

Rate Adaptation for Secure HARQ Protocols

Mael Le Treust, Leszek Szczecinski, Fabrice Labeau

▶ **To cite this version:**

Mael Le Treust, Leszek Szczecinski, Fabrice Labeau. Rate Adaptation for Secure HARQ Protocols. 2017. hal-01404320v2

HAL Id: hal-01404320

https://hal.science/hal-01404320v2

Preprint submitted on 13 Nov 2017 (v2), last revised 14 Apr 2018 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Rate Adaptation for Secure HARQ Protocols

Maël Le Treust, Leszek Szczecinski* and Fabrice Labeau†
ETIS UMR 8051, Université Paris Seine, Université Cergy-Pontoise, ENSEA, 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 the hybrid-automatic repeat request (HARQ) transmission over block fading channel in the presence of an eavesdropper, where the secrecy of the transmission is ensured via introduction of dummy-messages. Since the encoder only knows the statistics of the channel-state, the secrecy and the reliability are defined in a probabilistic framework. 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 match 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 the throughput. Numerical examples illustrate that, comparing to existing alternatives, splitting of the dummy-message rate provides higher 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 in 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 information with arbitrary reliability [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 were analyzed in the literature from the point of view of throughput, outage probability, and average delay, e.g., [3]–[8].

Retransmissions in HARQ provide additional degrees of freedom which can be exploited to design a code which provides a suitable "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

Security is an issue 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 between the legitimate decoder and the eavesdropper channels, and characterized the rate at which the legitimate users can communicate not only reliably but also guarantees the secrecy of the transmitted message.[1] 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

Work supported by the government of Quebec under grant #PSR-SIIRI-435 and ENSEA under grant BQR-HARQ-2014; conducted as part of the project Labex MME-DII (ANR11-LBX-0023-01); presented in part at the IEEE Information Theory Workshop, Sept. 2013 [1]. This work was carried out, in part, when Maël Le Treust was a post-doctoral researcher with INRS and McGill University.

[1]Note that we use here, secrecy as a unique mean to guarantee the security of a transmission, but secrecy can be combined with cryptography as well.

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,[2] 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], and [36] 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 retransmits 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 and in [42] using low-density parity-check (LDPC) codes. In [43], the authors investigate secure HARQ protocols based on multiple encoding, by using new dummy-messages at each transmission.

It is worthwhile to mention that the notion of secrecy may be defined in many different ways, including "perfect", "weak" and "strong secrecy" [29], "effective secrecy", "privacy" and "stealth" [44], "semantic security" [45], or "covert communications" [46], [47]. Each of these notions provide different degrees of secrecy, based on probabilistic arguments or worst case scenarios.

The goal of this work is not investigate the comparison between these different notions but rather to develop a coding scheme tailored for HARQ transmissions. We use the same secrecy metric, namely "weak secrecy", as in the previous articles on that subject [39], [43] which also follow the Wyner's work [26].

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. 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 match between the dummy-message rates and the realization of the eavesdropper channels. 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. In our view, the ASR-code generalizes the coding scheme presented in [39] in a most natural manner as, for a particular choice of the dummy-message rates, ASR-code is equivalent to the coding proposed in [39].
- We characterize the trade-off between connection and secrecy outage probabilities and show the optimal rate allocation for discrete channels and for Rayleigh fading channels 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 main differences with our previous work [1] are:

- We consider an arbitrary number of possible retransmissions, whereas only one retransmission was considered in [1]; this affects non-trivially the expressions of connection and secrecy outages probabilities.
- We consider a more practical case of Rayleigh block-fading channels and analyze the corresponding solutions.
- We provide a full version of proof of Theorem 4, while only a sketch was shown in [1].

The work is organized as follows. Sec. II presents the channel model under investigation, the HARQ-code as well as defines our new protocol called ASR-code. The main result is Theorem 4 which proves that the error probability and the information 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. III-A. The example of a discrete channel-state is shown in Sec. III-B whereas Rayleigh fading channels are investigated in Sec. IV. Sec. V concludes the paper and the proofs of the results are stated in the Appendix.

II. Secure HARQ Protocol

We consider a HARQ protocol with L possible transmissions shown schematically in Fig. 1 for $L = 2$. Each transmission $l \in \{1, \dots, L\}$ corresponds to a block of $n \in \mathbb{N}$ symbols. Capital letter X denotes the random variable, lowercase letter $x \in \mathcal{X}$ denotes the realization and $\mathcal{X}^n$ denotes the n-time Cartesian product of the set $\mathcal{X}$. The random message $M \in \mathcal{M}$ is uniformly distributed and $m \in \mathcal{M}$ denotes the realization.

During the first transmission, the encoder $\mathcal{C}$ uses the sequence of input symbols $x_1^n \in \mathcal{X}^n$ in order to transmit the message $m \in \mathcal{M}$ to the legitimate decoder $\mathcal{D}$. The decoder $\mathcal{D}$ (resp. eavesdropper $\mathcal{E}$) observes the sequence of channel

[2]There is not reason while eavesdropper would collaborate with the legitimate users.

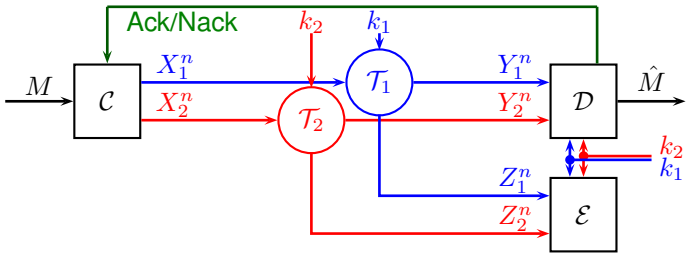


Fig. 1. State dependent wiretap channels $\mathcal{T}_i(y_i, z_i|x_i, k_i)$, with $i \in \{1, 2\}$. The second transmission starts if the encoder $\mathcal{C}$ receives a Nack feedback from the legitimate decoder. The state parameters $k_1 \in \mathcal{K}_1$ and $k_2 \in \mathcal{K}_2$ are chosen arbitrarily, stay constant during the transmission and are available only at the legitimate decoder $\mathcal{D}$ and at the eavesdropper $\mathcal{E}$.

outputs $y_1^n \in \mathcal{Y}^n$ (resp. $z_1^n \in \mathcal{Z}^n$) and tries to decode (resp. to infer) the transmitted message $m \in \mathcal{M}$. The decoder $\mathcal{D}$ sends a $\mathsf{Ack}_1/\mathsf{Nack}_1$ 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_{l-1} feedback after $l-1 \in \{1, \dots, L\}$ transmissions, then the message $m \in \mathcal{M}$ was not correctly decoded yet. The encoder starts retransmitting the message $m \in \mathcal{M}$ over transmission $l \in \{1, \dots, L\}$ with input sequence $x_l^n \in \mathcal{X}^n$. The decoder $\mathcal{D}$ (resp. eavesdropper $\mathcal{E}$) tries to decode (resp. to infer) the transmitted message $m \in \mathcal{M}$ from sequences of channel outputs $(y_1^n, y_2^n, \dots y_l^n) \in \mathcal{Y}^{l\times n}$ (resp. $(z_1^n, z_2^n, \dots z_l^n) \in \mathcal{Z}^{l\times n}$), where $\mathcal{Y}^{l\times n} = \overbrace{\mathcal{Y}^n \times \dots \times \mathcal{Y}^n}^{l}$ is the l-time Cartesian self-product of set $\mathcal{Y}^n$. If the maximal number of transmissions L is attained, the encoder drops message $m \in \mathcal{M}$ and starts sending the next message $m' \in \mathcal{M}$. The notation $\Delta(\mathcal{X})$ stands for the set of the probability distributions $\mathcal{P}(X)$ over the set $\mathcal{X}$. We assume that the channel is memoryless with transition probability $\mathcal{T}(y, z|x, k)$ depending on a state parameter $k \in \mathcal{K}$, for example a fading coefficient. The state parameters $(k_1, k_2, \dots, k_L) \in \mathcal{K}^L$ stay constant during the transmission of a block of $n \in \mathbb{N}$ symbols and are chosen at random with i.i.d. probability distribution $\mathcal{P}_k \in \Delta(\mathcal{K})$, from one block to another. The state parameters $(k_1, k_2, \dots, k_L) \in \mathcal{K}^L$ are observed by the decoder and the eavesdropper but not by the encoder.

At transmission $l \in \{1, \dots, L\}$, the state-dependent wiretap channel is given by

$$\mathcal{T}^n(y_l^n, z_l^n|x_l^n, k_l) = \prod_{i=1}^{n} \mathcal{T}(y_l(i), z_l(i)|x_l(i), k_l), \tag{1}$$

where $x_l(i)$ (resp. $y_l(i)$, $z_l(i)$) denotes the i-th symbol of the transmission block x_l (resp. y_l, z_l) of length n. The channel statistics are known by both encoder $\mathcal{C}$ and decoder $\mathcal{D}$.

Definition 1 *A HARQ-code $c_n \in \mathcal{C}(n, \mathsf{R}, L)$ with stochastic encoder is a vector of encoding and decoding functions $c_n = \Big((f_l)_{l\in\{1,\dots,L\}}, (g_l)_{l\in\{1,\dots,L\}}\Big)$, defined for each transmission $l \in \{1, \dots, L\}$ as follows:*

$$f_l \;: \mathcal{M} \times \mathcal{X}^{(l-1)\times n} \times \{\mathsf{Ack}, \mathsf{Nack}\}^{l-1} \to \Delta(\mathcal{X}^n), \tag{2}$$
$$g_l \;: \mathcal{Y}^{l\times n} \times \mathcal{K}^l \longrightarrow \mathcal{M} \times \{\mathsf{Ack}, \mathsf{Nack}\}, \tag{3}$$

where the rate R defines the cardinality $|\mathcal{M}| = 2^{n\mathsf{R}}$ of the set of messages $\mathcal{M}$ and L is the maximal number of transmissions. We denote by $\mathcal{C}(n, \mathsf{R}, L)$, the set of HARQ-code with stochastic encoder.

Definition 2 *For each vector of state parameters $(k_1, \dots, k_L) \in \mathcal{K}^L$, the error probability $\mathcal{P}_e$ and the information leakage rate $\mathcal{L}_e$ of the HARQ-code $c_n \in \mathcal{C}(n, \mathsf{R}, L)$ are defined by:*

$$\mathcal{P}_e(c_n|k_1, \dots, k_L) = \mathcal{P}\Big(M \neq \hat{M}\Big|\; c_n, k_1, \dots, k_L\Big),$$
$$\mathcal{L}_e(c_n|k_1, \dots, k_L) = \frac{I\Big(M; Z_1^n, \dots, Z_L^n\Big|\; c_n, k_1, \dots, k_L\Big)}{n}.$$

The random variable $\hat{M}$ denotes the output message of the legitimate decoder. Depending on the number of transmissions $l \in \{1, \dots, L\}$, it is given by $\hat{M} = g_l(Y_1^n, \dots, Y_l^n, k_1, \dots, k_l)$. The non-zero leakage rate means that the eavesdropper can infer some information about the message M, which is undesirable.

In [39], 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 $(k_1, \dots, k_L) \in \mathcal{K}^L$. The coding scheme is based on Wyner's coding for the wiretap channel [26] and involves two parameters: the rate $\mathsf{R_s} \geq 0$, which is called the "secrecy rate" and corresponds to the amount of secret information to be transmitted to the legitimate decoder; and the rate $\mathsf{R_0} \geq 0$ which corresponds to the total size of the codebook. The difference $\mathsf{R_0} - \mathsf{R_s} \geq 0$ 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.

Then, the conditions which are sufficient for the transmission to be reliable and secure, given by

$$\mathsf{R_0} \;\leq\; \sum_{j\in 1}^{L} I(X_j; Y_j|k_j), \tag{4}$$
$$\mathsf{R_0} - \mathsf{R_s} \;\geq\; \sum_{j\in 1}^{L} I(X_j; Z_j|k_j), \tag{5}$$

define "the secure channel set" [39, Definition 2].

We note that (5) enforces high value of the dummy-message rate $\mathsf{R_0} - \mathsf{R_s}$ which must guarantee the secrecy for the maximal number of transmissions L. This, in turn, prevents the first transmissions to be reliable, especially when the number of possible transmission L is large.

From this observation stems the main contribution of our work which consists in splitting the dummy-message rate $\mathsf{R_0} - \mathsf{R_s}$ over L different parameters denoted by $\mathsf{R}_1, \mathsf{R}_2, \dots, \mathsf{R}_L$. Splitting the dummy-message rate makes the first transmissions more reliable, since the first dummy-message rates can be smaller than $\mathsf{R_0} - \mathsf{R_s}$ in [39]. 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 $l \in \{1,\dots,L\}$, fixed parameters ε, R, $\mathsf{R}_1,\dots,\mathsf{R}_L$ and a fixed probability distributions $\mathcal{P}_{\mathsf{x}}^\star \in \Delta(\mathcal{X})$, the set of secure channel states, denoted by $\mathcal{S}_l(\varepsilon,\mathsf{R},\mathsf{R}_1,\dots,\mathsf{R}_L,\mathcal{P}_{\mathsf{x}}^\star)$, is the union of channel states $(k_1,\dots,k_l) \in \mathcal{K}^l$ that satisfy the following set of equations:*

$$\mathsf{R}+\sum_{j=1}^{l}\mathsf{R}_j \leq \sum_{j=1}^{l} I(X_j;Y_j|k_j)-\varepsilon, \quad (6)$$

$$\sum_{j=1}^{l}\mathsf{R}_j \geq \sum_{j=1}^{l} I(X_j;Z_j|k_j)-\varepsilon, \quad (7)$$

$$\sum_{j=1}^{l-1}\mathsf{R}_j \geq \sum_{j=1}^{l-1} I(X_j;Z_j|k_j)-\varepsilon, \quad (8)$$

$$\vdots$$

$$\mathsf{R}_1 \geq I(X_1;Z_1|k_1)-\varepsilon. \quad (9)$$

Equation (6) guarantees the correct decoding whereas equations (7) - (9) guarantee that the secrecy condition is satisfied at each transmission $l=\{1,\dots,L\}$. We note that (6) - (9) generalize equations of [39]. That is, using $\mathsf{R}_2=\dots=\mathsf{R}_L=0$, $\mathsf{R}_1=\mathsf{R}_0-\mathsf{R}_s$ and $\mathsf{R}=\mathsf{R}_s$ we obtain (4) and (5).[3]

These conditions are represented graphically in Fig. 2 for $L=2$ transmissions.

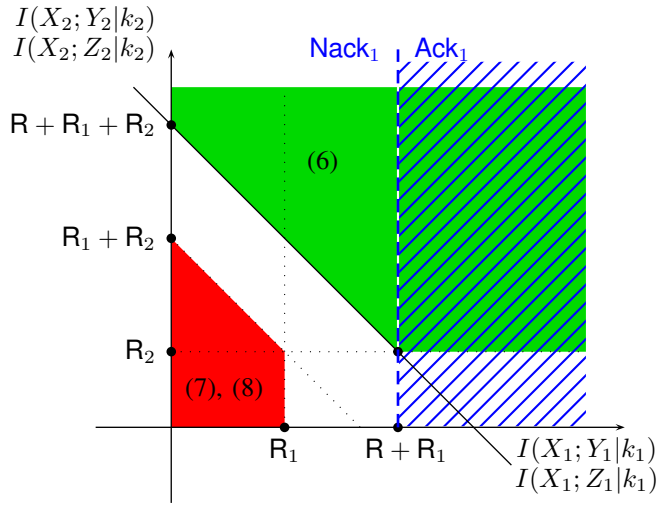


Fig. 2. Decoding and secrecy regions corresponding to the rates $(\mathsf{R},\mathsf{R}_1,\mathsf{R}_2)$, for $L=2$ transmissions. The second transmission starts only if there is a Nack$_1$, hence we disregard the dashed region of Ack$_1$. The green upper region corresponds to the decoding constraint of equation (6) for the mutual informations $I(X_1;Y_1|k_1)$ and $I(X_2;Y_2|k_2)$. 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 $I(X_2;Z_2|k_2)$.

We now prove the existence of a HARQ-code such that the error probability $\mathcal{P}_{\mathsf{e}}$ and the information leakage rate $\mathcal{L}_{\mathsf{e}}$ converge to zero, for all tuples of channel states $(k_1,\dots,k_L)$ that belong to $\bigcup_{l=1}^{L}\mathcal{S}_l(\varepsilon,\mathsf{R},\mathsf{R}_1,\dots,\mathsf{R}_L,\mathcal{P}_{\mathsf{x}}^\star)$.

Theorem 4 (Compound Wiretap Channel) *Fix the parameters R, $\mathsf{R}_1,\dots,\mathsf{R}_L$ and the input probability distribution $\mathcal{P}_{\mathsf{x}}^\star \in \Delta(\mathcal{X})$. 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 $c_n^\star \in \mathcal{C}(n,\mathsf{R},L)$ that satisfies equations* (10)*, for all channel states $(k_1,\dots,k_L)\in\bigcup_{l=1}^{L}\mathcal{S}_l(\varepsilon,\mathsf{R},\mathsf{R}_1,\dots,\mathsf{R}_L,\mathcal{P}_{\mathsf{x}}^\star)$.*

$$\mathcal{P}_{\mathsf{e}}\left(c_n^\star \,\middle|\, k_1,\dots,k_L\right)\leq\varepsilon, \quad \mathcal{L}_{\mathsf{e}}\left(c_n^\star \,\middle|\, k_1,\dots,k_L\right)\leq\varepsilon. \quad (10)$$

We note that the proof of Theorem 4, stated in Appendix A, involves multiples random binning schemes and cannot be obtained as a generalization of the coding scheme of [39, Appendix A].

In the rest of this article, the optimal sequence of HARQ-codes $c^\star=(c_n^\star)_{n\geq1}$ is called "Adaptation-Secrecy-Rate-code" (ASR-code) with parameters $\mathsf{R},\mathsf{R}_1,\dots,\mathsf{R}_L$. The additional degrees of freedom $\mathsf{R}_2,\dots,\mathsf{R}_L$ will be exploited to increase the secrecy throughput and to lower the expected number of transmissions and the connection and secrecy outages.

III. Secrecy Throughput, Connection and Secrecy Outages

A. Definitions

The channels under investigation are controlled by a state parameter $k\in\mathcal{K}$ 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 $(\mathcal{A}_l)_{l\in\{1,\dots,L\}}$ corresponding to the correct decoding (11) and the events $(\mathcal{B}_l)_{l\in\{1,\dots,L\}}$ corresponding to the secret transmission (12).

$$\mathcal{A}_l = \left\{\mathsf{R}+\sum_{j\in1}^{l}\mathsf{R}_j\leq\sum_{j\in1}^{l}I(X_j;Y_j|k_j)\right\}, \quad (11)$$

$$\mathcal{B}_l = \left\{\sum_{j\in1}^{l}\mathsf{R}_j\geq\sum_{j\in1}^{l}I(X_j;Z_j|k_j)\right\}, \quad (12)$$

Definition 5 *The connection outage probability $\mathcal{P}_{\mathsf{co}}$ and secrecy outage probability $\mathcal{P}_{\mathsf{so}}$ are defined by:*

$$\mathcal{P}_{\mathsf{co}}=\mathcal{P}\left(\bigcap_{l=1}^{L}\mathcal{A}_l^c\right), \qquad \mathcal{P}_{\mathsf{so}}=\mathcal{P}\left(\bigcup_{l=1}^{L}\mathcal{B}_l^c\right). \quad (13)$$

A connection outage occurs if for all transmissions $l\in\{1,\dots,L\}$, the decoding event $\mathcal{A}_l$ is not satisfied. A secrecy outage occurs if there exists a transmission $l\in\{1,\dots,L\}$, for which the secrecy event $\mathcal{B}_l$ is not satisfied.

Remark 6 Notation $\mathcal{A}^c$ stands for the complementary of $\mathcal{A}$. Letting the parameters $\mathsf{R}_2=\dots=\mathsf{R}_L=0$, this implies that $\mathcal{A}_{l-1}\subset\mathcal{A}_l$, $\mathcal{B}_l\subset\mathcal{B}_{l-1}$ and the definitions of $\mathcal{P}_{\mathsf{co}}$ and $\mathcal{P}_{\mathsf{so}}$ reduce to those shown in [39, Eqs. (21), (22)].

[3]Where, formally, ε should also be added as in (6) - (9).

Proposition 7 *Suppose that the random events $(\mathcal{B}_l)_{l\in\{1,\dots,L\}}$ are independent of the random events $(\mathcal{A}_l)_{l\in\{1,\dots,L\}}$. The secrecy outage probability writes:*

$$\begin{aligned}\mathcal{P}_{\mathsf{so}} &= 1-\sum_{j=2}^{L-1}\mathcal{P}\Big(\bigcap_{i=1}^{j}\mathcal{B}_i\Big)\cdot\Big(\mathcal{P}\Big(\bigcap_{i=1}^{j-1}\mathcal{A}_i^c\Big)-\mathcal{P}\Big(\bigcap_{i=1}^{j}\mathcal{A}_i^c\Big)\Big)\\ &- \mathcal{P}\Big(\mathcal{B}_1\Big)\cdot\mathcal{P}\Big(\mathcal{A}_1\Big)-\mathcal{P}\Big(\bigcap_{i=1}^{L}\mathcal{B}_i\Big)\cdot\mathcal{P}\Big(\bigcap_{i=1}^{L-1}\mathcal{A}_i^c\Big). \quad (14)\end{aligned}$$

Proof of Prop. 7 is stated in App. B. This formulation will be used for discrete channels in Sec. III-B and Gaussian channel in Sec. IV. We denote by $\mathsf{L}\in\{1,\dots,L\}$, the random number of transmission that depends on channel states parameters $(k_1,\dots,k_L)$ and rate parameters $(\mathsf{R},\mathsf{R}_1,\dots,\mathsf{R}_L)$.

$$\mathcal{P}(\mathsf{L}=1) = \mathcal{P}\Big(\mathcal{A}_1\Big), \quad (15)$$

$$\begin{aligned}\mathcal{P}(\mathsf{L}=l) &= \mathcal{P}\Big(\bigcap_{j=1}^{l-1}\mathcal{A}_j^c\cap\mathcal{A}_l\Big), \qquad \forall l\in\{2,\dots,L-1\}\\ &= \mathcal{P}\Big(\bigcap_{j=1}^{l-1}\mathcal{A}_j^c\Big)-\mathcal{P}\Big(\bigcap_{j=1}^{l}\mathcal{A}_j^c\Big), \quad (16)\end{aligned}$$

$$\mathcal{P}(\mathsf{L}=L) = \mathcal{P}\Big(\bigcap_{j=1}^{L-1}\mathcal{A}_j^c\Big). \quad (17)$$

The expected number of transmissions $\mathbb{E}[\mathsf{L}]$ is given by:

$$\mathbb{E}[\mathsf{L}] = \sum_{l=1}^{L} l\cdot\mathcal{P}(\mathsf{L}=l) = 1+\sum_{l=1}^{L-1}\mathcal{P}\Big(\bigcap_{j=1}^{l}\mathcal{A}_j^c\Big). \quad (18)$$

Since the number of transmissions L is a random variable, the expected number of bits correctly decoded is given by the Renewal-Reward Theorem as in [48], [4].

Definition 8 *The secrecy throughput η is defined as the expected number of bits correctly decoded by the legitimate decoder per channel use and can be obtained from the renewal-reward approach*

$$\begin{aligned}\eta &= \max_{\substack{\mathsf{R},\\ \mathsf{R}_1,\dots\mathsf{R}_L,}}\frac{\mathbb{E}[\mathsf{R}]}{\mathbb{E}[\mathsf{L}]}=\max_{\substack{\mathsf{R},\\ \mathsf{R}_1,\dots\mathsf{R}_L,}}\frac{\mathsf{R}\cdot(1-\mathcal{P}_{\mathsf{co}})}{1+\sum_{l=1}^{L-1}\mathcal{P}\big(\bigcap_{j=1}^{l}\mathcal{A}_j^c\big)},\\ \text{u.c.}&\begin{cases}\mathcal{P}_{\mathsf{co}} &\le \xi_{\mathsf{c}},\\ \mathcal{P}_{\mathsf{so}} &\le \xi_{\mathsf{s}}.\end{cases} \quad (19)\end{aligned}$$

The maximum is taken over the parameters $\mathsf{R},\mathsf{R}_1,\dots,\mathsf{R}_L$, such that the connection outage probability and the secrecy outage probability are lower than ξ_{c} and ξ_{s}, which are the constraints defined according to the requirements on the secrecy and reliability.

B. Example: Discrete Channel States

To illustrate the definitions we introduced we consider the scenario represented by Fig. 3, in which the channel states of the legitimate decoder and of the eavesdropper are discrete and uniformly distributed over $\{k^y,k'^y\}$ and $\{k^z,k'^z\}$. We define the operating point as $\xi_{\mathsf{c}}=0.25$ and $\xi_{\mathsf{s}}=0.125$, and assume the maximum number of transmission is $L=2$. We investigate

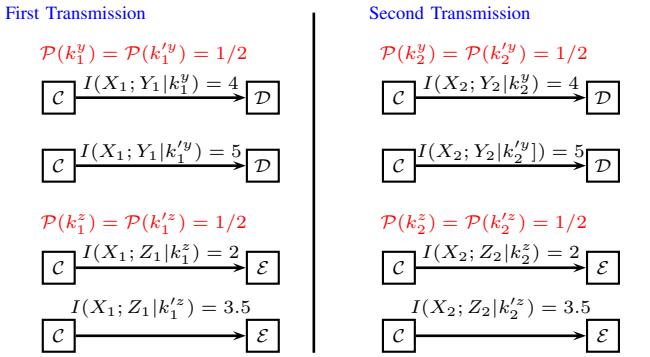


Fig. 3. In both transmissions, the capacity of the channel to the legitimate decoder takes two possible values $\{4,5\}$ with probability $(1/2,1/2)$ and the capacity of the channel to the eavesdropper takes two possible values $\{2,3.5\}$ with probability $(1/2,1/2)$.

the secrecy throughput of the ASR-code whose existence is stated in Theorem 4 and we compare its performance to the protocols shown in [39] and in [43].

• The secure HARQ protocol of [39] is a particular case of the ASR-code in which the dummy-message rate $\mathsf{R}_2=0$ is zero. As depicted on fig. 4, after $L=2$ transmissions, the decoding is correct if:

$$\mathsf{R}+\mathsf{R}_1 \le I(X_1;Y_1|k_1)+I(X_2;Y_2|k_2), \quad (20)$$

and the transmission is secret if:

$$\mathsf{R}_1 \ge I(X_1;Y_1|k_1)+I(X_2;Y_2|k_2). \quad (21)$$

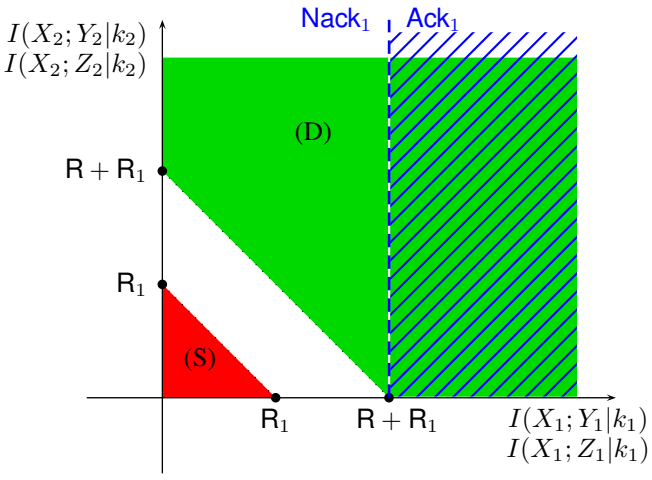


Fig. 4. Regions of correct decoding (D) and secret transmission (S) of [39], corresponding to equations (20) and (21).

• The S-HARQ protocol of [43, Sec. V] involves multiple dummy-message rates $(\mathsf{R}_1,\mathsf{R}_2)$. As depicted on fig. 5, after $L=2$ transmissions, the decoding is correct if:

$$\begin{aligned}\mathsf{R} &\le \max\Big(I(X_1;Y_1|k_1)-\mathsf{R}_1,0\Big)\\ &+ \max\Big(I(X_2;Y_2|k_2)-\mathsf{R}_2,0\Big), \quad (22)\end{aligned}$$

and the transmission is secret if:

$$\mathsf{R}_1 \geq I(X_1;Y_1|k_1), \qquad \mathsf{R}_2 \geq I(X_2;Y_2|k_2). \tag{23}$$

Fig. 2, 4 and 5 show that the decoding and the secrecy regions are different for the ASR-code and for the protocols of [39] and [43].

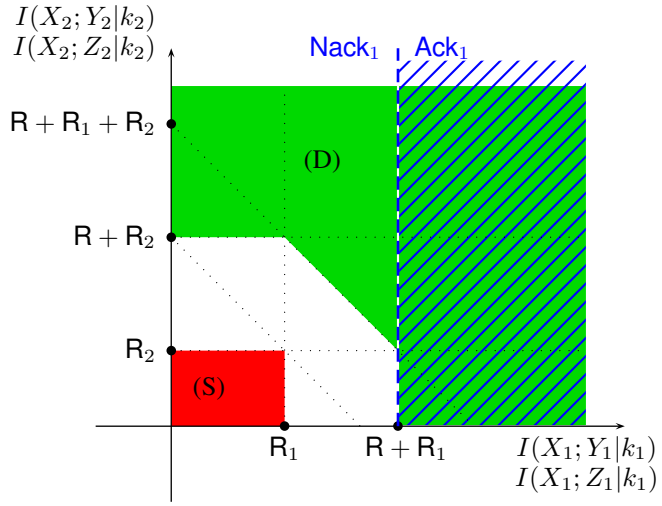


Fig. 5. Regions of correct decoding (D) and secret transmission (S) of [43], corresponding to equations (22) and (23).

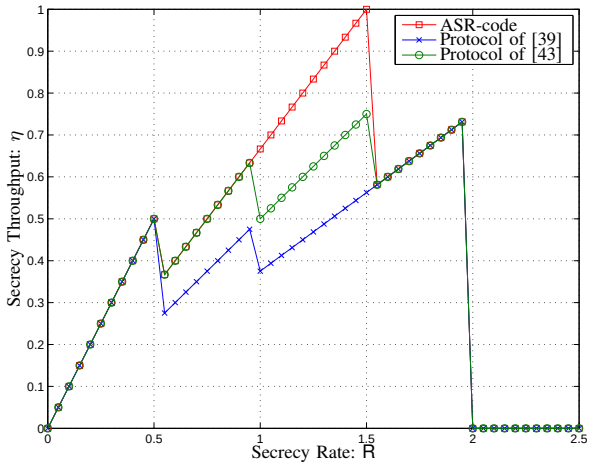


Fig. 6. Secrecy throughput for $L = 2$ possible transmissions and the constraints $\xi_{\mathsf{c}} = 0.25$, $\xi_{\mathsf{s}} = 0.125$.

Fig. 6 compares the secrecy throughput of ASR-code, and of the protocols of [39] and [43]; we observe the following

- The ASR-code outperforms both protocols [39] and [43] for the secrecy rate $\mathsf{R} = 1.5$, dummy message rates $(\mathsf{R}_1, \mathsf{R}_2) = (3.5, 2)$ and outage probabilities $(\mathcal{P}_{\mathsf{co}}, \mathcal{P}_{\mathsf{so}}) = (0, 0.125)$.
- For the protocol of [39], the optimal dummy-message rate $\mathsf{R}_1^{[39]} = 7$ corresponding to $L = 2$ transmissions is high and prevents the first transmission to be decoded correctly.
- For the protocol of [43], the optimal second dummy-message rate $\mathsf{R}_2^{[43]} = 3.5$ is higher than $\mathsf{R}_2 = 2$ for ASR-code. Hence, when the secrecy rate exceeds $\mathsf{R} \geq 1.5$, the connection outage probability increases to $\mathcal{P}_{\mathsf{co}} = 0.25$ and reduces the secrecy throughput.
- In the example we show, the ASR-code provides more than 33% of increase compared to the protocols of [39] and [43]. However, we hasten to say that the improvement depends on the adopted distribution of the channel gains. In particular, if the values of the channels to the eavesdropper are replaced by $\{2, 3\}$ (instead of $\{2, 3.5\}$), the protocol of [43] provides the same secrecy throughput $\eta = 1.333$ as the ASR-code, whereas the protocol of [39] provides a lower secrecy throughput of $\eta = 1.125$. Therefore, while we are sure our approach outperforms [39], the direct comparison with [43] is not obvious as also noted in [43, pp.1714]. Despite this cautionary statement, we did not find any example where the throughput of [43] is larger than the one offered by the ASR-code we propose.

IV. Rayleigh Block Fading Gaussian Wiretap Channel

A. Channel Model

We consider the Gaussian wiretap channel with Rayleigh block fading represented in Fig. 7 and defined as

$$Y = h_{\mathsf{d}} \cdot X + N_{\mathsf{d}}, \qquad Z = h_{\mathsf{e}} \cdot X + N_{\mathsf{e}}. \tag{24}$$

where N_{d} and N_{e} are i.i.d. zero-mean, unit-variance Gaussian variables.

We assume a normalized power constraint on the channel input $\mathbb{E}\big[|X|^2\big] \leq P = 1$. The state parameters $k = (h_{\mathsf{d}}, h_{\mathsf{e}}) \in$

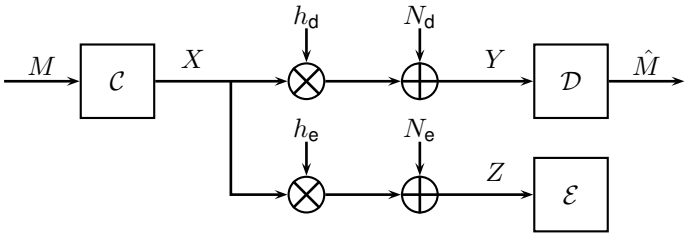


Fig. 7. Gaussian wiretap channel with Rayleigh block fading $(h_{\mathsf{d}}, h_{\mathsf{e}})$.

$\mathcal{K}$ are fading coefficients, distributed i.i.d. from one block to another with Rayleigh probability distribution. Since the mean of noise and power are normalized to 1, we introduce the notation $\mathsf{SNR}_{\mathsf{d}} = |h_{\mathsf{d}}|^2$ and $\mathsf{SNR}_{\mathsf{e}} = |h_{\mathsf{e}}|^2$. The mean SNRs are denoted by $\gamma_{\mathsf{d}} = \mathbb{E}[\mathsf{SNR}_{\mathsf{d}}] = \mathbb{E}\big[|h_{\mathsf{d}}|^2\big]$ and $\gamma_{\mathsf{e}} = \mathbb{E}[\mathsf{SNR}_{\mathsf{e}}] = \mathbb{E}\big[|h_{\mathsf{e}}|^2\big]$. For $x \geq 0$, the probability density function $f(x)$ and the cumulative distribution function $F(x)$ of the SNRs are defined by

$$f(x) = \frac{1}{\gamma} \cdot e^{-\frac{x}{\gamma}}, \qquad F(x) = 1 - e^{-\frac{x}{\gamma}}. \tag{25}$$

so the mutual informations write as

$$I(X;Y|h_{\mathsf{d}}) = \log(1 + \mathsf{SNR}_{\mathsf{d}}), \tag{26}$$
$$I(X;Z|h_{\mathsf{e}}) = \log(1 + \mathsf{SNR}_{\mathsf{e}}). \tag{27}$$

and depend on the random fading coefficients $k = (h_{\mathsf{d}}, h_{\mathsf{e}}) \in \mathcal{K}$.

The constraints ξ_c and ξ_s are not always compatible since the outage constraints $\mathcal{P}_{co} \leq \xi_c$ and $\mathcal{P}_{so} \leq \xi_s$ may not be satisfied simultaneously. We characterize the trade-off between connection outage probability and secrecy outage probability when only one transmission is allowed, i.e., $L = 1$.

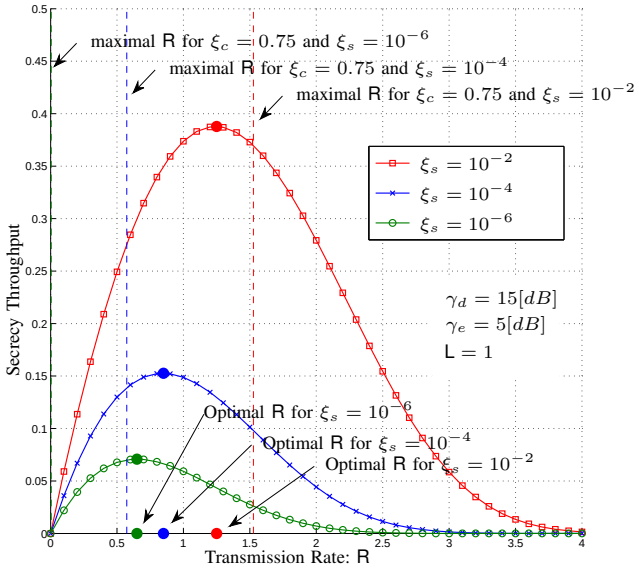


Fig. 8. Secrecy throughput depending on the secrecy rate $\mathsf{R} \geq 0$, for different secrecy constraints $\xi_s \in \{10^{-2}, 10^{-4}, 10^{-6}\}$ and a single $L = 1$ transmission. Vertical dashed lines represents the maximal secrecy rate R corresponding to the constraint $\xi_c = 0.75$.

Theorem 9 *Consider the case of $L = 1$ transmission.*
• *The constraints ξ_c and ξ_s are compatible if and only if*

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

• *For a fixed secrecy rate $R \geq 0$, the contraints ξ_c and ξ_s are compatible if and only if*

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

The proof of Theorem 9 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 γ_d/γ_e, i.e., the difference $\gamma_d - \gamma_e$ in [dB]. Fig. 8 represents the secrecy throughput for $L = 1$ transmission depending on the rate parameter R, for different constraints (ξ_c, ξ_s). The shape of the curve depends on the secrecy outage constraint $\mathcal{P}_{so} \leq \xi_s$. The connection outage constraint $\mathcal{P}_{co} \leq \xi_c$ truncates the secrecy throughput at the dashed lines.

B. Multiple Transmissions

We propose a numerical optimization of the secrecy throughput with respect to the rate parameters for the case of $L \geq 2$ multiple transmissions.

Since our objective is to demonstrate that the ASR-code outperforms the HARQ-code of [39], we show a simple example

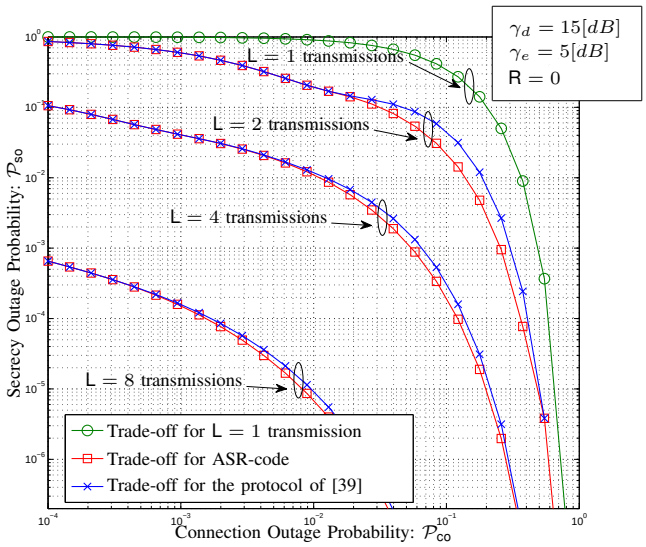


Fig. 9. Trade-off between the connection $\mathcal{P}_{co}$ and secrecy $\mathcal{P}_{so}$ outage probability, for zero rate $\mathsf{R} = 0$ and number of transmissions $L \in \{1, 2, 4, 8\}$.

where the dummy-message rate parameters $\mathsf{R}_2 = \mathsf{R}_3 = \ldots = \mathsf{R}_L$ are equal after the second transmission. This makes the presentation easier and avoids the tedious optimization which depends only on three parameters: $(\mathsf{R}, \mathsf{R}_1, \mathsf{R}_2)$.

For Rayleigh fading channels the protocol of [39] outperforms the one proposed in [43] as can be seen in [43, Fig. 6, Fig. 7, Fig. 8]. Thus, we only need to compare the performance of the ASR-code we proposed with the protocol of [39]. The main difference is that the latter uses two parameters $(\mathsf{R}, \mathsf{R}_1)$, while the ASR-code uses three rates $(\mathsf{R}, \mathsf{R}_1, \mathsf{R}_2)$.

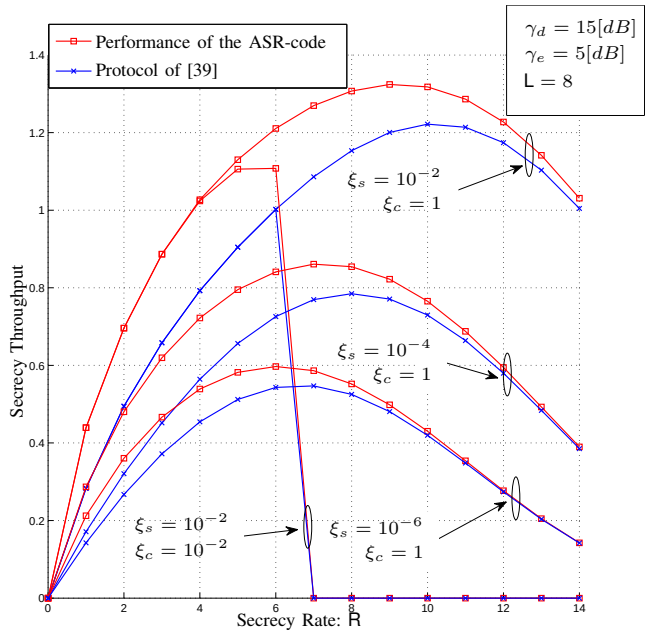


Fig. 10. Secrecy throughput depending on the secrecy rate R, under different pairs of constraints $(\xi_c, \xi_s) \in \{(1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6})\}$. For each setting, the ASR-code outperforms the protocol of [39].

Trade-off connection and secrecy outage probability

As mentioned in Sec IV-A, the constraints ξ_c and ξ_s are not always compatible. Fig. 9 represents the trade-off between the connection $\mathcal{P}_{co}$ and the secrecy $\mathcal{P}_{so}$ outages, depending on the maximal number of transmissions $L \in \{1, 2, 4, 8\}$, for $\mathsf{R} = 0$. For each setting, the trade-off for the protocol of [39] is more restrictive than for the ASR-code. Splitting the dummy-message rate over multiple transmission, i.e., with $\mathsf{R}_2 > 0$, provides a small improvement for this trade-off. For a given pair of constraints (ξ_c, ξ_s), there exists a minimal number of transmission L such that the connection and secrecy outage probability $\mathcal{P}_{co} \leq \xi_c$ and $\mathcal{P}_{so} \leq \xi_s$ satisfy the constraints.

Range of dummy-message rate $\mathsf{R}_1 \in [\mathsf{R}_1^{\min}, \mathsf{R}_1^{\max}]$

The minimal rate R_1 should guarantee that during the first transmission, the equation $\mathcal{P}\big(I(X_1; Z_1|k_1) \geq \mathsf{R}_1\big) = \xi_s$ is satisfied with equality. If the inequality was strict $\mathcal{P}\big(I(X_1; Z_1|k_1) \geq \mathsf{R}_1\big) < \xi_s$, 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 $\mathsf{R}_1^{\min} \leq \mathsf{R}_1$ is defined by:

$$\mathsf{R}_1^{\min} \quad = \quad \log_2\Big(1 - \gamma_e \cdot \log_2(\xi_s)\Big). \tag{30}$$

The maximal rate R_1 should guarantee that the secrecy outage probability for L possible transmissions, is equal to ξ_s. A larger dummy-message rate R_1 would be a waste of transmission resources. This induces a maximal rate $\mathsf{R}_1^{\max} \geq \mathsf{R}_1$, defined by:

$$\mathsf{R}_1^{\max} \quad \text{s.t.} \quad \mathcal{P}\bigg(\sum_{j\in 1}^{L} I(X_j; Z_j|k_j) \geq \mathsf{R}_1^{\max}\bigg) = \xi_s. \tag{31}$$

The dummy-message rate $\mathsf{R}_1^{\max}$ is optimal for the protocol of [39], i.e., where second rate $\mathsf{R}_2 = 0$ is zero.

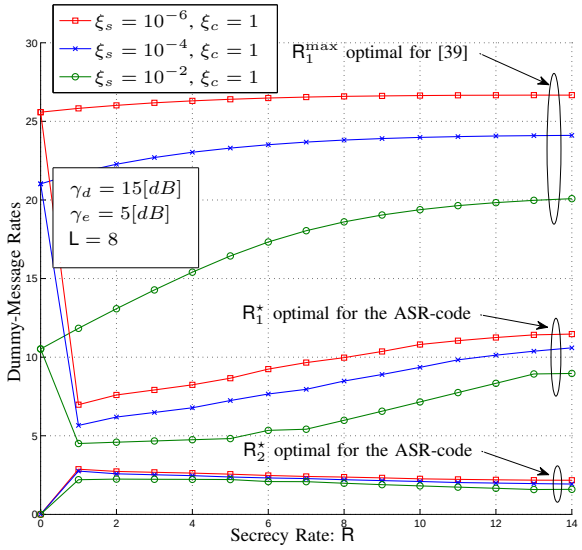


Fig. 11. Optimal rates $(\mathsf{R}_1^\star, \mathsf{R}_2^\star)$ for the ASR-code and $\mathsf{R}_1^{\max}$ for the protocol of [39], depending on the secrecy rate R under different pairs of constraints $(\xi_c, \xi_s) \in \big\{(1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6})\big\}$.

Optimization of dummy-message rates $(\mathsf{R}_1, \mathsf{R}_2)$

We fixe the secrecy rate $\mathsf{R} \geq 0$ and for each rate $\mathsf{R}_1^{\min} \leq \mathsf{R}_1 \leq \mathsf{R}_1^{\max}$, we find $\mathsf{R}_2^\star(\mathsf{R}_1)$ such that the secrecy outage constraint $\mathcal{P}_{so} = \xi_s$ is satisfied with equality. Then, we optimize the secrecy throughput regarding the pair of rates $\big(\mathsf{R}_1, \mathsf{R}_2^\star(\mathsf{R}_1)\big)$ and the secrecy rate R.

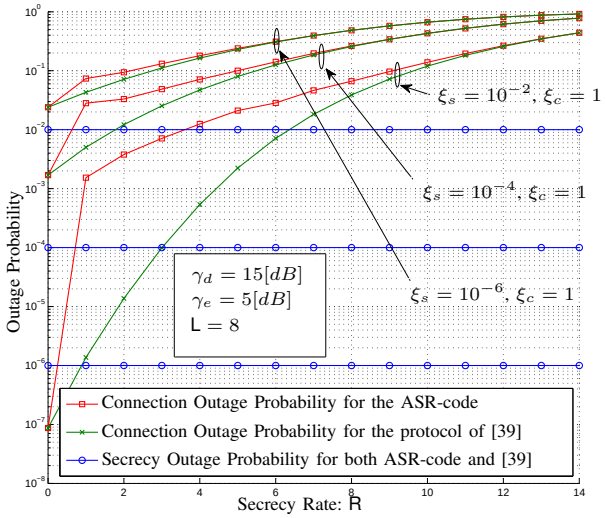


Fig. 12. Connection and secrecy outage probability for the ASR-code and for the protocol of [39], depending on the secrecy rate R under different pairs of constraints $(\xi_c, \xi_s) \in \big\{(1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6})\big\}$.

Numerical Results

Figure 10 compares the secrecy throughput for the ASR-code and for the protocol of [39]. These two curves are drawn depending the secrecy rate $\mathsf{R} \geq 0$, by considering four pairs of constraints:

$$(\xi_c, \xi_s) \in \Big\{(1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6}), (10^{-2}, 10^{-2})\Big\}.$$

- As mentioned in the following tabular, splitting the dummy-message rate using $(\mathsf{R}_1, \mathsf{R}_2)$ improves the secrecy throughput respectively by more than 8%, compared to the approach of [39], with only one parameter $\mathsf{R}_1^{\max}$, i.e., with $\mathsf{R}_2 = 0$.
- Tightening the secrecy constraint ξ_s, reduces the secrecy throughput.
- As mentioned for one transmission in Sec. IV-A, the connection outage constraint ξ_c induces a truncation of the secrecy throughput. This is illustrated by the curves corresponding to: $(\xi_c, \xi_s) \in \big\{(1, 10^{-2}), (10^{-2}, 10^{-2})\big\}$.
- The optimal rates $(\mathsf{R}_1^\star, \mathsf{R}_2^\star)$ for the ASR-code are presented in Fig. 11. As expected, the first parameter $\mathsf{R}_1^\star < \mathsf{R}_1^{\max}$ is lower for the ASR-code than for the protocol of [39]. Therefore, the first transmissions are more likely to be decoded correctly and this increases the secrecy throughput.
- The connection outage probability $\mathcal{P}_{co}$ corresponding to the optimal parameters $(\mathsf{R}, \mathsf{R}_1^\star, \mathsf{R}_2^\star)$ of the ASR-code are presented in Fig. 12. For $(\xi_c, \xi_s) = (1, 10^{-2})$, the secrecy rate $\mathsf{R} = 6$ induces a connection outage probability close to $\mathcal{P}_{co} \simeq 10^{-2}$ that corresponds to the truncation of the secrecy throughput for $\mathsf{R} \geq 6$, on Fig. 10. The connection outage probability is larger for the ASR-code than for the protocol of [39] because the total dummy-message rate $\mathsf{R}_1 + (L-1) \cdot \mathsf{R}_2 > \mathsf{R}_1^{\max}$ is greater. However, this does

Constraints (ξ_c, ξ_s)	$(1, 10^{-6})$	$(1, 10^{-4})$	$(1, 10^{-2})$	$(10^{-2}, 10^{-2})$
Maximal secrecy throughput η with $\mathsf{R}_1^{\max}$, $\mathsf{R}_2 = 0$	0.55	0.78	1.22	1.00
Maximal secrecy throughput η with $(\mathsf{R}_1^\star, \mathsf{R}_2^\star)$	0.60	0.86	1.32	1.11
Increase of secrecy throughput	9%	10%	8%	11%
$\mathbb{E}[\mathsf{L}]$ with $\mathsf{R}_1^{\max}$, $\mathsf{R}_2 = 0$	7.76	7.57	7.20	5.94
$\mathbb{E}[\mathsf{L}]$ with $(\mathsf{R}_1^\star, \mathsf{R}_2^\star)$	6.92	6.53	6.14	5.36
Reduction of exp. number of transmissions	−10%	−14%	−15%	−10%

not prevent the secrecy throughput of the ASR-code to be greater than for the protocol of [39].

- The expected number of transmissions $\mathbb{E}[\mathsf{L}]$ is represented in Fig. 13. The following table provides the secrecy throughput and the expected number of transmissions $\mathbb{E}[\mathsf{L}]$, for different constraints.
- Compared to the protocol of [39], the ASR-code increases the secrecy throughput η by more than 8% and reduces the expected number of transmissions $\mathbb{E}[\mathsf{L}]$ by more than 10%.

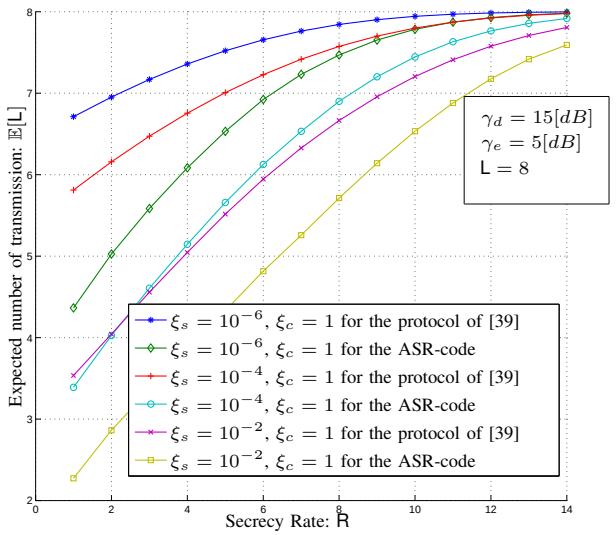


Fig. 13. Expected number of transmissions $\mathbb{E}[\mathsf{L}]$ for the ASR-code and for the protocol of [39], depending on the secrecy rate R with different pairs of constraints $(\xi_c, \xi_s) \in \{(1, 10^{-2}), (1, 10^{-4}), (1, 10^{-6})\}$.

V. Conclusion

We investigate secure HARQ protocols for state-dependent channels 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.

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 (32).

$$(k_1, k_2) \in \mathcal{S}_1^c(\varepsilon, \mathsf{R}, \mathsf{R}_1, \mathcal{P}_{\mathsf{x}}^\star) \cap \mathcal{S}_2(\varepsilon, \mathsf{R}, \mathsf{R}_1, \mathsf{R}_2, \mathcal{P}_{\mathsf{x}}^\star). \quad (32)$$

The first transmission is not reliable, the encoder receives a NACK_1 feedback and starts a second transmission. More precisely, the channel states (k_1, k_2) satisfy equations (33), (34), (35), (36).

$$\begin{aligned} \mathsf{R} + \mathsf{R}_1 + \mathsf{R}_2 &\leq I(X_1; Y_1|k_1) + I(X_2; Y_2|k_2) - 8\varepsilon, & (33)\\ \mathsf{R} + \mathsf{R}_1 &> I(X_1; Y_1|k_1) - 4\varepsilon, & (34)\\ \mathsf{R}_1 + \mathsf{R}_2 &\geq I(X_1; Z_1|k_1) + I(X_2; Z_2|k_2) - 4\varepsilon, & (35)\\ \mathsf{R}_1 &\geq I(X_1; Z_1|k_1) - 4\varepsilon. & (36) \end{aligned}$$

Equations (33), (35), (36) correspond to the definition of the set of channel states $\mathcal{S}_2(\varepsilon, \mathsf{R}, \mathsf{R}_1, \mathsf{R}_2, \mathcal{P}_{\mathsf{x}}^\star)$ and equation (34) corresponds to the NACK_1 feedback, i.e., the first transmission failed $k_1 \notin \mathcal{S}_1^c(\varepsilon, \mathsf{R}, \mathsf{R}_1, \mathcal{P}_{\mathsf{x}}^\star)$. Combining (33) and (34), it induces equation (37) that will be used in the following.

$$\mathsf{R}_2 \leq I(X_2; Y_2|k_2) - 4\varepsilon. \quad (37)$$

Fig. 2 shows that equation (37) is a direct consequence of equation (33), since the second transmission starts only when there is a Nack_1 feedback. Let the length of the first transmission bloc $\bar{n} \in \mathbb{N}$ be larger than $(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8, n_9)$ given by equations (39), (40), (41), (42), (62), (63), (64), (65) and (66). We prove that there exists a HARQ-code $c^\star \in \mathcal{C}(n, \mathsf{R}, L)$ with stochastic encoder such that the error probability and the information leakage rate satisfy equation (38), for all channel states $(k_1, k_2) \in \mathcal{S}_1^c(\varepsilon, \mathsf{R}, \mathsf{R}_1, \mathcal{P}_{\mathsf{x}}^\star) \cap \mathcal{S}_2(\varepsilon, \mathsf{R}, \mathsf{R}_1, \mathsf{R}_2, \mathcal{P}_{\mathsf{x}}^\star)$,

$$\mathcal{P}_{\mathsf{e}}\left(c^\star \middle| k_1, k_2\right) \leq \varepsilon', \quad \mathcal{L}_{\mathsf{e}}\left(c^\star \middle| k_1, k_2\right) \leq \varepsilon', \quad (38)$$

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

Using similar arguments, the HARQ-code with stochastic encoder $c^\star \in \mathcal{C}(n, \mathsf{R}, L)$ can be extended to the case of L transmissions. The coding scheme is reliable and secure for all channel states $(k_1, \ldots, k_L) \in \bigcup_{l=1}^{L} \mathcal{S}_l(\varepsilon, \mathsf{R}, \mathsf{R}_1, \ldots, \mathsf{R}_L, \mathcal{P}_{\mathsf{x}}^\star)$ stated in definition 3.

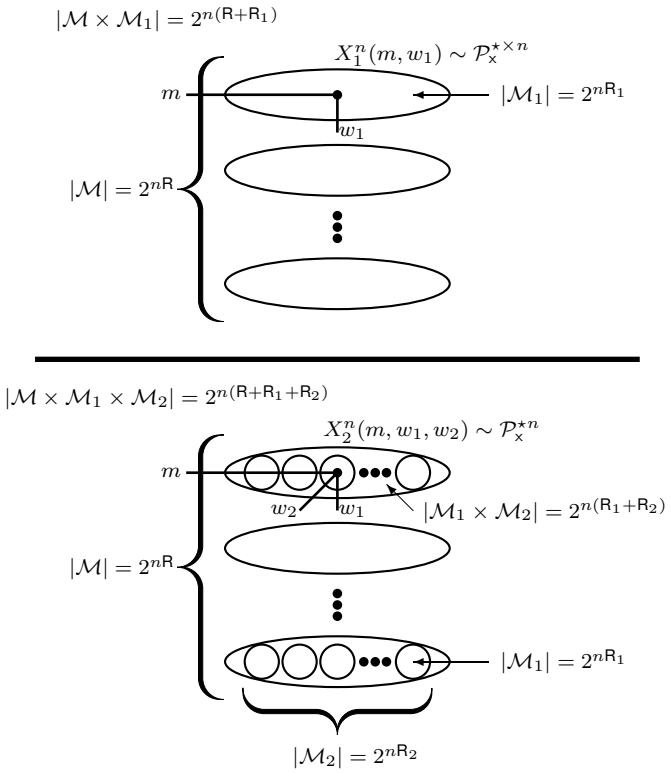


Fig. 14. Binning scheme of the random HARQ-code $C \in \mathcal{C}(n, \mathsf{R}, L)$ stated in section A-A for $L = 2$ transmissions. The parameters $n \in \mathbb{N}$, $\in \mathbb{R}^+$, $\mathsf{R} \in \mathbb{R}^+$, $\mathsf{R}_1 \in \mathbb{R}^+$, $\mathsf{R}_2 \in \mathbb{R}^+$ determine the cardinalities of the set of messages $|\mathcal{M}| = 2^{n\mathsf{R}}$, the cardinality of the bins $|\mathcal{M}_1| = 2^{n\mathsf{R}_1}$ and the number of sub-bins $|\mathcal{M}_2| = 2^{n\mathsf{R}_2}$. The random codewords $X_1^n(m, w_1)$ and $X_2^n(m, w_1, w_2)$ are generated with i.i.d. probability distribution $\mathcal{P}_{\mathsf{x}}^{\star \times n}$.

A. Random HARQ-Code

We consider a random HARQ-code $C \in \mathcal{C}(n, \mathsf{R}, L)$ with stochastic encoder, represented by figure 14 for $L = 2$ transmissions and defined as follows:

- *Random codebook for the first transmission.* Generate $|\mathcal{M} \times \mathcal{M}_1| = 2^{n(\mathsf{R}+\mathsf{R}_1)}$ sequences $X_1^n \in \mathcal{X}$ drawn from the probability distribution $\mathcal{P}_{\mathsf{x}}^{\star \times n}$. Randomly bin them into $|\mathcal{M}| = 2^{n\mathsf{R}}$ bins denoted by $m \in \mathcal{M}$, each of them containing $|\mathcal{M}_1| = 2^{n\mathsf{R}_1}$ sequences $X_1^n \in \mathcal{X}^n$ indexed by the parameter $w_1 \in \mathcal{M}_1$.
- *Encoding for the first transmission.* The encoder observes the realization of the message $m \in \mathcal{M}$. It chooses at random the parameter $w_1 \in \mathcal{M}_1$ using the uniform probability distribution and sends the sequence of channel inputs $x_1^n(m, w_1)$ through the channel $\mathcal{T}_1$.
- *First feedback from the decoder.* The decoder observes the realization of the channel state $k_1 \in \mathcal{K}_1$ and sends to the encoder the feedback "Ack_1" if it can decode after the first transmission (i.e. equation (34) is not satisfied). It sends the feedback "Nack_1" if it can not decode after the first transmission (i.e. equation (34) is satisfied).
- *Decoding fonction for "Ack_1".* The decoder observes the state parameter $k_1 \in \mathcal{K}_1$ and finds the pair of indexes $(m, w_1) \in \mathcal{M} \times \mathcal{M}_1$ 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 channel outputs. Its returns the index $m \in \mathcal{M}$ of the transmitted message.
- *Random codebook for the second transmission.* Generate $|\mathcal{M} \times \mathcal{M}_1 \times \mathcal{M}_2| = 2^{n(\mathsf{R}+\mathsf{R}_1+\mathsf{R}_2)}$ sequences $X_2^n \in \mathcal{X}^n$ drawn from the probability distribution $\mathcal{P}_{\mathsf{x}}^{\star \times n}$. Randomly bin them into $|\mathcal{M}| = 2^{n\mathsf{R}}$ bins denoted by $m \in \mathcal{M}$, each of them containing $|\mathcal{M}_1 \times \mathcal{M}_2| = 2^{n(\mathsf{R}_1+\mathsf{R}_2)}$ sequences $X_2^n \in \mathcal{X}^n$ 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 $|\mathcal{M}_2| = 2^{n\mathsf{R}_2}$ sub-bins containing $|\mathcal{M}_1| = 2^{n\mathsf{R}_1}$ sequences $X_2^n \in \mathcal{X}^n$. 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 symboles $X_2^n(m, w_1, w_2) \in \mathcal{X}^n$.
- *Encoding for the second transmission.* If the encoder receives a "Nack_1" 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 $x_2^n(m, w_1, w_2)$.
- *Second feedback from the decoder.* The decoder observes the realization of the channel state $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$ and sends to the encoder the feedback "Ack_2" if it can decode (i.e. equation (33) is satisfied). It sends the feedback "Nack_2" if it can not decode (i.e. equation (33) is satisfied).
- *Decoding function for "Ack_2".* The decoder observes the state parameters $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$ and finds the triple of indexes $(m, w_1, w_2) \in \mathcal{M} \times \mathcal{M}_1 \times \mathcal{M}_2$ 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 $x_2^n(m, w_1, w_2) \in A_\varepsilon^{\star n}(y_2^n | k_2)$ 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.
- *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 $(x_1^n, y_1^n, z_1^n) \notin A_\varepsilon^{\star n}(\mathcal{Q}_1 | k_1)$ or $(x_2^n, y_2^n, z_2^n) \notin A_\varepsilon^{\star n}(\mathcal{Q}_2 | k_2)$ are not jointly typical for the probability distributions $\mathcal{Q}_1 = \mathcal{P}_{\mathsf{x}}^\star \times \mathcal{T}_1 \in \Delta(\mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Z}_1)$ and $\mathcal{Q}_2 = \mathcal{P}_{\mathsf{x}}^\star \times \mathcal{T}_2 \in \Delta(\mathcal{X} \times \mathcal{Y}_2 \times \mathcal{Z}_2)$.

Remark 10 The parameter $n \in \mathbb{N}$ is the length of the transmission bloc, $|\mathcal{M}| = 2^{n\mathsf{R}}$ is the cardinality of the set of messages $\mathcal{M}$, $|\mathcal{M}_1| = 2^{n\mathsf{R}_1}$ is the cardinality of the set of dummy-messages $\mathcal{M}_1$ for the first transmission and $|\mathcal{M}_2| = 2^{n\mathsf{R}_2}$ is the cardinality of the set of dummy-messages $\mathcal{M}_2$ for the second transmission. We denote by $\mathcal{P}_{\mathsf{x}}^\star \in \Delta(\mathcal{X})$ 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 $(k_1, k_2) \in$

$\mathcal{S}_1^c(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathcal{P}_{\mathsf{x}}^\star)\cap\mathcal{S}_2(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathsf{R}_2,\mathcal{P}_{\mathsf{x}}^\star)$.

$$\mathbb{E}_c\Bigg[\mathcal{P}\Bigg(\Bigg\{(x_1^n,y_1^n,z_1^n)\notin A_\varepsilon^{\star n}(\mathcal{Q}_1|k_1)\Bigg\} \cup\Bigg\{(x_2^n,y_2^n,z_2^n)\notin A_\varepsilon^{\star n}(\mathcal{Q}_2|k_2)\Bigg\}\Bigg)\Bigg]\leq\varepsilon, \tag{39}$$

$$\mathbb{E}_c\Bigg[\mathcal{P}\Bigg(\Bigg\{\exists(m',w_1',w_2')\neq(m,w_1,w_2),\ \text{s.t.} \{x_1^n(m',w_1')\in A_\varepsilon^{\star n}(y_1^n|k_1)\} \cap\{x_2^n(m',w_1',w_2')\in A_\varepsilon^{\star n}(y_2^n|k_2)\}\Bigg\}\Bigg)\Bigg]\leq\varepsilon, \tag{40}$$

$$\mathbb{E}_c\Bigg[\mathcal{P}\Bigg(\Bigg\{\exists(m',w_1')\neq(m,w_1),\ \text{s.t.} \{x_1^n(m',w_1')\in A_\varepsilon^{\star n}(y_1^n|k_1)\} \cap\{x_2^n(m',w_1',w_2)\in A_\varepsilon^{\star n}(y_2^n|k_2)\}\Bigg\}\Bigg)\Bigg]\leq\varepsilon, \tag{41}$$

$$\mathbb{E}_c\Bigg[\mathcal{P}\Bigg(\Bigg\{\exists w_2'\neq w_2,\ \text{s.t.} \ x_2^n(m,w_1,w_2')\in A_\varepsilon^{\star n}(y_2^n|k_2)\Bigg\}\Bigg)\Bigg]\leq\varepsilon. \tag{42}$$

(39) comes from the typical sequences [49, pp. 26].
(40) comes from (33) and [49, pp. 46, Packing Lemma] since the codewords $(X_1^n(m',w_1'),X_2^n(m',w_1',w_2'))$ are independent of $(X_1^n(m,w_1),X_2^n(m,w_1,w_2))$.
(41) comes from (33) and [49, pp. 46, Packing Lemma].
(42) comes from (37) and [49, pp. 46, Packing Lemma].

This provides an upper bound on:

$$\mathbb{E}_c\Bigg[\mathcal{P}_{\mathsf{e}}\Bigg(C\Bigg|k_1,k_2\Bigg)\Bigg] \qu\leq\quad 4\varepsilon. \tag{43}$$

C. Expected information leakage rate

We provide an upper bound on the expected information leakage rate that is valid for all channel states $(k_1,k_2)\in\mathcal{S}_1^c(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathcal{P}_{\mathsf{x}}^\star)\cap\mathcal{S}_2(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathsf{R}_2,\mathcal{P}_{\mathsf{x}}^\star)$. To this purpose, we introduce four auxiliary random variables V_1, J_1, V_2 and J_2 that belong to the sets $\mathcal{M}_{\mathsf{V}_1}$, $\mathcal{M}_{\mathsf{J}_1}$, $\mathcal{M}_{\mathsf{V}_2}$ and $\mathcal{M}_{\mathsf{J}_2}$ with cardinality $|\mathcal{M}_{\mathsf{V}_1}|=2^{n\mathsf{R}_{\mathsf{V}_1}}$, $|\mathcal{M}_{\mathsf{J}_1}|=2^{n\mathsf{R}_{\mathsf{J}_1}}$, $|\mathcal{M}_{\mathsf{V}_2}|=2^{n\mathsf{R}_{\mathsf{V}_2}}$ and $|\mathcal{M}_{\mathsf{J}_2}|=2^{n\mathsf{R}_{\mathsf{J}_2}}$ given by:

$$\begin{aligned}
\mathsf{R}_{\mathsf{V}_1} &= I(X_1;Z_1|k_1)+I(X_2;Z_2|k_2) \\
&- \min\Bigg(I(X_2;Z_2|k_2),\mathsf{R}_2\Bigg)-4\varepsilon, &(44)\\
\mathsf{R}_{\mathsf{V}_2} &= \min\Bigg(I(X_2;Z_2|k_2),\mathsf{R}_2\Bigg)-4\varepsilon, &(45)\\
\mathsf{R}_{\mathsf{J}_1} &= \mathsf{R}_1-\mathsf{R}_{\mathsf{V}_1} \\
&= \min\Bigg(\mathsf{R}_1-I(X_1;Z_1|k_1)+4\varepsilon,\mathsf{R}_1+\mathsf{R}_2 \\
&- I(X_1;Z_1|k_1)-I(X_2;Z_2|k_2)+4\varepsilon\Bigg), &(46)\\
\mathsf{R}_{\mathsf{J}_2} &= \mathsf{R}_2-\mathsf{R}_{\mathsf{V}_2} \\
&= \max\Bigg(\mathsf{R}_2-I(X_2;Z_2|k_2),0\Bigg)+4\varepsilon. &(47)
\end{aligned}$$

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 $\mathsf{R}_{\mathsf{V}_1}$, $\mathsf{R}_{\mathsf{V}_2}$ and $\mathsf{R}_{\mathsf{J}_2}$ are positive. Equations (35) and (36) guarantees that parameter $\mathsf{R}_{\mathsf{J}_1}$ is positive for all channel states $(k_1,k_2)\in\mathcal{S}_1^c(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathcal{P}_{\mathsf{x}}^\star)\cap\mathcal{S}_2(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathsf{R}_2,\mathcal{P}_{\mathsf{x}}^\star)$. In this section, each bin $m\in\mathcal{M}$ is re-organized as follows:

- First, we divide each sub-bin $w_2\in\mathcal{M}_2$ of size $2^{n\mathsf{R}_1}$ into $2^{n\mathsf{R}_{\mathsf{J}_1}}$ sub-sub-bins of size $2^{n\mathsf{R}_{\mathsf{V}_1}}$.
- Second, we concatenate the sub-bins $w_2\in\mathcal{M}_2$ into $2^{n\mathsf{R}_{\mathsf{J}_2}}$ super-sub-bins containing $2^{n\mathsf{R}_{\mathsf{V}_2}}$ sub-bins $w_2\in\mathcal{M}_2$.

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 $W_2=(V_2,J_2)$.

$$\begin{aligned}
& n\cdot\mathbb{E}_c\Bigg[\mathcal{L}_{\mathsf{e}}\Bigg(C\Bigg|k_1,k_2\Bigg)\Bigg] \\
=\ & I(M,W_1,W_2;Z_1^n,Z_2^n|C,k_1,k_2) &(48)\\
-\ & H(W_1,W_2|M,C,k_1,k_2) &(49)\\
+\ & H(W_1,W_2|M,C,Z_1^n,Z_2^n,k_1,k_2). &(50)
\end{aligned}$$

- The first term (48) satisfies:

$$\begin{aligned}
& I(M,W_1,W_2,C;Z_1^n,Z_2^n|k_1,k_2) \\
\leq\ & I(X_1^n,X_2^n;Z_1^n,Z_2^n|k_1,k_2) &(51)\\
=\ & n\cdot(I(X_1;Z_1|k_1)+\cdot I(X_2;Z_2|k_2)). &(52)
\end{aligned}$$

(51) comes from the Markov chain $(C,M,W_1,W_2)\multimap(X_1^n,X_2^n)\multimap(Z_1^n,Z_2^n)$ for all channel states $(k_1,k_2)\in\mathcal{S}_1^c(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathcal{P}_{\mathsf{x}}^\star)\cap\mathcal{S}_2(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathsf{R}_2,\mathcal{P}_{\mathsf{x}}^\star)$.
(52) comes from the independent generation of the sequences X_1^n and X_2^n with i.i.d. probability distributions $\mathcal{P}_{\mathsf{x}}^\star$.

- The second term (49) satisfies:

$$H(W_1,W_2|M,C,k_1,k_2)=n\cdot(\mathsf{R}_1+\mathsf{R}_2). \tag{53}$$

(53) comes from the fact that the random variable W_1 and W_2 are drawn independently of (M,C,k_1,k_2) and uniformly distributed over the sets $\mathcal{M}_1$, $\mathcal{M}_2$ of cardinality $2^{n\mathsf{R}_1}$, $2^{n\mathsf{R}_2}$.

- The third term (50) satisfies:

$$\begin{aligned}
& H(W_1,W_2|M,C,Z_1^n,Z_2^n,k_1,k_2) \\
=\ & H(V_1,J_1,V_2,J_2|M,C,Z_1^n,Z_2^n,k_1,k_2) &(54)\\
=\ & H(J_1,J_2|M,C,Z_1^n,Z_2^n,k_1,k_2) \\
+\ & H(V_1,V_2|J_1,J_2,M,C,Z_1^n,Z_2^n,k_1,k_2) &(55)\\
\leq\ & n\cdot(\mathsf{R}_{\mathsf{J}_1}+\mathsf{R}_{\mathsf{J}_2}) \\
+\ & H(V_1,V_2|J_1,J_2,M,C,Z_1^n,Z_2^n,k_1,k_2) &(56)\\
=\ & n\cdot\Bigg(\mathsf{R}_1+\mathsf{R}_2-I(X_1;Z_1|k_1)-I(X_2;Z_2|k_2)+8\varepsilon\Bigg) \\
+\ & H(V_1,V_2|J_1,J_2,M,C,Z_1^n,Z_2^n,k_1,k_2) &(57)\\
\leq\ & n\cdot\Bigg(\mathsf{R}_1+\mathsf{R}_2-I(X_1;Z_1|k_1)-I(X_2;Z_2|k_2) \\
+\ & \varepsilon\cdot\Big(9+20\log_2|\mathcal{X}|\Big)\Bigg). &(58)
\end{aligned}$$

(54) comes from replacing indexes $(w_1,w_2)\in\mathcal{M}_1\times\mathcal{M}_2$ by auxiliary indexes $(v_1,j_1,v_2,j_2)\in\mathcal{M}_{\mathsf{V}_1}\times\mathcal{M}_{\mathsf{J}_1}\times\mathcal{M}_{\mathsf{V}_2}\times\mathcal{M}_{\mathsf{J}_2}$.
(55) and (56) come from the properties of the entropy function and the cardinalities $|\mathcal{M}_{\mathsf{J}_1}|=2^{n\mathsf{R}_{\mathsf{J}_1}}$ and $|\mathcal{M}_{\mathsf{J}_2}|=2^{n\mathsf{R}_{\mathsf{J}_2}}$.
(57) comes from the equations (46) and (47),

satisfied for all channel states $(k_1,k_2) \in \mathcal{S}_1^c(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathcal{P}_{\mathsf{x}}^\star) \cap \mathcal{S}_2(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathsf{R}_2,\mathcal{P}_{\mathsf{x}}^\star)$ and the equation: $\max(\mathsf{a},\mathsf{b})+\min(\mathsf{a},\mathsf{b})=\mathsf{a}+\mathsf{b}$.
(58) comes from Lemma 1, that is based on Fano's inequality.

Equations (52), (53) and (58) provide an upper bound on:

$$\mathbb{E}_c\Big[\mathcal{L}_{\mathsf{e}}\Big(C\Big|k_1,k_2\Big)\Big] \;\leq\; \varepsilon\cdot\big(9+20\log_2|\mathcal{X}|\big). \quad (59)$$

This analysis can be extended to the case of $L>2$ transmissions by introducing the random variables $\mathsf{R}_{\mathsf{V}_\mathsf{L}}$ and $\mathsf{R}_{\mathsf{J}_\mathsf{L}}$.

Lemma 1 *Fano's inequality provides the upper bound:*

$$\begin{aligned} &H(V_1,V_2|J_1,J_2,M,C,Z_1^n,Z_2^n,k_1,k_2)\\ \leq\;& n\cdot\Big(\varepsilon+20\varepsilon\cdot\log_2|\mathcal{X}|\Big). \end{aligned} \quad (60)$$

Proof. [Lemma 1] Suppose that the eavesdropper implements the decoding g_{e} defined by equation (61) as follows:

- *Decoding of the eavesdropper* g_{e} takes the sequence of channel outputs $Z_1^n\in\mathcal{Z}_1^n$, $Z_2^n\in\mathcal{Z}_2^n$, the message $M\in\mathcal{M}$, the indexes $J_1\in\mathcal{M}_{\mathsf{J}_1}$, $J_2\in\mathcal{M}_{\mathsf{J}_2}$ and the HARQ-code $C\in\mathcal{C}(n,\mathsf{R},L)$ and returns the indexes $V_1\in\mathcal{M}_{\mathsf{V}_1}$, $V_2\in\mathcal{M}_{\mathsf{V}_2}$ and the sequences $X_1^n(M,V_1,J_1)\in\mathcal{X}^n$ and $X_2^n(M,V_1,J_1,V_2,J_2)\in\mathcal{X}^n$ that are jointly typical with $Z_1^n\in\mathcal{Z}_1^n$ and $Z_2^n\in\mathcal{Z}_2^n$.

$$\begin{aligned} g_{\mathsf{e}}:\;& \mathcal{Z}_1^n\times\mathcal{Z}_2^n\times\mathcal{M}\times\mathcal{M}_{\mathsf{J}_1}\times\mathcal{M}_{\mathsf{J}_2}\\ &\times\mathcal{K}_1\times\mathcal{K}_2\times\mathcal{C}(n,\mathsf{R},\mathsf{R}_{\mathsf{W}},\mathsf{R}_{\mathsf{L}},\mathcal{P}_{\mathsf{x}_1}^\star,\mathcal{P}_{\mathsf{x}_2}^\star)\\ &\longrightarrow \mathcal{X}^n\times\mathcal{X}^n\times\mathcal{M}_{\mathsf{V}_1}\times\mathcal{M}_{\mathsf{V}_2}. \end{aligned} \quad (61)$$

An error occurs if this decoding function g_{e} returns sequences of inputs and indexes $(\hat{x}_1^n,\hat{x}_2^n,\hat{v}_1,\hat{v}_2)\neq g_{\mathsf{e}}(z_1^n,z_2^n,m,j_1,j_2,c,k_1,k_2)$ 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}.

$$\begin{aligned} &\mathbb{E}_c\Big[\mathcal{P}\Big(\Big\{(x_1^n,z_1^n)\notin A_\varepsilon^{\star n}(\mathcal{Q}_1|k_1)\Big\}\\ &\quad\cup\Big\{(x_2^n,z_2^n)\notin A_\varepsilon^{\star n}(\mathcal{Q}_2|k_2)\Big\}\Big)\Big]\leq\varepsilon, \end{aligned} \quad (62)$$

$$\begin{aligned} &\mathbb{E}_c\Big[\mathcal{P}\Big(\Big\{\exists(v_1',v_2')\neq(v_1,v_2),\ \text{s.t.}\\ &\quad\{x_1^n(m,v_1',j_1)\in A_\varepsilon^{\star n}(z_1^n|k_1)\}\\ &\quad\cap\{x_2^n(m,v_1',j_1,v_2',j_2)\in A_\varepsilon^{\star n}(z_2^n|k_2)\}\Big\}\Big)\Big]\leq\varepsilon, \end{aligned} \quad (63)$$

$$\begin{aligned} &\mathbb{E}_c\Big[\mathcal{P}\Big(\Big\{\exists v_1'\neq v_1,\ \text{s.t.}\\ &\quad\{x_1^n(m,v_1',j_1)\in A_\varepsilon^{\star n}(z_1^n|k_1)\}\\ &\quad\cap\{x_2^n(m,v_1',j_1,v_2,j_2)\in A_\varepsilon^{\star n}(z_2^n|k_2)\}\Big\}\Big)\Big]\leq\varepsilon, \end{aligned} \quad (64)$$

$$\begin{aligned} &\mathbb{E}_c\Big[\mathcal{P}\Big(\Big\{\exists v_2'\neq v_2,\ \text{s.t.}\\ &\quad x_2^n(m,v_1,j_1,v_2',j_2)\in A_\varepsilon^{\star n}(z_2^n|k_2)\Big\}\Big)\Big]\leq\varepsilon. \end{aligned} \quad (65)$$

(62) comes from properties of typical sequences [49, pp. 26].
(63) comes from (44), (45) and [49, pp. 46, Packing Lemma].
(64) comes from (44) and [49, pp. 46, Packing Lemma].
(65) comes from (45) and [49, pp. 46, Packing Lemma].

Equations (62), (63), (64) and (65) prove that the expected probability of this decoding g_e is upper bounded by 4ε.

$$\begin{aligned} &H(V_1,V_2|M,J_1,J_2,C,Z_1^n,Z_2^n,k_1,k_2)\\ \leq\;& n\cdot\Big(\varepsilon+20\cdot\varepsilon\cdot\log_2|\mathcal{X}|\Big). \end{aligned} \quad (66)$$

Equation (66) comes from [49, pp. 19, Fano's Inequality] and $n\geq n_9=\frac{1}{\varepsilon}$ and equations (44) and (45) which imply that $\log_2|\mathcal{M}_{\mathsf{V}_1}|\leq 2n\cdot\log_2|\mathcal{X}|$ and $\log_2|\mathcal{M}_{\mathsf{V}_2}|\leq n\cdot\log_2|\mathcal{X}|$. □

D. Conclusion

For all $\varepsilon>0$, there exists $\bar{n}$, for all $n\geq\bar{n}$, there exists HARQ-code $c^\star\in\mathcal{C}(n,\mathsf{R},L)$ such that $\mathcal{P}_{\mathsf{e}}\big(c^\star\big|k_1,k_2\big)\leq\varepsilon$ and $\mathcal{L}_{\mathsf{e}}\big(c^\star\big|k_1,k_2\big)\leq\varepsilon$, for all $(k_1,k_2)\in\mathcal{S}_1^c(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathcal{P}_{\mathsf{x}}^\star)\cap\mathcal{S}_2(\varepsilon,\mathsf{R},\mathsf{R}_1,\mathsf{R}_2,\mathcal{P}_{\mathsf{x}}^\star)$.

APPENDIX B
PROOF OF PROPOSITION 7

Proof. We assume that the random events $(\mathcal{B}_l)_{l\in\{1,\dots,L\}}$ are independent of the random events $(\mathcal{A}_l)_{l\in\{1,\dots,L\}}$.

$$\mathcal{P}_{\mathsf{so}} = \mathcal{P}\Big(\bigcup_{i=1}^{L}\mathcal{B}_i^c\Big)=1-\mathcal{P}\Big(\bigcap_{i=1}^{L}\mathcal{B}_i\Big) \quad (67)$$

$$= 1-\sum_{j=1}^{L}\mathcal{P}\Big(\bigcap_{i=1}^{j}\mathcal{B}_i\Big|\mathsf{L}=j\Big)\cdot\mathcal{P}\Big(\mathsf{L}=j\Big) \quad (68)$$

$$= 1-\sum_{j=1}^{L}\mathcal{P}\Big(\bigcap_{i=1}^{j}\mathcal{B}_i\Big)\cdot\mathcal{P}\Big(\mathsf{L}=j\Big) \quad (69)$$

$$\begin{aligned} &= 1-\sum_{j=2}^{L-1}\mathcal{P}\Big(\bigcap_{i=1}^{j}\mathcal{B}_i\Big)\cdot\Big(\mathcal{P}\Big(\bigcap_{i=1}^{j-1}\mathcal{A}_i^c\Big)-\mathcal{P}\Big(\bigcap_{i=1}^{j}\mathcal{A}_i^c\Big)\Big)\\ &\quad-\mathcal{P}\Big(\mathcal{B}_1\Big)\cdot\mathcal{P}\Big(\mathcal{A}_1\Big)-\mathcal{P}\Big(\bigcap_{i=1}^{L}\mathcal{B}_i\Big)\cdot\mathcal{P}\Big(\bigcap_{i=1}^{L-1}\mathcal{A}_i^c\Big). \end{aligned} \quad (70)$$

(67) comes from the properties of the probability $\mathcal{P}_{\mathsf{so}}$.
(68) comes from the definition of the HARQ-code, if j transmissions occurs, then $\bigcup_{i=1}^{L}\mathcal{B}_i^c=\bigcup_{i=1}^{j}\mathcal{B}_i^c$.
(69) comes from the independence of the events $(\mathcal{B}_l)_{l\in\{1,\dots,L\}}$ with events $(\mathcal{A}_l)_{l\in\{1,\dots,L\}}$ hence with transmission number L.
(70) comes from the probability of having L transmission. □

APPENDIX C
PROOF OF THEOREM 9

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

$$\mathcal{P}_{\mathsf{co}}=1-e^{-\frac{2^{\mathsf{R}_1}-1}{\gamma_{\mathsf{d}}}}\leq\xi_{\mathsf{c}},\quad \mathcal{P}_{\mathsf{so}}=e^{-\frac{2^{\mathsf{R}_1}-1}{\gamma_{\mathsf{e}}}}\leq\xi_{\mathsf{s}}. \quad (71)$$

ξ_{c} and ξ_{s} are compatible if there exists R_1 satisfying (71), i.e.,

$$\log_2\Big(1-\gamma_{\mathsf{e}}\cdot\ln(\xi_{\mathsf{s}})\Big)\leq\mathsf{R}_1\leq\log_2\Big(1-\gamma_{\mathsf{d}}\cdot\ln\Big(1-\xi_{\mathsf{c}}\Big)\Big).$$

The existence of parameter R_1 is given by the above inequalities and this proves the first point of Theorem 9.
Second Point. The parameter R_1 should satisfy :

$$\log_2(1-\gamma_{\mathsf{e}}\cdot\ln(\xi_{\mathsf{s}}))\leq\mathsf{R}_1\leq\log_2(1-\gamma_{\mathsf{d}}\cdot\ln(1-\xi_{\mathsf{c}}))-\mathsf{R}.$$

Hence, the parameter R_1 exists if and only if:

$$\mathsf{R} \leq \log_2 \left(\frac{1 - \gamma_{\mathsf{d}} \cdot \ln(1 - \xi_{\mathsf{c}})}{1 - \gamma_{\mathsf{e}} \cdot \ln(\xi_{\mathsf{s}})} \right).$$

□

REFERENCES

[1] M. Le Treust, L. Szczecinski, and F. Labeau, "Secrecy & rate adaptation for secure HARQ protocols," in *Proc. 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. Telatar and R. G. Gallager, "Combining queueing theory with information theory for multiaccess," *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 channel," *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 diversity 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-division 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. Pfletschinger and M. Navarro, "Adaptive HARQ for imperfect channel knowledge," in *International ITG Conference on Source and Channel Coding (SCC)*, Jan. 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 Inter. 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. Jabi, 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. Piantanida, "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. Guillen 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. Hausl and A. Chindapol, "Hybrid ARQ with cross-packet channel coding," *IEEE Commun. Lett.*, vol. 11, no. 5, pp. 434–436, May 2007.

[20] J. Chui 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.

[21] D. Duyck, D. Capirone, C. Hausl, and M. Moeneclaey, "Design of diversity-achieving LDPC codes for H-ARQ with cross-packet channel coding," in *IEEE 21st Int. Symp. on Personal Indoor and Mobile Radio Communications (PIMRC)*, 2010, pp. 263–268.

[22] K. Trillingsgaard and P. Popovski, "Block-fading channels with delayed CSIT at finite blocklength," in *IEEE Inter. Symp. Inf. Theory (ISIT)*, June 2014, pp. 2062–2066.

[23] K. D. Nguyen, R. Timo, and L. K. Rasmussen, "Causal-CSIT rate adaptation for block-fading channels," in *IEEE Inter. Symp. Inf. Theory (ISIT)*, June 2015, pp. 351–355.

[24] A. Benyouss, M. Jabi, M. Le Treust, and L. Szczecinski, "Joint coding/decoding for multi-message HARQ," *Proc. of the IEEE Proc. of the Wireless Comm. and Networking Conf. (WCNC), Doha, Quatar*, 2016.

[25] M. Jabi, A. Benyouss, M. Le Treust, E. Pierre-Doray, and L. Szczecinski, "Adaptative cross-packet HARQ," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2022 – 2035, 2017.

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

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

[28] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, 1978.

[29] M. Bloch and J. Barros, *Physical Layer Security-From Information Theory to Security Engineering*. Cambridge University Press, Oct. 2011.

[30] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[31] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2453–2469, 2008.

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

[33] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[34] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2799, Sept. 2010.

[35] M. R. Bloch and J. N. Laneman, "Exploiting partial channel state information for secrecy over wireless channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1840–1849, Sept. 2013.

[36] Z. Rezki, A. Khisti, and M. S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652–3664, Oct. 2014.

[37] P. H. Lin and E. Jorswieck, "On the fast fading Gaussian wiretap channel with statistical channel state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 46–58, Jan. 2016.

[38] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, March 2011.

[39] 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, no. 4, pp. 1575–1591, Aug. 2009.

[40] Z. Mheich, M. Le Treust, F. Alberge, P. Duhamel, and L. Szczecinski, "Rate-adaptive secure HARQ protocol for block-fading channels," in *22nd European Signal Processing Conference (EUSIPCO)*, Sept. 2014, pp. 830–834.

[41] Z. Mheich, M. Le Treust, F. Alberge, and P. Duhamel, "Rate adaptation for incremental redundancy secure HARQ," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 765–777, Feb. 2016.

[42] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, June 2012.

[43] S. Tomasin and N. Laurenti, "Secure HARQ with multiple encoding over block fading channels: Channel set characterization and outage analysis," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1708–1719, Oct. 2014.

[44] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *IEEE Inter. Symp. Inf. Theory (ISIT)*, June 2014, pp. 601–605.

[45] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3863–3879, July 2016.

[46] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[47] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, June 2016.

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

[49] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, Dec. 2011.