Secrecy & Rate Adaptation for secure HARQ protocols

Maël Le Treust, Leszek Szczecinski, Fabrice Labeau

Secrecy & Rate Adaptation for Secure HARQ Protocols

Maël Le Treust*†, Leszek Szczecinski* and Fabrice Labeau†
* Université INRS - Centre EMT, Montréal, Québec, Canada
† Mc Gill University, Montréal, Québec, Canada
{letreust},{leszek}@emt.inrs.ca, fabrice.labeau@mcgill.ca

***Abstract*—This paper is dedicated to the study of HARQ protocols under a secrecy constraint. An encoder sends information to a legitimate decoder while keeping it secret from the eavesdropper. Our objective is to provide a coding scheme that satisfies both reliability and confidentiality conditions. This problem has been investigated in the literature using a coding scheme that involves a unique secrecy parameter. The uniqueness of this parameter is sub-optimal for the throughput criteria and we propose a new coding scheme that introduces additional degrees of freedom. Our code involves Secrecy Adaptation and Rate Adaptation and we called it SARA-code. The first contribution is to prove that the SARA-code has small error probability and small information leakage rate. The second contribution is to show, over a numerical example, that the SARA-code improves the secrecy throughput.**

***Index Terms*—Hybrid Automatic Retransmission Request, Physical Layer Security, State Dependent Wiretap Channel.**

I. Introduction

Reliability is a fundamental challenge for wireless communication that can be took up by the so-called Hybrid Automatic Retransmission reQuest (HARQ) protocol. A single-bit acknowledgement feedback ACK/NACK indicates to the encoder whether the decoding was successful or not. Multiple retransmissions enhance the reliability of the communication by adapting the rate of transmitted information to the channel capacity. An information theoretical analysis of HARQ protocols can be found in [1] and improvements of HARQ protocols using a rate allocation and codewords-length adaptation can be found in [2], [3], [4] and [5].

Confidentiality arises as a natural question in wireless communication because all other wireless devices can listen to the traffic and extract some confidential information. Instead of using a secret key, Wyner [6] shows that the statistics of the channel can be exploited in order to secure the transmitted information. Csiszar and Körner [7] extended the result of Wyner [6] and characterize the secrecy capacity of the general wiretap channel. In [8], the authors proposed to adapt the HARQ protocols in order to guarantee simultaneously the reliability and the confidentiality. The coding scheme proposed in [8] is based on a mother code that involves a unique secrecy parameter. The uniqueness of this secrecy parameter is a strong drawback for this secure HARQ protocol because it must be adapted to all possible retransmissions even if they don't occur.

This work was supported by the government of Quebec under grant #PSR-SIIRI-435.

We investigate the secure HARQ protocol by introducing additional degrees of freedom in terms of secrecy parameters. We deepen the information theoretical analysis of [8] by considering state dependent wiretap channels represented by Fig. 1. One objective of our work is called "secrecy adaptation" and consists in splitting the secrecy constraints of each transmission over different parameters. A second objective, called "rate adaptation" and treated in [9], is to reduce the duration of the retransmission in order to increase the information rate. The first contribution of our work is to guarantee the existence of a coding scheme that involves Secrecy Adaptation and Rate Adaptation, called a SARA-code, with small error probability and small information leakage rate. The second contribution of our work is to show a numerical example for which the SARA-code improves the secrecy throughput.

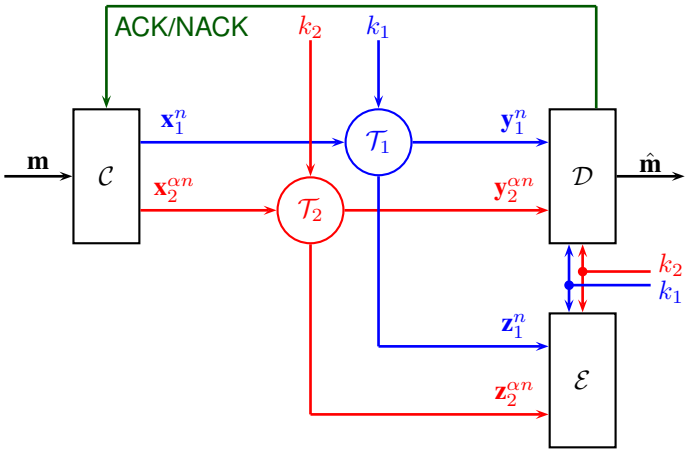

Fig. 1. State dependent wiretap channels, for the first $\mathcal{T}_1(\mathbf{y}_1, \mathbf{z}_1|\mathbf{x}_1, k_1)$ and for the second $\mathcal{T}_2(\mathbf{y}_2, \mathbf{z}_2|\mathbf{x}_2, k_2)$ transmissions. After the end of the first transmission, the decoder $\mathcal{D}$ sends a ACK/NACK feedback to the encoder $\mathcal{C}$. The second transmission starts if the encoder $\mathcal{C}$ receives a NACK feedback from the legitimate decoder. The state parameters $k_1 \in \mathcal{K}_1$ and $k_2 \in \mathcal{K}_2$ are chosen arbitrarily, stay constant during the transmission and are available only at the legitimate decoder $\mathcal{D}$ and at the eavesdropper $\mathcal{E}$. The duration $\alpha \cdot n \in \mathbb{N}$ of the second transmission is not necessarily equal to duration $n \in \mathbb{N}$ of the first transmission.

Section II presents the channel model under investigation and the concept of HARQ-code. The existence of a SARA-code is stated in Section III. The performance of this code is measured by the throughput defined in Section IV. A simple example with two transmissions is investigated in Section V. Section VI provides a sketch of the proof for the existence of a SARA-code and Section VII concludes the article.

II. System model

We consider a scenario with two transmissions described by Fig. 1. During the first transmission, encoder $\mathcal{C}$ uses the sequence of input symbols $x_1^n \in \mathcal{X}_1^n$ in order to transmit the message $m \in \mathcal{M}$ to the legitimate decoder $\mathcal{D}$. Decoder $\mathcal{D}$ (resp. Eavesdropper $\mathcal{E}$) observes the sequence of channel outputs $y_1^n \in \mathcal{Y}_1^n$ (resp. $z_1^n \in \mathcal{Z}_1^n$) and tries to decode (resp. to infer) the transmitted message $m \in \mathcal{M}$. Decoder $\mathcal{D}$ sends a ACK/NACK feedback over a perfect channel that indicates to the encoder, whether it has decoded correctly or not. If the encoder receives a NACK feedback, the second transmission starts over the wiretap channel $\mathcal{T}_2$ with input sequence $x_2^{\alpha n} \in \mathcal{X}_2^{\alpha n}$ of length $\alpha \cdot n \in \mathbb{N}$. Decoder $\mathcal{D}$ (resp. Eavesdropper $\mathcal{E}$) tries to decode (resp. to infer) the transmitted message $m \in \mathcal{M}$ from both sequences of channel outputs $y_1^n \in \mathcal{Y}_1^n$ and $y_2^{\alpha n} \in \mathcal{Y}_2^{\alpha n}$ (resp. $z_1^n \in \mathcal{Z}_1^n$ and $z_2^{\alpha n} \in \mathcal{Z}_2^{\alpha n}$). The random variable are denoted by $\mathbf{m}$, $\hat{\mathbf{m}}$, $\mathbf{x}_1^n$, $\mathbf{x}_2^{\alpha n}$, $\mathbf{y}_1^n$, $\mathbf{y}_2^{\alpha n}$, $\mathbf{z}_1^n$, $\mathbf{z}_2^{\alpha n}$ and the message $\mathbf{m} \in \mathcal{M}$ is uniformly distributed. The notation $\Delta(\mathcal{X})$ stands for the set of the probability distributions $\mathcal{P}(\mathbf{x})$ over the set $\mathcal{X}$.

The channels are memoryless i.e. the n-times transition probability and the αn-times transition probability are given by equations (1) and (2). The state parameters $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$ are chosen arbitrarily, stay constant during the transmission and are observed by the decoder and the eavesdropper.

$$\mathcal{T}_1^{\otimes n}(y_1^n, z_1^n | x_1^n, k_1) = \prod_{i=1}^{n} \mathcal{T}_1(y_1(i), z_1(i) | x_1(i), k_1), \quad (1)$$

$$\mathcal{T}_2^{\otimes \alpha n}(y_2^{\alpha n}, z_2^{\alpha n} | x_2^{\alpha n}, k_2) = \prod_{i=1}^{\alpha n} \mathcal{T}_2(y_2(i), z_2(i) | x_2(i), k_2). \quad (2)$$

Definition 1 *A HARQ-code $c_n \in \mathcal{C}(n, \alpha, \mathsf{R})$ with stochastic encoder is a tuple of functions $c_n = (f_1, g_1, f_2, g_2)$ defined by equations (3), (4), (5) and (6).*

$$f_1 : \mathcal{M} \longrightarrow \Delta(\mathcal{X}_1^n), \quad (3)$$
$$g_1 : \mathcal{K}_1 \times \mathcal{Y}_1^n \longrightarrow \{\mathit{ACK}, \mathit{NACK}\} \times \mathcal{M}, \quad (4)$$
$$f_2 : \mathcal{M} \times \mathcal{X}_1^n \times \{\mathit{ACK}, \mathit{NACK}\} \longrightarrow \Delta(\mathcal{X}_2^{\alpha n}), \quad (5)$$
$$g_2 : \mathcal{Y}_1^n \times \mathcal{Y}_2^{\alpha n} \times \mathcal{K}_1 \times \mathcal{K}_2 \longrightarrow \mathcal{M}. \quad (6)$$

Denote by $\mathcal{C}(n, \alpha, \mathsf{R})$, the set of HARQ-code with stochastic encoder. The rate R defines the cardinality $|\mathcal{M}| = 2^{n\mathsf{R}}$ of the set of messages $\mathcal{M}$.

Definition 2 *For each pair of state parameters $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$, the error probability $\mathcal{P}_e$ and the information leakage rate $\mathcal{L}_e$ of the HARQ-code $c_n \in \mathcal{C}(n, \alpha, \mathsf{R})$ are defined by equations (7) and (8).*

$$\mathcal{P}_e\left(c_n \middle| k_1, k_2\right) = \mathcal{P}\left(\boldsymbol{m} \neq \hat{\boldsymbol{m}} \middle| c_n, k_1, k_2\right), \quad (7)$$

$$\mathcal{L}_e\left(c_n \middle| k_1, k_2\right) = \frac{I\left(\boldsymbol{m}; \boldsymbol{z}_1^n, \boldsymbol{z}_2^n \middle| c_n, k_1, k_2\right)}{n}. \quad (8)$$

The random variable $\hat{\boldsymbol{m}}$ denote the output message of the decoder. Depending on the number of transmissions, it is given by $\hat{\boldsymbol{m}} = g_1(\boldsymbol{y}_1^n, k_1)$ or by $\hat{\boldsymbol{m}} = g_2(\boldsymbol{y}_1^n, \boldsymbol{y}_2^n, k_1, k_2)$.

III. Main Result

The objective of this section is to prove the existence of a HARQ-code that has small error probability and small information leakage rate for a whole range of channel states. We introduce the probability distributions $\mathcal{P}_{\mathsf{x}_1}^\star \in \Delta(\mathcal{X}_1)$ and $\mathcal{P}_{\mathsf{x}_2}^\star \in \Delta(\mathcal{X}_2)$ over the channel inputs that will define all the following mutual informations. The rates $\mathsf{R}_{\mathsf{W}_1}$ and $\mathsf{R}_{\mathsf{W}_2}$ denote the amount of secrecy that are introduced implicitly into the HARQ-code in order to confuse the eavesdropper.

Definition 3 (Channel States) *For fixed parameters ε, α, R, $\mathsf{R}_{\mathsf{W}_1}$, $\mathsf{R}_{\mathsf{W}_2}$ and a fixed probability distributions $\mathcal{P}_{\mathsf{x}_1}^\star \in \Delta(\mathcal{X}_1)$ and $\mathcal{P}_{\mathsf{x}_2}^\star \in \Delta(\mathcal{X}_2)$, the set of secure channel states $\mathcal{L}(\varepsilon, \alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}, \mathcal{P}_{\mathsf{x}_1}^\star, \mathcal{P}_{\mathsf{x}_2}^\star)$ is the union of channel states $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$ that satisfy equations (9) and (10) **or** that satisfy equations (11), (12) and (13).*

$$\mathsf{R} + \mathsf{R}_{\mathsf{W}_1} \leq I(\boldsymbol{x}_1; \boldsymbol{y}_1 | k_1) - \varepsilon, \quad (9)$$
$$\mathsf{R}_{\mathsf{W}_1} \geq I(\boldsymbol{x}_1; \boldsymbol{z}_1 | k_1) - \varepsilon, \quad (10)$$

$$\mathsf{R} + \mathsf{R}_{\mathsf{W}_1} + \mathsf{R}_{\mathsf{W}_2} \leq I(\boldsymbol{x}_1; \boldsymbol{y}_1 | k_1) + \alpha \cdot I(\boldsymbol{x}_2; \boldsymbol{y}_2 | k_2) - \varepsilon, \quad (11)$$
$$\mathsf{R}_{\mathsf{W}_1} + \mathsf{R}_{\mathsf{W}_2} \geq I(\boldsymbol{x}_1; \boldsymbol{z}_1 | k_1) + \alpha \cdot I(\boldsymbol{x}_2; \boldsymbol{z}_2 | k_2) - \varepsilon, \quad (12)$$
$$\mathsf{R}_{\mathsf{W}_1} \geq I(\boldsymbol{x}_1; \boldsymbol{z}_1 | k_1) - \varepsilon. \quad (13)$$

Equation (9) (resp. (11)) guarantees that the decoding of the first (resp. of the second) transmission is successful and equation (10) (resp. (12) and (13)) guarantees that the first (resp. that the second) transmission is secured.

Theorem 4 (Code existence) *Fix the parameters α, R, $\mathsf{R}_{\mathsf{W}_1}$, $\mathsf{R}_{\mathsf{W}_2}$ and the input probability distributions $\mathcal{P}_{\mathsf{x}_1}^\star$ and $\mathcal{P}_{\mathsf{x}_2}^\star$. For all $\varepsilon > 0$, there exists a length $\bar{n} \in \mathbb{N}$ such that for all $n \geq \bar{n}$, there exists a HARQ-code $c_n^\star \in \mathcal{C}(n, \alpha, \mathsf{R})$ that satisfies equations (14) and (15) for all channel states $(k_1, k_2) \in \mathcal{L}(\varepsilon, \alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}, \mathcal{P}_{\mathsf{x}_1}^\star, \mathcal{P}_{\mathsf{x}_2}^\star)$.*

$$\mathcal{P}_e\left(c_n^\star \middle| k_1, k_2\right) \leq \varepsilon, \quad (14)$$
$$\mathcal{L}_e\left(c_n^\star \middle| k_1, k_2\right) \leq \varepsilon. \quad (15)$$

A sketch of the proof of Theorem 4 is provided in section VI and the full version is available in [10]. For every tuple of parameters $(\alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2})$, Theorem 4 guarantees the existence of a sequence of HARQ-code $c^\star = (c_n^\star)_{n \geq 1}$ with $c_n^\star \in \mathcal{C}(n, \alpha, \mathsf{R})$, such that the error probability and the information leakage rate converge to zero for a whole range of channel states. In the rest of this article, the sequence of optimal HARQ-code $c^\star = (c_n^\star)_{n \geq 1}$ is called "Secrecy-Adaptation-Rate-Adaptation-code" (SARA-code) with parameters $(\alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2})$. Note that the SARA-code is one of the possible realization of the random HARQ-code stated in section VI-A. The performances of the SARA-code are evaluated by the secure throughput, defined in section IV.

Remark 5 The result stated in Theorem 4 can be easily extended to the case of $I \in \mathbb{N}$ transmissions. To illustrate this, we provide here a short analysis for the case of $I = 3$ transmissions. We introduce the parameters $\mathsf{R}_{\mathsf{W}_3} \in \mathbb{R}$, $\beta \in \mathbb{R}$, $\mathcal{P}_{\mathsf{x}_3}^\star \in \Delta(\mathcal{X}_3)$ and $k_3 \in \mathcal{K}_3$. The set of secure channel states for

3 transmissions $\mathcal{L}_3(\varepsilon,\alpha,\beta,\mathsf{R},\mathsf{R}_{\mathsf{W}_1},\mathsf{R}_{\mathsf{W}_2},\mathsf{R}_{\mathsf{W}_3},\mathcal{P}^\star_{\mathsf{x}_1},\mathcal{P}^\star_{\mathsf{x}_2},\mathcal{P}^\star_{\mathsf{x}_3})$ is the union of channel states $(k_1,k_2,k_3)\in\mathcal{K}_1\times\mathcal{K}_2\times\mathcal{K}_3$ that satisfy equations (9) and (10) **or** that satisfy equations (11), (12) and (13) **or** that satisfy equations (16), (17), (18) and (19).

$$\begin{aligned}\mathsf{R}+\mathsf{R}_{\mathsf{W}_1}+\mathsf{R}_{\mathsf{W}_2}+\mathsf{R}_{\mathsf{W}_3} &\leq I(\mathbf{x}_1;\mathbf{y}_1|k_1)\\ &\quad+\alpha\cdot I(\mathbf{x}_2;\mathbf{y}_2|k_2)+\beta\cdot I(\mathbf{x}_3;\mathbf{y}_3|k_3)-\varepsilon, \quad (16)\\ \mathsf{R}_{\mathsf{W}_1}+\mathsf{R}_{\mathsf{W}_2}+\mathsf{R}_{\mathsf{W}_3} &\geq I(\mathbf{x}_1;\mathbf{z}_1|k_1)\\ &\quad+\alpha\cdot I(\mathbf{x}_2;\mathbf{z}_2|k_2)+\beta\cdot I(\mathbf{x}_3;\mathbf{z}_3|k_3)-\varepsilon, \quad (17)\\ \mathsf{R}_{\mathsf{W}_1}+\mathsf{R}_{\mathsf{W}_2} &\geq I(\mathbf{x}_1;\mathbf{z}_1|k_1)+\alpha\cdot I(\mathbf{x}_2;\mathbf{z}_2|k_2)-\varepsilon, \quad (18)\\ \mathsf{R}_{\mathsf{W}_1} &\geq I(\mathbf{x}_1;\mathbf{z}_1|k_1)-\varepsilon. \quad (19)\end{aligned}$$

The proof of Theorem 4 can be adapted to the case of $I=3$ transmission using a binning scheme with three levels for the inputs $\mathbf{x}_3^n\in\mathcal{X}_3^n$ of the third channel. The same arguments apply for the case of $I\in\mathbb{N}$ transmissions.

Remark 6 The result stated in Theorem 4 is a generalization of the result of Theorem 1 stated in [8]. Indeed, fixing the parameters $\mathsf{R}_{\mathsf{W}_2}=0$ and $\alpha=1$ the system of equations stated in definition 3 reduces to the equations (20) and (21) **or** (22) and (23) where the rates parameters are defined differently $\mathsf{R}_{\mathsf{W}_1}=2\mathsf{R}_{\mathsf{o}}-2\mathsf{R}_{\mathsf{s}}$ and $\mathsf{R}=2\mathsf{R}_{\mathsf{s}}$.

$$\begin{aligned}2\mathsf{R}_{\mathsf{o}} &\leq I(\mathbf{x}_1;\mathbf{y}_1|k_1)-\varepsilon, \quad (20)\\ 2\mathsf{R}_{\mathsf{o}}-2\mathsf{R}_{\mathsf{s}} &\geq I(\mathbf{x}_1;\mathbf{z}_1|k_1)-\varepsilon, \quad (21)\\ 2\mathsf{R}_{\mathsf{o}} &\leq I(\mathbf{x}_1;\mathbf{y}_1|k_1)+I(\mathbf{x}_2;\mathbf{y}_2|k_2)-\varepsilon, \quad (22)\\ 2\mathsf{R}_{\mathsf{o}}-2\mathsf{R}_{\mathsf{s}} &\geq I(\mathbf{x}_1;\mathbf{z}_1|k_1)+I(\mathbf{x}_2;\mathbf{z}_2|k_2)-\varepsilon. \quad (23)\end{aligned}$$

The result stated in Theorem 4 introduces two additional degree of freedom $(\mathsf{R}_{\mathsf{W}_2},\alpha)$ that will be exploited to increase the maximal secrecy throughput.

IV. Secrecy throughput of a SARA-code

In order to define the secrecy throughput of the SARA-code with parameters $(\alpha,\mathsf{R},\mathsf{R}_{\mathsf{W}_1},\mathsf{R}_{\mathsf{W}_2})$, we introduce the information events $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{D}$ given by equations (24), (25), (26), and (27).

$$\begin{aligned}\mathcal{A} &= \left\{\mathsf{R}+\mathsf{R}_{\mathsf{W}_1}\leq I(\mathbf{x}_1;\mathbf{y}_1|k_1)\right\}, \quad (24)\\ \mathcal{B} &= \left\{\mathsf{R}_{\mathsf{W}_1}\geq I(\mathbf{x}_1;\mathbf{z}_1|k_1)\right\}, \quad (25)\\ \mathcal{C} &= \left\{\mathsf{R}+\mathsf{R}_{\mathsf{W}_1}+\mathsf{R}_{\mathsf{W}_2}\leq I(\mathbf{x}_1;\mathbf{y}_1|k_1)+\alpha\cdot I(\mathbf{x}_2;\mathbf{y}_2|k_2)\right\}, \quad (26)\\ \mathcal{D} &= \left\{\mathsf{R}_{\mathsf{W}_1}+\mathsf{R}_{\mathsf{W}_2}\geq I(\mathbf{x}_1;\mathbf{z}_1|k_1)+\alpha\cdot I(\mathbf{x}_2;\mathbf{z}_2|k_2)\right\}. \quad (27)\end{aligned}$$

Events $\mathcal{A}$ and $\mathcal{C}$ are decoding events and events $\mathcal{B}$ and $\mathcal{D}$ are secrecy leakage events.

Definition 7 *The connection outage probability $\mathcal{P}_{\mathsf{co}}$ and secrecy outage probability $\mathcal{P}_{\mathsf{so}}$ are defined by equations (28) and (29).*

$$\begin{aligned}\mathcal{P}_{\mathsf{co}} &= \mathcal{P}\left(\mathcal{A}^c\cap\mathcal{C}^c\right), \quad (28)\\ \mathcal{P}_{\mathsf{so}} &= \mathcal{P}\left(\mathcal{B}^c\cup\left(\mathcal{A}^c\cap\mathcal{D}^c\right)\right). \quad (29)\end{aligned}$$

Remark 8 Letting the parameters $\mathsf{R}_{\mathsf{W}_2}=0$ and $\alpha=1$, this implies that $\mathcal{A}\subset\mathcal{C}$, $\mathcal{D}\subset\mathcal{B}$ and the definitions of $\mathcal{P}_{\mathsf{co}}$ and $\mathcal{P}_{\mathsf{so}}$ reduce to equations (21) and (22) in [8].

Definition 9 *The maximal secrecy throughput is defined by equation (30) and it measures the expected number of bits decoded by the legitimate decoder per channel use.*

$$\begin{aligned}\eta &= \max_{\mathsf{R},\mathsf{R}_{\mathsf{W}_1},\mathsf{R}_{\mathsf{W}_2},\alpha}\left(\frac{\mathsf{R}\cdot(1-\mathcal{P}_{\mathsf{co}})}{1+\alpha\cdot(1-\mathcal{P}(\mathcal{A}))}\right), \quad (30)\\ &\text{s.c.} \begin{cases}\mathcal{P}_{\mathsf{co}} &\leq \xi_{\mathsf{c}},\\ \mathcal{P}_{\mathsf{so}} &\leq \xi_{\mathsf{s}}.\end{cases}\end{aligned}$$

The maximum is taken over the parameters R, $\mathsf{R}_{\mathsf{W}_1}$, $\mathsf{R}_{\mathsf{W}_2}$, α such that the connection outage probability and the secrecy outage probability are lower than ξ_{c} and ξ_{s}.

V. Numerical Results

We consider an example represented by Fig. 2 where the connection and the secrecy outage probability must be lower than $\xi_{\mathsf{c}}=1/4=0.25$ and $\xi_{\mathsf{s}}=1/8=0.125$. These values are rather large and this is due to the small cardinality of the set of channel states. We investigate the optimal performances of the SARA-code whose existence is stated in Theorem 4 and we compare it to the coding scheme introduced in [8] where the parameters $\mathsf{R}_{\mathsf{W}_2}=0$ and $\alpha=1$ are fixed.

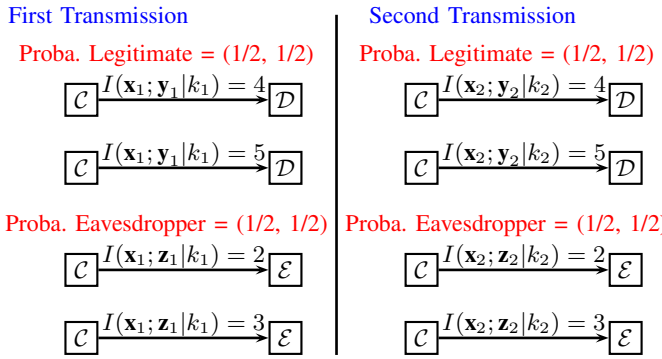

Fig. 2. In both transmissions, the channel of the legitimate decoder takes two possible values $I(\mathbf{x}_1;\mathbf{y}_1|k_1)\in\{4,5\}$ with probability $(1/2,1/2)$ and the channel of the eavesdropper takes two possible values $I(\mathbf{x}_1;\mathbf{z}_1|k_1)\in\{2,3\}$ with probability $(1/2,1/2)$.

A. Coding Scheme with parameters $(\mathsf{R}_{\mathsf{W}_2},\alpha)=(0,1)$ [8]

Fig. 3 and 4 show that the optimal parameters are $(\mathsf{R},\mathsf{R}_{\mathsf{W}_1})=(3,6)$ and the secrecy throughput is equal to

$$\eta_{\mathsf{p}}=\frac{3\cdot(1-0.25)}{1+1\cdot(1-0)}=\frac{9}{8}=1.125. \quad (31)$$

The parameters are directly adapted to the case of two transmissions. The secrecy rate is very large $\mathsf{R}_{\mathsf{W}_1}=6$, hence the secrecy outage has probability $\mathcal{P}_{\mathsf{so}}=0$. The remaining rate is used to transmit information $\mathsf{R}=3$ and it induces a connection outage probability of $\mathcal{P}_{\mathsf{co}}=0.25$.

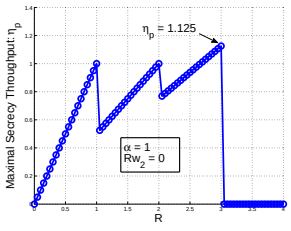

Fig. 3. Throughput η_{p} optimized over $\mathsf{R}_{\mathsf{W}_1}$ depending on the rate parameter R for $(\mathsf{R}_{\mathsf{W}_2}, \alpha) = (0, 1)$.

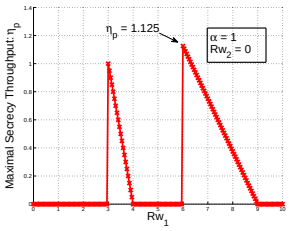

Fig. 4. Throughput η_{p} optimized over R depending on the rate parameter $\mathsf{R}_{\mathsf{W}_1}$ for $(\mathsf{R}_{\mathsf{W}_2}, \alpha) = (0, 1)$.

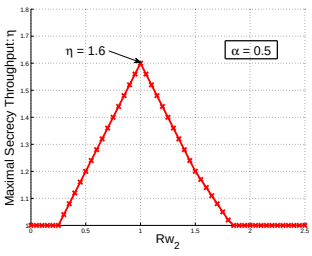

Fig. 7. Maximal secrecy throughput η optimized over $(\mathsf{R}, \mathsf{R}_{\mathsf{W}_1})$ depending on $\mathsf{R}_{\mathsf{W}_2}$ for a fixed $\alpha = 0.5$.

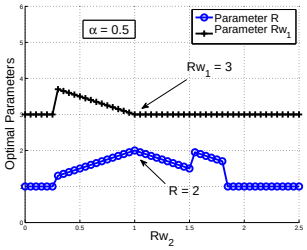

Fig. 8. Optimal $(\mathsf{R}, \mathsf{R}_{\mathsf{W}_1})$ depending on $\mathsf{R}_{\mathsf{W}_2}$ for a fixed $\alpha = 0.5$.

B. SARA-code with parameters $\alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}$

The SARA-code introduces two additional degrees of freedom $(\mathsf{R}_{\mathsf{W}_2}, \alpha)$ that are optimized in order to increase the maximal secrecy throughput.

1) Impact of parameter $\mathsf{R}_{\mathsf{W}_2}$ for a fixed $\alpha = 1$:

- Fig. 5 shows that the maximal secrecy throughput is equal to $\eta = 4/3 \simeq 1.333$ for a range of parameter $\mathsf{R}_{\mathsf{W}_2} \in \{2, 3\}$ and for a fixed parameter $\alpha = 1$.
- Fig. 6 shows that the corresponding optimal parameters are $(\mathsf{R}, \mathsf{R}_{\mathsf{W}_1}) = (2, 3)$.

The secrecy outage probability is equal to $\mathcal{P}_{\mathsf{so}} = 1/8 = 0.125$ and the connection outage probability is equal to $\mathcal{P}_{\mathsf{co}} = 0$. The SARA-code allows to split the secrecy constraints over two parameters $(\mathsf{R}, \mathsf{R}_{\mathsf{W}_1}) = (2, 3)$ instead of only one $\mathsf{R}_{\mathsf{W}_1} = 6$. It induces a positive probability of decoding in the first transmission that increase the secrecy throughput.

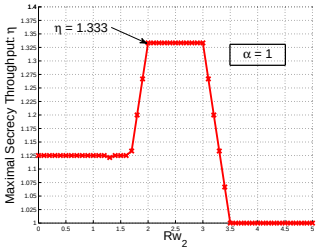

Fig. 5. Maximal secrecy throughput η optimized over $(\mathsf{R}, \mathsf{R}_{\mathsf{W}_1})$ depending on $\mathsf{R}_{\mathsf{W}_2}$ for a fixed $\alpha = 1$.

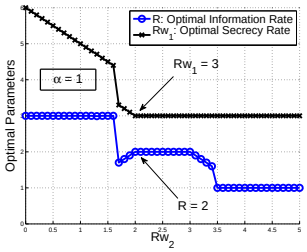

Fig. 6. Optimal $(\mathsf{R}, \mathsf{R}_{\mathsf{W}_1})$ depending on $\mathsf{R}_{\mathsf{W}_2}$ for a fixed $\alpha = 1$.

2) Impact of both additional parameters $(\mathsf{R}_{\mathsf{W}_2}, \alpha)$:

- Fig. 7 shows that the maximal secrecy throughput is equal to $\eta = 1.6$ for optimal parameters $\alpha = 0.5$ and $\mathsf{R}_{\mathsf{W}_2} = 1$.
- Fig. 8 shows that the optimal parameters $(\mathsf{R}, \mathsf{R}_{\mathsf{W}_1}) = (2, 3)$ correspond to the secrecy throughput $\eta = 1.6$.

The secrecy outage probability is equal to $\mathcal{P}_{\mathsf{so}} = 1/8 = 0.125$ and the connection outage probability is equal to $\mathcal{P}_{\mathsf{co}} = 0$. The secrecy rate $\mathsf{R}_{\mathsf{W}_1} = 3$ of the SARA-code is adapted only for the first transmission. With probability $\mathcal{P}(\mathcal{A}) = 1/2$, the transmitted message is correctly decoded after the first transmission. If the second transmission occurs, the parameter $\alpha = 0.5$ reduces appropriately the duration of the second transmission such that the decoder can decode correctly. Hence the secrecy rate for the second transmission can also be reduced to $\mathsf{R}_{\mathsf{W}_2} = 1$ and the maximal secrecy throughput is given by equation (32).

$$\eta = \frac{2 \cdot 1}{1 + 0.5 \cdot (1 - 0.5)} = \frac{8}{5} = 1.6. \tag{32}$$

For this example described by Fig. 2, the SARA-code provides more than 42% of increase compared to the coding scheme presented in [8].

VI. Sketch of the Proof of Theorem 4

Fix the parameters $\varepsilon > 0$, $\alpha \geq 0$, $\mathsf{R} \geq 0$, $\mathsf{R}_{\mathsf{W}_1} \geq 0$, $\mathsf{R}_{\mathsf{W}_2} \geq 0$ and the probability distributions $\mathcal{P}^{\star}_{\mathsf{x}_1} \in \Delta(\mathcal{X}_1)$ and $\mathcal{P}^{\star}_{\mathsf{x}_2} \in \Delta(\mathcal{X}_1)$. Denote $\mathcal{L}'(\varepsilon, \alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}, \mathcal{P}^{\star}_{\mathsf{x}_1}, \mathcal{P}^{\star}_{\mathsf{x}_2})$ the set of channel states $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$ corresponding to two transmissions, that satisfy the equations (33), (34), (35) and (36).

$$\begin{aligned}
\mathsf{R} + \mathsf{R}_{\mathsf{W}_1} + \mathsf{R}_{\mathsf{W}_2} &\leq I(\mathbf{x}_1; \mathbf{y}_1 | k_1) + \alpha \cdot I(\mathbf{x}_2; \mathbf{y}_2 | k_2) - 8\varepsilon(1 + \alpha), && (33)\\
\mathsf{R} + \mathsf{R}_{\mathsf{W}_1} &> I(\mathbf{x}_1; \mathbf{y}_1 | k_1) - 4\varepsilon(1 + \alpha), && (34)\\
\mathsf{R}_{\mathsf{W}_1} + \mathsf{R}_{\mathsf{W}_2} &\geq I(\mathbf{x}_1; \mathbf{z}_1 | k_1) + \alpha \cdot I(\mathbf{x}_2; \mathbf{z}_2 | k_2) - 4\varepsilon(1 + \alpha), && (35)\\
\mathsf{R}_{\mathsf{W}_1} &\geq I(\mathbf{x}_1; \mathbf{z}_1 | k_1) - 4\varepsilon(1 + \alpha). && (36)
\end{aligned}$$

A. Random HARQ-Code

We introduce the concept of random HARQ-code $\mathbf{c} \in \mathcal{C}(n, \alpha, \mathsf{R})$ with stochastic encoder, defined as follows:

- *Random codebook* $\boldsymbol{x}_1^n$. Generate $|\mathcal{M} \times \mathcal{M}_{\mathsf{W}_1}| = 2^{n(\mathsf{R}+\mathsf{R}_{\mathsf{W}_1})}$ sequences $\mathbf{x}_1^n \in \mathcal{X}_1$ drawn from the probability distribution $\mathcal{P}^{\star \otimes n}_{\mathsf{x}_1}$. Randomly bin them into $|\mathcal{M}| = 2^{n\mathsf{R}}$ bins denoted by $m \in \mathcal{M}$, each of them containing $|\mathcal{M}_{\mathsf{W}_1}| = 2^{n\mathsf{R}_{\mathsf{W}_1}}$ sequences $\mathbf{x}_1^n \in \mathcal{X}_1^n$ indexed by the parameter $w_1 \in \mathcal{M}_{\mathsf{W}_1}$.
- *Random codebook* $\boldsymbol{x}_2^{\alpha n}$. Generate $|\mathcal{M} \times \mathcal{M}_{\mathsf{W}_1} \times \mathcal{M}_{\mathsf{W}_2}| = 2^{\alpha n(\mathsf{R}' + \mathsf{R}'_{\mathsf{W}_1} + \mathsf{R}'_{\mathsf{W}_2})}$ sequences $\mathbf{x}_2^{\alpha n} \in \mathcal{X}_2^{\alpha n}$ drawn from the probability distribution $\mathcal{P}^{\star \otimes \alpha n}_{\mathsf{x}_2}$. Randomly bin them into $|\mathcal{M}| = 2^{\alpha n \mathsf{R}'}$ bins denoted by $m \in \mathcal{M}$, each of them containing $|\mathcal{M}_{\mathsf{W}_1} \times \mathcal{M}_{\mathsf{W}_2}| = 2^{\alpha n(\mathsf{R}'_{\mathsf{W}_1} + \mathsf{R}'_{\mathsf{W}_2})}$ sequences $\mathbf{x}_2^{\alpha n} \in \mathcal{X}_2^{\alpha n}$ indexed by a pair of parameters $(w_1, w_2) \in \mathcal{M}_{\mathsf{W}_1} \times \mathcal{M}_{\mathsf{W}_2}$. Each bin $m \in \mathcal{M}$ is divided into $|\mathcal{M}_{\mathsf{W}_2}| = 2^{\alpha n \mathsf{R}'_{\mathsf{W}_2}}$ sub-bins containing $|\mathcal{M}_{\mathsf{W}_1}| = 2^{\alpha n \mathsf{R}'_{\mathsf{W}_1}}$ sequences $\mathbf{x}_2^{\alpha n} \in \mathcal{X}_2^{\alpha n}$. Denote by $w_2 \in \mathcal{M}_{\mathsf{W}_2}$ the index of the sub-bins and by $w_1 \in \mathcal{M}_{\mathsf{W}_1}$ the index of the sequence of symboles $\mathbf{x}_2^{\alpha n}(m, w_1, w_2) \in \mathcal{X}_2^{\alpha n}$.

Remark 10 The parameters R', $\mathsf{R}'_{\mathsf{W}_1}$, $\mathsf{R}'_{\mathsf{W}_2}$ satisfy $n\mathsf{R} = \alpha n \mathsf{R}'$, $n\mathsf{R}_{\mathsf{W}_1} = \alpha n \mathsf{R}'_{\mathsf{W}_1}$ and $n\mathsf{R}_{\mathsf{W}_2} = \alpha n \mathsf{R}'_{\mathsf{W}_2}$.

- *Encoding function over the first channel.* The encoder observes the realization of the message $m \in \mathcal{M}$. It chooses at random the parameter $w_1 \in \mathcal{M}_{\mathsf{W}_1}$ using the uniform probability distribution and sends through the first channel $\mathcal{T}_1$ the sequence of channel inputs $x_1^n(m, w_1)$.
- *Feedback from the decoder.* The decoder observes the realization of the channel state $k_1 \in \mathcal{K}_1$ and send to the encoder the feedback ACK if it can decode after the first transmission (i.e. equation (34) is not satisfied) and it sends the feedback NACK if it can not decode after the first transmission (i.e. equation (34) is satisfied) the transmitted message.
- *Decoding fonction for ACK.* The decoder observes the state parameter $k_1 \in \mathcal{K}_1$ and finds the pair of indexes $(m, w_1) \in \mathcal{M} \times \mathcal{M}_{\mathsf{W}_1}$ such that $x_1^n(m, w_1) \in A_\varepsilon^{\star n}(y_1^n|k_1)$ is jointly typical with the sequence of outputs of the first channel $\mathcal{T}_1$. Its returns the index $m \in \mathcal{M}$ of the transmitted message.
- *Encoding function for NACK.* If the encoder receives a NACK feedback, it chooses at random the parameter $w_2 \in \mathcal{M}_{\mathsf{W}_2}$ using the uniform probability distribution and sends through the second channel $\mathcal{T}_2$ the sequence of channel inputs $x_2^{\alpha n}(m, w_1, w_2)$.
- *Decoding fonction for NACK.* The decoder observes the state parameters $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$ and finds the triple of indexes $(m, w_1, w_2) \in \mathcal{M} \times \mathcal{M}_{\mathsf{W}_1} \times \mathcal{M}_{\mathsf{W}_2}$ such that $x_1^n(m, w_1) \in A_\varepsilon^{\star n}(y_1^n|k_1)$ is jointly typical with the sequence of outputs of the first channel $\mathcal{T}_1$ and such that $x_2^{\alpha n}(m, w_1, w_2) \in A_\varepsilon^{\star \alpha n}(y_2^{\alpha n}|k_2)$ is jointly typical with the sequence of outputs of the second channel $\mathcal{T}_2$. Its returns the index $m \in \mathcal{M}$ of the transmitted message.
- *An error* is declared when the sequences $(x_1^n, y_1^n, z_1^n) \notin A_\varepsilon^{\star n}(\mathcal{Q}_1|k_1)$ or $(x_2^{\alpha n}, y_2^{\alpha n}, z_2^{\alpha n}) \notin A_\varepsilon^{\star \alpha n}(\mathcal{Q}_2|k_2)$ are not jointly typical for the probability distributions $\mathcal{Q}_1 = \mathcal{P}_{\mathsf{x}_1}^\star \otimes \mathcal{T}_1 \in \Delta(\mathcal{X}_1 \times \mathcal{Y}_1 \times \mathcal{Z}_1)$ and $\mathcal{Q}_2 = \mathcal{P}_{\mathsf{x}_2}^\star \otimes \mathcal{T}_2 \in \Delta(\mathcal{X}_2 \times \mathcal{Y}_2 \times \mathcal{Z}_2)$.

B. Expected error probability

Equations (33) and (34) guarantee that the expected error probability of the random HARQ-code $\mathbf{c} \in \mathcal{C}(n, \alpha, \mathsf{R})$ is bounded by ε for all channel states $(k_1, k_2) \in \mathcal{L}'(\varepsilon, \alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}, \mathcal{P}_{\mathsf{x}_1}^\star, \mathcal{P}_{\mathsf{x}_2}^\star)$.

$$\mathbb{E}_c\left[\mathcal{P}_{\mathsf{e}}\left(\mathbf{c}\middle|k_1, k_2\right)\right] \leq 4\varepsilon. \tag{37}$$

C. Expected information leakage rate

Equations (35) and (36) guarantee that the expected error probability of the random HARQ-code $\mathbf{c} \in \mathcal{C}(n, \alpha, \mathsf{R})$ is bounded by ε for all channel states $(k_1, k_2) \in \mathcal{L}'(\varepsilon, \alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}, \mathcal{P}_{\mathsf{x}_1}^\star, \mathcal{P}_{\mathsf{x}_2}^\star)$.

$$\mathbb{E}_c\left[\mathcal{L}_{\mathsf{e}}\left(\mathbf{c}\middle|k_1, k_2\right)\right] \leq \varepsilon \cdot \left(9 + 8\alpha + 10\log_2|\mathcal{X}_1| + 15\alpha \cdot \log_2|\mathcal{X}_2|\right). \tag{38}$$

D. Conclusion

The above result can be extended for all channel states $(k_1, k_2) \in \mathcal{L}(\varepsilon, \alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}, \mathcal{P}_{\mathsf{x}_1}^\star, \mathcal{P}_{\mathsf{x}_2}^\star)$. Define ε' in terms of ε in the following manner:

$$\varepsilon' \quad = \quad 4\varepsilon + \varepsilon \cdot \left(9 + 8\alpha + 10\log_2|\mathcal{X}_1| + 15\alpha \cdot \log_2|\mathcal{X}_2|\right)$$

The random HARQ-code with stochastic encoder $\mathbf{c} \in \mathcal{C}(n, \alpha, \mathsf{R})$ satisfies the following equations for all channel states $(k_1, k_2) \in \mathcal{L}(\varepsilon, \alpha, \mathsf{R}, \mathsf{R}_{\mathsf{W}_1}, \mathsf{R}_{\mathsf{W}_2}, \mathcal{P}_{\mathsf{x}_1}^\star, \mathcal{P}_{\mathsf{x}_2}^\star)$.

$$\begin{aligned} & \mathbb{E}_c\left[\mathcal{P}_{\mathsf{e}}\left(\mathbf{c}\middle|k_1, k_2\right)\right] + \mathbb{E}_c\left[\mathcal{L}_{\mathsf{e}}\left(\mathbf{c}\middle|k_1, k_2\right)\right] && \leq \varepsilon' \\ \Longrightarrow \quad & \exists c^\star \in \mathcal{C}(n, \alpha, \mathsf{R}), \quad \left[\mathcal{P}_{\mathsf{e}}\left(c^\star\middle|k_1, k_2\right) + \mathcal{L}_{\mathsf{e}}\left(c^\star\middle|k_1, k_2\right)\right] && \leq \varepsilon'. \end{aligned}$$

This proves the existence of a HARQ-code $c^\star \in \mathcal{C}(n, \alpha, \mathsf{R})$ such that equations $\mathcal{P}_{\mathsf{e}}(c^\star|k_1, k_2) \leq \varepsilon'$ and $\mathcal{L}_{\mathsf{e}}(c^\star|k_1, k_2) \leq \varepsilon'$. The full version of the proof is available in [10].

VII. Conclusion

This paper is devoted to the problem of HARQ protocols under a secrecy constraint. The objective is to provide a coding scheme that satisfies both reliability and confidentiality conditions. We provide a new coding scheme that involves Secrecy Adaptation and Rate Adaptation and we called it SARA-code. The first contribution is to prove that the SARA-code has small error probability and small information leakage rate. The second contribution is to show that the secrecy throughput of the SARA-code is greater than those stated in the related literature. Block fading Gaussian channels will be considered in a future extension of this work.

References

[1] G. Caire and D. Tuninetti, "Throughput of hybrid-ARQ protocols for gaussian collision channel," *IEEE Trans. Inf. Theory*, vol. 47, pp. 1971–1988, July 2001.

[2] D. Djonin, A. Karmokar, and V. Bhargava, "Joint rate and power adaptation for type-I hybrid ARQ systems over correlated fading channels under different buffer-cost constraints," *IEEE Trans. Veh. Technol.*, vol. 57, pp. 421– 435, Jan. 2008.

[3] E. Visotsky, S. Yakun, V. Tripathi, M. Honig, and R. Peterson, "Reliability-based incremental redundancy with convolutional codes," *IEEE Trans. Commun.*, vol. 53, pp. 987 – 997, June 2005.

[4] S. Pfletschinger and M. Navarro, "Adaptive HARQ for imperfect channel knowledge," in *Source and Channel Coding (SCC), 2010 Internat. ITG Conference on*, pp. 1–6, Jan. 2010.

[5] E. Uhlemann, L. Rasmussen, A. Grant, and P. Wiberg, "Optimal incremental-redundancy strategy for type-II hybrid ARQ," in *Inf. Theory, 2003. Proceedings. IEEE Internat. Symposium on*, 2003.

[6] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[8] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, pp. 1575 – 1591, Aug. 2009.

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

[10] M. Le Treust, "Technical report on security & rate adaptations for secure HARQ protocols," Tech. Rep., https://sites.google.com/site/maelletreust/A.pdf?attredirects=0&d=1, Apr. 2013.