Rate Adaptation for Incremental Redundancy Secure HARQ

Zeina Mheich, Maël Le Treust, Florence Alberge, Pierre Duhamel

▶ **To cite this version:**

Zeina Mheich, Maël Le Treust, Florence Alberge, Pierre Duhamel. Rate Adaptation for Incremental Redundancy Secure HARQ. IEEE Transactions on Communications, 2016, 64 (2), pp.765-777. 10.1109/TCOMM.2015.2514284 . hal-01273989

HAL Id: hal-01273989
https://hal.science/hal-01273989

Submitted on 15 Feb 2016

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.

Rate Adaptation for Incremental Redundancy Secure HARQ

Zeina Mheich[1], Maël Le Treust[2], Florence Alberge[1], and Pierre Duhamel[1]
1. Univ. Paris-Sud, UMR8506 Orsay, F-91405; CNRS, Gif-sur-Yvette, F-91192;
Supélec, Gif-sur-Yvette, F-91192, France
Tel: +33 1 69851757; fax: +33 1 69851765
e-mail:{alberge, zeina.mheich, pierre.duhamel}@lss.supelec.fr
2. ETIS, CNRS UMR8051, ENSEA, Université de Cergy-Pontoise,
6, avenue du Ponceau, 95014 Cergy-Pontoise, France
e-mail: mael.le-treust@ensea.fr

***Abstract*—This paper studies secure communication based on incremental redundancy (INR) secure hybrid automatic retransmission request (HARQ) protocol over block-fading wiretap channels. The transmitter has no instantaneous channel state information (CSI) available from either main channel or the eavesdropper channel, hence the coding rates cannot be adapted to instantaneous channel conditions. We investigate the outage performance for two schemes of INR secure HARQ protocols: case 1) when there exists two reliable multi-bit feedback channels from both legitimate receiver and eavesdropper to the transmitter carrying a function of outdated CSI, case 2) when there is a multi-bit feedback channel only from legitimate receiver. In both cases, we demonstrate that using the information carried via multi-bit feedback channels, the transmitter can adapt the coding rates in order to achieve a better secrecy throughput using a smaller number of transmissions comparing to the ACK/NACK feedback channel model. For some parameters, our rate adaptation protocol achieves a strictly positive secrecy throughput whereas it is equal to zero for the protocol with ACK/NACK feedback. We show that for some set of parameters, the loss of secrecy throughput between case 1 and case 2 is very small compared to the gain provided by both protocols.**

I. INTRODUCTION

Automatic repeat request (ARQ) is a protocol for error control in data transmission. When the receiver detects an error in a packet, it automatically requests the transmitter to resend the packet. This process is repeated until the packet is error free or the error continues beyond a predetermined number of transmissions. Thus the main components of an ARQ system are an *error-detection* code and a feedback channel from the receiver to the source. Hybrid-ARQ (HARQ) allows to combine the advantages of both ARQ and forward error correction (FEC). The FEC part of the system is an *error-correcting* code aiming to correct errors at the receiver. At the source, the packet, including the error-detection bits, is encoded using a FEC encoder. After FEC decoding at the receiver side, the parity-check bits allow the error-detection decoder to decide on the necessity to ask for a retransmission via the feedback channel. In this work, we consider incremental redundancy HARQ which exhibits higher throughput efficiency by adapting the code redundancy to channel conditions. In this scheme, when the first transmission cannot be decoded reliably and a retransmission is required, the transmitter sends additional parity bits possibly under different channel conditions. The receiver combines the values of the new parity bits with those previously received. Thus each retransmission contains different information than the previous ones. Incremental redundancy HARQ is easily realized with rate-compatible punctured channel codes. In [1], the authors provide an information-theoretic analysis of the throughput performance of HARQ protocols over block-fading Gaussian collision channels. References [2]-[4] focused on mother code and their puncturing for incremental redundancy HARQ scheme.

In addition to channel impairments, wireless communication is also susceptible to eavesdropping due to its broadcast nature. Consequently, the security of data communication over wireless networks has become an important concern. Traditionally, security is implemented at the higher layers of the protocol stack by using cryptographic techniques; however these techniques rely on the assumption of insufficient computational capabilities of the eavesdroppers. In his seminal work [5], Wyner initiates the physical layer security by introducing the wiretap channel in which a sender exploits the statistics of the channel to send a secret message to a receiver in the presence of an eavesdropper. Wyner assumes in his channel model that the signal received by the eavesdropper is a degraded version of the legitimate receiver signal. Then, this model was generalized in [6] where the channels do not obey necessarily any degradation relationship. The effect of fading on secure communication was studied in [7], [8].

Going from security based on cryptographic tools to physical layer security is a paradigm shift which raises many questions. One main objection to the physical layer approach is the degradation assumption, which initially was assumed necessary at an instantaneous level. In our setting, all channels, including the eavesdropper's one are characterized by their average properties. This is a first relaxation of the constraints, obtained at the expense of allowing some "outage" security events, which will be monitored and maintained at an acceptable level.

Part of this work has been presented at the 2014 European Signal Processing Conference (EUSIPCO 2014).

In [9], the authors studied secure packet communication over frequency-flat block-fading Gaussian channels, based on secure HARQ protocols with the joint consideration of channel coding, secrecy coding, and retransmission protocols. In particular, the error and secrecy performance of repetition time diversity (RTD) and incremental redundancy (INR) protocols are investigated based on Wyner code sequences, which ensure that the confidential message is decoded successfully by the legitimate receiver and is kept completely secret from the eavesdropper for a given set of channel realizations. They show that there exists a rate-compatible Wyner code family which suits the secure INR protocol.

In the system model of [9], the transmitter obtains a 1-bit ACK/NACK feedback from the legitimate receiver to declare a successful/unsuccessful decoding via an error free public channel. Incremental redundancy is also considered under the assumption that the sub-codewords have the same length in each retransmission. The transmitter can choose the coding rates based on the knowledge of channel statistics to maximize the secrecy throughput under reliability and secrecy constraints. In this paper, we generalize the assumptions of [9] by allowing the feedback channel(s) to carry soft information through multi-bit feedback channels. We study secure communication based on incremental redundancy HARQ protocols in two cases. In the first case, the transmitter makes use of multi-bit feedback channels from both destination and eavesdropper, carrying a function of outdated CSI, to adapt the rate. The fact that the eavesdropper also feedbacks information is clearly unrealistic, but this situation allows to propose a solution for the case where there is no feedback from the eavesdropper. A part of the results concerning the first case was presented in [10] where it is shown that the adaptive protocol with two-feedback channels can achieve significant gain in secrecy throughput with respect to the non-adaptive protocol. In this paper, we extend this study to analyze also the effect of channel conditions on the achievable gain. Additional contributions with respect to [10] include a second case study in which we investigate a more realistic model, where only the legitimate receiver sends multi-bit feedback to the transmitter. The main originality of this work is that the proposed scheme (case 2) does not require any feedback from the eavesdropper. In both cases, the secrecy throughput is maximized by adapting the coding rates at the transmitter based on the information received via the feedback channel(s). This is done by allowing the lengths of sub-codewords to change at each retransmission. Due to the absence of instantaneous CSI, the transmitter cannot adapt the coding rates to actual channel conditions. As a result, outage performance of secure HARQ is considered as in [9].

The gains of variable rate transmission over the fixed-rate for the predefined families of code were shown in many works as in [11]-[13]. Specifically, reference [11] considers a point-to-point communication system where the reliability of the communication is the only concern. However, this paper investigates the rate adaptation for incremental redundancy HARQ under both reliability and secrecy constraints. This introduces additional and significant challenges in the design with respect to [11] because the wiretap code requires the joint consideration of the code rate and the secrecy rate to ensure both reliability and security of communication. Hence, we have introduced a new parameter in the design which we have called "ratio of secret bit transmitted". This parameter is used to adjust the security level to a target value. An additional challenge with respect to [11] is that the wiretap channel involves two receiving nodes, which led us to the possibility of designing two secure adaptive HARQ protocols (case 1 and case 2) based on different assumptions on the availability of the feedback channel from the eavesdropper. The rate adaption policies are determined using dynamic programming method. The optimization problem is more complex to solve than that in [11], due to the presence of a secrecy constraint. Then, the paper evaluates the performance gain obtained with adaptive-rate transmissions over the non-adaptive rate. The loss experienced with this scheme compared to the situation with full information (case 1) is evaluated and comparison to the non-adaptive protocol in [9] is also provided. It will be clear from the numerical experiments that the adaptive scheme outperforms the non-adaptive scheme independently of channel conditions and that, for some particular channel conditions, both adaptive schemes (case 1 and case 2) exhibit similar performance.

The paper is organized as follows. The system model is described in section II. In section III, the basic principles of incremental redundancy and the transmission protocol are briefly reviewed leading to the problem statement given in section IV. The optimization problem under consideration is tackled in section V in which a numerical solution based on dynamic programming is given. The practical interest of the proposed method is questioned in section VI. A comparison with the results in [9] is also provided.

II. System Model and Preliminaries

We consider the block fading wiretap channel in Figure 1 in which a transmitter X sends confidential messages to a legitimate receiver Y in the presence of an eavesdropper Z which listens to the transmission. Both the main channel (source-destination channel) and the eavesdropper channel (source-eavesdropper channel) experience K-block fading in which channels remain constant over a block but vary independently from block to block. At the transmitter, a confidential message w with length M_i (information bits) is encoded into codeword x^N of N symbols $x_1, x_2, .., x_N$. We assume that the code can be constructed with arbitrary rate. There exists well known codes which offer this possibility such as rateless codes [14]. Rateless codes can encode a message into a number of symbols such that knowledge of any fraction of them allows one to recover the original message (with high probability). Although they are well-studied in literature to ensure the reliability of communication systems, practical rateless code design for secure HARQ protocols appears to be a challenging problem. The codeword x^N is divided into K subsets of the symbols $\mathbf{x}_k$, $k = 1, .., K$, called sub-codewords. The codeword occupies K slots: for $k = 1, .., K$, the k^{th} block $\mathbf{x}_k$ is sent in the k^{th} slot and received by the legitimate receiver through the channel gain $\sqrt{h_k}$ and by the eavesdropper through the channel gain $\sqrt{g_k}$.

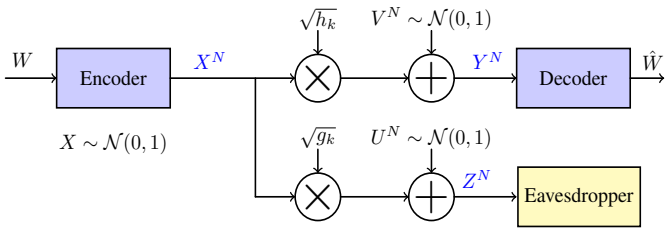

Figure 1. System model: the block fading wiretap channel.

The t^{th} received symbol x_t in the k^{th} block is given by:

$$y_t = \sqrt{h_k} \cdot x_t + v_t, \tag{1}$$
$$z_t = \sqrt{g_k} \cdot x_t + u_t, \tag{2}$$

where index k indicates the block number, $t = 1, .., N$ is the index of the transmitted symbol, v_t and u_t are zero mean unit variance i.i.d. Gaussian noise samples of the main channel and the eavesdropper channel respectively at time t. We assume that codeword symbols are samples of a zero mean real Gaussian distribution with unit average power, i.e. $\mathbb{E}[X^2] \leq 1$, where X is a random variable denoting the transmitted signal. Thus the signal-to-noise ratios (SNRs) received at the legitimate receiver and the eavesdropper are respectively h_k and g_k at the k^{th} transmission. We consider Rayleigh block fading, thus the main channel instantaneous SNR, and the eavesdropper channel instantaneous SNR are characterized by two exponential probability distribution functions:

$$p_H(x) = \frac{1}{\overline{h}} \cdot e^{-\frac{x}{\overline{h}}}, \tag{3}$$
$$p_G(x) = \frac{1}{\overline{g}} \cdot e^{-\frac{x}{\overline{g}}}, \tag{4}$$

where $\overline{h}$ and $\overline{g}$ are the average SNRs of the main channel and the eavesdropper channel respectively. We consider the setting where the transmitter has no instantaneous channel state information available from either the main channel or the eavesdropper channel, but knows only channel statistics. For each channel (main channel or eavesdropper channel), the constant gain during each block is assumed to be perfectly known at the respective receiver but unknown at the transmitter.

Consider a single block transmission (i.e. $K = 1$) and introduce Wyner codes. In [5], Wyner introduced the notion of wiretap channel which is the simplest channel model that takes security constraints into account. In a wiretap channel, the source wishes to convey a message $w \in \mathcal{W}$, which is chosen uniformly at random from the message set $\mathcal{W}$, to the legitimate receiver through the main channel. The sender performs this task by encoding w as a vector x^N of length N and transmitting x^N. Let $C(N, R_0, R_s)$ denote the Wyner code used to transmit the confidential message set $\mathcal{W} = \{1, 2, .., 2^{NR_s}\}$. Here, N is the codeword length, R_0 is the main channel code rate and R_s ($R_s \leq R_0$) is the secrecy information rate. The basic idea of Wyner codes is to use a stochastic encoder to increase the secrecy level [5]. We refer the reader to [15] and [16] for more details about information theoretic secrecy. Throughout this paper, we use $M_i = N \cdot R_s$ to denote the number of information bits (which is fixed) and $M_0 = N \cdot R_0$ to denote the total number of bits transmitted, which includes the M_d dummy bits that are necessary to ensure secrecy. We define the "ratio of secret bits transmitted" by $\gamma = \frac{M_i}{M_0} = \frac{M_i}{M_i + M_d}$. The number of dummy bits M_d can be chosen by the transmitter according to channel statistics. We can observe that $\gamma \in [0, 1]$. When γ is close to 0, the secrecy is more robust since the number M_d of dummy bits is large. At the opposite, when γ is close to 1, the number M_d of dummy bit is small and the secrecy is less robust.

Assume that the transmitted signals are received at the legitimate receiver and the eavesdropper via channel SNRs h and g respectively. Let $P_e(h)$ be the average decoding error probability for the legitimate receiver:

$$P_e(h) = \sum_{w \in \mathcal{W}} \Pr\{\hat{w} \neq w | w \text{ sent}, h\} \Pr(w), \tag{5}$$

where $\hat{w}$ is the output of the legitimate decoder after observing y^N given that the message w is sent. To measure the amount of information that the eavesdropper receives about W, we use the following normalized conditional entropy $H(W|g, z^N)/N$ which is called the equivocation rate. We want the equivocation rate to be as high as possible, and ideally it should equal the rate R_s. Thus *(weak) secrecy*[1] is achieved if for all $\epsilon > 0$ the equivocation rate satisfies:

$$\frac{H(W|g, z^N)}{N} \geq \frac{H(W)}{N} - \epsilon. \tag{6}$$

We recall now the definition 1 in [9] about *good* code, for the sake of clarity and completeness in presentation. A code C of length N is *good* for a wiretap channel with the channel SNRs pair (h, g) if $P_e(h) \leq \epsilon$ (reliability condition) and the secrecy requirement (6) can be achieved (security condition) for all $\epsilon > 0$ and sufficiently large N. According to [9, Definition 2], the secure channel set, for a given pair of rates (R_0, R_s) and a fixed input distribution $p(x)$, is the union of all channel pair (h, g) satisfying:

$$R_0 \leq I(X; Y), \tag{7}$$
$$R_0 - R_s \geq I(X; Z). \tag{8}$$

In [9, Lemma 1] the authors prove also that there exists a Wyner code $C \in \mathcal{C}(N, R_0, R_s)$, generated based on $p(x)$, good for all channel pairs (h, g) belonging to the secure set (7)-(8).

The codebook is revealed to all nodes. We further assume that the coding is random with long codewords and that receivers implement typical-set decoding which allows to find the performance limits for any practical scheme.

III. Incremental redundancy secure HARQ protocols

Consider incremental redundancy secure HARQ as a transmission protocol. Hereafter, we describe this protocol in the case where one-bit feedback is available from the legitimate receiver. The mother code in the INR secure HARQ is a Wyner

[1] In [9], this condition is called "perfect secrecy". However, in this work, we assume that perfect secrecy is restricted to Shannon's definition which requires exact statistical independence between the message and its corresponding codeword.

code of length N. The N-symbols of the codeword are divided into K sub-codewords $\mathbf{x_k}$, $k = 1, .., K$ each one being of length N_k where $N = \sum_{k=1}^{K} N_k$. The ARQ process starts by sending the first sub-codeword $\mathbf{x}_1$ under the channel SNRs pair (h_1, g_1). Decoding of this code is performed at the receiver, while the secrecy level is measured at the eavesdropper. The transmitted N_1 symbols form a codeword of a punctured Wyner code of length N_1 [9]. If a second retransmission is requested by the receiver due to unsuccessful decoding via a NACK feedback message, the second sub-codeword $\mathbf{x}_2$ is sent under possibly different channel conditions (h_2, g_2). Now decoding and equivocation calculation are performed at the receiver and the eavesdropper respectively by combining the previous block $\mathbf{x}_1$ with the new block $\mathbf{x}_2$. The transmitted symbols until the k^{th} transmission form also a codeword of a punctured Wyner code of length $\sum_{i=1}^{k} N_i$. This continues until the maximum number of transmission attempts K is reached or until successful decoding of the message at the legitimate receiver. Thus, the length of the overall transmitted codeword ($\sum_{i=1}^{\mathcal{K}} N_i$, where $\mathcal{K}$ is the last transmission) is not fixed at the transmitter (in general, it is less or equal than N) because it depends on the feedback messages. Figure 2 gives an illustration of the incremental redundancy scheme when the receiver decodes successfully all information bits at the third transmission.

In the system model of [9], the transmitter obtains a 1-bit ACK/NACK feedback from the legitimate receiver to declare successful/unsuccessful decoding via an error free public channel. The authors considered an incremental redundancy scheme based on rate-compatible Wyner secrecy codes, when the K sub-codewords $\mathbf{x_k}$ have the same length. They proved the existence of *good* Wyner code sequences, which ensure reliability and security conditions for an HARQ session under certain channel realizations. In this work, we study the case where the transmitter uses multi-bit feedback channels from both the legitimate receiver and the eavesdropper or from the legitimate receiver only, and which are assumed error free. Based on this, an adaptive scheme is provided in which the transmitter may adapt the sub-codewords $\mathbf{x_k}$ length to the actual situation (Figure 2). On a practical side, we can assume that the sub-codewords corresponding to different messages are gathered in frames that have a fixed number of symbols. This assumption allows to deal with variable-length codewords implementability in TDMA-type communication systems and to compare with the non-adaptive protocol in [9] for the same fading block length (cf. [11, Fig. 1]).

After k transmissions, each receiver applies maximum likelihood decoding based on all received channel observations. The condition of successful decoding at the legitimate receiver after k transmissions is that the average accumulated mutual information is larger than the overall transmission rate. This condition was written for equal length sub-codewords in (7). In our system model where the sub-codewords $\mathbf{x_k}$ may not have the same length, this condition reads:

$$\frac{\sum_{l=1}^{k} C_l^{\mathcal{D}} \cdot N_l}{\sum_{l=1}^{k} N_l} \geq \frac{M_0}{\sum_{l=1}^{k} N_l}, \tag{9}$$

where N_l is the duration of the sub-codeword sent at l^{th} transmission and $C_l^{\mathcal{D}} = I(X;Y|h_l) = \frac{1}{2}\log_2(1+h_l)$ since a Gaussian input alphabet was assumed. For convenience, we normalize the values of N_l using $\rho_l = \frac{N_l}{M_0}$ which is interpreted as the redundancy brought by the l^{th} sub-codeword. Now (9) can be written as follows:

$$I_k^{\mathcal{D}} \stackrel{\triangle}{=} \sum_{l=1}^{k} C_l^{\mathcal{D}} \cdot \rho_l \geq 1. \tag{10}$$

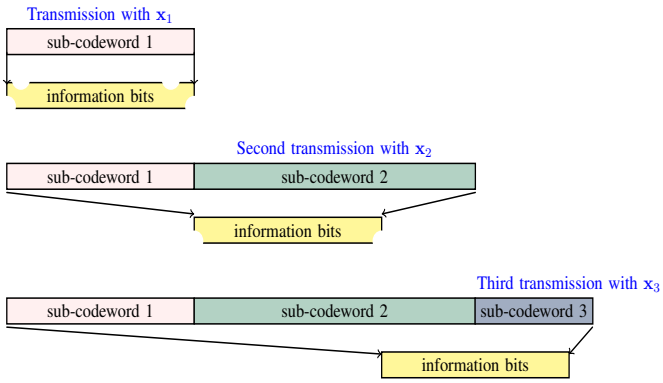

Figure 2. Illustration of the decoding process when the transmitter uses incremental redundancy scheme. Firstly, the transmitter sends "sub-codeword 1" and the legitimate receiver tries to extract the information bits from the received sequence. The distorted yellow rectangle means that legitimate receiver has failed to decode. Then, the legitimate receiver sends a NACK to the transmitter which transmits the "sub-codeword 2". This process continues until a successful decoding by the legitimate receiver or until the maximum number of transmission is reached.

The condition for secrecy at the eavesdropper after k transmissions is that the average accumulated mutual information should be less than the difference between the transmission rate (the main channel code rate) and the secrecy information rate:

$$\frac{\sum_{l=1}^{k} C_l^{\mathcal{E}} \cdot N_l}{\sum_{l=1}^{k} N_l} \leq \frac{M_0 - M_i}{\sum_{l=1}^{k} N_l}, \tag{11}$$

equivalently,

$$I_k^{\mathcal{E}} \stackrel{\triangle}{=} \sum_{l=1}^{k} C_l^{\mathcal{E}} \cdot \rho_l + \gamma \leq 1, \tag{12}$$

where $C_l^{\mathcal{E}} = I(X;Z|g_l) = \frac{1}{2}\log_2(1+g_l)$, and $\gamma = \frac{M_i}{M_0}$. This condition was given in (8) for $K = 1$. In (10) and (12), we observe that $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ increase with k, for some ρ_k and γ, $k = 1, .., K$. This characterizes the existence of a tradeoff between the reliability and secrecy requirements. The conditions (9) and (11) that guarantee the existence of a "good code" can be proven using the results in [9, Theorem 1] and [17, Theorem 4].

We assume that the transmitter uses error-free multi-bit feedback channels either from both the legitimate receiver and the eavesdropper or from the legitimate receiver only, depending on the situation. From (10) and (12) we observe that the *decoding error* events and the *non-security* events in the k-th transmission at the legitimate receiver and the eavesdropper depend on two set of quantities : $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ which can be communicated to the sender via the multi-bit feedback channels and on $C_k^{\mathcal{D}}$ and $C_k^{\mathcal{E}}$ which are unknown

at the transmitter due to the absence of instantaneous CSI. Consequently, $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ are the only parameters which can be used by the transmitter to adapt the redundancy ρ_k via a scalar function.

We consider two cases of redundancy adaptation:

- Case 1: where the legitimate receiver and the eavesdropper send at the k^{th} transmission the values of $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ obtained from the previous transmission $(k-1)$ to the transmitter using multi-bit feedback channels. Thus, $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ are the parameters required to adapt the redundancy ρ_k. We consider the following policy for the transmission attempt k

$$\rho_k = \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}), \quad k = 1, ..., K,$$

where

$$\rho_k = \begin{cases} \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) & \text{if } I_{k-1}^{\mathcal{D}} < 1 \text{ and } I_{k-1}^{\mathcal{E}} \leq 1, \\ \rho_k(I_{k-1}^{\mathcal{D}}) & \text{if } I_{k-1}^{\mathcal{D}} < 1 \text{ and } I_{k-1}^{\mathcal{E}} > 1, \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

The first condition in (13) corresponds to the case where the message is kept secret from eavesdropping but not yet decoded successfully by the legitimate receiver (existence of a connection outage), until the $(k-1)^{\text{th}}$ transmission. The second condition characterizes the existence of a secrecy outage while the legitimate receiver still not capable to decode successfully the message at the $(k-1)^{\text{th}}$ transmission. The last condition corresponds to the end of the transmission due to successful decoding of the intended message by the legitimate receiver.

- Case 2: where only legitimate receiver sends the value of $I_{k-1}^{\mathcal{D}}$ to the transmitter via the feedback channel. In this case, which is more realistic than case 1, ρ_k is adapted using $I_{k-1}^{\mathcal{D}}$ only

$$\rho_k = \begin{cases} \rho_k(I_{k-1}^{\mathcal{D}}) & \text{if } I_{k-1}^{\mathcal{D}} < 1, \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

The first condition in (14) corresponds to the case where the legitimate receiver has not decoded successfully the message at the $(k-1)^{\text{th}}$ transmission, thus the transmitter continues the ARQ transmission process. In the second condition, the transmitter finishes the transmission in the opposite case.

We should note that throughout the manuscript, we may drop the dependence of ρ_k on $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ in case 1 or $I_{k-1}^{\mathcal{D}}$ in case 2, and use only the notation ρ_k. However, it should be kept in mind that the ρ_k are functions of feedback value(s).

The main difference between our work and [9] is that [9] considers the special case where $\rho_k = \rho \; \forall k$, so we refer to the INR secure HARQ studied in [9] as the non-adaptive scheme. The goal now is to find the rate adaptation policies ρ_k, for each possible value of the pair $(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})$ in case 1 and $I_{k-1}^{\mathcal{D}}$ in case 2, and γ which maximize the performance criterion defined in the next section.

IV. Problem Formulation

The secrecy throughput is a relevant performance criterion to evaluate secure HARQ protocols as it can be directly related to the channel secrecy capacity. Based on the renewal-reward theorem [1], [18], the secrecy throughput is defined by the ratio between the number of information bits received reliably by the destination M_i^* and the expected number of channel uses $\overline{N}$ required by the HARQ protocol to deliver the packet in up to K transmission attempts:

$$\eta = \frac{M_i^*}{\overline{N}}.$$

Since the transmitter has no instantaneous channel information, we consider here the outage performance of secure HARQ protocols. Hence, the service quality is acceptable as long as the percentage of information bits not successfully decoded by the legitimate receiver is less than ξ_e and the percentage of information bits successfully decoded by the eavesdropper is less than ξ_s. Thus, we define the connection outage probability f_0 by the probability of decoding failure after K transmissions at the legitimate receiver and the secrecy outage probability f_s by the probability of a successful decoding at the eavesdropper in the last transmission. The outage probabilities are used to characterize the tradeoff between the reliability of the legitimate communication link and the confidentiality with respect to the eavesdropper's link. The optimization problem under consideration is stated below.

Result 1 (Secrecy throughput): The secrecy throughput reads:

$$\eta(\gamma, \rho_1, ..., \rho_K) = \begin{cases} \gamma \cdot \frac{1-f_0}{\sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}}\{\rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})\}} \\ \text{in case 1,} \\ \gamma \cdot \frac{1-f_0}{\sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}}\{\rho_k(I_{k-1}^{\mathcal{D}})\}} \\ \text{in case 2.} \end{cases} \tag{15}$$

Where f_0 depends also on the ρ_k for $k = 1, .., K$.

Proof: We have $M_i^* = M_i \cdot (1 - f_0)$ where f_0 is the connection outage probability.

The expected number of channel uses is given by $\overline{N} = \sum_{k=1}^{K} \overline{N}_k$, where $\overline{N}_k$ is the expected number of channel uses in the k^{th} transmission attempt:

$$\overline{N}_k = \mathbb{E}\{N_k\} = \mathbb{E}\{M_0 \cdot \rho_k\}. \tag{16}$$

Hence,

$$\overline{N}_k = \begin{cases} M_0 \cdot \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}}\{\rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})\} \\ = M_0 \cdot \int_0^1 dx \int_{\gamma}^{\infty} dy \; \rho_k(x,y) \cdot p_{I_{k-1}^{\mathcal{D}} \; I_{k-1}^{\mathcal{E}}}(x,y) \\ \text{in case 1,} \\ M_0 \cdot \mathbb{E}_{I_{k-1}^{\mathcal{D}}}\{\rho_k(I_{k-1}^{\mathcal{D}})\} \\ = M_0 \cdot \int_0^1 dx \cdot \rho_k(x) \cdot p_{I_{k-1}^{\mathcal{D}}}(x) \\ \text{in case 2.} \end{cases}$$

which completes the proof. ■

Result 2 (Connection outage probability): The connection outage probability reads:

$$f_0 = \Pr\{I_K^{\mathcal{D}} < 1\} = \mathbb{E}_{C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}}\{\mathbb{I}(I_K^{\mathcal{D}} < 1)\} \quad (17)$$

$$= \int_0^1 dx \int_\gamma^\infty dy \; p_{I_K^{\mathcal{D}} \; I_K^{\mathcal{E}}}(x,y), \quad (18)$$

where $\mathbb{I}(x) = 1$ if x is true and $\mathbb{I}(x) = 0$ if x is false, $p_{I_K^{\mathcal{D}} \; I_K^{\mathcal{E}}}(x,y)$ is the joint probability density function (pdf) of $I_K^{\mathcal{D}}$ and $I_K^{\mathcal{E}}$ where $I_K^{\mathcal{D}} \in [0,\infty)$ and $I_K^{\mathcal{E}} \in [\gamma,\infty)$.

The secrecy outage probability is given in the result below.

Result 3 (Secrecy outage probability): Let $\mathcal{K}$ denote the random variable of the number of transmissions in an HARQ session (the index of the last transmission). The secrecy outage probability f_s reads:

$$f_s = \sum_{k=1}^{K} \Pr(\mathcal{K}=k) \cdot \Pr(I_k^{\mathcal{E}} > 1), \quad (19)$$

where

$$\Pr(I_k^{\mathcal{E}} > 1) = \mathbb{E}_{C_1^{\mathcal{E}},..,C_k^{\mathcal{E}}}\{\mathbb{I}(I_k^{\mathcal{E}} > 1)\} \quad (20)$$

$$= \int_0^1 dx \int_1^\infty dy \; p_{I_k^{\mathcal{D}} \; I_k^{\mathcal{E}}}(x,y), \quad (21)$$

and where

$$\Pr(\mathcal{K}=k) = \mathbb{E}_{C_1^{\mathcal{D}},..,C_{k-1}^{\mathcal{D}}}\{\mathbb{I}(I_{k-1}^{\mathcal{D}} < 1)\} - \mathbb{E}_{C_1^{\mathcal{D}},..,C_k^{\mathcal{D}}}\{\mathbb{I}(I_k^{\mathcal{D}} < 1)\} \;\; for \;\; k < K, \quad (22)$$

and

$$\Pr(\mathcal{K}=K) = \Pr(I_{K-1}^{\mathcal{D}} < 1) = \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}}\{\mathbb{I}(I_{K-1}^{\mathcal{D}} < 1)\}. \quad (23)$$

Proof: The secrecy outage probability f_s can be expressed as

$$f_s = \Pr(I_{\mathcal{K}}^{\mathcal{E}} > 1) = \sum_{k=1}^{K} \Pr(I_{\mathcal{K}}^{\mathcal{E}} > 1, \mathcal{K}=k),$$

leading to

$$f_s = \sum_{k=1}^{K} \Pr(\mathcal{K}=k) \cdot \Pr(I_k^{\mathcal{E}} > 1).$$

The event $\{\mathcal{K}=k\}$, i.e. the last transmission number is k, happens when the last transmission in which the legitimate receiver has decoded successfully the message is the k^{th} transmission, for $k < K$. However, the event $\{\mathcal{K}=K\}$ happens when the legitimate receiver has not decoded yet the message at the $(k-1)^{\text{th}}$ transmission indifferently if the decoding is successful or not at the k^{th} transmission because the maximum number of transmission is achieved. Thus, the probability mass function of $\mathcal{K}$ can be expressed as [9]: $\Pr(\mathcal{K}=k) = \Pr(I_{k-1}^{\mathcal{D}} < 1, I_k^{\mathcal{D}} \geq 1) = \Pr(I_{k-1}^{\mathcal{D}} < 1) - \Pr(I_k^{\mathcal{D}} < 1) = \mathbb{E}_{C_1^{\mathcal{D}},..,C_{k-1}^{\mathcal{D}}}\{\mathbb{I}(I_{k-1}^{\mathcal{D}} < 1)\} - \mathbb{E}_{C_1^{\mathcal{D}},..,C_k^{\mathcal{D}}}\{\mathbb{I}(I_k^{\mathcal{D}} < 1)\}$ for $k < K$ and $\Pr(\mathcal{K}=K) = \Pr(I_{K-1}^{\mathcal{D}} < 1) = \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}}\{\mathbb{I}(I_{K-1}^{\mathcal{D}} < 1)\}$. ■

The secrecy throughput in (15) depends on the channel model and on the coding and decoding scheme. Here, we assume that the coding and decoding scheme is capacity-achieving as in [1] and as a result, we provide the performance limits for any practical scheme. The secrecy throughput optimization problem under outages constraints reads:

$$\max_{\gamma,\rho_1,...,\rho_K} \quad \eta(\gamma,\rho_1,...,\rho_K)$$
$$s.t. \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases} \quad (24)$$

where ξ_ϵ and ξ_s are the target outage probabilities and where the expression of $\eta(\gamma,\rho_1,...,\rho_K)$, f_0 and f_s are given in results 1 to 3.

V. Constrained secrecy throughput optimization using dynamic programming

The design of the adaptive incremental redundancy HARQ scheme consists in finding the rate adaptation policies ρ_k, $k = 1,...,K$ and γ which maximize the secrecy throughput under constraints on outage probabilities. Based on channel statistics, we can obtain the code parameters that achieve the maximum secrecy throughput while satisfying the outage constraints.

Obviously, solving the multidimensional problem (24) using exhaustive search over all optimization variables would be unmanageable. Therefore, we separate the problem as an exhaustive search to optimize γ. Thus, we solved problem (24) for many different values of $\gamma \in [0,1]$, and for each of these $\gamma \in [0,1]$, we maximize the secrecy throughput subject to ρ_k only. The optimization problem can now be written as

$$\max_{\rho_1,...,\rho_K} \quad \eta(\gamma;\rho_1,...,\rho_K)$$
$$s.t. \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases} \quad (25)$$

Note that f_0 and f_s depend on the ρ_k for $k = 1,..,K$. We will describe later how to make the choice of γ in the simulations. Assume now that γ is fixed to an arbitrary value in $[0,1]$. In the following, we propose an algorithm to solve (25) using the "dynamic programming" approach for the two cases under study. The proposed solution is not guaranteed to be a global optimum but can bring, as shown later, significant improvements in secrecy throughput with respect to that proposed in [9].

A. Constrained secrecy throughput optimization for a fixed γ in case 1

Recall that in case 1, the transmitter uses feedback channels from both legitimate receiver and eavesdropper i.e. $\rho_k = \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})$, $k = 1,..,K$. The optimization procedure is described below. This is an off-line procedure intended to compute the optimal values of ρ_k for any values of feedback channels, $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$. The optimization is based on dynamic programming. A similar method was used in [11] for a point-to-point communication system without eavesdropper. We provide here an extension in the context of secure communications. Let $\mathcal{R} = \{\rho\}$ denote the set of all adaptation policies functions with $\rho = (\rho_1,..,\rho_K)$. Also define as $\mathcal{R}_{\xi_\epsilon,\xi_s} = \{\rho : f_0(\rho) = \xi_\epsilon, f_s(\rho) = \xi_s\}$ the set of all adaptation policies leading to a connection outage $f_0(\rho) = \xi_\epsilon$ and a

secrecy outage $f_s(\rho) = \xi_s$. Consequently, the optimization problem in (25) can be written as:

$$\hat{\eta} = \max_{\xi_\epsilon^* \le \xi_\epsilon, \xi_s^* \le \xi_s} \max_{\rho \in \mathcal{R}_{\xi_\epsilon^*, \xi_s^*}} \gamma \cdot \frac{1-\xi_\epsilon^*}{D(\rho)} \tag{26}$$

$$= \max_{\xi_\epsilon^* \le \xi_\epsilon, \xi_s^* \le \xi_s} \gamma \cdot \frac{1-\xi_\epsilon^*}{\min_{\rho \in \mathcal{R}_{\xi_\epsilon^*, \xi_s^*}} D(\rho)} \tag{27}$$

$$= \max_{\xi_\epsilon^* \le \xi_\epsilon, \xi_s^* \le \xi_s} \gamma \cdot \frac{1-\xi_\epsilon^*}{U(\xi_\epsilon^*, \xi_s^*)} \tag{28}$$

where ξ_ϵ and ξ_s are the target outage probabilities, $D(\rho) = \sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}} \Big\{ \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \Big\}$ is the denominator in the throughput expression (15), and $U(\xi_\epsilon^*, \xi_s^*)$ is given by:

$$U(\xi_\epsilon, \xi_s) = \min_{\rho \in \mathcal{R}} D(\rho) \quad \text{s.t.} \quad f_0(\rho) = \xi_\epsilon \quad \text{and} \quad f_s(\rho) = \xi_s. \tag{29}$$

The design of adaptation policies requires solving the auxiliary optimization problem in (29). Then, we form a dual problem using Lagrangian multipliers λ_1 and λ_2 for the constraints on f_0 and f_s:

$$J^{\lambda_1,\lambda_2} = \min_{\rho \in \mathcal{R}} \quad D(\rho) + \lambda_1 \cdot \big(f_0(\rho) - \xi_\epsilon\big) + \lambda_2 \cdot \big(f_s(\rho) - \xi_s\big). \tag{30}$$

The notation J^{λ_1,λ_2} means that the solution depends on the choice of λ_1 and λ_2.

We are interested in evaluating $U(\xi_\epsilon, \xi_s)$ for many values of ξ_ϵ and ξ_s. Since for each couple of λ_1 and λ_2 corresponds a connection outage f_0 and a secrecy outage f_s, we can solve (30) for different λ_1 and λ_2. Thus, to solve (15) we employ auxiliaries weighting multipliers λ_1 and λ_2 and try to minimize the denominator of (15), f_0 and f_s at the same time as:

$$J^{\lambda_1,\lambda_2} = \min_{\rho_1,...,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}} \Big\{ \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \Big\} + \lambda_1 \cdot f_0(\rho_1, ..., \rho_K) + \lambda_2 \cdot f_s(\rho_1, ..., \rho_K). \tag{31}$$

The terms $\lambda_1 \cdot \xi_\epsilon$ and $\lambda_2 \cdot \xi_s$ are removed since they are irrelevant to the optimization.

Since the convexity of the optimization problem is unknown, we solve problem (31) for multiple initialization of (λ_1, λ_2), to increase the probability of falling into a global optimum. Then we obtain a set of λ_1 and λ_2 values associated with the corresponding throughput $\eta^{*\lambda_1,\lambda_2}$, and the corresponding outage probabilities $f_0^{\lambda_1,\lambda_2}$ and $f_s^{\lambda_1,\lambda_2}$. From this set, we choose λ_1 and λ_2 which maximize η while satisfying the outage probabilities constraints in order to solve (26). In experiments, a gradient-search method is used in order to update alternately λ_1 and λ_2. Because we don't know about the convexity of the optimization problem in (31), we solve it many times with different initialization of λ_1 and λ_2. Now, we explain the method for solving (31) for a *fixed* couple of (λ_1, λ_2) and how to calculate the corresponding secrecy throughput and outage probabilities. We can observe that the values of $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ at time k can be written as follows

$$I_k^{\mathcal{D}} = I_{k-1}^{\mathcal{D}} + C_k^{\mathcal{D}} \cdot \rho_k, \tag{32}$$

$$I_k^{\mathcal{E}} = I_{k-1}^{\mathcal{E}} + C_k^{\mathcal{E}} \cdot \rho_k, \tag{33}$$

where $I_0^{\mathcal{D}} = 0$ and $I_0^{\mathcal{E}} = \gamma$. This is the key point for writing recursively the objective function in (31).

Result 4 (Dynamic programming formulation): The optimization problem in (31) is reduced to $(K-1) \cdot L_1 \cdot L_2 + 1$ one dimensional optimization sub-problems. The optimal rate-adaptation policies associated with the given λ_1, λ_2 and γ are obtained as solution of

$$J_K^{\lambda_1,\lambda_2}(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}}) = \min_{\rho_K} \ \rho_K + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_{K-1}^{\mathcal{E}}}{\rho_K} \right) \right\} \right] + \lambda_1 \cdot F_{C^{\mathcal{D}}} \left(\frac{1 - I_{K-1}^{\mathcal{D}}}{\rho_K} \right), \tag{34}$$

$$J_k^{\lambda_1,\lambda_2}(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) = \min_{\rho_k} \ \rho_k + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{D}}} \left(\frac{1 - I_{k-1}^{\mathcal{D}}}{\rho_k} \right) \right\} \cdot \left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_{k-1}^{\mathcal{E}}}{\rho_k} \right) \right\} \right] + \mathbb{E}_{C_k^{\mathcal{D}}, C_k^{\mathcal{E}}} \left\{ J_{k+1}^{\lambda_1,\lambda_2}(I_{k-1}^{\mathcal{D}} + C_k^{\mathcal{D}} \cdot \rho_k, I_{k-1}^{\mathcal{E}} + C_k^{\mathcal{E}} \cdot \rho_k) \right\}, \quad \text{for } k < K. \tag{35}$$

where $F_{C^{\mathcal{D}}}$ and $F_{C^{\mathcal{E}}}$ are the cumulative density functions of $C^{\mathcal{D}}$ and $C^{\mathcal{E}}$ respectively.

Proof: See the Appendix. ∎

The recursive nature of the above equations is characteristic of the dynamic programming (DP). Now, to solve (34)–(35) for given λ_1 and λ_2, we start from the last problem $J_K^{\lambda_1,\lambda_2}$, where we should obtain the value of ρ_K that minimize $J_K^{\lambda_1,\lambda_2}$ for all values of $I_{K-1}^{\mathcal{D}}$ and $I_{K-1}^{\mathcal{E}}$. According to (13), we must be interested in the values of $I_{K-1}^{\mathcal{D}}$ and $I_{K-1}^{\mathcal{E}}$ in the intervals $T = [0, 1)$ and $S = [\gamma, 1]$ respectively. Thus $I_{K-1}^{\mathcal{D}}$ and $I_{K-1}^{\mathcal{E}}$ have to be discretized to L_1 and L_2 points over T and S respectively. Hence, $\rho_K(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}})$ is $L_1 \times L_2$ matrix. To solve (48), we should solve $L_1 \cdot L_2$ one-dimensional problems where the only variable is ρ_K. In (48), and for fixed $(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}})$, we know that (i) $\mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) = 1$ since $I_{K-1}^{\mathcal{D}} \in T$, (ii) $\mathbb{E}_{C_K^{\mathcal{E}}} \big\{ \mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K > 1) \big\} = 1 - F_{C^{\mathcal{E}}} \big(\frac{1 - I_{K-1}^{\mathcal{E}}}{\rho_K} \big)$ and (iii) $\mathbb{E}_{C_K^{\mathcal{D}}} \big\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1) \big\} = F_{C^{\mathcal{D}}} \big(\frac{1 - I_{K-1}^{\mathcal{D}}}{\rho_K} \big)$, where F_{C^i} is the cumulative density function of C^i, $i \in \{\mathcal{D}, \mathcal{E}\}$, calculated using (3) and (4). By putting these expressions into (45)-(48) leads to (34)-(35). The problem should be solved starting from step K and going recursively up to $k = 1$ to find all the policies ρ_k $\big($which are $L_1 \times L_2$ matrices, except ρ_1 which has one element according to (32) and (33)$\big)$.

Since we need to calculate the outage probabilities f_0 and f_s in order to update the Lagrangian multiplier, we should calculate the joint probability distributions of $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ for $k = 1, .., K$ and then use them in (18) and (19).

For each set of policies, we can find the joint probability distribution of $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ starting from $k = 1$ and going recursively up to $k = K$. Due to the independence of channels,

for $k=1$ the joint cumulative density function of $I_1^{\mathcal{D}}, I_1^{\mathcal{E}}$ is

$$F_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x,y) = \Pr\left(\rho_1 \cdot C_1^{\mathcal{D}} < x, \gamma + \rho_1 \cdot C_1^{\mathcal{E}} < y\right) = F_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right) \cdot F_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right),$$

which differentiated yields the joint pdf

$$p_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x,y) = \frac{1}{\rho_1} \cdot p_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right) \cdot \frac{1}{\rho_1} \cdot p_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right), \quad (36)$$

where $p_{C^{\mathcal{D}}}$ and $p_{C^{\mathcal{E}}}$ are the probability density functions of the i.i.d random variables $C_1^{\mathcal{D}}, .., C_K^{\mathcal{D}}$ and $C_1^{\mathcal{E}}, .., C_K^{\mathcal{E}}$ respectively.

For $k > 1$, the joint cumulative density function is calculated recursively:

$$F_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = \Pr\left(I_{k-1}^{\mathcal{D}} + \rho_k \cdot C_k^{\mathcal{D}} < x, I_{k-1}^{\mathcal{E}} + \rho_k \cdot C_k^{\mathcal{E}} < y\right)$$

$$= \int_0^x \int_\gamma^y \Pr\left(I_{k-1}^{\mathcal{D}} + \rho_k \cdot C_k^{\mathcal{D}} < x, I_{k-1}^{\mathcal{E}} + \rho_k \cdot C_k^{\mathcal{E}} < y \middle| I_{k-1}^{\mathcal{D}} = \alpha, I_{k-1}^{\mathcal{E}} = \beta\right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\, d\alpha\, d\beta$$

$$= \int_0^x \int_\gamma^y F_{C^{\mathcal{D}}}\left(\frac{x-\alpha}{\rho_k(\alpha,\beta)}\right) \cdot F_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)}\right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\, d\alpha\, d\beta$$

thus the joint pdf obtained by differentiating the joint cumulative density function can be calculated recursively using $p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(x,y)$:

$$p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = \int_0^x \int_\gamma^y \frac{1}{\rho_k(\alpha,\beta)} \cdot p_{C^{\mathcal{D}}}\left(\frac{x-\alpha}{\rho_k(\alpha,\beta)}\right) \cdot \frac{1}{\rho_k(\alpha,\beta)} \cdot p_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)}\right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\, d\alpha\, d\beta. \quad (37)$$

In the case where $\rho_k(x,y) = 0$ we have $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(x,y)$. All the integrals are approximated using the rectangular method.

For each fixed λ_1 and λ_2, we can calculate the secrecy throughput (15) using $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y)$ and $\rho_k(x,y)$ for $k = 1, ..., K$. The algorithm is summarized in Table I. We recall that this throughput is obtained for an arbitrary fixed $\gamma \in [0,1]$. Now we discuss the choice of γ. In the simulations, we observe that the secrecy throughput increases when γ increases. However, when γ is greater than a certain value between 0 and 1, it is impossible to obtain outage probabilities less than target probabilities regardless of λ_1 and λ_2 values. Thus the best choice γ^* is the maximum value of γ which can verify outage probabilities constraints.

B. Constrained secrecy throughput optimization in case 2

We study here case 2 where the transmitter obtains no feedback from the eavesdropper but only from legitimate receiver. Consequently, $I_{k-1}^{\mathcal{D}}$ is the only parameter used by the transmitter to adapt the redundancy ρ_k. As in case 1, γ is fixed and the secrecy throughput η is maximized by minimizing the denominator of (15), f_0 and f_s at the same time. Exhaustive search method is used to optimize γ as in case 1.

The optimization problem for a fixed γ can be written as follows:

$$L^{\lambda_1,\lambda_2} = \min_{\rho_1,\ldots,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}}\left\{\rho_k(I_{k-1}^{\mathcal{D}})\right\} + \lambda_1 \cdot f_0 + \lambda_2 \cdot f_s \quad (38)$$

$$= \min_{\rho_1,\ldots,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}}\left\{\rho_k(I_{k-1}^{\mathcal{D}})\right\} + \lambda_1 \cdot \mathbb{E}_{I_K^{\mathcal{D}}}\left[\mathbb{I}\left(I_K^{\mathcal{D}} < 1\right)\right] + \lambda_2 \cdot \sum_{k=1}^{K-1} \mathbb{E}_{I_k^{\mathcal{D}}}\left[\mathbb{I}\left(I_{k-1}^{\mathcal{D}} < 1\right) - \mathbb{I}\left(I_k^{\mathcal{D}} < 1\right)\right] \cdot \Pr\left(I_k^{\mathcal{E}} > 1\right) + \lambda_2 \cdot \mathbb{E}_{I_{K-1}^{\mathcal{D}}}\left[\mathbb{I}\left(I_{K-1}^{\mathcal{D}} < 1\right)\right] \cdot \Pr\left(I_K^{\mathcal{E}} > 1\right). \quad (39)$$

In case 1, solving the optimization problem was equivalent, for a fixed γ, λ_1 and λ_2, to solve (34) and (35) for $k = 1, .., K$. All optimization problems in (34), (35) are done off-line for all the values of $I_{k-1}^{\mathcal{E}}$. Thus in this case, the output of the problems (34), (35), i.e., the ρ_k will depend also on the value of $I_{k-1}^{\mathcal{E}}$. Then to calculate the secrecy outage probability, we have derived the joint pdf $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}$, for $k = 1, .., K$, and we have used them in (18) and (19). However, in case 2, we cannot use $I_{k-1}^{\mathcal{E}}$ as a state in a dynamic programming method as in case 1, since ρ_k depends only on $I_{k-1}^{\mathcal{D}}$. Thus to solve problem (39), we should obtain the pdf $\bar{z}_k$ of $I_k^{\mathcal{E}}$, as a function of optimization variables, to evaluate $f_{sk} = \Pr(I_k^{\mathcal{E}} > 1)$ in equation (19) and to use it in (39), where $I_k^{\mathcal{E}} = \sum_{l=1}^{k} C_l^{\mathcal{E}} \cdot \rho_l + \gamma$. The pdf $\bar{z}_k$ can be expressed as

$$\bar{z}_k(x) = z_1(x) * ... * z_k(x) \quad (40)$$

$$= \bar{z}_{k-1}(x) * z_k(x), \quad (41)$$

where $*$ is the convolution operator and z_l are the pdf of random variables $R_l = C_l^{\mathcal{E}} \cdot \rho_l$. However, using the exact expression of the pdf $\bar{z}_k$ makes the problem intractable by dynamic programming method, since if we consider $\bar{z}_{k-1}$ as a second state, we need to solve the sub-optimization problems for all the values of the state $\bar{z}_{k-1}$ which vary between 0 and ∞ (see eg. [11]). To make the optimization problem tractable, an approximation of the i.i.d. random variables R_l by Gaussian variables can be used as in [19], [11]. However, using Gaussian approximation requires to solve a dynamic programming optimization problem with three-dimensional state which is time consuming. We propose here an alternative which consists in using the results obtained in the previous section for case 1. Thus to solve problem (39), we use as an intermediate step the expressions of ρ_k obtained for case 1 when ρ_k is a function of $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$, for fixed λ_1 and λ_2.

Table I
THE ALGORITHM USED TO SOLVE (31) FOR A FIXED $\gamma \in [0,1]$.

Step 0	$\lambda_1 \leftarrow \lambda_1^{(0)}$, $\lambda_2 \leftarrow \lambda_2^{(0)}$
Step ℓ	0. Set $\lambda_1 \leftarrow \lambda_1^{(\ell-1)}$ and $\lambda_2 \leftarrow \lambda_2^{(\ell-1)}$ 1. Solve $J^{\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)}}$ in (31) to obtain ρ_k for $k=1,..,K$: 1.1. Start with $k=K$, find the 2-D function $\rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})$: for $i^{\mathcal{D}} = 0:\Delta_i:1$ for $i^{\mathcal{E}} = \gamma:\Delta_i:1$ Solve (34) with $I_{k-1}^{\mathcal{D}} = i^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}} = i^{\mathcal{E}}$ end for end for 1.2. Go recursively back and solve (35) for $k = K-1,..,2$ using the off-line procedure in 1.1. 1.3. For $k=1$ solve (35) only with $I_{k-1}^{\mathcal{D}} = 0$ and $I_{k-1}^{\mathcal{E}} = \gamma$, then obtain ρ_1 2. Calculate the joint pdf of $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ for $k=1,..,K$ using (36), (37) and the ρ_k obtained in 1. 2.1. Start with $k=1$, find $p_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x,y)$ using (36) as follows: for $i^{\mathcal{D}} = 0:\Delta_i:i_m^{\mathcal{D}}$ for $i^{\mathcal{E}} = \gamma:\Delta_i:i_m^{\mathcal{E}}$ Calculate $p_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(i^{\mathcal{D}}, i^{\mathcal{E}})$ using (36) where $i_m^{\mathcal{D}}$ and $i_m^{\mathcal{E}}$ are fixed in simulations such that $p_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x,y)$ is negligible for $x > i_m^{\mathcal{D}}$ or $y > i_m^{\mathcal{E}}$ end for end for 2.2. Calculate the joint pdf of $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ for $k=2,..,K$ using (37) and the same method in 2.1. 3. Using the joint pdf in 2., calculate the connection outage probability $f_0^{(\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)})}$ using (18). 4. Update λ_1: $\lambda_1^{(\ell)} = [\lambda_1^{(\ell-1)} + \beta(f_0^{(\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)})} - \xi_\epsilon)]^+$ where $[.]^+ = \max(.,0)$ 5. Repeat steps 1. and 2. with $\lambda_1 \leftarrow \lambda_1^{(\ell)}$, $\lambda_2 \leftarrow \lambda_2^{(\ell-1)}$ 6. Calculate the outage $f_s^{(\lambda_1^{(\ell)},\lambda_2^{(\ell-1)})}$ using (19). 7. Update λ_2: $\lambda_2^{(\ell)} = [\lambda_2^{(\ell-1)} + \beta(f_s^{(\lambda_1^{(\ell)},\lambda_2^{(\ell-1)})} - \xi_s)]^+$
Stopping criterion	$\lvert\lambda_1^{(\ell)} - \lambda_1^{(\ell-1)}\rvert \le \epsilon_1$ $\lvert\lambda_2^{(\ell)} - \lambda_2^{(\ell-1)}\rvert \le \epsilon_2$ β, ϵ_1 and ϵ_2 are chosen in experiments to be sufficiently small.

Since in case 2, ρ_k is a function of $I_{k-1}^{\mathcal{D}}$ only, we propose to marginalize ρ_k w.r.t. $I_{k-1}^{\mathcal{E}}$ as the following

$$\rho_k(I_{k-1}^{\mathcal{D}}) = \int_{\gamma}^{\infty} \rho_k(I_{k-1}^{\mathcal{D}}, x) \cdot \frac{p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(I_{k-1}^{\mathcal{D}}, x)}{\int_{\gamma}^{\infty} p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(I_{k-1}^{\mathcal{D}}, y) dy} \cdot dx, \tag{42}$$

for $k=1,..,K$, where $p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}$ are the joint pdf calculated in case 1. The joint pdf $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}$ must be calculated again for $k=1,..,K$, using $\rho_k = \rho_k(I_{k-1}^{\mathcal{D}})$ in (42).

The solution in (42) provides a less computational demanding method to obtain ρ_k as a function of $I_{k-1}^{\mathcal{D}}$ only.

VI. NUMERICAL APPLICATION

In this section we provide numerical examples for the secrecy throughput maximization problem under outage constraints in the two considered cases of rate adaptation.

Figure 3, depicts the secrecy throughput η as a function of the maximum number of transmissions K using the "non-adaptive scheme" described in [9] (see Fig.7 in [9]) and the two adaptive INR schemes described in this paper. The parameter settings are as follows: $\overline{h} = 15$ dB, $\overline{g} = 5$ dB, $\xi_\epsilon = 10^{-3}$ and $\xi_s = 10^{-3}$.

As explained above, there is an intrinsic tradeoff between the throughput to the destination and the information leakage to the eavesdropper: larger sub-codewords increase the throughput, but also reduce the level of secrecy, since the eavesdropper can obtain more information from the received signal. Therefore, the result of the optimization can be fully evaluated by looking at the secrecy throughput vs K, the sub-codewords lengths being (hidden) optimization parameters. The results show that a notable gain is obtained using the rate-adaptive schemes (cases 1 and 2) when $K > 3$. However, when K is small, e.g. for $K = 1$ or 3, the secrecy throughput η is still negligible using adaptive schemes due to insufficient diversity. The secrecy throughput converges when $K \to \infty$ to the ergodic value $\eta^* = \mathbb{E}\big[C(H) - C(G)\big] = 1.31$ where $C(x) = \frac{1}{2} \cdot \log_2(1+x)$ and the distributions of H and G are given in (3) and (4). For $K = 11$, the case 1 of rate adaptation achieves 48% of η^* while the non-adaptive scheme achieves only 32%. We observe in Figure 3, that the gain case 2 (more realistic since only a feedback from legitimate receiver is considered) has a performance in terms of secrecy rate which is very close to that of case 1 (not very realistic, since it requires cooperation from the eavesdropper). This is clearly due to the fact that the eavesdropper has a somewhat poor channel, which does not allow him to understand much of the transmitted signal.

Now, consider another average SNRs setting as follows: $\bar{h} = 10$ dB and $\bar{g} = 5$ dB. In this case, when $K \to \infty$ the secrecy throughput approaches the ergodic secrecy capacity which is equal to $\eta^* = 0.59$. Obviously, decreasing the gap between

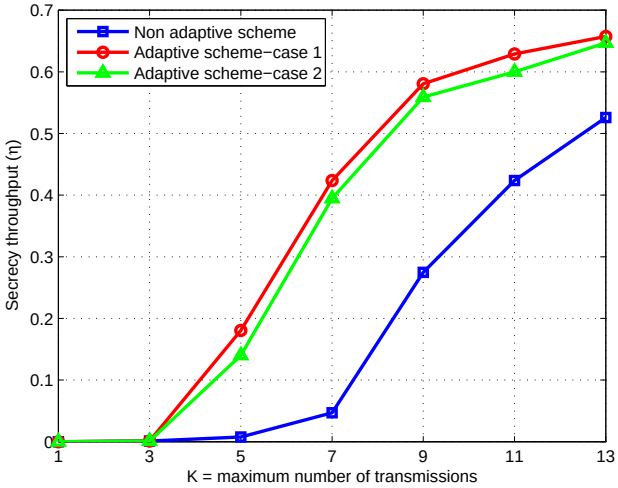

Figure 3. Secrecy throughput η versus the maximum number of transmissions K. $\xi_\epsilon = \xi_s = 10^{-3}$, $(\bar{h}, \bar{g}) = (15, 5)$ dB.

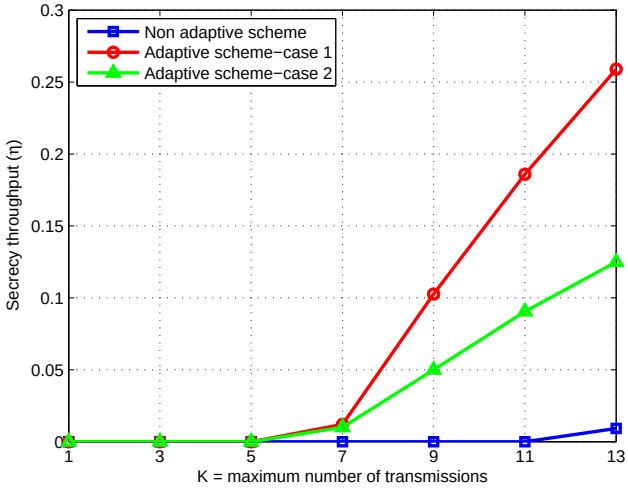

Figure 4. Secrecy throughput η vs the maximum number of transmissions K. $\xi_\epsilon = \xi_s = 10^{-2}$, $(\bar{h}, \bar{g}) = (10, 5)$ dB.

average SNRs will decrease the ergodic secrecy capacity. In experiments, we first considered the same target outage probabilities as in the previous example $\xi_s = \xi_\epsilon = 10^{-3}$ and we tested all the values of $K \in \{3, 5, 7, 9\}$. However, for all these values of K we obtained null secrecy throughput in case 1 of rate adaptation due to the bad channel conditions: the channel statistics never allows to reach this level of secrecy outage. Thus we have studied the secrecy throughput for greater outage probabilities when $\xi_s = \xi_\epsilon = 10^{-2}$. Figure 4, shows the maximal secrecy throughput versus K in this case study. We observe that in this example, the gap in secrecy throughput between case 1 and case 2 is noticeable. This is because, when we have the advantage of a feedback channel from the eavesdropper, bad channel conditions can be compensated by knowing about the situation at the eavesdropper. When $K = 13$, case 1 can achieve 43.5% of η^*, versus only 21% in case 2. Figure 4 shows also that the first non-null secrecy throughput η when $\xi_s = \xi_\epsilon = 10^{-2}$ for the non-adaptive scheme is obtained when $K = 13$, i.e. we need 6 more transmissions to achieves a non-null η compared to adaptive schemes.

As a result, one can conclude that using multi-bit feedback channels by the transmitter to adapt the redundancy at each transmission is very advantageous compared to the non-adaptive scheme with ACK/NACK feedback channel.

We recall that the secrecy throughput is maximized w.r.t. ρ_k for $k = 1, .., K$ and the ratio of secret bits transmitted γ. The values of γ, obtained from the algorithm proposed in Table I to solve problem (25), are given in Figure 5 as a (increasing) function of the maximum number of transmissions K. We observe that the secrecy throughput is increasing with γ. Indeed, when K is small, the reliability condition in (10) will impose the transmitter to provide sufficient redundancy from the first transmissions which leads to small possible values of γ in order to achieve the secrecy condition in (12). We observe also that for a fixed K, the largest value of γ is obtained for the adaptive scheme in case 1, due to the presence of two feedback

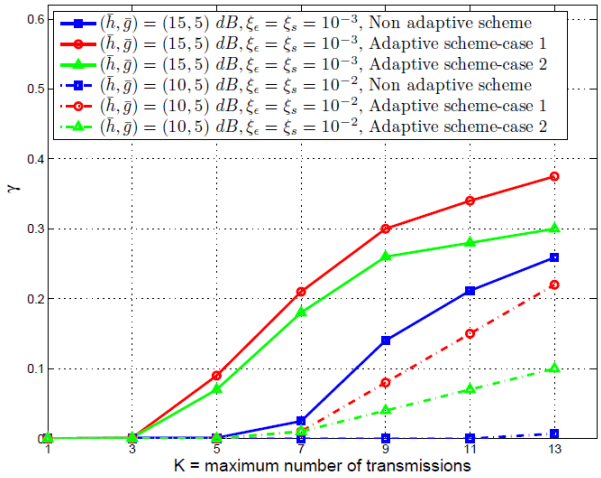

Figure 5. The values of $\gamma = \frac{R_s}{R_0}$ outputted by the proposed algorithm versus the maximum number of transmissions K.

channels from legitimate receiver and eavesdropper. Since in case 2, there is a lack of information from eavesdropper side, the transmitter needs to add more dummy bits in order to ensure secrecy which leads to smaller γ than case 1. In the non-adaptive scheme, there is also no information about (outdated) CSI from the legitimate receiver; so, according to (10) the transmitter needs to add more redundancy comparing to case 2 in order to assure reliable transmission (remember that in the non-adaptive scheme $\rho_k = \rho$, $\forall k$ in (10)). Thus the maximal possible value of γ to achieve a secure communication will decrease according to (12) w.r.t case 2.

The size of the sub-codewords can be determined using the values of ρ_k , $k = 1, .., K$, and γ obtained from the proposed algorithm as well as the feedback value(s). Indeed, we have $\rho_k = \frac{N_k}{M_0}$, where $M_0 = M_i + M_d$, M_i is the number of information bits which is known at the transmitter and M_d is the number of dummy bits which can be obtained using the value of γ (i.e., $\gamma = \frac{M_i}{M_i + M_d}$). Then, the size of the sub-

codewords for the k^{th} transmission is equal to $N_k = \rho_k M_0$.

In Figures 6–9, we show, as example, the adaptation policies ρ_k in case 1 obtained using the proposed algorithm in Table I, for the transmission $k = 2, 3, 4, 5$ respectively when $K = 5$, $\gamma = 0.09$, $(\bar{h}, \bar{g}) = (15, 5)$ dB and $\xi_s = \xi_\epsilon = 10^{-3}$. For $k = 1$, the rate adaptation solution is equal to $\rho_1 = 0.2$. The ρ_k are two dimensional functions of $I^{\mathcal{D}}_{k-1}$ and $I^{\mathcal{E}}_{k-1}$ when $k > 1$ in case 1. We recall that when $I^{\mathcal{D}}_{k-1} \geq 1$, $\rho_k = 0$ and when $I^{\mathcal{E}}_{k-1} \geq 1$, $\rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}) = \rho_k(I^{\mathcal{D}}_{k-1}, 1)$. An another example is shown in Figure 10, for the rate adaptation solution ρ_k in case 2, for each $k = 1, .., 5$ when $K = 5$, $\gamma = 0.07$, $(\bar{h}, \bar{g}) = (15, 5)$ dB and $\xi_s = \xi_\epsilon = 10^{-3}$. Obviously, we observe in Figures 6–10, that when the amount of accumulated information at the legitimate receiver $(I^{\mathcal{D}}_{k-1})$ is small, the transmitter would have to use long sub-codewords to ensure a successful decoding of the information message. We note that in case 2, the rate adaptation solution obtained in experiments require for some considered values of K, what is called "packet-dropping" in [11]: knowing in the k^{th} transmission that the accumulated mutual information $I^{\mathcal{D}}_{k-1}$ at the legitimate receiver is below a threshold I_{th} the transmitter terminates the HARQ process, i.e. $\rho_k(I^{\mathcal{D}}_{k-1}) = 0$, when $I^{\mathcal{D}}_{k-1} < I_{th}$.

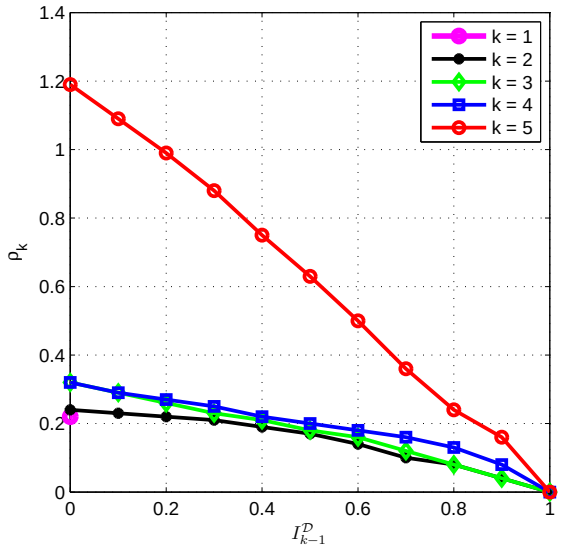

Figure 10. $\rho_k(I^{\mathcal{D}}_{k-1})$ in case 2 when $\gamma = 0.07$, $K = 5$, $(\bar{h}, \bar{g}) = (15, 5)$ dB, $\xi_s = \xi_\epsilon = 10^{-3}$.

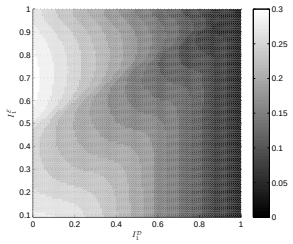

Figure 6. $\rho_2(I^{\mathcal{D}}_1, I^{\mathcal{E}}_1)$ in case 1 when $\gamma = 0.09$, $K = 5$, $(\bar{h}, \bar{g}) = (15, 5)$ dB, $\xi_s = \xi_\epsilon = 10^{-3}$.

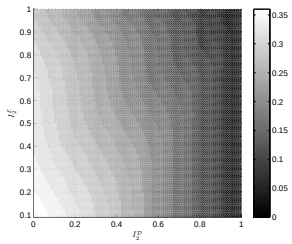

Figure 7. $\rho_3(I^{\mathcal{D}}_2, I^{\mathcal{E}}_2)$ in case 1 when $\gamma = 0.09$, $K = 5$, $(\bar{h}, \bar{g}) = (15, 5)$ dB, $\xi_s = \xi_\epsilon = 10^{-3}$.

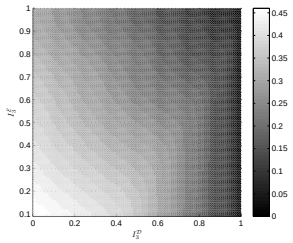

Figure 8. $\rho_4(I^{\mathcal{D}}_3, I^{\mathcal{E}}_3)$ in case 1 when $\gamma = 0.09$, $K = 5$, $(\bar{h}, \bar{g}) = (15, 5)$ dB, $\xi_s = \xi_\epsilon = 10^{-3}$.

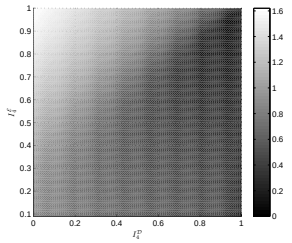

Figure 9. $\rho_5(I^{\mathcal{D}}_4, I^{\mathcal{E}}_4)$ in case 1 when $\gamma = 0.09$, $K = 5$, $(\bar{h}, \bar{g}) = (15, 5)$ dB, $\xi_s = \xi_\epsilon = 10^{-3}$.

VII. Conclusion and Perspectives

This paper addresses the reliable and secure communication over block-fading wiretap channel based on incremental redundancy secure HARQ protocol. The transmitter has no instantaneous CSI but knows channel statistics. We have studied two cases of secure HARQ protocols. In the first case, the transmitter can receive information from both legitimate receiver and eavesdropper via multi-bit feedback channels while in the second case there is sole feedback from legitimate receiver, which is much more realistic. We analyzed rate adaptation for both cases using outdated CSI and we used dynamic programming method to solve the secrecy throughput optimization problem under outage constraints. We have shown via examples that multi-bit feedback combined with rate adaptation can bring noticeable improvements in terms of secrecy throughput compared to the non-adaptive scheme in [9]. We have also observed that the gap between the secrecy throughput in the case 1 and the case 2 depends on channel conditions and the maximum number of transmission K, and can be quite small.

An extension of this work could be also to optimize the number of additional dummy bits (or γ) in each transmission, while it is here optimized for the whole transmission; this can improve the secrecy throughput as shown in [17]. Another extension to increase applicability of the results would be to consider finite input alphabets, since a Gaussian alphabet which was considered in this paper is not implementable in practice.

Appendix
Proof of Result 4

By using the dependencies of $I^{\mathcal{D}}_k$ and $I^{\mathcal{E}}_k$ on $C^{\mathcal{D}}_1, .., C^{\mathcal{D}}_k$ and $C^{\mathcal{E}}_1, .., C^{\mathcal{E}}_k$ respectively, and using (18) and (19) we can write

(31) as follows:

$$
\begin{aligned}
&J^{\lambda_1,\lambda_2} = \\
&\min_{\rho_1,\ldots,\rho_K} \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}},C_1^{\mathcal{E}},..,C_{K-1}^{\mathcal{E}}} \left\{ \sum_{k=1}^{K} \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \right\} \\
&+ \lambda_1 \cdot \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}} \left\{ \mathbb{I}(I_K^{\mathcal{D}} < 1) \right\} \right] \\
&+ \lambda_2 \cdot \sum_{k=1}^{K-1} \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_k^{\mathcal{D}}} \left\{ \mathbb{I}(I_{k-1}^{\mathcal{D}} < 1) - \mathbb{I}(I_k^{\mathcal{D}} < 1) \right\} \cdot \right. \\
&\left. \mathbb{E}_{C_1^{\mathcal{E}},..,C_k^{\mathcal{E}}} \left\{ \mathbb{I}(I_k^{\mathcal{E}} > 1) \right\} \right] \\
&+ \lambda_2 \cdot \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}} \left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \right. \\
&\left. \mathbb{E}_{C_1^{\mathcal{E}},..,C_K^{\mathcal{E}}} \left\{ \mathbb{I}(I_K^{\mathcal{E}} > 1) \right\} \right] \qquad (43)
\end{aligned}
$$

Using (32) and (33) and due to the independence of the main channel and eavesdropper's channel, the previous optimization problem is equivalent to solve:

$$
\begin{aligned}
J^{\lambda_1,\lambda_2} = \min_{\rho_1,\ldots,\rho_K} &\mathbb{E}_{C_1^{\mathcal{D}},C_1^{\mathcal{E}}} \left\{ \rho_1 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_0^{\mathcal{D}} < 1) - \right. \right. \right. \\
&\left. \mathbb{I}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1 < 1) \right\} \cdot \left\{ \mathbb{I}(I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1 > 1) \right\} \Big] \\
&+ \mathbb{E}_{C_2^{\mathcal{D}},C_2^{\mathcal{E}}} \left\{ \rho_2 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_1^{\mathcal{D}} < 1) \right. \right. \right. \\
&\left. \left. - \mathbb{I}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2 < 1) \right\} \cdot \left\{ \mathbb{I}(I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2 > 1) \right\} \right] \\
&+ .... \\
&+ \mathbb{E}_{C_K^{\mathcal{D}},C_K^{\mathcal{E}}} \left\{ \rho_K + \lambda_1 \cdot \mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1) + \lambda_2 \cdot \right. \\
&\left. \left[\left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \left\{ \mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K > 1) \right\} \right] \right. \\
&\left. \left. \left. \right\} ... \right\} \right\}. \qquad (44)
\end{aligned}
$$

We observe that the initial complicated problem can be simplified by breaking it into simpler subproblems in a recursive manner:

$$
J^{\lambda_1,\lambda_2} = J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}}) \qquad (45)
$$

$$
\begin{aligned}
J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}}) = \min_{\rho_1} &\mathbb{E}_{C_1^{\mathcal{D}},C_1^{\mathcal{E}}} \left\{ \rho_1 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_0^{\mathcal{D}} < 1) - \right. \right. \right. \\
&\left. \mathbb{I}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1 < 1) \right\} \cdot \left\{ \mathbb{I}(I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1 > 1) \right\} \Big] \\
&+ J_2^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1, I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1) \Big\}. \qquad (46)
\end{aligned}
$$

$$
\begin{aligned}
J_2^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}}, I_1^{\mathcal{E}}) = \min_{\rho_2} &\mathbb{E}_{C_2^{\mathcal{D}},C_2^{\mathcal{E}}} \left\{ \rho_2 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_1^{\mathcal{D}} < 1) - \right. \right. \right. \\
&\left. \mathbb{I}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2 < 1) \right\} \cdot \left\{ \mathbb{I}(I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2 > 1) \right\} \Big] \\
&+ J_3^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2, I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2) \Big\}. \qquad (47)
\end{aligned}
$$

...

$$
\begin{aligned}
J_K^{\lambda_1,\lambda_2}(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}}) = \min_{\rho_K} &\mathbb{E}_{C_K^{\mathcal{D}},C_K^{\mathcal{E}}} \left\{ \rho_K + \right. \\
&\lambda_2 \cdot \left[\left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \left\{ \mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K > 1) \right\} \right] \\
&\left. + \lambda_1 \cdot \mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1). \right. \qquad (48)
\end{aligned}
$$

which leads to the desired result.

REFERENCES

[1] G. Caire and D. Tuninetti, "The throughput of hybrid-ARQ protocols for the Gaussian collision channel," *IEEE Trans. Inf. Theor.*, vol. 47, no. 5, pp. 1971–1988, July 2001.

[2] E. Soijanin, N. Varnica, and P. Whiting, "Punctured vs Rateless Codes for Hybrid ARQ," in *Information Theory Workshop, 2006. ITW '06 Punta del Este. IEEE*, March 2006, pp. 155–159.

[3] C. Leanderson and G. Caire, "The performance of incremental redundancy schemes based on convolutional codes in the block-fading Gaussian collision channel," *IEEE Trans. on Wireless Comm.*, vol. 3, no. 3, pp. 843–854, May 2004.

[4] S. Sesia, G. Caire, and G. Vivier, "Incremental redundancy hybrid ARQ schemes based on low-density parity-check codes," *IEEE Transactions on Communications*, vol. 52, no. 8, pp. 1311–1321, Aug 2004.

[5] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theor.*, vol. 24, no. 3, pp. 339–348, 1978.

[7] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theor.*, vol. 54, no. 10, pp. 4687–4698, 2008.

[8] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theor.*, vol. 54, no. 6, pp. 2470–2492, 2008.

[9] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theor.*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[10] Z. Mheich, M. Le Treust, F. Alberge, P. Duhamel, and L. Szczecinski, "Rate-adaptive secure HARQ protocol for block-fading channels," in *Proc. of the 22nd European Signal Processing Conference*, Lisbon, Sept. 2014.

[11] L. Szczecinski, S. Khosravirad, P. Duhamel, and M. Rahman, "Rate allocation and adaptation for incremental redundancy truncated HARQ," *IEEE Transactions on Communications*, vol. 61, no. 6, pp. 2580–2590, June 2013.

[12] L. Szczecinski, C. Correa, and L. Ahumada. Variable-rate Retransmissions for Incremental Redundancy Hybrid ARQ. [Online]. Available: http://arxiv.org/abs/1207.0229

[13] S. R. Khosravirad, L. Szczecinski, and F. Labeau, "Rate-Adaptive HARQ in Relay-based Cooperative Transmission," in *Proc. of the IEEE International Conference on Communications (ICC)*, June 2013.

[14] A. Shokrollahi, "Raptor codes," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2551–2567, June 2006.

[15] M. Bloch and J. Barros, *Physical layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[16] A. El Gamal and Y. H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[17] M. Le Treust, L. Szczecinski, and F. Labeau, "Secrecy & Rate Adaptation for secure HARQ protocols," in *Proc of the 2013 IEEE Information Theory Workshop (ITW)*, Sevilla, Sept 2013, pp. 1–5.

[18] M. Zorzi and R. R. Rao, "On the use of renewal theory in the analysis of ARQ protocols," *IEEE Transactions on Communications*, vol. 44, no. 9, pp. 1077–1081, Sep. 1996.

[19] P. Wu and N. Jindal, "Performance of hybrid-arq in block-fading channels: A fixed outage probability analysis," *IEEE Transactions on Communications*, vol. 58, no. 4, pp. 1129–1141, April 2010.