



HAL
open science

On the Resilience of Wireless Multiuser Networks to Passive and Active Eavesdroppers

Arsenia Chorti, Samir Perlaza, Zhu Han, Harold Vincent Poor

► **To cite this version:**

Arsenia Chorti, Samir Perlaza, Zhu Han, Harold Vincent Poor. On the Resilience of Wireless Multiuser Networks to Passive and Active Eavesdroppers. *IEEE Journal on Selected Areas in Communications*, 2013. hal-01686327

HAL Id: hal-01686327

<https://hal.science/hal-01686327v1>

Submitted on 17 Jan 2018

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.

On the Resilience of Wireless Multiuser Networks to Passive and Active Eavesdroppers

Arsenia Chorti^{†,*}, Samir M. Perlaza[†], Zhu Han[‡], H. Vincent Poor[†]

[†]Dep. EE, Equad 19 Olden Street, Princeton University, Princeton, New Jersey 08544, USA

^{*}ICS-FORTH N. Plastira 100, Vassilika Vouton, GR-700 13 Heraklion, Crete, Greece

[‡]Dep. ECE, N324, Engineering Building 1, University of Houston, Houston, TX 77004.

{achorti, perlaza, poor}@princeton.edu, zhan2@mail.uh.edu

Abstract—Physical layer security can provide alternative means for securing the exchange of confidential messages in wireless applications. In this paper, the resilience of wireless multiuser networks to *passive* (interception of the broadcast channel) and *active* (interception of the broadcast channel and false feedback) eavesdroppers is investigated. Stochastic characterizations of the secrecy capacity (SC) are obtained in scenarios involving a base station and several destinations. The expected values and variances of the SC along with the probabilities of secrecy outages are evaluated in the following cases: (i) in the presence of passive eavesdroppers without any side information; (ii) in the presence of passive eavesdroppers with side information about the number of eavesdroppers; and (iii) in the presence of a single active eavesdropper with side information about the behavior of the eavesdropper. This investigation demonstrates that substantial secrecy rates are attainable on average in the presence of passive eavesdroppers as long as minimal side information is available. On the other hand, it is further found that active eavesdroppers can potentially compromise such networks unless statistical inference is employed to restrict their ability to attack. Interestingly, in the high signal to noise ratio regime, multiuser networks become insensitive to the activeness or passiveness of the attack.

Index Terms—Secrecy capacity, secrecy rate, physical layer security, outage probability, multiuser diversity, multiple eavesdroppers, slow fading and side information.

I. INTRODUCTION

Security in the exchange of information has been primarily treated as an inherently applied subject, despite the theoretical formulation of *perfect secrecy* early on [1]. In actual networks, security commonly relies on cryptographic algorithms [2] implemented at upper layers of the protocol stack. Recently, a compelling complementary approach for enhancing the securing of wireless systems has risen from the area of information theory and has become a focal point of research in the wireless community. The breakthrough concept of physical layer security is to exploit the characteristics of the wireless medium such as fading or noise to ensure secrecy in wireless transmissions [3], [4], [5], [6].

Seminal earlier analyses that investigated security aspects of the wiretap channel [7] and the broadcast channel with confidential messages (BCC) [8] have established that a noisy

communication channel can offer opportunities for perfectly secure exchange of information. The performance measure of interest, the secrecy capacity (SC), was defined as the largest communication rate for which encoding schemes exist that simultaneously guarantee reliability in the exchange of information with a legitimate user and perfect secrecy with respect to an eavesdropper. It has been demonstrated that the SC is strictly positive when the wiretap channel is on average a degraded version of the main channel. Specifically in the case of Gaussian encoders, the SC can be expressed as the difference between the main and the eavesdropper's channel capacities, C_M and C_W respectively, [9],

$$C_s = [C_M - C_W]^+ = [\log(1 + \text{SNR}_M) - \log(1 + \text{SNR}_W)]^+ \quad (1)$$

where $[\cdot]^+ = \max(\cdot, 0)$, SNR_M and SNR_W denote the signal-to-noise-ratios (SNRs) of the main and eavesdropping channels, respectively¹.

Similar results were obtained for wireless fading channels [10], [11], [12] and multiple input multiple output (MIMO) systems [13], [14], [15], [16] to cite but a few. Furthermore, many investigations have considered systems with friendly or un-trusted relays [17], [18], [19] approaches relying on intentionally degrading the eavesdropper SNR using friendly interferers [20], [21], [22], etc. Finally, more recently, investigations have appeared for scenarios involving multiple legitimate users and a single eavesdropper [23], [24] or a single legitimate user and multiple eavesdroppers [25]. Some work from resource allocation perspective can be found in [26], [27], [28].

In this paper, we build on earlier works that provide single letter characterizations of the SC for the broadcast fading channel and investigate broadcast networks in the presence of multiple eavesdroppers. We assume that a central management unit (base station (BS)) decides on the allocation of network resources (bandwidth and power) in order to convey secret messages to one of K destinations. Evidently, in this setting, the SC depends on the relative SNR levels of the strongest user (in terms of SNR) and the strongest eavesdropper. The ordering of the respective SNRs involves the use of *order statistics* of the respective channel gains. We model the channel coefficients as realizations of a random process with

This work was supported in part by the IOF "APLOE" (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community and in part by the Qatar National Research Fund (QNRF) and U.S. National Science Foundation Grants CCF-1016671, CNS-0905556, CNS-1117560, CNS-0953377 and ECCS-1028782.

¹Logarithms hereafter are taken base 2.

an underlying Rayleigh probability density function (pdf)². Assuming that the wireless channel is memoryless and the multiplicative fading coefficients are stationary and ergodic over time, we are primarily concerned with the *stochastic characterization* of the SC as a function of the cell size K , the side information available and the fierceness of the attack.

In particular, to the best of our knowledge, the present paper presents the first systematic probabilistic characterization of the SC in the following cases:

- 1) *Purely antagonistic networks in the absence of any side information.* In this worst case scenario, all subscribed users in a network can in parallel act as eavesdroppers, intercepting the exchange of confidential messages intended for other users. Characterizing probabilistically the SC in the absence of any side information, we readily demonstrate that any opportunities for secure exchange of information vanish with an increase in the size of the network, i.e. with increasing K , the average SC tends to 0. Our findings indicate that in real networks, securing any single user against all other users or alternatively an *arbitrarily large* number of adversaries is not attainable in practical terms.
- 2) *Networks with distinct sets of legitimate users and eavesdroppers.* In actual commercial applications, intuitively, only a small number of adversaries may have an interest in compromising the security of the network. Based on this reasoning, we next consider the scenario in which the sets of legitimate users and eavesdroppers are distinct. Furthermore, we assume that *quantitative side information* is available regarding the cardinality of the set of eavesdroppers. Such minimal knowledge proves a decisive factor for secure network planning purposes; we demonstrate that upper-bounding the number of passive eavesdroppers and increasing the cell size leads to substantial opportunities for realizing perfectly secure transmissions.
- 3) *Networks in the presence of a single active eavesdropper.* In our model, an active eavesdropper possesses an optimal receiver, has global channel state information (CSI) and additionally exchanges signalling messages with the BS, appearing as a legitimate user. The goal of this adversary is not only to intercept the broadcast channel but also to interfere with the decision making process regarding the allocation of resources in order to increase the amount of secret information leaked. Our findings indicate that in order for the BS to counteract such malicious behavior, *qualitative side information* is required concerning *behavioral* aspects of the active eavesdropper tactics. Intuitively, a fiercer type of attack requires stronger defence mechanisms.

The paper is organized as follows: the problem formulation is outlined in Section II. The scenario of passive eavesdropping without side information is examined in Section III, while in Section IV results are presented when quantitative side information is available. In Section V, the case of active

²Our results can straightforwardly be extended to the general case of Nakagami- m distributions.

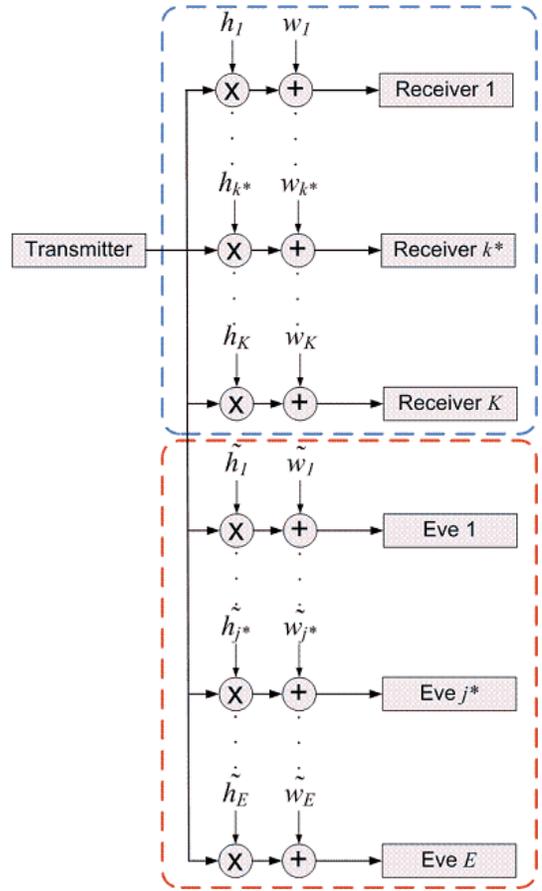


Fig. 1. Broadcast network in the presence of multiple eavesdroppers.

eavesdropping is investigated, which is formulated as a one-shot two player zero-sum game. In Section VI, the SC in the high SNR regime is stochastically characterized while in Section VII heuristic transmission strategies are compared. Finally, Section VIII includes the conclusions of this study.

II. PROBLEM FORMULATION

Consider the system set up illustrated in Fig. 1 corresponding to a typical downlink scenario in a multiuser network. A central management unit or BS communicates with a set $\mathcal{K} = \{1, 2, \dots, K\}$ of $K = |\mathcal{K}|$ destinations in the presence of a set $\mathcal{E} = \{1, 2, \dots, E\}$ of $E = |\mathcal{E}|$ eavesdroppers. Communication occurs in consecutive transmission frames. During each time frame, the BS transmits to destination $k^* \in \mathcal{K}$ a message $\mathbf{s} = (s(1), \dots, s(q)) \in \mathcal{S}^q$, whose elements are uniformly drawn from a set of source symbols \mathcal{S} .

In the present investigation, the destination k^* is determined on the sole criterion of keeping the eavesdroppers as ignorant as possible of the message transmitted by the source. Towards this end, the BS employs an encoding function $\varphi : \mathcal{S}^q \rightarrow \mathcal{X}^n$, with \mathcal{X} the set of transmitted symbols. Each codeword is a sequence of n -elements denoted by $\mathbf{x} = \varphi(\mathbf{s})$, $\mathbf{x} = (x(1), \dots, x(n))$, satisfying a frame-based average power

constraint,

$$\mathbb{E} [\mathbf{x}^2] = \frac{1}{n} \sum_{i=1}^n \mathbb{E} [x^2(i)] \leq p_{\max}. \quad (2)$$

For random encoding arguments to hold, we further assume that i) the channel realizations between the source and all destinations and eavesdroppers remain constant during a given frame, and ii) communication frames are long enough to allow the transmission of infinite length codewords, $n \rightarrow \infty$, invoking that the channel capacities can be asymptotically reached. In this framework and focusing on one transmission frame, the channel realization between the source and destination k is denoted by h_k , with $k \in \mathcal{K}$. Similarly, the channel realization between the source and the eavesdropper j is denoted by \tilde{h}_j , with $j \in \mathcal{E}$.

All channel realizations are assumed to be ergodic over time and independent and identically distributed (i.i.d.) from channel to channel drawn from a zero-mean unit variance complex Gaussian distribution. Thus, all channel gains $g_k = |h_k|^2$ and $\tilde{g}_j = |\tilde{h}_j|^2$ are random variables drawn from a chi-square probability distribution with 2 degrees of freedom, with underlying pdf

$$f(\lambda) = e^{-\lambda}, \quad (3)$$

and a corresponding cumulative distribution function (cdf)

$$F(\lambda) = 1 - e^{-\lambda}. \quad (4)$$

It is noteworthy that the results presented in the following sections can straightforwardly be generalized to the case of Nakagami- m channels by appropriately defining $f(\lambda)$ and $F(\lambda)$, respectively [29].

During a given communication frame, the outputs of optimal receivers at destination k , $\mathbf{y}_k = (y_k(1), \dots, y_k(n))$ and eavesdropper j , $\mathbf{z}_j = (z_j(1), \dots, z_j(n))$ are expressed, respectively, as follows:

$$\forall k \in \mathcal{K}, \quad \mathbf{y}_k = g_k \mathbf{x} + \mathbf{w}_k, \quad (5)$$

$$\forall j \in \mathcal{E}, \quad \mathbf{z}_j = \tilde{g}_j \mathbf{x} + \tilde{\mathbf{w}}_j. \quad (6)$$

$\mathbf{y}_k \in \mathcal{Y}^n$ and $\mathbf{z}_j \in \mathcal{Z}^n$, where \mathcal{Y} and \mathcal{Z} are observations at the destination and the eavesdropper. The terms $\mathbf{w}_k = (w_k(1), \dots, w_k(n))$ and $\tilde{\mathbf{w}}_j = (\tilde{w}_j(1), \dots, \tilde{w}_j(n))$ are n -dimensional vectors whose components are zero-mean unit-variance circularly symmetric complex Gaussian random variables.

At destination k , the decoding function $\phi_k : \mathcal{Y}^n \rightarrow \mathcal{S}^q$ is used to recover the source symbols from the observations. The error probability associated with the code (φ, ϕ) during a particular transmission interval at destination k is defined as

$$P_e^{(k)} = \Pr(\phi_k(\mathbf{y}_k) \neq \mathbf{s}). \quad (7)$$

The level of ignorance of eavesdropper j with respect to the transmitted message is measured by its equivocation rate $R_e^{(j)}$. That is, the rate of the entropy of the message \mathbf{S} conditioned on the received signal \mathbf{Z}_j and the channel realizations \mathbf{h} and $\tilde{\mathbf{h}}$,

$$R_e^{(j)} = \frac{1}{n} H(\mathbf{S} | \mathbf{Z}_j, \mathbf{h}, \tilde{\mathbf{h}}). \quad (8)$$

In the following, we focus on information theoretic perfect secrecy, implying that the equivocation rate is at least equal to the rate of the message R . Perfectly secret transmission at rate R is achieved at destination k^* if for any arbitrarily small $\epsilon > 0$, there exists a sequence of codes $(2^{nR}, n)$ such that for $n \rightarrow \infty$, the following hold [7], [8]:

$$P_e^{(k^*)} \leq \epsilon, \quad (9)$$

$$\forall j \in \mathcal{E}, \quad R_e^{(j)} = \frac{1}{n} H(\mathbf{S} | \mathbf{S}_j, \mathbf{h}, \tilde{\mathbf{h}}) \geq R - \epsilon. \quad (10)$$

During a given transmission frame, the secrecy capacity C_s is the maximum achievable rate R that satisfies both (9) and (10), i.e.,

$$\begin{aligned} C_s &= \max_{\mathbb{E}[\mathbf{x}^2] < p_{\max}} I(\mathbf{X}; \mathbf{Y}_{k^*} | \mathbf{h}, \tilde{\mathbf{h}}) - I(\mathbf{X}; \mathbf{Z}_{j^*} | \mathbf{h}, \tilde{\mathbf{h}}) \\ &= [\log(1 + g_{k^*} p_{\max}) - \log(1 + \tilde{g}_{j^*} p_{\max})]^+, \end{aligned} \quad (11)$$

where indices k^* and j^* denote the most capable (in terms of SNR) of the destinations and eavesdroppers, respectively. Solving the optimization problem (11) to p_{\max} is a consequence of the monotonicity of the SC as a function of the power in slow fading conditions. For fast fading channels, transmitting at constant power under an average power constraint is no longer optimal and power control should be adopted [30].

Finally, an underlying assumption of the present study is that potential eavesdropping terminals do not cooperate, i.e., we examine the scenario of non-colluding eavesdroppers. This is a plausible assumption in a purely individualistic network where an eavesdropper would hesitate to reveal its identity to probably ‘‘friendly’’ eavesdroppers in order not to jeopardize its own safety (being identified and ‘‘removed’’ from the network). The more pessimistic scenario of optimally cooperating eavesdroppers is to be investigated in future work.

III. STOCHASTIC CHARACTERIZATION OF THE SC IN ABSENCE OF SIDE INFORMATION

We commence our investigation by examining the case in which the BS has no side information regarding the existence of eavesdroppers. As a worst case approach, the network is treated as purely antagonistic; the BS assumes that all subscribed users act as passive eavesdroppers intercepting the broadcasting of confidential messages to other users. Aiming at evaluating lower bounds, in this scenario the set of destinations \mathcal{K} is extended to include *any* terminal that can act as an eavesdropper, i.e., $\mathcal{E} \subset \mathcal{K}$. We finally note that in this *blind* approach, we should in principle allow the number of eavesdroppers to grow unboundedly, i.e., $K \rightarrow \infty$. In this setting, *only* the strongest of K destinations has potentially a non-zero SC. The SC during a transmission frame strictly depends on the SNR difference between the destination with the highest SNR and the destination with the second highest SNR. For ease of notation, we denote the former with index k^* and the latter with index k^{**} , i.e.,

$$k^* = \arg \max_{k \in \mathcal{K}} g_k, \quad (12)$$

$$k^{**} = \arg \max_{k \in \mathcal{K} \setminus \{k^*\}} g_k. \quad (13)$$

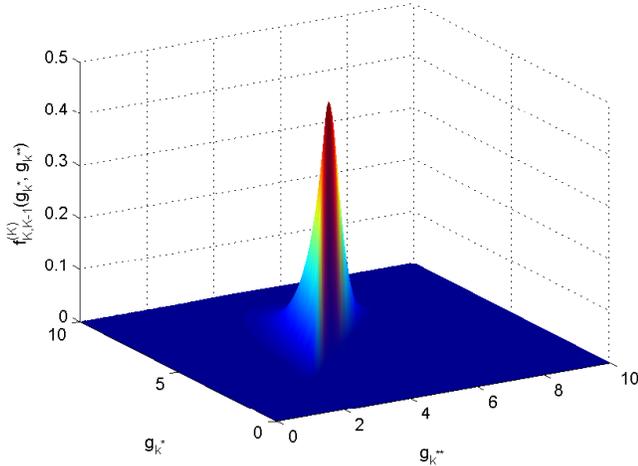


Fig. 2. Joint probability of the K -th and $(K-1)$ -th order statistics of the fading channel for $K = 100$.

Building on the assumption that the channel realizations g_{k^*} and $g_{k^{**}}$ are i.i.d. random variables, their pdfs $f_K^{(K)}(g_{k^*})$ and $f_{K-1}^{(K)}(g_{k^{**}})$, respectively, are the K -th and $(K-1)$ -th order statistics of a sample of K channel realizations:

$$f_K^{(K)}(\lambda) = KF(\lambda)^{K-1}f(\lambda), \quad (14)$$

$$f_{K-1}^{(K)}(\lambda) = K(K-1)F(\lambda)^{K-2}(1-F(\lambda))f(\lambda) \quad (15)$$

with cdfs $F_K^{(K)}(\lambda)$ and $F_{K-1}^{(K)}(\lambda)$, respectively. The concept of ordering the channel gains in physical layer security studies is a central point of our approach and its significance will be emphasized throughout the rest of this study.

The random variables g_{k^*} and $g_{k^{**}}$ are generated through a *common* ordering operation over the set of K channel realizations, which is clearly a nonlinear transformation. As a result, they are not independent [31]. Based on the general expression for the joint pdf of any two order statistics [31], the joint pdf $f_{K,K-1}^{(K)}(g_{k^*}, g_{k^{**}})$ of g_{k^*} and $g_{k^{**}}$ is derived as

$$f_{K,K-1}^{(K)}(g_{k^*}, g_{k^{**}}) = K(K-1)F(g_{k^{**}})^{K-2}f(g_{k^{**}}) \times f(g_{k^*})U(g_{k^*} - g_{k^{**}}), \quad (16)$$

where $U(\cdot)$ is the step function and is depicted in Fig. 2.

The SC is a random process that we will fully characterize in the following, generalizing the reasoning presented in [10] and [11], assuming that the fading channel is wide sense stationary³. We begin by deriving the pdf of the SC and then evaluate its expected value and variance.

Theorem 1 [Pdf of the SC without side information]: The pdf $f_{C_s}(C_s)$ of the SC C_s when the legitimate destination is chosen following (12) and all the other destinations are considered as passive eavesdroppers can be expressed as

$$f_{C_s}(C_s) = \ln(2)K(K-1)\beta(2^{C_s}, p, K)2^{C_s} \times \exp\left(-\frac{2^{C_s}-1}{p}\right)U(C_s), \quad (17)$$

³The assumption of a wide sense stationary fading channel can be removed if we let the underlying pdfs of the channel coefficients become time dependent functions.

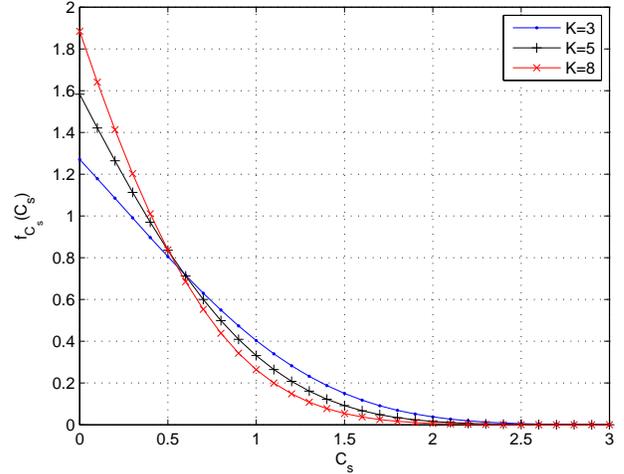


Fig. 3. Pdf of the SC in a set of K destinations without side information.

where

$$\beta(\lambda, p, K) = \int_0^\infty (p\mu + 1)[1 - \exp(-\mu)]^{K-2} \times \exp(-(1+\lambda)\mu) d\mu. \quad (18)$$

Proof: In order to derive the pdf of the SC $C_s = \left[\log\left(\frac{1+g_{k^*}p_{max}}{1+g_{k^{**}}p_{max}}\right)\right]^+$, we note that the pdf of the ratio $\xi = \frac{\lambda}{\mu}$ of two non-negative dependent random variables with joint pdf $f_{\Lambda M}(\lambda, \mu)$ can be expressed as [32]:

$$f_{\Xi}(\xi) = \int_0^\infty \mu f_{\Lambda M}(\mu\xi, \mu) d\mu. \quad (19)$$

Furthermore, the pdf of the output of a hard limiter $\xi = [\lambda]^+$ when the pdf of the input is $f_{\Lambda}(\lambda)$, is a discontinuous function at the origin and equals

$$f_{\Xi}(\xi) = f_{\Lambda}(\xi)U(\xi) + Pr(\lambda \leq 0)\delta(\xi). \quad (20)$$

From the previous discussion, the pdf of the SC is derived from the joint pdf of g_{k^*} and $g_{k^{**}}$ by performing the following sequence of operations: i) $\phi = 1 + g_{k^*}p$, $\psi = 1 + g_{k^{**}}p$, ii) $\xi = \frac{\phi}{\psi}$, iii) $\eta = \log(\xi)$, and iv) $C_s = [\eta]^+$. \square

In Fig. 3 the pdf of the SC is depicted for $K = 3, 5$ and 8 destinations. As the number of destinations increases, the pdf mass concentrates on smaller values of the SC, implying that with increasing cell size the expected value of the SC decreases. We conjecture that for $K \rightarrow \infty$, the probability mass of the SC is concentrated at the point $C_s = 0^+$. Evidence of the validity of this conjecture is provided by the evaluation of the expected value and the variance of the SC:

Proposition 1 [Expected value and variance of the SC]: The expected value and the variance of the SC when the legitimate destination is chosen following (12) and all the other destinations are considered as passive eavesdroppers can be given by

$$\mathbb{E}[C_s] = \int_0^{+\infty} \int_0^\lambda \log\left(\frac{1+\lambda p_{max}}{1+\mu p_{max}}\right) f_{K,K-1}^{(K)}(\lambda, \mu) d\mu d\lambda \quad (21)$$

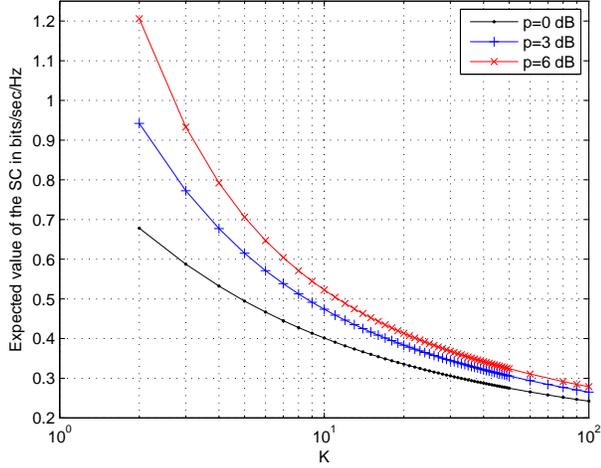


Fig. 4. Expected value of the SC without side information as a function of K .

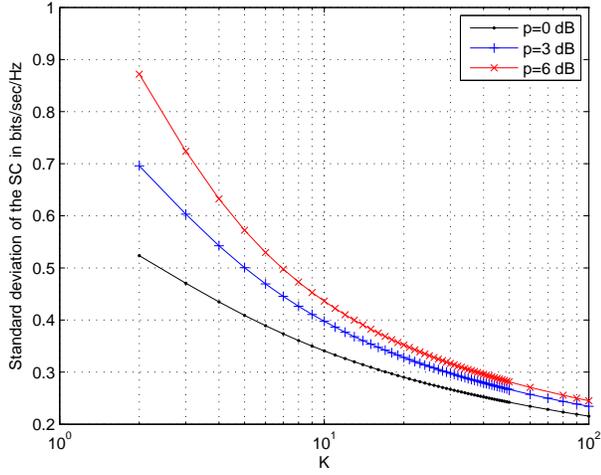


Fig. 5. Standard deviation of the SC without side information as a function of K .

and

$$\begin{aligned} \mathbb{E}[C_s^2] - \mathbb{E}[C_s]^2 &= \int_0^{+\infty} \int_0^\lambda \log^2\left(\frac{1 + \lambda p_{\max}}{1 + \mu p_{\max}}\right) \\ &\times f_{K,K-1}^{(K)}(\lambda, \mu) d\mu d\lambda - \mathbb{E}[C_s]^2 \end{aligned} \quad (22)$$

respectively.

Numerical evaluations⁴ of the expectation and the standard deviation of the secrecy capacity are depicted in Figs. 4 and 5, respectively. As expected, the average SC reduces monotonically with the cardinality K of \mathcal{K} . This is due to the fact that the probability of finding two destinations with similar SNR levels increases monotonically with K . Thus, from (21) it becomes clear that in the absence of any side information, the broadcasting of secret messages can be compromised, unless a substantial decrease in the transmission rate can be tolerated.

We further note that the mean value of the ratio of the standard deviation to the expected value is roughly equal to

⁴All numerical integrations hereafter were executed in MAPLE 16 ®.

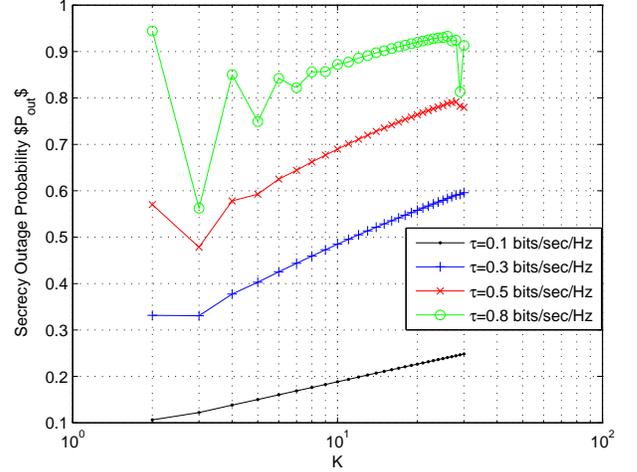


Fig. 6. Secrecy outage probability without side information as a function of K for $p_{\max} = 0$ dB.

0.85 (it increases slightly with an increase in the cell size). The large variations around the expected value impose further restrictions in the design of perfectly secure multiuser network transmission protocols.

On the contrary, given the problem formulation, the probability of a positive secrecy capacity is unity and can be derived noting that by definition $g_{k^*} \geq g_{k^{**}}$:

Proposition 2 [Secrecy outage probability]: In a set of K non-colluding destinations, the probability of a positive secrecy capacity is the probability mass of $f_{K,K-1}^{(K)}(g_{k^*}, g_{k^{**}})$ in the entire plane of admissible values of g_{k^*} and $g_{k^{**}}$ and is therefore unity,

$$\Pr(C_s > 0) = \int_0^\infty \int_0^\lambda f_{K,K-1}^{(K)}(\lambda, \mu) d\mu d\lambda = 1. \quad (23)$$

The probability of a secrecy outage, with respect to a target threshold secrecy capacity value τ , is the probability mass of $f_{K,K-1}^{(K)}(g_{k^*}, g_{k^{**}})$ in the left of the plane $g_{k^{**}} = \frac{1 + g_{k^*} p_{\max} - 2^\tau}{2^\tau p_{\max}}$ and is given by

$$\begin{aligned} P_{out} &= \Pr(C_s \leq \tau) = 1 - \Pr\left(\log \frac{1 + \lambda p_{\max}}{1 + \mu p_{\max}} > \tau\right) \\ &= 1 - \int_0^\infty \int_0^{\frac{1 + \lambda p_{\max} - 2^\tau}{2^\tau p_{\max}}} f_{K,K-1}^{(K)}(\lambda, \mu) d\mu d\lambda. \end{aligned} \quad (24)$$

In Fig. 6 numerical evaluations of the secrecy outage probability are depicted for $p_{\max} = 0$ dB. These numerical evaluations further stress the dramatic effect - in terms of perfect secrecy - of the antagonistic relations between all destinations, even for medium size networks of $K = 30$ destinations. For example, transmitting perfectly secret messages at a rate of 0.5 bits/sec/Hz is only possible roughly 20% of the time due to the fact that the most capable destination in a given transmission frame is being attacked by $K - 1 = 29$ eavesdroppers. Finally, it is noted that for $\tau = 0.8$ bits/sec/Hz numerical errors in the evaluation of the outage probability result in less accurate evaluations.

The importance of side information in multiuser networks is highlighted in the next section where reverse conclusions are drawn by adopting a more realistic and less pessimistic point of view. The investigations presented next are motivated by the intuition that in typical commercial applications the vast majority of destinations have no interest in eavesdropping; malicious behavior is on the contrary confined to a small set of adversaries.

IV. STOCHASTIC CHARACTERIZATION OF THE SC WITH SIDE INFORMATION

In this section, we consider that there exists a set \mathcal{E} of eavesdroppers that wish to decode secret messages and that this set is distinct from the set of destinations \mathcal{K} , i.e., $\mathcal{E} \cap \mathcal{K} = \emptyset$. Nevertheless, although the individual identities of the eavesdroppers are unknown, side information is available regarding the cardinality $E = |\mathcal{E}|$ of the set of potential eavesdropping terminals⁵. Amongst this population, we employ index j^* to denote the eavesdropping terminal that has the highest statistical advantage for eavesdropping. In the present work we further assume that the eavesdroppers are not cooperating.

A. Side Information over the Exact Number of Eavesdroppers

Assuming that side information over the exact number of eavesdroppers is available, the pdf $f_E^{(E)}(\tilde{g}_{j^*})$ of the channel gain \tilde{g}_{j^*} of the most capable eavesdropper (in terms of SNR strength) can be characterized as the E -th order statistics of a sample of E channel realizations,

$$f_E^{(E)}(\lambda) = EF(\lambda)^{E-1}f(\lambda) \quad (25)$$

with cdf $F_E^{(E)}(\lambda)$. It is important to note that in the case under examination g_k^* and \tilde{g}_{j^*} are generated from two *independent* ordering operations and consequently are independent (we make no assumption over the ordering of g_{k^*} with respect to \tilde{g}_{j^*}). The joint pdf $f_{K,E}^{(K)(E)}(g_k^*, \tilde{g}_{j^*})$ of the channel gain of the strongest destination and the strongest eavesdropper is merely the product of the marginal distributions, i.e.,

$$f_{K,E}^{(K)(E)}(g_k^*, \tilde{g}_{j^*}) = f_K^{(K)}(g_k^*)f_E^{(E)}(\tilde{g}_{j^*}). \quad (26)$$

As a result the pdf of the SC is derived as follows:

Theorem 2 [Pdf of the SC with side information]: The pdf $f_{C_s^}(C_s^*)$ of the SC C_s^* in a set of K non-colluding destinations in the presence of a distinct set of E non-colluding eavesdroppers can be expressed as*

$$f_{C_s^*}(C_s^*) = f_{C_{k^*}^*}(C_s^*) \otimes f_{C_{j^*}^*}(-C_s^*)U(C_s^*) + Pr(C_{k^*}^* \leq C_{j^*}^*)\delta(C_s^*) \quad (27)$$

where

$$C_{k^*}^* = \log(1 + g_{k^*}p), \quad (28)$$

$$C_{j^*}^* = \log(1 + \tilde{g}_{j^*}p), \quad (29)$$

$$f_{C_{k^*}^*}(\lambda) = \ln(2)p^{-1}2^\lambda f_K^{(K)}((2^\lambda - 1)p^{-1}), \quad (30)$$

$$f_{C_{j^*}^*}(\lambda) = \ln(2)p^{-1}2^\lambda f_E^{(E)}((2^\lambda - 1)p^{-1}), \quad (31)$$

⁵In a sense we assume that a statistical characterization of the vulnerability of the wireless network has been performed and priors were extracted.

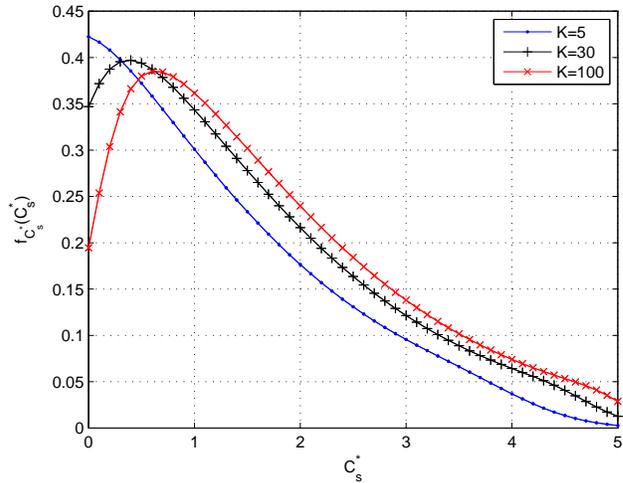


Fig. 7. Pdf of the SC with side information over the existence of $E = 1$ eavesdropper. The weights of the delta discontinuities at the origin (not depicted here) are $Pr(C_{k^*}^* \leq C_{j^*}^*) = 0.17, 0.02, 0.01$ for $K = 5, 30$, and 100 , respectively.

where \otimes denotes convolution and

$$\begin{aligned} Pr(C_{k^*}^* \leq C_{j^*}^*) &= Pr(g_{k^*} \leq \tilde{g}_{j^*}) \\ &= \int_0^\infty \int_\lambda^\infty f_K^{(K)}(\lambda) f_E^{(E)}(\mu) d\mu d\lambda \quad (32) \end{aligned}$$

Proof: The derivation of (27) is straightforward based on the subtraction of two independent random variables and passing the output through a hard limiter. (32) is the consequence of defining p on a continuous support so that $Pr(p = 0) = 0$. \square

Numerical evaluations of the pdf of the SC are depicted in Fig. 7 for a single eavesdropper in networks of $K = 5, 30$, and 100 destinations. With increasing cell size K , the probability mass concentrates to higher values of the SC C_s^* , reversing the conclusions drawn in the section without side information. Furthermore, with $K \rightarrow \infty$ the discontinuity of C_s^* at the origin vanishes, i.e., $Pr(C_{k^*}^* \leq C_{j^*}^*) \rightarrow 0$, implying that almost surely a positive SC can be established.

In the case of non-cooperative eavesdroppers, the expected value and the variance of the SC of the network with respect to a set \mathcal{E} , $E = |\mathcal{E}|$ of eavesdroppers can be expressed as

Proposition 3 [Expected value and variance of the SC]: The average SC of a set of K non-colluding destinations with respect to a distinct set of E non-colluding passive eavesdroppers is given by

$$\mathbb{E}[C_s^*] = \int_0^{+\infty} \int_0^\lambda \log\left(\frac{1 + \lambda p_{\max}}{1 + \mu p_{\max}}\right) dF_E^{(E)}(\mu) dF_K^{(K)}(\lambda), \quad (33)$$

and

$$\begin{aligned} \mathbb{E}[C_s^{*2}] - \mathbb{E}[C_s^*]^2 &= \int_0^{+\infty} \int_0^\lambda \log^2\left(\frac{1 + \lambda p_{\max}}{1 + \mu p_{\max}}\right) \\ &\quad \times f_K^{(K)}(\lambda) f_E^{(E)}(\mu) d\mu d\lambda - \mathbb{E}[C_s^*]^2 \quad (34) \end{aligned}$$

respectively, with $f_K^{(K)}(\lambda)d\lambda = dF_K^{(K)}(\lambda)$ and $f_E^{(E)}(\mu)d\mu = dF_E^{(E)}(\mu)$.

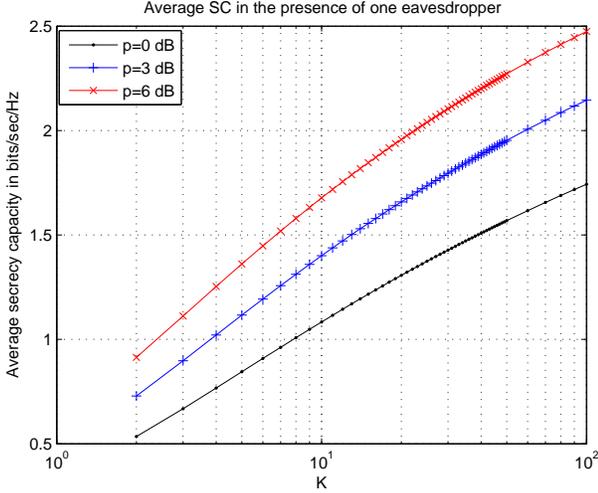


Fig. 8. Expected value of the SC with side information over the existence of a single eavesdropper as a function of K .

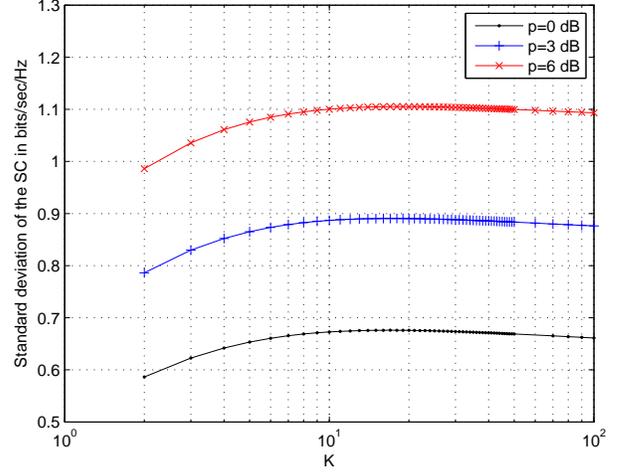


Fig. 10. Standard deviation of the SC with side information over the existence of a single eavesdropper as a function of K .

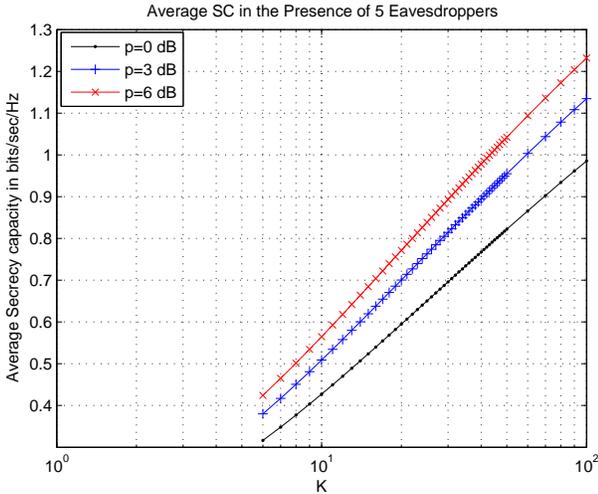


Fig. 9. Expected value of the SC with side information over the existence of $E = 5$ eavesdroppers as a function of K .

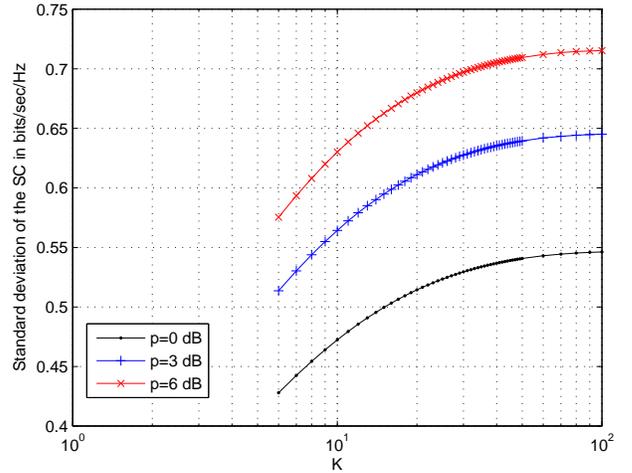


Fig. 11. Standard deviation of the SC with side information over the existence of $E = 5$ eavesdroppers as a function of K .

Numerical evaluations of (33) are depicted in Figs. 8 and 9 in the presence of $E = 1$ and $E = 5$ eavesdropping terminals, respectively. Notably, in the case of a single eavesdropper, the expected value of the SC approaches substantial values as the cell size increases. This results from the substantial increase in the probability of finding a destination with a higher SNR than the eavesdropper. This observation recalls the notion of multi-user diversity [33]. Furthermore, albeit the expected value of the SC decreases with increasing numbers of eavesdroppers, substantial secrecy rates are still attainable on average when the legitimate users outnumber the eavesdroppers, i.e., $E \ll K$.

Furthermore, numerical evaluations of (34) are depicted in Figs. 10 and 11 for $E = 1$ and $E = 5$ eavesdroppers respectively. The ratio of the standard deviation to the expected value monotonically decreases with increasing K , while the standard deviation decreases with increasing E . For $E = 1$ and $p_{max} = 0$ dB, it ranges from approximately 1 for $K = 2$ to

approximately 0.38 for $K = 100$. This effect is the immediate consequence of keeping the number of eavesdroppers constant while increasing K . Therefore, increasing the cell size in the presence of a limited number of adversaries creates some room for network planning and rate adaptation around the expected value of the secrecy capacity. Relevant directions will be discussed in the final section of this paper.

Finally, the probability of a secrecy outage can be derived as

Proposition 4 [Secrecy outage probability]: In a set of K non-colluding terminals, the probability of a positive SC with respect to a distinct set of E non-colluding eavesdroppers is the probability mass of $f_{K,E}^{(K)(E)}(g_{k^*}, \tilde{g}_{j^*})$ in the left of the plane $g_{k^*} = \tilde{g}_{j^*}$ and is given by

$$\begin{aligned} Pr(C_s^* > 0) &= Pr(g_{k^*} > \tilde{g}_{j^*}) \\ &= \int_0^\infty \int_0^\lambda f_K^{(K)}(\lambda) f_E^{(E)}(\mu) d\mu d\lambda. \end{aligned} \quad (35)$$

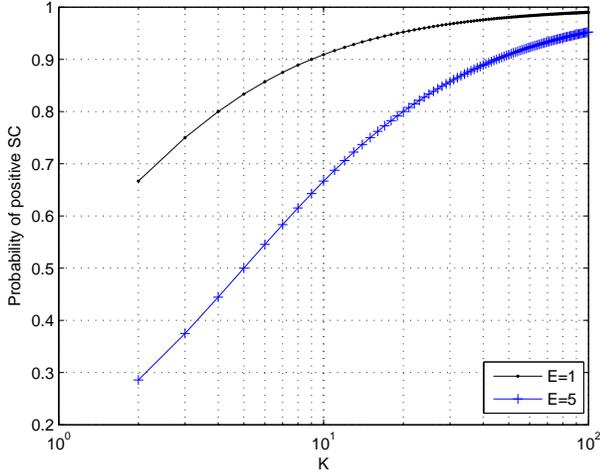


Fig. 12. Probability of positive SC with side information over the existence of E eavesdroppers as a function of K .

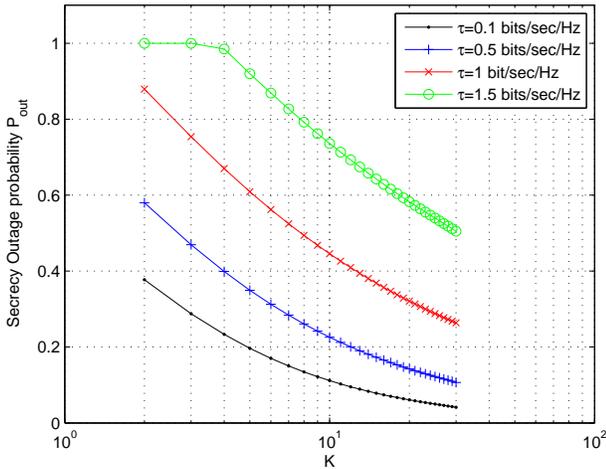


Fig. 13. Secrecy outage probability with side information over the existence of a single eavesdropper as a function of K .

The probability of a secrecy outage, with respect to a target threshold secrecy capacity value τ , is the probability mass of $f_{K,E}^{(K)(E)}(g_{k^*}, \tilde{g}_{j^*})$ in the left of the plane $\tilde{g}_{j^*} = \frac{1+g_{k^*}p_{\max}-2^\tau}{2^\tau p_{\max}}$ and is given by

$$\begin{aligned} P_{out} &= Pr(C_s^* \leq \tau) = 1 - Pr\left(\log \frac{1+g_{k^*}p_{\max}}{1+\tilde{g}_{j^*}p_{\max}} > \tau\right) \\ &= 1 - \int_0^\infty \int_0^{\frac{1+\lambda p_{\max}-2^\tau}{2^\tau p_{\max}}} f_K^{(K)}(\lambda) f_E^{(E)}(\mu) d\lambda d\mu \end{aligned} \quad (36)$$

In Fig. 12 numerical evaluations of the probability of positive SC are depicted for $E = 1$ and $E = 5$ eavesdroppers. Increasing the cell size to $K = 100$ destinations invokes that in the presence of a single eavesdropper a positive secrecy capacity can be established almost surely. Additionally, in Fig. 13 the probability of a secrecy outage has been evaluated in the case of $E = 1$ eavesdropper. It is noteworthy that a target secrecy rate of 0.5 bits/sec/Hz can be established approximately 90% of the time for a cell size of $K = 30$

destinations; moderate perfectly secure rates are attainable with high probability when $E \ll K$.

B. Side Information over the Distribution of the Number of Eavesdroppers

Relaxing the requirement for obtaining side information on the *exact* number of eavesdropping terminals, we now explore the case where a probability mass function (pmf) over the number of eavesdroppers is available. We define the random variable ε of the number of eavesdropping terminals, i.e. for a specific realization ε_i of ε we have $|\mathcal{E}| = \varepsilon_i$, with pmf

$$f_{\mathcal{E}}(\varepsilon) = \sum_i Pr(\varepsilon_i) \delta(\varepsilon - \varepsilon_i). \quad (37)$$

Noting that ε , g_{k^*} and \tilde{g}_{j^*} are independent and that their joint pdf is concentrated on the discrete points ε_i , we can employ the results of the previous section and derive the pdf of the SC as follows:

Theorem 3 [Pdf of the SC with side information over the distribution of the number of eavesdroppers]: The pdf $f_{C_s^*}(C_s^*)$ of the SC C_s^* in a set of K non colluding destinations in the presence of a distinct set of ε non colluding eavesdroppers with pmf $f_{\mathcal{E}}(\varepsilon)$ can be expressed as

$$\begin{aligned} f_{C_s^*}(C_s^*) &= f_{C_{k^*}^*}(C_s^*) \otimes f_{C_{e_i}^*}(-C_s^*) U(C_s^*) \\ &+ Pr(C_{k^*}^* \leq C_{e_i}^*) \delta(C_s^*) \end{aligned} \quad (38)$$

where

$$C_{e_i}^* = \log(1 + \tilde{g}_{j^*} p) \quad (39)$$

$$f_{C_{e_i}^*}(\lambda) = \sum_i Pr(\varepsilon_i) \ln(2) p^{-1} 2^\lambda f_{\varepsilon_i}^{(\varepsilon_i)}((2^\lambda - 1) p^{-1}) \quad (40)$$

$$\begin{aligned} Pr(C_{k^*}^* \leq C_{e_i}^*) &= \sum_i Pr(\varepsilon_i) \int_0^\infty \int_\lambda^\infty f_K^{(K)}(\lambda) f_{\varepsilon_i}^{(\varepsilon_i)}(\mu) d\mu d\lambda. \end{aligned} \quad (41)$$

We have so far demonstrated the importance of side information in broadcast networks with multiple eavesdroppers. It has been shown that understanding the vulnerability of the wireless network to passive attacks can create opportunities for building perfectly secure systems with satisfactory data rates for common commercial applications. However, given the extra effort devoted to enhancing the robustness of the network, it is only reasonable to assume that potential eavesdroppers will on the other hand take countermeasures to mitigate any advantages gained. In the next section we investigate such a scenario. A single eavesdropper tries to confuse the BS in order to establish opportunities for listening to secret conversations, i.e. the eavesdropper becomes *active*.

V. STOCHASTIC CHARACTERIZATION OF THE SC WITH SIDE INFORMATION IN THE PRESENCE OF AN ACTIVE EAVESDROPPER

Next, we consider the scenario in which a single *active* eavesdropper is registered in the network as a subscribed user and exchanges signaling messages with the BS. For simplicity, it is further assumed that the only objective of this malicious

user is to decode private messages of *any* legitimate user (this scenario is a subcase of the Byzantine attack [34] [35]). The information accumulated by the eavesdropper depends on the transmission rate and its equivocation rate, with eavesdropping referring to overhearing other users' data.

In this setting, the eavesdropper should intuitively adopt the following strategy:

- 1) If it has the highest CSI during a given channel realization, i.e., $\tilde{g}_{j^*} > g_{k^*}$, then it can report a false CSI $\hat{g}_{j^*} < g_{k^*}$ to the BS. If the BS does not identify the forgery, it will transmit a private message \mathbf{x} to a legitimate user k^* . In this case, the eavesdropper will be able to at least partially decode \mathbf{x} ;
- 2) If the eavesdropper does not have the highest SNR, it might not be able to eavesdrop. In this case, it can report a higher false CSI $\hat{g}_{j^*} > g_{k^*}$ claiming network resources from the BS. If the BS chooses to transmit to the eavesdropper, although no private information is leaked, the network resources are wasted as none of the legitimate destinations receives any new information.

In such a setting, it would appear that the legitimate users are completely unprotected against active attacks. Nevertheless, at least in principle, deviations in reported CSIs could be bounded around the true value. For example, in the case of a dense network primarily populated by legitimate users, the BS can employ statistical tests to isolate malicious nodes [36]. Bearing this in mind, we are interested in investigating the network's resilience to active eavesdroppers. That is, eavesdroppers that can mislead the transmitter by introducing false information about their own CSI.

Let us assume the following: (i) the BS can potentially transmit *only* to the user with the highest *reported* CSI and (ii) the eavesdropper *always* reports a CSI \hat{g}_{j^*} that deviates from its true CSI \tilde{g}_{j^*} by a certain additive quantity ϵ , i.e., $\hat{g}_{j^*} = \tilde{g}_{j^*} + \epsilon$. Given these assumptions, we define the following function $u : \mathbb{R}^+ \times \mathbb{R} \rightarrow \mathbb{R}$, with

$$\begin{aligned} u(p, \epsilon) &= \log \left(\frac{1 + g_{k^*} p}{1 + \tilde{g}_{j^*} p} \right) \mathbb{1}_{\{g_{k^*} > \tilde{g}_{j^*} + \epsilon\}}, \\ &= \log \left(\frac{1 + g_{k^*} p}{1 + \tilde{g}_{j^*} p} \right) \mathbb{1}_{\{g_{k^*} > \hat{g}_{j^*}\}}, \end{aligned} \quad (42)$$

where $\mathbb{1}_{\{\cdot\}}$ denotes the indicator function. The BS should aim at the maximization of $u(p, \epsilon)$, while the eavesdropper at its minimization.

Discussing the problem in more detail, we identify the following cases:

- 1) When $g_{k^*} > \hat{g}_{j^*}$ and $g_{k^*} > \tilde{g}_{j^*}$, then $u(p, \epsilon) > 0$. Thus, the strict positiveness of u is a necessary and sufficient condition for guaranteeing perfect secrecy.
- 2) When $u(p, \epsilon) = 0$, the BS either does not transmit at all or it transmits to the eavesdropper. In this case, no private messages are leaked. However, the network efficiency is compromised.
- 3) When $u(p, \epsilon) < 0$, the eavesdropper is able to partially decode the messages of a legitimate user.

In the following, we study the optimal behavior of the BS and the eavesdropper with respect to the function u , by

adopting the assumption of full CSI availability at both the transmitter and eavesdropper. This serves only as a first theoretical approximation to determine secrecy rate bounds under the assumption of fully rational base station and eavesdropper.

A. BS Optimal Strategy

Given the action adopted by the eavesdropper, the optimal action of the BS is to choose its transmit power to maximize the function u in (42). That is, the best response of the transmitter, denoted by $\text{BR}_B : \mathbb{R} \rightarrow \{0, p_{\max}\}$, is

$$\text{BR}_B(\epsilon) = \arg \max_{p \in \{0, p_{\max}\}} u(p, \epsilon). \quad (43)$$

Thus, we write

$$\text{BR}_B(\epsilon) = \begin{cases} p_{\max}, & \text{if } g_{k^*} > \max(\tilde{g}_{j^*}, \hat{g}_{j^*}), \\ 0, & \text{otherwise.} \end{cases} \quad (44)$$

B. Eavesdropper Optimal Strategy

The choices of the eavesdropper consist of reporting a forged CSI $\hat{g}_{j^*} = \tilde{g}_{j^*} + \epsilon$, greater or lower than its true CSI value \tilde{g}_{j^*} . Indeed, the optimal choice of $\epsilon \in \mathbb{R}$ is the one that minimizes the function u given the choice on the transmit power $p \in \{0, p_{\max}\}$ made by the BS. We define the best response of the eavesdropper by $\text{BR}_e : \{0, p_{\max}\} \rightarrow \mathbb{R}$, where,

$$\text{BR}_e(p) = \arg \min_{\epsilon \in \mathbb{R}} u(p, \epsilon). \quad (45)$$

Thus, we write

$$\text{BR}_e(p) = \begin{cases} \hat{\epsilon}, & \text{if } g_{k^*} > \tilde{g}_{j^*}, \\ \check{\epsilon}, & \text{otherwise,} \end{cases} \quad (46)$$

where the additive errors $\hat{\epsilon}$ and $\check{\epsilon}$ must satisfy the following conditions to allow the eavesdropper to mislead the transmitter,

$$\hat{\epsilon} \in (|g_{k^*} - \tilde{g}_{j^*}|, +\infty), \quad (47)$$

$$\check{\epsilon} \in (-\infty, -|g_{k^*} - \tilde{g}_{j^*}|). \quad (48)$$

We remark that according to the given formulation, for any action adopted by the BS, the eavesdropper has infinite choices in ϵ . Observing (44) and (46), we conclude that the best strategy for the BS as well as the eavesdropper depends on each other's actions. Thus, in the following, we use game theoretic tools to investigate this competitive interaction.

C. Two Player Game Formulation

We model the competitive interaction between the BS and the eavesdropper by the following one-shot two-player zero sum game:

$$\mathcal{G}(g_{k^*}, \tilde{g}_{j^*}) = \{\mathcal{A}_B, \mathcal{A}_e, u\}. \quad (49)$$

In the course of this game, both g_{k^*} and \tilde{g}_{j^*} are parameters that are fixed and known to both players. The sets \mathcal{A}_B and \mathcal{A}_e contain the actions available to the BS and the eavesdropper:

$$\mathcal{A}_B = \{0, p_{\max}\}, \quad (50)$$

$$\mathcal{A}_e = \{\hat{\epsilon}, \check{\epsilon}\}. \quad (51)$$

For the sake of simplicity, we assume that both $\hat{\epsilon}$, and $\check{\epsilon}$ are fixed constants such that $\hat{\epsilon} > 0$ and $\check{\epsilon} < 0$. That is, both sets \mathcal{A}_e and \mathcal{A}_B are finite.

The value of u does not depend on the exact value of the additive error ϵ but only on its sign. When the actions p and ϵ are played, the benefit of the transmitter is $u(p, \epsilon)$ while the benefit of the eavesdropper is $-u(p, \epsilon)$. To explore the optimal strategies of the two players, we use the concept of the Nash equilibrium (NE), defined as follows:

Definition 1 (Nash Equilibrium): The strategy profile $(p^*, \epsilon^*) \in \mathcal{A}_B \times \mathcal{A}_e$ is a Nash equilibrium of the game $\mathcal{G}(g_{k^*}, \tilde{g}_{j^*})$ if

$$p^* \in BR_B(\epsilon^*) \text{ and } \epsilon^* \in BR_e(p^*). \quad (52)$$

Following Def. 1, we state the following lemma.

Lemma 1 (Equilibria in $\mathcal{G}(g_{k^}, \tilde{g}_{j^*})$):* Let $(p^*, \epsilon^*) \in \mathcal{A}_B \times \mathcal{A}_e$ be a Nash equilibrium of the game $\mathcal{G}(g_{k^*}, \tilde{g}_{j^*})$, with $\hat{\epsilon} > 0$ and $\check{\epsilon} < 0$. Then,

- If $g_{k^*} > \tilde{g}_{j^*} + \hat{\epsilon}$, then $(p^*, \epsilon^*) \in \{(p_{\max}, \hat{\epsilon}), (p_{\max}, \check{\epsilon})\}$;
- If $\tilde{g}_{j^*} + \hat{\epsilon} > g_{k^*} > \tilde{g}_{j^*}$, then $(p^*, \epsilon^*) \in \{(p_{\max}, \hat{\epsilon})\}$;
- If $\tilde{g}_{j^*} > g_{k^*} > \tilde{g}_{j^*} + \check{\epsilon}$, then $(p^*, \epsilon^*) \in \{(0, \check{\epsilon})\}$; and
- If $\tilde{g}_{j^*} + \check{\epsilon} > g_{k^*}$, then $(p^*, \epsilon^*) \in \mathcal{A}_B \times \mathcal{A}_e$.

The proof of Lemma 1 follows immediately from Def. 1. In particular, Lemma 1 indicates that there *always* exists at least one NE for the game $\mathcal{G}(g_{k^*}, \tilde{g}_{j^*})$, for all $(g_{k^*}, \tilde{g}_{j^*}) \in \mathbb{R}_{\pm}^2$. Nonetheless, the equilibrium is not necessarily unique. For instance when $g_{k^*} > \tilde{g}_{j^*}$ and condition (47) is not met, there exist two NEs: $(p_{\max}, \hat{\epsilon})$ and $(p_{\max}, \check{\epsilon})$. More interestingly, in this case, $u(p_{\max}, \hat{\epsilon}) = u(p_{\max}, \check{\epsilon}) = \log\left(\frac{1+g_{k^*}}{1+\tilde{g}_{j^*}}\right) > 0$. That is, independently of its forgery, the eavesdropper can neither be allocated the channel nor eavesdrop the communication. Hence, transmitting secret information to the receiver with the highest channel gain, independently of the action of the eavesdropper, is always a NE.

In contrast, when $g_{k^*} > \tilde{g}_{j^*}$ and condition (47) is met, there exists a unique NE: $(p_{\max}, \hat{\epsilon})$ and $u(p_{\max}, \hat{\epsilon}) = 0$. In this case, the transmitter decides to transmit but it chooses the eavesdropper as the destination as it appears as the receiver with the highest channel gain. No leak of secret information occurs. Albeit, the eavesdropper introduces a delay in the communication of the transmitter with one of the legitimate receivers.

On the contrary, when $g_{k^*} < \tilde{g}_{j^*}$ and condition (48) is not met, there exist four NEs. Basically, any possible combination of actions is an NE and more interestingly $u(p_{\max}, \hat{\epsilon}) = 0$ for all $(p_{\max}, \hat{\epsilon}) \in \mathcal{A}_B \times \mathcal{A}_e$. This is due to the fact that the transmitter, if it transmits, always chooses the eavesdropper as the destination, and thus, no secret information is leaked. However, none of the legitimate receivers is able to receive secret information. On the contrary, when condition (48) is met, there exists only one NE: $(0, \check{\epsilon})$ and $u(0, \check{\epsilon}) = 0$. Here, the transmitter remains silent and no information is transmitted to any of the destinations.

Thus, when conditions (47) and (48) are met the transmitter is unable to convey secret messages to the legitimate destinations at the NE. However, no leak of secret information occurs either. This implies that when an eavesdropper is able

to properly set its additive error term ϵ , it cannot eavesdrop secret messages but it can introduce an infinitely long delay in the network before a legitimate destination receives a secret message.

On the contrary, when the eavesdropper is unable to set up its error terms ϵ following both (47) and (48), then the transmitter is able to convey secret messages to the legitimate receivers as long as $g_{k^*} > \tilde{g}_{j^*}$.

We describe the average secrecy rate (SR) at the NE in the following proposition.

Proposition 5 [Expected value of the SR with one active eavesdropper]: In the game $\mathcal{G}(g_{k^*}, \tilde{g}_{j^*})$ with K legitimate users and a single active eavesdropper, when the conditions (47) and (48) are not satisfied, the average secrecy rate at the NE is

$$\mathbb{E}[R_s(\hat{\epsilon})] = \int_0^{+\infty} \int_0^{\lambda - \frac{\hat{\epsilon}}{p_{\max}}} \log\left(\frac{1 + \lambda p_{\max}}{1 + \mu p_{\max}}\right) dF(\mu) dF_K^{(K)}(\lambda). \quad (53)$$

Otherwise, when both conditions (47) and (48) are true,

$$\mathbb{E}[R_s(\hat{\epsilon})] = 0. \quad (54)$$

From Prop. 5, it can be inferred that when conditions (47) and (48) are not met the respective loss in the achievable average secrecy rate as a function of $\hat{\epsilon}$ is

$$\begin{aligned} \Delta R_s(\hat{\epsilon}) &= \mathbb{E}[C_s^*] - \mathbb{E}[R_s] \\ &= \int_0^{+\infty} \int_{\lambda - \frac{\hat{\epsilon}}{p_{\max}} +}^{\lambda} \log\left(\frac{1 + \lambda p_{\max}}{1 + \mu p_{\max}}\right) dF(\mu) dF_K^{(K)}(\lambda). \end{aligned} \quad (55)$$

The result in (55) shows that the larger $\hat{\epsilon}$ in the interval (47), the more significant the reduction of the secrecy rate is with respect to the case of a passive eavesdropper.

Another interesting point is that

$$\lim_{\hat{\epsilon} \rightarrow \infty} \mathbb{E}[R_s(\hat{\epsilon})] = 0, \quad (56)$$

which implies that if the eavesdropper can choose $\hat{\epsilon}$ arbitrarily large, it can fully block the transmission of secret messages in the system. Nonetheless, an unreasonably large difference $|g_{k^*} - \tilde{g}_{j^*}|$ could be used as an indicator of the existence of malicious behavior and serve as a tool for the identification of active eavesdroppers, e.g. [37], [38].

VI. STOCHASTIC CHARACTERIZATION OF THE SC WITH SIDE INFORMATION IN THE HIGH SNR REGIME

Interestingly, in the high SNR regime, for finite $\hat{\epsilon} < \infty$, the system becomes robust to active attacks, since

$$C_{sH}^* = \lim_{p_{\max} \rightarrow \infty} R_s(\hat{\epsilon}) = \lim_{p_{\max} \rightarrow \infty} C_s^* = \left[\log\left(\frac{g_{k^*}}{\tilde{g}_{j^*}}\right) \right]^+ \quad (57)$$

This implies that in the high SNR regime, the SC of the system is independent of whether the eavesdropper is active or passive.

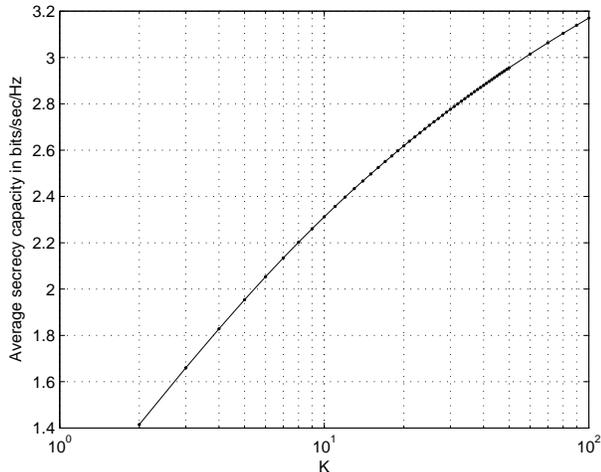


Fig. 14. Expected value of the SC in the high SNR regime in the presence of one active or passive eavesdropper as a function of K .

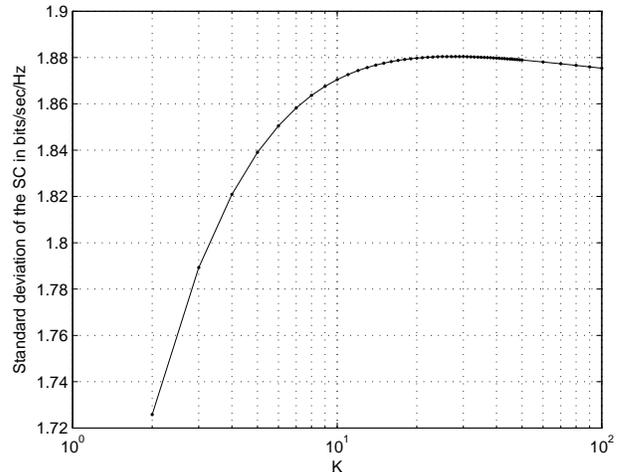


Fig. 15. Standard deviation of the SC in the high SNR regime in the presence of one active or passive eavesdropper as a function of K .

Theorem 4 [Pdf of the SC in the High SNR]: In the high SNR regime, the pdf $f_{C_{sH}^}(C_{sH}^*)$ of the SC C_{sH}^* in a set of K non-colluding destinations in the presence of a single passive or active eavesdropper can be expressed as*

$$f_{C_{sH}^*}(C_{sH}^*) = f_{C_{kH}^*}(C_{sH}^*) \otimes f_{C_{jH}^*}(-C_{sH}^*)U(C_{sH}^*) + Pr(C_{k^*} \leq C_{j^*})\delta(C_{sH}^*) \quad (58)$$

where

$$C_{kH}^* = \log(g_{k^*}), \quad (59)$$

$$C_{jH}^* = \log(\tilde{g}_{j^*}), \quad (60)$$

$$f_{C_{kH}^*}(\lambda) = \ln(2)2^\lambda f_K^{(K)}(2^\lambda), \quad (61)$$

$$f_{C_{jH}^*}(\lambda) = \ln(2)2^\lambda f(2^\lambda). \quad (62)$$

Proposition 6 [Expected value and variance of the SC in the high SNR]: In the high SNR regime, the expected value and the variance of the SC in a set of K non-colluding destinations in the presence of a single active or passive eavesdropper are given, respectively, by

$$\mathbb{E}[C_{sH}^*] = \int_0^{+\infty} \int_0^\lambda \log\left(\frac{\lambda}{\mu}\right) dF(\mu) dF_K^{(K)}(\lambda) \quad (63)$$

and

$$\begin{aligned} \mathbb{E}[C_{sH}^{*2}] - \mathbb{E}[C_{sH}^*]^2 &= \int_0^{+\infty} \int_0^\lambda \log^2\left(\frac{\lambda}{\mu}\right) dF(\mu) \\ &\quad \times dF_K^{(K)}(\lambda) - \mathbb{E}[C_{sH}^*]^2. \end{aligned} \quad (64)$$

Numerical evaluations of the expected value and the standard deviation of the SC in the high SNR regime are depicted in Fig. 14 and Fig. 15, respectively. It is clear that in such scenarios opportunities of perfectly secure transmission can be substantiated.

Finally, we have the following

Proposition 7 [Secrecy outage probability]: The secrecy outage probability with respect to a threshold SC τ is evaluated

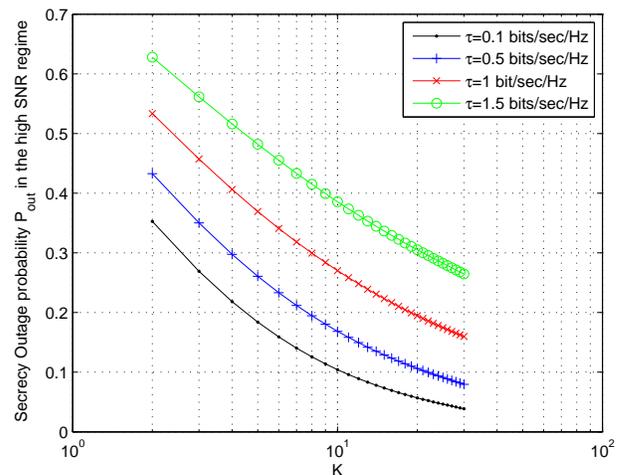


Fig. 16. Probability of a secrecy outage with respect to a target threshold SC value in the high SNR regime in the presence of one active or passive eavesdropper as a function of K .

as the probability mass of $f_{C_{sH}^*}(C_{sH}^*)$ in the left of the plane $\tilde{g}_{j^*} = \frac{g_{k^*}}{2^\tau}$,

$$Pr(C_{sH}^* < \tau) = 1 - \int_0^\infty \int_0^{\frac{\lambda}{2^\tau}} f_K^{(K)}(\lambda) f(\mu) d\mu d\lambda \quad (65)$$

The secrecy outage probability is depicted in Fig. 16. Notably, it is demonstrated that for a medium cell size of $K = 30$ destinations in the presence of a single active or passive eavesdropper, a perfectly secure transmission rate of 0.5 bits/sec/Hz is attainable more than 93% of the time.

VII. HEURISTIC TRANSMISSION STRATEGIES IN THE HIGH SNR REGIME

In the following, we compare two heuristic transmission approaches. A systematic investigation of possible transmission strategies is a subject for planned future research. The present section serves as an example of how the results presented

in this paper can be employed towards making informed decisions regarding the allocation of resources, parametrically to the network layout.

In the first approach, the BS always transmits at the destination with the highest reported CSI at a constant rate R_c equal to the expected value of the SC minus the standard deviation, i.e.,

$$R_c = \mathbb{E}[C_{sH}^*] - \sqrt{\mathbb{E}[C_{sH}^{*2}] - \mathbb{E}[C_{sH}^*]^2}. \quad (66)$$

In the second approach, the BS adopts an on/off approach based on a comparison of the highest reported channel gain to the expected value of the K -th order statistic of the channel gains; the BS chooses not to transmit if the former is lower than the latter. In the opposite case it transmits at a rate R_v equal to expected value of the SC minus the standard deviation, i.e.,

$$R_v = \begin{cases} \mathbb{E}[C_{sH}^*] - \sqrt{\mathbb{E}[C_{sH}^{*2}] - \mathbb{E}[C_{sH}^*]^2}, & g_{k^*} \geq \mathbb{E}[g_{k^*}], \\ 0, & \text{otherwise.} \end{cases} \quad (67)$$

In the following we evaluate the information leaked in the two heuristic strategies. In both cases it is assumed that the BS employs encoding schemes that ensure perfect secrecy as long as the transmission rate is smaller than the SC.

A. Constant Rate Transmission

For the constant rate transmission approach, information is leaked to the eavesdropper during those transmission intervals for which $R_c \geq C_{sH}^*$. The probability of this event is evaluated as

$$\begin{aligned} P_c &= Pr(R_c \geq C_{sH}^*) = Pr(g_{k^*} \leq 2^{R_c} \tilde{g}_{j^*}) \\ &= \int_0^\infty \int_0^{2^{R_c} \tilde{g}_{j^*}} dF_K^{(K)}(g_{k^*}) dF(\tilde{g}_{j^*}). \end{aligned} \quad (68)$$

Therefore, in N transmission intervals, assuming N is sufficiently large, the expected value of the information leaked, denoted by $I_c(N)$, in ergodic channel conditions, can be expressed as

$$I_c(N) = NP_c \left(\mathbb{E}[C_{sH}^*] - \sqrt{\mathbb{E}[C_{sH}^{*2}] - \mathbb{E}[C_{sH}^*]^2} \right). \quad (69)$$

B. Variable Rate Transmission

In the case of variable rate transmission, information is leaked when $g_{k^*} \geq \mathbb{E}[g_{k^*}]$ and $R_v \geq C_{sH}^*$. These two events are independent and as a result, information is leaked when $\mathbb{E}[g_{k^*}] \leq g_{k^*} \leq 2^{R_v} \tilde{g}_{j^*}$. Therefore, information is leaked with probability P_v , evaluated as

$$\begin{aligned} P_v &= Pr(\mathbb{E}[g_{k^*}] \leq g_{k^*} \leq 2^{R_v} \tilde{g}_{j^*}) \\ &= \int_0^\infty \int_{\mathbb{E}[g_{k^*}]}^{2^{R_v} \tilde{g}_{j^*}} dF_K^{(K)}(g_{k^*}) dF(\tilde{g}_{j^*}). \end{aligned} \quad (70)$$

Clearly, $P_v \leq P_c$. The expected value of the information leaked, denoted by $I_v(N)$, in N transmission intervals, assuming N is sufficiently large and the channel is ergodic, can be expressed as

$$I_v(N) = NP_v \left(\mathbb{E}[C_{sH}^*] - \sqrt{\mathbb{E}[C_{sH}^{*2}] - \mathbb{E}[C_{sH}^*]^2} \right). \quad (71)$$

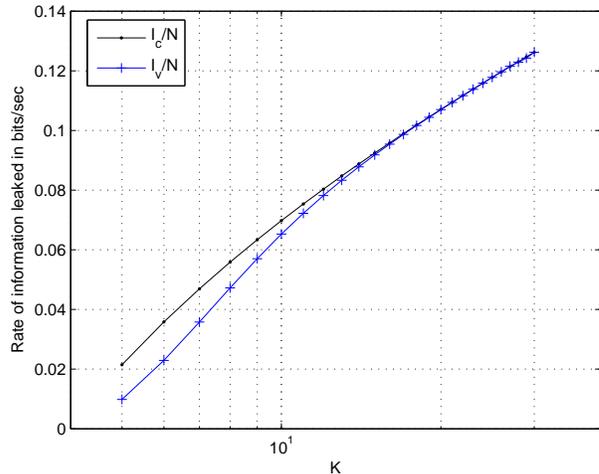


Fig. 17. Rate of information leaked for the constant rate and variable rate transmission approaches in the high SNR regime in the presence of one active or passive eavesdropper as a function of K .

In the constant rate approach, information is leaked with a higher probability than in the variable rate approach. In Fig. 17 we depict numerical evaluations of the rate of information leaked per transmission interval, i.e. I_c/N and I_v/N , respectively. Interestingly, as the cell size increases, the rate of information leaked is the same for both transmission approaches, indicating that with increasing K , the K -th order statistic of the channel gains is with a high probability close to its expected value.

VIII. CONCLUSIONS

In this paper, we have presented an extensive set of results regarding the stochastic characterization of SCs in wireless multiuser networks. In our setting, a management unit wishes to transmit secret messages to a set of destinations. It has been demonstrated that in a purely antagonistic scenario and in absence of any information about the existence of potential eavesdroppers, such an endeavor could be seriously compromised. Nevertheless, if quantitative side information is available regarding the cardinality of the set of passive eavesdroppers, substantial secrecy rates are attainable on average. Indeed, the achievable secrecy rates increase with the ratio between the number of legitimate users and the number of eavesdroppers.

Furthermore, the effect of an active eavesdropper has been systematically evaluated through the use of game theoretic tools. Here, the difference between an active and a passive eavesdropper is captured in behavioral aspects. The former, interacts with the BS providing false feedback, for instance, false CSI. We have formulated the competitive interaction between the BS and the active eavesdropper as an one-shot zero-sum game and evaluated upper bounds for the achievable average secrecy rates. Our analysis suggests that in order to minimize the loss incurred by such attacks, extra side information is required.

Notably, we have found that in the high SNR regime, the network is insensitive to the passiveness or activeness of

the attack. It has been demonstrated that in such scenarios, moderate perfectly secure rates are achievable with a very high probability in medium size networks. Finally, the results presented in this paper can serve as the basis for the comparison of practical transmission strategies with respect to the cell size.

REFERENCES

- [1] C. Shannon, "A mathematical theory of cryptography," *Bell System Technical J.*, vol. 28, p. 656715, Oct. 1949.
- [2] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. John Wiley and Sons, Inc., 1996.
- [3] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Hanover, MA: Now Publishers, 2009.
- [4] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. New York, NY: Springer, 2010.
- [5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press.
- [6] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications Magazine*, vol. 1, no. 19, pp. 40–47, Feb. 2012, invited article.
- [7] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1385–1357, Oct. 1975.
- [8] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [9] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [10] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
- [11] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Information Theory*, vol. 54, no. 10, pp. 4687–5403, Oct. 2008.
- [12] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 6, no. 54, pp. 2470–2492, Jun. 2008.
- [13] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: the 2-2-1 channel," *IEEE Trans. Information Theory*, vol. 55, no. 9, p. 4033 4039, Sep. 2009.
- [14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part I: The MISOME wiretap channel," *IEEE Trans. Information Theory*, vol. 56, no. 7, pp. 3088– 3104, Jul. 2010.
- [15] —, "Secure transmission with multiple antennas - part II: The MIMOME wiretap channel," *IEEE Trans. Information Theory*, vol. 56, no. 11, pp. 5515– 5532, Nov. 2010.
- [16] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 2, p. 704 716, Apr. 2012.
- [17] D. Lun, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Processing*, vol. 58, no. 3, part 2, pp. 1845–1888, Mar. 2010.
- [18] R. Zhang, L. Song, Z. Han, and B. J. M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. of IEEE Global Communications Conf.*, Miami, USA, 6-10 Dec. 2010, pp. 1–6.
- [19] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secrecy analysis of unauthenticated amplify-and-forward relaying with antenna selection," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2012, pp. 2481 – 2484.
- [20] X. Tang, R. Liu, P. Spasojevic, and H.V. Poor, "Interference assisted secret communication," *IEEE Trans. Information Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
- [21] A. Chorti and H. V. Poor, "Achievable secrecy rates in physical layer secure systems with a helping interferer," in *Proc. IEEE Int. Conference on Computing, Networking and Communications*, 2012, pp. 18–22.
- [22] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 388–396, Feb. 2012.
- [23] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting with multiuser diversity," in *Allerton 2006*, 2006.
- [24] J. Hyoungsook, K. Namshik, C. Jinho, L. Hyuckjae, and H. Jeongseok, "On multiuser secrecy rate in flat fading channel," in *Proc. IEEE Military Communications Conference (MILCOM)*, Boston, MA, Oct. 2009.
- [25] M. Z. I. Sarkar and T. Ratnarajah, "Secure communications through Rayleigh fading SIMO channel with multiple eavesdroppers," in *Proc. IEEE International Conference on Communications (ICC)*, Cape Town, South Africa, May 2010.
- [26] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, Jun. 2009, special issue on Wireless Physical Layer Security.
- [27] O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
- [28] Q. Li and W. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Transactions Signal Processing*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.
- [29] M. Z. I. Sarkar and T. Ratnarajah, "Secure communication through Nakagami- m fading MISO channel," in *Proc. IEEE International Conference on Communications (ICC)*, Kyoto, Japan, Jun. 2011.
- [30] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, UK: Cambridge University Press, 2011.
- [31] H.-C. Yang and M.-S. Alouini, *Diversity, Adaptation and Scheduling in MIMO and OFDM Systems*. Cambridge University Press, 2011.
- [32] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. New York, NY: McGraw-Hill Higher Education, 2002, 4th edition.
- [33] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Proc. IEEE International Conference on Communications (ICC)*, vol. 1, Seattle, USA, Jun. 1995, pp. 331–335 vol.1.
- [34] R. S. L. L. Lamport and M. Pease, "The byzantine generals problem," *ACM Trans. Programming Languages Syst.*, vol. 4, no. 3, p. 382401, Jul. 1982.
- [35] V. M. S. Marano and L. Tong, "Distributed detection in the presence of Byzantine attack," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16–29, Jan. 2009.
- [36] A. L. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE J. Selected Areas in Communications*, vol. 25, no. 6, pp. 1124–1134, Aug. 2007.
- [37] A. Algans, K. I. Pedersen, and P. E. Mogensen, "Experimental analysis of the joint statistical properties of azimuth spread, delay spread, and shadow fading," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 3, pp. 523–531, Apr. 2002.
- [38] L. Woongsup and C. Dong-Ho, "A new neighbor discovery scheme based on spatial correlation of wireless channel," in *Proc. IEEE Vehicular Technology Conference (VTC-Spring)*, Barcelona, Spain, Apr. 2009.