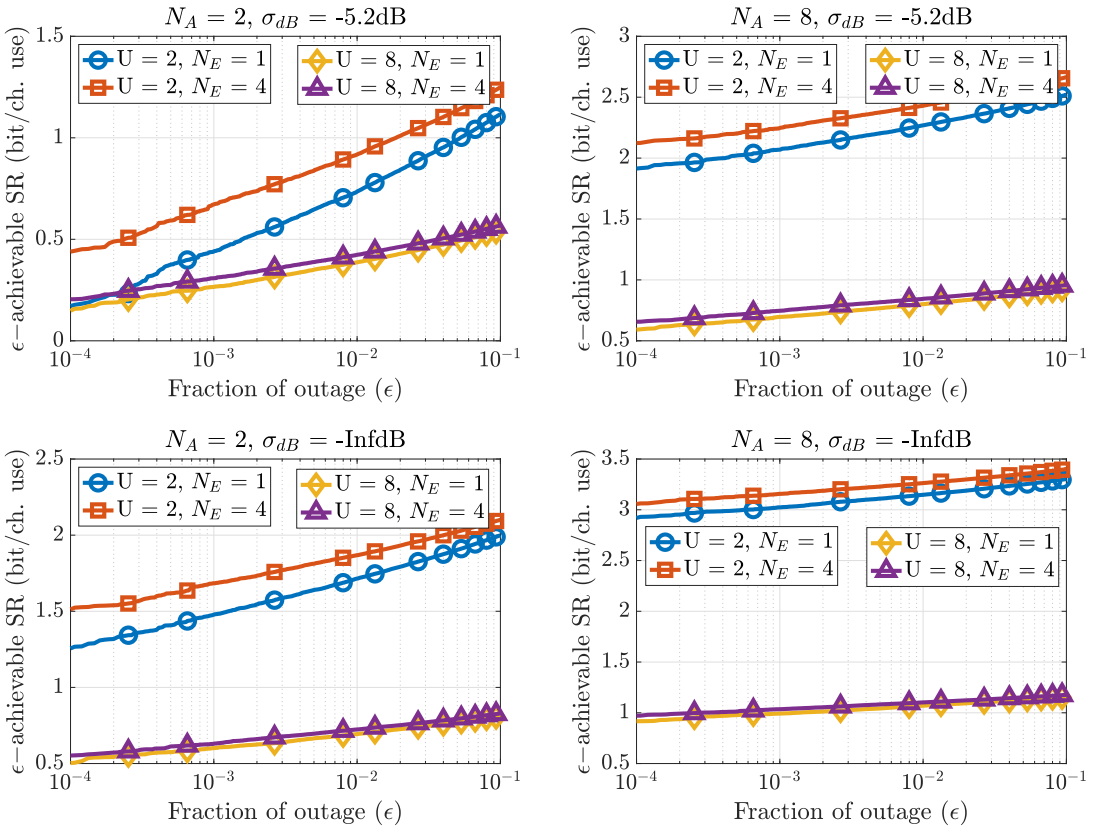

Figure 6.22: ϵ-achievable secrecy rate as a function of the fraction of outage, $\delta_{\text{B}} = 10$dB, OC decoder

Figure 6.22 presents the $\epsilon-$achievable SR for the MISO-ME OC scenario, and for the same set of parameters that are used in Figure 6.21. It can be observed that Eve's number of antennas influence the outage performances. This influence is more pronounced at lower BOR values. In addition, higher performances are obtained when she is equipped with a larger number of antennas. It is therefore preferable for Eve to possess less antennas in a MISO-ME OC scenario. Otherwise, the same conclusions can be drawn as for the MISO-ME SDS scenario.

Scenario 3: maximum ratio combining decoder

Figure 6.24 highlights the $\epsilon-$achievable SR performances of the MISO-ME MRC scenario as a function of the fraction of outage, for different number of Eve's antennas, when no CSI error is considered. Between each sub-plot, the number of Alice's antennas and/or the BOR factor are made variable. It is seen that positive $\epsilon-$achievable SRs are obtained for lower percentages of outage when the BOR increases. As an example, with $N_A = 2$, $N_E = 6$, $\sigma_{\text{dB}} = -\infty$dB, and $U = 2$, a non-zero $\epsilon-$achievable SRs is possible with at least 26.2% of outage occurring. For the same set of parameters but $U = 8$, it is attained as soon as 5.8% of outage occurs. Therefore, operating at higher BOR values, although it decreases the ESR, reduces the percentage of outages. In addition, the $\epsilon-$achievable SRs is very

sensible to the number of Eve's antennas. In fact, for $N_A = 8$, no CSI error, $U = 2$, and $N_E = 1$, a non-zero $\epsilon-$achievable SRs is obtained as soon as more than 0.035% of outage is acceptable, but 9.4% when $N_E = 6$ for instance. Finally, one can observe that, when N_A increases, the $\epsilon-$achievable SRs increases as well, for a given outage percentage.

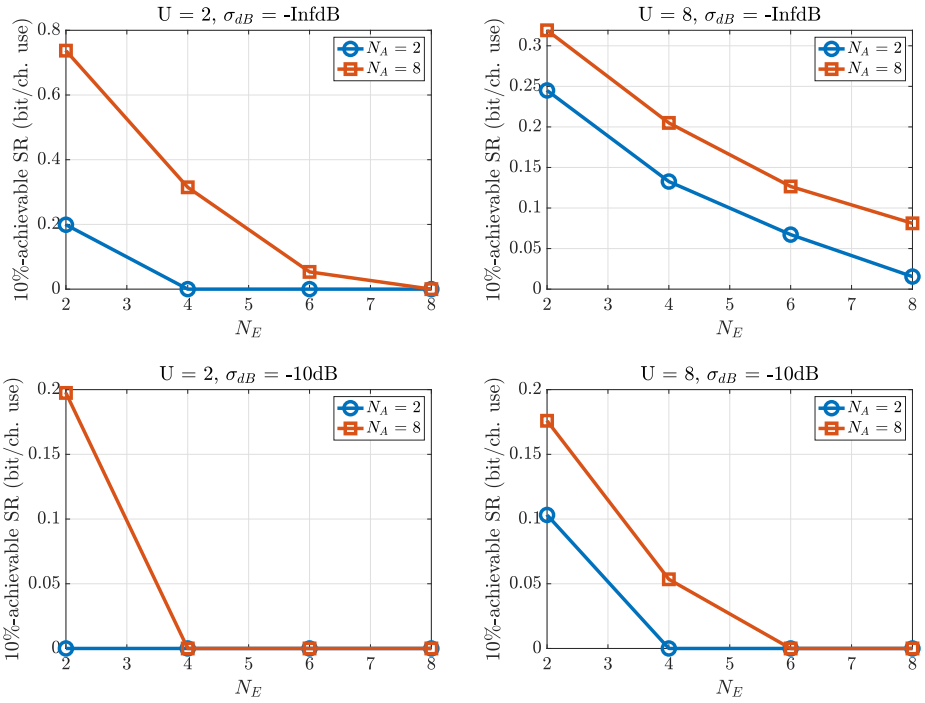

Figure 6.23: 10%-achievable secrecy rate as a function of N_E, $\delta_{\mathrm{B}} = 10$dB, MRC decoder

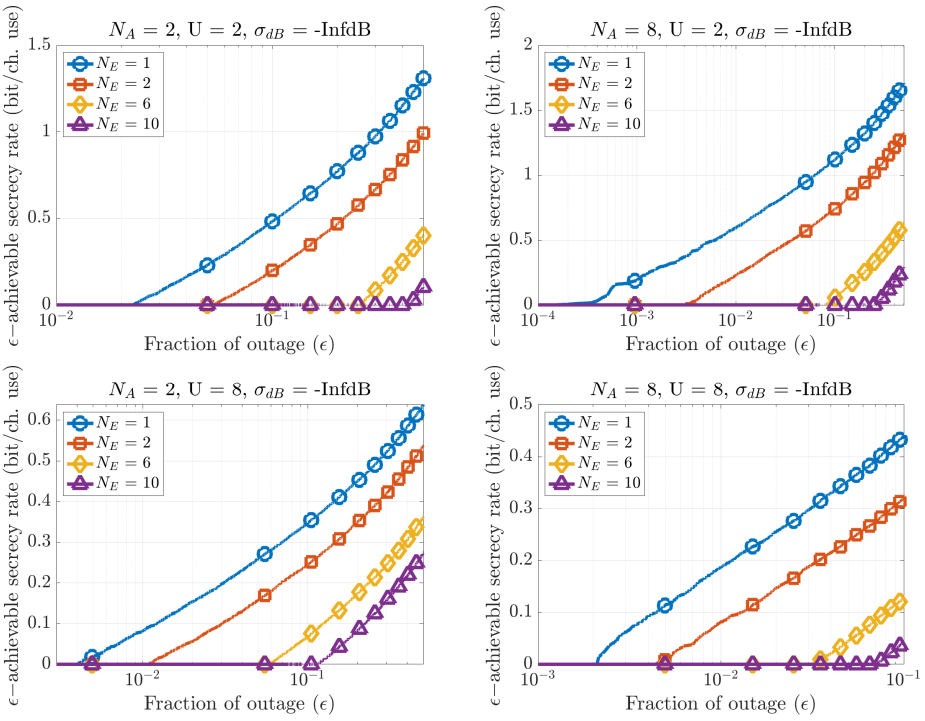

Figure 6.24: ϵ-achievable secrecy rate as a function of the fraction of outage, $\delta_{\mathrm{B}} = 10$dB, MRC decoder

Figure 6.23 highlights the influence of Eve's number of antennas on the 10%−achievable SR performances, for different N_A. Between each sub-plot, the BOR factor and/or the CSI estimation error are made variable. First, one can observe that the 10%−achievable SR decreases when N_E increases or N_A decreases. In addition, when the spreading factor increases, the 10%−achievable SR stays positive for larger number of eavesdropping antennas. In addition, for a given number of Alice's antennas and estimation error, higher BOR values allow to keep positive outage performances for higher number of Eve's antennas.

6.2.7 Conclusions on MISO system

The first part of this chapter highlights the secrecy performances of the MISO system, in the presence of one or multiple cooperative passive eavesdroppers.

Analytic derivation methodology
Three scenarios are presented depending on the TDD handshake procedures between Alice and Bob. For each scenario, an approximation of the ergodic secrecy rate is derived. It is shown that the approximations fit well the exact ergodic secrecy rate performances obtained via simulations, and are therefore used as closed-form expressions throughout this chapter to derive a certain number of useful metrics.
As for the SISO system, the communication parameters are designed in order to **guarantee a targeted per-symbol ESR**. To do so, worst case assumptions in terms of secrecy are considered, such has Eve being equipped with a noise-free hardware and/or is situated close to Alice, i.e., Eve having an arbitrarily large SNR, or Eve being equipped with an arbitrarily large number of antennas.
The analytic model of the ESR, depending on the investigated scenario, allows Alice to determine an analytic expression of the required SNR at Bob to guarantee Δ bit per channel use of secure rate. Thanks to this expression, Alice is able to derive:

- the maximal allowed main CSI error she can perform,
- the maximal number of allowed eavesdropping antennas,
- the optimal amount of data energy to inject.

Main results
The secrecy performances of the MISO system are similar to the ones obtained with the SISO system, but are enhanced when Alice's number of antennas increases. The same conclusions as for the SISO system can therefore be drawn.

It is shown that Alice's choice on the BOR value of the communication results from a trade-off. Knowing the CSI error variance and Bob's SNR, it is preferable for Alice to communicate at lower BORs to maximize the secure ergodic communication rate. However, if low outage percentages are desired, Alice is recommended to communicate at higher BOR values.
When the handshake procedures 1 or 2 are considered, i.e., SDS or OC decoders at Eve, the trade-off arises when very low outage percentages are allowed (typically lower than 0.1%) and/or if Alice strongly misestimates Bob's CSI. When N_A increases, lower outage percentages are allowed.
When the handshake procedure between Alice and Bob allows Eve to implement an MRC decoder, i.e., handshake procedure 3, this trade-off occurs for larger percentages of outage (typically more than 1%) and when Alice more accurately estimates Bob's CSI.

In addition, it is observed that Eve's number of antennas does not influence the secrecy performances of the SDS scenario. More, for the OC scenario, the worst-case situation is obtained with $N_E = 1$, i.e., it is penalizing for Eve to be equipped with a multi-antenna receiving structure. Therefore, in the context of IoT, it can be concluded that the SDS and OC scenarios are very promising to secure a DL communication between a multi-antenna BS and a single-antenna UE. Indeed, it is proven that Alice

can guarantee a positive ESR while keeping low outage percentages, regardless the number of Eve's antennas. These schemes are therefore robust against passive eavesdropping.
However, when the eavesdropper implements an MRC receiver, its number of antennas strongly impacts the secrecy performances. Indeed, Eve benefits from a frequency diversity gain as well as an array gain, therefore leading to high decoding capabilities, i.e., to low secrecy performances. No secrecy performance can therefore be a-priori guaranteed by Alice.

Table 6.2 summarizes the performances of the MISO system.

Table 6.2: MISO system: secrecy performance summary

	MISO-ME SDS	**MISO-ME OC**	**MISO-ME MRC**
Guaranteed ESR expression	Equation (6.36), Fig. 6.5 and 6.6. ESR is independent of N_E. It increases with an increase of N_A. Indeed, Bob's capacity is enhanced when N_A increases, and Eve's capacity is independent of N_A. It decreases with an increase of U, or an increase of σ. It stays positive for large CSI errors and high BORs.	Equation (6.38), Fig. 6.7, 6.8, and 6.9. Worst case obtained for $N_E = 1$. It increases with an increase of N_A. Indeed, Bob's capacity is enhanced when N_A increases, and Eve's capacity is penalized when N_A increases. Highest secrecy performances obtained, i.e., lowest capabilities at Eve. Same conclusions as for the MISO-ME SDS scenario.	Equation (6.41), Fig. 6.10 and 6.11. ESR decreases with an increase of N_E, U, or σ. It increases with an increase of N_A. For large σ and N_E, it is more likely to communicate at higher BORs to obtain positive ESRs. Lowest secrecy performances since Eve benefits from an array gain and a frequency diversity gain due to the MRC decoder.
Impact of imperfect CSI estimation	Equation (6.44), Fig. 6.14. $\sigma_{\max}^{\text{SDS}}$ decreases if Δ or U increase. $\sigma_{\max}^{\text{SDS}}$ increases if N_A increases. Perfect estimation needed if an arbitrarily large ESR aims to be targeted. Always possible to guarantee a positive ESR, i.e., $\sigma_{\max}^{\text{SDS}} = 1$ if $\Delta \to 0^+$.	Equation (6.45), Fig. 6.15. Same conclusions as for MISO-ME SDS, but less stricter conditions than (6.44) to achieve the same secrecy performances.	Equation (6.46), Fig. 6.16. $\sigma_{\max}^{\text{MRC}}$ decreases if Δ, or N_E, or U increase. $\sigma_{\max}^{\text{MRC}}$ increases if N_A increases. Perfect estimation needed if an arbitrarily large ESR aims to be targeted. Not always possible to ensure a positive ESR, i.e., $\sigma_{\max}^{\text{MRC}} < 1$ if $\Delta \to 0^+$. Much stricter conditions than for the SDS and OC scenarios.
Condition on maximal N_E	No condition since ESR independent of N_E.	No condition since worst-case scenario obtained for $N_E = 1$.	Equation (6.43), Fig. 6.12 and 6.13. $N_{E,\max}$ decreases with an increase of the maximal ESR that can be targeted. It slightly increases with an increase of N_A. It decreases with an increase of U, except at low ESRs where the frequency diversity gain predominates the rate decrease due to the spreading. It is very sensible to Alice's main CSI estimation accuracy.
Required SNR at Bob	Equation (6.37), Fig. 6.17. $\delta_{\text{B}}^{\text{SDS}}$ increases if U or Δ increase. It decreases if N_A increases.	Equation (6.40), Fig. 6.18. Same conclusions as for the MISO-ME SDS scenario, but slightly lower SNRs required to achieve the same secrecy performances.	Equation (6.42), Fig 6.19 and 6.20. $\delta_{\text{B}}^{\text{SDS}}$ increases if U, or Δ, or N_E increase. More sensible to the CSI accuracy than the other scenarios. It decreases if N_A increases. Much higher required SNRs to achieve the same secrecy performances compared to SDS and OC scenarios.
Outage consideration	Fig. 6.21. Higher BORs are desired to maximize the $\epsilon-$achievable SR when low outage percentages are desired, whatever σ_{dB}, N_A, and N_E. In particular, N_E does not influence the outage performances.	Fig. 6.22. Same conclusions as for the MISO-ME SDS scenario. However, increasing N_E increases the outage performances. In addition, lower outage performance are obtained compared to the MISO-ME SDS scenario.	Fig. 6.24 and 6.23. $\epsilon-$achievable SR decreases when N_E increases. It increases when N_A increases. Higher BORs are desired to keep positive $\epsilon-$achievable SR when σ_{dB} or N_E increases.
Performance summary	High ESR values since very poor decoding performance at Eve. Secrecy performances do not depend on N_E. Eve does not benefit from frequency diversity. In particular, Eve's EC is identical to the SISO-ME SDS EC. Lower BORs enhance the ESR. Higher BORs are desired to increase the $\epsilon-$achievable SR when low outage percentages are allowed. It therefore exists a trade-off on the BOR design.	Highest secrecy performances, i.e., lowest decoding capabilities at Eve. The worst-case scenario is obtained for the single-antenna eavesdropper scenario. The same conclusions can be drawn as for the MISO-ME SDS scenario.	Lowest secrecy performances since MRC at Eve, leading to a frequency diversity gain. The choice on the BOR value results from a trade-off. Alice can choose a BOR value either to maximize the ESR and the $\epsilon-$achievable secrecy rate by decreasing the BOR value, if N_E and σ are not too large. However, it is more likely to communicate at higher BORs if Eve is equipped with a large number of antennas, or if Alice's CSI estimation accuracy decreases.

6.3 Single-Input Multi-Output

6.3.1 Introduction

In this second part of the chapter, the secrecy performances of a SIMO system are assessed. As a reminder, two SIMO schemes are investigated depending on whether Alice does precode or not the transmitted data.

A SIMO system may correspond to a secure UL communication between a single-antenna UE (here, Alice) and a multi-antenna BS (here, Bob), in the presence of a single or multi-antenna eavesdropper, as depicted in Figure 4.9.

6.3.2 Assumptions

As a reminder, the dimensions and the natures of the matrices in a SIMO system are given in section 4.5.3. To study the SIMO system, several assumptions are undertaken:

- There are Q subcarriers per OFDM block, with a BOR of U, and $N = Q/U$ data symbols are transmitted per OFDM block.
- Alice possesses $N_A = 1$ antenna.
- Bob possesses $N_B > 1$ antennas.
- Eve possesses $N_E = 1$ antenna in a SIMO-SE configuration, or $N_E > 1$ antenna in a SIMO-ME configuration.
- No spatial correlation between Bob's antennas is assumed.
- No spatial correlation between Eve's antennas is assumed.
- No spatial correlation between Bob's antennas and Eve's antenna is assumed.
- No frequency correlation amongst Bob's subcarriers is assumed, i.e., $h_{B,k,i} \perp\!\!\!\perp h_{B,k,j}$, $\forall k = 1...N_B$, $\forall i \neq j$, $i = 1...Q$, $j = 1...Q$.
- No frequency correlation amongst Eve's subcarriers is assumed, i.e., $h_{E,k,i} \perp\!\!\!\perp h_{E,k,j}$, $\forall k = 1...N_E$,$\forall i \neq j$, $i = 1...Q$, $j = 1...Q$.
- No frequency correlation amongst the estimated error's subcarriers made by Alice and Bob's subcarriers is assumed, i.e., $h_{B,k,i} \perp\!\!\!\perp \Delta h_{B,k,j}$, $\forall k = 1...N_B$, $\forall i, j = 1...Q$.
- No frequency correlation amongst the estimated error's subcarriers made by Alice is assumed, i.e., $\Delta h_{B,k,i} \perp\!\!\!\perp \Delta h_{B,k,j}$, $\forall k = 1...N_B$, $\forall i \neq j$, $i = 1...Q$, $j = 1...Q$.

The uncorrelated spatial and frequency assumptions are justified similarly to the MISO system(see section 6.2.2).

The communication parameters used to study the SIMO system are given in Table 6.3:

Symbol	Description	Value
α	Ratio between the useful and the total signal power.	$\alpha \in [0,1]$
σ	CSI estimation error variance.	$\sigma \in [0,1]$
σ_{dB}	CSI estimation error variance in dB.	$\sigma_{\text{dB}} \in \mathbb{R}^-$
ϵ	Fraction of outage.	$\epsilon \in [0,1]$
Δ	Targeted ergodic secrecy rate in bit/channel use.	$\Delta \in \mathbb{R}^+$
Q	# of OFDM subcarriers.	$Q = 256$
U	Spreading factor.	$U = 2^n$, $n \in \{2,4,8,16,32\}$
N	# of symbols per OFDM block.	$N = Q/U$
N_A	# of antenna at Alice.	$N_A = 1$
N_B	# of antennas at Bob.	$N_B > 1$
N_E	# of antenna(s) at Eve.	$N_E \geq 1$

Table 6.3: SIMO communication parameters

6.3.3 Preliminaries

For both SIMO schemes, the expressions of the received signals at Bob and Eve's positions, the decoding structures implemented at Eve, as well as the AN generation condition, are recalled in this section to facilitate the reader's understanding.

As a reminder, Bob's ESINR is given by:

$$\mathbb{E}\left[\gamma_B\right] = \mathbb{E}\left[\frac{|B_1|^2}{|B_2+B_3|^2}\right], \tag{6.50}$$

with B_1, B_2, and B_3 being respectively the data, noise, and AN components of the received signal at Bob. An approximation of Bob's ESINR for a particular symbol n is given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] \approx \frac{\mathbb{E}\left[|B_{1,n}|^2\right]}{\mathbb{E}\left[|B_{2,n}|^2\right] + \mathbb{E}\left[|B_{3,n}|^2\right]}. \tag{6.51}$$

At Eve, depending on the decoder, the ESINR is given by:

$$\mathbb{E}\left[\gamma_E^{\text{D}}\right] = \mathbb{E}\left[\frac{\left|E_1^{\text{D}}\right|^2}{\left|E_2^{\text{D}}+E_3^{\text{D}}\right|^2}\right], \tag{6.52}$$

with E_1^{D}, E_2^{D}, and E_3^{D} respectively being the data, noise, and AN components of the received signal at Eve. From (6.52), an approximation of the ESINR of the n^{th} symbol is:

$$\mathbb{E}\left[\gamma_{E,n}^{\text{D}}\right] \approx \frac{\mathbb{E}\left[\left|E_{1,n}^{\text{D}}\right|^2\right]}{\mathbb{E}\left[\left|E_{2,n}^{\text{D}}\right|^2\right] + \mathbb{E}\left[\left|E_{3,n}^{\text{D}}\right|^2\right]} \tag{6.53}$$

6.3.3.1 Scheme 1 : SIMO without precoding

The block diagram of the SIMO scheme without data precoding is depicted in Figure 4.9.

Received signal expressions

From chapter 4, in a SIMO system without precoding made by Alice, the received signal at Bob is

given by (see equation (4.25)):

$$\begin{aligned}\mathbf{y}_{\mathbf{B}}^{\text{SIMO, no precod}} = &\underbrace{\sqrt{\alpha(1-\sigma)}\mathbf{S}^H\sum_{k=1}^{N_B}||\mathbf{H}_{\mathbf{B},k}||^2\mathbf{S}\mathbf{x}+\sqrt{\alpha\sigma}\mathbf{S}^H\sum_{k=1}^{N_B}\mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}_{\mathbf{B},k}^H\mathbf{S}\mathbf{x}}_{B_1}\\ &+\underbrace{\sqrt{(1-\alpha)\sigma}\mathbf{S}^H\sum_{k=1}^{N_B}\mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}_{\mathbf{B},k}^H\mathbf{w}+\mathbf{S}^H\sum_{k=1}^{N_B}\widehat{\mathbf{H}}_{\mathbf{B},k}^H\mathbf{v}_{\mathrm{B},k}}_{B_2}\\ &+\underbrace{\sqrt{(1-\alpha)(1-\sigma)}\mathbf{S}^H\sum_{k=1}^{N_B}||\mathbf{H}_{\mathbf{B},k}||^2\mathbf{w}}_{B_3}.\end{aligned} \tag{6.54}$$

At the eavesdropper's position, the received sequence is given by:

$$\mathbf{y}_{\mathrm{E}}^{\text{SIMO, no precod},\mathbf{D}} = \underbrace{\sqrt{\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\mathbf{S}\mathbf{x}}_{E_1^{\mathrm{D}}}+\underbrace{\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{D}_{\mathbf{E},k}\mathbf{v}_{\mathrm{E},k}}_{E_2^{\mathrm{D}}}+\underbrace{\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{D}_{\mathbf{E},k}\mathbf{H}_{\mathbf{E},k}\mathbf{w}}_{E_3^{\mathrm{D}}}, \tag{6.55}$$

where $\mathbf{D}_{\mathbf{E},k}$ is a $Q\times Q$ decoding matrix whose nature depends on the investigated scenario, i.e., on the handshake procedure between Alice and Bob.

Decoding structure at Eve

It was seen in section 4.6.3.4 that, when Alice does not precode the transmitted data, Bob must know his CSI in order to implement an MRC receiver. This is possible only if Alice sends an unprecoded pilot to Bob, which also allows Eve to perfectly estimate her own CSI. From that, she is able to implement an MRC decoder as well. Consequently, in the SIMO-ME without precoding scheme, only one decoding scheme is investigated at Eve. That is, Eve implements:

$$\mathbf{D}_{\mathbf{E}}^{\mathrm{MRC}} = \mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{H}_{\mathbf{E},k}^H. \tag{6.56}$$

The received signal at Eve is therefore expressed as:

$$\mathbf{y}_{\mathrm{E}}^{\text{SIMO, no precod}} = \underbrace{\sqrt{\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}||\mathbf{H}_{\mathbf{E},k}||^2\mathbf{S}\mathbf{x}}_{E_1^{\mathrm{MRC}}}+\underbrace{\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{H}_{\mathbf{E},k}^H\mathbf{v}_{\mathrm{E},k}}_{E_2^{\mathrm{MRC}}}+\underbrace{\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_E}||\mathbf{H}_{\mathbf{E},k}||^2\mathbf{w}}_{E_3^{\mathrm{MRC}}}, \tag{6.57}$$

AN generation

In a SIMO-ME system without data precoding, the AN is generated such that:

$$\mathbf{S}^H\sum_{k=1}^{N_B}\left|\left|\widehat{\mathbf{H}}_{\mathbf{B},k}\right|\right|^2\mathbf{w} = \mathbf{0}_N. \tag{6.58}$$

6.3.3.2 Scheme 2 : SIMO with precoding

The block diagram of the SIMO scheme with data precoding is depicted in Figure 4.10.

Received signal expressions
From chapter 4, in a SIMO system with data precoding made by Alice, the received signal at Bob is given by (see equation (4.32)):

$$\mathbf{y}_{\mathbf{B}}^{\text{SIMO, precod}} = \underbrace{\sqrt{\frac{\alpha}{N_B}}\mathbf{S}^H \sum_{k=1}^{N_B}\sum_{k'=1}^{N_B} \mathbf{H}_{\mathbf{B},k}\widetilde{\mathbf{H}}_{\mathbf{B},k'}\mathbf{S}\mathbf{x}}_{B_1} + \underbrace{\mathbf{S}^H \sum_{k=1}^{N_B}\mathbf{v}_{\text{B}}}_{B_2} + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_B}\mathbf{H}_{\mathbf{B},k}\mathbf{w}}_{B_3}. \tag{6.59}$$

As a reminder, the scaling factor $\frac{1}{\sqrt{N_B}}$ ensures energy normalization at the transmitter side, i.e., it ensures a total energy per transmitted symbol of 1.
At the eavesdropper's position, the received sequence is given by:

$$\mathbf{y}_{\text{E}}^{\text{SIMO, precod,}\mathbf{D}} = \underbrace{\sqrt{\frac{\alpha}{N_B}}\mathbf{S}^H \sum_{k=1}^{N_B}\sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k}^H\mathbf{D}_{\mathbf{E},l}\mathbf{H}_{\mathbf{E},l}\mathbf{S}\mathbf{x}}_{E_1^{\text{D}}} + \underbrace{\mathbf{S}^H \sum_{l=1}^{N_E}\mathbf{D}_{\mathbf{E},l}\mathbf{v}_{\text{E},l}}_{E_2^{\text{D}}} + \underbrace{\sqrt{\frac{(1-\alpha)}{N_B}}\mathbf{S}^H \sum_{l=1}^{N_E}\mathbf{D}_{\mathbf{E},l}\mathbf{w}}_{E_3^{\text{D}}}, \tag{6.60}$$

where $\mathbf{D}_{\mathbf{E},l}$ is a $Q \times Q$ decoding matrix whose nature depends on the investigated scenario, i.e., on the handshake procedure between Alice and Bob.

Decoding structures at Eve
The decoding structures at Eve are given in Sections 4.6.3.

TDD handshake procedure SIMO precoding 1: same decoding structure decoder.

The handshake procedure is presented in Figure 4.12. Eve is only able to know $\mathbf{H_{BE}}$ which is of no help. She implements the same decoding structure as Bob:

$$\mathbf{D}_{\mathbf{E}}^{\text{SDS}} = \mathbf{S}^H \sum_{k=1}^{N_E}\mathbf{I}_Q. \tag{6.61}$$

TDD handshake procedure SIMO precoding 2: own channel decoder.

The handshake procedure is presented in Figure 4.13. Eve implements a decoding structure that takes benefit from her own channel knowledge:

$$\mathbf{D}_{\mathbf{E}}^{\text{OC}} = \mathbf{S}^H \sum_{k=1}^{N_E}\mathbf{H}_{\mathbf{E},k}^H. \tag{6.62}$$

TDD handshake procedure SIMO precoding 3: maximum ratio combining decoder.

The handshake procedure is presented in Figure 4.14. Eve can access to the knowledge of her equivalent channel. She therefore implements an MRC decoding structure:

$$\mathbf{D}_{\mathbf{E}}^{\text{MRC}} = \mathbf{S}^H \frac{1}{\sqrt{N_B}} \sum_{k=1}^{N_B}\sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{H}_{\mathbf{E},l}^H. \tag{6.63}$$

AN generation
In a SIMO-ME system with data precoding, the AN signal is designed such that:

$$\mathbf{S}^H \sum_{k=1}^{N_B}\widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{w} = \mathbf{0}_N. \tag{6.64}$$

6.3.4 Ergodic secrecy rate modeling

As for the SISO system investigated in Chapter 5 and the MISO system investigated in section 6.2, the metric of interest is the ESR, defined in (5.11). In order to obtain a model for the ESR, analytic expressions of the ESINRs must be determined. In the following, the ESINR expressions for the two considered SIMO schemes are derived.

6.3.4.1 Scheme 1 : SIMO without precoding

6.3.4.1.1 Bob's ergodic SINR

From (6.54), the received components at Bob, when no data precoding is implemented at the transmitting side, are:

$$B_{1,n} = \frac{\sqrt{\alpha(1-\sigma)}}{U} \sum_{k=1}^{N_B} \sum_{i=0}^{U-1} |h_{\mathrm{B},k,i}|^2 + \frac{\sqrt{\alpha\sigma}}{U} \sum_{k=1}^{N_B} \sum_{i=0}^{U-1} h_{\mathrm{B},k,i} \Delta h^*_{\mathrm{B},k,i}, \tag{6.65a}$$

$$B_{2,n} = \frac{1}{\sqrt{U}} \sum_{k=1}^{N_B} \sum_{i=0}^{U-1} \hat{h}^*_{\mathrm{B},k,i} v_{\mathrm{B},k,i} \tag{6.65b}$$

$$B_{3,n} = \sqrt{\frac{1-\alpha}{U}} \sum_{k=1}^{N_B} \sum_{i=0}^{U-1} h_{\mathrm{B},k,i} \hat{h}^*_{\mathrm{B},k,i} w_i. \tag{6.65c}$$

As detailed in Appendices E.1.1.1, E.1.1.2, and E.1.1.3, the components can respectively be derived as:

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \frac{\alpha N_B}{U} \left[U N_B (1-\sigma) + 1\right] \tag{6.66a}$$

$$\mathbb{E}\left[|B_{2,n}|^2\right] = N_B \sigma^2_{\mathrm{B}} \tag{6.66b}$$

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha) N_B \sigma}{U}. \tag{6.66c}$$

Bob's noise variance is defined as:

$$\sigma^2_{\mathrm{B}} = \frac{1}{U \delta_B}, \tag{6.67}$$

where δ_B is the SNR at Bob in linear scale, and $1/U$ is the received energy per symbol component. Introducing (6.66a), (6.66b), and (6.66c) into (6.51), the per-symbol approximated ESINR at Bob in a SIMO-ME system without precoding is given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] \approx \frac{\frac{\alpha N_B}{U} \left[U N_B (1-\sigma) + 1\right]}{N_B \sigma^2_{\mathrm{B}} + \frac{(1-\alpha) N_B \sigma}{U}} = \frac{\alpha \left[U N_B (1-\sigma) + 1\right]}{U \sigma^2_{\mathrm{B}} + (1-\alpha)\sigma}. \tag{6.68}$$

The approximated EC at Bob is therefore expressed as:

$$C_B \approx \log_2\left(1 + \mathbb{E}\left[\gamma_{B,n}\right]\right) = \log_2\left(1 + \frac{\alpha \left[U N_B (1-\sigma) + 1\right]}{U \sigma^2_{\mathrm{B}} + (1-\alpha)\sigma}\right). \tag{6.69}$$

Bob's approximated EC in a SIMO without data precoding scheme is identical to Bob's approximated EC in a MISO configuration (6.13), with N_A replaced by N_B. This can be understood since, in both situations, an MRC decoding structure is considered either at TX (MISO) or RX (SIMO).

Figure 6.25 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_B$) with the approximated EC at Bob (C_B) given in (6.69), for different number of Bob's antennas, with different spreading factors and/or CSI estimation errors between each sub-figure, and at fixed SNR $\delta_B = 10$dB. The exact EC is found by Monte Carlo simulations, and is given by:

$$\widehat{C}_B = \mathbb{E}\left[\log_2\left(1 + \gamma_{B,n}\right)\right]. \tag{6.70}$$

From Figure 6.25, one observes that (6.69) fits well the exact EC and can therefore be used as a closed-form approximation for the rest of this study. As expected, Bob's EC increases if he is equipped with a growing number of antennas. In addition, the channel capacity increases if the BOR factor increases. Finally, it is seen that the EC is affected when Alice misestimates Bob's CSI.

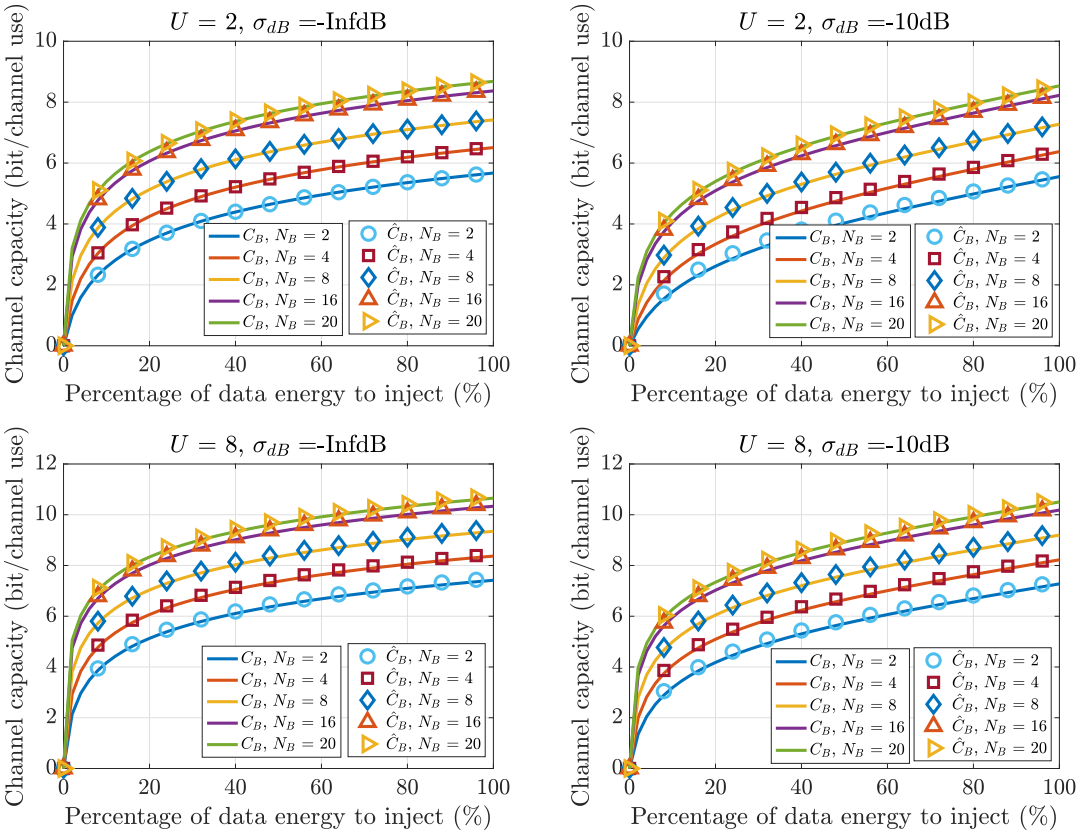

Figure 6.25: Comparison between approximated EC and exact EC at Bob: SIMO without precoding, $\delta_B = 10$dB, 100.000 realizations

6.3.4.1.2 Eve's ergodic SINR

The derivation of Eve's ESINR is conducted in this section for the scenario where she implements an MRC decoder. From (6.57), the received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\text{MRC}} = \frac{\sqrt{\alpha}}{U} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} |h_{\text{E},k,i}|^2 \tag{6.71a}$$

$$E_{2,n}^{\text{MRC}} = \frac{1}{\sqrt{U}} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} h_{\text{E},k,i}^* v_{\text{E},k,i} \tag{6.71b}$$

$$E_{3,n}^{\text{MRC}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}} \sum_{k=1}^{N_E} \sum_{i=0}^{U-1} |h_{\text{E},k,i}|^2 w_i. \tag{6.71c}$$

As detailed in Appendices E.2.1.1, E.2.1.2, and E.2.1.3, the components can respectively be derived as:

$$\mathbb{E}\left[|E_{1,n}^{\text{MRC}}|^2\right] = \frac{\alpha}{U} N_E (U N_E + 1) \tag{6.72a}$$

$$\mathbb{E}\left[|E_{2,n}^{\text{MRC}}|^2\right] = N_E \sigma_{\text{E}}^2 \tag{6.72b}$$

$$\mathbb{E}\left[|E_{3,n}^{\text{MRC}}|^2\right] = (1-\alpha) \frac{N_E \left(1 + \frac{N_E}{N_B+1}\right)}{U}. \tag{6.72c}$$

Eve's noise variance is defined as:

$$\sigma_{\mathrm{E}}^2 = \frac{1}{U\delta_E}, \tag{6.73}$$

where δ_E is the SNR at Eve in linear scale, and $1/U$ is the received energy per symbol component. Introducing (6.72a), (6.72b), and (6.72c) into (6.53), the per-symbol approximated ESINR at Eve in a SIMO-ME system without precoding is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right] \approx \frac{\frac{\alpha}{U}N_E(UN_E+1)}{N_E\sigma_{\mathrm{E}}^2 + (1-\alpha)\frac{N_E\left(1+\frac{N_E}{N_B+1}\right)}{U}} = \frac{\alpha(UN_E+1)}{U\sigma_{\mathrm{E}}^2 + (1-\alpha)\left(1+\frac{N_E}{N_B+1}\right)}. \tag{6.74}$$

From (6.74), it is interesting to note that Eve's ESINR depends on Bob's number of antennas. In particular, it increases when N_B increases.
From (6.74), the approximated EC at Eve is expressed as:

$$C_E^{\mathrm{MRC}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right]\right) = \log_2\left(1+\frac{\alpha(UN_E+1)}{U\sigma_{\mathrm{E}}^2 + (1-\alpha)\left(1+\frac{N_E}{N_B+1}\right)}\right). \tag{6.75}$$

The exact EC is found by Monte Carlo simulations (100.000 realizations) as:

$$\widehat{C}_E^{\mathrm{MRC}} = \mathbb{E}\left[\log_2\left(1+\gamma_{E,n}^{\mathrm{MRC}}\right)\right]. \tag{6.76}$$

Figure 6.26 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_E^{\mathrm{MRC}}$) with the approximated EC at Eve (C_E^{MRC}), for different number of Eve's antennas, with different spreading factors and/or CSI estimation errors between each sub-figure, at fixed SNR $\delta_E = 10$dB, and at fixed $N_B = 8$.

From Figure 6.26, one observes that (6.75) fits well the exact EC, and can therefore be used as a closed-form approximation for the rest of this study. As expected, Eve's EC increases if she is equipped with a larger number of antennas. In addition, the channel capacity increases if the BOR factor increases.

Figure 6.27 outlines the evolution of Eve's EC as a function of Bob's number of antennas. It is observed that the channel capacity increases when Bob is equipped with more antennas. Indeed, as seen in (6.72c), the ergodic energy of the AN term is inversely proportional to N_B, i.e., Eve EC is proportional to N_B.

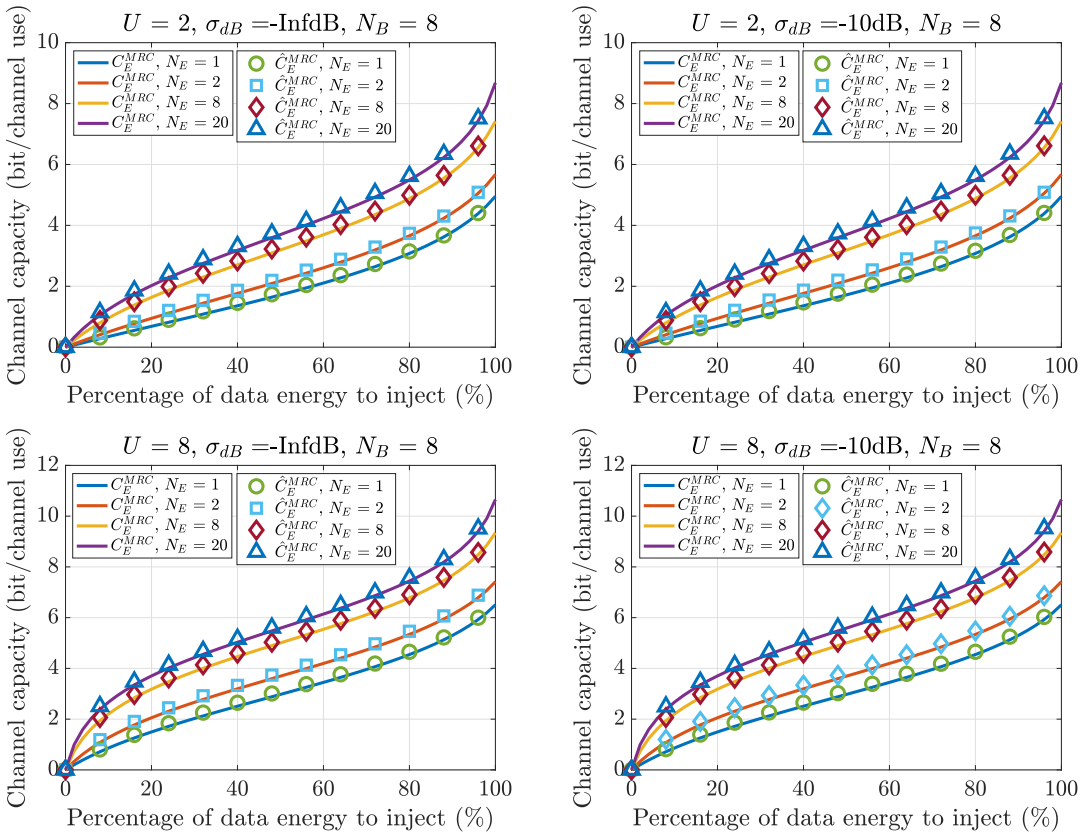

Figure 6.26: Comparison between approximated EC and exact EC at Eve: SIMO without precoding, $\delta_E = 10$dB, 100.000 realizations

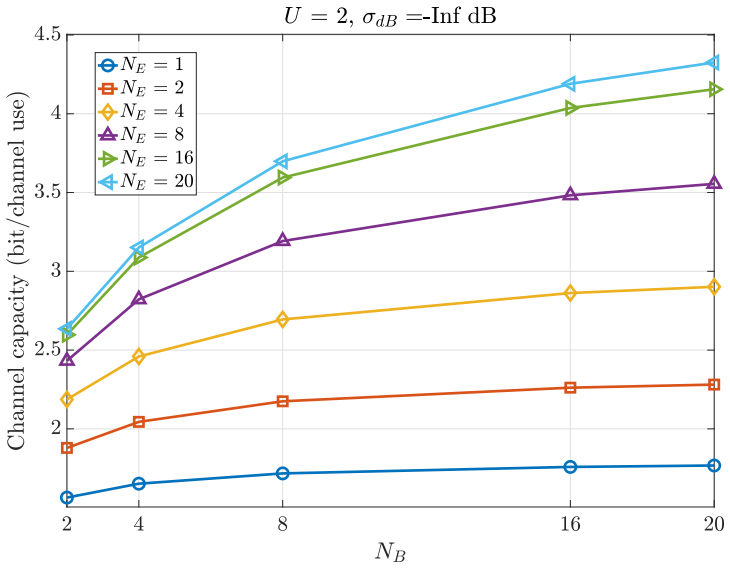

Figure 6.27: Eve's EC as a function of N_B, SIMO without precoding, $\delta_E = 10$dB

From the definition of Eve's ESINR (6.74), one can conclude that Eve's ESINR is an increasing function in N_E, which is upper bounded when $N_E \to +\infty$. Considering the worst case scenario, i.e., $\sigma_{\mathrm{E}}^2 = 0$, it comes:

$$\left.\frac{\alpha(N_B+1)(U+1)}{(1-\alpha)(N_B+2)}\right|_{N_E=1} \leq \mathbb{E}\left[\gamma_{E,n}^{\mathrm{MRC}}\right] \leq \left.\frac{\alpha U(N_B+1)}{(1-\alpha)}\right|_{N_E\to+\infty}. \tag{6.77}$$

Eve's approximated EC upper bound takes the following form:

$$C_E^{\mathrm{MRC,UP}}\Big|_{N_E\to+\infty} \approx \log_2\left(1+\frac{\alpha U(N_B+1)}{(1-\alpha)}\right). \tag{6.78}$$

Figure 6.28 compares C_E^{MRC} defined in (6.75), as a function of N_E, with the upper bound $C_E^{\mathrm{MRC,UP}}$ defined in (6.78).

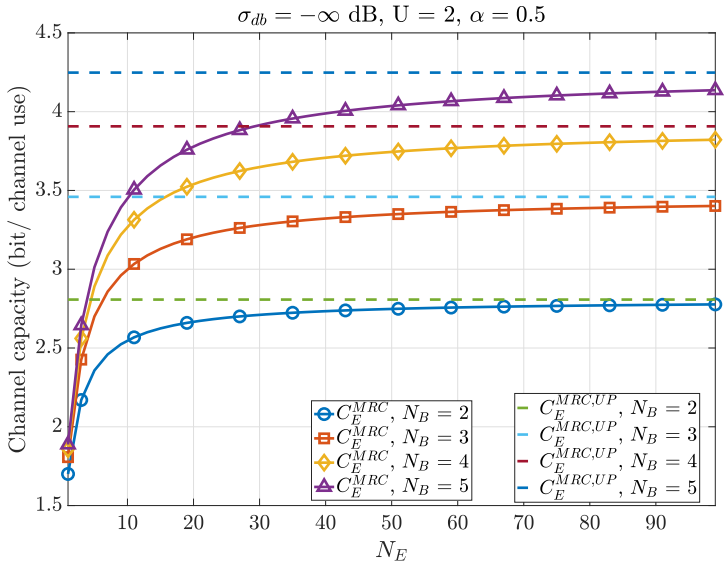

Figure 6.28: Eve's EC as a function of N_B, SIMO without precoding, $\delta_E = 10$dB

It is observed that Eve's capacity comes close to its bound (6.78) when N_E increases, and that the bound remains an upper one for all values of N_E. Therefore, when $N_E \to +\infty$, Eve has the highest decoding capabilities, which corresponds to the worst-case scenario in terms of secrecy. Consequently, only the scenario where Eve possesses an arbitrarily large number of antennas is investigated in next sections, related to the SIMO-ME scheme without data precoding.

Notation 6.1

To lighten the notations, since only the worst-case is investigated in a SIMO-ME scheme without data precoding, i.e., $N_E \to +\infty$, the superscript UP is omitted in the following of this chapter. Therefore, Eve's capacity in a SIMO-ME scheme without data precoding, when $N_E \to +\infty$, is written C_E^{MRC} instead of $C_E^{\mathrm{MRC,UP}}$.

6.3.4.2 Scheme 2 : SIMO with precoding

6.3.4.2.1 Bob's ergodic SINR

Bob's received signal is given by (6.59). Therefore, the received components at Bob, when Alice

implements a data precoding, are:

$$B_{1,n} = \frac{\sqrt{\alpha}}{\sqrt{N_B}U} \sum_{k=1}^{N_B} \sum_{k'=1}^{N_B} \sum_{i=0}^{U-1} h_{\mathrm{B},k,i} \hat{h}^*_{\mathrm{B},k',i}, \tag{6.79a}$$

$$B_{2,n} = \frac{1}{\sqrt{U}} \sum_{k=1}^{N_B} \sum_{i=0}^{U-1} v_{\mathrm{B},k,i} \tag{6.79b}$$

$$B_{3,n} = \sqrt{\frac{1-\alpha}{U}} \sum_{k=1}^{N_B} \sum_{i=0}^{U-1} h_{\mathrm{B},k,i} w_i. \tag{6.79c}$$

As detailed in Appendices E.1.2.1, E.1.2.2, and E.1.2.3, the components can respectively be derived as:

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \frac{\alpha N_B}{U}\left[U(1-\sigma)+1\right] \tag{6.80a}$$

$$\mathbb{E}\left[|B_{2,n}|^2\right] = N_B \sigma_{\mathrm{B}}^2 \tag{6.80b}$$

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)N_B\sigma}{U}. \tag{6.80c}$$

Introducing (6.80a), (6.80b), and (6.80c) into (6.51), the per-symbol approximated ESINR at Bob in a SIMO-ME system with data precoding is given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] \approx \frac{\frac{\alpha N_B}{U}\left[U(1-\sigma)+1\right]}{N_B\sigma_{\mathrm{B}}^2 + \frac{(1-\alpha)N_B\sigma}{U}} = \frac{\alpha\left[U(1-\sigma)+1\right]}{U\sigma_{\mathrm{B}}^2 + (1-\alpha)\sigma}. \tag{6.81}$$

From (6.81), it is seen that Bob's ESINR does not depend on the number of antennas he is equipped with. In particular, expression (6.81) is similar to Bob's ESINR expression in a SISO system (5.18). The approximated EC at Bob is therefore expressed as:

$$C_B \approx \log_2\left(1+\mathbb{E}\left[\gamma_{B,n}\right]\right) = \log_2\left(1+\frac{\alpha\left[U(1-\sigma)+1\right]}{U\sigma_{\mathrm{B}}^2 + (1-\alpha)\sigma}\right). \tag{6.82}$$

Figure 6.29 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_B$) with the approximated EC at Bob (C_B) obtained be Monte Carlo simulations (100.000 realizations), for different number of Bob's antennas, with different spreading factors and/or CSI estimation errors between each sub-figure, and at fixed SNR $\delta_B = 10$dB.

From Figure 6.29, one observes a good agreement between (6.82) and the exact EC, which is therefore used as a closed-form approximation for the rest of this study. As expected from Bob's ESINR approximation (6.81), the EC does not depend on N_B. However, it increases if the BOR factor increases, and decreases if Alice estimates less accurately Bob's CSI. It can also be verified that the EC values obtained in Figure 6.29 are similar to the ones obtained in a SISO-SE system, presented in Figure 5.1.

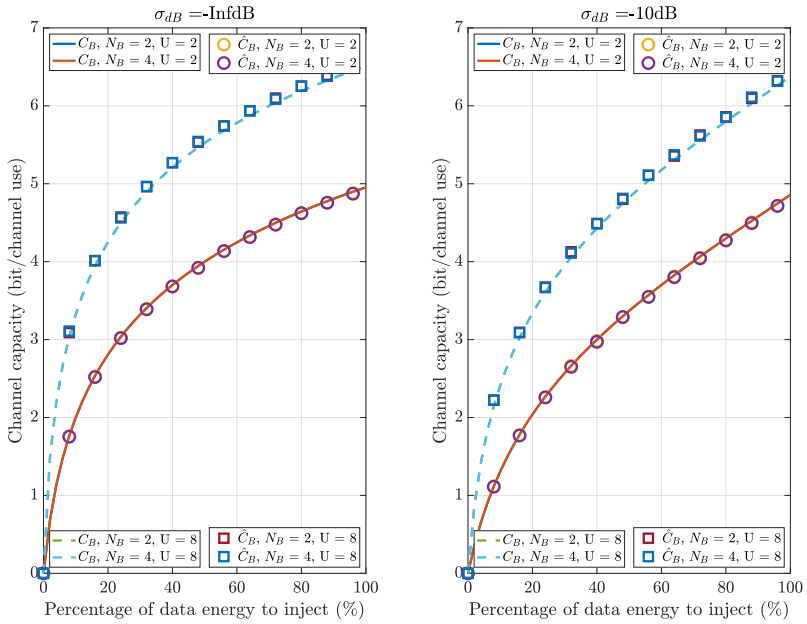

Figure 6.29: Comparison between approximated EC and exact EC at Bob: SIMO with precoding, $\delta_B = 10$dB, 100.000 realizations

6.3.4.2.2 Eve's ergodic SINR

The derivation of Eve's ESINR is conducted in this section for the three investigated TDD handshake procedures.

TDD handshake procedure SIMO precoding 1: same decoding structure decoder

When Eve implements an SDS decoder, by replacing (6.61) into (6.60), the received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{SDS}} = \underbrace{\frac{\sqrt{\alpha}}{\sqrt{N_B}}\mathbf{S}^H \sum_{k=1}^{N_B}\sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},l}\widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x}}_{E_1^{\mathrm{SDS}}} + \underbrace{\mathbf{S}^H \sum_{l=1}^{N_E} \mathbf{v}_{\mathrm{E},l}}_{E_2^{\mathrm{SDS}}} + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H \sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},l}\mathbf{w}}_{E_3^{\mathrm{SDS}}}. \tag{6.83}$$

From (6.83) , the received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\mathrm{SDS}} = \frac{\sqrt{\alpha}}{\sqrt{N_B U}} \sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},l,i}\hat{h}_{\mathrm{B},k,i}^* \tag{6.84a}$$

$$E_{2,n}^{\mathrm{SDS}} = \frac{1}{\sqrt{U}} \sum_{l=1}^{N_E}\sum_{i=0}^{U-1} v_{\mathrm{E},l,i} \tag{6.84b}$$

$$E_{3,n}^{\mathrm{SDS}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}} \sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},l,i} w_i. \tag{6.84c}$$

As detailed in Appendices E.2.2.1.1, E.2.2.1.2, and E.2.2.1.3, the components can respectively be derived as:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{SDS}}|^2\right] = \frac{\alpha N_E}{U} \tag{6.85a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{SDS}}|^2\right] = N_E\sigma_{\mathrm{E}}^2 \tag{6.85b}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{SDS}}|^2\right] = \frac{(1-\alpha)N_E}{U}. \tag{6.85c}$$

Eve's noise variance is defined as:

$$\sigma_{\mathrm{E}}^2 = \frac{1}{U\delta_E}, \tag{6.86}$$

where δ_E is the SNR at Eve in linear scale, and $1/U$ is the received energy per symbol component. Introducing (6.85a), (6.85b), and (6.85c) into (6.53), the per-symbol approximated ESINR at Eve in a SIMO-ME SDS scenario with data precoding is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{SDS}}\right] \approx \frac{\frac{\alpha N_E}{U}}{N_E\sigma_{\mathrm{E}}^2 + \frac{(1-\alpha)N_E}{U}} = \frac{\alpha}{U\sigma_{\mathrm{E}}^2 + (1-\alpha)}. \tag{6.87}$$

From (6.87), Eve's approximated ESINR is identical to the one obtained in a SISO-SE SDS scenario (see (5.27)). Indeed, in a SIMO-ME SDS scenario with data precoding at Alice, Eve benefits from an array gain N_E which similarly impacts her received symbol components (data, noise, and AN) in (6.85). This gain has therefore no impact on Eve's EC, and one comes back to the SISO-SE SDS scenario reported here for convenience:

$$C_E^{\mathrm{SDS}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{SDS}}\right]\right) = \log_2\left(1+\frac{\alpha}{U\sigma_{\mathrm{E}}^2+(1-\alpha)}\right). \tag{6.88}$$

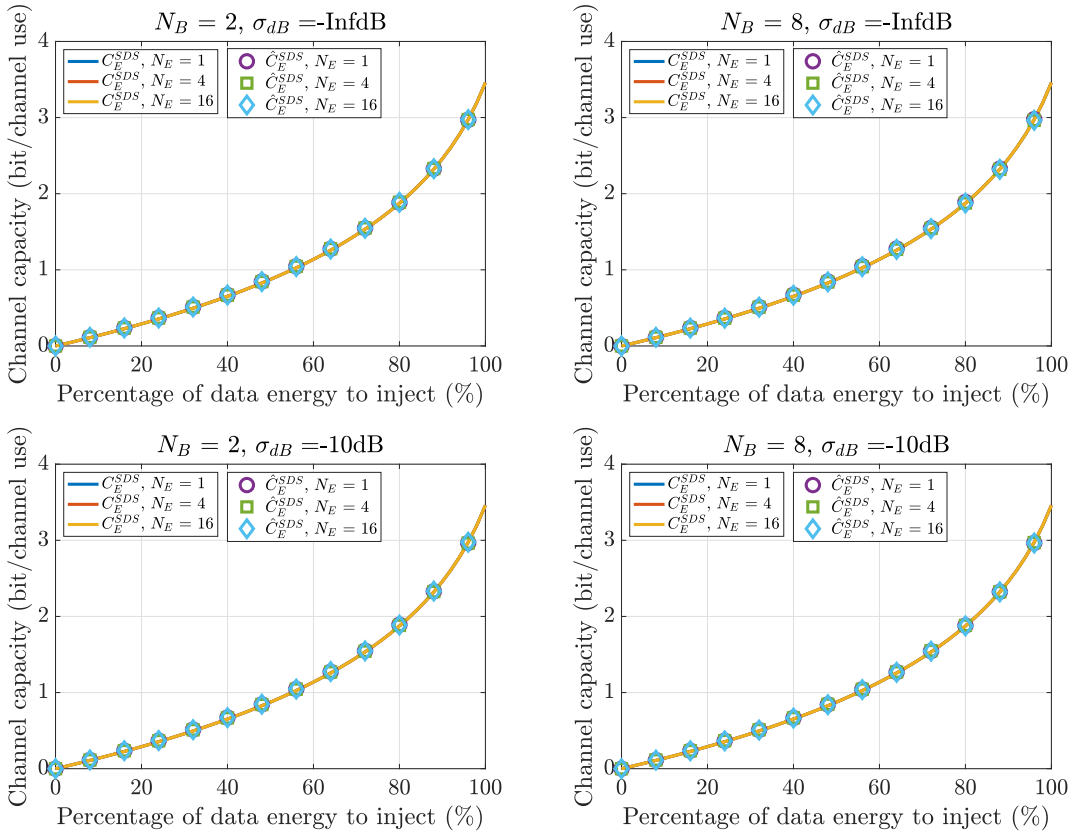

Figure 6.30: Comparison between approximated EC and exact EC at Eve: SIMO with precoding, SDS decoder, $\delta_E = 10$dB, 100.000 realizations

Figure 6.30 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_E^{\mathrm{SDS}}$) obtained by Monte Carlo simulations (100.000 realizations) with the approximated EC at Eve (C_E^{SDS}) given in (6.88), for different number of Eves antennas, with different number of Bob's antennas and/or CSI estimation errors between each sub-figure, at fixed SNR $\delta_E = 10$dB, and at fixed $U = 2$.

As anticipated from the above discussion, Eve's capacity does not depend on her number of antennas nor on Bob's number of antennas. Furthermore, one can observe that (6.88) fits well the exact EC, such that it can be used as a closed-form approximation for the rest of the study. In addition, the EC values observed in Figure 6.30 are identical to the ones obtained in Figure 5.2, which shows the EC at Eve in a SISO-SE SDS scenario.

TDD handshake procedure SIMO precoding 2: own channel decoder
When Eve implements a OC decoder, by replacing (6.62) into (6.60), her received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{OC}} = \underbrace{\frac{\sqrt{\alpha}}{\sqrt{N_B}}\mathbf{S}^H \sum_{k=1}^{N_B}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},l}||^2 \widehat{\mathbf{H}}_{\mathbf{B},k}^H \mathbf{S}\mathbf{x}}_{E_1^{\mathrm{OC}}} + \underbrace{\mathbf{S}^H \sum_{l=1}^{N_E} \mathbf{H}_{\mathbf{E},lk}^H \mathbf{v}_{\mathrm{E},l}}_{E_2^{\mathrm{OC}}} + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H \sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},l}||^2 \mathbf{w}}_{E_3^{\mathrm{OC}}}. \tag{6.89}$$

From (6.89), the received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\mathrm{OC}} = \frac{\sqrt{\alpha}}{\sqrt{N_B}U} \sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2 \hat{h}_{\mathrm{B},k,i}^* \tag{6.90a}$$

$$E_{2,n}^{\mathrm{OC}} = \frac{1}{\sqrt{U}} \sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},l,i}^* v_{\mathrm{E},l,i} \tag{6.90b}$$

$$E_{3,n}^{\mathrm{OC}} = \frac{\sqrt{1-\alpha}}{\sqrt{U}} \sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2 w_i. \tag{6.90c}$$

As detailed in Appendices E.2.2.2.1, E.2.2.2.2, and E.2.2.2.3, the components can respectively be derived as:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{OC}}|^2\right] = \frac{\alpha N_E(N_E+1)}{U} \tag{6.91a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{OC}}|^2\right] = N_E\sigma_{\mathrm{E}}^2 \tag{6.91b}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{OC}}|^2\right] = \frac{(1-\alpha)N_E(N_E+1)}{U}. \tag{6.91c}$$

Introducing (6.91a), (6.91b), and (6.91c) into (6.53), the per-symbol approximated ESINR at Eve in a SIMO-ME OC scenario with data precoding is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right] \approx \frac{\frac{\alpha N_E(N_E+1)}{U}}{N_E\sigma_{\mathrm{E}}^2 + \frac{(1-\alpha)N_E(N_E+1)}{U}} = \frac{\alpha(N_E+1)}{U\sigma_{\mathrm{E}}^2 + (1-\alpha)(N_E+1)}. \tag{6.92}$$

From (6.92), Eve's approximated ESINR is identical to the one obtained in a SISO-ME OC (see (5.70)). The approximated EC at Eve is therefore expressed as:

$$C_E^{\mathrm{OC}} \approx \log_2\left(1+\mathbb{E}\left[\gamma_{E,n}^{\mathrm{OC}}\right]\right) = \log_2\left(1+\frac{\alpha(N_E+1)}{U\sigma_{\mathrm{E}}^2 + (1-\alpha)(N_E+1)}\right). \tag{6.93}$$

Figure 6.31 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_E^{\mathrm{OC}}$) obtained by Monte Carlo simulations (100.000 realizations) with the approximated EC at Eve (C_E^{OC}) given in (6.93). The same set of parameters is considered as for the SIMO-ME SDS scenario, shown in Figure 6.30.

As anticipated from the above discussion, Eve's capacity does not depend on Bob's number of antennas. In addition, it is observed that Eve's EC slightly increases when N_E increases, mainly when $\alpha \to 1$, which can be anticipated from equation (6.92). Furthermore, one can observe that (6.93) fits well the exact EC, such that it can be used as a closed-form approximation for the rest of the study. In

addition, the EC values observed in Figure 6.31 are identical to the ones obtained in Figure 5.17, which shows the EC at Eve in a SISO-ME OC scenario.

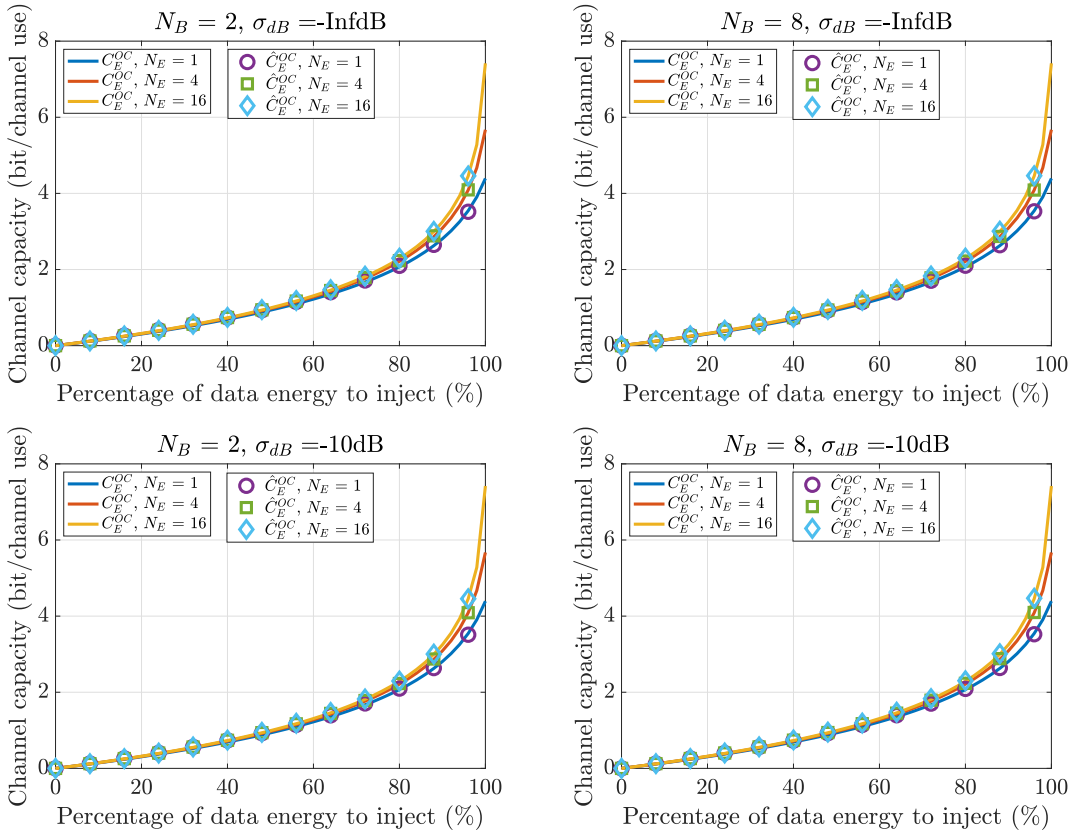

Figure 6.31: Comparison between approximated EC and exact EC at Eve: SIMO with precoding, OC decoder, $\delta_E = 10$dB, 100.000 realizations

TDD handshake procedure SIMO precoding 3: maximum ration combining decoder

When Eve implements a nMRC decoder, by replacing (6.63) into (6.60), her received signal becomes:

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{MRC}} = \underbrace{\frac{\sqrt{\alpha}}{N_B}\mathbf{S}^H \sum_{k=1}^{N_B}\sum_{k'=1}^{N_B}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},l}||^2 \widehat{\mathbf{H}}_{\mathbf{B},k}^H \widehat{\mathbf{H}}_{\mathbf{B},k'}\mathbf{S}\mathbf{x}}_{E_1^{\mathrm{MRC}}} + \underbrace{\frac{1}{\sqrt{N_B}}\mathbf{S}^H \sum_{k=1}^{N_B}\sum_{l=1}^{N_E} \widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{H}_{\mathbf{E},lk}^H \mathbf{v}_{\mathrm{E},l}}_{E_2^{\mathrm{MRC}}} + \underbrace{\frac{\sqrt{1-\alpha}}{\sqrt{N_B}}\mathbf{S}^H \sum_{k=1}^{N_B}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},l}||^2 \widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{w}}_{E_3^{\mathrm{MRC}}}. \tag{6.94}$$

From (6.94), the received n^{th} symbol components can be expressed as:

$$E_{1,n}^{\text{MRC}} = \frac{\sqrt{\alpha}}{N_B U} \sum_{k=1}^{N_B} \sum_{k'=1}^{N_B} \sum_{l=1}^{N_E} \sum_{i=0}^{U-1} |h_{\text{E},l,i}|^2 \hat{h}_{\text{B},k,i}^* \hat{h}_{\text{B},k',i} \tag{6.95a}$$

$$E_{2,n}^{\text{MRC}} = \frac{1}{\sqrt{N_B U}} \sum_{k=1}^{N_B} \sum_{l=1}^{N_E} \sum_{i=0}^{U-1} \hat{h}_{\text{B},k,i} h_{\text{E},l,i}^* v_{\text{E},l,i} \tag{6.95b}$$

$$E_{3,n}^{\text{MRC}} = \frac{\sqrt{1-\alpha}}{\sqrt{N_B U}} \sum_{k=1}^{N_B} \sum_{l=1}^{N_E} \sum_{i=0}^{U-1} \hat{h}_{\text{B},k,i} |h_{\text{E},l,i}|^2 w_i. \tag{6.95c}$$

As detailed in Appendices E.2.2.3.1, E.2.2.3.2, and E.2.2.3.3, the components can respectively be derived as:

$$\mathbb{E}\left[|E_{1,n}^{\text{MRC}}|^2\right] = \frac{\alpha N_E}{U} \left[N_E(U+1)+2\right] \tag{6.96a}$$

$$\mathbb{E}\left[|E_{2,n}^{\text{MRC}}|^2\right] = N_E \sigma_{\text{E}}^2 \tag{6.96b}$$

$$\mathbb{E}\left[|E_{3,n}^{\text{MRC}}|^2\right] = \frac{(1-\alpha)}{U+1} N_E. \tag{6.96c}$$

Introducing (6.96a), (6.96b), and (6.96c) into (6.53), the per-symbol approximated ESINR at Eve in a SIMO-ME MRC scenario with data precoding is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{\text{MRC}}\right] \approx \frac{\frac{\alpha N_E}{U}\left[N_E(U+1)+2\right]}{N_E \sigma_{\text{E}}^2 + \frac{(1-\alpha)}{U+1} N_E} = \frac{\frac{\alpha}{U}\left[N_E(U+1)+2\right]}{\sigma_{\text{E}}^2 + \frac{(1-\alpha)}{U+1}}. \tag{6.97}$$

From (6.97), Eve's approximated ESINR is identical to the one obtained in a SISO-ME MRC scenario (see (5.75)). Compared to the SDS and OC scenarios, Eve's ESINR is about $N_E U$ times higher. This arises from the fact that, when she implements an MRC receiver, she benefits from a frequency diversity gain U and an array gain N_E since she is able to coherently sum up her received symbol components. The approximated EC at Eve is therefore expressed as:

$$C_E^{\text{MRC}} \approx \log_2\left(1 + \mathbb{E}\left[\gamma_{E,n}^{\text{MRC}}\right]\right) = \log_2\left(1 + \frac{\frac{\alpha}{U}\left[N_E(U+1)+2\right]}{\sigma_{\text{E}}^2 + \frac{(1-\alpha)}{U+1}}\right). \tag{6.98}$$

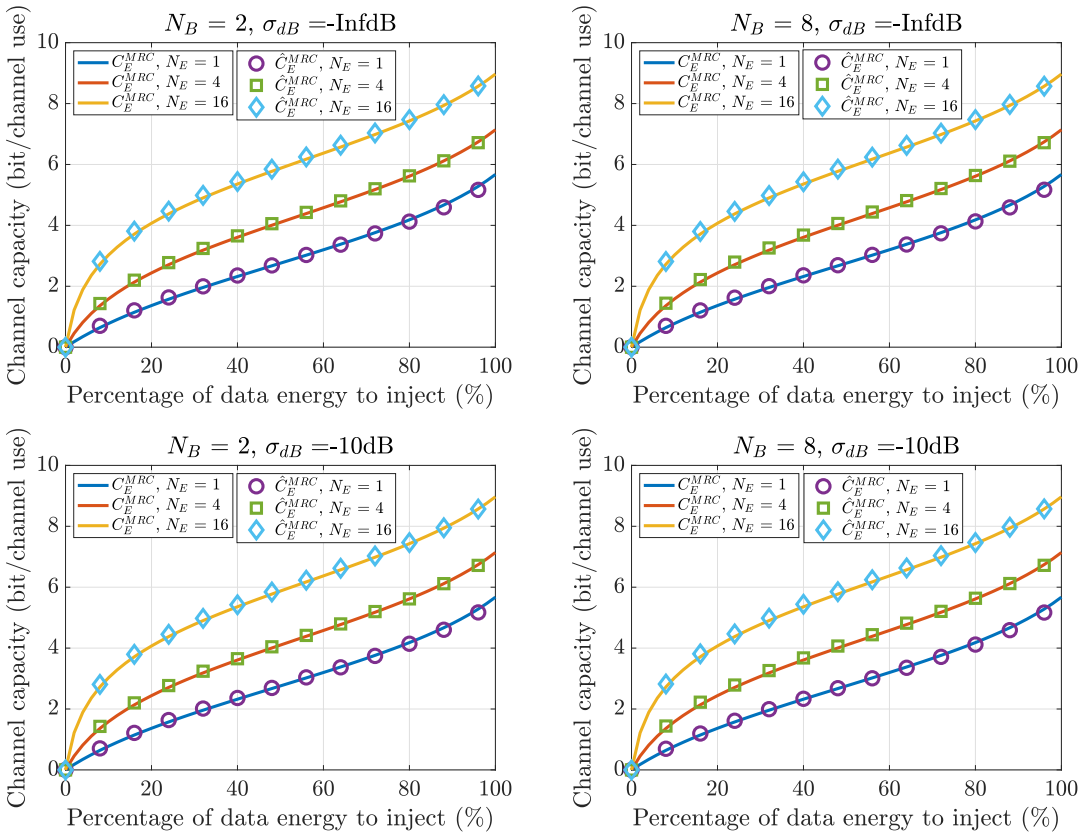

Figure 6.32: Comparison between approximated EC and exact EC at Eve: SIMO with precoding, MRC decoder, $\delta_E = 10$dB, 100.000 realizations

Figure 6.32 shows the accuracy of the approximation on the EC, by comparing the exact EC ($\widehat{C}_E^{\text{MRC}}$) obtained by Monte Carlo simulations (100.000 realizations) with the approximated EC at Eve (C_E^{MRC}) given in (6.98). The same set of parameters is considered as for the SIMO-ME SDS and OC scenarios, shown in Figures 6.30 and 6.31, respectively.

As anticipated from the above discussion, Eve's capacity does not depend on Bob's number of antennas. In addition, it is observed that Eve's EC increases when N_E increases, which can be anticipated from equation (6.97). Furthermore, one can observe that (6.98) fits well the exact EC, such that it can be used as a closed-form approximation for the rest of the study. In addition, the EC values observed in Figure 6.32 are identical to the ones obtained in Figure 5.18, which shows the EC at Eve in a SISO-ME MRC scenario.

6.3.5 Guaranteeing secrecy rate

As for the SISO and the MISO systems, Alice needs to a priori know the per-symbol ESR over which she can securely communicate with Bob. In order to do so, Alice must design the communication parameters that guarantee a targeted communicated ESR, depending on the handshake procedures with Bob. As a reminder, two SIMO schemes are investigated. In the first one, termed as SIMO without data precoding, only the scenario where Eve implements an MRC decoding structure is considered. In the SIMO with data precoding scheme, three scenarios are investigated:

- SIMO precoding, scenario 1: Eve implements the SDS decoder.
- SIMO precoding, scenario 2: Eve implements the OC decoder.
- SIMO precoding, scenario 3: Eve implements the MRC decoder.

For each scenario, the required SNR at Bob, upper bounds on Eve's maximal number of allowed antennas, upper bounds on the allowed CSI error performed by Alice, and the optimal amount of data energy to inject, to guarantee a per-symbol communication ESR= Δ, are derived in Sections 6.3.5.1, 6.3.5.2, 6.3.5.3, and 6.3.5.4, respectively. As usual, the worst case scenario in terms of secrecy is considered. That is, Eve's SNR $\rightarrow +\infty$, which is obtained by setting $\sigma_{\mathrm{E}}^2 = 0$ in Eve's capacity expressions.

6.3.5.1 Required SNR at Bob

As a reminder, the transmitted energy per symbol is 1. Since one symbol is spread over U subcarriers, the transmitted energy per symbol component is $1/U$. In addition, it is considered normalized channels, such that the received energy per symbol component is $1/U$. Therefore, Bob's SNR per symbol component is defined as :

$$\delta_{\mathrm{B}}^{\mathrm{D}} = 1\frac{1}{U\sigma_{\mathrm{B}}^2}. \tag{6.99}$$

6.3.5.1.1 Scheme 1 : SIMO without precoding As a reminder, the worst case scenario in terms of secrecy is obtained when Eve is equipped with an arbitrarily large number of antennas. From that, one has to consider Eve's EC upper bound (6.78).

Introducing (6.69) and (6.78) into the per-symbol ESR expression (5.11), and considering $\sigma_{\mathrm{E}}^2 = 0$, the guaranteed ESR, in a SIMO-ME scheme without data precoding performed by Alice, is given by:

$$R_{s,n}^{\mathrm{MRC}} = \Delta = \frac{1}{U}\left[\log_2\left(1+\frac{\alpha\left[UN_B(1-\sigma)+1\right]}{U\sigma_{\mathrm{B}}^2+(1-\alpha)\sigma}\right)-\log_2\left(1+\frac{\alpha U(N_B+1)}{(1-\alpha)}\right)\right]. \tag{6.100}$$

It is interesting to remark that the ESR expression (6.100) can be bounded. The upper bound is found when $N_B \rightarrow +\infty$, and is given by:

$$R_{s,n}^{\mathrm{MRC,UP}} = \frac{1}{U}\left[\log_2\left(\frac{(1-\alpha)(1-\sigma)}{(1-\alpha)\sigma+U\sigma_{\mathrm{B}}^2}\right)\right]. \tag{6.101}$$

The lower bound is found when $N_B = 2$ (which is the minimum number of antennas at Bob since a SIMO system is considered), and is given by:

$$R_{s,n}^{\mathrm{MRC,LO}} = \frac{1}{U}\left[\log_2\left(\frac{U\sigma_{\mathrm{B}}^2+\alpha(1-\sigma)(2U+1)+\sigma}{U\sigma_{\mathrm{B}}^2+(1-\alpha)\sigma}.\frac{(1-\alpha)}{\alpha(3U-1)+1}\right)\right]. \tag{6.102}$$

Consequently, $R_{s,n}^{\mathrm{MRC,UP}}$ and $R_{s,n}^{\mathrm{MRC,LO}}$ are respectively the upper and lower bounds on the achievable ESR, in a SIMO-ME without data precoding scheme, when the worst-case scenario regarding the eavesdropper is considered, i.e., $N_E \rightarrow +\infty$, and $\sigma_{\mathrm{E}}^2 = 0$.
Figure 6.33 illustrates the ESR as a function of α, for different N_B, with fixed $\sigma_{\mathrm{dB}} = -\infty$dB, and with variable U between each sub-figure. The upper bound (6.101) is also shown. First, it can be observed that the ESR increases when Bob is equipped with a growing number of antennas, but stays below the upper bound (6.101). In addition, it is seen that the ESR decreases when the spreading factor increases. When U or N_B increase, the ESR is maximized when more AN energy is injected. Finally, compared to the SISO-ME scenario investigated in Chapter 5 and presented in Figure 6.33, this scheme exhibits better secrecy performances. Indeed, in a SIMO-ME without data precoding scenario, one can ensure positive ESRs even with Eve is equipped with an arbitrarily large number of antennas.

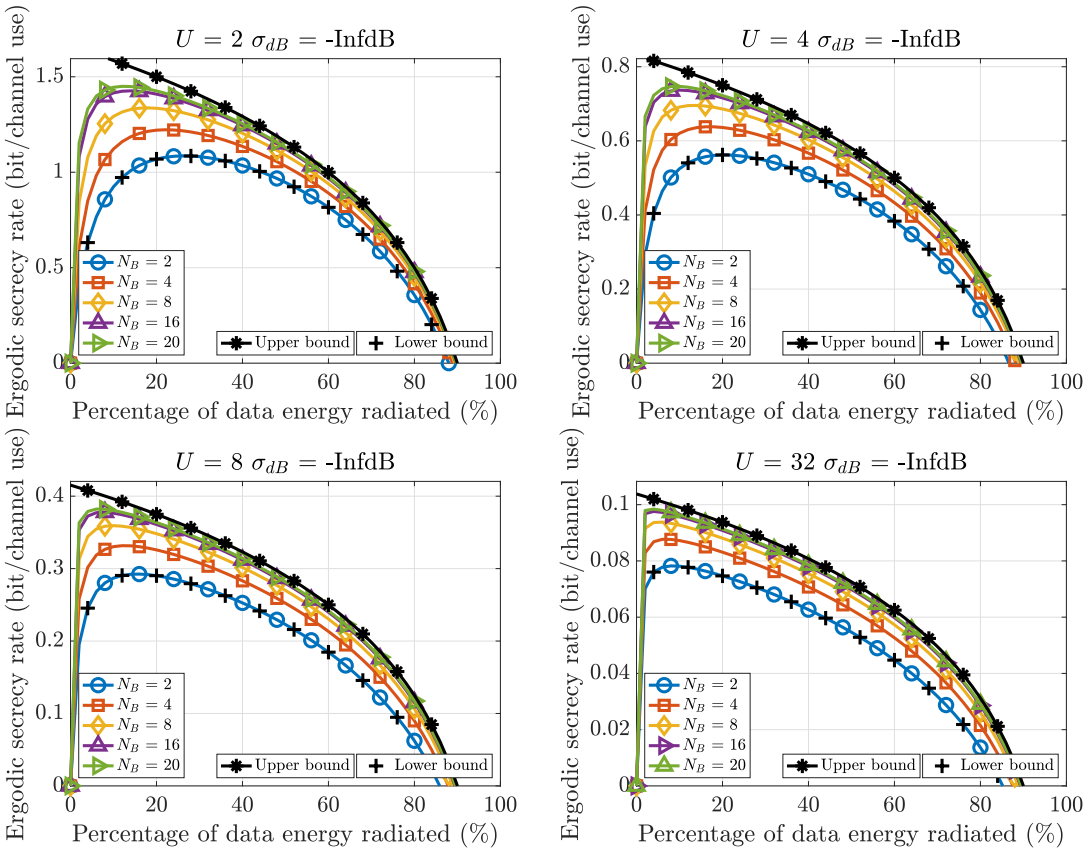

Figure 6.33: Guaranteed ergodic secrecy rate, SIMO without precoding, MRC decoder, $\delta_B = 10$dB

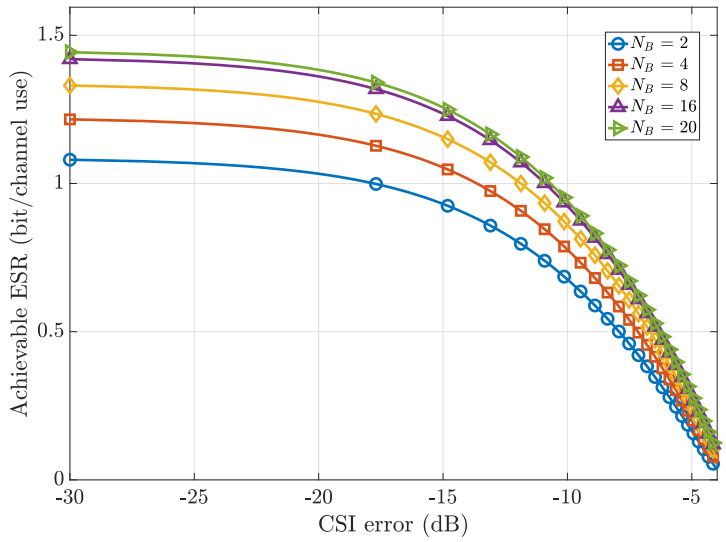

Figure 6.34: Maximal guaranteed ergodic secrecy rate, SIMO without precoding, MRC decoder, $U = 2$, $\delta_B = 10$dB

Figure 6.34 outlines the impact of Alice's CSI estimation's accuracy on the ESR performances, at fixed $U = 2$, and for different values of N_B. It is observed that the achievable ESR decreases when σ_{dB} increases, as expected. However, positive ESRs can be guaranteed even for poor CSI estimation, whatever the BOR factor.
After manipulating equation (6.100), one obtains the required SNR at Bob to guarantee ESR $= \Delta$,

when Alice does not precode the transmitted data and Eve implements the MRC decoder:

$$\delta_{\mathrm{B}}^{\mathrm{MRC}} = \frac{\alpha T_0^{\mathrm{MRC}} + T_1^{\mathrm{MRC}}}{\alpha^2 T_2^{\mathrm{MRC}} + \alpha T_3^{\mathrm{MRC}} + T_4^{\mathrm{MRC}}}, \tag{6.103}$$

where:

$$\begin{aligned}
T_0^{\mathrm{MRC}} &= 2^{\Delta U}(UN_B + U - 1) + 1 \\
T_1^{\mathrm{MRC}} &= 2^{\Delta U} - 1 \\
T_2^{\mathrm{MRC}} &= 2^{\Delta U}\sigma(UN_B + U - 1) - (UN_B(1-\sigma) + (1-\sigma)) \\
T_3^{\mathrm{MRC}} &= 2^{\Delta U}\sigma(2 - UN_B - U) + UN_B(1-\sigma) + 1 - 2\sigma \\
T_4^{\mathrm{MRC}} &= -\sigma(2^{\Delta U} - 1).
\end{aligned}$$

6.3.5.1.2 Scheme 2 : SIMO with precoding

As a reminder, when Alice precodes the transmitted data in a SIMO scheme, Bob's EC is similar to the SISO EC, found in (5.19).

Scheme 2, scenario 1: SDS decoder

Introducing (6.82) and (6.88) into the per-symbol ESR expression (5.11), and considering $\sigma_{\mathrm{E}}^2 = 0$, the guaranteed ESR, in a SIMO-ME scheme with data precoding when Eve implements an SDS decoder, is given by:

$$R_{s,n}^{\mathrm{SDS}} = \Delta = \frac{1}{U}\left[\log_2\left(1 + \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U\sigma_{\mathrm{B}}^2 + (1-\alpha)\sigma}\right) - \log_2\left(1 + \frac{\alpha}{1-\alpha}\right)\right], \tag{6.104}$$

which is equivalent to the SISO-SE SDS scenario, given in (5.41). Consequently, the ESR performances can be found in Figure 5.5. The required SNR at Bob is given in equation (5.42).

Scheme 2, scenario 2: OC decoder

Introducing (6.82) and (6.93) into the per-symbol ESR expression (5.11), and considering $\sigma_{\mathrm{E}}^2 = 0$, the guaranteed ESR, in a SIMO-ME scheme with data precoding when Eve implements an OC decoder, is given by:

$$R_{s,n}^{\mathrm{OC}} = \Delta = \frac{1}{U}\left[\log_2\left(1 + \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U\sigma_{\mathrm{B}}^2 + (1-\alpha)\sigma}\right) - \log_2\left(1 + \frac{\alpha}{1-\alpha}\right)\right]. \tag{6.105}$$

Expression (6.105) is equivalent to the SIMO-ME SDS expression (6.104). Therefore, when one studies the SIMO-ME OC scenario, one comes back to the SISO-SE SDS scenario, given in (5.41). The ESR performances can be found in Figure 5.5. The required SNR at Bob is given in equation (5.44).

Scheme 2, scenario 3: MRC decoder

Introducing (6.82) and (6.98) into the per-symbol ESR expression (5.11), and considering $\sigma_{\mathrm{E}}^2 = 0$, the guaranteed ESR, in a SIMO-ME scheme with data precoding when Eve implements an MRC decoder, is given by:

$$R_{s,n}^{\mathrm{MRC}} = \Delta = \frac{1}{U}\left[\log_2\left(1 + \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U\sigma_{\mathrm{B}}^2 + (1-\alpha)\sigma}\right) - \log_2\left(1 + \frac{\frac{\alpha}{U}\left[N_E(U+1)+2\right]}{\frac{(1-\alpha)}{U+1}}\right)\right]. \tag{6.106}$$

Expression (6.106) is equivalent to the SISO-ME MRC expression (5.78). The ESR performances can therefore be found in Figures 5.19 and 5.20. The required SNR at Bob is given in equation (5.79).

6.3.5.2 Maximal eavesdropper antennas allowed

6.3.5.2.1 Scheme 1 : SIMO without precoding

There is no condition to determine on the maximal number of Eve's antennas that is allowed to be able to guarantee a communication ESR = Δ. Indeed, it was proven that the worst-case situation is attained when Eve is equipped with an arbitrarily large number of antennas. That is, it is considered that $N_E \to +\infty$ when studying the SIMO-ME scheme without data precoding. In other words, Eve can possess an infinite number of antennas and a positive ESR is still achievable.

6.3.5.2.2 Scheme 2 : SIMO with precoding

Scheme 2, scenario 1: SDS decoder

There is no condition to determine on the maximal number of Eve's antennas that is allowed to be able to guarantee a communication ESR = Δ. Indeed, the SIMO-ME SDS scheme with data precoding is similar to the SISO-SE SDS scenario.

Scheme 2, scenario 2: OC decoder

There is no condition to determine on the maximal number of Eve's antennas that is allowed to be able to guarantee a communication ESR = Δ. Indeed, the SIMO-ME SDS scheme with data precoding is similar to the SISO-SE SDS scenario.

Scheme 2, scenario 3: MRC decoder

The condition on $N_{E,\max}$ is similar to the one derived in a SISO-ME MRC scheme. That is, it can be found in (5.80). To remind, $N_{E,\max}$ is given by:

$$N_{E,\max} = \left\lfloor \frac{U(U+1)(1-\sigma) - (U+2)2^{\Delta U}\sigma}{(U+1)^2 2^{\Delta U}\sigma} \right\rfloor^+, \tag{6.107}$$

where $\lfloor x \rfloor^+$ is the maximum between 0 and the nearest integer lower or equal to x. The performances of (6.107) are shown in Figures 5.21 and 5.22.

6.3.5.3 Maximal CSI error allowed

6.3.5.3.1 Scheme 1 : SIMO without precoding

Expression (6.103) gives the required SNR at Bob to guarantee a per-symbol communication ESR = Δ when Eve implements an MRC decoder in a SIMO without precoding scheme, as a function of the communication parameters. For a solution to exist, (6.103) must be positive, which in turn imposes a maximal CSI error $\sigma_{\max}^{\text{MRC}}$ that can be made by Alice to possibly reach the targeted ESR. Determining the maximal CSI error allows to find the domain of validity of the SNR expression, i.e., it allows to find an upper bound on Alice's CSI accuracy to be able to guarantee ESR=Δ bit/channel use. In other words, when $\sigma < \sigma_{\max}^{\text{MRC}}$, Alice can determine a finite SNR at Bob that enables a guaranteed communication ESR = Δ. At $\sigma = \sigma_{\max}^{\text{MRC}}$, Bob's SNR needs to be infinite to possibly reach the targeted ESR. From (6.103), it can be shown that:

$$\sigma_{\max}^{\text{MRC}} = -\left. \frac{2S_1^{\text{MRC}} S_2^{\text{MRC}} + S_4^{\text{MRC}}}{2\left(\left(S_1^{\text{MRC}}\right)^2 + S_3^{\text{MRC}}\right)} \right|_{\sigma_{\max}^{\text{MRC}} \in [0,1]}, \tag{6.108}$$

where

$$\begin{aligned}
S_1^{\text{MRC}} &= -UN_B\left(2^{\Delta U}+1\right) + 2\left(2^{\Delta U}-1\right) - U2^{\Delta U} \\
S_2^{\text{MRC}} &= UN_B + 1 \\
S_3^{\text{MRC}} &= 4\left(2^{\Delta U}-1\right)\left(2^{\Delta U}(UN_B+U-1) + UN_B + 1\right) \\
S_4^{\text{MRC}} &= -4\left(2^{\Delta U}-1\right)(UN_B+1).
\end{aligned}$$

Interestingly, when Alice aims to target $\Delta \to 0^+$, the CSI error she can perform is bounded by:

$$\sigma_{\max}^{\text{MRC}}\Big|_{\Delta\to 0^+} = \frac{UN_B+1}{2UN_B+U}. \tag{6.109}$$

From (6.109), a maximal CSI error of 50% is allowed when $U=2$, and when $\Delta \to 0^+$ bit/channel use of ESR is aimed. In addition, expression (6.109) can be bounded by:

$$\frac{2U+1}{5U}\Big|_{N_B=2} \leq \sigma_{\max}^{\text{MRC}}\Big|_{\Delta\to 0^+} \leq \frac{1}{2}\Big|_{N_B\to+\infty}. \tag{6.110}$$

Figure 6.35 presents the upper bound on the CSI error allowed at Alice as a function of the maximal ESR that can be targeted, for different spreading factor, and with variable N_B between each sub-figure. First, it is seen that the maximal CSI error allowed decreases when U increases to reach a given ESR. This is anticipated from the fact that, due to the rate decrease, it is more stringent to achieve a given secrecy performance at higher BOR. In addition, $\sigma_{\max}^{\text{MRC}}$ decreases when Δ increases, which is expected. Furthermore, when Bob is equipped with an increasing number of antennas, Alice can be less accurate on the CSI estimation. Finally, when $\Delta \to 0^+$, the maximal allowed error on the CSI estimation respects condition (6.109), as seen in Figure 6.35.

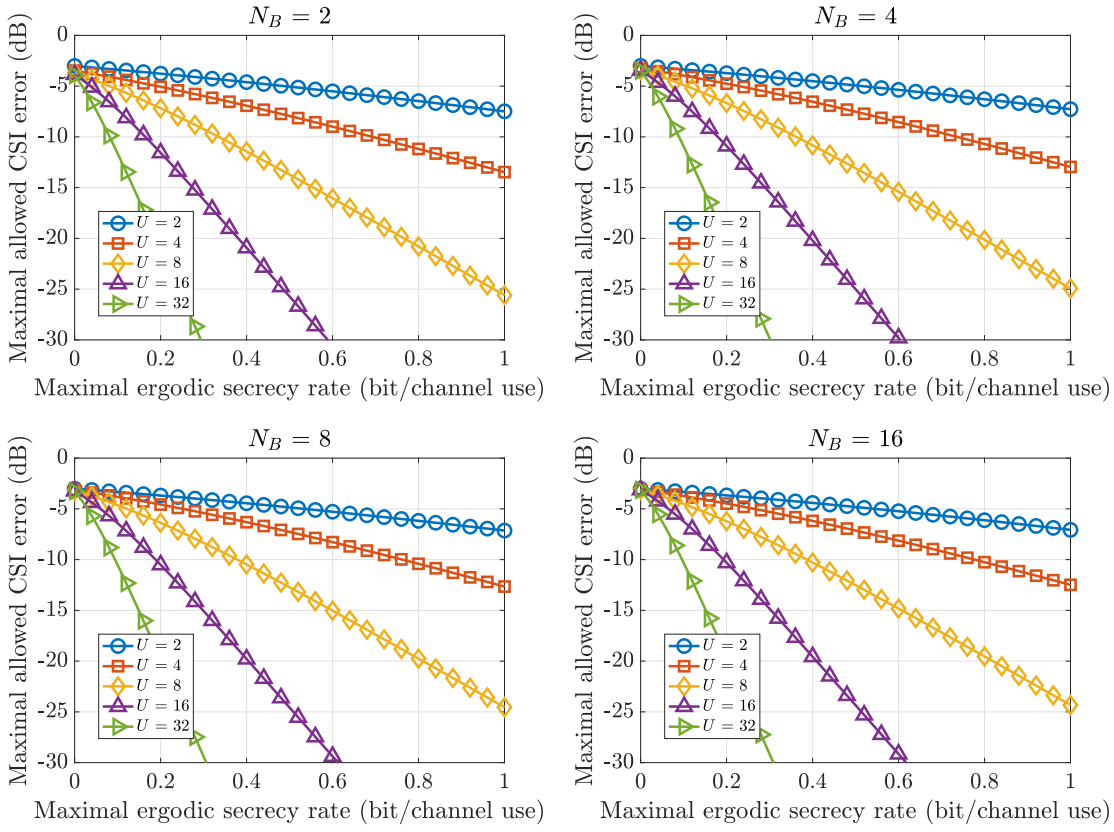

Figure 6.35: Maximal allowed CSI error as a function of the maximal ESR that can be guaranteed, SIMO without precoding, MRC decoder

6.3.5.3.2 Scheme 2 : SIMO with precoding

The condition on $\sigma_{\max}^{\text{SDS}}$, $\sigma_{\max}^{\text{OC}}$, and $\sigma_{\max}^{\text{MRC}}$ are respectively similar to the ones obtained for the SISO-SE SDS, OC, and the SISO-ME MRC scenarios. It is respectively found in (5.47) (Figure 5.7), in (5.48) (Figure 5.7), and in (5.81) (Figures 5.23 and 5.24).

6.3.5.4 Optimal amount of data energy to inject

6.3.5.4.1 Scheme 1 : SIMO without precoding

With the terms defined in (6.103), one can show that:

$$\alpha_{\text{opt}}^{\text{MRC}} = \left. \frac{-T_1^{\text{MRC}} T_2^{\text{MRC}} - \sqrt{\left(T_1^{\text{MRC}}\right)^2 \left(T_2^{\text{MRC}}\right)^2 + T_0^{\text{MRC}} T_2^{\text{MRC}} \left(T_0^{\text{MRC}} T_4^{\text{MRC}} - T_2^{\text{MRC}} T_3^{\text{MRC}}\right)}}{T_0^{\text{MRC}} T_2^{\text{MRC}}} \right|_{\substack{\sigma \leq \sigma_{\max}^{\text{MRC}}, \\ \alpha_{\text{opt}}^{\text{MRC}} \in [0,1]}} \tag{6.111}$$

Equation (6.111) determines the amount of data that Alice has to inject, in order to minimize the required SNR at Bob that guarantees a per-symbol communication ESR$= \Delta$ bit/channel use, when Eve performs the MRC decoder in a SIMO-ME without data precoding scheme. To obtain the corresponding SNR values, the parameter α in (6.103) is replaced with the values obtained in equation (6.111).
Figure 6.36 shows the required SNR at Bob as a function of the targetted ESR, for different BORs, at fixed $N_B = 8$, and with different CSI errors between each sub-figure. As expected, the required SNR increases when U or σ_{dB} increase, when one wants to target a given ESR. It also increases when an increased ESR aims to be guaranteed.
Figure 6.37 outlines the influence of the number of antennas at Bob on the required SNR, at $\Delta = 0.5$ bit/channel use, $U = 4$, and for different CSI errors, i.e., 0%, 1%, 5%, and 10% of error. It can be stated that the required SNR decreases when N_B increases, but saturates at high N_B. This is expected since the highest secrecy performances are obtained when $N_B \to +\infty$. From that, less stringent conditions on Bob's required SNR are allowed to target a given ESR, when N_B increases.

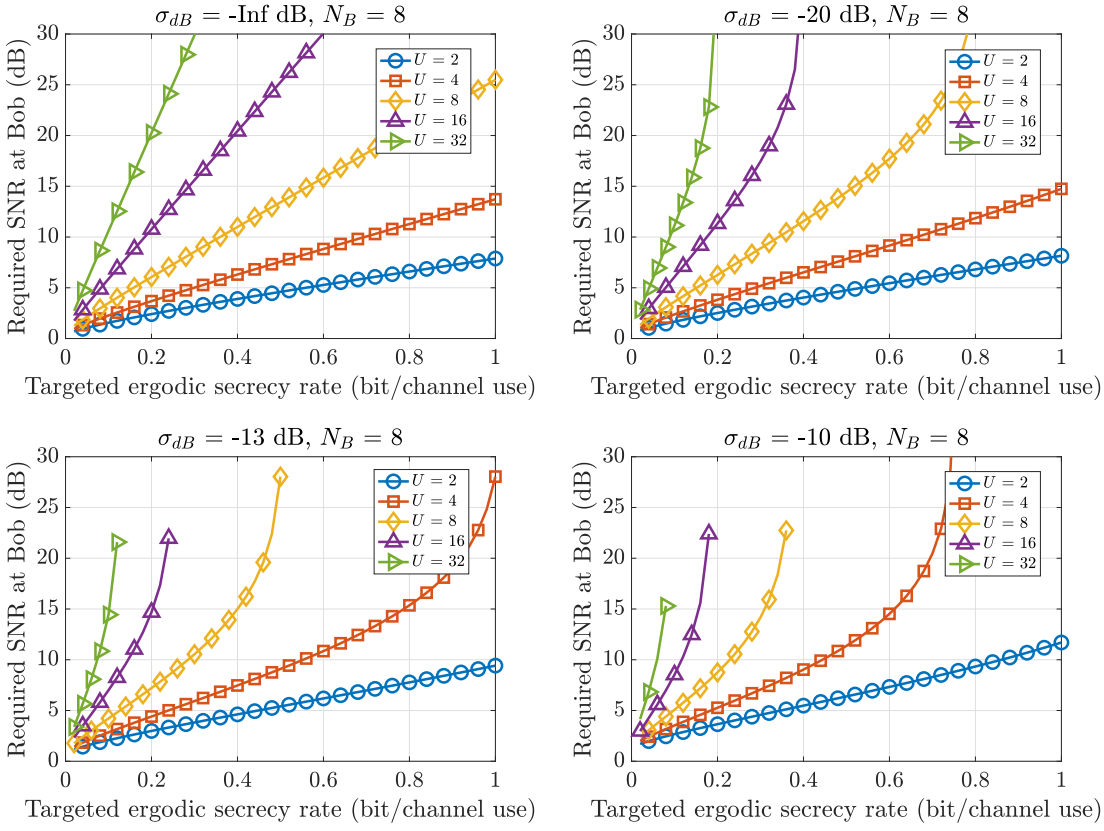

Figure 6.36: Required SNR at Bob as a function of the guaranteed ESR, SIMO without precoding, MRC decoder

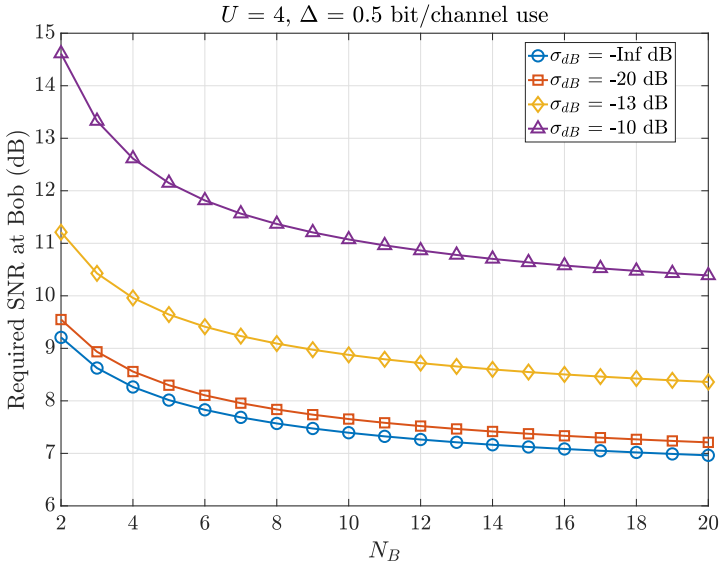

Figure 6.37: Required SNR at Bob as a function of N_B, SIMO without precoding, MRC decoder

6.3.5.4.2 Scheme 2 : SIMO with precoding

The optimal amount of data energy to inject in SIMO-ME SDS, OC, and MRC scenarios with data precoding, are respectively similar to the ones obtained for the SISO-SE SDS, OC, and the SISO-ME MRC scenarios. It is determined thanks to (5.51), (5.52), and (5.83). The required SNR at Bob for the SDS, OC, and MRC scenarios are presented in Figures 5.10, and 5.25, respectively.

6.3.6 Secrecy outage consideration

The following section studies the $\epsilon-$achievable SR performance for the two investigated SIMO schemes. It illustrates that outages occur if the instantaneous secrecy rate that can be supported by the communication is lower than the actual ESR at which Bob and Alice communicate, resulting to leakage to Eve. The performances are obtained by Monte Carlo simulations considering 100.000 realizations of the instantaneous secrecy rate to be able to observe very low outage percentages. It is assumed, as always, that Eve is noiseless.

6.3.6.1 Scheme 1 : SIMO without precoding

In this scenario, the results are obtained considering $N_E = 100$ in order to simulate an eavesdropper with a large number of antennas. As a reminder, it corresponds to the worst case scenario in terms of secrecy.

The left part Figure 6.38 presents the $\epsilon-$achievable SR as a function of the fraction of outage, for different BORs, at fixed N_B=2, $N_E = 100$, and when Alice estimates Bob's CSI with 30% of error. It is observed that, even in this configuration where Alice misestimates strongly Bob's CSI, higher BOR values lead to lower outage performances. Indeed, a zero secrecy outage is obtained as soon as less than 7.7% of outage occurs with $U = 8$. With $U = 2$, the 7.7%-achievable SR equals 0.07 bit/channel use. The right part of Figure 6.38 confirms that lower BOR values are more likely to be used to enhance the outage performances, whatever the CSI estimation error made by Alice.

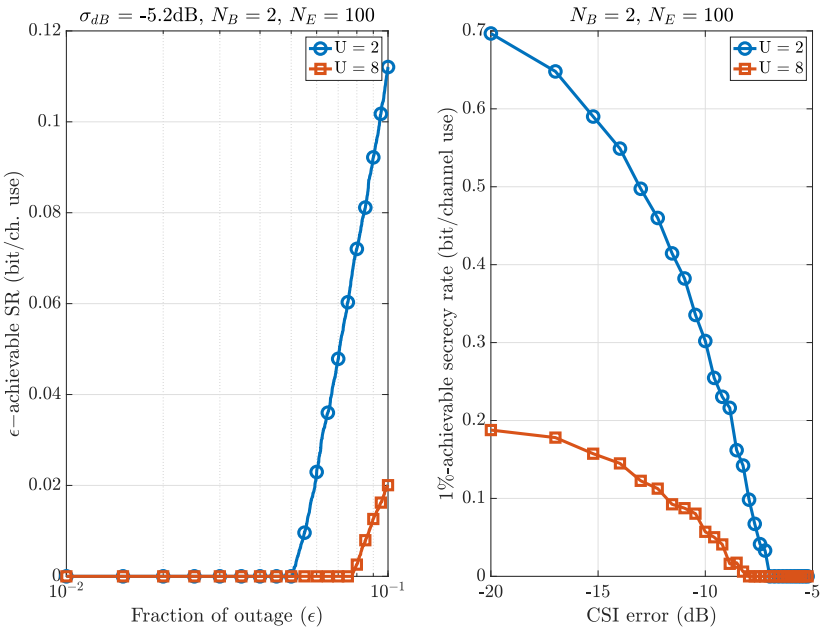

Figure 6.38: $\epsilon-$achievable secrecy rate as a function of the fraction of outage, SIMO without precoding, $\delta_B = 10$dB, MRC decoder

From the discussions about Figure 6.38, it can be concluded that, even in the worst case scenarios, i.e., noise-free eavesdropper, large number of Eve's antennas, low number of Bob's antennas, and with perfect CSI estimation made by Alice, it is more likely to communicate at low BORs to enhance the outage secrecy performances. Alice's choice on the BOR does not result to a trade-off.

6.3.6.2 Scheme 2 : SIMO with precoding

Scheme 2, scenario 1: SDS decoder

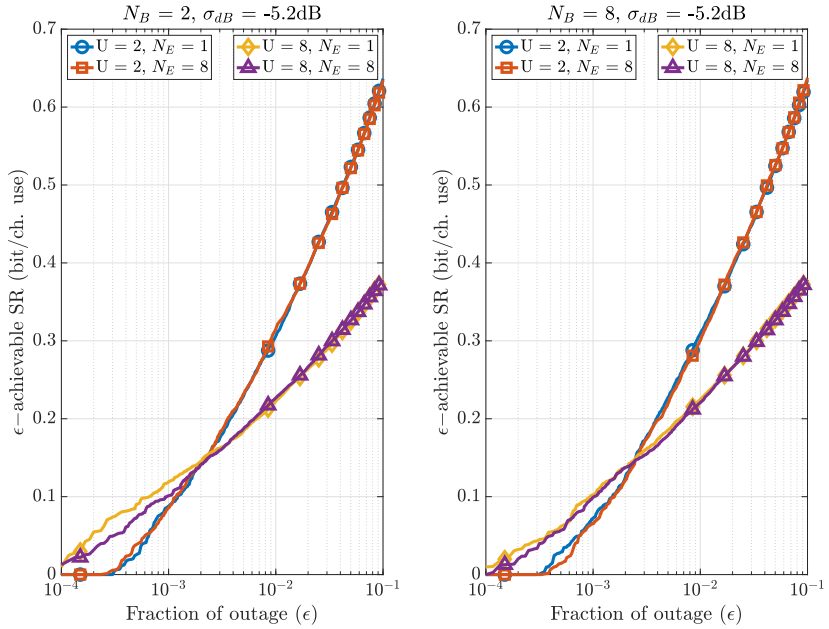

Figure 6.39: $\epsilon-$achievable secrecy rate as a function of the fraction of outage, SIMO with precoding, $\delta_B = 10$dB, SDS decoder

Figure 6.39 presents the $\epsilon-$achievable SR as a function of the fraction of outage, when 30% of CSI error is considered, for different BOR factors, and different number of Eve's antennas. Between each sub-figure, the number of Bob's antennas changes. It is observed that the outage performances do not depend on N_B nor N_E. In particular, it is similar to the SISO-SE SDS outage performances presented in Figure 5.12. The same conclusions can be drawn, i.e., Alice is more likely to communicate with higher BOR values if she aims to establish a communication with low percentages of outage and if she strongly misestimates Bob's CSI. When Alice's accuracy on Bob's CSI estimation increases, the point where she is more likely to communicate with higher BOR values occurs for lower outage percentages.

Scheme 2, scenario 2: OC decoder

Figure 6.40 presents the $\epsilon-$achievable SR as a function of the fraction of outage for the same set of parameters as used in the SDS scenario. It can be observed that the performances do not depend on N_B, but depend on N_E. Lower number of Eve's antennas allow higher outage performances, i.e., it is not convenient for Eve to be equipped for a large number of antennas if she implements an OC decoder in a SIMO-ME scheme with data precoding. In addition, the outage performances are similar to the ones obtained in a SISO-ME OC scenario (see Figure 5.27). The same conclusions as for the SISO-ME OC scenario can be drawn, i.e., Alice is more likely to communicate at higher BOR values if she strongly misestimates Bob's CSI and/or she aims to limit the outage occurrence. When Alice's accuracy on Bob's CSI estimation increases, the point where she is more likely to communicate with higher BOR values occurs for lower outage percentages. In addition, non-zero ϵ-achievable SRs are obtained for higher fraction of outage compared to the SIMO-ME SDS scheme presented in Figure 6.39.

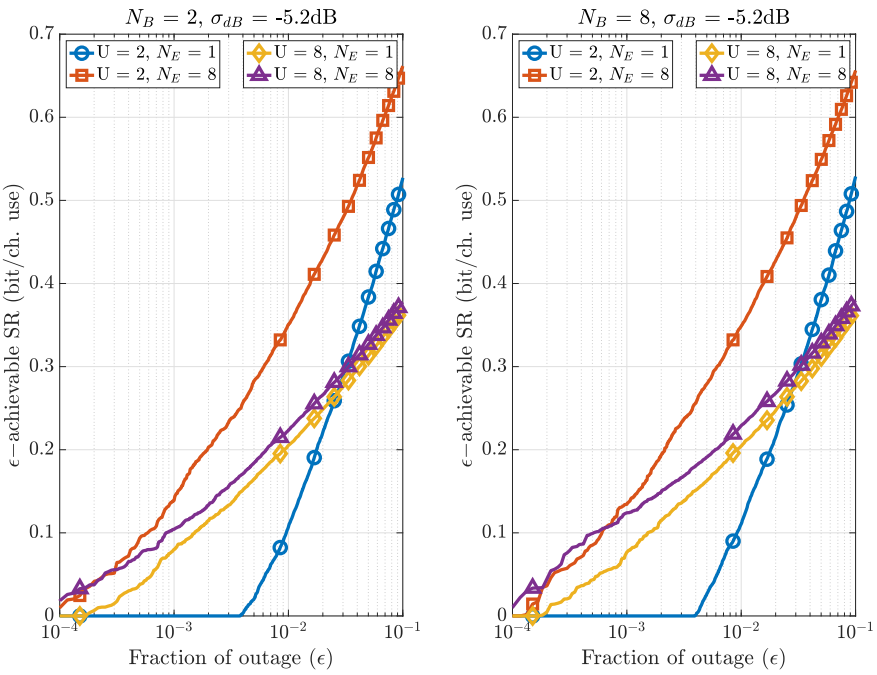

Figure 6.40: $\epsilon-$achievable secrecy rate as a function of the fraction of outage, SIMO with precoding, $\delta_B = 10$dB, OC decoder

Scheme 2, scenario 3: MRC decoder

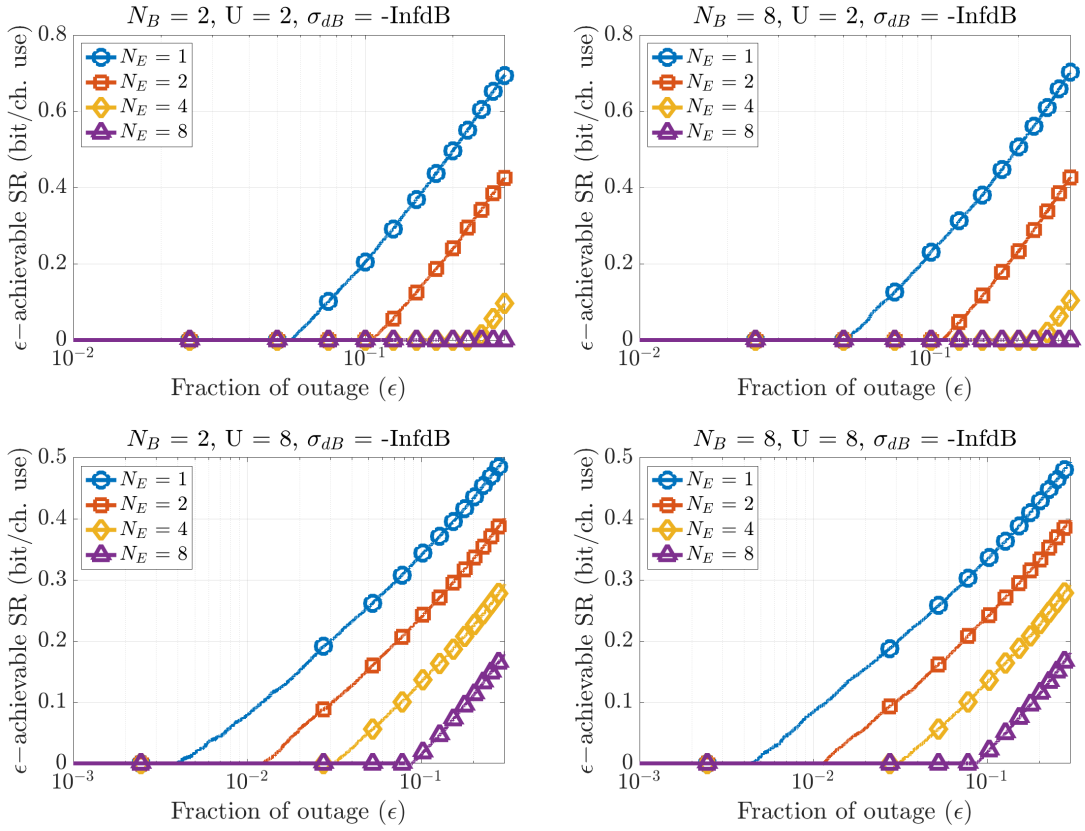

Figure 6.41: $\epsilon-$achievable secrecy rate as a function of the fraction of outage, SIMO with precoding, $\delta_B = 10$dB, MRC decoder

Figure 6.41 presents the $\epsilon-$achievable SR as a function of the fraction of outage for different number of Eve's antennas and when no CSI error is assumed. Between each sub-figure, the number of Bob's antennas and/or the BOR factor changes. It can be stated that larger number of Eve's antennas strongly degrades the outage performances. As an example, when $U = 2$, no CSI error, $N_B = 2$, and $N_E = 2$, a non-null secrecy outage is achievable as soon as more than 10.9% of outage is allowed. For the same set of parameters but $N_E = 4$, it can be achieved as soon as 24.2% of outage is allowed. The performances are similar to the ones obtained in a SISO-ME MRC scenario (see Figures 5.29 and 5.30). The same conclusions can therefore be drawn, i.e., low BOR values are more likely to be used when Bob's CSI estimation error is low, and when Eve is equipped with a relatively low number of antennas. However, increasing the BOR allows to obtain positive ϵ-achievable SRs for higher CSI estimation errors and larger number of eavesdropping antennas.

6.3.7 Conclusions on SIMO system

The second part of this chapter highlights the secrecy performances of SIMO systems. In particular, two schemes are studied, depending on whether Alice does precode or not the transmitted data signal.

When the transmitter does not precode the data, the MRC that was usually performed at the transmitter side, thanks to the FD TR precoding, is now performed at the receiving side. To do so, Bob must know his CSI, which is obtained thanks to pilots from Alice. This allows Eve to intercept the pilots and therefore to perfectly estimate her own CSI. Consequently, she may implement an MRC receiver as well, which is the most suited decoding structure. It is also assumed that Alice's estimation of Bob's CSI, required to design the AN signal, is not perfect. In addition, Bob's estimation of his own CSI is not perfect too, and it is considered that the estimation error is similar to Alice's one.

The second scheme occurs when Alice does precode the transmitted data with the sum of Bob's CSIs coming from each of his antennas. As always, Alice misestimates Bob's CSI. In that situation, three scenarios are investigated depending on the TDD handshake procedures. The amount of CSI knowledge Eve can obtain from the handshakes is assumed to be perfect.

Analytic derivation methodology
For each scenario, an approximation of the ESR is derived, which is in good agreement with the exact ESR performances obtained via simulations. As for the SISO and MISO systems, the communication parameters are designed in order **to guarantee a targeted per-symbol ESR**. To do so, worst case assumptions in terms of secrecy are considered, such has Eve being equipped with a noise-free hardware and/or is situated close to Alice, i.e., Eve having an arbitrarily large SNR, or Eve being equipped with an arbitrarily large number of antennas.
The analytic model of the ESR, depending on the investigated scenario, allows Alice to determine an analytic expression of the required SNR at Bob to guarantee Δ bit per channel use of secure rate. Thanks to this expression, Alice is able to derive:

- the maximal allowed main CSI error she can perform,
- the maximal number of allowed eavesdropping antennas,
- the optimal amount of data energy to inject.

SIMO without precoding : Main results
When Alice does not precode the data, it is proven that the worst-case scenario, in addition to being noiseless, is attained when Eve possesses an arbitrarily large number of antennas. Even with this configuration, it is shown that positive ESRs can be guaranteed. Furthermore, the worst situation regarding Bob is obtained when $N_B = 2$. Positive secrecy performances can still be achieved with this configuration, even for poor CSI estimates. Knowing the CSI error variance and Bob's SNR, Alice is more likely to communicate at lower BORs to maximize the secure ergodic communication rate, as well as to maximize the achievable communication rate under outage constraints.

SIMO with precoding : Main results
When Alice precodes the data, it is shown that the ESR performances of the SDS, OC, and MRC scenarios are respectively similar to SISO-SE SDS, the SISO-SE OC, and the SISO-ME MRC scenarios, i.e., there is no influence of Bob's number of antennas. Consequently, the same trade-off arises on Alice's choice on the BOR as for the SISO system. To remind, it is preferable for Alice to communicate at lower BORs to maximize the secure ergodic communication rate, but at higher BORs to minimize the outage percentage.

In addition, in the context of IoT, the SDS and OC schemes with data precoding are promising to secure an UL communication between a single-antenna UE and a multi-antenna BS. Indeed, it is shown that positive ESRs can be guaranteed while keeping low outage percentages, regardless the number of Eve's antennas. However, Alice is not able to guarantee some secrecy when Eve implements an MRC decoder since Eve's number of antennas strongly degrades the secrecy performances.

Finally, the study of the SIMO configuration with data precoding is motivated since its secrecy performances (ESR and outage) outperform the performances of the SIMO scenario without data precoding. In particular, when the SDS or the OC schemes with data precoding are considered, non-zero ϵ-achievable SRs are obtained for lower values of ϵ, i.e., less outage, compared to the SIMO scheme without data precoding (see Figures 6.39 and 6.40 w.r.t. Figure 6.38). More, the ESR performances of the SDS and OC schemes with data precoding outperform the ESR performances of the scheme without precoding (see Figure 5.5 w.r.t. 6.33).

Table 6.4 summarizes the performances of the SIMO system.

Table 6.4: SIMO system: secrecy performance summary

	SIMO-ME no precoding	**SIMO-ME precoding: SDS**	**SIMO-ME precoding: OC**	**SIMO-ME precoding: MRC**
Guaranteed ESR expression	Equation (6.100), Fig. 6.33 and 6.34. Worst-case ESR when $N_E \to +\infty$, but it remains bounded. It increases with an increase of N_B. Bounds on worst-case ESR given in (6.101) and (6.102).	Equation (6.104). ESR equivalent to the SISO-SE SDS scenario. The same conclusions as for the SISO-SE SDS scenario can therefore be drawn. The performances can be found in Figure 5.5.	Equation (6.105). ESR equivalent to the SISO-SE OC scenario. The same conclusions as for the SISO-SE OC scenario can therefore be drawn. The performances can be found in Figure 5.5.	Equation (6.106). ESR equivalent to the SISO-ME MRC scenario. The same conclusions as for the SISO-ME MRC scenario can therefore be drawn. The performances can be found in Figures 5.19 and 5.20.
Impact of imperfect CSI estimation	Equation (6.108). When Alice aims to target $\Delta \to 0^+$, the condition is given in (6.109) and is bounded by (6.110). The performances can be found in Figure 6.35. $\sigma^{\text{MRC}}_{\max}$ decreases when U and/or Δ increase. It increases when N_B increases.	$\sigma^{\text{SDS}}_{\max}$ is similar to the one obtained for the SISO-SE SDS scenario. It is found in (5.47), and the performances can be observed in Figure 5.7.	$\sigma^{\text{OC}}_{\max}$ is similar to the one obtained for the SISO-SE OC scenario. It is found in (5.48), and the performances can be observed in Figure 5.7.	$\sigma^{\text{MRC}}_{\max}$ is similar to the one obtained for the SISO-ME MRC scenario. It is found in (5.81), and the performances can be observed in Figures 5.23 and 5.24.
Condition on maximal N_E	No condition since worst-case scenario obtained for $N_E \to +\infty$.	No condition since ESR independent of N_E.	No condition since ESR independent of N_E.	Equation (6.107). The same conclusions as for the SISO-ME MRC scenario can therefore be drawn. The performances can be found in Figures 5.21 and 5.22.
Required SNR at Bob	Equation (6.103). The performances can be observed in Figures 6.36 and 6.37. The required SNR decreases when N_B increases. It increases when Δ, and/or U, and/or σ_{dB} increase.	Equation (5.42). Same conclusions as for the SISO-SE SDS scenario. The performances can be observed in Figure 5.10.	Equation (5.44). Same conclusions as for the SISO-SE OC scenario. The performances can be observed in Figure 5.10.	Equation (5.79). Same conclusions as for the SISO-ME MRC scenario. The performances can be observed in Figure 5.25.
Outage consideration	Figures 6.38. $\epsilon-$achievable SR increases when N_B increases. It decreases with an increase of U and/or an increase of σ_{dB}. Positive $\epsilon-$achievable SRs are obtained even for poor CSI estimations made by Alice. It is better to communicate at low BORs to enhance the $\epsilon-$achievable SR performances if low percentages of outage are desired.	Similar to the SISO-ME SDS scenario. The performances are seen in Figure 6.39. Alice has to communicate at higher BORs to enhance the $\epsilon-$achievable SR performances if low percentages of outage are desired.	Similar to the SISO-SE OC scenario. The performances are seen in Figure 6.40. Alice has to communicate at higher BORs to enhance the $\epsilon-$achievable SR performances if low percentages of outage are desired.	Similar to the SISO-ME MRC scenario. The performances are seen in Figure 6.41. In particular, Alice's choice on the BOR factor results from a trade-off. Knowing, the CSI error variance and Bob's SNR, Alice can choose a low BOR value to enhance the $\epsilon-$achievable SR performances when N_E is not large and σ_{dB} is low. However, if Eve is equipped with a large number of antennas or σ_{dB} is large, it is more likely to communicate at higher BORs.
Performance summary	It is shown that is is possible to guarantee positive secrecy performances even in the worst case scenario, i.e., noiseless eavesdropper equipped with an arbitrarily large number of antennas, and when the legitimate receiver only has two antennas. Low BORs are more likely to be used to enhance the ESR as well as the secrecy rate under outage constraints. Lower secrecy performances (ESR and outage) compared to the SIMO SDS and OC schemes with data precoding.	The same conclusions can be drawn as for the SISO-ME SDS scenario. Low BORs are preferable to enhance the ESR. However, higher BOR values are more likely to be used if low outage percentages are allowed. It therefore exists a trade-off on Alice's choice of the BOR. It also is possible to guarantee positive secrecy performances (ESR and ϵ-achievable SR) regardless of the number of Eve's antennas.	The same conclusions can be drawn as for the SISO-ME OC scenario. Low BORs are preferable to enhance the ESR. However, higher BOR values are more likely to be used if low outage percentages are allowed. It therefore exists a trade-off on Alice's choice of the BOR. It is also possible to guarantee positive secrecy performances (ESR and ϵ-achievable SR) regardless of the number of Eve's antennas. Slightly lower secrecy performances are obtained compared to the SDS scenario.	The same conclusions can be drawn as for the SISO-ME MRC scenario. In particular, little can be done against large number of cooperative eavesdroppers, or if Alice has low accuracies on Bob's CSI estimation. The choice on the BOR value results from a trade-off. Alice can choose a BOR either to maximize the ESR and the $\epsilon-$achievable secrecy rate by decreasing the BOR value, if N_E and σ are not too large. It is more likely to communicate at higher BORs if Eve is equipped with a large number of antennas, or if σ_{dB} increases.

6.4 Conclusion on multi-antenna systems

Under the considered assumptions whereby Eve experiences a Rayleigh channel, uncorrelated to Bob's one, it is shown that it is possible to guarantee a positive ergodic secrecy rate for both MISO and SIMO configurations. This means that a secure communication can occur between a multiple-antenna base station and a single-antenna user equipment in both DL and UL. To do so, handshake procedures in TDD relying on reciprocity are required, i.e., Bob must not explicitly feedback his channel estimate that could be intercepted by Eve. Furthermore, the BOR spreading factor involved in the FD TR precoder is a relevant degree of freedom which allows reducing the outage occurrence at the expense of the ESR. Finally, the closed-form expressions obtained for the ESR enables Alice to know a-priori the rate at which she can communicate while ensuring no data leakage to Eve and reliable decoding at Bob.

7 | Conclusions and Perspectives

This PhD work has presented a new practical and promising PLS scheme allowing one to guarantee the security at the physical layer of a point-to-point communication, in the context of IoT.

Chapter 1 introduces the concept of security in wireless networks, which appears to be multidisciplinary field. It is shown that cross-layer security protocols are needed to fully benefit from the degrees of freedom offered at different layers of the OSI protocol, therefore enhancing the robustness of practical systems against attacks. With the increased number of connected objects, i.e., with the idea of IoT, PLS has emerged as a promising solution to secure wireless communications and circumvent the limitations faced with classical cryptography-based schemes. IoT devices can benefit from the flexibility and the architecture of large scale, decentralized, and heterogeneous networks, such as in 5G. Having everything densely connected, wireless communications in IoT networks are particularly prone to passive eavesdropping attacks, which are therefore investigated in this work. Considering the security in IoT networks, different system configurations need to be studied, namely, SISO systems (for single-antenna node-to-node communications), MISO systems (for DL communication from a multi-antenna BS to single-antenna node), and SIMO systems (for UL communications from single-antenna node to multi-antenna BS).

In this PhD work, security at the physical layer means providing a reliable communication at the legitimate receiver, while guaranteeing confidentiality from the eavesdropper, i.e., no information leakage to the eavesdropper. Information theory lays the foundations for PLS, which are discussed in chapter 2. Wyner demonstrates that a positive secrecy capacity rate is achievable, by designing wiretap codes, as soon as a physical advantage is provided to Bob's channel over Eve's channel. The secrecy capacity is then simply characterized as the difference between Bob's and Eve's channel capacities. It is shown that, in a block-fading environment with multiple passive eavesdroppers, which is the scenario considered in this work, the ergodic secrecy rate is a suitable metric to evaluate the PLS performances. In addition, outage has to be investigated. It highlights the fact that information leakage occurs when the instantaneous secure rate that can be supported by the communication is lower that the ergodic secrecy rate at which Alice and Bob actually communicate. Consequently, the joint study of ergodic secrecy rate and ϵ-achievable secrecy rate is conducted in this manuscript. However, information theory describes the fundamental limits of communication systems without relying on the practical limitations. From that, this work focuses on the design of a practical PLS scheme aiming to provide a physical advantage to Bob over Eve in a multipath block-fading environment, and on top of which a wiretap code is to be constructed to achieve the secrecy performances.

Chapter 3 presents a state-of-the-art of PLS techniques that provide an advantage to the main channel over the eavesdropper's channel. Two approaches can be conducted to do so, namely, by designing channel-based adaptation schemes, and/or by injecting artificial noise. It is outlined that the secrecy performances strongly depend on the amount of CSI knowledge that can be acquired at the different communication's ends. In particular, in practical scenarios, Alice is only able to obtain an estimated version of Bob's CSI which is subject to errors. Several PLS techniques considering an imperfect main CSI knowledge at the transmitter are therefore presented. Some shortcomings from the literature are identified. First, none of the presented PLS schemes allows the transmitter to a-priori guarantee a

desired secrecy rate, which is however necessary to build wiretap codes allowing to achieve reliability and confidentiality, as mentioned in chapter 2. Indeed, either bounds on the achievable secrecy performances are detailed, or optimization procedures that need to be numerically solved are characterized, or schemes that do not consider the worst-case scenario regarding the eavesdropper are investigated, i.e., eavesdroppers have few CSI knowledge, limited decoding capabilities, or limited number of antennas. In addition, while some of the presented PLS schemes are robust to imperfect CSI knowledge at the transmitter side, it requires complex optimization procedures that need to be solved in order to fully recover from the secrecy loss. These recovery schemes are therefore unsuited for devices with limited computing capabilities, such as encountered with IoT objects, for instance. Furthermore, the amount of CSI that can be acquired at the eavesdropper is not well discussed and justified. It depends on the communication protocol, particularly on the handshake procedure, and in turns, directly influences the secrecy performances of the communication. It is therefore of prime importance to discuss the decoding capabilities of the eavesdropper.

Motivated by the aforementioned shortcomings, a practical channel-based adaptation PLS scheme, with AN injection, and considering imperfect main CSI, is studied in this PhD work. The PLS scheme is presented in chapter 4. In particular, a time reversal precoder is considered which presents inherent anti-eavesdropping abilities due to the focusing gain it offers at the legitimate receiver's position only. The time reversal precoder is implemented in the frequency domain into an OFDM modulation, which makes it compatible with existing standards, such as in 5G or LTE networks, for instance. In addition, to benefit from the focusing gain offered by time reversal precoding, each transmitted data symbol is spread in the frequency domain by a BOR factor, introducing the frequency diversity needed to inject an artificial noise signal. The AN injection requires additional frequency resources which makes the considered PLS scheme more suited for applications requiring high level of security. It is also considered that the channels are spatially uncorrelated, and that there is no frequency correlation amongst the channel subcarriers. The channel coefficients are Rayleigh distributed, which corresponds to urban or indoor environments with rich multipaths. Furthermore, practical handshake procedures between Alice and Bob are detailed, leading to different decoding structures that can be implemented at Eve, and so, different security performances. Three handshakes are described for TDD systems in SISO, MISO, and SIMO configurations, leading to three decoding structures at Eve, namely, SDS, OC, and MRC decoders. Two handshakes procedures for FDD systems are considered in a SISO configuration, namely, AN killer, and LMMSE decoders.

The secrecy performances of the considered PLS scheme, in terms of ergodic secrecy rate and ϵ-achievable secrecy rate, are studied in chapters 5 and 6, respectively for the single-antenna system (SISO system), and the multi-antenna systems (MISO and SIMO systems). For scenarios considering TDD handshake procedures, an approximation of the ergodic secrecy rate is derived. It is shown that the approximation fits well the exact ergodic secrecy rate performances obtained via simulations, and is therefore used as closed-form expressions to derive a certain number of useful metrics. The communication parameters are designed in order for the transmitter to *guarantee* a targeted ergodic secrecy rate. To do so, worst-case assumptions regarding the eavesdropper are undertaken. That is, it is assumed that the CSI knowledge Eve can get from the handshake procedures is perfect, Eve is equipped with a noise-free hardware and/or is situated close to Alice, i.e., Eve has an arbitrarily large SNR and can be equipped with an arbitrarily large number of antennas. In particular, the required SNR at Bob, the maximal allowed main CSI error performed by Alice, the optimal amount of data energy to inject, as well as the maximal number of allowed eavesdropping antennas (in the case of multi-antenna eavesdropper) are derived to guarantee a desired ergodic secrecy rate.

Introducing more redundancy/diversity by increasing the BOR factor reduces the ergodic secrecy rate and results in an overhead. However, it makes the scheme more robust w.r.t. CSI error and it also decreases the information leakage to the eavesdropper. In particular, it is demonstrated that Alice's choice on the BOR of the communication results from a trade-off. When Eve implements an SDS or

an OC decoder, for every system's configuration, i.e., SISO, MISO, or SIMO, knowing the CSI error variance and Bob's SNR, Alice can choose a BOR value either to maximize the ESR (by decreasing the BOR value), i.e., higher data rate transmission, or to ensure a communication with low outage percentages (by increasing the BOR value), i.e., less data leakage to Eve. The same trade-off arises when Eve implements an MRC decoder in SISO or MISO configurations. However, in these scenarios, little can be done if Alice strongly misestimates Bob's CSI, or if Eve is equipped with a large number of antennas. Nevertheless, when Alice does not precode the data in a SIMO configuration with Eve implementing an MRC decoder, it is shown that a positive secrecy rate can be guaranteed, but with lower outage performances w.r.t. the SIMO-ME SDS and OC schemes with data precoding, even if Eve is equipped with an arbitrarily large number of antennas.

From the study conducted in chapters 5 and 6, it turns out that the two TDD handshake procedures leading to the implementation of the SDS or the OC decoding structures are very promising. Indeed, for every system configuration, i.e., SISO, MISO, and SIMO, it is proven that Alice can design the communication parameters in order to ensure a positive ergodic secrecy rate, while guaranteeing low outage percentages (typically below 1%), regardless the number of Eve's antennas. These scenarios make the PLS scheme considered in this PhD robust against passive eavesdropping in IoT networks.

Finally, the performances of the FDD scenarios are assessed for the SISO-SE scenario only. The reason is that, when considering the AN killer or the LMMSE decoders, it is not possible for Alice to a-priori guarantee a secure communication with Bob. Indeed, when a noise-free eavesdropper is considered, Eve's decoding capabilities becomes arbitrarily large which therefore jeopardizes any attempt for the transmitter to provide a positive secrecy rate, even if Eve is equipped with only one antenna.

At the end of this PhD work, several perspectives can be outlined.
First, the proposed work assumes uncorrelated Rayleigh-fading channels. A study of the secrecy performances with frequency correlation amongst subchannels has to be undertaken since it is expected that the ESR may decrease with larger correlation. Second, an optimized precoding scheme can be implemented that automatically adapts the numerology when spreading the data in order to obtain a subcarrier correlation as low as possible. In doing so, the scheme benefits from the maximal frequency diversity in a correlated environment and the secrecy rate is expected to be enhanced compared to a classical spreading implementation. Third, the ESR expressions should be corrected to take into account the remaining correlation, either thanks to closed-form expressions or to tables. This will prevent Alice to communicate at a rate greater than the maximal ESR that ensures no data leakage. Finally, the impact of spatial correlation amongst the transmitter's antennas (in a MISO configuration) or the receiver's antennas (in a SIMO configuration) has to be carried out.

A natural extension of the work is to provide secure communications in a multi-casting scenario, i.e., providing security for multi-users. As an example, considering IoT networks in a node-to-multi-nodes configuration, if multiple legitimate users share the same resources, the AN can be introduced in all legitimate user's null spaces thanks to the design of the BOR factor. Indeed, with a BOR factor of U, an AN signal that lies in the null space of up to U-1 legitimate users can be generated. If a new protected link is entering the network, a new AN design procedure must take place to consider this user. In addition, spatial division multiple access (SDMA) can be used to create focusing beams to different legitimate users and increase system capacity and transmission quality.

It has been seen that the proposed scheme can only offer very low effective secrecy rate. It can therefore be implemented as part of a layered architecture to perform cross-layer security. Indeed, the investigated PLS scheme can securely distillate and update cryptographic keys that are then used by Alice and Bob to communicate.

Another perspective is to derive closed-form expressions of the outage performance. It allows one to

jointly optimize the communication parameters to ensure a targeted ergodic secrecy rate, while limiting the outage percentages below a predefined threshold.

Implementing the proposed PLS scheme into existing standards is also left as a perspective.

An improved AN injection scheme can be considered. Indeed, since Alice estimates Bob's instantaneous CSI, she can inject the AN with different energy at each subcarrier, depending on Bob's sub-channel fading conditions. In doing so, the ergodic secrecy rate is expected to be enhanced.

Finally, deriving the secrecy performances for the FDD scenarios is left as a perspective too.

Appendices

A | Momentum computation of circularly symmetric complex-valued random normal variables

A.1 Real-valued random normal variable

For real-valued random variable, the moment-generating function is an alternative specification of its probability distribution. In particular, it allows to compute the moments of the probability distribution as:

$$m_n = \mathbb{E}[X^n] = M_X^{(n)}(0) = \left.\frac{d^n M_X}{dt^n}\right|_{t=0} \tag{A.1}$$

For a real normal random variable $\mathbb{N}(\mu, \sigma^2)$, the moment-generating function is given by:

$$M_X = e^{t\mu + \frac{1}{2}\sigma^2 t^2} \tag{A.2}$$

Therefore:

$$\begin{aligned} \mathbb{E}\left[|X|^2\right] &= M_2 = \sigma^2 + \mu^2 \\ \mathbb{E}\left[|X|^4\right] &= M_4 = 3(\sigma^2)^2 + 6\sigma^2\mu^2 + \mu^4 \end{aligned} \tag{A.3}$$

A.2 Complex-valued random normal variable

A circularly symmetric complex-valued random normal variable is defined as $Z = X + iY$ where $X \sim \mathbb{N}(\mu_x, \sigma_x^2)$ and $Y \sim \mathbb{N}(\mu_y, \sigma_y^2)$. From that, it comes:

$$\begin{aligned} |Z|^2 &= X^2 + Y^2 \\ |Z|^4 &= X^4 + 2X^2Y^2 + Y^4 \end{aligned} \tag{A.4}$$

Since X and Y are independent, by taking into account (A.3) and (A.4), the moments of Z are given by:

$$\begin{aligned} \mathbb{E}\left[|Z|^2\right] &= \sigma_x^2 + \mu_x^2 + \sigma_y^2 + \mu_y^2 \\ \mathbb{E}\left[|Z|^4\right] &= 3(\sigma_x^2)^2 + 6\sigma_x^2\mu_x^2 + \mu_x^4 + 2\left[(\sigma_x^2 + \mu_x^2)(\sigma_y^2 + \mu_y^2)\right] + 3(\sigma_y^2)^2 + 6\sigma_y^2\mu_y^2 + \mu_y^4 \end{aligned} \tag{A.5}$$

From (A.5), if $Z \sim \mathbb{CN}(0,1)$, it comes: $\mathbb{E}\left[|Z|^2\right] = 1$, and $\mathbb{E}\left[|Z|^4\right] = 2$.

B | Single-Input Single-Output Single-eavesdropper

B.1 Linear minimum mean square error decoder expression

At Eve, the received signal is given by:

$$\mathbf{y}_{\mathrm{E}} = \sqrt{\alpha}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_{\mathbf{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}}, \tag{B.1}$$

where $\Gamma_{\mathrm{E}} = \mathbf{H}_{\mathbf{E}}\mathbf{H}_{\mathbf{B}}^{H}\mathbf{S}$. The LMMSE decoder minimizes the MSE of the estimated symbol

$$\hat{\mathbf{x}}_{\mathrm{E}} = \mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}}\mathbf{y}_{\mathrm{E}}. \tag{B.2}$$

It needs to satisfy the orthogonality principle, such that:

$$\mathbb{E}\left[(\hat{\mathbf{x}}_{\mathrm{E}} - \mathbf{x})\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] = \mathbf{0}_N \tag{B.3a}$$

$$\Leftrightarrow \mathbb{E}\left[(\mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}}\mathbf{y}_{\mathrm{E}} - \mathbf{x})\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] = \mathbf{0}_N \tag{B.3b}$$

$$\Leftrightarrow \mathbb{E}\left[\mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}}\mathbf{y}_{\mathrm{E}}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] = \mathbb{E}\left[\mathbf{x}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] \tag{B.3c}$$

$$\Leftrightarrow \mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}} = \mathbb{E}\left[\mathbf{x}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right]\left(\mathbb{E}\left[\mathbf{y}_{\mathrm{E}}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right]\right)^{-1} \tag{B.3d}$$

$$\begin{aligned}\Leftrightarrow \mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}} = {} & \mathbb{E}\left[\mathbf{x}\left(\sqrt{\alpha}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_{\mathbf{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}}\right)^{H}\right] \\ & \left(\mathbb{E}\left[\left(\sqrt{\alpha}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_{\mathbf{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}}\right)\left(\sqrt{\alpha}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_{\mathbf{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}}\right)^{H}\right]\right)^{-1}\end{aligned} \tag{B.3e}$$

$$\begin{aligned}\Leftrightarrow \mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}} = {} & \left(\sqrt{\alpha}\mathbb{E}\left[\mathbf{x}\mathbf{x}^{H}\Gamma_{\mathrm{E}}^{H}\right] + \sqrt{1-\alpha}\mathbb{E}\left[\mathbf{x}\mathbf{w}^{H}\mathbf{H}_{\mathbf{E}}^{H}\right] + \mathbb{E}\left[x\mathbf{v}_{\mathrm{E}}^{H}\right]\right) \\ & \left(\mathbb{E}\left[\alpha\Gamma_{\mathrm{E}}\Gamma_{\mathrm{E}}^{H}\mathbf{x}\mathbf{x}^{H} + (1-\alpha)\mathbf{H}_{\mathbf{E}}\mathbf{w}\mathbf{w}^{H}\mathbf{H}_{\mathbf{E}}^{H} + \mathbf{v}_{\mathrm{E}}\mathbf{v}_{\mathrm{E}}^{H}\right]\right)^{-1}\end{aligned} \tag{B.3f}$$

$$\Leftrightarrow \mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}} = \sqrt{\alpha}\sigma_{\mathrm{X}}^{2}\Gamma_{\mathrm{E}}^{H}\left(\alpha\sigma_{\mathrm{X}}^{2}\Gamma_{\mathrm{E}}\Gamma_{\mathrm{E}}^{H} + (1-\alpha)\left|\left|\mathbf{H}_{\mathbf{E}}\right|\right|^{2}\sigma_{\mathrm{AN}}^{2}\mathbf{I}_Q + \sigma_{\mathrm{E}}^{2}\mathbf{I}_Q\right)^{-1} \tag{B.3g}$$

$$\Leftrightarrow \mathbf{D}_{\mathbf{E}}^{\mathrm{LMMSE}} = \sqrt{\alpha}\Gamma_{\mathrm{E}}^{H}\left(\alpha\Gamma_{\mathrm{E}}\Gamma_{\mathrm{E}}^{H} + (1-\alpha)\left|\left|\mathbf{H}_{\mathbf{E}}\right|\right|^{2}\sigma_{\mathrm{AN}}^{2}\mathbf{I}_Q + \sigma_{\mathrm{E}}^{2}\mathbf{I}_Q\right)^{-1} \tag{B.3h}$$

B.2 Bob ergodic SINR modeling

B.2.1 Data term

$$\mathbb{E}\left[|B_1|^2\right] = \mathbb{E}\left[\left|\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H_B}\widehat{\mathbf{H}}_\mathbf{B}^*\mathbf{S}\right|\right|^2\right] \tag{B.4a}$$

$$= \mathbb{E}\left[\left|\sqrt{\alpha(1-\sigma)}\mathbf{S}^H||\mathbf{H_B}||^2\mathbf{S} + \sqrt{\alpha\sigma}\mathbf{S}^H\mathbf{H_B}\Delta\mathbf{H}_\mathbf{B}^*\mathbf{S}\right|^2\right] \tag{B.4b}$$

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{i=0}^{U-1}|h_{\mathrm{B},i}|^2 + \frac{\sqrt{\alpha\sigma}}{U}\sum_{i=0}^{U-1}h_{\mathrm{B},i}\Delta h_{\mathrm{B},i}^*\right|^2\right] \tag{B.4c}$$

$$= \frac{\alpha(1-\sigma)}{U^2}\left[\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},i}|^4\right] + \mathbb{E}\left[\sum_{i=0}^{U-1}\sum_{\substack{j=0\\ j\neq i}}^{U-1}|h_{\mathrm{B},i}|^2|h_{\mathrm{B},j}|^2\right]\right] + \frac{\alpha\sigma}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},i}|^2|\Delta h_{\mathrm{B},i}|^2\right] \tag{B.4d}$$

$$= \frac{1}{U^2}\alpha(1-\sigma)(2U+U(U+1)) + \frac{\alpha\sigma U}{U^2} \tag{B.4e}$$

$$= \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U}, \tag{B.4f}$$

where the following holds from Appendix A: $\mathbb{E}\left[|h_{\mathrm{B},i}|^2\right] = \mathbb{E}\left[|\Delta h_{\mathrm{B},i}|^2\right] = 1$, and $\mathbb{E}\left[|h_{\mathrm{B},i}|^4\right] = 2$, since $\mathbf{H_B} \sim \mathbb{CN}(0,1)$ and $\Delta\mathbf{H_B} \sim \mathbb{CN}(0,1)$.

B.2.2 AWGN term

$$\mathbb{E}\left[|B_2|^2\right] = \mathbb{E}\left[\left|\left|\mathbf{S}^H\mathbf{v}_\mathrm{B}\right|\right|^2\right] \tag{B.5a}$$

$$\mathbb{E}\left[|B_{2,n}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{B},n+iN}|^2\right] = \sigma_\mathrm{B}^2. \tag{B.5b}$$

B.2.3 AN term

$$\mathbb{E}\left[|B_3|^2\right] = \mathbb{E}\left[\left|\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H_B}\mathbf{w}\right|\right|^2\right]. \tag{B.6}$$

The AN is generated such that: $\mathbf{S}^H\widehat{\mathbf{H}}_\mathbf{B}\mathbf{w} = 0$. In addition, $\widehat{\mathbf{H}}_\mathbf{B} = \sqrt{1-\sigma}\mathbf{H_B} + \sqrt{\sigma}\Delta\mathbf{H_B}$, such that (B.6) becomes:

$$\mathbb{E}\left[|B_3|^2\right] = \mathbb{E}\left[\left|\left|-\sqrt{\frac{(1-\alpha)\sigma}{1-\sigma}}\mathbf{S}^H\Delta\mathbf{H_B}\mathbf{w}\right|\right|^2\right] \tag{B.7a}$$

$$= \frac{(1-\alpha)\sigma}{1-\sigma}\mathbb{E}\left[\left|\left|\mathbf{S}^H\Delta\mathbf{H_B}\mathbf{w}\right|\right|^2\right]. \tag{B.7b}$$

Let's rewrite: $\mathbf{w} = \sqrt{1-\sigma}\hat{\mathbf{w}} + \sqrt{\sigma}\mathbf{w}_\Delta$, where $\mathbf{S}^H\Delta\mathbf{H_B}\mathbf{w}_\Delta = \mathbf{0}_N$ and $\hat{\mathbf{w}} \perp\!\!\!\perp \Delta\mathbf{H_B}$, such that:

$$\mathbb{E}\left[|B_3|^2\right] = \frac{(1-\alpha)\sigma}{1-\sigma}(1-\sigma)\mathbb{E}\left[\left|\left|\mathbf{S}^H\Delta\mathbf{H_B}\hat{\mathbf{w}}\right|\right|^2\right] \tag{B.8a}$$

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)\sigma}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|\Delta h_{\mathrm{B},n+iN}|^2\,|\hat{w}_{n+iN}|^2\right] \tag{B.8b}$$

$$= \frac{(1-\alpha)\sigma}{U}U\frac{1}{U} = \frac{(1-\alpha)\sigma}{U}. \tag{B.8c}$$

B.3 Eve ergodic SINR modeling

B.3.1 SDS decoder

B.3.1.1 Data term

$$\mathbb{E}\left[|\mathbf{E}_1^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H_E}\widehat{\mathbf{H}}_\mathbf{B}^*\mathbf{S}\right|\right|^2\right] \tag{B.9a}$$

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{SDS}}|^2\right] = \alpha\mathbb{E}\left[\frac{1}{U^2}\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^2\left|\tilde{h}_{\mathrm{B},n+iN}^*\right|^2\right] \tag{B.9b}$$

$$= \frac{\alpha}{U^2}U = \frac{\alpha}{U}. \tag{B.9c}$$

B.3.1.2 AWGN term

$$\mathbb{E}\left[|\mathbf{E}_2^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\left|\mathbf{S}^H\mathbf{v}_\mathrm{E}\right|\right|^2\right] \tag{B.10a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{SDS}}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{E},n+iN}|^2\right] = \frac{1}{U}U\sigma_\mathrm{E}^2 = \sigma_\mathrm{E}^2. \tag{B.10b}$$

B.3.1.3 AN term

$$\mathbb{E}\left[|\mathbf{E}_3^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H_E}\mathbf{w}\right|\right|^2\right] \tag{B.11a}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{SDS}}|^2\right] = \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}w_i|^2\right] = \frac{1-\alpha}{U}U\frac{1}{U} = \frac{1-\alpha}{U}. \tag{B.11b}$$

B.3.2 OC decoder

B.3.2.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{OC}}|^2\right] = \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}h_{\mathrm{B},i}^*\,|h_{\mathrm{E},i}|^2\right|^2\right] \tag{B.12a}$$

$$= \frac{\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},i}|^2\,|h_{\mathrm{E},i}|^4\right] \tag{B.12b}$$

$$= \frac{\alpha}{U^2}2U = \frac{2\alpha}{U}. \tag{B.12c}$$

B.3.2.2 AWGN term

$$\mathbb{E}\left[|\mathbf{E}_2^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\left|\mathbf{S}^H\mathbf{H}_{\mathbf{E}}^*\mathbf{v}_{\mathrm{E}}\right|\right|^2\right] \tag{B.13a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{OC}}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},i}|^2|v_{\mathrm{E},i}|^2\right] = \sigma_{\mathrm{E}}^2. \tag{B.13b}$$

B.3.2.3 AN term

$$\mathbb{E}\left[|\mathbf{E}_3^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\left|\sqrt{1-\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathbf{E}}\right|^2\mathbf{w}\right|\right|^2\right] \tag{B.14a}$$

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{OC}}|^2\right] = \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},i}|^4|w_i|^2\right] \tag{B.14b}$$

$$= \frac{2(1-\alpha)}{U}. \tag{B.14c}$$

B.3.3 MF decoder

B.3.3.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{MF}}|^2\right] = \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}\left|\tilde{h}_{\mathrm{B},i}\right|^2|h_{\mathrm{E},i}|^2\right|^2\right] \tag{B.15a}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|\tilde{h}_{\mathrm{B},i}\right|^4|h_{\mathrm{E},i}|^4 + \sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}\left|\tilde{h}_{\mathrm{B},i}\right|^2|h_{\mathrm{E},i}|^2\left|\tilde{h}_{\mathrm{B},j}\right|^2|h_{\mathrm{E},j}|^2\right] \tag{B.15b}$$

$$= \frac{\alpha}{U^2}\left(4U + U(U-1)\right) = \frac{\alpha(U+3)}{U}. \tag{B.15c}$$

B.3.3.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{MF}}|^2\right] = \mathbb{E}\left[\left|\left|\mathbf{S}^H\mathbf{H}_{\mathbf{E}}^*\widehat{\mathbf{H}}_{\mathbf{B}}\mathbf{v}_{\mathrm{E}}\right|\right|^2\right] \tag{B.16a}$$

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{MF}}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},i}|^2|\tilde{h}_{\mathrm{B},i}|^2|v_{\mathrm{E},i}|^2\right] \tag{B.16b}$$

$$= \sigma_{\mathrm{E}}^2. \tag{B.16c}$$

B.3.3.3 AN term

The component $E_{3,n}^{\mathrm{MF}}$ depends on $\mathbf{w}$ and $\widehat{\mathbf{H}}_{\mathbf{B}}$ which are correlated via the AN design (4.8). The expectation is therefore not straightforward to compute.
As a reminder, the AN is generated such that:

$$\mathbf{A}\mathbf{w} = \mathbf{0}_N \tag{B.17}$$

with:

$$\mathbf{A} = \mathbf{S}^H \widehat{\mathbf{H}}_\mathbf{B} = \mathbf{U}\mathbf{\Sigma}\mathbf{V_1}^H \in \mathbb{C}^{N\times Q} \tag{B.18}$$

Omitting the $1-\alpha$ as well as the normalization factor in (4.10), the AN term at Eve is given by:

$$\begin{aligned}\mathbf{v} &= \mathbf{A}|\mathbf{H_E}|^2\mathbf{w} = \mathbf{S}^H\widehat{\mathbf{H}}_\mathbf{B}|\mathbf{H}_E|^2\mathbf{w} \\ &= \mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H|\mathbf{H_E}|^2\mathbf{V}_2\mathbf{w}',\end{aligned} \tag{B.19}$$

where $\mathbf{U}\in\mathbb{C}^{N\times N}$ contains left singular vectors, $\mathbf{\Sigma}\in\mathbb{R}^{N\times N}$ is a diagonal matrix containing non zero singular values, $\mathbf{V}_1\in\mathbb{C}^{Q\times N}$ contains right singular vectors associated to non zero singular values of $\mathbf{A}$, $\mathbf{V}_2\in\mathbb{C}^{Q\times Q-N}$ contains right singular vectors that span the right null space of $\mathbf{A}$, $\mathbb{E}\left[\tilde{\mathbf{w}}\tilde{\mathbf{w}}^H\right] = \mathbf{I_{Q-N}}$. Note that $\mathbf{w}'$ is independent from the other random variables and has a unit covariance matrix. Therefore, it can be shown that:

$$\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) = \mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{V}_2^H|\mathbf{H}_E|^2\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right), \tag{B.20}$$

Let's rewrite $|\mathbf{H_E}|^2 = \sum_{q=1}^{Q}|h_{E,q}|^2\mathbf{e}_q\mathbf{e}_q^T$ where $\mathbf{e}_q$ is an all zero vector except a 1 at row q:

$$\begin{aligned}\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) &= \sum_{q=1}^{Q}\sum_{q'=1}^{Q}\mathbb{E}(|h_{E,q}|^2|h_{E,q'}|^2)\mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right) \\ &= \sum_{q=1}^{Q}\mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right) + \mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H\mathbf{V}_2\mathbf{V}_2^H\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right),\end{aligned} \tag{B.21}$$

where the second term cancels out since $\mathbf{V}_2^H\mathbf{V}_1 = \mathbf{0}$. Since all elements of $\mathbf{v}$ have same variance, the following holds:

$$\begin{aligned}\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) &= \frac{1}{N}\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) \\ &= \frac{1}{N}\mathbb{E}\left(\mathbf{\Sigma}^2\mathbf{V}_1^H\sum_{q=1}^{Q}\left(\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\right)\mathbf{V}_1\right).\end{aligned} \tag{B.22}$$

Let's rewrite $\mathbf{V}_1 = \sum_l \mathbf{e}_l\mathbf{v}_{1,l}^H$ where $\mathbf{v}_{1,l}^H$ is the l-th row of $\mathbf{V}_1$ (of dimension $N\times 1$) with only one non-zero element.

$$\begin{aligned}\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) &= \frac{1}{N}\sum_{q=1}^{Q}\sum_{l}\sum_{l'}\mathbb{E}\left(\mathbf{\Sigma}^2\mathbf{v}_{1,l}\mathbf{e}_{l'}^T\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{e}_l\mathbf{v}_{1,l}^H\right) \\ &= \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\mathbf{\Sigma}^2\mathbf{v}_{1,q}\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{v}_{1,q}^H\right).\end{aligned} \tag{B.23}$$

Let's rewrite $\mathbf{V}_2 = \sum_l \mathbf{e}_l\mathbf{v}_{2,l}^H$ where $\mathbf{v}_{2,l}^H$ is the l-th row of $\mathbf{V}_2$ (of dimension $Q-N\times 1$) with $U-1$ non-zero elements:

$$\begin{aligned}\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) &= \frac{1}{N}\sum_{q=1}^{Q}\sum_{l}\sum_{l'}\mathbb{E}\left(\mathbf{\Sigma}^2\mathbf{v}_{1,q}\mathbf{e}_q^T\mathbf{e}_l\mathbf{v}_{2,l}^H\mathbf{v}_{2,l'}\mathbf{e}_{l'}^T\mathbf{e}_q\mathbf{v}_{1,q}^H\right) \\ &= \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\|\mathbf{v}_{2,q}\|^2\mathbf{v}_{1,q}^H\mathbf{\Sigma}^2\mathbf{v}_{1,q}\right),\end{aligned} \tag{B.24}$$

where $\mathbf{v}_{1,q}^H\mathbf{\Sigma}^2\mathbf{v}_{1,q} := \|\mathbf{v}_{1,q}\|^2\sigma_n^2$ is a scalar. Therefore:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\|\mathbf{v}_{2,q}\|^2\|\mathbf{v}_{1,q}\|^2\sigma_n^2\right). \tag{B.25}$$

Since $\mathbf{V}$ forms an orthonormal basis, i.e., $\mathbf{V}^H\mathbf{V} = \mathbf{I}_Q$, it is found that $\|\mathbf{v}_{1,q}\|^2 + \|\mathbf{v}_{2,q}\|^2 = 1$. Then:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left[\left(\|\mathbf{v}_{1,q}\|^2 - \|\mathbf{v}_{1,q}\|^4\right)\sigma_n^2\right]. \tag{B.26}$$

To determine (B.26), the transformations performed by the SVD on $\mathbf{A}$ in order to obtain $\mathbf{v}_{1,q}$ and σ_n^2 need to be determined. One can show that:

$$\sigma_n = \sqrt{\sum_{i=1}^{U}\left|z_{(n-1)U+i}\right|^2}, n = 1...N, \tag{B.27}$$

where $z_i = z_{i,x} + jz_{i,y} \sim \mathcal{CN}(0, \frac{1}{U})$. Therefore:

$$\mathbb{E}\left[\sigma_n^2\right] = 1. \tag{B.28}$$

Without loss of generality, $\mathbb{E}\left[\|v_{1,1}\|^2\right]$ and $\mathbb{E}\left[\|v_{1,1}\|^4\right]$ can be computed since all components of $\mathbf{V}_1$ are identically distributed:

$$\mathbb{E}\left[\|v_1\|^2\right] = \mathbb{E}\left[\left|\frac{z_1^*}{\sigma_1}\right|^2\right] = \frac{1}{U}. \tag{B.29}$$

For the moment of order 4, knowing that $\mathbb{E}\left[|z_i|^4\right] = \frac{2}{U^2}$:

$$\begin{aligned}\mathbb{E}\left[\|v_1\|^4\right] = \mathbb{E}\left[\left|\frac{z_1^*}{\sigma_1}\right|^4\right] &= \mathbb{E}\left[\frac{|z_1|^4}{\left(\sum_{i=1}^{U}|z_i|^2\right)^2}\right] \\ &= \frac{2}{U(U+1)}.\end{aligned} \tag{B.30}$$

Finally, eq.(B.26) can be computed as:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\left[\left(\frac{1}{U} - \frac{2}{U(U+1)}\right)1\right] = \frac{U-1}{U+1}. \tag{B.31}$$

Keeping into account the normalization factor in (4.10) and the $(1-\alpha)$ term, it follows:

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{MF}}|^2\right] = (1-\alpha)\frac{1}{U-1}\frac{U-1}{U+1} = \frac{1-\alpha}{U+1}. \tag{B.32}$$

C | Single-Input Single-Output Multi-eavesdropper

Eve ergodic SINR modeling

C.1 SDS decoder

C.1.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},k,i}\hat{h}_{\mathrm{B},i}^{*}\right|^2\right] \tag{C.1a}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\left(\sum_{k=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},k,i}\hat{h}_{\mathrm{B},i}^{*}\right)\left(\sum_{k'=1}^{N_E}\sum_{j=0}^{U-1} h_{\mathrm{E},k',j}\hat{h}_{\mathrm{B},j}^{*}\right)^{H}\right] \tag{C.1b}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},k,i}|^2\left|\hat{h}_{\mathrm{B},i}^{*}\right|^2\right] \tag{C.1c}$$

$$= \frac{\alpha}{U^2}N_E U = \frac{\alpha N_E}{U}. \tag{C.1d}$$

C.1.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1} v_{\mathrm{E},k,i}\right|^2\right] \tag{C.2a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1} |v_{\mathrm{E},k,i}|^2\right] \tag{C.2b}$$

$$= N_E\sigma_{\mathrm{E}}^2. \tag{C.2c}$$

C.1.3 AN term

$$\mathbb{E}\left[\left|E_{3,n}^{\mathrm{SDS}}\right|^2\right] = \mathbb{E}\left[\left|\frac{1-\alpha}{\sqrt{U}}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},k,i}w_i\right|^2\right] \tag{C.3a}$$

$$= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},k,i}\right|^2\left|w_i^2\right|\right] \tag{C.3b}$$

$$= \frac{(1-\alpha)}{U}N_E U\frac{1}{U} = \frac{(1-\alpha)N_E}{U} \tag{C.3c}$$

C.2 OC decoder

C.2.1 Data term

$$\mathbb{E}\left[\left|E_{1,n}^{\mathrm{OC}}\right|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},k,i}\right|^2\hat{h}_{\mathrm{B},i}^*\right|^2\right] \tag{C.4a}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\left(\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},k,i}\right|^2\hat{h}_{\mathrm{B},i}^*\right)\left(\sum_{k'=1}^{N_E}\sum_{j=0}^{U-1}\left|h_{\mathrm{E},k',j}\right|^2\hat{h}_{\mathrm{B},j}^*\right)^H\right] \tag{C.4b}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},k,i}\right|^4\left|\hat{h}_{\mathrm{B},i}\right|^2 + \sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},k,i}\right|^2\left|h_{\mathrm{E},k',i}\right|^2\left|\hat{h}_{\mathrm{B},i}\right|^2\right] \tag{C.4c}$$

$$= \frac{\alpha}{U^2}\left(2N_E U + N_E(N_E-1)U\right) = \frac{\alpha N_E(N_E+1)}{U} \tag{C.4d}$$

C.2.2 AWGN term

$$\mathbb{E}\left[\left|E_{2,n}^{\mathrm{OC}}\right|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}h_{\mathrm{E},ki}^* v_{\mathrm{E},k,i}\right|^2\right] \tag{C.5a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},k,i}\right|^2\left|v_{\mathrm{E}k,i}\right|^2\right] \tag{C.5b}$$

$$= \frac{1}{U}N_E U\sigma_{\mathrm{E}}^2 = N_E\sigma_{\mathrm{E}}^2 \tag{C.5c}$$

C.2.3 AN term

$$\mathbb{E}\left[\left|E_{3,n}^{\mathrm{OC}}\right|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2 w_i\right|^2\right] \tag{C.6a}$$

$$= \frac{1-\alpha}{U}\mathbb{E}\left[\left(\frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2 w_i\right)\left(\frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{k'=1}^{N_E}\sum_{j=0}^{U-1}|h_{\mathrm{E},k',j}|^2 w_j\right)^H\right] \tag{C.6b}$$

$$= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^4|w_i|^2\sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{E},k',i}|^2|w_i|^2\right] \tag{C.6c}$$

$$= \frac{(1-\alpha)}{U}\left(2N_E U\frac{1}{U} + N_E U(N_E-1)\frac{1}{U}\right) = \frac{(1-\alpha)N_E(N_E+1)}{U}. \tag{C.6d}$$

C.3 MRC decoder

C.3.1 Data term

$$\mathbb{E}\left[\left|E_{1,n}^{\mathrm{MRC}}\right|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_E}|h_{\mathrm{E},k,i}|^2\left|\hat{h}_{\mathrm{B},i}\right|^2\right|^2\right] \tag{C.7a}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\left(\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_E}|h_{\mathrm{E},k,i}|^2\left|\hat{h}_{\mathrm{B},i}\right|^2\right)\left(\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_E}|h_{\mathrm{E},k',j}|^2\left|\hat{h}_{\mathrm{B},j}\right|^2\right)^H\right] \tag{C.7b}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\Bigg[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^4\left|\hat{h}_{\mathrm{B},i}\right|^4\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{E},k,j}|^2\left|\hat{h}_{\mathrm{B},i}\right|^2\left|\hat{h}_{\mathrm{B},j}\right|^2$$
$$+\sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{E},k',i}|^2\left|\hat{h}_{\mathrm{B},i}\right|^4+\sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{E},k',j}|^2\left|\hat{h}_{\mathrm{B},i}\right|^2\left|\hat{h}_{\mathrm{B},j}\right|^2\Bigg] \tag{C.7c}$$

$$= \frac{\alpha}{U^2}\left[4N_E U + N_E U(U-1) + 2N_E(N_E-1)U + N_E(N_E-1)U(U-1)\right] \tag{C.7d}$$

$$= \frac{\alpha N_E}{U}\left[N_E(U+1)+2\right] \tag{C.7e}$$

C.3.2 AWGN term

$$\mathbb{E}\left[\left|E_{2,n}^{\mathrm{OC}}\right|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{i=0}^{U-1}\sum_{k=1}^{N_E}h_{\mathrm{E},k,i}^{*}\hat{h}_{\mathrm{B},i}v_{\mathrm{E},k,i}\right|^2\right] \tag{C.8a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{B},i}|^2|v_{\mathrm{E}k,i}|^2\right] \tag{C.8b}$$

$$= \frac{1}{U}N_E U\sigma_{\mathrm{E}}^2 = N_E\sigma_{\mathrm{E}}^2. \tag{C.8c}$$

C.3.3 AN term

The component $E_{3,n}^{\text{MRC}}$ depends on $\mathbf{w}$ and $\widehat{\mathbf{H}}_{\mathbf{B}}$ which are correlated via the AN design (4.8). The expectation is therefore not straightforward to compute.
As a reminder, the AN is generated such that:

$$\mathbf{A}\mathbf{w} = \mathbf{0}_N \tag{C.9}$$

with:

$$\mathbf{A} = \mathbf{S}^H \widehat{\mathbf{H}}_{\mathbf{B}} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V_1}^H \in \mathbb{C}^{N\times Q} \tag{C.10}$$

Omitting the $1-\alpha$ as well as the normalization factor in (4.10), the AN term at Eve is given by:

$$\begin{aligned}\mathbf{v} &= \mathbf{A}\sum_{k=1}^{N_E}\left|\mathbf{H}_{\mathbf{E},k}\right|^2\mathbf{w} = \mathbf{S}^H\widehat{\mathbf{H}}_{\mathbf{B}}\sum_{k=1}^{N_E}\left|\mathbf{H}_{\mathbf{E},k}\right|^2\mathbf{w}\\ &= \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\sum_{k=1}^{N_E}\left|\mathbf{H}_{\mathbf{E},k}\right|^2\mathbf{V}_2\mathbf{w}',\end{aligned} \tag{C.11}$$

where $\mathbf{U}\in\mathbb{C}^{N\times N}$ contains left singular vectors, $\boldsymbol{\Sigma}\in\mathbb{R}^{N\times N}$ is a diagonal matrix containing non zero singular values, $\mathbf{V}_1\in\mathbb{C}^{Q\times N}$ contains right singular vectors associated to non zero singular values of $\mathbf{A}$, $\mathbf{V}_2\in\mathbb{C}^{Q\times Q-N}$ contains right singular vectors that span the right null space of $\mathbf{A}$, $\mathbb{E}\left[\tilde{\mathbf{w}}\tilde{\mathbf{w}}^H\right] = \mathbf{I}_{\mathbf{Q-N}}$. Note that $\mathbf{w}'$ is independent from the other random variables and has a unit covariance matrix. Therefore, it can be shown that:

$$\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right] = \mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\sum_{k=1}^{N_E}\left|\mathbf{H}_{\mathbf{E},k}\right|^2\mathbf{V}_2\mathbf{V}_2^H\sum_{k'=1}^{N_E}\left|\mathbf{H}_{\mathbf{E},k'}\right|^2\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right]. \tag{C.12}$$

Let's rewrite $\left|\mathbf{H}_{\mathbf{E},k}\right|^2 = \sum_{q=1}^{Q}|h_{E,k,q}|^2\mathbf{e}_q\mathbf{e}_q^T$ where $\mathbf{e}_q$ is an all zero vector except a 1 at row q:

$$\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right] = \sum_{k=1}^{N_E}\sum_{k'=1}^{N_E}\sum_{q=1}^{Q}\sum_{q'=1}^{Q}\mathbb{E}\left[h_{E,k,q}|^2|h_{E,k',q'}|^2\right]\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.13}$$

From that, there are 4 possibilities: $k=k'$ and $q=q'$ or $q\neq q'$, or $k\neq k'$ and $q=q'$ or $q\neq q'$. It comes:

$$\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right] = \sum_{k=1}^{N_E}\sum_{q=1}^{Q}\mathbb{E}\left[|h_{E,k,q}|^4\right]\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14a}$$

$$+\sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{q=1}^{Q}\mathbb{E}\left[|h_{E,k,q}|^2|h_{E,k'q}|^2\right]\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14b}$$

$$+\sum_{k=1}^{N_E}\sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\mathbb{E}\left[|h_{E,k,q}|^2|h_{E,k,q'}|^2\right]\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14c}$$

$$+\sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\mathbb{E}\left[|h_{E,k,q}|^2|h_{E,k',q'}|^2\right]\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14d}$$

$$=2N_E\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14e}$$

$$+N_E(N_E-1)\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14f}$$

$$+N_E\sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14g}$$

$$+N_E(N_E-1)\sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14h}$$

$$=N_E\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14i}$$

$$+N_E^2\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\sum_{q=1}^{Q}\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\sum_{q'=1}^{Q}\mathbf{e}_{q'}\mathbf{e}_q'^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14j}$$

$$=N_E\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right]+N_E^2\mathbb{E}\left[\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}_1^H\mathbf{V}_2\mathbf{V}_2^H\mathbf{V}_1\boldsymbol{\Sigma}^H\mathbf{U}^H\right] \tag{C.14k}$$

where the second term of (C.14k) cancels out since $\mathbf{V}_2^H\mathbf{V}_1=\mathbf{0}$. From that, it is observed that equation (C.14k) is exactly equals to N_E times (B.21). As a consequence, the expected energy of the received AN at Eve when she implements a MRC in a SISO-ME configuration is equal to N_E times the expected energy of the received AN at Eve when she implements a MF in a SISO-SE configuration. That is:

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{MRC}}|^2\right]=\frac{(1-\alpha)}{U+1}N_E. \tag{C.15}$$

D | Multi-Input Single-Output Multi-eavesdropper

D.1 Bob ergodic SINR modeling

D.1.1 Data term

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha(1-\sigma)}}{N_A U}\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2 + \frac{\sqrt{\alpha\sigma}}{N_A U}\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}h_{\mathrm{B},k,i}\Delta h^*_{\mathrm{B},k,i}\right|^2\right] \tag{D.1a}$$

$$= \frac{1}{N_A^2U^2}\mathbb{E}\left[\left(\sqrt{\alpha(1-\sigma)}\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2 + \frac{\sqrt{\alpha\sigma}}{N_A U}\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}h_{\mathrm{B},k,i}\Delta h^*_{\mathrm{B},k,i}\right)\right.$$
$$\left.\left(\sqrt{\alpha(1-\sigma)}\sum_{k'=1}^{N_A}\sum_{j=0}^{U-1}|h_{\mathrm{B},k',j}|^2 + \frac{\sqrt{\alpha\sigma}}{N_A U}\sum_{k'=1}^{N_A}\sum_{j=0}^{U-1}h_{\mathrm{B},k',j}\Delta h^*_{\mathrm{B},k',j}\right)^H\right] \tag{D.1b}$$

$$= \frac{1}{N_A^2U^2}\mathbb{E}\left[\alpha(1-\sigma)\left(\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^4 + \sum_{k=1}^{N_A}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},kj}|^2\right.\right.$$
$$\left.+\sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k',i}|^2 + \sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k',j}|^2\right) \tag{D.1c}$$
$$\left.+\alpha\sigma\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|\Delta h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k,i}|^2\right]$$

$$= \frac{1}{N_A^2U^2}\left[\alpha(1-\sigma)\left(2N_AU + N_AU(U-1) + N_AU(N_A-1) + N_AU(U-1)(N_A-1)\right)\right. \tag{D.1d}$$
$$\left.+\alpha\sigma N_AU\right]$$

$$= \frac{\alpha}{N_AU}\left[(1-\sigma)U + (1-\sigma)N_A + (1-\sigma)(N_AU - N_A - U + 1) + \sigma\right] \tag{D.1e}$$

$$= \frac{\alpha}{N_AU}\left[N_AU(1-\sigma) + 1\right]; \tag{D.1f}$$

D.1.2 AWGN term

$$\mathbb{E}\left[|B_{2,n}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{N_A U}}\sum_{i=0}^{U-1} v_{\mathrm{B},i}\right|^2\right] \tag{D.2a}$$

$$= \frac{1}{N_A U}\mathbb{E}\left[\left(\sum_{i=0}^{U-1} v_{\mathrm{B},i}\right)\left(\sum_{j=0}^{U-1} v_{\mathrm{B},j}\right)^H\right] \tag{D.2b}$$

$$= \frac{1}{N_A U} U\sigma_{\mathrm{B}}^2 = \frac{\sigma_{\mathrm{B}}^2}{N_A}. \tag{D.2c}$$

D.1.3 AN term

$$\mathbb{E}\left[|B_3|^2\right] = \mathbb{E}\left[\left|\left|\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_A}\mathbf{H}_{\mathbf{B},k}\mathbf{w}\right|\right|^2\right]. \tag{D.3}$$

The AN is generated such that $\mathbf{S}^H\sum_{k=1}^{N_A}\widehat{\mathbf{H}}_{\mathbf{B},k}\mathbf{w} = \mathbf{0}_N$. In addition:

$$\begin{aligned}&\sum_{k=1}^{N_A}\widehat{\mathbf{H}}_{\mathbf{B},k} = \sqrt{1-\sigma}\sum_{k=1}^{N_A}\mathbf{H}_{\mathbf{B},k} + \sqrt{\sigma}\sum_{k=1}^{N_A}\Delta\mathbf{H}_{\mathbf{B},k}\\ \Leftrightarrow &\sum_{k=1}^{N_A}\mathbf{H}_{\mathbf{B},k} = \sum_{k=1}^{N_A}\frac{\widehat{\mathbf{H}}_{\mathbf{B},k} - \sqrt{\sigma}\Delta\mathbf{H}_{\mathbf{B},k}}{\sqrt{1-\sigma}}\end{aligned} \tag{D.4}$$

From that, equation (D.3) becomes:

$$\mathbb{E}\left[|B_3|^2\right] = \mathbb{E}\left[\left|\left|\sqrt{1-\alpha}\mathbf{S}^H\sum_{k=1}^{N_A}\frac{\widehat{\mathbf{H}}_{\mathbf{B},k} - \sqrt{\sigma}\Delta\mathbf{H}_{\mathbf{B},k}}{\sqrt{1-\sigma}}\mathbf{w}\right|\right|^2\right] \tag{D.5a}$$

$$= \frac{(1-\alpha)\sigma}{1-\sigma}\mathbb{E}\left[\left|\left|\mathbf{S}^H\sum_{k=1}^{N_A}\Delta\mathbf{H}_{\mathbf{B},k}\mathbf{w}\right|\right|^2\right] \tag{D.5b}$$

Let's rewrite: $\mathbf{w} = \sqrt{1-\sigma}\hat{\mathbf{w}} + \sqrt{\sigma}\mathbf{w}_\Delta$, where $\mathbf{S}^H\sum_{k=1}^{N_A}\Delta\mathbf{H}_{\mathbf{B},k}\mathbf{w}_\Delta = \mathbf{0}_N$ and $\hat{\mathbf{w}} \perp\!\!\!\perp \Delta\mathbf{H}_{\mathbf{B},k}$, such that:

$$\mathbb{E}\left[|B_3|^2\right] = \frac{(1-\alpha)\sigma}{1-\sigma}(1-\sigma)\mathbb{E}\left[\left|\left|\mathbf{S}^H\sum_{k=1}^{N_A}\Delta\mathbf{H}_{\mathbf{B},k}\hat{\mathbf{w}}\right|\right|^2\right] \tag{D.6a}$$

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)\sigma}{UN_A}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|\Delta h_{B,k,i}|^2\,|w_i|^2\right] \tag{D.6b}$$

$$= \frac{(1-\alpha)\sigma}{UN_A}N_A U\frac{1}{UN_A} = \frac{(1-\alpha)\sigma}{N_A U}. \tag{D.6c}$$

D.2 Eve ergodic SINR modeling

D.2.1 SDS Decoder

D.2.1.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{N_A U}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},kl,i}\hat{h}_{\mathrm{B},k,i}^{*}\right|^2\right] \tag{D.7a}$$

$$= \mathbb{E}\left[\left(\frac{\sqrt{\alpha}}{N_A U}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},kl,i}\hat{h}_{\mathrm{B},k,i}^{*}\right)\left(\frac{\sqrt{\alpha}}{N_A U}\sum_{k'=1}^{N_A}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1} h_{\mathrm{E},k'l',j}\hat{h}_{\mathrm{B},k',j}^{*}\right)^H\right] \tag{D.7b}$$

$$= \frac{\alpha}{N_A^2 U^2}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\right] \tag{D.7c}$$

$$= \frac{\alpha}{N_A^2 U^2} U N_A N_E = \frac{\alpha N_E}{N_A} \tag{D.7d}$$

D.2.1.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{N_A U}}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} v_{\mathrm{E},l,i}\right|^2\right] \tag{D.8a}$$

$$= \frac{1}{N_A U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|v_{\mathrm{E},l,i}|^2\right] \tag{D.8b}$$

$$= \frac{1}{N_A U} U N_E \sigma_{\mathrm{E}}^2 = \frac{N_E}{N_A}\sigma_{\mathrm{E}}^2 \tag{D.8c}$$

D.2.1.3 AN term

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{1-\alpha}}{\sqrt{N_A U}}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},kl,i}w_i\right|^2\right] \tag{D.9a}$$

$$= \frac{1-\alpha}{N_A U}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},kl,i}w_i\sum_{k'=1}^{N_A}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1} h_{\mathrm{E},k'l',j}w_j\right] \tag{D.9b}$$

One must have in (D.9b): $i=j$, $k=k'$, $l=l'$. It comes:

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{SDS}}|^2\right] = \frac{1-\alpha}{N_A U}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2|w_i|^2\right] \tag{D.10a}$$

$$= \frac{1-\alpha}{N_A U} N_A N_E U \frac{1}{N_A U} = \frac{(1-\alpha)N_E}{N_A U} \tag{D.10b}$$

D.2.2 OC Decoder

D.2.2.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{N_A U}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\,\hat{h}_{\mathrm{B},k,i}^*\right|^2\right] \tag{D.11a}$$

$$= \frac{\alpha}{N_A^2U^2}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\,\hat{h}_{\mathrm{B},k,i}^*\sum_{k'=1}^{N_A}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1}h_{\mathrm{E},k'l',j}{}^2\hat{h}_{\mathrm{B},k',j}\right] \tag{D.11b}$$

One must have in (D.11b): $i=j$, $k=k'$, $l=l'$, or $i=j$, $k=k'$, $l\neq l'$. It comes:

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{OC}}|^2\right] = \frac{\alpha}{N_A^2U^2}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^4\left|\hat{h}_{\mathrm{B},k,i}\right|^2+\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},kl',i}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\right] \tag{D.12a}$$

$$= \frac{\alpha}{N_A^2U^2}\left[2UN_AN_E+UN_AN_E(N_E-1)\right] \tag{D.12b}$$

$$= \frac{\alpha N_E(N_E+1)}{N_AU} \tag{D.12c}$$

D.2.2.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{N_AU}}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}h_{\mathrm{E},kl,i}v_{\mathrm{E},l,i}\right|^2\right] \tag{D.13a}$$

$$= \frac{1}{N_AU}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\,|v_{\mathrm{E},l,i}|^2\right] \tag{D.13b}$$

$$= \frac{1}{N_AU}UN_AN_E\sigma_{\mathrm{E}}^2 = N_E\sigma_{\mathrm{E}}^2 \tag{D.13c}$$

D.2.2.3 AN term

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{1-\alpha}}{\sqrt{N_AU}}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\,w_i\right|^2\right] \tag{D.14a}$$

$$= \frac{1-\alpha}{N_AU}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\,w_i\sum_{k'=1}^{N_A}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1}\left|h_{\mathrm{E},k'l',j}\right|^2w_j^*\right] \tag{D.14b}$$

One must have in (D.14b): $i=j$, $k=k'$, $l=l'$, or $i=j$, $k=k'$, $l\neq l'$, or $i=j$, $k\neq k'$, $l=l'$, or $i=j$, $k\neq k'$, $l\neq l'$. It comes:

$$\begin{aligned}\mathbb{E}\left[\left|E_{3,n}^{\mathrm{OC}}\right|^2\right] =& \frac{1-\alpha}{N_A U}\mathbb{E}\Bigg[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},kl,i}\right|^4\left|w_i\right|^2+\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},kl,i}\right|^2\left|h_{\mathrm{E},kl',i}\right|^2\left|w_i\right|^2 \\ &+\sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},kl,i}\right|^2\left|h_{\mathrm{E},k'l,i}\right|^2\left|w_i\right|^2+\sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},kl,i}\right|^2\left|h_{\mathrm{E},k'l',i}\right|^2\left|w_i\right|^2\Bigg] \end{aligned} \tag{D.15a}$$

$$= \frac{1-\alpha}{N_A U}UN_AN_E\frac{1}{N_A U}\left[2+N_A-1+N_E-1+(N_A-1)(N_E-1)\right] \tag{D.15b}$$

$$= \frac{(1-\alpha)N_E}{N_A U}(N_AN_E+1) \tag{D.15c}$$

D.2.3 MRC Decoder

D.2.3.1 Data term

$$\mathbb{E}\left[\left|E_{1,n}^{\mathrm{MRC}}\right|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{N_A U}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},kl,i}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\right|^2\right] \tag{D.16a}$$

$$= \frac{\alpha}{N_A^2U^2}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},kl,i}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\sum_{k'=1}^{N_A}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1}{h_{\mathrm{E},k'l',j}}^2\left|\hat{h}_{\mathrm{B},k',j}\right|^2\right] \tag{D.16b}$$

One must have in (D.16b): $i=j$, $k=k'$, $l=l'$, or $i=j$, $k=k'$, $l\neq l'$, or $i=j$, $k\neq k'$, $l=l'$, or $i=j$, $k\neq k'$, $l\neq l'$, or $i\neq j$, $k=k'$, $l=l'$, or $i\neq j$, $k=k'$, $l\neq l'$, or $i\neq j$, $k\neq k'$, $l=l'$, or $i\neq j$, $k\neq k'$, $l\neq l'$.

It comes:

$$\begin{aligned}\mathbb{E}\left[|E_{1,n}^{\mathrm{MRC}}|^2\right] =& \frac{\alpha}{N_A^2U^2}\mathbb{E}\Bigg[\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^4\left|\hat{h}_{\mathrm{B},k,i}\right|^4+\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},kl',i}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^4\\
&+\sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},k'l,i}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',i}\right|^2\\
&+\sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},k'l',i}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',i}\right|^2\\
&+\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},kl,j}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k,j}\right|^2\\
&+\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},kl',j}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k,j}\right|^2\Bigg]\\
&+\sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},k'l,j}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',j}\right|^2\Bigg]\\
&+\sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},kl,i}|^2\left|h_{\mathrm{E},k'l',j}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',j}\right|^2\Bigg].\end{aligned} \tag{D.17a}$$

In each term of (D.17a), a factor UN_AN_E can be put outside. It follows:

$$\begin{aligned}\mathbb{E}\left[|E_{1,n}^{\mathrm{MRC}}|^2\right] =& \frac{\alpha N_E}{N_AU}\left[4+N_A-1+2(N_E-1)+N_AN_E-N_E-N_A+1+U-1+N_AU-U-N_A\right.\\
&\left.+1+N_EU-U-N_E+1+(U-1)(N_A-1)(N_E-1)\right]\end{aligned} \tag{D.18a}$$

$$= \frac{\alpha N_E}{N_AU}\left[2+N_E(N_AU+1)\right]. \tag{D.18b}$$

D.2.3.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{MRC}}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{N_AU}}\sum_{k=1}^{N_A}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}h_{\mathrm{E},kl,i}\hat{h}_{\mathrm{B},k,i}^{*}v_{\mathrm{E},l,i}\right|^2\right] \tag{D.19a}$$

$$= \frac{1}{N_AU}\mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},kl,i}|^2|h_{\mathrm{B},k,i}|^2|v_{\mathrm{E},l,i}|^2\right] \tag{D.19b}$$

$$= \frac{1}{N_AU}UN_AN_E\sigma_{\mathrm{E}}^2 = N_E\sigma_{\mathrm{E}}^2 \tag{D.19c}$$

D.2.3.3 AN term

The component $E_{3,n}^{\mathrm{MRC}}$ depends on $\mathbf{w}$ and $\widehat{\mathbf{H}}_{\mathbf{B},k}$ which are correlated via the AN design (4.15). The expectation is therefore not straightforward to compute.
As a reminder, the AN is generated such that:

$$\mathbf{A}\mathbf{w} = \mathbf{0}_N \tag{D.20}$$

with:

$$\mathbf{A} = \mathbf{S}^H \sum_{k=1}^{N_A} \widehat{\mathbf{H}}_{\mathbf{B},k} = \mathbf{U}\mathbf{\Sigma}\mathbf{V_1}^H \in \mathbb{C}^{N\times Q} \tag{D.21}$$

Omitting the $1-\alpha$ as well as the normalization factor in (4.17), the AN term at Eve is given by:

$$\begin{aligned}\mathbf{v} &= \mathbf{A}\sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},lk}||^2 \mathbf{w} = \mathbf{S}^H \widehat{\mathbf{H}}_{\mathbf{B}} \sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},lk}||^2 \mathbf{w} \\ &= \mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H \sum_{l=1}^{N_E} ||\mathbf{H}_{\mathbf{E},lk}||^2 \mathbf{V}_2 \mathbf{w}',\end{aligned} \tag{D.22}$$

Equation (D.22) is equivalent to (C.11), such that:

$$\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right] = N_E \sum_{q=1}^{Q} \mathbb{E}\left[\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_1 \mathbf{\Sigma}^H \mathbf{U}^H\right] \tag{D.23}$$

From that, and remembering (B.26), it can be shown that:

$$\begin{aligned}\frac{1}{N}\mathbb{E}\left[|\mathbf{v}|^2\right] &= N_E \frac{1}{N} \sum_{q=1}^{Q} \mathbb{E}\left[\left(\|\mathbf{v}_{1,q}\|^2 - \|\mathbf{v}_{1,q}\|^4\right)\sigma_n^2\right] \\ &= \frac{1}{N}\sum_{q=1}^{Q}\sum_{k=1}^{N_A} \mathbb{E}\left[\left(|\mathbf{v}_{1,k,q}|^2 - |\mathbf{v}_{1,k,q}|^4\right)\sigma_{n,k}^2\right]\end{aligned} \tag{D.24}$$

To determine (D.24), the transformations performed by the SVD on $\mathbf{A}$ in order to obtain $\mathbf{v}_{1,k,q}$ and σ_{nk}^2 need to be determined.
One has:

$$|\mathbf{v}_{1,k,q}|^2 = \frac{|z_{k,q}|^2}{|\sigma_{1k}|^2} \tag{D.25a}$$

$$|\mathbf{v}_{1,k,q}|^4 = \frac{|z_{k,q}|^4}{|\sigma_{1k}|^4} \tag{D.25b}$$

One can show that:

$$\sigma_{1k} = \sqrt{\sum_{k=1}^{N_A}\sum_{i=0}^{U-1} |z_{k,i}|^2}, \tag{D.26}$$

where $z_{k,i} \sim \mathcal{CN}(0, \frac{1}{N_A U})$. Therefore:

$$\mathbb{E}\left[|z_{k,i}|^2\right] = \mathbb{E}\left[\left|\frac{1}{N_A U}\hat{h}_{\mathrm{B},k,i}\right|^2\right] = \frac{1}{N_A U} \tag{D.27a}$$

$$\mathbb{E}\left[|z_{k,i}|^4\right] = \mathbb{E}\left[\left|\frac{1}{N_A U}\hat{h}_{\mathrm{B},k,i}\right|^4\right] = \frac{2}{N_A^2 U^2}. \tag{D.27b}$$

From that:

$$\mathbb{E}\left[|\sigma_{1k}|^2\right] = \mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|z_{k,i}|^2\right] = \frac{1}{N_A U} N_A U = 1. \tag{D.28}$$

In addition:

$$\mathbb{E}\left[|\sigma_{1k}|^4\right] = \mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|z_{k,i}|^2\sum_{k'=1}^{N_A}\sum_{j=0}^{U-1}|z_{k',j}|^2\right] \tag{D.29a}$$

$$= \mathbb{E}\left[\sum_{k=1}^{N_A}\sum_{i=0}^{U-1}|z_{k,i}|^4 + \sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{i=0}^{U-1}|z_{k,i}|^2|z_{k',i}|^2 + \sum_{k=1}^{N_A}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|z_{k,i}|^2|z_{k,j}|^2 + \sum_{k=1}^{N_A}\sum_{\substack{k'=1\\k'\neq k}}^{N_A}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|z_{k,i}|^2|z_{k',j}|^2\right] \tag{D.29b}$$

$$= UN_A\left[\frac{2}{N_A^2U^2} + \frac{N_A-1}{N_A^2U^2} + \frac{U-1}{N_A^2U^2} + \frac{(U-1)(N_A-1)}{N_A^2U^2}\right] \tag{D.29c}$$

$$= \frac{N_AU+1}{N_AU}. \tag{D.29d}$$

With (D.25), (D.27), (D.28), and (D.29), it follows:

$$\mathbb{E}\left[\left(|\mathbf{v}_{1,k,q}|^2 - |\mathbf{v}_{1,k,q}|^4\right)|\sigma_{1k}|^2\right] = \frac{1}{N_AU} - \frac{\frac{2}{N_A^2U^2}}{\frac{N_AU+1}{N_AU}} = \frac{1}{N_AU}\frac{N_AU-1}{N_AU+1}. \tag{D.30}$$

Equation (D.24) becomes:

$$\begin{aligned}\frac{1}{N}\mathbb{E}\left[|\mathbf{v}|^2\right] &= N_E\frac{1}{N}\sum_{q=1}^{Q}\sum_{k=1}^{N_A}\mathbb{E}\left[\left(|\mathbf{v}_{1,k,q}|^2 - |\mathbf{v}_{1,q}|^4\right)\sigma_{n,k}^2\right]\\ &= N_E\frac{1}{N}\sum_{q=1}^{Q}\sum_{k=1}^{N_A}\frac{1}{N_AU}\frac{N_AU-1}{N_AU+1}\\ &= N_E\frac{1}{N}QN_A\frac{1}{N_AU}\frac{N_AU-1}{N_AU+1} = N_E\frac{N_AU-1}{N_AU+1}.\end{aligned} \tag{D.31}$$

Considering the $(1-\alpha)$ term and the normalization factor in (4.17), the AN term at Eve is finally given by:

$$\mathbb{E}\left[|E_{3n}^{\mathrm{MRC}}|^2\right] = N_E\frac{N_AU-1}{N_AU+1}\frac{(1-\alpha)}{N_AU-1} \tag{D.32a}$$

$$= \frac{(1-\alpha)N_E}{N_AU+1}. \tag{D.32b}$$

E | Single-Input Multi-Output Multi-eavesdropper

E.1 Bob ergodic SINR modeling

E.1.1 Scheme 1 : SIMO without precoding

E.1.1.1 Data term

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2 + \frac{\sqrt{\alpha\sigma}}{U}\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}h_{\mathrm{B},k,i}\Delta h^*_{\mathrm{B},k,i}\right|^2\right] \tag{E.1a}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\Bigg[\left((1-\sigma)\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2 + \sqrt{\sigma}\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}h_{\mathrm{B},k,i}\Delta h^*_{\mathrm{B},k,i}\right) \left(\sqrt{1-\sigma}\sum_{k'=1}^{N_B}\sum_{j=0}^{U-1}|h_{\mathrm{B},k',j}|^2 + \sqrt{\sigma}\sum_{k'=1}^{N_B}\sum_{j=0}^{U-1}h_{\mathrm{B},k',j}\Delta h_{\mathrm{B},k',j}\right)^H\Bigg] \tag{E.1b}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\Bigg[(1-\sigma)\Bigg[\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^4 + \sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k',i}|^2 + \sum_{k=1}^{N_B}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k,j}|^2 + \sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k',j}|^2\Bigg] + \sigma\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|\Delta h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k,i}|^2\Bigg] \tag{E.1c}$$

$$= \frac{\alpha}{U^2}\left[(1-\sigma)\left[2UN_B + UN_B(N_B-1) + U(U-1)N_B + U(U_1)N_B(N_B-1)\right] + \sigma UN_B\right] \tag{E.1d}$$

$$= \frac{\alpha N_B}{U}\left[(1-\sigma)\left[2+N_B-1+U-1+(U-1)(N_B-1)\right] + \sigma\right] \tag{E.1e}$$

$$= \frac{\alpha N_B}{U}\left[UN_B(1-\sigma)+1\right]. \tag{E.1f}$$

E.1.1.2 AWGN term

$$\mathbb{E}\left[|B_{2,n}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}\hat{h}^*_{\mathrm{B},k,i}v_{\mathrm{B},k,i}\right|^2\right] \tag{E.2a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2|v_{\mathrm{B},k,i}|^2\right] \tag{E.2b}$$

$$= \frac{1}{U}UN_B\sigma^2_{\mathrm{B}} = N_B\sigma^2_{\mathrm{B}}. \tag{E.2c}$$

E.1.1.3 AN term

From Bob's estimated channel formula, it comes:

$$\sqrt{1-\alpha}\mathbb{E}\left[\mathbf{S}^H\sum_{k=1}^{N_E}\mathbf{H}_{\mathbf{B},k}\widehat{\mathbf{H}}^H_{\mathbf{B},k}\mathbf{w}\right] = \sqrt{1-\alpha}\mathbb{E}\left[\mathbf{S}^H\sum_{k=1}^{N_B}\widehat{\mathbf{H}}_{\mathbf{B},k}\left(\sqrt{1-\sigma}\widehat{\mathbf{H}}^H_{\mathbf{B},k}+\sqrt{\sigma}\Delta\mathbf{H}^H_{\mathbf{B},k}\right)\mathbf{w}\right] \tag{E.3a}$$

$$= \sqrt{(1-\alpha)\sigma}\mathbb{E}\left[\mathbf{S}^H\sum_{k=1}^{N_B}\mathbf{H}_{\mathbf{B},k}\Delta\mathbf{H}^H_{\mathbf{B},k}\mathbf{w}\right] \tag{E.3b}$$

Therefore, it follows:

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)\sigma}{U}\mathbb{E}\left[\left(\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}h_{\mathrm{B},k,i}\Delta h_{\mathrm{B},k,i}w_i\right)\left(\sum_{k'=1}^{N_B}\sum_{j=0}^{U-1}h_{\mathrm{B},k',j}\Delta h_{\mathrm{B},k',j}w_j\right)^H\right] \tag{E.4a}$$

$$= \frac{(1-\alpha)\sigma}{U}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2|\Delta h_{\mathrm{B},k,i}|^2|w_i|^2\right] \tag{E.4b}$$

$$= \frac{(1-\alpha)\sigma}{U}UN_B\frac{1}{U} \tag{E.4c}$$

$$= \frac{(1-\alpha)\sigma N_B}{U} \tag{E.4d}$$

E.1.2 Scheme 2 : SIMO with precoding

E.1.2.1 Data term

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{\sqrt{N_B}U}\sum_{k=1}^{N_B}\sum_{k'=1}^{N_B}\sum_{i=0}^{U-1} h_{\mathrm{B},k,i}\hat{h}^*_{\mathrm{B},k',i}\right|^2\right] \tag{E.5a}$$

$$= \frac{\alpha}{N_B U^2}\mathbb{E}\Bigg[\left(\sum_{k=1}^{N_B}\sum_{k'=1}^{N_B}\sum_{i=0}^{U-1} h_{\mathrm{B},k,i}(\sqrt{1-\sigma}h^*_{\mathrm{B},k',i} + \sqrt{\sigma}\Delta h^*_{\mathrm{B},k',i})\right) \left(\sum_{l=1}^{N_B}\sum_{l'=1}^{N_B}\sum_{j=0}^{U-1} h_{\mathrm{B},l,j}(\sqrt{1-\sigma}h^*_{\mathrm{B},l',j} + \sqrt{\sigma}\Delta h^*_{\mathrm{B},l',j})\right)^H\Bigg] \tag{E.5b}$$

$$\begin{aligned}= \frac{\alpha}{N_B U^2}\mathbb{E}\Bigg[(1-\sigma)\Bigg[&\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^4 + 2\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{i=0}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k',i}|^2 \\ &+ \sum_{k=1}^{N_B}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k,j}|^2 + \sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k',j}|^2\Bigg] \\ &+ \sigma\Bigg[\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|\Delta h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k,i}|^2 + \sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{i=0}^{U-1}|\Delta h_{\mathrm{B},k,i}|^2|h_{\mathrm{B},k',i}|^2\Bigg]\Bigg]\end{aligned} \tag{E.5c}$$

$$= \frac{\alpha}{N_B U^2}N_B U\left[(1-\sigma)\left[2+2N_B-2+U-1+(U_1)(N_B-1)\right]+\sigma(1+N_B-1)\right] \tag{E.5d}$$

$$= \frac{\alpha N_B}{U}\left[(1-\sigma)\left[2+N_B-1+U-1+(U-1)(N_B-1)\right]+\sigma\right] \tag{E.5e}$$

$$= \frac{\alpha N_B}{U}\left[U(1-\sigma)+1\right]. \tag{E.5f}$$

E.1.2.2 AWGN term

$$\mathbb{E}\left[|B_{2,n}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{k=1}^{N_B}\sum_{i=0}^{U-1} v_{\mathrm{B},ki}\right|^2\right] \tag{E.6a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{i=0}^{U-1}|v_{\mathrm{B},k,i}|^2\right] \tag{E.6b}$$

$$= \frac{1}{U}UN_B\sigma^2_{\mathrm{B}} = N_B\sigma^2_{\mathrm{B}}. \tag{E.6c}$$

E.1.2.3 AN term

From Bob's estimated channel formula, it comes:

$$\sqrt{1-\alpha}\mathbb{E}\left[\mathbf{S}^H\sum_{k=1}^{N_B}\mathbf{H}_{\mathbf{B},k}\mathbf{w}\right] = \sqrt{1-\alpha}\mathbb{E}\left[\mathbf{S}^H\sum_{k=1}^{N_B}\left(\sqrt{1-\sigma}\widehat{\mathbf{H}}_{\mathbf{B},k}+\sqrt{\sigma}\Delta\mathbf{H}_{\mathbf{B},k}\right)\mathbf{w}\right] \tag{E.7a}$$

$$= \sqrt{(1-\alpha)\sigma}\mathbb{E}\left[\mathbf{S}^H\sum_{k=1}^{N_B}\Delta\mathbf{H}_{\mathbf{B},k}\mathbf{w}\right] \tag{E.7b}$$

Therefore, it follows:

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)\sigma}{U}\mathbb{E}\left[\left(\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\Delta h_{\mathrm{B},k,i}w_i\right)\left(\sum_{k'=1}^{N_E}\sum_{j=0}^{U-1}\Delta h_{\mathrm{B},k',j}w_j\right)^H\right] \tag{E.8a}$$

$$= \frac{(1-\alpha)\sigma}{U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|\Delta h_{\mathrm{B},k,i}|^2|w_i|^2\right] \tag{E.8b}$$

$$= \frac{(1-\alpha)\sigma}{U}UN_B\frac{1}{U} \tag{E.8c}$$

$$= \frac{(1-\alpha)\sigma N_B}{U} \tag{E.8d}$$

E.2 Eve ergodic SINR modeling

E.2.1 Scheme 1 : SIMO without precoding

E.2.1.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{MRC}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2\right|^2\right] \tag{E.9a}$$

$$\begin{aligned}= \frac{\alpha}{U^2}\mathbb{E}\Bigg[&\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2 + \sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{E},k',i}|^2 \\ &+ \sum_{k=1}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{E},k,j}|^2 + \sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{E},k,i}|^2|h_{\mathrm{E},k',j}|^2\Bigg]\end{aligned} \tag{E.9b}$$

$$= \frac{\alpha}{U^2}UN_E(2+U-1+N_E-1+(U-1)(N_E-1)) = \frac{\alpha}{U}N_E(UN_E+1). \tag{E.9c}$$

E.2.1.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{MRC}}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}h_{\mathrm{E},k,i}^*v_{\mathrm{E},k,i}\right|^2\right] \tag{E.10a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{i=0}^{U-1}|h_{\mathrm{E},k,i}|^2|v_{\mathrm{E},k,i}|^2\right] \tag{E.10b}$$

$$= \frac{1}{U}UN_E\sigma_{\mathrm{E}}^2 = N_E\sigma_{\mathrm{E}}^2 \tag{E.10c}$$

E.2.1.3 AN term

The AN should satisfy:

$$\mathbf{A}\mathbf{w} = \mathbf{0}_N \tag{E.11}$$

with:

$$\mathbf{A} = \mathbf{S}^H\sum_{k=1}^{N_B}||\mathbf{H}_{\mathbf{B},k}||^2 = \mathbf{U}\mathbf{\Sigma}\mathbf{V_1}^H \in \mathbb{C}^{N\times Q} \tag{E.12}$$

with $\mathbf{U}\in\mathbb{C}^{N\times N}$ contains left singular vectors, $\mathbf{\Sigma}\in\mathbb{R}^{N\times N}$ is a diagonal matrix containing non zero singular values, $\mathbf{V}_1\in\mathbb{C}^{Q\times N}$ contains right singular vectors associated to non zero singular values of $\mathbf{A}$.

The expected energy per received symbol of the AN at Eve has to be computed. It is given by:

$$\tilde{\mathbf{v}} = \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} ||\mathbf{H_{E},}_k||^2 \mathbf{w} \tag{E.13}$$

$$= \sqrt{1-\alpha}\mathbf{S}^H \sum_{k=1}^{N_E} ||\mathbf{H_{E},}_k||^2 \mathbf{V_2}\tilde{\mathbf{w}} \tag{E.14}$$

with $\mathbb{E}\left[\tilde{\mathbf{w}}\tilde{\mathbf{w}}^H\right] = \mathbf{I_{Q-N}}$, $\mathbf{V}_2 \in \mathbb{C}^{Q\times Q-N}$ contains right singular vectors that span the right null space of $\mathbf{A}$.
In the following we define $\mathbf{v}$ by omitting the factor $\sqrt{1-\alpha}$ in $\tilde{\mathbf{v}}$. Also, It is found that $\mathbb{E}\left[\mathbf{w}\mathbf{w}^H\right] = \frac{U-1}{U}\mathbf{I_Q}$. However, in simulation, it is considered that $\mathbb{E}\left[\mathbf{w}\mathbf{w}^H\right] = \frac{1}{U}\mathbf{I_Q}$. Therefore, the final result that will be derived below should be multiplied by $\frac{1}{U-1}$ to fit with the simulations hypothesis.
As a consequence, one has to compute:

$$\frac{1}{N}\mathbb{E}\left[||\mathbf{v}||^2\right] = \frac{1}{N} tr\left(\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right]\right) \tag{E.15}$$

where $tr(.)$ is the trace operator. Equation (E.15) is the mean energy per component of the vector $\mathbf{v}$, defined as:

$$\mathbf{v} = \mathbf{S}^H \sum_{k=1}^{N_E} ||\mathbf{H_{E},}_k||^2 \mathbf{V_2}\tilde{\mathbf{w}} \tag{E.16}$$

It follows:

$$\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right] = \mathbb{E}\left[\mathbf{S}^H \sum_{k=1}^{N_E} ||\mathbf{H_{E},}_k||^2 \mathbf{V_2}\tilde{\mathbf{w}}\tilde{\mathbf{w}}^H{\mathbf{V_2}}^H \sum_{k'=1}^{N_E} ||\mathbf{H_{E},}_{k'}||^2 \mathbf{S}\right] \tag{E.17}$$

$$= \mathbf{S}^H \mathbb{E}\left[\sum_{k=1}^{N_E} ||\mathbf{H_{E},}_k||^2 \mathbf{V_2}\mathbf{V_2}^H \sum_{k'=1}^{N_E} ||\mathbf{H_{E},}_{k'}||^2\right] \mathbf{S} \tag{E.18}$$

$||\mathbf{H_{E},}_k||^2$ can be rewrite as $||\mathbf{H_{E},}_k||^2 = \sum_{q=1}^{Q} |h_{E,k,q}|^2 \mathbf{e_q}\mathbf{e_q^T}$ where $\mathbf{e_q}$ is an all-zero vector of dimension $Q \times 1$, with a one at row q. Therefore, since $||\mathbf{H}_{E,k}||^2$ is an random variable independent from the others, it comes:

$$\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right] = \mathbf{S}^H \mathbb{E}\left[\sum_{k=1}^{N_E}\sum_{k'=1}^{N_E}\sum_{q=1}^{Q}\sum_{q'=1}^{Q} |h_{E,k,q}|^2 |h_{E,k',q'}|^2\right] \mathbb{E}\left[\mathbf{e_q}{\mathbf{e_q}}^T \mathbf{V_2}\mathbf{V_2}^H \mathbf{e_{q'}}{\mathbf{e_{q'}}}^T\right] \mathbf{S} \tag{E.19}$$

$$= \mathbf{S}^H \sum_{k=1}^{N_E}\sum_{k'=1}^{N_E}\sum_{q=1}^{Q}\sum_{q'=1}^{Q} \mathbb{E}\left[|h_{E,k,q}|^2 |h_{E,k',q'}|^2\right] \mathbb{E}\left[\mathbf{e_q}{\mathbf{e_q}}^T \mathbf{V_2}\mathbf{V_2}^H \mathbf{e_{q'}}{\mathbf{e_{q'}}}^T\right] \mathbf{S} \tag{E.20}$$

$$= \mathbf{S}^H \sum_{q=1}^{Q}\sum_{k=1}^{N_E} \mathbb{E}\left[|h_{E,k,q}|^4\right] \mathbb{E}\left[\mathbf{e_q}{\mathbf{e_q}}^T \mathbf{V_2}\mathbf{V_2}^H \mathbf{e_q}{\mathbf{e_q}}^T\right] \mathbf{S} \tag{E.21}$$

$$+ \mathbf{S}^H \sum_{q=1}^{Q}\sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E} \mathbb{E}\left[|h_{E,k,q}|^2 |h_{E,k',q}|^2\right] \mathbb{E}\left[\mathbf{e_q}{\mathbf{e_q}}^T \mathbf{V_2}\mathbf{V_2}^H \mathbf{e_q}{\mathbf{e_q}}^T\right] \mathbf{S} \tag{E.22}$$

$$+ \mathbf{S}^H \sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\sum_{k=1}^{N_E} \mathbb{E}\left[|h_{E,k,q}|^2 |h_{E,k,q'}|^2\right] \mathbb{E}\left[\mathbf{e_q}{\mathbf{e_q}}^T \mathbf{V_2}\mathbf{V_2}^H \mathbf{e_{q'}}{\mathbf{e_{q'}}}^T\right] \mathbf{S} \tag{E.23}$$

$$+ \mathbf{S}^H \sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\sum_{k=1}^{N_E}\sum_{\substack{k'=1\\k'\neq k}}^{N_E} \mathbb{E}\left[|h_{E,k,q}|^2 |h_{E,k',q'}|^2\right] \mathbb{E}\left[\mathbf{e_q}{\mathbf{e_q}}^T \mathbf{V_2}\mathbf{V_2}^H \mathbf{e_{q'}}{\mathbf{e_{q'}}}^T\right] \mathbf{S} \tag{E.24}$$

$$=2N_E\mathbf{S}^H\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S} \tag{E.25}$$

$$+N_E(N_E-1)\mathbf{S}^H\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S} \tag{E.26}$$

$$+N_E\mathbf{S}^H\sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_{q'}}\mathbf{e_{q'}}^T\right]\mathbf{S} \tag{E.27}$$

$$+N_E(N_E-1)\mathbf{S}^H\sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_{q'}}\mathbf{e_{q'}}^T\right]\mathbf{S} \tag{E.28}$$

$$=N_E(N_E+1)\mathbf{S}^H\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S} \tag{E.29}$$

$$+N_E^2\mathbf{S}^H\sum_{q=1}^{Q}\sum_{\substack{q'=1\\q'\neq q}}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_{q'}}\mathbf{e_{q'}}^T\right]\mathbf{S} \tag{E.30}$$

$$=N_E\mathbf{S}^H\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S}+N_E^2\mathbf{S}^H\sum_{q=1}^{Q}\sum_{q'=1}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_{q'}}\mathbf{e_{q'}}^T\right]\mathbf{S} \tag{E.31}$$

$$=N_E\mathbf{S}^H\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S}+N_E^2\mathbf{S}^H\mathbb{E}\left[\mathbf{V_2}\mathbf{V_2}^H\right]\mathbf{S} \tag{E.32}$$

Going from (E.31) to (E.32) comes from the fact that $\sum_{q=1}^{Q}\mathbf{e_q}\mathbf{e_q}^T=\mathbf{I_Q}$. From that, it comes:

$$\frac{1}{N}\mathbb{E}\left[||\mathbf{v}||^2\right]=\frac{1}{N}tr\left(\mathbb{E}\left[\mathbf{v}\mathbf{v}^H\right]\right) \tag{E.33}$$

$$=\frac{1}{N}tr\left(N_E\mathbf{S}^H\sum_{q=1}^{Q}\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S}+N_E^2\mathbf{S}^H\mathbb{E}\left[\mathbf{V_2}\mathbf{V_2}^H\right]\mathbf{S}\right) \tag{E.34}$$

$$=\underbrace{\frac{N_E}{N}\sum_{q=1}^{Q}tr\left(\mathbf{S}^H\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S}\right)}_{(1)}+\underbrace{\frac{N_E^2}{N}tr\left(\mathbf{S}^H\mathbb{E}\left[\mathbf{V_2}\mathbf{V_2}^H\right]\mathbf{S}\right)}_{(2)} \tag{E.35}$$

The first term of (E.35) is easy to compute:

$$(1)=\frac{N_E}{N}\sum_{q=1}^{Q}tr\left(\mathbf{S}^H\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T\mathbf{V_2}\mathbf{V_2}^H\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S}\right) \tag{E.36}$$

$$=\frac{N_E}{N}\sum_{q=1}^{Q}tr\left(\mathbf{S}^H\mathbb{E}\left[\mathbf{e_q}\mathbf{e_q}^T||\mathbf{v_{2,q}}||^2\mathbf{e_q}\mathbf{e_q}^T\right]\mathbf{S}\right) \tag{E.37}$$

$$=\frac{N_E}{N}Q\frac{1}{U}\frac{U-1}{U}=N_E\frac{U-1}{U} \tag{E.38}$$

where $\mathbf{v_{2,q}}$ is the q^{th} column of $\mathbf{V_2}^H$ (of dimension $Q-N\times 1$).
For the second term in (E.35), it can be noticed that $\mathbf{V_2}\mathbf{V_2}^H$ can be rewritten as:

$$\mathbf{V_2}\mathbf{V_2}^H=\mathbf{I}_Q-\mathbf{A}^H\left(\mathbf{A}\mathbf{A}^H\right)^{-1}\mathbf{A} \tag{E.39}$$

with $\mathbf{A}$ defined in (E.12). Introducing (E.39) in the second term of (E.35), it comes:

$$(2)=\frac{N_E^2}{N}\,tr\left(\mathbf{S}^H\mathbb{E}\left[\mathbf{I}_Q-\mathbf{A}^H\left(\mathbf{A}\mathbf{A}^H\right)^{-1}\mathbf{A}\right]\mathbf{S}\right) \tag{E.40}$$

$$= \underbrace{\frac{N_E^2}{N}\, tr\left(\mathbf{S}^H \mathbb{E}\left[\mathbf{I}_Q\right]\mathbf{S}\right)}_{(2.1)} - \underbrace{\frac{N_E^2}{N} tr\left(\mathbf{S}^H \mathbb{E}\left[\mathbf{A}^H\left(\mathbf{A}\mathbf{A}^H\right)^{-1}\mathbf{A}\right]\mathbf{S}\right)}_{(2.2)} \tag{E.41}$$

Term (2.1) in (E.41) can be computed as:

$$(2.1) = \frac{N_E^2}{N} tr\left(\mathbf{S}^H \mathbb{E}\left[\mathbf{I}_Q\right]\mathbf{S}\right) \tag{E.42}$$

$$= \frac{N_E^2}{N} tr\left(\mathbf{S}^H\mathbf{S}\right) = \frac{N_E^2}{N} tr\left(\mathbf{I}_N\right) = N_E^2 \tag{E.43}$$

The second term of (E.41) is given by:

$$(2.2) = \frac{N_E^2}{N}\, tr\left(\mathbf{S}^H \mathbb{E}\left[\mathbf{A}^H\left(\mathbf{A}\mathbf{A}^H\right)^{-1}\mathbf{A}\right]\mathbf{S}\right) \tag{E.44}$$

$$= \frac{N_E^2}{N}\, \mathbb{E}\left[tr\left(\mathbf{S}^H\mathbf{A}^H\left(\mathbf{A}\mathbf{A}^H\right)^{-1}\mathbf{A}\mathbf{S}\right)\right] \tag{E.45}$$

$$= \frac{N_E^2}{N}\, \mathbb{E}\left[tr\left(\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{B,k}||^2 \mathbf{S}\left(\mathbf{S}^H \sum_{k'=1}^{N_B} ||\mathbf{H}_{B,k'}||^2 \sum_{k''=1}^{N_B} ||\mathbf{H}_{B,k''}||^2 \mathbf{S}\right)^{-1} \mathbf{S}^H \sum_{k'''=1}^{N_B} ||\mathbf{H}_{B,k'''}||^2 \mathbf{S}\right)\right] \tag{E.46}$$

$$= \frac{N_E^2}{N}\, \mathbb{E}\left[tr\left(\mathbf{S}^H \sum_{k'''=1}^{N_B} ||\mathbf{H}_{B,k'''}||^2 \mathbf{S}\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{B,k}||^2 \mathbf{S}\left(\mathbf{S}^H \sum_{k'=1}^{N_B} ||\mathbf{H}_{B,k'}||^2 \sum_{k''=1}^{N_B} ||\mathbf{H}_{B,k''}||^2 \mathbf{S}\right)^{-1}\right)\right] \tag{E.47}$$

$$= \frac{N_E^2}{N}\, \mathbb{E}\left[tr\left(\left(\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{B,k}||^2 \mathbf{S}\right)^2 \left(\mathbf{S}^H \sum_{k'=1}^{N_B} ||\mathbf{H}_{B,k'}||^2 \sum_{k''=1}^{N_B} ||\mathbf{H}_{B,k''}||^2 \mathbf{S}\right)^{-1}\right)\right] \tag{E.48}$$

$$= \frac{N_E^2}{N}\, \mathbb{E}\left[tr\left(\mathbf{X}\mathbf{Y}^{-1}\right)\right] \tag{E.49}$$

Going from (E.46) to (E.47) holds since $tr\left(\mathbf{MN}\right) = tr\left(\mathbf{NM}\right)$ if $\mathbf{M}$ and $\mathbf{N}$ are squared matrices of same dimension.
Since $\mathbf{X}$ and $\mathbf{Y}$ are diagonal matrices in (E.49), the trace of $\mathbf{X}\mathbf{Y}^{-1}$ is simply the sum of the diagonal elements of the product $\mathbf{X}\mathbf{Y}^{-1}$. If we denote $\lambda_{x,i}$, $\forall i = 1...N$ and $\lambda_{y,i}$, $\forall i = 1...N$ as the eigenvalues of $\mathbf{X}$ and $\mathbf{Y}$ respectively, (E.49) becomes[1]:

$$\frac{N_E^2}{N}\, \mathbb{E}\left[tr\left(\mathbf{X}\mathbf{Y}^{-1}\right)\right] = \frac{N_E^2}{N} \sum_{i=1}^{N} \mathbb{E}\left[\frac{\lambda_{x,i}}{\lambda_{y,i}}\right] = N_E^2\, \mathbb{E}\left[\frac{\lambda_{x,i}}{\lambda_{y,i}}\right] \tag{E.50}$$

One can notice that the matrices $\mathbf{X}$ and $\mathbf{Y}$ can be written as:

$$\mathbf{X} = \tilde{\mathbf{X}}\tilde{\mathbf{X}}^H = \left(\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{B,k}||^2 \mathbf{S}\right)\left(\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{B,k}||^2 \mathbf{S}\right)^H \tag{E.51}$$

$$\mathbf{Y} = \tilde{\mathbf{Y}}\tilde{\mathbf{Y}}^H = \left(\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{B,k}||^2\right)\left(\mathbf{S}^H \sum_{k=1}^{N_B} ||\mathbf{H}_{B,k}||^2\right)^H \tag{E.52}$$

Furthermore, the eigenvalues of $\mathbf{X}$ (resp. $\mathbf{Y}$) are the square of the singular values of $\tilde{\mathbf{X}}$, (resp. $\tilde{\mathbf{Y}}$). If we denote $\sigma_{x,i}$, $\forall i = 1...N$ and $\sigma_{y,i}$, $\forall i = 1...N$ as the singular values of $\tilde{\mathbf{X}}$ and $\tilde{\mathbf{Y}}$ respectively, it is found that:

$$\sigma_{x,i} = \sqrt{\mathbb{E}\left[|\tilde{x}_i|^2\right]}, \tag{E.53}$$

[1] The diagonal elements of a diagonal matrix are its eigenvalues.

$$\sigma_{y,i} = \sqrt{\mathbb{E}\left[|\tilde{y}_i|^2\right]} \tag{E.54}$$

where $\tilde{x}_i$ (resp. $\tilde{y}_i$) is the i^{th} diagonal element of $\tilde{\mathbf{X}}$ (resp. $\tilde{\mathbf{Y}}$).
Therefore:

$$\sigma_{x,i}^2 = \lambda_{x,i} = \mathbb{E}\left[|\tilde{x}_i|^2\right] = \mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_B}|h_{B,k,i}|^2\right|^2\right] \tag{E.55}$$

$$= \frac{1}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}\sum_{k=1}^{N_B}|h_{B,k,i}|^2\sum_{j=0}^{U-1}\sum_{k'=1}^{N_B}|h_{B,k',j}|^2\right] \tag{E.56}$$

$$= \frac{1}{U^2}\mathbb{E}\Big[\sum_{i=0}^{U-1}\sum_{k=1}^{N_B}|h_{B,k,i}|^4 + \sum_{i=0}^{U-1}\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}|h_{B,k,i}|^2|h_{B,k',i}|^2 \tag{E.57}$$

$$+ \sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}\sum_{k=1}^{N_B}|h_{B,k,i}|^2|h_{B,k,j}|^2 + \sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}|h_{B,k,i}|^2|h_{B,k',j}|^2\Big] \tag{E.58}$$

$$= \frac{1}{U^2}\left[2UN_B + UN_B(N_B-1) + U(U-1)N_B + U(U-1)N_B(N_B-1)\right] \tag{E.59}$$

$$= \frac{N_B(N_BU+1)}{U} \tag{E.60}$$

Similarly:

$$\sigma_{y,i}^2 = \lambda_{y,i} = \mathbb{E}\left[|\tilde{y}_i|^2\right] = \mathbb{E}\left[\frac{1}{U}\sum_{i=0}^{U-1}\sum_{k=1}^{N_B}\sum_{k'=1}^{N_B}|h_{B,k,i}|^2|h_{B,k',i}|^2\right] \tag{E.61}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\sum_{k=1}^{N_B}|h_{B,k,i}|^4 + \sum_{i=0}^{U-1}\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}|h_{B,k,i}|^2|h_{B,k',i}|^2\right] \tag{E.62}$$

$$= \frac{1}{U}\left[2UN_B + UN_B(N_B-1)\right] \tag{E.63}$$

$$= N_B(N_B+1) \tag{E.64}$$

With (E.60) and (E.64) into (E.50), it turns out:

$$(2.2) = N_E^2\frac{N_BU+1}{N_BU+U} \tag{E.65}$$

Equation (E.41) can then be computed with (E.43) and (E.65) as:

$$(2) = (2.1) - (2.2) = N_E^2 - N_E^2\frac{N_BU+1}{N_BU+U} = N_E^2\frac{U-1}{U(N_B+1)} \tag{E.66}$$

The mean AN energy per received component at Eve, i.e., (E.35), can now be found thanks to (E.38) and (E.66) as:

$$\frac{1}{N}\mathbb{E}\left[||\mathbf{v}||^2\right] = (1) + (2) = N_E\frac{U-1}{U} + N_E^2\frac{U-1}{U(N_B+1)} \tag{E.67}$$

$$= N_E\frac{U-1}{U}\left(1 + \frac{N_E}{N_B+1}\right) \tag{E.68}$$

Finally, taking into account the scaling factor to have $\mathbb{E}\left[||\mathbf{w}||^2\right] = \frac{1}{U}\mathbf{I}_Q$ as well as the $\sqrt{1-\alpha}$ factor, it comes:

$$\frac{1}{N}\mathbb{E}\left[||\tilde{\mathbf{v}}||^2\right] = \frac{1-\alpha}{U}N_E\left(1 + \frac{N_E}{N_B+1}\right) \tag{E.69}$$

E.2.2 Scheme 2 : SIMO with precoding

E.2.2.1 SDS Decoder

E.2.2.1.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{\sqrt{N_B}U}\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},l,i}\hat{h}_{\mathrm{B},k,i}^{*}\right|^2\right] \tag{E.70a}$$

$$= \frac{\alpha}{N_B U^2}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},l,i}\hat{h}_{\mathrm{B},k,i}^{*}\sum_{k'=1}^{N_B}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1} h_{\mathrm{E},l',j}\hat{h}_{\mathrm{B},k',j}\right] \tag{E.70b}$$

$$= \frac{\alpha}{N_B U^2}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2\left|\hat{h}_{\mathrm{B},k,i}^{*}\right|^2\right] \tag{E.70c}$$

$$= \frac{\alpha N_E}{U}. \tag{E.70d}$$

E.2.2.1.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} v_{\mathrm{E},l,i}\right|^2\right] \tag{E.71a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |v_{\mathrm{E},l,i}|^2\right] \tag{E.71b}$$

$$= N_E\sigma_{\mathrm{E}}^2. \tag{E.71c}$$

E.2.2.1.3 AN term

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{SDS}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},l,i}w_i\right|^2\right] \tag{E.72a}$$

$$= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2|w_i|^2\right] \tag{E.72b}$$

$$= \frac{(1-\alpha)N_E}{U}. \tag{E.72c}$$

E.2.2.2 OC Decoder

E.2.2.2.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{\sqrt{N_B}U}\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2\hat{h}_{\mathrm{B},k,i}^{*}\right|^2\right] \tag{E.73a}$$

$$= \frac{\alpha}{N_B U^2}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2\hat{h}_{\mathrm{B},k,i}^{*}\sum_{k'=1}^{N_B}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1} \left|h_{\mathrm{E},l',j}\right|^2\hat{h}_{\mathrm{B},k',j}^{*}\right] \tag{E.73b}$$

$$= \frac{\alpha}{N_B U^2}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^4\left|\hat{h}_{\mathrm{B},k,i}\right|^2 + \sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2\left|h_{\mathrm{E},l',i}\right|^2\left|\hat{h}_{\mathrm{B},k,i}\right|^2\right] \tag{E.73c}$$

$$= \frac{\alpha}{N_B U^2}UN_BN_E(2+N_E-1) = \frac{\alpha}{U}N_E(N_E+1) \tag{E.73d}$$

E.2.2.2.2 AWGN term

$$\mathbb{E}\left[|E_{2,n}^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\frac{1}{\sqrt{U}}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} h_{\mathrm{E},l,i}^{*} v_{\mathrm{E},l,i}\right|^2\right] \tag{E.74a}$$

$$= \frac{1}{U}\mathbb{E}\left[\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2 |v_{\mathrm{E},l,i}|^2\right] \tag{E.74b}$$

$$= N_E\sigma_{\mathrm{E}}^2. \tag{E.74c}$$

E.2.2.2.3 AN term

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{OC}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2 w_i\right|^2\right] \tag{E.75a}$$

$$= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^4 |w_i|^2 + \sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2 |h_{\mathrm{E},l',i}|^2 |w_i|^2\right] \tag{E.75b}$$

$$= \frac{(1-\alpha)}{U}\frac{1}{U}N_E U(2+N_E-1) \tag{E.75c}$$

$$= \frac{(1-\alpha)}{U}N_E(N_E+1). \tag{E.75d}$$

E.2.2.3 MRC Decoder

E.2.2.3.1 Data term

$$\mathbb{E}\left[|E_{1,n}^{\mathrm{MRC}}|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{N_B U}\sum_{k=1}^{N_B}\sum_{k'=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2 \hat{h}_{\mathrm{B},k,i}^{*}\hat{h}_{\mathrm{B},k',i}\right|^2\right] \tag{E.76a}$$

$$= \frac{\alpha}{N_B^2U^2}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{k'=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1} |h_{\mathrm{E},l,i}|^2 \hat{h}_{\mathrm{B},k,i}^{*}\hat{h}_{\mathrm{B},k',i}\sum_{k''=1}^{N_B}\sum_{k'''=1}^{N_B}\sum_{l'=1}^{N_E}\sum_{j=0}^{U-1} |h_{\mathrm{E},l',j}|^2 \hat{h}_{\mathrm{B},k'',j}^{*}\hat{h}_{\mathrm{B},k''',j}\right] \tag{E.76b}$$

$$
\begin{aligned}
=&\frac{\alpha}{N_B^2U^2}\mathbb{E}\Bigg[\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^4|h_{\mathrm{E},l,i}|^4+2\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',i}\right|^2|h_{\mathrm{E},l,i}|^4\\
&+\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^4|h_{\mathrm{E},l,i}|^2|h_{\mathrm{E},l',i}|^2\\
&+2\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',i}\right|^2|h_{\mathrm{E},l,i}|^2|h_{\mathrm{E},l',i}|^2\\
&+\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k,j}\right|^2|h_{\mathrm{E},l,i}|^2|h_{\mathrm{E},l,j}|^2\\
&+\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',j}\right|^2|h_{\mathrm{E},l,i}|^2|h_{\mathrm{E},l,j}|^2\\
&+\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k,j}\right|^2|h_{\mathrm{E},l,i}|^2|h_{\mathrm{E},l',j}|^2\\
&+\sum_{k=1}^{N_B}\sum_{\substack{k'=1\\k'\neq k}}^{N_B}\sum_{l=1}^{N_E}\sum_{\substack{l'=1\\l'\neq l}}^{N_E}\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2\left|\hat{h}_{\mathrm{B},k',j}\right|^2|h_{\mathrm{E},l,i}|^2|h_{\mathrm{E},l',j}|^2\Bigg]
\end{aligned}
\tag{E.76c}
$$

$$
\begin{aligned}
=&\frac{\alpha N_E}{UN_B}\Big[4+4(N_B-1)+2(N_E-1)+2(N_B-1)(N_E-1)+(U-1)\\
&+(U-1)(N_B-1)+(U-1)(N_E-1)+(U-1)(N_B-1)(N_E-1)\Big]
\end{aligned}
\tag{E.76d}
$$

$$
=\frac{\alpha N_E}{UN_B}\left(2N_B+N_BN_E+UN_BN_E\right) \tag{E.76e}
$$

$$
=\frac{\alpha N_E}{U}\left[N_E(U+1)+2\right]. \tag{E.76f}
$$

E.2.2.3.2 AWGN term

$$
\mathbb{E}\left[|E_{2,n}^{\mathrm{MRC}}|^2\right]=\mathbb{E}\left[\left|\frac{1}{\sqrt{N_BU}}\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\hat{h}_{\mathrm{B},k,i}h_{\mathrm{E},l,i}^*v_{\mathrm{E},l,i}\right|^2\right] \tag{E.77a}
$$

$$
=\frac{1}{UN_B}\mathbb{E}\left[\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\left|\hat{h}_{\mathrm{B},k,i}\right|^2|h_{\mathrm{E},l,i}|^2|v_{\mathrm{E},l,i}|^2\right] \tag{E.77b}
$$

$$
=\frac{1}{UN_B}UN_BN_E\sigma_{\mathrm{E}}^2=N_E\sigma_{\mathrm{E}}^2. \tag{E.77c}
$$

E.2.2.3.3 AN term

$$
\mathbb{E}\left[|E_{3,n}^{\mathrm{MRC}}|^2\right]=\mathbb{E}\left[\left|\frac{\sqrt{1-\alpha}}{\sqrt{N_BU}}\sum_{k=1}^{N_B}\sum_{l=1}^{N_E}\sum_{i=0}^{U-1}\hat{h}_{\mathrm{B},k,i}|h_{\mathrm{E},l,i}|^2w_i\right|^2\right] \tag{E.78a}
$$

It directly comes that $\mathbb{E}\left[|E_{3,n}^{\mathrm{MRC}}|^2\right]$ is identical to the SISO-ME MRC scenario. It comes:

$$\mathbb{E}\left[|E_{3,n}^{\mathrm{MRC}}|^2\right] = \frac{(1-\alpha)}{U+1} N_E. \tag{E.79a}$$

Publications

[56] Golstein, Sidney, Nguyen, Trung-Hien, Horlin, François, Doncker, Philippe De, and Sarrazin, Julien. "Physical Layer Security in Frequency-Domain Time-Reversal SISO OFDM Communication". In: *2020 International Conference on Computing, Networking and Communications (ICNC)*. 2020, pp. 222–227. DOI: 10.1109/ICNC47757.2020.9049811 (see pp. 32, 38, 75).

[149] Golstein, Sidney, Rottenberg, François, Horlin, François, Doncker, Philippe De, and Sarrazin, Julien. "Physical Layer Security in an OFDM Time Reversal SISO Communication with Imperfect Channel State Information." In: *IEEE Access, submitted under minor reviewing*. 2022 (see p. 75).

[150] Golstein, Sidney, Rottenberg, François, Horlin, François, Doncker, Philippe De, and Sarrazin, Julien. "Physical Layer Security in an OFDM Time Reversal SISO Communication with Imperfect Channel State Information and Multiple Eavesdroppers." In: *IEEE Communications Letters, in preparation*. 2022 (see p. 75).

[153] Golstein, Sidney, Rottenberg, François, Horlin, François, Doncker, Philippe De, and Sarrazin, Julien. "Physical Layer Security in Time Reversal MISO/SIMO Communications with Imperfect Channel State Information and Multiple Eavesdroppers." In: *Journal Article, in preparation*. 2022 (see p. 119).

[154] Golstein, Sidney, Molineaux, Guylian, Odhiambo, Michael, Horlin, François, Doncker, Philippe De, and Sarrazin, Julien. "Spatial data focusing using time resources". In: *2019 Proc. of the 9th MC meeting and 9th Technical Meeting, organized by the COST Action CA15104, IRACON, Dublin, Ireland*. 2019.

[155] Golstein, Sidney, Odhiambo, Michael, Horlin, Francois, De Doncker, Philippe, and Sarrazin, Julien. "Focalisation Spatiale de Données via une approche temporelle". In: *Conference JNM 2019*. 21ème Journées Nationales Microondes. Caen, France, May 2019. https://hal.sorbonne-universite.fr/hal-03152245.

[156] Golstein, Sidney, Nguyen, Trung-Hien, Horlin, François, De Doncker, Philippe, and Sarrazin, Julien. "Influence du canal de propagation sur la sécurité d'une communication SISO utilisant le retournement temporel dans le domaine fréquentiel et l'ajout de bruit artificiel". In: *GDR Ondes 2019*. Huitième conférence plénière biennale du GDR ONDES -CentraleSupélec Gif-sur-Yvette -28-29 octobre 2019. Gyf-sur-Yvette, France, Oct. 2019. https://hal.sorbonne-universite.fr/hal-02870348.

Bibliography

[1] Bloch, Matthieu and Barros, João. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011. DOI: 10.1017/CBO9780511977985 (see pp. 1, 10, 12, 14, 18, 20, 21, 23, 67).

[2] *Cisco. Annual Internet Report (2018–2023). 2020. Available online:* https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf. Accessed: 2021-21-11 (see p. 1).

[3] Hamamreh, Jehad M., Furqan, Haji M., and Arslan, Huseyin. "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey". In: *IEEE Communications Surveys Tutorials* 21.2 (2019), pp. 1773–1828. DOI: 10.1109/COMST.2018.2878035 (see pp. 1, 3, 24, 25, 29, 31, 32, 36).

[4] Shakiba-Herfeh, Mahdi, Chorti, Arsenia, and Poor, H. Vince. "Physical Layer Security: Authentication, Integrity and Confidentiality". In: *ArXiv* abs/2001.07153 (2021) (see pp. 1, 4).

[5] Zou, Yulong, Wang, Xianbin, and Hanzo, L. "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends". In: *Proceedings of the IEEE* 104 (Sept. 2016). DOI: 10.1109/JPROC.2016.2558521 (see pp. 1, 4, 5).

[6] Liu, Yiliang, Chen, Hsiao-Hwa, and Wang, Liangmin. "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges". In: *IEEE Communications Surveys Tutorials* 19.1 (2017), pp. 347–376. DOI: 10.1109/COMST.2016.2598968 (see pp. 1, 4, 5).

[7] Wu, Yongpeng, Khisti, Ashish, Xiao, Chengshan, Caire, Giuseppe, Wong, Kai-Kit, and Gao, Xiqi. "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead". In: *IEEE Journal on Selected Areas in Communications* 36.4 (2018), pp. 679–695. DOI: 10.1109/JSAC.2018.2825560 (see p. 1).

[8] Alves, Hirley, Souza, Richard Demo, Debbah, Mérouane, and Bennis, Mehdi. "Performance of transmit antenna selection physical layer security schemes". In: *IEEE Signal Processing Letters* 19.6 (2012), pp. 372–375 (see p. 2).

[9] Yang, Nan, Suraweera, Himal A, Collings, Iain B, and Yuen, Chau. "Physical layer security of TAS/MRC with antenna correlation". In: *IEEE Transactions on Information Forensics and Security* 8.1 (2012), pp. 254–259 (see p. 2).

[10] Tran, Duc-Dung, Ha, Dac-Binh, Tran-Ha, Vu, and Hong, Een-Kee. "Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels". In: *IETE Journal of Research* 61.4 (2015), pp. 363–371 (see p. 2).

[11] Gao, Y., Hu, S., Tang, W., Li, Y., Sun, Y., Huang, D., Cheng, S., and Li, X. "Physical Layer Security in 5G Based Large Scale Social Networks: Opportunities and Challenges". In: *IEEE Access* 6 (2018), pp. 26350–26357 (see p. 2).

[12] Mezzavilla, Marco, Polese, Michele, Zanella, Andrea, Dhananjay, Aditya, Rangan, Sundeep, Kessler, Coitt, Rappaport, Theodore S., and Zorzi, Michele. "Public Safety Communications above 6 GHz: Challenges and Opportunities". In: *IEEE Access* 6 (2018), pp. 316–329. DOI: 10.1109/ACCESS.2017.2762471 (see p. 2).

[13] Al-Fuqaha, Ala, Guizani, Mohsen, Mohammadi, Mehdi, Aledhari, Mohammed, and Ayyash, Moussa. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications". In: *IEEE Communications Surveys Tutorials* 17.4 (2015), pp. 2347–2376. DOI: 10.1109/COMST.2015.2444095 (see p. 2).

[14] *Ericsson Mobility Report, June 2021, Available online:* https://www.ericsson.com/4a03c2/assets/local/reports-papers/mobility-report/documents/2021/june-2021-ericsson-mobility-report.pdf. Accessed: 2021-21-11 (see p. 2).

[15] Melki, Reem, Noura, Hassan N., Mansour, Mohammad M., and Chehab, Ali. "A survey on OFDM physical layer security". In: *Physical Communication* 32 (2019), pp. 1 –30. ISSN: 1874-4907. DOI: https://doi.org/10.1016/j.phycom.2018.10.008. http://www.sciencedirect.com/science/article/pii/S1874490718302817 (see pp. 3, 4, 29, 33, 42).

[16] Lin, Jie, Yu, Wei, Zhang, Nan, Yang, Xinyu, Zhang, Hanlin, and Zhao, Wei. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications". In: *IEEE Internet of Things Journal* 4.5 (2017), pp. 1125–1142. DOI: 10.1109/JIOT.2017.2683200 (see p. 3).

[17] Yadav, Poonam, Kumar, Sandeep, and Kumar, Rajesh. "A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges". In: *Transactions on Emerging Telecommunications Technologies* 32.9 (2021), e4270. DOI: https://doi.org/10.1002/ett.4270. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ett.4270. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4270 (see pp. 3, 41, 42).

[18] Zhang, Junqing, Rajendran, Sekhar, Sun, Zhi, Woods, Roger, and Hanzo, Lajos. "Physical Layer Security for the Internet of Things: Authentication and Key Generation". In: *IEEE Wireless Communications* 26.5 (2019), pp. 92–98. DOI: 10.1109/MWC.2019.1800455 (see pp. 3, 4).

[19] Kurose, James F. and Ross, Keith W. *Computer Networking: A Top-Down Approach*. 7th ed. Boston, MA: Pearson, 2016. ISBN: 978-0-13-359414-0 (see p. 4).

[20] Chorti, Arsenia, Perlaza, Samir M., Han, Zhu, and Poor, H. Vincent. "Physical layer security in wireless networks with passive and active eavesdroppers". In: *2012 IEEE Global Communications Conference (GLOBECOM)*. 2012, pp. 4868–4873. DOI: 10.1109/GLOCOM.2012.6503890 (see p. 5).

[21] Shannon, C. E. "Communication Theory of Secrecy Systems*". In: *Bell System Technical Journal* 28.4 (1949), pp. 656–715. DOI: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/j.1538-7305.1949.tb00928.x. https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1949.tb00928.x (see p. 13).

[22] Wyner, A. D. "The wire-tap channel". In: *The Bell System Technical Journal* 54.8 (1975), pp. 1355–1387 (see p. 14).

[23] Liang, Yingbin, Kramer, Gerhard, Poor, H. Vincent, and Shamai, Shlomo. "Compound wiretap channels". English (US). In: *Eurasip Journal on Wireless Communications and Networking* 2009 (2009). ISSN: 1687-1472. DOI: 10.1155/2009/142374 (see p. 16).

[24] Leung-Yan-Cheong, S. "On a special class of wiretap channels (Corresp.)" In: *IEEE Transactions on Information Theory* 23.5 (1977), pp. 625–627. DOI: 10.1109/TIT.1977.1055763 (see p. 19).

[25] Leung-Yan-Cheong, S. and Hellman, M. "The Gaussian wire-tap channel". In: *IEEE Transactions on Information Theory* 24.4 (1978), pp. 451–456. DOI: 10.1109/TIT.1978.1055917 (see p. 19).

[26] Khisti, Ashish and Wornell, Gregory W. "Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel". In: *IEEE Transactions on Information Theory* 56.11 (2010), pp. 5515–5532. DOI: 10.1109/TIT.2010.2068852 (see pp. 20, 34).

[27] Oggier, Frédérique and Hassibi, Babak. "The Secrecy Capacity of the MIMO Wiretap Channel". In: *IEEE Transactions on Information Theory* 57.8 (2011), pp. 4961–4972. DOI: 10.1109/TIT.2011.2158487 (see pp. 20, 34).

[28] Liu, Tie and Shamai, Shlomo. "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel". In: *IEEE Transactions on Information Theory* 55.6 (2009), pp. 2547–2553. DOI: 10.1109/TIT.2009.2018322 (see p. 20).

[29] Gopala, Praveen Kumar, Lai, Lifeng, and El Gamal, Hesham. "On the Secrecy Capacity of Fading Channels". In: *IEEE Transactions on Information Theory* 54.10 (2008), pp. 4687–4698. DOI: 10.1109/TIT.2008.928990 (see pp. 22, 31).

[30] Thangaraj, Andrew, Dihidar, Souvik, Calderbank, A. R., McLaughlin, Steven W., and Merolla, Jean-Marc. "Applications of LDPC Codes to the Wiretap Channel". In: *IEEE Transactions on Information Theory* 53.8 (2007), pp. 2933–2945. DOI: 10.1109/TIT.2007.901143 (see pp. 23, 24).

[31] Mahdavifar, Hessam and Vardy, Alexander. "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes". In: *IEEE Transactions on Information Theory* 57.10 (2011), pp. 6428–6443. DOI: 10.1109/TIT.2011.2162275 (see p. 24).

[32] Ling, Cong, Luzzi, Laura, Belfiore, Jean-Claude, and Stehlé, Damien. "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel". In: *IEEE Transactions on Information Theory* 60.10 (2014), pp. 6399–6416. DOI: 10.1109/TIT.2014.2343226 (see p. 24).

[33] Chorti, Arsenia, Hollanti, Camilla, Belfiore, Jean-Claude, and Poor, H. Vincent. *Physical Layer Security: A Paradigm Shift in Data Confidentiality*. Sept. 2015 (see p. 24).

[34] Güvenkaya, Ertuğrul, Hamamreh, Jehad M., and Arslan, Hüseyin. "On physical-layer concepts and metrics in secure signal transmission". In: *Physical Communication* 25 (2017), pp. 14–25. ISSN: 1874-4907. DOI: https://doi.org/10.1016/j.phycom.2017.08.011. https://www.sciencedirect.com/science/article/pii/S1874490717300903 (see pp. 24–26).

[35] Bloch, Matthieu, Barros, JoÃo, Rodrigues, Miguel R. D., and McLaughlin, Steven W. "Wireless Information-Theoretic Security". In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2515–2534. DOI: 10.1109/TIT.2008.921908 (see pp. 24, 31).

[36] Morrison, Kyle and Goeckel, Dennis. "Secrecy Rate Pair Constraints for Secure Throughput". In: *2014 IEEE Military Communications Conference*. 2014, pp. 479–484. DOI: 10.1109/MILCOM.2014.87 (see p. 25).

[37] Gungor, Onur, Tan, Jian, Koksal, Can Emre, El-Gamal, Hesham, and Shroff, Ness B. "Secrecy Outage Capacity of Fading Channels". In: *IEEE Transactions on Information Theory* 59.9 (2013), pp. 5379–5397. DOI: 10.1109/TIT.2013.2265691 (see pp. 25, 32).

[38] Klinc, Demijan, Ha, Jeongseok, McLaughlin, Steven W., Barros, João, and Kwak, Byung-Jae. "LDPC codes for the Gaussian wiretap channel". In: *2009 IEEE Information Theory Workshop*. 2009, pp. 95–99. DOI: 10.1109/ITW.2009.5351456 (see p. 25).

[39] Klinc, Demijan, Ha, Jeongseok, McLaughlin, Steven W., Barros, Joao, and Kwak, Byung-Jae. "LDPC for Physical Layer Security". In: *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*. 2009, pp. 1–6. DOI: 10.1109/GLOCOM.2009.5426065 (see p. 25).

[40] Hamamreh, Jehad M., Yusuf, Marwan, Baykas, Tuncer, and Arslan, Huseyin. "Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation". In: *2016 IEEE Wireless Communications and Networking Conference*. 2016, pp. 1–7. DOI: 10.1109/WCNC.2016.7564987 (see p. 26).

[41] Chen, X., Ng, D. W. K., Gerstacker, W. H., and Chen, H. "A Survey on Multiple-Antenna Techniques for Physical Layer Security". In: *IEEE Communications Surveys Tutorials* 19.2 (2017), pp. 1027–1053 (see p. 29).

[42] Liang, Yingbin, Poor, H. Vincent, and Shamai, Shlomo. "Secure Communication Over Fading Channels". In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2470–2492. DOI: 10.1109/TIT.2008.921678 (see pp. 31, 32).

[43] Rezki, Zouheir, Khisti, Ashish, and Alouini, Mohamed-Slim. "On the Secrecy Capacity of the Wiretap Channel With Imperfect Main Channel Estimation". In: *IEEE Transactions on Communications* 62.10 (2014), pp. 3652–3664. DOI: 10.1109/TCOMM.2014.2356482 (see pp. 32, 43, 53).

[44] Jeon, Hyoungsuk, Kim, Namshik, Choi, Jinho, Lee, Hyuckjae, and Ha, Jeongseok. "Bounds on Secrecy Capacity Over Correlated Ergodic Fading Channels at High SNR". In: *IEEE Transactions on Information Theory* 57.4 (2011), pp. 1975–1983. DOI: 10.1109/TIT.2011.2112190 (see p. 32).

[45] Li, Ming, Kundu, Sandipan, Pados, Dimitris A., and Batalama, Stella N. "Waveform Design for Secure SISO Transmissions and Multicasting". In: *IEEE Journal on Selected Areas in Communications* 31.9 (2013), pp. 1864–1874. DOI: 10.1109/JSAC.2013.130918 (see p. 32).

[46] Hamamreh, Jehad M. and Arslan, Huseyin. "Secure Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and Beyond". In: *IEEE Communications Letters* 21.5 (2017), pp. 1191–1194. DOI: 10.1109/LCOMM.2017.2651801 (see p. 32).

[47] Hamamreh, Jehad M. and Arslan, Huseyin. "Time-frequency characteristics and PAPR reduction of OTDM waveform for 5G and beyond". In: *2017 10th International Conference on Electrical and Electronics Engineering (ELECO)*. 2017, pp. 681–685 (see p. 32).

[48] Du, Qinghe, Sun, Li, Ren, Pinyi, and Wang, Yichen. "Statistical security model and power adaptation over wireless fading channels". In: *2015 International Conference on Wireless Communications Signal Processing (WCSP)*. 2015, pp. 1–6. DOI: 10.1109/WCSP.2015.7341246 (see p. 32).

[49] Furqan, Haji M., Hamamreh, Jehad M., and Arslan, Huseyin. "Enhancing physical layer security of OFDM systems using channel shortening". In: *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2017, pp. 1–5. DOI: 10.1109/PIMRC.2017.8292335 (see p. 32).

[50] Lei, Weijia and Yao, Li. "Performance Analysis of Time Reversal Communication Systems". In: *IEEE Communications Letters* 23.4 (2019), pp. 680–683. DOI: 10.1109/LCOMM.2019.2901484 (see p. 32).

[51] Lei, Weijia, Yang, Miaomiao, Yao, Li, and Lei, Hongjiang. "Physical Layer Security Performance Analysis of the Time Reversal Transmission System". In: *IET Communications* 14 (Nov. 2019). DOI: 10.1049/iet-com.2019.0872 (see p. 32).

[52] Oestges, Claude, Kim, A.D., Papanicolaou, George, and Paulraj, A.J. "Characterization of space-time focusing in time-reversed random fields". In: *Antennas and Propagation, IEEE Transactions on* 53 (Feb. 2005), pp. 283 –293. DOI: 10.1109/TAP.2004.836399 (see p. 32).

[53] Dubois, Thierry, Crussière, Matthieu, and Hélard, Maryline. "On the use of Time Reversal for digital communications with non-impulsive waveforms". In: *2010 4th International Conference on Signal Processing and Communication Systems*. 2010, pp. 1–6. DOI: 10.1109/ICSPCS.2010.5709739 (see p. 32).

[54] Nguyen, Trung-Hien, Monfared, Shaghayegh, Determe, Jean-François, Louveaux, Jérôme, De Doncker, Philippe, and Horlin, François. "Performance Analysis of Frequency Domain Precoding Time-Reversal MISO OFDM Systems". In: *IEEE Communications Letters* 24.1 (2020), pp. 48–51. DOI: 10.1109/LCOMM.2019.2949556 (see pp. 32, 51).

[55] Nguyen, Trung-Hien, Louveaux, Jérôme, De Doncker, Philippe, and Horlin, François. "Performance Analysis of Matched-Filter Precoded MISO-OFDM Systems in the Presence of Imperfect CSI". In: *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. 2020, pp. 1–5. DOI: 10.1109/VTC2020-Spring48590.2020.9128971 (see p. 32).

[57] Saltzberg, B. "Performance of an Efficient Parallel Data Transmission System". In: *IEEE Transactions on Communication Technology* 15.6 (1967), pp. 805–811. DOI: 10.1109/TCOM.1967.1089674 (see p. 33).

[58] Chang, Robert W. "Synthesis of band-limited orthogonal signals for multichannel data transmission". In: *The Bell System Technical Journal* 45.10 (1966), pp. 1775–1796. DOI: 10.1002/j.1538-7305.1966.tb02435.x (see p. 33).

[59] Bingham, J.A.C. "Multicarrier modulation for data transmission: an idea whose time has come". In: *IEEE Communications Magazine* 28.5 (1990), pp. 5–14. DOI: 10.1109/35.54342 (see p. 33).

[60] Schwartz, Mischa. *Mobile Wireless Communications*. Cambridge University Press, 2004. DOI: 10.1017/CBO9780511811333 (see p. 33).

[61] Prasad, Ramjee. 2004 (see p. 33).

[62] Liu, Ruoheng and Trappe, W. *Securing Wireless Communications at the Physical Layer*. Jan. 2009. ISBN: 978-1-4419-1384-5. DOI: 10.1007/978-1-4419-1385-2 (see p. 33).

[63] Renna, Francesco, Laurenti, Nicola, and Poor, H. Vincent. "Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels". In: *IEEE Transactions on Information Forensics and Security* 7.4 (2012), pp. 1354–1367. DOI: 10.1109/TIFS.2012.2195491 (see p. 33).

[64] Laurenti, N., Tomasin, S., and Renna, F. "Resource allocation for secret transmissions on parallel Rayleigh channels". In: *2014 IEEE International Conference on Communications (ICC)*. 2014, pp. 2209–2214. DOI: 10.1109/ICC.2014.6883651 (see p. 33).

[65] Hamamreh, Jehad M., Basar, Ertugrul, and Arslan, Huseyin. "OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services". In: *IEEE Access* 5 (2017), pp. 25863–25875. DOI: 10.1109/ACCESS.2017.2768558 (see p. 33).

[66] Lee, Yonggu, Jo, Hanseong, Ko, Youngwook, and Choi, Jinho. "Secure Index and Data Symbol Modulation for OFDM-IM". In: *IEEE Access* 5 (2017), pp. 24959–24974. DOI: 10.1109/ACCESS.2017.2768540 (see p. 33).

[67] Yusuf, Marwan and Arslan, Huseyin. "Enhancing physical-layer security in wireless communications using signal space diversity". In: *MILCOM 2016 - 2016 IEEE Military Communications Conference*. 2016, pp. 1190–1194. DOI: 10.1109/MILCOM.2016.7795492 (see p. 33).

[68] Naito, Katsuhiro, Sakakibara, Hiroki, Mukai, Yosuke, Mori, Kazuo, and Kobayashi, Hideo. "Channel state based secure wireless communication". In: *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2016, pp. 828–834. DOI: 10.1109/INFCOMW.2016.7562191 (see p. 34).

[69] Nguyen, Trung-Hien, Determe, Jean-François, Monfared, Shaghayegh, Louveaux, Jérôme, De Doncker, Philippe, and Horlin, François. "Focusing gain analysis of time-reversal precoding in MISO OFDM communication systems". In: *Physical Communication* 43 (2020), p. 101220. ISSN: 1874-4907. DOI: https://doi.org/10.1016/j.phycom.2020.101220. https://www.sciencedirect.com/science/article/pii/S1874490720302974 (see pp. 34, 51).

[70] Khisti, Ashish and Wornell, Gregory W. "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel". In: *IEEE Transactions on Information Theory* 56.7 (2010), pp. 3088–3104. DOI: 10.1109/TIT.2010.2048445 (see pp. 34, 39).

[71] Reboredo, Hugo, Xavier, João, and Rodrigues, Miguel R. D. "Filter Design With Secrecy Constraints: The MIMO Gaussian Wiretap Channel". In: *IEEE Transactions on Signal Processing* 61.15 (2013), pp. 3799–3814. DOI: 10.1109/TSP.2013.2262275 (see p. 35).

[72] Geraci, Giovanni, Egan, Malcolm, Yuan, Jinhong, Razi, Adeel, and Collings, Iain B. "Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding". In: *IEEE Transactions on Communications* 60.11 (2012), pp. 3472–3482. DOI: 10.1109/TCOMM.2012.072612.110686 (see p. 35).

[73] Shafiee, Shabnam and Ulukus, Sennur. "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints". In: *2007 IEEE International Symposium on Information Theory*. 2007, pp. 2466–2470. DOI: 10.1109/ISIT.2007.4557589 (see p. 35).

[74] Li, Zang, Trappe, Wade, and Yates, Roy. "Secret Communication via Multi-antenna Transmission". In: *2007 41st Annual Conference on Information Sciences and Systems*. 2007, pp. 905–910. DOI: 10.1109/CISS.2007.4298439 (see p. 35).

[75] Ding, Yuan and Fusco, Vincent. "Directional modulation transmitter synthesis using particle swarm optimization". In: *2013 Loughborough Antennas Propagation Conference (LAPC)*. 2013, pp. 500–503. DOI: 10.1109/LAPC.2013.6711950 (see p. 35).

[76] Daly, M. P. and Bernhard, J. T. "Directional Modulation Technique for Phased Arrays". In: *IEEE Transactions on Antennas and Propagation* 57.9 (2009), pp. 2633–2640 (see p. 35).

[77] Babakhani, A., Rutledge, D. B., and Hajimiri, A. "Transmitter Architectures Based on Near-Field Direct Antenna Modulation". In: *IEEE Journal of Solid-State Circuits* 43.12 (2008), pp. 2674–2692 (see p. 35).

[78] Babakhani, A., Rutledge, D. B., and Hajimiri, A. "A Near-Field Modulation Technique Using Antenna Reflector Switching". In: *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*. 2008, pp. 188–605 (see p. 35).

[79] Valliappan, N., Lozano, A., and Heath, R. W. "Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication". In: *IEEE Transactions on Communications* 61.8 (2013), pp. 3231–3245 (see p. 35).

[80] Eltayeb, Mohammed E., Choi, Junil, Al-Naffouri, Tareq Y., and Heath, Robert W. "On the Security of Millimeter Wave Vehicular Communication Systems Using Random Antenna Subsets". In: *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. 2016, pp. 1–5. DOI: 10.1109/VTCFall.2016.7881128 (see p. 35).

[81] Bereyhi, Ali, Asaad, Saba, Muller, Ralf R., Schaefer, Rafael F., and Rabiei, Amir M. "On Robustness of Massive MIMO Systems against Passive Eavesdropping under Antenna Selection". In: *2018 IEEE Global Communications Conference (GLOBECOM)*. 2018, pp. 1–7. DOI: 10.1109/GLOCOM.2018.8647880 (see p. 35).

[82] Ouyang, Chongjun, Ou, Zeliang, Zhang, Lu, and Yang, Hongwen. "Optimal Transmit Antenna Selection Algorithm in Massive MIMOME Channels". In: *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. 2019, pp. 1–6. DOI: 10.1109/WCNC.2019.8886342 (see p. 35).

[83] Shang, Peng, Zhu, Guangxi, Tan, Li, Su, Gang, and Li, Tan. "Transmit Antenna Selection for the Distributed MIMO Systems". In: *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*. Vol. 2. 2009, pp. 449–453. DOI: 10.1109/NSWCTC.2009.79 (see p. 35).

[84] Negi, R. and Goel, S. "Secret communication using artificial noise". In: *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.* Vol. 3. 2005, pp. 1906–1910 (see p. 36).

[85] Goel, S. and Negi, R. "Secret communication in presence of colluding eavesdroppers". In: *MILCOM 2005 - 2005 IEEE Military Communications Conference*. 2005, 1501–1506 Vol. 3 (see p. 36).

[86] Goel, S. and Negi, R. "Guaranteeing Secrecy using Artificial Noise". In: *IEEE Transactions on Wireless Communications* 7.6 (2008), pp. 2180–2189 (see pp. 36, 38, 39).

[87] Hamamreh, Jehad M. and Arslan, Huseyin. "Joint PHY/MAC Layer Security Design Using ARQ With MRC and Null-Space Independent PAPR-Aware Artificial Noise in SISO Systems". In: *IEEE Transactions on Wireless Communications* 17.9 (2018), pp. 6190–6204. DOI: 10.1109/TWC.2018.2855163 (see p. 36).

[88] Qin, Haohao, Sun, Yin, Chang, Tsung-Hui, Chen, Xiang, Chi, Chong-Yung, Zhao, Ming, and Wang, Jing. "Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs". In: *IEEE Transactions on Wireless Communications* 12.6 (2013), pp. 2717–2729. DOI: 10.1109/TCOMM.2013.050713.120730 (see p. 37).

[89] Qin, Haohao, Chen, Xiang, Zhong, Xiaofeng, He, Fei, Zhao, Ming, and Wang, Jing. "Joint power allocation and artificial noise design for multiuser wiretap OFDM channels". In: *2013 IEEE International Conference on Communications (ICC)*. 2013, pp. 2193–2198. DOI: 10.1109/ICC.2013.6654853 (see p. 37).

[90] Liu, Wenfei, Li, Ming, Ti, Guangyu, Tian, Xiaowen, and Liu, Qian. "Transmit filter and artificial noise aided physical layer security for OFDM systems". In: *2016 8th International Conference on Wireless Communications Signal Processing (WCSP)*. 2016, pp. 1–5. DOI: 10.1109/WCSP.2016.7752562 (see p. 37).

[91] Yang, Fan, Zhang, Kai, Zhai, Yongzhi, Quan, Jinguo, and Dong, Yuhan. "Artificial Noise Design in Time Domain for Indoor SISO DCO-OFDM VLC Wiretap Systems". In: *Journal of Lightwave Technology* 39.20 (2021), pp. 6450–6458. DOI: 10.1109/JLT.2021.3104469 (see p. 37).

[92] Yusuf, Marwan and Arslan, Huseyin. "Controlled Inter-Carrier Interference for Physical Layer Security in OFDM Systems". In: *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. 2016, pp. 1–5. DOI: 10.1109/VTCFall.2016.7880940 (see p. 37).

[93] Hussain, Mukhtar, Du, Qinghe, Sun, Li, and Ren, Pinyi. "Security protection over wireless fading channels by exploiting frequency selectivity". In: *2016 8th International Conference on Wireless Communications Signal Processing (WCSP)*. 2016, pp. 1–5. DOI: 10.1109/WCSP.2016.7752566 (see p. 37).

[94] He, Biao, She, Yechao, and Lau, Vincent K. N. "Artificial Noise Injection for Securing Single-Antenna Systems". In: *IEEE Transactions on Vehicular Technology* 66.10 (2017), pp. 9577–9581. DOI: 10.1109/TVT.2017.2703159 (see p. 37).

[95] Xu, Qian, Ren, Pinyi, Du, Qinghe, and Sun, Li. "Security-aware waveform and artificial noise design for time-reversal-based transmission". In: *IEEE Transactions on Vehicular Technology* 67.6 (2018), pp. 5486–5490 (see p. 37).

[96] Li, Si, Li, Na, Tao, Xiaofeng, Liu, Zunning, Wang, Haowei, and Xu, Jin. "Artificial noise inserted secure communication in time-reversal systems". In: *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE. 2018, pp. 1–6 (see p. 37).

[97] Li, Si, Li, Na, Liu, Zunning, Wang, Haowei, Xu, Jin, and Tao, Xiaofeng. "Artificial noise aided path selection for secure TR communications". In: *2017 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE. 2017, pp. 1–6 (see p. 37).

[98] Lei, Weijia, Zhang, Weihan, Yang, Miaomiao, Lei, Hongjiang, and Xie, Xianzhong. "Optimization of pre-processing filter for time-reversal multi-user secure transmission systems based on artificial noise". In: *Digital Signal Processing* 109 (2021), p. 102933. ISSN: 1051-2004. DOI: https://doi.org/10.1016/j.dsp.2020.102933. https://www.sciencedirect.com/science/article/pii/S1051200420302785 (see p. 37).

[99] Güvenkaya, Ertuğrul and Arslan, Hüseyin. "Secure communication in frequency selective channels with fade-avoiding subchannel usage". In: *2014 IEEE International Conference on Communications Workshops (ICC)*. 2014, pp. 813–818. DOI: 10.1109/ICCW.2014.6881300 (see p. 38).

[100] Akitaya, Tomoki, Asano, Shunta, and Saba, Takahiko. "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems". In: *2014 IEEE International Conference on Communications Workshops (ICC)*. 2014, pp. 807–812. DOI: 10.1109/ICCW.2014.6881299 (see p. 38).

[101] Zhang, J., Marshall, A., Woods, R., and Duong, T. Q. "Design of an OFDM Physical Layer Encryption Scheme". In: *IEEE Transactions on Vehicular Technology* 66.3 (2017), pp. 2114–2127 (see p. 38).

[102] Umebayashi, K., Nakabayashi, F., and Suzuki, Y. "A study on secure pilot signal design for OFDM systems". In: *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014 Asia-Pacific*. 2014, pp. 1–5 (see p. 38).

[103] Liu, Shuiyin, Hong, Yi, and Viterbo, Emanuele. "Artificial Noise Revisited". In: *IEEE Transactions on Information Theory* 61.7 (2015), pp. 3901–3911. DOI: 10.1109/TIT.2015.2437882 (see p. 39).

[104] Anand, Narendra, Lee, Sung-Ju, and Knightly, Edward W. "STROBE: Actively securing wireless communications using Zero-Forcing Beamforming". In: *2012 Proceedings IEEE INFOCOM*. 2012, pp. 720–728. DOI: 10.1109/INFCOM.2012.6195817 (see p. 39).

[105] Wiesel, Ami, Eldar, Yonina C., and Shamai, Shlomo. "Zero-Forcing Precoding and Generalized Inverses". In: *IEEE Transactions on Signal Processing* 56.9 (2008), pp. 4409–4418. DOI: 10.1109/TSP.2008.924638 (see p. 39).

[106] El Shafie, Ahmed, Ding, Zhiguo, and Al-Dhahir, Naofal. "Spatio-Temporal Artificial Noise Design for Secure MISOSE-OFDM Systems". In: *2016 IEEE Global Communications Conference (GLOBECOM)*. 2016, pp. 1–6. DOI: 10.1109/GLOCOM.2016.7842286 (see p. 39).

[107] Shafie, Ahmed El, Ding, Zhiguo, and Al-Dhahir, Naofal. "Hybrid Spatio-Temporal Artificial Noise Design for Secure MIMOME-OFDM Systems". In: *IEEE Transactions on Vehicular Technology* 66.5 (2017), pp. 3871–3886. DOI: 10.1109/TVT.2016.2600255 (see p. 39).

[108] Li, Qiaolong, Song, Huawei, and Huang, Kaizhi. "Achieving Secure Transmission with Equivalent Multiplicative Noise in MISO Wiretap Channels". In: *IEEE Communications Letters* 17.5 (2013), pp. 892–895. DOI: 10.1109/LCOMM.2013.040213.122870 (see p. 39).

[109] Wang, Hui-Ming, Zheng, Tongxing, and Mu, Pengcheng. "Secure MISO wiretap channels with multi-antenna passive eavesdropper via artificial fast fading". In: *2014 IEEE International Conference on Communications (ICC)*. 2014, pp. 5396–5401. DOI: 10.1109/ICC.2014.6884179 (see p. 39).

[110] Wang, Hui-Ming, Zheng, Tongxing, and Xia, Xiang-Gen. "Secure MISO Wiretap Channels With Multiantenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading". In: *IEEE Transactions on Wireless Communications* 14.1 (2015), pp. 94–106. DOI: 10.1109/TWC.2014.2332164 (see p. 39).

[111] Mukherjee, A. and Swindlehurst, A. L. "Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI". In: *IEEE Transactions on Signal Processing* 59.1 (2011), pp. 351–361 (see pp. 39, 53).

[112] Liu, Ta-Yuan, Lin, Pin-Hsun, Lin, Shih-Chun, Hong, Y.-W. Peter, and Jorswieck, Eduard Axel. "To avoid or not to avoid CSI leakage in physical layer secret communication systems". In: *IEEE Communications Magazine* 53.12 (2015), pp. 19–25. DOI: 10.1109/MCOM.2015.7355561 (see pp. 41, 42).

[113] Shi, Yan, Badi, Mahmoud, Rajan, Dinesh, and Camp, Joseph. "Channel Reciprocity Analysis and Feedback Mechanism Design for Mobile Beamforming Systems". In: *IEEE Transactions on Vehicular Technology* 70.6 (2021), pp. 6029–6043. DOI: 10.1109/TVT.2021.3079837 (see p. 42).

[114] Love, David J., Heath, Robert W., N. Lau, Vincent K., Gesbert, David, Rao, Bhaskar D., and Andrews, Matthew. "An overview of limited feedback in wireless communication systems". In: *IEEE Journal on Selected Areas in Communications* 26.8 (2008), pp. 1341–1365. DOI: 10.1109/JSAC.2008.081002 (see p. 42).

[115] Xia, Pengfei and Giannakis, G.B. "Design and analysis of transmit-beamforming based on limited-rate feedback". In: *IEEE Transactions on Signal Processing* 54.5 (2006), pp. 1853–1863. DOI: 10.1109/TSP.2006.871967 (see p. 42).

[116] Marzetta, T.L. and Hochwald, B.M. "Fast transfer of channel state information in wireless systems". In: *IEEE Transactions on Signal Processing* 54.4 (2006), pp. 1268–1278. DOI: 10.1109/TSP.2006.870543 (see p. 42).

[117] Kobayashi, Mari, Jindal, Nihar, and Caire, Giuseppe. "Training and Feedback Optimization for Multiuser MIMO Downlink". In: *IEEE Transactions on Communications* 59.8 (2011), pp. 2228–2240. DOI: 10.1109/TCOMM.2011.051711.090752 (see p. 42).

[118] Salim, Umer and Slock, Dirk T. M. "How Much Feedback Is Required for TDD Multi-Antenna Broadcast Channels with User Selection?" In: *EURASIP Journal on Advances in Signal Processing* 2010 (2010), pp. 1–14 (see p. 42).

[119] Kim, Tùng T. and Poor, H. Vincent. "Secure Communications With Insecure Feedback: Breaking the High-SNR Ceiling". In: *IEEE Transactions on Information Theory* 56.8 (2010), pp. 3700–3711. DOI: 10.1109/TIT.2010.2050798 (see p. 42).

[120] Hyadi, Amal, Rezki, Zouheir, and Alouini, Mohamed-Slim. "An Overview of Physical Layer Security in Wireless Communication Systems With CSIT Uncertainty". In: *IEEE Access* 4 (2016), pp. 6121–6132. DOI: 10.1109/ACCESS.2016.2612585 (see p. 42).

[121] Song, B. and Haardt, M. "Effects of Imperfect Channel State Information on Achievable Rates of Precoded Multi-User MIMO Broadcast Channels with Limited Feedback". In: *2009 IEEE International Conference on Communications*. 2009, pp. 1–5. DOI: 10.1109/ICC.2009.5198965 (see pp. 42, 43).

[122] Jorswieck, Eduard, Tomasin, Stefano, and Sezgin, Aydin. "Broadcasting Into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing". In: *Proceedings of the IEEE* 103.10 (2015), pp. 1702–1724. DOI: 10.1109/JPROC.2015.2469602 (see p. 42).

[123] Cepeda, R., Fitton, M., and Nix, A. "The performance of robust adaptive modulation over wireless channels with non reciprocal interference". In: *Vehicular Technology Conference. IEEE 55th Vehicular Technology Conference. VTC Spring 2002 (Cat. No.02CH37367)*. Vol. 3. 2002, 1497–1501 vol.3. DOI: 10.1109/VTC.2002.1002866 (see p. 42).

[124] Björnson, Emil, Hoydis, Jakob, Kountouris, Marios, and Debbah, Mérouane. "Massive MIMO Systems With Non-Ideal Hardware: Energy Efficiency, Estimation, and Capacity Limits". In: *IEEE Transactions on Information Theory* 60.11 (2014), pp. 7112–7139. DOI: 10.1109/TIT.2014.2354403 (see pp. 43, 44).

[125] Nguyen, Ba, Thang, Nguyen, Tran, Xuan Nam, and Dũng, Lê. "Impacts of Imperfect Channel State Information, Transceiver Hardware, and Self-Interference Cancellation on the Performance of Full-Duplex MIMO Relay System". In: *Sensors* 20 (Mar. 2020), p. 1671. DOI: 10.3390/s20061671 (see pp. 43, 44).

[126] Jiang, Xiwen and Kaltenberger, Florian. "Channel Reciprocity Calibration in TDD Hybrid Beamforming Massive MIMO Systems". In: *IEEE Journal of Selected Topics in Signal Processing* 12.3 (2018), pp. 422–431. DOI: 10.1109/JSTSP.2018.2819118 (see p. 43).

[127] Lin, Chia-Hua, Tsai, Shang-Ho, and Lin, Yuan-Pei. "Secure Transmission Using MIMO Precoding". In: *IEEE Transactions on Information Forensics and Security* 9.5 (2014), pp. 801–813. DOI: 10.1109/TIFS.2014.2309211 (see p. 43).

[128] Li, Qiang and Ma, Wing-Kin. "Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming". In: *IEEE Transactions on Signal Processing* 59.8 (2011), pp. 3799–3812. DOI: 10.1109/TSP.2011.2146775 (see p. 43).

[129] Mu, Pengcheng, Li, Zongze, and Wang, Bo. "Secure On–Off Transmission in Slow Fading Wiretap Channel With Imperfect CSI". In: *IEEE Transactions on Vehicular Technology* 66.10 (2017), pp. 9582–9586. DOI: 10.1109/TVT.2017.2703861 (see p. 43).

[130] He, Biao and Zhou, Xiangyun. "Secure On-Off Transmission Design With Channel Estimation Errors". In: *IEEE Transactions on Information Forensics and Security* 8.12 (2013), pp. 1923–1936. DOI: 10.1109/TIFS.2013.2284754 (see pp. 43, 53).

[131] Liu, Xiaochen, Gao, Yuanyuan, Zang, Guozhen, and Sha, Nan. "Artificial-Noise-Aided Robust Beamforming for MISOME Wiretap Channels with Security QoS". In: *2019 IEEE 19th International Conference on Communication Technology (ICCT)*. 2019, pp. 795–799. DOI: 10.1109/ICCT46805.2019.8947004 (see p. 43).

[132] Liang, Ya-Lan, Wang, Yung-Shun, Chang, Tsung-Hui, Hong, Y.-W. Peter, and Chi, Chong-Yung. "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise". In: *2009 IEEE International Symposium on Information Theory*. 2009, pp. 2351–2355. DOI: 10.1109/ISIT.2009.5205966 (see p. 43).

[133] Lin, Shih-Chun, Chang, Tsung-Hui, Liang, Ya-Lan, Hong, Y.-W. Peter, and Chi, Chong-Yung. "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem". In: *IEEE Transactions on Wireless Communications* 10.3 (2011), pp. 901–915. DOI: 10.1109/TWC.2011.010411.100374 (see p. 43).

[134] Wang, Hui-Ming, Wang, Chao, and Ng, Derrick Wing Kwan. "Artificial Noise Assisted Secure Transmission Under Training and Feedback". In: *IEEE Transactions on Signal Processing* 63.23 (2015), pp. 6285–6298. DOI: 10.1109/TSP.2015.2465301 (see p. 43).

[135] Rezki, Zouheir, Khisti, Ashish, and Alouini, Mohamed-Slim. "Ergodic Secret Message Capacity of the Wiretap Channel with Finite-Rate Feedback". In: *IEEE Transactions on Wireless Communications* 13.6 (2014), pp. 3364–3379. DOI: 10.1109/TWC.2014.041014.131593 (see p. 43).

[136] Hu, Jianwei, Yang, Weiwei, Yang, Nan, Zhou, Xiangyun, and Cai, Yueming. "On–Off-Based Secure Transmission Design With Outdated Channel State Information". In: *IEEE Transactions on Vehicular Technology* 65.8 (2016), pp. 6075–6088. DOI: 10.1109/TVT.2015.2477427 (see p. 44).

[137] Ferdinand, Nuwan S., Costa, Daniel Benevides da, and Latva-aho, Matti. "Effects of Outdated CSI on the Secrecy Performance of MISO Wiretap Channels with Transmit Antenna Selection". In: *IEEE Communications Letters* 17.5 (2013), pp. 864–867. DOI: 10.1109/LCOMM.2013.040213.122696 (see p. 44).

[138] Yang, Yunchuan, Wang, Wenbo, Zhao, Hui, and Zhao, Long. "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation". In: *Journal of Communications and Networks* 14.4 (2012), pp. 374–384. DOI: 10.1109/JCN.2012.6292244 (see p. 44).

[139] Hu, Jianwei, Cai, Yueming, Yang, Nan, and Yang, Weiwei. "A New Secure Transmission Scheme With Outdated Antenna Selection". In: *IEEE Transactions on Information Forensics and Security* 10.11 (2015), pp. 2435–2446. DOI: 10.1109/TIFS.2015.2464703 (see p. 44).

[140] Huang, Yuzhen, Al-Qahtani, Fawaz S., Duong, Trung Q., and Wang, Jinlong. "Secure Transmission in MIMO Wiretap Channels Using General-Order Transmit Antenna Selection With Outdated CSI". In: *IEEE Transactions on Communications* 63.8 (2015), pp. 2959–2971. DOI: 10.1109/TCOMM.2015.2442248 (see p. 44).

[141] Kavaiya, Sagar, Patel, Dhaval K., Ding, Zhiguo, Guan, Yong Liang, and Sun, Sumei. "Physical Layer Security in Cognitive Vehicular Networks". In: *IEEE Transactions on Communications* 69.4 (2021), pp. 2557–2569. DOI: 10.1109/TCOMM.2020.3038904 (see p. 44).

[142] Odeyemi, Kehinde O., Owolawi, Pius A., and Olakanmi, Oladayo O. "On the performance of underlay cognitive radio system with random mobility under imperfect channel state information". In: *International Journal of Communication Systems* 33.15 (2020). e4561 IJCS-20-0280.R2, e4561. DOI: https://doi.org/10.1002/dac.4561. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/dac.4561. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4561 (see p. 44).

[143] Tran, Xuan Nam, Nguyen, Ba Cao, and Tran, Dinh Tan. "Outage probability of two-way full-duplex relay system with hardware impairments". In: *2019 3rd International Conference on Recent Advances in Signal Processing, Telecommunications Computing (SigTelCom)*. 2019, pp. 135–139. DOI: 10.1109/SIGTELCOM.2019.8696213 (see p. 44).

[144] Boulogeorgos, Alexandros-Apostolos, Karas, Dimitrios, and Karagiannidis, George. "How Much Does I/Q Imbalance Affect Secrecy Capacity?" In: *IEEE Communications Letters* 20 (Apr. 2016). DOI: 10.1109/LCOMM.2016.2558561 (see p. 44).

[145] Zhu, Jun, Schober, Robert, and Bhargava, Vijay K. "Physical layer security for massive MIMO systems impaired by phase noise". In: *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. 2016, pp. 1–5. DOI: 10.1109/SPAWC.2016.7536826 (see p. 44).

[146] Proakis, J.G. and Salehi, M. *Digital Communications, 5th edition*. McGraw-Hill Higher Education, 2008. https://books.google.fr/books?id=tOpKAQAACAAJ (see pp. 48–50).

[147] De Doncker, Philippe. *Communication channels, ELEC-H415*. URL: https://www.ulb.be/en/programme/elec-h415. Last visited on 2021/11/25. 2021-2022 (see p. 49).

[148] Ahmed, S., Noguchi, T., and Kawai, M. "Selection of Spreading Codes for Reduced PAPR in MC-CDMA Systems". In: *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*. 2007, pp. 1–5 (see p. 51).

[151] Tran, H., Tran, H., Kaddoum, G., Tran, D., and Ha, D. "Effective secrecy-SINR analysis of time reversal-employed systems over correlated multi-path channel". In: *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2015, pp. 527–532 (see p. 78).

[152] Zhu, Jun, Schober, Robert, and Bhargava, Vijay K. "Secure Transmission in Multicell Massive MIMO Systems". In: *IEEE Transactions on Wireless Communications* 13.9 (2014), pp. 4766–4781. DOI: 10.1109/TWC.2014.2337308 (see p. 78).