Rate Adaptation for Secure HARQ Protocols

Maël Le Treust, Leszek Szczecinski* and Fabrice Labeau†
ETIS, UMR 8051 / ENSEA, Université Cergy-Pontoise, CNRS,
6, avenue du Ponceau, 95014 Cergy-Pontoise CEDEX, FRANCE
* INRS, Montreal, Canada
† McGill University, Montreal, Canada
mael.le-treust@ensea.fr, leszek@emt.inrs.ca, fabrice.labeau@mcgill.ca

Abstract—This paper investigates secure transmission using HARQ protocol when the encoder only knows the statistics of the channel-state. We analyze the tradeoff between reliability and secrecy probabilistic guarantees. The conventional approach of ensuring the secrecy via introduction of dummy-message is followed. However, unlike the previous works on this subject, we design a coding strategy tailored to HARQ by splitting the dummy-message rate over several rate parameters. These additional degrees of freedom improve the matching between the dummy-message rates and the realizations of the eavesdropper channels. We evaluate the performance in terms of secrecy outage probability, connection outage probability and secrecy throughput. For Rayleigh fading channel, the splitting of the dummy-message rate provides higher secrecy throughput and lower expected duration/average delay.

Index Terms—hybrid automatic repeat request, physical layer security, state-dependent wiretap channel, channel state information, secrecy outage probability and secrecy throughput.

I. INTRODUCTION

This work is concerned with the transmission of information over wireless block-fading channels, where the channel state information (CSI), which captures the essence of channel statistics, is not available at the transmitter but can be estimated by the receivers. In such a scenario, the transmission is inherently i) unreliable due to unpredictable fading, and ii) unsecure due to possibility of eavesdropping when communicating over broadcasting medium. The successful communication and the secrecy can thus only be defined/guaranteed in probabilistic terms. The principal question we want to investigate is how the constraints on the secrecy and the reliability are related when transmissions are carried out using hybrid automatic repeat request (HARQ) protocol, and how to construct the coding to take advantage of the additional dimension offered by retransmissions.

A. State of art

Reliability and HARQ
Reliability is a key issue for modern communications and is deeply related to the knowledge—by the transmitters—of the channel statistics often summarized in one parameter, which defines the CSI, e.g., the signal-to-noise ratio (SNR). When both encoder and decoder know the CSI it is possible to design an appropriate coding scheme that conveys reliably a maximal number of information bits [2]. When the CSI is unavailable at the transmitter, the successful transmission cannot be guaranteed leading to the concepts of outage probability and throughput.

To deal with the unavoidable transmission errors, the so-called hybrid automatic repeat request (HARQ) protocol is often used: a single-bit acknowledgement feedback Ack/Nack indicates whether the decoding was successful or not. Then, the transmitter may transmit the same message many times, till it is successfully received—the event indicated by the Ack. HARQ protocols was analyzed in the literature from the point of view of throughput, outage probability, and average delay [3]–[8].

Retransmissions in HARQ provide additional dimensions which can be exploited to design a code which provides a good “match” between the transmission rate and the channel realizations. For example, in [9]–[18], codewords-length was varied throughout the retransmissions. A different approach was taken by [19]–[25] which kept the codeword length constant and rather relied on the design of new coding schemes to increase the throughput.

Secrecy
Confidentiality issue arises in wireless communications due to the broadcast nature of the transmission medium. An eavesdropper within the communication range can “overhear” the transmitted signals and extract some private information.

Instead of using cryptographic methods to protect the message, Wyner [26] proposed to exploit the difference of quality between the channel of the legitimate decoder and of the eavesdropper, and characterized the rate at which the legitimate users can communicate securely and reliably. These results were further generalized in [27], [28] under assumption of CSI knowledge, which has a significant impact on security in wireless network [29]. In [30], the authors proved that secure communication is possible even when the eavesdropper has, on average, a channel stronger than that of the receiver. However, the legitimate users must have perfect knowledge of their CSI and estimate the CSI of the eavesdropper. In [31], the problem of broadcasting confidential messages to multiple receivers over parallel and fast-fading channels was investigated while [32] characterizes the secrecy capacity of slow-fading wiretap channel under different CSI assumptions. The ergodic secrecy
capacity was characterized in [33] assuming full CSI at both legitimate transmitters.

The assumption of the knowledge of the eavesdropper’s CSI is an idealization. So [34] studied the case where the channel to the eavesdropper experiences fading not known to the legitimate users. The effect of partial CSI on achievable secure communication rates and on secret-key generation was also investigated in [35, 36] and provided bounds on the ergodic secrecy capacity. The case of transmission without CSI at the encoder was investigated in [37], where the ergodic secrecy capacity for fast fading wiretap channel was characterized; and in [38], which proposed an alternative secrecy outage formulation to measure the probability that message transmission fails to achieve perfect secrecy.

Secrecy and HARQ
Retransmissions in HARQ may be used not only to increase the reliability or the throughput, but also to increase the secrecy. This issue was investigated in [39] using extension of the Wyner code [26] with the introduction of dummy messages. In the absence of the CSI, the coding parameters were chosen using the statistics of the CSI. Then, receiving a Nack feedback, the encoder retransmit the message but has no guarantee of reliability nor secrecy which are then characterized via random events of the secrecy outage and the connection outage. Improvement of the secure HARQ protocol was investigated in [40, 41] with variable-length coding, in [42] with substitution of the dummy-messages at each transmission and in [43] using low-density parity-check (LDPC) code.

B. Contributions and organizations
A natural trade-off arises between reliability and security in the wiretap channel: when the dummy-message rate increases, it decreases the secrecy outage probability but increases the connection outage probability. One important drawback of the coding schemes proposed in [39], is that the dummy-message rate is unique and should guarantee the secrecy for a large number of possible transmissions, even if the expected duration/average delay of the transmission is much lower [11]. In this work, we address this issue upfront and design an original wiretap code by splitting the dummy-message rate over several rate parameters. These additional degrees of freedom improve the matching between the dummy-message rates and the realization of the eavesdropper channel. The contributions of this work are the following:

- We propose a new wiretap code, called “Adaptation-Secrecy-Rate-code” (ASR-code) and we prove it has an arbitrarily small error probability and an arbitrarily small information leakage rate, for a whole set of channel states.
- We characterize the trade-off between connection and secrecy outage probabilities and show the optimal rate allocation for discrete channels and for Rayleigh fading channel with one transmission.
- We present a numerical optimization for multiple transmissions over Rayleigh fading channel: using the splitting of the dummy-message rate, we achieve a higher throughput with a lower expected duration/average delay.

The work is organized as follows. Section II presents the channel model under investigation and the concept of HARQ-code. The ASR-code is described in Sec. III and Theorem IV proves the error probability and the leakage rate converge to zero for large block-length. The performance of the ASR-code is measured by the secrecy throughput and the secrecy/connection outage probability, defined in Sec. [V]
Discrete channel-states are investigated in Section [V] and Rayleigh fading channel are investigated in Sec. [VI]. Section VII concludes the article and the proofs of the results are stated in the Appendix.

II. SECURITY FOR HARQ
We consider a HARQ protocol with L possible transmissions shown schematically in Fig. I for L = 2. Each transmission \( i \in \{1, \ldots, L\} \) corresponds to a block of \( n \in \mathbb{N} \) symbols. Capital letter \( X \) denotes the random variable, lowercase letter \( x \in X \) denotes the realization and \( X^n \) denotes the n-time cartesian product of the set \( X \). The random message \( m \in M \) is uniformly distributed and \( m \in M \) denotes the realization.

During the first transmission, the encoder \( C \) uses the sequence of input symbols \( x^n_i \in X^n \) in order to transmit the message \( m \in M \) to the legitimate decoder \( D \). The decoder \( D \) (resp. eavesdropper \( E \)) observes the sequence of channel outputs \( y^n_i \in Y^n \) (resp. \( z^n_l \in Z^n \)) and tries to decode (resp. to infer) the transmitted message \( m \in M \). The decoder \( D \) sends a Ack\(_{i}/\text{Nack}\) feedback over a perfect channel that indicates to the encoder, whether the first transmission was correctly decoded or not.

If the encoder receives a Nack\(_{i−1} \) feedback after \( l−1 \in \{1, \ldots, L\} \) transmissions, then the message \( m \in M \) was not correctly decoded yet. The encoder starts retransmit the message \( m \in M \) over transmission \( l \in \{1, \ldots, L\} \) with input sequence \( x^n_i \in X^n \). The decoder \( D \) (resp. eavesdropper \( E \)) tries to decode (resp. to infer) the transmitted message \( m \in M \) from sequences of channel outputs \( (y^n_1, y^n_2, \ldots, y^n_l) \in Y^{l \times n} \) (resp. \( (z^n_1, z^n_2, \ldots, z^n_l) \in Z^{l \times n} \)), where \( Y^{l \times n} = Y^n \times \cdots \times Y^n \) is the l-time Cartesian product of set \( Y^n \). If the maximal number of transmissions \( L \) is attained, the encoder drops message \( m \in M \) and starts sending the next message \( m' \in M \). The notation \( \Delta(X) \) stands for the set of the probability distributions \( \mathcal{P}(X) \) over the set \( X \).

We assume that the channel is memoryless with transition probability \( T(y, z|x, k) \) depending on a state parameter \( k \in K \), for example a fading coefficient. The state parameters \( (k_1, k_2, \ldots, k_L) \in K^L \) stay constant during the transmission block of \( n \in \mathbb{N} \) symbols and are chosen at random with i.i.d. probability distribution \( \mathcal{P}_k \in \Delta(K) \), from one block to another. The state parameters \( (k_1, k_2, \ldots, k_L) \in K^L \) are observed by the decoder and the eavesdropper but not by the encoder.

\[
T^n(y^n_i, z^n_i|x^n_i, k_l) = \prod_{i=1}^{n} T(y(i), z(i)|x(i), k_l). \tag{1}
\]
and are feedback to the encoder
\[ R \leq \text{transmissions}. \]

After the end of the first transmission, the decoder \( D \) sends a Ack/Nack feedback to the encoder \( C \). The second transmission starts if the encoder \( C \) receives a Nack feedback from the legitimate decoder. The state parameters \( k_1 \in K_1 \) and \( k_2 \in K_2 \) are chosen arbitrarily, stay constant during the transmission and are available only at the legitimate decoder \( D \) and at the eavesdropper \( E \).

At transmission \( l \in \{1, \ldots, L\} \), the state-dependent wiretap channel is given by equation (1) and its statistics are known by both encoder \( C \) and decoder \( D \).

**Definition 1** A HARQ-code \( c_n \in \mathcal{C}(n, R, L) \) with stochastic encoder is a vector of encoding and decoding functions \( c_n = (f_l)_l \subset \mathcal{C}(n, R, L) \), defined for each transmission \( l \in \{1, \ldots, L\} \) by:
\[
\begin{align*}
 f_l : & \mathcal{X}^{(l-1) \times n} \times \{\text{Ack}, \text{Nack}\} \times \mathcal{Y}^{l-1} \rightarrow \mathcal{X}^n, \\
 g_l : & \mathcal{Y}^{l-1} \times k^l \rightarrow \mathcal{X}^{n} \times \{\text{Ack}, \text{Nack}\},
\end{align*}
\]
where the rate \( R \) defines the cardinality \( |M| = 2^{nR} \) of the set of messages \( M \) and \( L \) is the maximal number of transmissions. We denote by \( \mathcal{C}(n, R, L) \), the set of HARQ-code with stochastic encoder.

**Definition 2** For each vector of state parameters \( (k_1, \ldots, k_L) \in \mathcal{K}^L \), the error probability \( P_\theta \) and the information leakage rate \( L_\theta \) of the HARQ-code \( c_n \in \mathcal{C}(n, R, L) \) are defined by:
\[
\begin{align*}
 P_\theta(c_n | k_1, \ldots, k_L) = & \mathcal{P}(M \neq \hat{M} | c_n, k_1, \ldots, k_L), \\
 L_\theta(c_n | k_1, \ldots, k_L) = & \frac{1}{n} \mathcal{I}(M; Z_n^1, \ldots, Z_n^L | c_n, k_1, \ldots, k_L).
\end{align*}
\]
The random variable \( \hat{M} \) denotes the output message of the decoder. Depending on the number of transmissions \( l \in \{1, \ldots, L\} \), it is given by \( \hat{M} = g_l(Y_1^n, \ldots, Y_l^n, k_1, \ldots, k_l) \).

In [26], the authors prove the existence of a HARQ-code that has small error probability and small information leakage rate for a whole range of channel states \( (k_1, \ldots, k_L) \in \mathcal{K}^L \). The coding scheme is based on Wyner’s coding for the wiretap channel [26] and involves two parameters. The rate \( R_s \geq 0 \) is called the “secretary rate” and corresponds to the amount of secret information to be transmitted to the legitimate decoder.

The rate \( R_0 \geq 0 \) corresponds to the total size of the codebook. The difference \( R_0 - R_s \geq 0 \) is called the “dummy-message rate” and corresponds to the amount of randomness that will be introduced in the codebook, in order to confuse the eavesdropper. Definition 2 in [39] provides the normalized versions of equations (1) and (2). This conditions are sufficient for the transmission to be reliable and secure.

\[
R_0 \leq \sum_{j \in \hat{M}} I(X_j; Y_j | k_j),
\]
\[
R_0 - R_s \geq \sum_{j \in \hat{M}} I(X_j; Z_j | k_j).
\]

**III. VARIABLE-RATE SECURE HARQ**

Equation (3) imposes a strong condition on the dummy-message rate \( R_0 - R_s \) since it should be adapted to the maximal number of transmissions \( L \). The high value of \( R_0 - R_s \) prevents the first transmissions to be reliable, especially when the number of possible transmission \( L \) is large. In this work, we split the dummy-message rate \( R_0 - R_s \) over \( L \) different parameters denoted by \( R_1, R_2, \ldots, R_L \). When only two transmissions occur, the secrecy constraints will only depends on the first two rates \( (R_1, R_2) \) and not on the rates \( R_3, \ldots, R_L \). Splitting the dummy-message rate makes the first transmissions more reliable. The price is paid by a more complex encoding/decoding; also the outage analysis is more involved, since the \( L \) dummy-message rate parameters induce \( L \) constraints, stated in equations (7) - (9) of Definition 3.

**Definition 3 (Channel States)** For fixed number of transmissions \( l \in \{1, \ldots, L\} \), fixed parameters \( \varepsilon, R, R_1, \ldots, R_L \) and a fixed probability distributions \( P^*_r \in \Delta(X) \), the set of secure channel states, denoted by \( S_l(\varepsilon, R, R_1, \ldots, R_L, P^*_r) \), is the union of channel states \( (k_1, \ldots, k_l) \in \mathcal{K}^l \) that satisfy equations (6) - (9).

\[
R + \sum_{j \in \hat{M}} R_j \leq \sum_{j \in \hat{M}} I(X_j; Y_j | k_j) - \varepsilon,
\]
\[
\sum_{j \in \hat{M}} R_j \geq \sum_{j \in \hat{M}} I(X_j; Z_j | k_j) - \varepsilon,
\]
\[
\sum_{j \in \hat{M}} I(X_j; Z_j | k_j) - \varepsilon.
\]

Equation (6) guarantees the correct decoding whereas equations (6) - (9) guarantee that the secrecy condition is satisfied at each transmission \( l \in \{1, \ldots, L\} \). These conditions are represented in Fig. 2 for \( L = 2 \) transmissions. Fixing the parameters \( R_2 = \ldots = R_L = 0 \), the system of equations (6) - (9) reduces to equations (4) and (5) where the rates parameters are defined by \( R_1 = R_0 - R_s \) and \( R = R_s \). The splitting of the dummy-message rate introduces additional degrees of freedom \( R_2, \ldots, R_L \) that will be exploited to increase the
performs of the protocol, in terms of secrecy throughput, connection and secrecy outages. We prove that there exists a HARQ-code that satisfies the secrecy and reliability conditions for all tuples of channel states that belong to: \( (k_1, \ldots, k_L) \in \bigcup_{l=1}^{L} S_l(v, R, R_1, \ldots, R_L, P^*_x) \).

Fig. 2. Decoding and secrecy regions corresponding to the rates \((R, R_1, R_2)\), for \( L = 2 \) transmissions. The second transmission starts only if there is a Nack\(_1\) feedback, hence we disregard the dashed region of Ack\(_1\). The green upper region corresponds to the decoding constraint of equation (8) for the mutual informations \( I(X_1; Y_1|k_1) \) and \( I(X_2; Z_2|k_2) \). The red lower region corresponds to the secrecy constraints of equations (7), (8) for the mutual informations \( I(X_1; Z_1|k_1) \) and \( I(X_2; Z_2|k_2) \).

Theorem 4 (Compound Wiretap Channel) Fix the parameters \( R, R_1, \ldots, R_L \) and the input probability distribution \( P^*_x \in \Delta(\mathcal{X}) \). 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 \( c^*_n \in C(n, R, L) \) that satisfies equations (10), for all channel states \((k_1, \ldots, k_L) \in \bigcup_{l=1}^{L} S_l(v, R, R_1, \ldots, R_L, P^*_x) \).

The proof of Theorem 4 is provided in Appendix A. Theorem 4 guarantees the existence of a sequence of HARQ-codes \( c^*_n \) with \( c^*_n \in C(n, R, L) \), such that the probability error and the information leakage rate converge to zero for a whole range of channel states.

Remark 5 The result stated in Theorem 4 is a generalization of the result of Theorem 1 stated in [39]. Indeed, both results coincide when we choose the rate parameters \( R_2 = \ldots = R_L = 0 \). However, the achievability proof, especially the codebook construction, are different.

In the rest of this article, the optimal sequence of HARQ-codes \( c^*_n = (c^*_n)_{n \geq 1} \) is called "Adaptation-Secrecy-Rate-code" (ASR-code) with parameters \( R, R_1, \ldots, R_L \). The additional degrees of freedom \( R_2, \ldots, R_L \) introduced by the ASR-code will be exploited to increase the secrecy throughput and to lower the expected number of transmission and the connection and secrecy outages.

IV. SECRECY THROUGHPUT, CONNECTION AND SECRECY OUTAGES

The channels under investigation are controlled by a state parameter \( k \in K \) observed by the decoder and by the eavesdropper but not by the encoder. We investigate the secure transmission over this state-dependent wiretap channel based on the outage approach. In this setting, the quality of the channel of the eavesdropper is not known by the legitimate encoder and decoder. We introduce the events \( (A_l)_{l \in \{1, \ldots, L\}} \) corresponding to the correct decoding (11) and the events \( (B_l)_{l \in \{1, \ldots, L\}} \) corresponding to the secret transmission (12).

\[
A_l = \left\{ \sum_{j=1}^{L} R_j \leq \sum_{j=1}^{L} I(X_j; Y_j|k_j) \right\}, \quad (11)
\]

\[
B_l = \left\{ \sum_{j=1}^{L} R_j \geq \sum_{j=1}^{L} I(X_j; Z_j|k_j) \right\}, \quad (12)
\]

Definition 6 The connection outage probability \( P_{\text{co}} \) and secrecy outage probability \( P_{\text{so}} \) are defined by:

\[
P_{\text{co}} = P\left( \bigcup_{l=1}^{L} A_l \right), \quad P_{\text{so}} = P\left( \bigcup_{l=1}^{L} B_l \right). \quad (13)
\]

A connection outage occurs if for all transmissions \( l \in \{1, \ldots, L\} \), the decoding event \( A_l \) is not satisfied. A secrecy outage occurs if there exists a transmission \( l \in \{1, \ldots, L\} \), for which the secrecy event \( B_l \) is not satisfied.

Remark 7 Notation \( A^c \) stands for the complement of \( A \). Letting the parameters \( R_2 = \ldots = R_L = 0 \), this implies that \( A_{l-1} \subset A_l \), \( B_l \subset B_{l-1} \) and the definitions of \( P_{\text{co}} \) and \( P_{\text{so}} \) reduce to equations (21) and (22) in [39].

We denote by \( L \in \{1, \ldots, L\} \), the random number of transmission that depends on channel states parameters \((k_1, \ldots, k_L)\) and rate parameters \((R, R_1, \ldots, R_L)\).

\[
P(L = 1) = P(A_1), \quad (14)
\]

\[
P(L = l) = P\left( \bigcap_{j=1}^{l-1} A_j \cap A_l \right), \quad \forall l \in \{2, \ldots, L - 1\}
\]

\[
= P\left( \bigcap_{j=1}^{l-1} A_j \right) - P\left( \bigcap_{j=1}^{l-1} A_j \right), \quad (15)
\]

\[
P(L = L) = P\left( \bigcap_{j=1}^{L-1} A_j \right). \quad (16)
\]

The expected number of transmissions \( E[L] \) is given by:

\[
E[L] = \sum_{l=1}^{L} l \cdot P(L = l) = 1 + \sum_{l=1}^{L-1} P\left( \bigcap_{j=1}^{l-1} A_j \right). \quad (17)
\]

When the random events \( (B_l)_{l \in \{1, \ldots, L\}} \) are independent of the random events \( (A_l)_{l \in \{1, \ldots, L\}} \), we reformulate the secrecy outage probability \( P_{\text{so}} \). This hypothesis is satisfied by the discrete channels of Sec. V and by the Gaussian wiretap channel with Rayleigh block fading of Sec. VI.
Proposition 8 Suppose that the random events \((B_i)_{i \in \{1, \ldots, L\}}\) are independent of the random events \((A_i)_{i \in \{1, \ldots, L\}}\). The secrecy outage probability writes:

\[
P_{so} = 1 - \frac{1}{L} \sum_{j=2}^{L-1} P\left( \bigcap_{i=1}^{j} B_i \right) \cdot P\left( \bigcap_{i=1}^{j-1} A_i \right) - P\left( \bigcap_{i=1}^{j} A_i \right)
\]

\[
- P\left( B_1 \right) \cdot P\left( A_1 \right) - P\left( \bigcap_{i=1}^{L-1} B_i \right) \cdot P\left( \bigcap_{i=1}^{L-1} A_i \right).
\]

Proof of Prop. 8 is stated in App. B. Since the number of transmissions \(L\) is a random variable, the expected number of bits correctly decoded is given by the Renewal-Reward Theorem \([44], [4]\). The performance of the HARQ protocol is evaluated in terms of secrecy throughput, stated in Definition 9. It is equal to the ratio between the expected information rate \(E[R]\) and the expected number of transmissions \(E[L]\), stated in equation (17).

Definition 9 Fix the outages parameters \((\xi_c, \xi_e)\). The secrecy throughput is defined by equation (19) and measures the expected number of bits correctly decoded by the legitimate decoder per channel use.

\[
\eta = \max_{n_1, \ldots, n_L} \frac{E[R]}{E[L]} = \max_{n_1, \ldots, n_L} \frac{R \cdot (1 - P_{so})}{1 + L - 1 \cdot P\left( \bigcap_{i=1}^{L} A_i \right)},
\]

subject to \(P_{so} \leq \xi_c, P_{so} \leq \xi_e\). The maximum is taken over the parameters \(R, R_1, \ldots, R_L\), such that the connection outage probability and the secrecy outage probability are lower than \(\xi_c, \xi_e\).

Fig. 3. In both transmissions, the capacity of the channel to the legitimate decoder takes two possible values \(\{4, 5\}\) with probability \((1/2, 1/2)\) and the capacity of the channel to the eavesdropper takes two possible values \(\{2, 3\}\) with probability \((1/2, 1/2)\).

V. AN INTUITION WITH DISCRETE CHANNEL STATES

We consider the scenario represented by Fig. 3, in which the channel states of the legitimate and of the eavesdropper are discrete and uniformly distributed over \(\{k^v, k'^v\}\) and \(\{k^e, k'^e\}\). We assume the connection and the secrecy outage probability must be lower than \(\xi_c = 1/4 = 0.25\) and \(\xi_e = 1/8 = 0.125\) for \(L = 2\) possible transmissions. We investigate the optimal performances of the ASR-code whose existence is stated in Theorem 4 and we compare it to the coding scheme introduced in [39], in which the dummy-message rate \(R_2 = 0\) is zero.

A. ASR-code with optimization over \(R_1\) only

We consider the framework of [39] where the second dummy-message rate is null \(R_2 = 0\). The optimal dummy-message rate \(R^*_1 = 6\) is high since it must be adapted to two transmissions. This prevents the first transmission to be decoded correctly. Fig. 4 and 5 show that the optimal parameters are \((R^0, R^*_1) = (3, 6)\). The probability of having a NACK after the first transmission is equal to: \(P(\text{NACK}_1) = 1\). The secrecy throughput is equal to

\[
\eta = \frac{3 \cdot (1 - 0.25)}{1 + 1 \cdot (1 - 0)} = \frac{9}{8} = 1.125.
\]

The secrecy outage has probability \(P_{so} = 0\), since the dummy-message rate \(R^*_1 = 6\) is larger than the two best channels of the eavesdropper. The optimal secrecy rate is \(R^0 = 3\) and it induces a connection outage probability of \(P_{co} = 0.25\).

B. ASR-code with optimization over both \(R_1\) and \(R_2\)

We consider the framework of [39] with \(R_2 = 0\). The optimal dummy-message rate \(R^*_1 = 6\) is high since it must be adapted to two transmissions. This prevents the first transmission to be decoded correctly. Fig. 4 and 5 show that the optimal parameters are \((R^0, R^*_1) = (3, 6)\). The secrecy outage has probability \(P_{so} = 0\), since the dummy-message rate \(R^*_1 = 6\) is larger than the two best channels of the eavesdropper. The optimal secrecy rate is \(R^0 = 3\) and it induces a connection outage probability of \(P_{co} = 0.25\).

- Fig. 6 shows that the secrecy throughput is equal to \(\eta = 4/3 \approx 1.333\) for a range of parameter \(R^*_1 \in [2, 3]\). In this interval the secrecy outage probability \(P_{so} \leq \xi_e = 1/8 = 0.125\) satisfies the constraint, the connection outage probability is equal to \(P_{co} = 0\) and \(P(\text{ACK}_1) = 0.5\) stay constant. Hence the secrecy throughput is constant for \(R^*_1 \in [2, 3]\).
- Fig. 7 shows that the corresponding optimal parameters are \((R^0, R^*_1) = (2, 3)\).

The secrecy outage probability is equal to \(P_{so} = 1/8 = 0.125\) and the connection outage probability is equal to \(P_{co} = 0\).

\[
\eta = \frac{2 \cdot (1 - 0.5)}{1 + (1 - 0.5)} = \frac{4}{3} \approx 1.333.
\]

The ASR-code allows to split the secrecy constraint over two parameters \((R^0, R^*_1) = (3, 2)\) instead of only \(R^*_1 = 6\). It induces a positive probability of decoding in the first transmission \(P(\text{ACK}_1) = 0.5\), that increases the secrecy throughput.
For this example described by Fig. 3, the ASR-code provides more than 18, 5% of increase compared to the approach of [39], with a secrecy rate $R^* = 2$ lower than $R^0 = 3$.

VI. RAYLEIGH BLOCK FADING GAUSSIAN WIRETAP CHANNEL

We consider the Gaussian wiretap channel with Rayleigh block fading defined by (22) and represented in Fig. 8

$$Y = h_d \cdot X + N_d, \quad Z = h_e \cdot X + N_e.$$  \tag{22} 

$N_d$ and $N_e$ are independent and i.i.d. $\mathcal{N}(0, 1)$ additive white Gaussian noise. We assume a normalized power constraint on the channel input $E[|X|^2] \leq P = 1$. The state parameters

$$L = 1 \text{ transmission. The connection outage and the secrecy outage probabilities are stated in equations (26) and (27).}$$

$$P_{co} = P\left(R + R_1 > I(X; Y|h_d)\right) = 1 - e^{-\frac{R + R_1}{\gamma_d}}, \tag{26}$$  $$P_{so} = P\left(R_1 < I(X; Z|h_e)\right) = e^{-\frac{R_1}{\gamma_e}}. \tag{27}$$

The outage parameters $\xi_c$ and $\xi_s$ are not always compatible since the outage constraints $P_{co} \leq \xi_c$ and $P_{so} \leq \xi_s$ may not be satisfied simultaneously. We characterize the trade-off between connection outage probability and secrecy outage probability.

Theorem 10 Consider the case of $L = 1$ transmission.

- Outage parameters $\xi_c$ and $\xi_s$ are compatible if and only if:

$$\xi_s \geq \left(1 - \xi_c\right)^{\frac{\gamma_d}{\gamma_e}} \iff \xi_s^{\gamma_d} - (1 - \xi_c)^{\gamma_d} \geq 0. \tag{28}$$

- For a fixed secrecy rate $R \geq 0$, outage parameters $\xi_c$ and $\xi_s$ are compatible if and only if:

$$R \leq \log_2 \left(1 - \frac{\gamma_d \cdot \ln(1 - \xi_c)}{1 - \gamma_e \cdot \ln(\xi_s)}\right). \tag{29}$$

The proof of Theorem 10 is stated in App. C. Equation (28) emphasizes that the trade-off between the connection and the secrecy outage probability only depends on the ratio $\gamma_d/\gamma_e$, i.e., the difference $\gamma_d - \gamma_e$ in [dB]. The trade-off between connection and secrecy outage probability (28) is represented in Fig. 9 for different parameters $(\gamma_d, \gamma_e)$ and for $R = 0$. 

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure8}
\caption{Gaussian wiretap channel with Rayleigh block fading $(h_d, h_e)$.}
\end{figure}
The maximization problem for the secrecy throughput writes as follows:

$$\eta = \max_{\mathbf{R}, R_1} \mathbf{R} \cdot e^{-\frac{R + R_1 - 1}{\gamma_d}},$$ (30)

u.c. \[
\begin{align*}
R + R_1 &\leq \log_2 \left(1 - \gamma_d \cdot \ln(1 - \xi_c)\right), \\
R_1 &\geq \log_2 \left(1 - \gamma_d \cdot \ln(\xi_s)\right).
\end{align*}
\]

This problem has a solution if and only if the outage parameters $\xi_c, \xi_s$ are compatible, i.e., satisfy the conditions of Theorem 10. Since the secrecy throughput is decreasing in $R_1$, the optimal parameter is $R_1^* = \log_2 \left(1 - \gamma_d \cdot \ln(\xi_s)\right)$. We denote by $\hat{R} = \log_2 \left(\frac{1 - \gamma_d \cdot \ln(1 - \xi_c)}{1 - \gamma_d \cdot \ln(\xi_s)}\right)$ the maximal secrecy rate, compatible with the outage parameters $(\xi_c, \xi_s)$. The derivative of the criteria $\Phi(\mathbf{R}) = \mathbf{R} \cdot e^{-\frac{R_1 - 1}{\gamma_d}}$ is:

$$\Phi'(\mathbf{R}) = e^{-\frac{R_1 - 1}{\gamma_d}} \times \left(1 - R \cdot 2^R \cdot \frac{\ln(2) \cdot (1 - \gamma_d \cdot \ln(\xi_s))}{\gamma_d}\right).$$ (31)

We denote by $\hat{R} \geq 0$, the evaluation of the Lambert W function at

$$\hat{R} \cdot 2^\hat{R} = \frac{\gamma_d}{\ln(2) \cdot (1 - \gamma_d \cdot \ln(\xi_s))}.$$ (32)

The function $\Phi(\mathbf{R})$ increases for $\hat{R} \leq \hat{R}$ and then decreases, hence the maximum of $\Phi(\mathbf{R})$ is achieved by $\hat{R}$. The optimal secrecy rate is equal to the minimum: $R^* = \min(\hat{R}, \mathbf{R})$.

Fig. 10 represents the secrecy throughput for $L = 1$ transmission depending on the rate parameter $\gamma$. The shape of the curve depends on the secrecy outage constraint $\xi_c$. The connection outage constraint $\xi_c$ truncates the secrecy throughput, since the optimal secrecy rate $R^*$ should be smaller than $\mathbf{R}$.

**B. Multiple Transmissions**

We propose a numerical optimization of the secrecy throughput with respect to the rate parameters for the case of $L > 1$ multiple transmissions. In order to reduce the complexity of the optimization, we restrict our study to the case where the dummy-message rate parameters $R_2 = R_3 = \ldots = R_L$ are equal after the second transmission. In that case, the optimization problem depends only on three parameters: $(\gamma, R_1, R_2)$ instead of $L + 1$ parameter $(\gamma, R_1, \ldots, R_L)$. We compare this setting to the one of [39] that involves only two parameters $(\gamma, R_1)$, i.e., where rates $R_2 = R_3 = \ldots = R_L = 0$ are null.

**Trade-off connection and secrecy outage probability**

As mentioned in Sec VI-A, the outage parameters $\xi_c$ and $\xi_s$ are not always compatible. Fig. 11 represents the trade-off between the connection $P_{\text{co}}$ and secrecy $P_{\text{so}}$ outage probabilities, for zero rate $R = 0$ and number of transmissions $L \in \{1, 2, 4, 8\}$.

**Range of dummy-message rate** $R_1 \in [R_{1,\text{min}}, R_{1,\text{max}}]$

The minimal rate $R_1$ should guarantee that during the first transmission, the equation $P(I(X_1; Z_1|k_1) \geq R_1) = \xi_s$ is satisfied with equality. If the inequality was strict $P(I(X_1; Z_1|k_1) \geq R_1) < \xi_s$, then it would be possible to decrease the rate parameter $R_1$ in order to increase the secrecy rate $R$ and the corresponding throughput. The minimal rate

---

Fig. 10. Secrecy throughput depending on the secrecy rate $\gamma \geq 0$, for different secrecy outage constraints $\xi_c \in \{10^{-2}, 10^{-4}, 10^{-6}\}$. Vertical dotted lines represent the maximal secrecy rate $R$ corresponding to the connection outage constraint $\xi_c = 0.75$.

Fig. 11. Trade-off between the connection $P_{\text{co}}$ and secrecy $P_{\text{so}}$ outage probability, for zero rate $R = 0$ and number of transmissions $L \in \{1, 2, 4, 8\}$.
We fixe the secrecy rate of [39], i.e., where second rate is zero.

A larger dummy-message rate would be a waste of transmission resources. This induces a maximal rate $R_1^{\text{max}}$, with $R_2 = 0$.

$$R_1^{\text{min}} \leq R_1$$ is defined by:

$$R_1^{\text{min}} = \log_2 \left( 1 - \gamma \cdot \log_2 \xi \right). \quad (33)$$

The maximal rate $R_1$ should guarantee that the secrecy outage probability for $L$ possible transmissions, is equal to $\xi$. A larger dummy-message rate $R_1$ would be a waste of transmission resources. This induces a maximal rate $R_1^{\text{max}} \geq R_1$, defined by:

$$R_1^{\text{max}} \quad \text{s.t.} \quad \mathcal{P} \left( \sum_{j \in 1}^L I(X_j; Z_j | k_j) \geq R_1^{\text{max}} \right) = \xi. \quad (34)$$

The dummy-message rate $R_1^{\text{max}}$ is optimal in the framework of [39], i.e., where second rate $R_2 = 0$ is zero.

**Optimization of dummy-message rates** $(R_1, R_2)$

We fixe the secrecy rate $R \geq 0$ and for each rate $R_1^{\text{min}} \leq R_1 \leq R_1^{\text{max}}$, we find $R_2^{\text{opt}}(R_1)$ such that the secrecy outage probability $\mathcal{P}_{so} = \xi_{s}$ is satisfied with equality. Then, we optimize the secrecy throughput regarding the pair of rates $(R_1, R_2^{\text{opt}}(R_1))$ and the secrecy rate $R$.

**Numerical Results**

Figure [12] compares the secrecy throughput with two optimal rates $(R_1^{\text{opt}}, R_2^{\text{opt}})$, to the secrecy throughput with only one rate $R_1^{\text{max}}$. These two curves are drawn depending the secrecy rate $R \geq 0$, by considering four pairs of outage parameters:

$$(\xi_{c}, \xi_{s}) \in \{ (1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6}), (1, 10^{-2}) \}.$$

- As mentioned in the following tabular, splitting the dummy-message rate using $(R_1, R_2)$ improves the secrecy throughput respectively by more than 8%, compared to the approach of [39], with only one parameter $R_1^{\text{max}}$, i.e., with $R_2 = 0$.

**Fig. 12.** Secrecy throughput depending on the secrecy rate $R$, under different pairs of outage constraints $(\xi_{c}, \xi_{s}) \in \{ (1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6}) \}$. For each setting, the highest curve corresponds to the optimal pair of dummy-message rates $(R_1^{\text{opt}}, R_2^{\text{opt}})$, whereas the lowest curve correspond to the unique rate $R_1^{\text{max}}$, with $R_2 = 0$.

**Fig. 13.** Optimal rates $(R_1^{\text{opt}}, R_2^{\text{opt}})$ and $R_1^{\text{max}}$, depending on the secrecy rate $R$ under different pairs of outage constraints $(\xi_{c}, \xi_{s}) \in \{ (1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6}) \}$.

**Fig. 14.** Connection and secrecy outage probability for optimal $(R_1^{\text{opt}}, R_2^{\text{opt}})$, depending on the secrecy rate $R$ under different pairs of outage constraints $(\xi_{c}, \xi_{s}) \in \{ (1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6}) \}$.

- Tightening the secrecy outage constraint $\xi_{s}$, reduces the secrecy throughput.
- As mentioned for one transmission in Sec. VI-A, the connection outage constraint $\xi_{c}$ induces a truncation of the secrecy throughput. This is illustrated by the curves corresponding to: $(\xi_{c}, \xi_{s}) \in \{ (1, 10^{-2}), (10^{-2}, 10^{-2}) \}$.
- The optimal pair $(R_1^{\text{opt}}, R_2^{\text{opt}})$ corresponding to Fig. [12] are presented in Fig. [13] The optimal rate $R_1^{\text{opt}} < R_1^{\text{max}}$ is reduced compared to the case where $R_2 = 0$, and this is compensated by a strictly positive $R_2 > 0$. Hence, the first transmissions are correctly decoded with a larger probability, compared to the approach stated in [39].
- The connection outage probability $P_{so}$ corresponding to the parameters $(R, R_1^{\text{opt}}, R_2^{\text{opt}})$ of Fig. [12] and Fig. [13] are
The parameters of this tabular correspond to Fig. [12] [13] [14] [15]

| Outage parameters \((\xi_c, \xi_s)\) | \((1, 10^{-6})\) | \((1, 10^{-2})\) | \((1, 10^{-4})\) | \((1, 10^{-6})\) |
|-------------------------------------|----------------|----------------|----------------|----------------|
| Maximal secrecy throughput \(\eta\) with \(R^\text{max}_1, R_2 = 0\) | 0.55 | 0.78 | 1.22 | 1.00 |
| Maximal secrecy throughput \(\eta\) with \(R^\text{max}_1, R_2 \) | 0.60 | 0.86 | 1.32 | 1.11 |
| Increase of secrecy throughput | 9% | 10% | 8% | 11% |
| \(E[L]\) with \(R^\text{max}_1, R_2 = 0\) | 7.76 | 7.57 | 7.20 | 5.94 |
| \(E[L]\) with \(R^\text{max}_1, R_2 \) | 6.92 | 6.53 | 6.14 | 5.36 |
| Reduction of exp. number of transmissions | -10% | -14% | -15% | -10% |

The parameters of this tabular correspond to Fig. [12] [13] [14] [15] for \((\xi_c, \xi_s) = (1, 10^{-2})\), the secrecy rate \(R = 6\) induces a connection outage probability close to \(P_\text{co} \approx 10^{-6}\) that corresponds to the truncation of the secrecy throughput for \(R \geq 6\), on Fig. [12]. The connection outage probability is larger than in the approach of [39] because the total dummy-message rate \(R_1 + (L - 1) \cdot R_2 > R^\text{max}_1\) is greater. However, the corresponding secrecy throughput with \((R^*_1, R^*_2)\) is still larger than with \(R^\text{max}_1\) and \(R_2 = 0\).

- The expected number of transmissions \(E[L]\) corresponding to the settings of Fig. [12] Fig. [13] Fig. [14] is presented in Fig. [15]. The following tabular provides the expected number of transmissions \(E[L]\) corresponding to the maximal secrecy throughput \(\eta\) of Fig. [12].

- The ASR-code increases the secrecy throughput \(\eta\) by more than 8% and reduces the expected number of transmissions \(E[L]\) by more than 10%.

![Graph](image)

The presence of multiple transmissions rounds in HARQ offers new dimensions which we exploit in the design of the code to ensure secrecy and reliability. This was done in the literature, using a unique dummy-message. Our work follows this idea but, unlike previous works, we design a new code tailored for HARQ protocol, by splitting the dummy-message rate over several rate parameters. These additional degrees of freedom improve the matching between the dummy-message rates and the realization of the eavesdropper channel. We evaluate the performance in terms of secrecy outage probability, connection outage probability and secrecy throughput. For Rayleigh fading channel, the splitting of the dummy-message rate provides higher secrecy throughput and lower expected duration/average delay.

**APPENDIX A**

**PROOF OF THEOREM 4**

We prove the Theorem 4 considering \(L = 2\) transmissions. We provide a coding scheme that is reliable and secure for all pair of channel states \((k_1, k_2)\) that satisfy equation (35).

\[(k_1, k_2) \in S_1^2(\varepsilon, R, R_1, P^*_2) \cap S_2(\varepsilon, R, R_1, R_2, P^*_2).\]  

(35)

The first transmission is not reliable, the encoder receives a NACK feedback and starts a second transmission. More precisely, the channel states \((k_1, k_2)\) satisfy equations (36), (37), (38), (39).

\[R + R_1 + R_2 \leq I(X_1; Y_1|k_1) + I(X_2; Y_2|k_2) - 8\varepsilon\]  

(36)

\[R + R_1 > I(X_1; Y_1|k_1) - 4\varepsilon.\]  

(37)

\[R_1 + R_2 \geq I(X_1; Z_1|k_1) + I(X_2; Z_2|k_2) - 4\varepsilon.\]  

(38)

\[R_1 \geq I(X_1; Z_1|k_1) - 4\varepsilon.\]  

(39)

Equations (36), (38), (39) correspond to the definition of the set of channel states \(S_2(\varepsilon, R, R_1, R_2, P^*_2)\) and equation (37) corresponds to the NACK feedback, i.e., the first transmission failed \(k_1 \notin S_1^2(\varepsilon, R, R_1, P^*_2)\). Combining (36) and (37), it induces equation (40) that will be used in the following.

\[R_2 \leq I(X_2; Y_2|k_2) - 4\varepsilon.\]  

(40)

Fig. 2 shows that equation (40) is a direct consequence of equation (36), since the second transmission starts only when there is a NACK feedback. Let the length of the first transmission bloc \(n \in \mathbb{N}\) be larger than \((R_1, n_2, n_3, n_4, n_5, n_6, n_7, n_2, n_3, n_5)\) given by equations (42), (43), (44), (45), (46), (66), (67), (68) and (69). We prove that there exists a HARQ-code \(c^* \in C(n, R, L)\) with stochastic encoder such that the error probability and the information.

VII. CONCLUSION

We investigate secure HARQ protocol for state-dependent channel where the encoder only knows the statistics of the channel-state. Then, the reliability and security are defined in probabilistic sense and there is a trade-off between the constraints we can impose on these two criteria.
leakage rate satisfy equation (41), for all channel states $(k_1, k_2) \in S_1(\varepsilon, \mathbf{R}, \mathbf{P}_x) \cap S_2(\varepsilon, \mathbf{R}, \mathbf{R}_2, \mathbf{P}_x)$,

$$P(c^*|k_1, k_2) \leq \varepsilon', \quad \mathcal{L}(c^*|k_1, k_2) \leq \varepsilon', \quad (41)$$

with $\varepsilon' = \varepsilon \cdot (13 + 20 \log_2 |\mathcal{X}|)$.

Using similar arguments, the HARQ-code with stochastic encoder $c^* \in \mathcal{C}(n, \mathbf{R}, \mathbf{L})$ can be extended to the case of $L$ transmissions. The coding scheme is reliable and secure for all channel states $(k_1, \ldots, k_L) \in \bigcup_{l=1}^L S_l(\varepsilon, \mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_L, \mathbf{P}_x)$ stated in definition 5.

$$|\mathcal{M} \times \mathcal{M}_1| = 2^{n(R_1+R_1)}$$

$$|\mathcal{M}| = 2^{nR_1}$$

$$X^n_1(m, w_1) \sim \mathcal{P}_x$$

$$|\mathcal{M}_1| = 2^{nR_1}$$

$$|\mathcal{M}| = 2^{nR_2}$$

$$X^n_2(m, w_1, w_2) \sim \mathcal{P}_x$$

$$|\mathcal{M}_2| = 2^{nR_2}$$

Fig. 16. Binning scheme of the random HARQ-code $C \in \mathcal{C}(n, \mathbf{R}, \mathbf{L})$ stated in section 4.5.1 for $L = 2$ transmissions. The parameters $n \in \mathbb{N}$, $\mathbf{R} \in \mathbb{R}^+$, $\mathbf{R}_1 \in \mathbb{R}^+$, $\mathbf{R}_2 \in \mathbb{R}^+$ determine the cardinalities of the set of messages $|\mathcal{M}| = 2^{nR}$, the cardinality of the bins $|\mathcal{M}_1| = 2^{nR_1}$ and the number of sub-bins $|\mathcal{M}_2| = 2^{nR_2}$. The random codewords $X^n_1(m, w_1)$ and $X^n_2(m, w_1, w_2)$ are generated with i.i.d. probability distribution $\mathcal{P}_x$.

A. Random HARQ-Code

We consider a random HARQ-code $C \in \mathcal{C}(n, \mathbf{R}, \mathbf{L})$ with stochastic encoder, represented by figure 16 for $L = 2$ transmissions and defined as follows:

- **Random codebook for the first transmission.** Generate $|\mathcal{M} \times \mathcal{M}_1| = 2^{n(R_1+R_1)}$ sequences $X^n_1 \in \mathcal{X}$ drawn from the probability distribution $\mathcal{P}_x$. Randomly bin them into $|\mathcal{M}| = 2^{nR}$ bins denoted by $m \in \mathcal{M}$, each of them containing $|\mathcal{M}_1| = 2^{nR_1}$ sequences $X^n_1 \in \mathcal{X}$ indexed by the parameter $w_1 \in \mathcal{M}_1$. If the encoder receives a “Nack” feedback, the second transmission starts. Encoder chooses at random the parameter $w_2 \in \mathcal{M}_2$ using the uniform probability distribution and sends the sequence of channel inputs $x^n_2(m, w_1, w_2)$.

- **Second feedback from the decoder.** The decoder observes the realization of the channel state $(k_1, k_2) \in K_1 \times K_2$ and sends to the encoder the feedback “Ack” if it can decode after the first transmission (i.e. equation (37) is satisfied). It sends the feedback “Nack” if it can not decode after the first transmission (i.e. equation (37) is satisfied).

- **Decoding function for “Ack”.** The decoder observes the state parameter $k_1 \in K_1$ and finds the pair of indexes $(m, w_1) \in M \times M_1$ such that $x^n_1(m, w_1) \in A^n_1(y^n_1|k_1)$ is jointly typical with the sequence of channel outputs. It returns the index $m \in \mathcal{M}$ of the transmitted message.

- **Random codebook for the second transmission.** Generate $|\mathcal{M} \times \mathcal{M}_1 \times \mathcal{M}_2| = 2^{n(R_1+R_1+R_2)}$ sequences $X^n_2 \in \mathcal{X}$ drawn from the probability distribution $\mathcal{P}_x$. Randomly bin them into $|\mathcal{M}| = 2^{nR}$ bins denoted by $m \in \mathcal{M}$, each of them containing $|\mathcal{M}_1 \times \mathcal{M}_2| = 2^{n(R_1+R_2)}$ sequences $X^n_2 \in \mathcal{X}$ indexed by a pair of parameters $(w_1, w_2) \in \mathcal{M}_1 \times \mathcal{M}_2$. Each bin $m \in \mathcal{M}$ is divided into $|\mathcal{M}_2| = 2^{nR_2}$ sub-bins containing $|\mathcal{M}_1| = 2^{nR_1}$ sequences $X^n_2 \in \mathcal{X}$. We denote by $w_2 \in \mathcal{M}_2$ the index of the sub-bins and by $w_1 \in \mathcal{M}_1$ the index of the sequence of symbols $x^n_2(m, w_1, w_2) \in \mathcal{X}$.

- **Encoding for the second transmission.** If the encoder receives a “Nack” feedback, the second transmission starts. Encoder chooses at random the parameter $w_2 \in \mathcal{M}_2$ using the uniform probability distribution and sends the sequence of channel inputs $x^n_2(m, w_1, w_2)$.

- **Second feedback from the decoder.** The decoder observes the realization of the channel state $(k_1, k_2) \in K_1 \times K_2$ and sends to the encoder the feedback “Ack” if it can decode (i.e. equation (36) is satisfied). It sends the feedback “Nack” if it can not decode (i.e. equation (36) is satisfied).

- **Decoding function for “Ack”.** The decoder observes the state parameters $(k_1, k_2) \in K_1 \times K_2$ and finds the triple of indexes $(m, w_1, w_2) \in M \times M_1 \times M_2$ such that $x^n_1(m, w_1) \in A^n_1(y^n_1|k_1)$ is jointly typical with the sequence of outputs of the first channel $T_1$ and such that $x^n_2(m, w_1, w_2) \in A^n_2(y^n_2|k_2)$ is jointly typical with the sequence of outputs of the second channel $T_2$. It returns the index $m \in \mathcal{M}$ of the transmitted message.

- **Larger number of transmissions $L > 2$.** The same procedure involving random codebook, encoding, feedbacks and decoding is repeated for $L > 2$ transmissions.

- **An error is declared when the sequences $(x^n_1, y^n_1, z^n) \notin A^n_1(Q_1|k_1)$ or $(x^n_2, y^n_2, z^n) \notin A^n_2(Q_2|k_2)$ are not jointly typical for the probability distributions $Q_1 = \mathcal{P}_x \times T_1 \in \Delta(\mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Z}_1)$ and $Q_2 = \mathcal{P}_x \times T_2 \in \Delta(\mathcal{X} \times \mathcal{Y}_2 \times \mathcal{Z}_2)$.

**Remark 11** The parameter $n \in \mathbb{N}$ is the length of the transmission bloc, $|\mathcal{M}| = 2^{nR}$ is the cardinality of the set of messages $\mathcal{M}$, $|\mathcal{M}_1| = 2^{nR_1}$ is the cardinality of the set of dummy-messages $\mathcal{M}_1$ for the first transmission and $|\mathcal{M}_2| = 2^{nR_2}$ is the cardinality of the set of dummy-messages $\mathcal{M}_2$ for the second transmission. We denote by $P_\mathcal{X} \in \Delta(\mathcal{X})$ the probability distribution of the sequences of channel inputs.
B. Expected error probability

We upper bound the expected error probability for fixed messages \((m, w_1, w_2)\) and channel states \((k_1, k_2)\) in \(S_1(\varepsilon, R, R_1, P_x^R) \cap S_2(\varepsilon, R, R_1, R_2, P_x^R)\).

\[
\mathbb{E}_c \left[ \mathcal{P} \left( \left\{ (x^n_1, y^n_1, z^n_1) \notin A^n_\varepsilon(Q_1|k_1) \right\} \cup \left\{ (x^n_2, y^n_2, z^n_2) \notin A^n_\varepsilon(Q_2|k_2) \right\} \right) \right] \leq \varepsilon, \tag{42}
\]

\[
\mathbb{E}_c \left[ \mathcal{P} \left( \left\{ \exists (m', w'_1, w'_2) \neq (m, w_1, w_2), \text{ s.t.} \right. \right. \\
\left. \left. \{x_1^n(m', w'_1) \in A^n_\varepsilon(y_1^n(k_1)) \right. \\
\left. \cup \{x_2^n(m', w'_1, w'_2) \in A^n_\varepsilon(y_2^n(k_2)) \right\} \right\} \right) \leq \varepsilon, \tag{43}
\]

\[
\mathbb{E}_c \left[ \mathcal{P} \left( \left\{ \exists m', w'_1 \neq (m, w_1), \text{ s.t.} \right. \right. \\
\left. \left. \{x_1^n(m', w'_1) \in A^n_\varepsilon(y_1^n(k_1)) \right. \\
\left. \cup \{x_2^n(m', w'_1, w'_2) \in A^n_\varepsilon(y_2^n(k_2)) \right\} \right\} \right) \leq \varepsilon, \tag{44}
\]

\[
\mathbb{E}_c \left[ \mathcal{P} \left( \left\{ \forall w'_2 \neq w_2, \text{ s.t.} \right. \right. \\
\left. \left. \{x_2^n(m, w_1, w'_2) \in A^n_\varepsilon(y_2^n(k_2)) \right\} \right\} \right) \leq \varepsilon. \tag{45}
\]

The idea of this proof is to adapt the size of the set of dummy-messages to the realizations of the mutual informations \(I(X_1; Z_1|k_1)\) and \(I(X_2; Z_2|k_2)\). The parameters \(R_{V_1}, R_{V_2}\) and \(R_{k_1}\) are positive. Equations (38) and (39) guarantees that parameter \(R_{k_1}\) is positive for all channel states \((k_1, k_2)\) in \(S_1(\varepsilon, R, R_1, P_x^R) \cap S_2(\varepsilon, R, R_1, R_2, P_x^R)\). In this section, each bin \(m \in M\) is re-organized as follows:

- First, we divide each sub-bin \(w_2 \in M_2\) of size \(2^nR_{V_2}\) into \(2^{nR_{V_1}}\) sub-bins of size \(2^{nR_{V_1}}\).
- Second, we concatenate the sub-bins \(w_2 \in M_2\) into \(2^{nR_{V_2}}\) super-sub-bins containing \(2^{nR_{V_1}}\) sub-bins \(w_2 \in M_2\).

This analysis does not modify the random code \(C\) but it allows to provide an upper bound over the information leakage rate. The parameters \(W_1\) and \(W_2\) correspond to the pairs of auxiliary random variables \(W_1 = (V_1, J_1)\) and \(W_2 = (V_2, J_2)\).

\[
n \cdot \mathbb{E}_c \left[ L_{q_2} \left( C \left| k_1, k_2 \right. \right) \right] = I(M, W_1, W_2; Z^n_1, Z^n_2 | C, k_1, k_2) \tag{51}
\]

\[
n \cdot \mathbb{E}_c \left[ L_{q_1} \left( C \left| k_1, k_2 \right. \right) \right] = I(W_1, W_2 | M, C, Z^n_1, Z^n_2, k_1, k_2). \tag{53}
\]

- The first term (51) satisfies:
  \[
  I(M, W_1, W_2; Z^n_1, Z^n_2 | k_1, k_2) \leq I(X^n_1, X^n_2; Z^n_1, Z^n_2 | k_1, k_2) \tag{54}
  \]
  \[
  = n \cdot (I(X_1; Z_1|k_1) + I(X_2; Z_2|k_2)). \tag{55}
  \]

- The second term (53) satisfies:
  \[
  H(W_1, W_2 | M, C, k_1, k_2) = n \cdot (R_{V_1} + R_{V_2}). \tag{56}
  \]

C. Expected information leakage rate

We provide an upper bound on the expected information leakage rate that is valid for all channel states \((k_1, k_2)\) in \(S_1(\varepsilon, R, R_1, P_x^R) \cap S_2(\varepsilon, R, R_1, R_2, P_x^R)\). To this purpose, we introduce four auxiliary random variables \(V_1, J_1, V_2\) and \(J_2\) that belong to the sets \(M_{V_1}, M_{J_1}, M_{V_2}\) and \(M_{J_2}\) with cardinality \(|M_{V_1}| = 2^nR_{V_1}, |M_{J_1}| = 2^nR_{J_1}, |M_{V_2}| = 2^nR_{V_2}\) and \(|M_{J_2}| = 2^nR_{J_2}\) given by:

\[
R_{V_1} = I(X_1^*; Z_1|k_1) + I(X_2^*; Z_2|k_2) - \min \left( I(X_2^*; Z_2|k_2), R_2 \right) - 4\varepsilon, \tag{47}
\]

\[
R_{V_2} = \min \left( I(X_2^*; Z_2|k_2), R_2 \right) - 4\varepsilon, \tag{48}
\]

\[
R_{J_1} = R_1 - R_{V_1} = \min \left( R_1 - I(X_1^*; Z_1|k_1) + 4\varepsilon, R_1 + R_2 - I(X_1^*; Z_1|k_1) - I(X_2^*; Z_2|k_2) + 4\varepsilon \right), \tag{49}
\]

\[
R_{J_2} = R_2 - R_{V_2} = \max \left( R_2 - I(X_2^*; Z_2|k_2), 0 \right) + 4\varepsilon. \tag{50}
\]

The parameters \(R_{V_1}, R_{V_2}\) and \(R_{J_1}\) are positive. Equations (38) and (39) guarantees that parameter \(R_{J_1}\) is positive for all channel states \((k_1, k_2)\) in \(S_1(\varepsilon, R, R_1, P_x^R) \cap S_2(\varepsilon, R, R_1, R_2, P_x^R)\). The first term (51) satisfies:

\[
H(W_1, W_2 | M, C, k_1, k_2) = n \cdot (R_{V_1} + R_{V_2}). \tag{56}
\]

The second term (53) satisfies:

\[
H(W_1, W_2 | M, C, Z^n_1, Z^n_2, k_1, k_2) \leq H(W_1, W_2 | M, C, Z^n_1, Z^n_2, k_1, k_2) \leq n \cdot (R_{J_1} + R_{J_2}). \tag{59}
\]

The parameters \(R_{V_1}, R_{V_2}\) and \(R_{J_1}\) are positive. Equations (38) and (39) guarantees that parameter \(R_{J_1}\) is positive for all channel states \((k_1, k_2)\) in \(S_1(\varepsilon, R, R_1, P_x^R) \cap S_2(\varepsilon, R, R_1, R_2, P_x^R)\).
(58) and (59) come from the properties of the entropy function and the cardinalities $|M_{(ij)}| = 2^{nR_i}$ and $|M_{(ji)}| = 2^{nR_j}$.
(60) comes from the equations (49) and (50), satisfied for all channel states $(k_1, k_2) \in S_1(\epsilon, R, R_1, P_2^*) \cap S_2(\epsilon, R, R_1, R_2, P_2^*)$ and the equation: $\max(a, b) + \min(a, b) = a + b$.
(61) comes from Lemma 1, that is based on Fano’s inequality.

Equations (55), (56) and (61) provide an upper bound on:
$$E_c \left[ I_e \left( C \left| k_1, k_2 \right. \right) \right] \leq \epsilon \cdot (9 + 20 \log_2 |\mathcal{X}|).$$ (62)

This analysis can be extended to the case of $L > 2$ transmissions by introducing the random variables $R_{v_i}$ and $R_{h_j}$.

**Lemma 1** Fano’s inequality provides the upper bound:
$$H(V_1, V_2 | J_1, J_2, C, Z_1^n, Z_2^n, k_1, k_2) \leq n \cdot \left( \epsilon + 20 \epsilon \cdot \log_2 |\mathcal{X}| \right).$$ (63)

**Lemma 7** Suppose that the eavesdropper implements the decoding $g_e$ defined by equation (63) as follows:
- **Decoding of the eavesdropper** $g_e$ takes the sequence of channel outputs $Z_1^n \in Z_1^n$, $Z_2^n \in Z_2^n$, the message $M \in \mathcal{M}$, the indexes $J_1 \in \mathcal{J}_{L_1}$, $J_2 \in \mathcal{J}_{L_2}$ and the HARQ-code $C \in \mathcal{C}(n, R, L)$ and returns the indexes $V_1 \in \mathcal{V}_{c_1}$, $V_2 \in \mathcal{V}_{c_2}$ and the sequences $X_1^n(M, V_1, J_1) \in \mathcal{X}^n$ and $X_2^n(M, V_1, J_2, J_2) \in \mathcal{X}^n$ that are jointly typical with $Z_1^n \in Z_1^n$ and $Z_2^n \in Z_2^n$.

$$g_e: \mathcal{Z}_1^n \times \mathcal{Z}_2^n \times \mathcal{X} \times \mathcal{J}_{L_1} \times \mathcal{J}_{L_2} \ni (z_1^n, z_2^n, x^n, v_1, v_2) \rightarrow (x^n, x^n, x_1^n, x_2^n).$$ (64)

An error occurs if this decoding function $g_e$ returns sequences of inputs and indexes $(x_1^n, x_2^n, v_1, v_2) \neq g_e(z_1^n, z_2^n, m, j_1, j_2, c, k_1, k_2)$ that are different from the original tuple $(x_1^n, x_2^n, v_1, v_2)$. We provide an upper bound over the expected error probability of this decoding function $g_e$.

$$E_c \left[ P \left( \left\{ (x_1^n, z_1^n) \notin A_c^n(2^n|k_1) \right\} \right) \right] \leq \epsilon.$$ (65)

$$E_c \left[ P \left( \left\{ (x_2^n, z_2^n) \notin A_c^n(2^n|k_2) \right\} \right) \right] \leq \epsilon.$$ (66)

$$E_c \left[ P \left( \left\{ \exists (v', v) : (v_1, v_2) \neq (v_1, v_2), \text{ s.t.} \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \left\{ x_1^n(m, v_1^n, j_1) \in A^n_c(z_1^n|k_1) \right\} \right] \right] \left\{ x_2^n(m, v_1^n, j_1, v_2^n, j_2) \in A^n_c(z_2^n|k_2) \right\} \left\{ \right\} \leq \epsilon.$$ (67)

$$E_c \left[ P \left( \left\{ \exists v_2^n \neq v_2, \text{ s.t.} \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \left\{ x_2^n(m, v_1^n, j_1, v_2^n, j_2) \in A^n_c(z_2^n|k_2) \right\} \left\{ \right\} \leq \epsilon.$$ (68)

Equations (65), (66), (67) and (68) prove that the expected probability of this decoding $g_e$ is upper bounded by $4 \epsilon$.

$$H(V_1, V_2 | M, J_1, J_2, C, Z_1^n, Z_2^n, k_1, k_2) \leq n \cdot \left( \epsilon + 20 \epsilon \cdot \log_2 |\mathcal{X}| \right).$$ (69)

Equation (69) comes from [45] pp. 19, Fano’s Inequality] and $n \geq n_g = \frac{1}{2}$ and equations (47) and (48) which imply that $\log_2 |\mathcal{M}_{V_1}| \leq 2n \cdot \log_2 |\mathcal{X}|$ and $\log_2 |\mathcal{M}_{V_2}| \leq n \cdot \log_2 |\mathcal{X}|$. ■

**D. Conclusion**

For all $\epsilon > 0$, there exists $n_0$, for all $n \geq n_0$, there exists HARQ-code $c^* \in \mathcal{C}(n, R, L)$ such that $P_{so}(c^*|k_1, k_2) \leq \epsilon$ and $E_c(c^*|k_1, k_2) \leq \epsilon$, for all $(k_1, k_2) \in S_1(\epsilon, R, R_1, P_2^*) \cap S_2(\epsilon, R, R_1, R_2, P_2^*)$.

**APPENDIX B**

**PROOF OF PROPOSITION 8**

**Proof:** We assume that the random events $(B_i)_{i \in \{1, \ldots, L\}}$ are independent of the random events $(A_i)_{i \in \{1, \ldots, L\}}$.

$$P_{so} = P \left( \bigcup_{i=1}^{L} B_i \right) = 1 - P \left( \bigcap_{i=1}^{L} B_i \right) = 1 - \sum_{j=1}^{L} P(\bigcap_{i=1}^{j} B_i) \cdot P(\bigcap_{i=j+1}^{L} A_i) \cdot P(\bigcap_{i=1}^{j} A_i) = P \left( \bigcup_{i=1}^{L} B_i \right) \cdot P(\bigcap_{i=1}^{L} A_i).$$ (70)

Equation (70) comes from the properties of the probability $P_{so}$.

Equation (71) comes from the definition of the HARQ-code, if $j$ transmissions occurs, then $\bigcup_{i=1}^{j} B_i = \bigcup_{i=1}^{j} B_i$.

Equation (72) comes from the independence of the events $(B_i)_{i \in \{1, \ldots, L\}}$ with events $(A_i)_{i \in \{1, \ldots, L\}}$ hence with transmission number $L$.

Equation (73) comes from the probability of having $L$ transmission.

**APPENDIX C**

**PROOF OF THEOREM 10**

**Proof:** **First Point.** Increasing $\mathcal{R}$ decreases the connection outage probability and does not affect the secrecy outage probability. Hence we consider the secrecy rate $\mathcal{R} = 0$.

$$P_{so} = 1 - e^{-\frac{R_{so}}{n}} \leq \xi_{c}, \quad P_{so} = e^{-\frac{R_{so}}{n}} \leq \xi_s.$$ (74)

$\xi_c$ and $\xi_s$ are compatible if there exists $R_1$ satisfying (74), i.e.,

$$\log_2 \left( 1 - \gamma_c \cdot \ln(\xi_c) \right) \leq R_1 \leq \log_2 \left( 1 - \gamma_s \cdot \ln \left( 1 - \xi_s \right) \right).$$
Hence, the parameter $R_1$ exists if and only if:

$$R \leq \log_2 \left( \frac{1 - \frac{1}{\gamma_d} \cdot \ln(1 - \xi_s)}{1 - \frac{1}{\gamma_d} \cdot \ln(1 - \xi_c)} \right).$$

### References

[1] M. Le Treust, L. Szczecinski, and F. Labeau, “Secrecy & rate adaptation for secure HARQ protocols,” in *IEEE Information Theory Workshop (ITW)*, Sept 2013, pp. 1–5.

[2] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.

[3] I. E. Teltar and R. G. Gallager, “Combining queueing theory with information theory for multaccess,” *IEEE J. Sel. Areas Commun.*, vol. 13, no. 6, pp. 963–969, Aug 1995.

[4] G. Caire and D. Tuninetti, “Throughput of hybrid-ARQ protocols for gaussian collision channels,” *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1971–1988, July 2001.

[5] M. Zorzi and R. R. Rao, “Throughput performance of ARQ selective-repeat with time di- versity in markov channels with unreliable feedback,” *Wireless Network*, vol. 2, pp. 63–75, 1996.

[6] “Performance of ARQ go-back-protocol in markov channels with unreliable feedback,” *Mobile Networks and Applications*, vol. 2, no. 9, pp. 183–193, 1997.

[7] M. Zorzi and F. Borgonovo, “Performance of capture-divison packet access with slow shadowing and power control,” *IEEE Trans. Veh. Technol.*, vol. 46, pp. 687–696, 1997.

[8] M. Zorzi, “Mobile radio slotted aloha with capture, diversity and retransmission control in the presence of shadowing,” *Wireless Networks*, vol. 4, pp. 379–388, 1998.

[9] E. Visotsky, S. Yakun, V. Tripathi, M. Honig, and R. Peterson, “Reliability-based incremental redundancy with convolutional codes,” *IEEE Trans. Commun.*, vol. 53, no. 6, pp. 987–997, June 2005.

[10] S. Pfletschner and M. Navarro, “Adaptive HARQ for imperfect channel knowledge,” in *International ITG Conference on Source and Channel Coding (SCC)*, Feb 2010, pp. 1–6.

[11] E. Uhlemann, L. Rasmussen, A. Grant, and P. Wiberg, “Optimal incremental-redundancy strategy for type-ii hybrid ARQ,” in *IEEE Int. Symp. Inf. Theory (ISIT)*, July 2003.

[12] L. Szczecinski, S. R. 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, June 2013.

[13] M. Zorzi, M. Benjillali, L. Szczecinski, and F. Labeau, “Energy efficiency of adaptive HARQ,” *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 818–831, Feb 2016.

[14] M. Jabi, A. E. Hamss, L. Szczecinski, and P. Plantanida, “Multipacket hybrid ARQ: Closing gap to the ergodic capacity,” *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5191–5205, Dec 2015.

[15] M. Jabi, L. Szczecinski, M. Benjillali, and F. Labeau, “Outage minimization via power adaptation and allocation in truncated hybrid ARQ,” *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 711–723, March 2015.

[16] P. Larsson, L. Rasmussen, and M. Skoglund, “Throughput analysis of hybrid-ARQ – a matrix exponential distribution approach,” *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 416–428, Jan. 2016.

[17] K. Nguyen, L. Rasmussen, A. Guiilen i Fabregas, and N. Letzepis, “MIMO ARQ with multibit feedback: Outage analysis,” *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 765–779, Feb. 2012.

[18] W. Lee, O. Simeone, J. Kang, S. Rangan, and P. Popovski, “HARQ buffer management: An information-theoretic view,” *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4539–4550, Nov. 2015.

[19] C. Haunl and A. Chindapol, “Hybrid ARQ with cross-packet channel coding,” *IEEE Commun. Lett.*, vol. 11, no. 5, pp. 434–436, May 2007.

[20] J. Chiu and A. Chindapol, “Design of cross-packet channel coding with low-density parity-check codes,” in *IEEE Information Theory Workshop on Information Theory for Wireless Networks*, July 2007, pp. 1–5.