RATE-ADAPTIVE SECURE HARQ PROTOCOL FOR BLOCK-FADING CHANNELS

Zeina Mheich[*], *Maël Le Treust*[†], *Florence Alberge*[*], *Pierre Duhamel*[*], *Leszek Szczecinski*[‡]

[*] L2S (Supelec–Univ Paris-Sud–CNRS), 91192 Gif/Yvette, France. [firstname.lastname@lss.supelec.fr]
[†] ETIS/ENSEA - UCP - CNRS, 95014 Cergy, France. [mael.le-treust@ensea.fr]
[‡] INRS-EMT, Montreal, Canada. [leszek@emt.inrs.ca]

ABSTRACT

This paper analyzes the achievable secrecy throughput in incremental redundancy secure HARQ protocols for communication over block-fading wiretap channels (WTC). The transmitter has no instantaneous channel state information (CSI) but can receive an outdated version of CSI from both legitimate receiver and eavesdropper through reliable multibit feedback channels. Using outdated CSI, the transmitter can adapt the coding rates. Since the transmitter cannot adapt the coding rates to the instantaneous channel conditions, we consider the outage performance of secure HARQ protocols. We show how to find the optimal rate-adaptation policies to maximize the secrecy throughput under constraints on outage probabilities. Numerical results for a Rayleigh-fading WTC show that the rate-adaptation using multilevel feedbacks provides important gains in secrecy throughput comparing to the non-adaptive model. The fact that the eavesdropper also feedbacks information may seem unrealistic, but obtained results can be understood as an upper limit of the possible secrecy throughput improvements.

Index Terms— HARQ, incremental redundancy, block fading, information-theoretic secrecy, rate adaptation.

1. INTRODUCTION

Automatic Repeat reQuest (ARQ), is an error-control protocol that automatically initiates a request to retransmit any data packet or frame from the sender after detecting corrupted data. When the transmitter fails to receive an acknowledgment (ACK) signal to confirm the data has been received, it usually retransmits the data and repeats the process a predetermined number of times until the transmitter receives the ACK. The hybrid ARQ (HARQ) protocols combine powerful channel coding with ARQ error-control to enhance the reliability of communication links. An information-theoretic analysis of the throughput performance of HARQ protocols over block-fading Gaussian collision channels can be found in [1]. The security of data communication over wireless networks is also becoming an important concern. In [2], 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.

This paper studies secure communication based on incremental redundancy HARQ protocols. Due to the absence of instantaneous CSI, the transmitter cannot adapt coding rates to channel conditions. Instead, fixed coding rates are used and the outage performance of secure HARQ is considered. Our work is basically inspired from [3] which presents an information-theoretic study of secure HARQ protocols for a block fading wiretap channel. In [3] the transmitter obtains a 1-bit ACK/NACK feedback from the destination to declare a successful/unsuccessful decoding and the incremental redundancy (INR) is considered when the sub-codewords have the same length in each retransmission (non-adaptive model). In this paper, the transmitter uses multilevel feedback channels from both destination and eavesdropper carrying outdated CSI. The coding rates can therefore be adapted using feedback channels, by allowing the lengths of sub-codewords to change at each retransmission, in order to maximize the secrecy throughput under constraints on outage probabilities. The optimal rate adaption policies are derived by solving this optimization problem using dynamic programming. This paper evaluates the performance gain obtained with adaptive-rate transmission over the non-adaptive rate, as was done in [4] for the non secure case.

2. SYSTEM MODEL AND PRELIMINARIES

We consider the block-fading wiretap channel in which a transmitter X sends confidential messages to a receiver Y in the presence of an eavesdropper Z which listens to the transmission. Both the main channel and eavesdropper's channel experience K-block fading in which channels remain constant over a block but vary independently from block to another. At the transmitter, a confidential message w of fixed length M_i (information bits) is encoded into a codeword x^N of N symbols $x_1, x_2, .., x_N$. We do not constrain N, i.e., we assume that a code with arbitrarily rate can be constructed as in [4]. Any subset of the symbols x_j is

The authors acknowledge the support of CNRS via the International Associate Laboratory "Control and Communications for Smart Grids" between Quebec and France.

called a sub-codeword. The codeword x^N is divided into K sub-codeword $\mathbf{x}_k$, $k = 1, .., K$. The kth block $\mathbf{x}_k$ is sent in the kth slot and received by the legitimate receiver and the eavesdropper through the channel gain $\sqrt{h_k}$ and $\sqrt{g_k}$ respectively. The tth received symbol x_t, sent in the kth block is given by

$$y_t = \sqrt{h_k} \cdot x_t + v_t \quad \text{and} \qquad z_t = \sqrt{g_k} \cdot x_t + u_t \tag{1}$$

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 and eavesdropper channels respectively at time t. We assume that codeword symbols are samples of a real Gaussian distribution with zero mean and unit variance. Thus the SNRs received at the legitimate receiver and the eavesdropper are respectively h_k and g_k in the kth transmission. The transmitter has no instantaneous CSI available from either the main channel or the eavesdropper channel, but knows the channel statistics. However, the constant gain during each block is assumed to be perfectly known at the corresponding receiver. We consider Rayleigh block fading, i.e., the instantaneous SNRs have the following probability density functions:

$$p_H(x) = \frac{1}{\overline{h}} \cdot e^{-\frac{x}{\overline{h}}} \quad \text{and} \qquad p_G(x) = \frac{1}{\overline{g}} \cdot e^{-\frac{x}{\overline{g}}} \tag{2}$$

where $\overline{h}$ and $\overline{g}$ are the average SNRs of the main and eavesdropper channels respectively.

Now, we consider a single block transmission (i.e. $K = 1$) and introduce Wyner codes. In a wiretap channel, the source wishes to convey a message w, which is chosen uniformly at random from the message set $\mathcal{W}$, to the legitimate receiver. The sender performs this task by encoding w as a vector x^N of length N and transmitting x^N. The basic idea of Wyner is to use a stochastic encoder in order to confuse the eavesdropper about the message sent and to provide secrecy [2]. Let $C(N, R_0, R_s)$ denote a Wyner code to transmit the confidential message set $\mathcal{W} = \{1, 2, .., 2^{NR_s}\}$ where R_0 is the main channel code rate and R_s ($R_s \leq R_0$) is the secrecy information rate. The rates pair (R_0, R_s) should satisfy [3]

$$R_0 \leq I(X;Y) \tag{3}$$

$$R_0 - R_s \geq I(X;Z) \tag{4}$$

in order to ensure reliable and secure communication.We use the notations $M_i = N \cdot R_s$ to denote the number of information bits (which is fixed) and $M_T = N \cdot R_0$ to denote the total number of bits transmitted, which includes the M_d dummy bits that are necessary to ensure secrecy. The corresponding rate $R' = R_0 - R_s$ is the rate sacrificed to provide secrecy. The codebook is assumed to be known at all nodes. We further assume that the coding is random with long codewords and that receivers implement typical-set decoding which allow us to find the performance limits for any practical scheme.

3. ADAPTIVE INR SCHEME

We consider incremental redundancy secure HARQ as a transmission protocol. 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 (the sub-codewords $\mathbf{x_k}$ may not have the same length) where $N = \sum_{k=1}^{K} N_k$. We define the "ratio of secret bits transmitted" by $\gamma = \frac{M_i}{M_T} = \frac{M_i}{M_i + M_d}$. The number of dummy bits M_d can be chosen by the transmitter according to channel statistics. 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. If a second retransmission is requested by the receiver due to unsuccessful decoding, 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 $\mathbf{x}_2$. This continues until the maximum number of transmission attempts K is reached or until successful decoding of the message at the legitimate receiver. After k transmissions, each receiver applies maximum likelihood decoding using the channel observations obtained up to the kth transmission. The condition of successful decoding at the legitimate receiver after k transmissions is that the average accumulated mutual information is larger than the overall code rate. This condition was written for $K = 1$ in (3). In our system model where the sub-codewords $\mathbf{x_k}$ may not have the same length, this condition can be written as

$$\frac{M_T}{\sum_{l=1}^{k} N_l} \leq \frac{\sum_{l=1}^{k} c_l^{\mathcal{D}} \cdot N_l}{\sum_{l=1}^{k} N_l} \tag{5}$$

where $c_l^{\mathcal{D}} = \frac{1}{2}\log_2(1 + h_l)$. For convenience, N_l is normalized as $\rho_l = \frac{N_l}{M_T}$ which is interpreted as the "redundancy" brought by the lth sub-codeword. Now the condition for successful decoding in (5) can be written as follows

$$I_k^{\mathcal{D}} \triangleq \sum_{l=1}^{k} c_l^{\mathcal{D}} \cdot \rho_l \geq 1 \tag{6}$$

where $I_k^{\mathcal{D}}$ is the "state of the decoder" at the legitimate receiver ($\mathcal{D}$). The condition for secrecy at the eavesdropper after k transmissions is that the average accumulated mutual information is less than the difference between the main channel code rate and the secrecy information rate

$$\frac{M_T}{\sum_{l=1}^{k} N_l} - \frac{M_i}{\sum_{l=1}^{k} N_l} \geq \frac{\sum_{l=1}^{k} c_l^{\mathcal{E}} \cdot N_l}{\sum_{l=1}^{k} N_l} \tag{7}$$

$$\text{equivalently,} \qquad I_k^{\mathcal{E}} \triangleq \sum_{l=1}^{k} c_l^{\mathcal{E}} \cdot \rho_l + \gamma \leq 1 \tag{8}$$

where $c_l^{\mathcal{E}} = \frac{1}{2}\log_2(1 + g_l)$. This condition was given in (4) for $K = 1$. We assume that the transmitter uses error-free multi-level feedback channels from the both the legitimate receiver and the eavesdropper. From (6) and (8) we know that the decoding error events in the k-th transmission at the legitimate receiver and the eavesdropper depend on $I^{\mathcal{D}}_{k-1}$ and $I^{\mathcal{E}}_{k-1}$ which can be communicated to the sender via the multi-level feedback channels and on $c^{\mathcal{D}}_k$ and $c^{\mathcal{E}}_k$ which are unknown at the transmitter. Consequently, $I^{\mathcal{D}}_{k-1}$ and $I^{\mathcal{E}}_{k-1}$ are the only parameters required to adapt the redundancy ρ_k via a scalar function. We consider the following policy for the transmission attempt k with $k \in \{1, ..., K\}$

$$\rho_k = \begin{cases} \rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}) & \text{if } I^{\mathcal{D}}_{k-1} < 1 \text{ and } I^{\mathcal{E}}_{k-1} \leq 1 \\ \\ \rho_k(I^{\mathcal{D}}_{k-1}) & \text{if } I^{\mathcal{D}}_{k-1} < 1 \text{ and } I^{\mathcal{E}}_{k-1} > 1 \\ \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

This makes our work different from [3] which considers the special case where $\rho_k = \rho \; \forall k$. The goal now is to find the rate adaptation policies ρ_k, for each possible value of the couple $(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1})$, and γ which maximize the performance criterion defined in the next section.

4. 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 reward-renewal theorem [5], 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

$$\eta = \frac{M_i^*}{\overline{N}} \tag{10}$$

Since the transmitter has no instantaneous CSI, we consider that the service quality is acceptable as long as the percentage of information bits unsuccessfully decoded by the destination 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 destination 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 w.r.t. eavesdropper's link.

- $M_i^* = M_i \cdot (1 - f_0)$, and f_0 can be written as

$$f_0 = \Pr\{I^{\mathcal{D}}_K < 1\} = \mathbb{E}_{C^{\mathcal{D}}_1,..,C^{\mathcal{D}}_K}\{\mathbb{I}(I^{\mathcal{D}}_K < 1)\} \tag{11}$$

$$= \int_0^1 dx \int_\gamma^\infty dy \; p_{I^{\mathcal{D}}_K \; I^{\mathcal{E}}_K}(x, y) \tag{12}$$

where $\mathbb{I}(x) = 1$ if x is true and $\mathbb{I}(x) = 0$ if x is false. $p_{I^{\mathcal{D}}_K \; I^{\mathcal{E}}_K}(x, y)$ is the joint pdf of $I^{\mathcal{D}}_K$ and $I^{\mathcal{E}}_K$.

- 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 kth transmission attempt

$$\overline{N}_k = M_T \cdot \mathbb{E}_{I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}}\{\rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1})\} \tag{13}$$

Thus the secrecy throughput can be written as

$$\eta = \gamma \cdot \frac{1 - f_0}{\sum_{k=1}^K \mathbb{E}_{I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}}\{\rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1})\}} \tag{14}$$

Let $\mathcal{K}$ denotes the number of transmission in an HARQ session. The secrecy outage probability f_s can be expressed as

$$f_s = \Pr(I^{\mathcal{E}}_{\mathcal{K}} > 1) = \sum_{k=1}^K \Pr(\mathcal{K} = k) \cdot \Pr(I^{\mathcal{E}}_k > 1) \tag{15}$$

- The probability mass function of $\mathcal{K}$ can be expressed as

$$\Pr(\mathcal{K} = k) = \Pr(I^{\mathcal{D}}_{k-1} < 1, I^{\mathcal{D}}_k \geq 1) \tag{16}$$

$$= \Pr(I^{\mathcal{D}}_{k-1} < 1) - \Pr(I^{\mathcal{D}}_k < 1) \tag{17}$$

$$= \mathbb{E}_{C^{\mathcal{D}}_1,..,C^{\mathcal{D}}_k}\{\mathbb{I}(I^{\mathcal{D}}_{k-1} < 1) - \mathbb{I}(I^{\mathcal{D}}_k < 1)\} \tag{18}$$

for $k < K$, and $\Pr(\mathcal{K} = K)$ is equal to

$$\Pr(I^{\mathcal{D}}_{K-1} < 1) = \mathbb{E}_{C^{\mathcal{D}}_1,..,C^{\mathcal{D}}_{K-1}}\{\mathbb{I}(I^{\mathcal{D}}_{K-1} < 1)\} \tag{19}$$

- The probability that the eavesdropper can decode the confidential message at the kth transmission is

$$\Pr(I^{\mathcal{E}}_k > 1) = \mathbb{E}_{C^{\mathcal{E}}_1,..,C^{\mathcal{E}}_k}\{\mathbb{I}(I^{\mathcal{E}}_k > 1)\} \tag{20}$$

$$= \int_0^\infty dx \int_1^\infty dy \; p_{I^{\mathcal{D}}_k \; I^{\mathcal{E}}_k}(x, y) \tag{21}$$

The secrecy throughput optimization problem under outages constraints can be written as

$$\begin{aligned} \max_{\gamma, \rho_1, ..., \rho_K} \quad & \eta(\gamma, \rho_1, ..., \rho_K) \\ s.t. & \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases} \end{aligned} \tag{22}$$

where ξ_ϵ and ξ_s are the target outage probabilities.

5. OPTIMIZATION METHOD

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 outage probabilities constraints. To solve this problem we use exhaustive search to find the optimal γ. Thus, we solved problem (22) for different values of $\gamma \in [0, 1]$. Once $\gamma \in [0, 1]$ is fixed, we solve (22) subject to ρ_k only. We will describe later how to make the choice of γ in the simulations. The optimization prodecure is described below. This is an off-line procedure intended to compute the optimal values of ρ_k for any values of feedbacks. Now suppose that γ is fixed to an arbitrary value in $[0,1]$. In order to solve (22) for a fixed γ, we employ two weighting multipliers λ_1 and λ_2 for the constraints on f_0 and f_s in (22) and we minimize: (i) the denominator of η in (14) and (ii) f_0 and f_s at the same time [4]

$$J^{\lambda_1\lambda_2} = \min_{\rho_1,\dots,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}} \{\rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})\} \\ + \lambda_1 \cdot f_0(\rho_1,\dots,\rho_K) + \lambda_2 \cdot f_s(\rho_1,\dots,\rho_K) \quad (23)$$

Problem (23) is solved for different values of (λ_1, λ_2). Then we obtain a set of λ_1 and λ_2 values associated with the corresponding optimal 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. We used gradient-search method in order to update λ_1 and λ_2. Now, we explain the method for solving (23) for a fixed value of (λ_1, λ_2) and how to calculate the corresponding secrecy throughput and outage probabilities. We can observe that the states of decoders at the legitimate receiver and the eavesdropper at time k can be written as a function of the previous states as follows,

$$I_k^{\mathcal{D}} = I_{k-1}^{\mathcal{D}} + C_k^{\mathcal{D}} \cdot \rho_k \text{ and } I_k^{\mathcal{E}} = I_{k-1}^{\mathcal{E}} + C_k^{\mathcal{E}} \cdot \rho_k \quad (24)$$

where $I_0^{\mathcal{D}} = 0$ and $I_0^{\mathcal{E}} = \gamma$. Using (12) and (15), problem (23) can be written as

$$J^{\lambda_1\lambda_2} = \min_{\rho_1,..,\rho_K} \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}},C_1^{\mathcal{E}},..,C_{K-1}^{\mathcal{E}}} \Bigg\{ \\ \textstyle\sum_{k=1}^{K} \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \Bigg\} + \lambda_1 \cdot \Bigg[\mathbb{E}_{C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}} \Bigg\{ \mathbb{I}(I_K^{\mathcal{D}} < 1) \Bigg\} \Bigg] + \\ \lambda_2 \cdot \Bigg[\textstyle\sum_{k=1}^{K-1} \mathbb{E}_{C_1^{\mathcal{D}},..,C_k^{\mathcal{D}}} \Bigg\{ \mathbb{I}(I_{k-1}^{\mathcal{D}} < 1) - \mathbb{I}(I_k^{\mathcal{D}} < 1) \Bigg\} + \\ \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}} \Bigg\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \Bigg\} \Bigg] \cdot \mathbb{E}_{C_1^{\mathcal{E}},..,C_K^{\mathcal{E}}} \Bigg\{ \mathbb{I}(I_K^{\mathcal{E}} > 1) \Bigg\} \quad (25)$$

Using (24), and due to the independence of the main and eavesdropper channels, problem (25) can be simplified by breaking it into simpler subproblems in a recursive manner

$$J^{\lambda_1\lambda_2} = J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}}) \quad (26)$$

$$J_1^{\lambda_1\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}}) = \min_{\rho_1} \mathbb{E}_{C_1^{\mathcal{D}}, C_1^{\mathcal{E}}} \Bigg\{ \rho_1 + \lambda_2 \cdot \Bigg[\Bigg\{ \mathbb{I}(I_0^{\mathcal{D}} < 1) - \\ \mathbb{I}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1 < 1) \Bigg\} \cdot \Bigg\{ \mathbb{I}(I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1 > 1) \Bigg\} \Bigg] \\ + J_2^{\lambda_1\lambda_2}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1, I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1) \Bigg\} \quad (27)$$

$$\cdots$$

$$J_{K-1}^{\lambda_1\lambda_2}(I_{K-2}^{\mathcal{D}}, I_{K-2}^{\mathcal{E}}) = \min_{\rho_{K-1}} \mathbb{E}_{C_{K-1}^{\mathcal{D}}, C_{K-1}^{\mathcal{E}}} \Bigg\{ \rho_{K-1} + \\ \lambda_2 \cdot \Bigg[\Bigg\{ \mathbb{I}(I_{K-2}^{\mathcal{D}} < 1) - \mathbb{I}(I_{K-2}^{\mathcal{D}} + C_{K-1}^{\mathcal{D}} \cdot \rho_{K-1} < 1) \Bigg\} \cdot \\ \Bigg\{ \mathbb{I}(I_{K-2}^{\mathcal{E}} + C_{K-1}^{\mathcal{E}} \cdot \rho_{K-1} > 1) \Bigg\} \Bigg] + \\ J_K^{\lambda_1\lambda_2}(I_{K-2}^{\mathcal{D}} + \rho_{K-1} C_{K-1}^{\mathcal{D}}, I_{K-2}^{\mathcal{E}} + \rho_{K-1} C_{K-1}^{\mathcal{E}}) \Bigg\} \quad (28)$$

$$J_K^{\lambda_1\lambda_2}(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}}) = \min_{\rho_K} \mathbb{E}_{C_K^{\mathcal{D}}, C_K^{\mathcal{E}}} \Bigg\{ \rho_K + \\ \lambda_2 \cdot \Bigg[\Bigg\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \Bigg\} \cdot \Bigg\{ \mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K > 1) \Bigg\} \Bigg] \\ + \lambda_1 \cdot \mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1) \Bigg\} \quad (29)$$

The recursive nature of the above equations is characteristic of the dynamic programming (DP). Now, to solve (26)–(29) 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 (9), 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 (29), we should solve $L_1 \cdot L_2$ one-dimensional problems where the only variable is ρ_K. In (29), 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) $\mathbb{E}_{C_K^{\mathcal{E}}}\{\mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K > 1)\} = 1 - F_{C^{\mathcal{E}}}\big(\frac{1 - I_{K-1}^{\mathcal{E}}}{\rho_K}\big)$ and (iii) $\mathbb{E}_{C_K^{\mathcal{D}}}\{\mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1)\} = F_{C^{\mathcal{D}}}\big(\frac{1 - I_{K-1}^{\mathcal{D}}}{\rho_K}\big)$, where F_{C^i} is the cumulative density function of C^i, $i \in \{\mathcal{D}, \mathcal{E}\}$, calculated using (2). The problem should be solved starting from step K and going recursively up to $k = 1$ to find all the optimum policies ρ_k $\big($which are $L_1 \times L_2$ matrices, except ρ_1 which has one element according to (24)$\big)$. By solving the DP optimization recursive process, the optimal rate-adaptation policies associated with the given λ_1 and λ_2 are derived. Since we need to calculate the outage probabilities f_0 and f_s in order to update the multipliers, 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 (12) and (15). 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

$$F_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x,y) = \Pr\left(\rho_1 \cdot C_1^{\mathcal{D}} < x, \gamma + \rho_1 \cdot C_1^{\mathcal{E}} < y\right) \quad (30)$$

$$= F_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right) \cdot F_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right) \quad (31)$$

which differentiated yields the joint pdf

$$p_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x,y) = \frac{1}{\rho_1} \cdot p_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right) \cdot \frac{1}{\rho_1} \cdot p_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right) \quad (32)$$

where p_{C^i} is the probability density function of the i.i.d random variables $C_1^i, .., C_K^i$ and $i \in \{\mathcal{D}, \mathcal{E}\}$. For $k > 1$, the joint cumulative density function is calculated recursively

$$F_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = \Pr\left(I_{k-1}^{\mathcal{D}} + \rho_k \cdot C_k^{\mathcal{D}} < x, I_{k-1}^{\mathcal{E}} + \rho_k \cdot C_k^{\mathcal{E}} < y\right)$$
$$= \int_0^x \int_\gamma^y F_{C^{\mathcal{D}}}\left(\tfrac{x-\alpha}{\rho_k(\alpha,\beta)}\right) \cdot$$
$$F_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)}\right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\, d\alpha\, d\beta \quad (33)$$

Thus the joint pdf obtained by differentiating the joint cumulative density function can be calculated recursively

$$p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = \int_0^x \int_\gamma^y \frac{1}{\rho_k(\alpha,\beta)} \cdot p_{C^{\mathcal{D}}}\left(\frac{x-\alpha}{\rho_k(\alpha,\beta)}\right) \cdot \frac{1}{\rho_k(\alpha,\beta)} \cdot$$
$$\cdot\, p_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)}\right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\, d\alpha\, d\beta \quad (34)$$

When $\rho_k(x,y) = 0$, we have $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(x,y)$ according to (33). For each fixed λ_1 and λ_2, we can calculate the secrecy throughput (14) using $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y)$ and $\rho_k(x,y)$ for $k = 1, ..., K$. Now we discuss the choice of γ. In the simulations, we observed 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 we will be interested to find the maximum value of γ which can verify outage probabilities constraints.

6. NUMERICAL APPLICATION

In this numerical example, the parameter settings are as follows: $\overline{h} = 15$ dB, $\overline{g} = 5$ dB, $\xi_\epsilon = 10^{-3}$ and $\xi_s = 10^{-3}$. The simulations are done for several values of the maximum number of transmissions K. Figure 1 shows the secrecy throughput η vs the K using the "INR scheme" described in [3] and the "adaptive INR scheme" described in this paper. There is obviously a tradeoff between the throughput to the destination and the information leakage to the eavesdropper: larger sub-codewords result in increased throughput to the destination, but also into a loss 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 the (hidden) optimization parameter. The results show that a notable gain is obtained using the rate-adaptive scheme when $K > 3$. However, when K is small, e.g. for $K = 1$ or 3, the secrecy throughput η is still negligible using the adaptive scheme due to insufficient diversity. The secrecy throughput converges when $K \to \infty$ to the ergodic value $\eta^* = 1.31$ calculated in [3]. For $K = 13$, the adaptive scheme achieves about 50% of η^* while the non-adaptive scheme achieves only 40%.

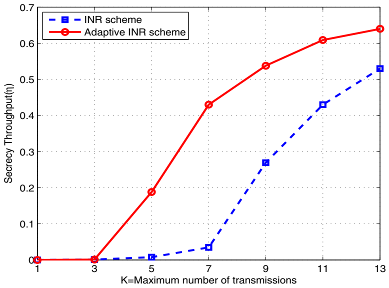

Fig. 1. Secrecy throughput η vs K.

7. CONCLUSION

In this paper, we considered secure communication over block-fading WTC based on secure HARQ protocol. The transmitter has no instantaneous CSI but can receive outdated CSI from both destination and eavesdropper via feedback channels. We analyzed rate adaptation for INR scheme using outdated CSI and we show provide the optimal adaptation policies which maximize the secrecy throughput under outage constraints. The proposed rate adaptive scheme provides notable gains in terms of secrecy throughput compared to non-adaptive scheme. A rate adaptive scheme based on sole feedbacks from destination is currently under consideration.

REFERENCES

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

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

[3] 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.

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

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