On the Secure Spectral Efficiency of URLLC with Randomly Located Colluding Eavesdroppers

Jamil Farhat, Glauber Brante, Richard Demo Souza, and João P. Vilela

***Abstract*—In this paper we investigate the secure spectral efficiency of an ultra-reliable low-latency communication (URLLC) system, where communications occur with short packets due to delay constraints, so that a finite blocklength formulation is considered. In addition, we assume that no feedback channel is available to implement automatic repeat request schemes, so that packet replication (PR) and interface diversity (ID) strategies are used to improve performance, which are then compared in terms of physical layer security while considering a Nakagami-m fading channel. Furthermore, we assume no knowledge of the instantaneous channel state information at Alice, neither with respect to Bob nor Eves, while the position of multiple colluding eavesdroppers are specified according to a Poisson Point Process (PPP). Numerical results show that the joint optimization of the blocklength, the transmit power and the amount of information bits per codeword are crucial to maximize the secure spectral efficiency. In addition, we also show that ID outperforms the PR strategy in most scenarios when the number of replications/interfaces increases.**

***Index Terms*—Physical Layer Security, Finite Blocklength, Stochastic Geometry, Packet Replication, Interface Diversity.**

I. Introduction

To provide Internet connectivity for billions of devices is a crucial requirement for wireless communications systems in 5G and beyond [1], [2]. According to [3], [4], there will be around 28 billion connected devices by 2021, of which more than 15 billion will be machine-type communications (MTC) and consumer-electronics devices. Additionally, according to [5], MTC will represent more than 29% of the total number of devices and connections by 2021.

Typical MTC scenario in 5G include traffic safety, industrial applications, remote manufacturing, *etc.* [6], all of which require high reliability while not being delay tolerant, and which are often denoted as critical MTC [4], [7]. Therefore, due to the characteristics of these applications, one of the challenges lies in building an ultra-reliable and low-latency communication (URLLC) system [2]. Furthermore, high degree of security is crucial in such scenarios [8], [9], which presents a trade-off, since low overhead is desired due to the low-latency constraints, while security mechanisms usually increase the overhead [10].

In order to reduce latency, URLLC uses short-packets. Then, the traditional capacity metrics characterized in an asymptotic regime, where the blocklength tends to infinity, can not be directly applied to the analysis and design of schemes in this context [2], [11]. The usual formulation of channel capacity represents the maximum rate that can be used for reliable communication, so that the error probability tends to zero when no restrictions are imposed to blocklength. However, when packets are shorter such analysis is not valid, and a more refined analysis is needed to determine the maximum achievable rate. Following [2], [12], [13], the maximum achievable rate with finite blocklength, $R^\star(n,\epsilon)$, is a function of the codeword length, n, and the associated packet error probability, ϵ. Therefore, an important consequence is that error probability tending to zero is not possible with short blocklengths.

The information theoretic formulation for finite blocklength performance in Rayleigh block-fading channels has been introduced in [14]. It has been shown that $R^\star(n,\epsilon)$ is not monotonic with respect to the channel coherence time, so that there exists a coherence time that maximizes $R^\star(n,\epsilon)$. More recently, a tutorial discussion on the impact of finite blocklength in terms of design and analysis of wireless communications systems is given in [2]. Moreover, the performance of resource allocation for finite blocklength has been studied by [15], while [16] analyzes the packet scheduling problem in an assembly production line considering perfect channel state information (CSI). Finally, the authors in [17] consider the trade-off between energy efficiency and spectral efficiency in a scenario without CSI.

In addition, security in MTC contexts also demands a careful rethinking [18], since complex cryptography algorithms may not be direct applicable due to *(i.)* the difficulty associated with sharing security keys in dense networks [19]; *(ii.)* the time in order to generate and share security keys in latency-sensitive networks [18]; and *(iii.)* the battery consumption due to the computational cost associated with cryptographic schemes. As a result, security at the physical layer (PHY) has gained considerable attention as a tool to improve lightweight cryptography protocols, in which the random fluctuations of the wireless channel are exploited in order to create low-complex secrecy mechanisms [20]–[22].

Considering PHY security with finite blocklength, the authors in [12] derived the bounds for the maximum secrecy rate in block-fading channels. Then, similarly to the analysis with infinite blocklength, *i.e.*, assuming Shannon capacity, the authors in [23] have shown that the secrecy capacity can still

J. Farhat and G. Brante are with the Federal University of Technology-Paraná, Brazil. E-mails: jfarhat@alunos.utfpr.edu.br, gbrante@utfpr.edu.br.

R. D. Souza is with the Federal University of Santa Catarina, Brazil, richard.demo@ufsc.br.

J. P. Vilela is with CRACS/INESC TEC and Dep. of Computer Science, Faculty of Sciences, University of Porto, as well as Centre for Informatics and Systems of the University of Coimbra, Portugal, jpvilela@dei.uc.pt.

This work was financed in part by CAPES, Finance Code 001, PrInt CAPES-UFSC "Automation 4.0", and CNPq Brazil. This work is supported by the European Regional Development Fund (FEDER), through the Regional Operational Programme of Lisbon (POR LISBOA 2020) and the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework [Project 5G with Nr. 024539 (POCI-01-0247-FEDER-024539)].

be formulated by the difference between the maximal achievable rates of legitimate and eavesdroppers channels. Then, an upper-bound for $R_s^\star(n, \epsilon, \delta)$ is provided, which represents the maximum secrecy rate given some information leakage probability (δ) with respect to the eavesdropper.

Recent studies analyze the average secrecy throughput in MTC scenarios, in which a multi-antenna eavesdropper is considered [24]. Then, many examples in the literature show that the use of retransmissions allows to adapt the communication rate in an efficient manner, so that only the necessary quantity of data is correctly decoded by the legitimate receiver, avoiding to increase the decoding probability at the eavesdroppers [25], [26]. For instance, incremental-redundancy hybrid automatic-repeat request (HARQ) is employed in [27] in order to improve secrecy, which is combined with dummy messages in the infinite blocklength regime. Moreover, colluding and non-colluding eavesdroppers are studied in [28], in which transmit antenna selection with a threshold-based diversity opportunistic scheduling is investigated.

However, the assumption of a feedback channel, required by HARQ schemes, may not be viable in URLLC scenarios, due to the communication latency associated with these protocols. Thus, other methods must be employed to improve the reliability of the system. The two alternatives considered in this work are packet replication (PR) and interface diversity (ID). With PR, the reliability is increased by the replication of the transmitted codewords, which occurs without the use of confirmation messages as in HARQ, *i.e.*, without the request from the legitimate receiver. Then, different from HARQ schemes, the receiver does not employ the downlink channel to transmit ACK/NACK packets due to the strict latency requirement, what is an advantage in terms of URLLC.

On the other hand, with ID the transmission occurs simultaneously using different communication interfaces, which can be of different technologies [29]. Let us remark that most mobile devices already have multiple radio interfaces, and this should even increase with 5G radios [30]. Therefore, interface diversity offers an additional degree of diversity which can be used to fulfil the stringent latency-reliability requirements. Then, with ID a packet coding is employed to distribute coded payload and redundancy data across the multiple available interfaces. An overview related to the concept of multi-connectivity and the proposal of an architecture candidate to enable such technique in cellular systems is presented in [31], while a framework combining reliability models with latency probability distributions to measure the performance of path diversity schemes has been proposed in [32].

In this paper, we analyze the PHY security in a scenario where the legitimate nodes employ either PR or ID, while we also assume multiple, randomly located, colluding eavesdroppers following a Poisson Point Process (PPP). To the best of our knowledge, the PHY security analysis of PR and ID strategies has not yet been considered in the literature. We also assume a delay-critical scenario, so that we employ a finite blocklength framework for analysis, while the legitimate transmitter has no knowledge of the instantaneous channel state information (CSI), since a feedback channel is not available. Then, the secure spectral efficiency connecting the packet error probability at the legitimate receiver and the information leakage at the eavesdroppers is employed, considering Nakagami-m fading channels. Our results show that the joint optimization of blocklength, transmit power, and the amount of information bits per codeword are crucial to maximize the secure spectral efficiency. Additionally, different from other works in the literature without secrecy constraints, we show that the increase of the maximum number of replications/interfaces is not always beneficial for the legitimate nodes, since the accumulated data is also beneficial for the eavesdroppers. Finally, we compare the proposed strategies and demonstrate that, in most scenarios, ID outperforms PR when the number of replications/interfaces increases.

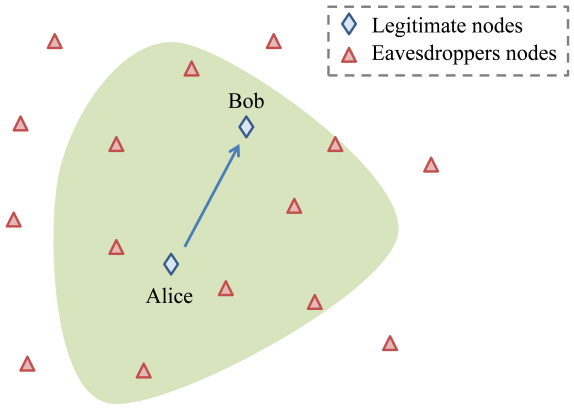

Fig. 1. System model considering a $\mathbb{R}^2$ plane with Alice communicating with Bob in the presence of multiple randomly located eavesdroppers, following a PPP with intensity λ_{E}.

The remainder of this paper is organized as follows. Section II presents the system model, while PR and ID schemes are described in Section III. The proposed optimization is introduced in Section IV, while some numerical examples are given in Section V. Finally, Section VI concludes the paper.

II. System Model

We consider two legitimate users, Alice (A) and Bob (B) communicating in the presence of multiple random located colluding Eves (E), or eavesdroppers. The spatial location of nodes can be modeled either deterministically or stochastically. In many cases, the node positions are unknown to the network designer *a priori*, so they may be treated as uniformly random according to a PPP [33]. Therefore, we assume that transmission occurs in a $\mathbb{R}^2$ plane, with the location of the eavesdroppers following a homogeneous PPP denoted by Φ_{E}, with intensity λ_{E}, as shown in Fig. 1. Additionally, for convenience, the frequently used notations are summarized in Table I.

A. Transmission Model

Given a transmission from Alice, the signal received at node $j \in \{\mathrm{B}, \mathrm{E}\}$ is

$$\mathbf{y} = \sqrt{\kappa_j P}\, h_j\, \mathbf{x} + \mathbf{w}_j, \tag{1}$$

where P is the transmit power, $\mathbf{x}$ is the signal vector composed of n symbols transmitted over a complex block-fading

TABLE I
FREQUENTLY USED NOTATIONS

Notation	Definition
P	Transmit power
h_j	Complex block-fading channel
m	Nakagami-m fading parameter
γ_j	Instantaneous signal-to-noise ratio
B	System bandwidth
κ_j	Path-loss parameter
G	Total antenna gain
f_{c}	Carrier frequency
c	Speed of light
υ	Path-loss exponent
M_{l}	Link margin
N_{f}	Noise figure
r_j	Distance between Alice and node j
C	Ergodic capacity of the channel
n	Codeword length
k_{B}	Number of bits transmitted by Alice
k_{E}	Number of equivocation bits
$\mathcal{R}_{\mathrm{B}}$	Alice-Bob channel rate
$\mathcal{R}_{\mathrm{E}}$	Colluding eavesdroppers' equivocation rate
$\mathcal{R}_{\mathrm{S}}$	Secure rate communication
δ	Maximum delay constraint
L	Total replicas or independent interfaces
k	Minimal number of fragments
ϵ	Packet error probability
ω	Total number of channel uses
τ_{S}	Secure spectral efficiency

channel with envelop h_j, modeled according to a Nakagami-m distribution, and $\mathbf{w}_j$ is the zero-mean complex Gaussian noise vector with variance $N_0/2$ per dimension, with N_0 being the unilateral noise power spectral density. Moreover, the path-loss is given by [34]

$$\kappa_j = \frac{G}{(4\pi f_{\mathrm{c}}/c)^2\, r_j^{\upsilon}\, M_{\mathrm{l}}\, N_{\mathrm{f}}}, \tag{2}$$

where G is the total antenna gain, f_{c} is the carrier frequency, c is the speed of light, υ is the path-loss exponent, M_{l} is the link margin, N_{f} is the noise figure at j, while r_j is the distance between Alice and the receiving node.

Then, the instantaneous signal-to-noise ratio (SNR) at the receiver is

$$\gamma_j = |h_j|^2\, \bar{\gamma}_j, \tag{3}$$

where

$$\bar{\gamma}_j = \frac{\kappa_j P}{N_0 B}, \tag{4}$$

with B being the system bandwidth.

B. Maximal Achievable Rate

When considering finite blocklength, the maximum achievable rate in a given fixed link is [2]

$$R^{\star}(n,\epsilon) = C - \sqrt{\frac{V}{n}}\, Q^{-1}(\epsilon) + \mathcal{O}\left(\frac{\log(n)}{n}\right), \tag{5}$$

where n is the length of the employed codeword, ϵ is the packet error probability, $\mathcal{O}\left(\frac{\log(n)}{n}\right)$ represents terms of order $\frac{\log(n)}{n}$, C is the ergodic capacity of the channel and $Q^{-1}(.)$ is the inverse of the Q-function. Additionally, $V = 1 - 2^{-2\,C}$ represents a precise measure of the random fluctuation of a channel with capacity C, denoted as channel dispersion [2].

In a security context, we assume the use of a wiretap code containing $2^{n\mathcal{R}_{\mathrm{B}}}$ codewords, where k_{B} is the number of bits transmitted by Alice in each frame [35], while $\mathcal{R}_{\mathrm{B}} = \frac{k_{\mathrm{B}}}{n}$ is the Alice-Bob channel rate. Then, a number of codewords per bin equal to $2^{n\mathcal{R}_{\mathrm{E}}}$ is defined, where $\mathcal{R}_{\mathrm{E}}$ is the colluding eavesdroppers' equivocation rate. Therefore, the rate of secure communication is $\mathcal{R}_{\mathrm{S}} = \mathcal{R}_{\mathrm{B}} - \mathcal{R}_{\mathrm{E}}$. Let us remark that defining $\mathcal{R}_{\mathrm{E}} = \frac{k_{\mathrm{E}}}{n}$ yields $k_{\mathrm{S}} = k_{\mathrm{B}} - k_{\mathrm{E}}$, which represents the total of information bits that are securely transmitted in each frame [20].

Then, if instantaneous CSI of both links is available, $\mathcal{R}_{\mathrm{B}}$ and $\mathcal{R}_{\mathrm{E}}$ can be adapted according to the instantaneous channel capacities, so that the wiretap code can yield perfect secrecy. However, considering that no instantaneous CSI of Eve is available at Alice, perfect secrecy is not guaranteed and a probability metric must be employed in order to measure the probability that the instantaneous eavesdropper channel capacity exceeds the rate $\mathcal{R}_{\mathrm{E}}$ [35]. Here, we also consider that the instantaneous CSI with respect to Bob is also not available at Alice, then a fixed total number of $2^{n\mathcal{R}_{\mathrm{B}}}$ codewords and a fixed number of codewords per bin equal to $2^{n\mathcal{R}_{\mathrm{E}}}$ must be chosen, so that a reliability outage event may also occur if $\mathcal{R}_{\mathrm{B}}$ exceeds the legitimate channel capacity [36].

Then, from (5) we can write the packet error probability, considering a quasi-static fading channel, as

$$\epsilon_j \approx \mathbb{E}\left[Q\left(\frac{C_j - \tilde{\mathcal{R}}_j}{\sqrt{V_j/n}}\right)\right] = \int_0^{\infty} Q\left(\frac{C_j - \tilde{\mathcal{R}}_j}{\sqrt{V_j/n}}\right) f_{\gamma}(\gamma_j)\, \mathrm{d}\gamma_j, \tag{6}$$

where $\tilde{\mathcal{R}}_j$ is a rate estimate, $j \in \{\mathrm{B}, \mathrm{E}\}$, while ϵ_{B} and ϵ_{E} represent, respectively, the packet error probability at Bob and the information leakage probability at Eve. Let us remark that this expression is approximate, whose tightness with simulation results will be shown in Section V.

In order to obtain a closed-form equation to (6), we resort to the linearization of the Q-function as in [37], so that

$$Q\left(p\left(\mu\, z\right)\right) \approx \Omega\left(\mu\, z\right) = \begin{cases} 1, & \mu\, z \leq \zeta^2 \\ \frac{1}{2} - \frac{\beta}{\sqrt{2\,\pi}}\left(\mu z - \theta\right), & \zeta^2 < \mu\, z < \varrho^2 \\ 0, & \mu\, z \geq \varrho^2 \end{cases} \tag{7}$$

where $p\left(\mu\, z\right) = \frac{C(\mu\, z) - \tilde{\mathcal{R}}_j}{\sqrt{V(\mu\, z)/n}}$, $\zeta^2 = \theta - \frac{1}{\beta}\sqrt{\frac{\pi}{2}}$, $\varrho^2 = \theta + \frac{1}{\beta}\sqrt{\frac{\pi}{2}}$, $\theta = 2^{\frac{k_j}{n}} - 1$ and $\beta = \sqrt{\frac{n}{2\pi}}\left(2^{\frac{k_j}{n}} - 1\right)^{-\frac{1}{2}}$.

III. URLLC STRATEGIES

In this section we derive the secure spectral efficiency metric for PR and ID schemes. Following [20], we write the total

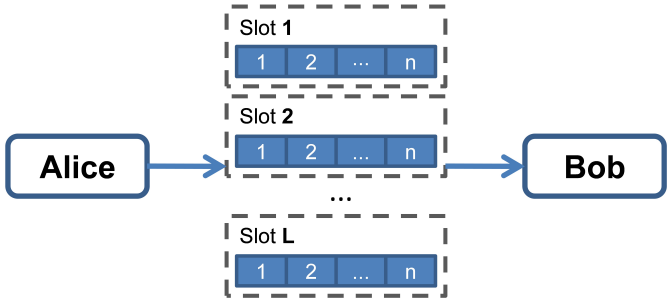

Fig. 2. PR with Alice transmitting L replicas of a length n codeword.

number of successfully transmitted secure information bits at each codeword as

$$\rho^{(\mathrm{sch})} = k_{\mathrm{S}} \left(1 - \epsilon_{\mathrm{B}}^{(\mathrm{sch})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{sch})}, \tag{8}$$

where $\mathrm{sch} \in \{\mathrm{PR}, \mathrm{ID}\}$ represents the employed strategy, $\left(1 - \epsilon_{\mathrm{B}}^{(\mathrm{sch})}\right)$ is the probability that Bob correctly decodes the message transmitted by Alice, while $\epsilon_{\mathrm{E}}^{(\mathrm{sch})}$ is the information leakage probability considering colluding eavesdroppers.

Then, we define the secure spectral efficiency as

$$\tau_{\mathrm{S}}^{(\mathrm{sch})} = \frac{\rho^{(\mathrm{sch})}}{\omega^{(\mathrm{sch})}}, \tag{9}$$

where $\omega^{(\mathrm{sch})}$ is the total number of channel uses to transmit a message from Alice to Bob. Furthermore, we consider a maximum delay constraint δ.

In the sequel we derive the packet error probability and information leakage probability for the PR and ID schemes.

A. Packet Replication (PR)

With PR, Alice transmits L replicas of the original message to Bob in different time slots, as illustrated by Fig. 2. Let us remark that different from HARQ approaches, we consider that Bob can not employ the downlink channel to transmit ACK/NACK packets due to the strictly latency requirements[1].

Bob combines the L replicas using maximal ratio combining (MRC). Thus, the channel capacity is

$$C_{\mathrm{B}}^{(\mathrm{PR})} = \log_2\left(1 + \sum_{w=1}^{L} \gamma_{\mathrm{B},w}\right), \tag{10}$$

where $\gamma_{\mathrm{B},w}$ is the instantaneous SNR at Bob for the w-th replica.

Moreover, since h is a random variable that follows a Nakagami-m distribution, the probability density function (PDF) and cumulative distribution function (CDF) of the MRC given w replications are respectively given by [39]

$$f_{\mathrm{MRC}}(\gamma_j, w) = \left(\frac{m}{\bar{\gamma}_j}\right)^{m\,w} \frac{\gamma_j^{m\,w-1}}{\Gamma\left(m\,w\right)} \exp\left(-m\frac{\gamma_j}{\bar{\gamma}_j}\right) \tag{11}$$

[1]Additionally, although the low latency characteristic of the proposed scenario, the statistical independence between the L replications can be ensured by the use of a time slotted channel hopping (TSCH) protocol, which uses channel hopping for frequency diversity gains [38].

and

$$F_{\mathrm{MRC}}(\gamma_j, w) = \frac{\Gamma\left(m\,w, m\,\frac{\gamma_j}{\bar{\gamma}_j}\right)}{\Gamma\left(m\,w\right)}, \tag{12}$$

where $\Gamma(\cdot)$ is the complete gamma function [40, §6.1.1] and $\Gamma(\cdot,\cdot)$ is the incomplete gamma function [40, §6.5.3].

Then, since $\sum_{w=1}^{L} \gamma_{\mathrm{B},w}$ follows the PDF in (11), the packet error probability for Bob after L replications is

$$\begin{aligned}
\epsilon_{\mathrm{B}}^{(\mathrm{PR})} \approx & \int_0^{\infty} Q\left(\frac{C_{\mathrm{B}}^{(\mathrm{PR})} - \tilde{\mathcal{R}}_{\mathrm{B}}}{\sqrt{V_{\mathrm{B}}^{(\mathrm{PR})}/n}}\right) f_{\mathrm{MRC}}(\gamma_{\mathrm{B}}, L)\,\mathrm{d}\gamma_{\mathrm{B}} \\
= & \int_0^{\zeta^2} f_{\mathrm{MRC}}(\gamma_{\mathrm{B}}, L)\,\mathrm{d}\gamma_{\mathrm{B}} + \int_{\zeta^2}^{\varrho^2} \frac{1}{2} f_{\mathrm{MRC}}(\gamma_{\mathrm{B}}, L)\,\mathrm{d}\gamma_{\mathrm{B}} \\
& - \int_{\zeta^2}^{\varrho^2} \frac{\beta}{\sqrt{2\,\pi}} \left(\gamma_{\mathrm{B}} - \theta\right) f_{\mathrm{MRC}}(\gamma_{\mathrm{B}}, L)\,\mathrm{d}\gamma_{\mathrm{B}} \\
= & \mathcal{F}(\zeta^2, L) + \left[\frac{1}{2} + \frac{\beta\,\theta}{\sqrt{2\pi}}\right]\left[\mathcal{F}(\varrho^2, L) - \mathcal{F}(\zeta^2, L)\right] \\
& - \frac{\beta}{\sqrt{2\pi}}\left[\mathcal{L}(\varrho^2, L) - \mathcal{L}(\zeta^2, L)\right],
\end{aligned} \tag{13}$$

where

$$\mathcal{F}(x, w) = 1 - \frac{\Gamma\left(mw, \frac{xw}{\bar{\gamma}_{\mathrm{B}}}\right)}{\Gamma(mw)}, \tag{14}$$

$$\mathcal{L}(x, w) = \bar{\gamma}_{\mathrm{B}} w - \frac{m^{mw} x^{1+mw} E_{-mw}\left(\frac{mx}{\bar{\gamma}_{\mathrm{B}}}\right)}{\bar{\gamma}_{\mathrm{B}}^{mw}\,\Gamma\left[mw\right]}, \tag{15}$$

with $E_n\left(x\right) = \int_1^{\infty} e^{-x\,t}\,t^{-n}\,\mathrm{d}t$ being the generalized exponential integral [40, §5.1.4].

At Eve, we consider a pessimistic approach, in the security point of view of the legitimate users, in which all eavesdroppers collude, exchanging information by means of a central processing unit, so that the capacity of Eve can be written as

$$C_{\mathrm{E}}^{(\mathrm{PR})} = \log_2\left(1 + \sum_{w=1}^{L} \sum_{e \in \Phi_{\mathrm{E}}} \gamma_{\mathrm{E},e,w}\right), \tag{16}$$

where $\gamma_{\mathrm{E},e,w}$ represents the instantaneous SNR of all Eves $e \in \Phi_{\mathrm{E}}$ colluded, after the w-th replication sent by Alice.

Then, we first define the CDF of MRC after colluding. Considering a PPP with intensity λ_{E}, we can follow the lemma in [41] to write

$$\begin{aligned}
& F_{\mathrm{MRC,col}}(y, w) = \\
& \exp\left[-\lambda_{\mathrm{E}} \int_0^{2\pi} \int_0^{\infty} r_{\mathrm{AE}}\Big(1 - F_{\mathrm{MRC}}(y, w)\Big)\mathrm{d}\,r_{\mathrm{AE}}\,\mathrm{d}\theta\right] \\
& = \exp\left[-\frac{\lambda_{\mathrm{E}}\,\pi\,\Gamma\left[\frac{1}{2} + mw\right]}{\sqrt{\frac{my}{\mathcal{G}}}\,\Gamma\left[mw\right]}\right],
\end{aligned} \tag{17}$$

where $\mathcal{G} = \frac{GP(4\pi f_{\mathrm{c}}/c)^{-2}}{N_0 B M_1 N_{\mathrm{f}}}$, and which holds for $\upsilon = 4$.

From (17), we define the PDF of MRC supposing multiple colluding Eves as

$$f_{\mathrm{MRC,col}}(y,w) = \frac{\lambda_{\mathrm{E}} m\pi\Gamma\left[\frac{1}{2}+mw\right]}{2\mathcal{G}\left(\frac{my}{\mathcal{G}}\right)^{\frac{3}{2}}\Gamma\left[mw\right]} \times \exp\left[-\frac{\lambda_{\mathrm{E}}\pi\Gamma\left[\frac{1}{2}+mw\right]}{\sqrt{\frac{my}{\mathcal{G}}}\Gamma\left[mw\right]}\right]. \tag{18}$$

Then, the information leakage probability at Eve, following a similar procedure as in (13), is

$$\begin{aligned}\epsilon_{\mathrm{E}}^{(\mathrm{PR})} \approx& \int_0^\infty Q\left(\frac{C_{\mathrm{E}}^{(\mathrm{PR})}-\tilde{\mathcal{R}}_{\mathrm{E}}}{\sqrt{V_{\mathrm{E}}^{(\mathrm{PR})}/n}}\right) f_{\mathrm{MRC,col}}(\gamma_{\mathrm{E}},L)\,\mathrm{d}\gamma_{\mathrm{E}}\\ =&F_{\mathrm{MRC,col}}(\zeta^2,L) - \frac{\beta}{\sqrt{2\pi}}\left[\mathcal{K}(\varrho^2,L)-\mathcal{K}(\zeta^2,L)\right]\\ &+\left[\frac{1}{2}+\frac{\beta\,\theta}{\sqrt{2\pi}}\right]\left[F_{\mathrm{MRC,col}}(\varrho^2,L)-F_{\mathrm{MRC,col}}(\zeta^2,L)\right],\end{aligned} \tag{19}$$

where

$$\begin{aligned}\mathcal{K}(y,w) =& \frac{\lambda_{\mathrm{E}} w\pi\mathcal{G}\Gamma\left[\frac{1}{2}+mw\right]}{\Gamma\left[1+mw\right]}\left[\sqrt{\frac{my}{\mathcal{G}}}\,e^{-\frac{\lambda_{\mathrm{E}}\pi\Gamma\left[\frac{1}{2}+mw\right]}{\sqrt{\frac{my}{\mathcal{G}}}\Gamma[mw]}}\right.\\ &\left.+\frac{\lambda_{\mathrm{E}}\pi\Gamma\left[\frac{1}{2}+mw\right]}{\Gamma\left[mw\right]}\mathrm{Ei}\left(-\frac{\lambda_{\mathrm{E}}\pi\Gamma\left[\frac{1}{2}+mw\right]}{\sqrt{\frac{my}{\mathcal{G}}}\Gamma\left[mw\right]}\right)\right],\end{aligned} \tag{20}$$

and $\mathrm{Ei}(x) = \int_{-x}^{\infty} e^{-t}\,t^{-1}\,\mathrm{d}t$ is the exponential integral function [40, §5.1.2].

Finally, the total number of channel uses with PR is

$$\omega^{(\mathrm{PR})} = \sum_{m=1}^{L} n. \tag{21}$$

Following [42], there is a minimum rate $\mathcal{R}'_{\mathrm{B}}$ that allows L replications in $B\delta$ channels uses, *i.e.*,

$$B\delta = L\,n = L\,\frac{k_{\mathrm{B}}}{\mathcal{R}'_{\mathrm{B}}}, \tag{22}$$

yielding

$$\mathcal{R}'_{\mathrm{B}} = L\,\frac{k_{\mathrm{B}}}{B\delta}. \tag{23}$$

Then, the secure spectral efficiency in (9) can be obtained with the aid of (13), (19) and (21).

B. Interface Diversity (ID)

With ID, the idea is to split Alice's message into different transmit interfaces [29], while each interface may use a different communication technology. Here we consider L independent interfaces transmitting a fraction $I = n/L$ of the original message, as illustrated in Fig. 3.

Similarly as in [29], we consider the use of rateless codes or Reed Solomon codes to generate the coded fragments to be sent through the different interfaces. Then, a k-out-of-L splitting strategy is considered, which implies that Bob successfully receives a message transmitted by Alice if at least k of L fragments of the original message are correctly decoded [29]. Furthermore, to perform a fair comparison with PR, we consider $B^{(\mathrm{ID})} = B \cdot L$.

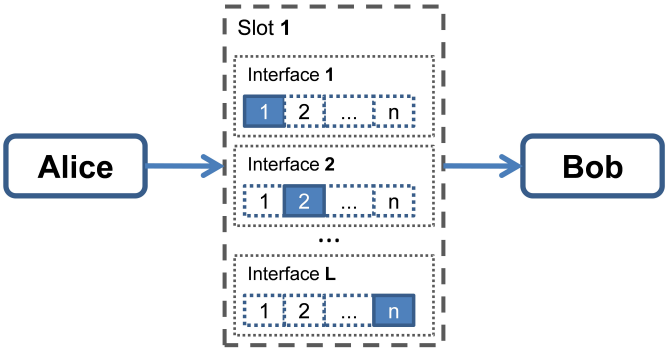

Fig. 3. ID with L interfaces, each transmitting a fraction $I = n/L = 1$ of Alice's message.

Then, the legitimate channel capacity at each interface is

$$C_{\mathrm{B}}^{(\mathrm{ID})} = \log_2(1+\gamma_{\mathrm{B}}), \tag{24}$$

while with respect to the colluding eavesdroppers

$$C_{\mathrm{E}}^{(\mathrm{ID})} = \log_2(1+\sum_{e\in\Phi}\gamma_{\mathrm{E},e}). \tag{25}$$

Thus, still considering each individual interface we have

$$\begin{aligned}\epsilon_{\mathrm{B}}^{(\mathrm{ID})} \approx& \int_0^\infty Q\left(\frac{C_{\mathrm{B}}^{(\mathrm{ID})}-\tilde{\mathcal{R}}_{\mathrm{B}}}{\sqrt{V_{\mathrm{B}}^{(\mathrm{ID})}/n}}\right) f_{\mathrm{MRC}}(\gamma_{\mathrm{B}},1)\,\mathrm{d}\gamma_{\mathrm{B}}\\ =&\mathcal{F}(\zeta^2,1)+\left[\frac{1}{2}+\frac{\beta\,\theta}{\sqrt{2\pi}}\right]\left[\mathcal{F}(\varrho^2,1)-\mathcal{F}(\zeta^2,1)\right]\\ &-\left[\frac{\beta}{\sqrt{2\pi}}\right]\left[\mathcal{L}(\varrho^2,1)-\mathcal{L}(\zeta^2,1)\right],\end{aligned} \tag{26}$$

recalling that $\mathcal{F}(x,w)$ and $\mathcal{L}(x,w)$ are respectively defined in (14) and (15).

Similarly, the leakage error probability at Eve for each interface is

$$\begin{aligned}\epsilon_{\mathrm{E}}^{(\mathrm{ID})} \approx& \int_0^\infty Q\left(\frac{C_{\mathrm{E}}^{(\mathrm{ID})}-\tilde{\mathcal{R}}_{\mathrm{E}}}{\sqrt{V_{\mathrm{E}}^{(\mathrm{ID})}/n}}\right) f_{\mathrm{MRC,col}}(\gamma_{\mathrm{E}},1)\,\mathrm{d}\gamma_{\mathrm{E}}\\ =&F_{\mathrm{MRC,col}}(\zeta^2,1) - \frac{\beta}{\sqrt{2\pi}}\left[\mathcal{K}(\varrho^2,1)-\mathcal{K}(\zeta^2,1)\right]\\ &+\left[\frac{1}{2}+\frac{\beta\,\theta}{\sqrt{2\pi}}\right]\left[F_{\mathrm{MRC,col}}(\varrho^2,1)-F_{\mathrm{MRC,col}}(\zeta^2,1)\right],\end{aligned} \tag{27}$$

with $\mathcal{K}(y,w)$ given by (20).

Then, since k-out-of-L fragments of the original message must be correctly decoded [29], the error probability at Bob and the leakage error probability at Eve are

$$\epsilon_j^{(\mathrm{ID})} = 1-\left[\sum_{r=k}^{L}\binom{L}{k}\left(1-\epsilon_j^{(\mathrm{interface})}\right)^r\left(\epsilon_j^{(\mathrm{interface})}\right)^{L-r}\right], \tag{28}$$

which represents the probability of node $j \in \{\mathrm{B},\mathrm{E}\}$ correctly decoding less than k fragments, and where $\epsilon_j^{(\mathrm{interface})}$ is the error probability at each interface

In addition, the total number of channel uses with ID is

$$\omega^{(\mathrm{ID})} = n, \tag{29}$$

so that the secure spectral efficiency can be obtained with the aid of (26), (27) and (28). Finally, the minimum rate $\mathcal{R}'_{\mathrm{B}}$ for the ID scheme can be obtained from (23) with $L = 1$.

IV. Optimization of the Secure Spectral Efficiency

In this section we aim at maximizing the secure spectral efficiency by finding the optimal values for n, P and the $(k_{\mathrm{B}}, k_{\mathrm{E}})$ pair, given a fixed k_{S}. We address each respective optimization individually in the following sections, while an overall optimization algorithm is provided in Section IV-D.

A. Optimization of the blocklength

The first optimization is performed with respect to the blocklength n, as follows

$$\max_{n} \quad \tau_{\mathrm{S}}^{(\mathrm{sch})} = \frac{k_{\mathrm{S}} \left(1-\epsilon_{\mathrm{B}}^{(\mathrm{sch})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{sch})}}{\omega^{(\mathrm{sch})}} \tag{30a}$$

$$\text{s.t.} \quad \mathcal{R}_{\mathrm{B}} = \frac{k_{\mathrm{B}}}{n} \geq \mathcal{R}'_{\mathrm{B}}. \tag{30b}$$

Then, the condition in (30b) can be transformed into a maximal blocklength $n_{\max}$ equal to the maximum number of information bits $k_{\mathrm{B,max}}$, which according to (23) yields

$$n_{\max} = \frac{k_{\mathrm{B,max}}}{\mathcal{R}_{\mathrm{B}}} = \frac{\mathcal{R}'_{\mathrm{B}} B \delta}{\mathcal{R}_{\mathrm{B}} L}. \tag{31}$$

Therefore, we can rewrite the optimization problem as

$$\max_{n} \quad \tau_{\mathrm{S}}^{(\mathrm{sch})} = \frac{k_{\mathrm{S}} \left(1-\epsilon_{\mathrm{B}}^{(\mathrm{sch})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{sch})}}{\omega^{(\mathrm{sch})}} \tag{32a}$$

$$\text{s.t.} \quad n \leq n_{\max}, \tag{32b}$$

so that the optimal blocklength, n', can be obtained by equating to zero the first derivative of $\tau_{\mathrm{S}}^{(\mathrm{sch})}$ with respect to n, *i.e.*,

$$\frac{\partial\, \tau_{\mathrm{S}}^{(\mathrm{sch})}}{\partial\, n} = \frac{\partial \left\{ \frac{k_{\mathrm{S}} \left(1-\epsilon_{\mathrm{B}}^{(\mathrm{sch})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{sch})}}{\omega^{(\mathrm{sch})}} \right\}}{\partial\, n} = 0 \tag{33}$$

where $\epsilon_{\mathrm{B}}^{(\mathrm{sch})}$, $\epsilon_{\mathrm{E}}^{(\mathrm{sch})}$ and $\omega^{(\mathrm{sch})}$ depend on the employed transmit strategy, as well as on the number of replications/interfaces[2]. Then, with the aid of the Leibniz's rule [40, §3.3.8], we can write

$$\begin{aligned} \frac{\partial\, \tau_{\mathrm{S}}^{(\mathrm{sch})}}{\partial\, n} = {} & \frac{\partial\, \frac{k_{\mathrm{S}}}{\omega^{(\mathrm{sch})}}}{\partial\, n} \epsilon_{\mathrm{B}}^{(\mathrm{sch})} \epsilon_{\mathrm{E}}^{(\mathrm{sch})} - \frac{k_{\mathrm{S}}}{\omega^{(\mathrm{sch})}} \frac{\partial\, \epsilon_{\mathrm{B}}^{(\mathrm{sch})}}{\partial\, n} \epsilon_{\mathrm{E}}^{(\mathrm{sch})} \\ & + \frac{k_{\mathrm{S}}}{\omega^{(\mathrm{sch})}} \frac{\partial\, \epsilon_{\mathrm{E}}^{(\mathrm{sch})}}{\partial\, n} + \frac{\partial\, \frac{k_{\mathrm{S}}}{\omega^{(\mathrm{sch})}}}{\partial\, n} \epsilon_{\mathrm{E}}^{(\mathrm{sch})} \\ & - \frac{k_{\mathrm{S}}}{\omega^{(\mathrm{sch})}} \epsilon_{\mathrm{B}}^{(\mathrm{sch})} \frac{\partial\, \epsilon_{\mathrm{E}}^{(\mathrm{sch})}}{\partial\, n}, \end{aligned} \tag{34}$$

which expresses the necessary derivatives in order to maximize the secure spectral efficiency.

However, due to the complexity of the involved problem, it is not possible to isolate n in order to obtain a closed-form solution to n'. As an alternative, a golden section algorithm with parabolic interpolation can be employed, which finds the maximum of an unimodal function by narrowing the range of values inside an interval [43]. The advantage of the golden section search technique to our setting is that it always converges to the true optimum when the objective function is unimodal [44], as it is our case. In addition, the parabolic interpolation feature helps in a faster convergence [45], with the advantage over Newton's method that no derivations are needed. Such algorithm is not the unique that can be employed to optimize the secure spectral efficiency in our scenario. Since the optimization is performed using the average CSI only, and not the instantaneous CSI, the optimization can be computed offline, *i.e.*, predefined in an design step of the network. As a consequence, there is no impact in terms of additional latency or complexity, once the algorithm does not need to be run prior to each data transmission. Then, in order to employ it, we demonstrate in Lemma 1 the concavity and unimodal characteristics of the secure spectral efficiency with respect to n, while the algorithm is detailed in Section IV-D.

Lemma 1: The secure spectral efficiency, $\tau_{\mathrm{S}}^{(\mathrm{sch})}$, tends to zero when $n \to 0$ and when $n \to \infty$. Additionally, $\tau_{\mathrm{S}}^{(\mathrm{sch})}$ is monotonically increasing when $x \leq n'$, and monotonically decreasing when $x \geq n'$.

Proof: Given an interval $x \in [0, \infty)$, the maximum value of the Q-function is obtained with $x = 0$, while $Q(x) \to 0$ when $x \to \infty$. Therefore, when $n \to 0$ in (6), the argument of the Q-function tends to zero, which implies in the function maximum, so that both $\epsilon_{\mathrm{B}}^{(\mathrm{sch})}$ and $\epsilon_{\mathrm{E}}^{(\mathrm{sch})}$ tend to one. Consequently, the total number of information bits $\rho^{(\mathrm{sch})} \to 0$ in (8). On the other hand, when $n \to \infty$ the number of channel uses $\omega \to \infty$, which implies in $\tau_{\mathrm{S}}^{(\mathrm{sch})} \to 0$. Additionally, with respect to the intermediate values in the interval $n \in (0, \infty)$, we numerically evaluate $\tau_{\mathrm{S}}^{(\mathrm{sch})}$ in order to show that it is unimodal with respect to n. The numerical results will that a unique maximum value exists with respect to the blocklength. ■

Finally, since $\tau_{\mathrm{S}}^{(\mathrm{sch})}$ is concave with respect to n, we reintroduce the constraint (32b) by defining the optimal blocklength as $n^\star = \min\{n', n_{\max}\}$.

B. Optimization of the $(k_{\mathrm{B}},k_{\mathrm{E}})$ pair

In order to find the optimal $(k_{\mathrm{B}},k_{\mathrm{E}})$ pair, we define the following optimization

$$\max_{k_{\mathrm{B}},k_{\mathrm{E}}} \quad \tau_{\mathrm{S}}^{(\mathrm{sch})} = \frac{k_{\mathrm{S}} \left(1-\epsilon_{\mathrm{B}}^{(\mathrm{sch})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{sch})}}{\omega^{(\mathrm{sch})}} \tag{35a}$$

$$\text{s.t.} \quad k_{\mathrm{B}} \leq k_{\mathrm{B,max}}, \tag{35b}$$

$$k_{\mathrm{E}} = k_{\mathrm{B}} - k_{\mathrm{S}} \text{ with fixed } k_{\mathrm{S}} \leq k_{\mathrm{B}}. \tag{35c}$$

Then, we first relax conditions (35b) and (35c), so that the optimal $(k'_{\mathrm{B}},k'_{\mathrm{E}})$ pair is obtained by replacing $k_{\mathrm{E}} = k_{\mathrm{B}} - k_{\mathrm{S}}$

[2]Notice that the $n_{\max}$ constraint has been removed here. Nevertheless, as we will show in the following, since (32a) is concave, it can be easily reintroduced at the end of the solution.

and by doing

$$\frac{\partial\,\tau_{\rm S}}{\partial\,k_{\rm B}} = \frac{\partial\left\{\frac{k_{\rm S}\left(1-\epsilon_{\rm B}^{(\rm sch)}\right)\epsilon_{\rm E}^{(\rm sch)}}{\omega^{(\rm sch)}}\right\}}{\partial\,k_{\rm B}} = 0. \tag{36}$$

However, due to the difficulty to find the optimal $(k_{\rm B},k_{\rm E})$ pair, we prove the concavity and unimodality of $\tau_{\rm S}$, with respect to $k_{\rm B}$ in Lemma 2, and employ a golden section search with parabolic interpolation to find the optimal pair, as further described in Section IV-D.

Lemma 2: The secure spectral efficiency, $\tau_{\rm S}$, tends to zero when either $k_{\rm B}\to 0$ or $k_{\rm B}\to\infty$. Moreover, $\tau_{\rm S}(x)$ always increases when $x\leq k'_{\rm B}$ and always decreases when $x\geq k'_{\rm B}$, so that $k'_{\rm B}$ represents the global optimal value for $k_{\rm B}$.

Proof: When $k_{\rm B}\to 0$, $k_{\rm S}$ also tends to zero, which implies in $\tau_{\rm S}^{(\rm sch)}\to 0$. On the contrary, when $k_{\rm B}\to\infty$ the minimum rate $\mathcal{R}'_{\rm B}$ also tends to ∞ according to (23). Therefore, the maximum delay constraint cannot be accomplished and $\tau_{\rm S}^{(\rm sch)}=0$. In addition, we numerically show that there is a unique maximum of $\tau_{\rm S}^{(\rm sch)}$ with respect to $k_{\rm B}$. ■

Finally, reintroducing the constraint in (35b), the optimal $k_{\rm B}$ is given by $k^\star_{\rm B}=\min\{k'_{\rm B},k_{\rm B\,max}\}$, while $k^\star_{\rm E}$ is obtained from $k^\star_{\rm B}$ with a fixed $k_{\rm S}$.

C. Power Optimization

With respect to the optimal power allocation, we define

$$\max_{P} \quad \tau_{\rm S} = \frac{k_{\rm S}\left(1-\epsilon_{\rm B}^{(\rm sch)}\right)\epsilon_{\rm E}^{(\rm sch)}}{\omega^{(\rm sch)}} \tag{37a}$$

$$\text{s.t.} \quad 0\leq P\leq P_{\max}. \tag{37b}$$

Relaxing (37b) the optimal $P'_{\rm A}$ is obtained by doing

$$\frac{\partial\,\tau_{\rm S}^{(\rm sch)}}{\partial\,P} = \frac{\partial\left\{\frac{k_{\rm S}\left(1-\epsilon_{\rm B}^{(\rm sch)}\right)\epsilon_{\rm E}^{(\rm sch)}}{\omega^{(\rm sch)}}\right\}}{\partial\,P} = 0, \tag{38}$$

for which the concavity and unimodality of $\tau_{\rm S}$ with respect to P, required by the golden section algorithm with parabolic interpolation, is demonstrated in Lemma 3.

Lemma 3: The secure spectral efficiency tends to zero when either $P\to 0$ or $P\to\infty$, while the function has a unimodal characteristic with respect to the power allocated at Alice, with the maximum at $P'_{\rm A}$.

Proof: When $P\to 0$, $\epsilon_{\rm B}\to 1$ since Bob is not able to correctly decode the transmissions from Alice. Therefore, the term $\rho^{(\rm sch)}\to 0$ in (8), which implies in $\tau_{\rm S}^{(\rm sch)}\to 0$. On the other hand, when $P\to\infty$, $\epsilon_{\rm E}\to 0$, which also implies in $\tau_{\rm S}^{(\rm sch)}\to 0$. In addition, with P within $(0,\infty)$, we show numerically that $\tau_{\rm S}^{(\rm sch)}$ is unimodal with respect to P. ■

Finally, reintroducing (37b), the power allocation is given by $P^\star=\min\{\max\{0,P'_{\rm A}\},P_{\max}\}$.

D. Optimization Algorithm

In order to obtain the optimal values $n^\star$, the pair $(k^\star_{\rm B},k^\star_{\rm E})$ and $P^\star$, we develop an algorithm to maximize $\tau_{\rm S}^{(\rm sch)}$ iteratively. The proposed algorithm is presented in Algorithm 1, which optimizes each parameter using three inner-loops, respectively for $n^\star$, $(k^\star_{\rm B},k^\star_{\rm E})$ and $P^\star$, and one outer-loop. The outer-loop defines the stop criterion of the algorithm and is iterated until the increase in terms of secure spectral efficiency is smaller than a predefined threshold ϵ. The inner-loops are associated with the golden section search algorithm with parabolic interpolation [43] for each optimized variable, whose stop criteria are respectively given by ϵ_n, ϵ_k and ϵ_P. The golden section search algorithm converges to the optimal point, given a set of tolerances, when the function to be optimized is unimodal, while the convergence is faster when the parabolic interpolation is employed [45]. Let us remark that other optimization strategies can be employed in order to obtain $n^\star$, $(k^\star_{\rm B},k^\star_{\rm E})$ and $P^\star$, such as, *e.g.*, reinforcement learning [46]. However, since the mathematical model of the optimization problem is clearly defined, we resort to the golden section search with parabolic interpolation to optimize each variable, which yields superlinear and guaranteed convergence.

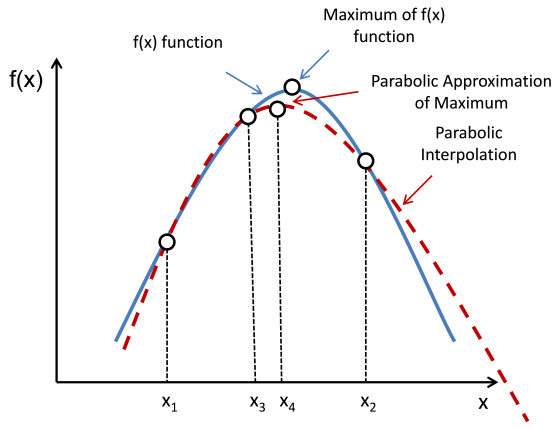

Fig. 4. Allocation of the optimal value of x in order to maximize a function $f(x)$ using the golden section search algorithm with parabolic interpolation.

Then, in order to solve (34), (36) and (38), Fig. 4 illustrates the iterative process, where we start choosing an initial triplet $\vartheta_0=(x_1,x_3,x_2)$, with $x_1<x_3<x_2$. Then, with ϑ_0, we interpolate a parabola, depicted by the dashed red line in Fig. 4, whose maximum is given by x_4. After that, $\tau_{\rm S}^{(\rm sch)}$, represented by the solid blue line in Fig. 4, is computed using the maximum value of the parabola, x_4. If $\tau_{\rm S}^{(\rm sch)}(x_4)>\tau_{\rm S}^{(\rm sch)}(x_3)$ the new triplet is defined by $\vartheta_1=(x_3,x_4,x_2)$, otherwise, $\vartheta_1=(x_1,x_3,x_4)$. Then, at each iteration the interval of the triplet becomes smaller, until the algorithm stops when a predefined tolerance with respect to such interval is achieved.

V. Numerical Results

In order to provide some numerical examples of the secure spectral efficiency, we assume that the path-loss exponent is $\upsilon=4$, which represents a common value of path loss exponent to model the environment of a building with obstructions (*e.g.*, walls) [47], while Alice and Bob are disposed along a line, with $r_{\rm AB}=100$ m, and the eavesdroppers follow a PPP with intensity $\lambda_{\rm E}=0.1$. Additionally, Nakagami-m with $m=2$ is considered, unless stated otherwise. Furthermore, $B=180$ kHz, $N_0=-174$ dBm/Hz, $M_{\rm l}=20$ dB, $G=5$ dBi,

Algorithm 1: Proposed Allocation Algorithm.

Input: $\tau_{\mathrm{S}}^{(\mathrm{sch})}$ and tolerances ϵ, ϵ_n, ϵ_k, ϵ_P;
Initialize: $i=1$, $\tau_{\mathrm{S},0}^{(\mathrm{sch})}=0$ and $\tau_{\mathrm{S},1}^{(\mathrm{sch})}=\tau_{\mathrm{S}}^{(\mathrm{sch})}$;
while $\tau_{\mathrm{S},i}^{(\mathrm{sch})}-\tau_{\mathrm{S},i-1}^{(\mathrm{sch})}\geq\epsilon$ **do**
    Optimization of the blocklength: solve (34) in order to find $n_i^\star$;
    Optimization of the $(k_{\mathrm{B}},k_{\mathrm{E}})$ pair: solve (36) in order to find $k_{\mathrm{B},i}^\star$ and $k_{\mathrm{E},i}^\star$;
    Power optimization: solve (38) in order to find $P_i^\star$;
end
$i++$;
Compute $\tau_{\mathrm{S},i}^{(\mathrm{sch})}$ using $n_{i-1}^\star$, $k_{\mathrm{B},i-1}^\star$, $k_{\mathrm{E},i-1}^\star$ and $P_{i-1}^\star$;

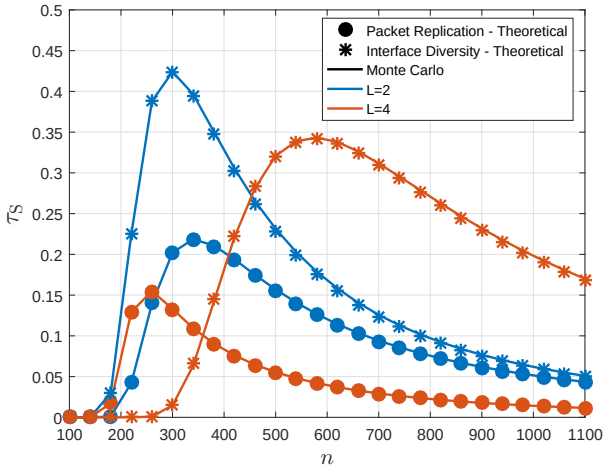

Fig. 5. Secure spectral efficiency as a function of n with $P=5$ dB, $k_{\mathrm{S}}=400$ and $k_{\mathrm{B}}=800$.

$N_{\mathrm{f}}=10$ dB, $f_{\mathrm{c}}=2.5$ GHz and $\delta=6.48$ ms, following the typical link latency defined in [42].

A. Secure Spectral Efficiency

First we investigate the secure spectral efficiency as a function of the blocklength, the $(k_{\mathrm{B}},k_{\mathrm{E}})$ pair and the transmit power at Alice, while no parameter optimization is performed at this point. Such analysis is important to demonstrate the unimodal characteristics of the curves as a function of n, k_{B} and power P, as indicated in Section IV. Moreover, the number of fragments that must be correctly decoded by the ID scheme is considered to be $k=L-1$ in the results below.

Fig. 5 plots τ_{S} as a function of n with $P=5$ dB, $k_{\mathrm{S}}=400$ and $k_{\mathrm{B}}=800$. As we observe, the optimal n for the PR strategy decreases with the increase of L, once a higher number of packet replications implies in more channel uses, which decreases τ_{S}. On the other hand, the optimal n increases with L for the ID scheme, since the spatial diversity gains in this strategy is associated with a higher number of interfaces. Additionally, we compare the expressions with Monte Carlo simulations, in which a good agreement is shown.

Next, Fig. 6 plots τ_{S} while varying k_{B} for fixed $k_{\mathrm{S}}=100$. Then, k_{E} is adapted accordingly in order to maintain $k_{\mathrm{S}}=k_{\mathrm{B}}-k_{\mathrm{E}}$. As we observe, there is an optimal $(k_{\mathrm{B}},k_{\mathrm{E}})$ pair that depends on the transmit scheme and on the number of replications/interfaces. Nevertheless, unlike Fig. 5, the optimal k_{B} for the PR strategy increases with the increase of L, while it decreases with L for the ID scheme. Furthermore, Fig. 7 plots τ_{S} as a function of the transmit power for both schemes, which indicates that each strategy and scenario has optimal values associated with n, k_{B} and P. Therefore, an appropriate choice of such parameters is of paramount importance in order to maximize τ_{S}. Finally, we can also observe that ID always outperforms PR in Figs. 5-7. However, these conclusions change when these parameters are properly optimized, as it is shown in the following.

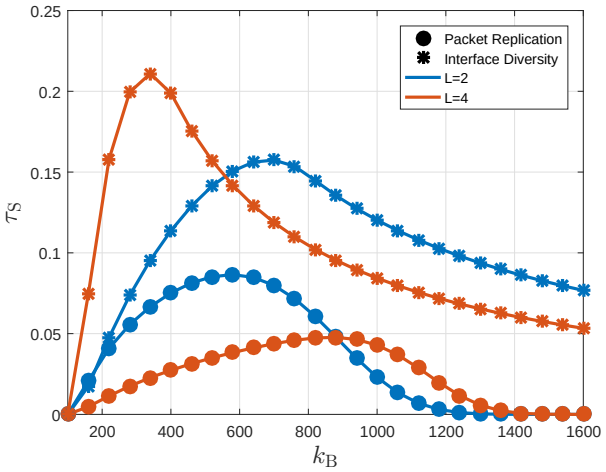

Fig. 6. Secure spectral efficiency as a function of k_{B} with $P=5$ dB, $n=300$ and $k_{\mathrm{S}}=100$.

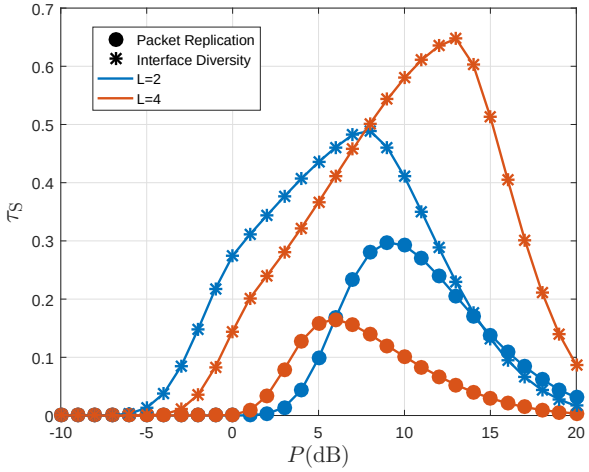

Fig. 7. Secure spectral efficiency as a function of P with $n=300$, $k_{\mathrm{B}}=1000$ and $k_{\mathrm{E}}=400$.

B. Parameter Optimization

Here we consider the joint optimization of n, P and the $(k_{\mathrm{B}},k_{\mathrm{E}})$ pair, for a fixed k_{S}, according to Section IV. Moreover, we do consider that the feedback channel is very slow compared to the forward channel. Then, CSI is not fed back to

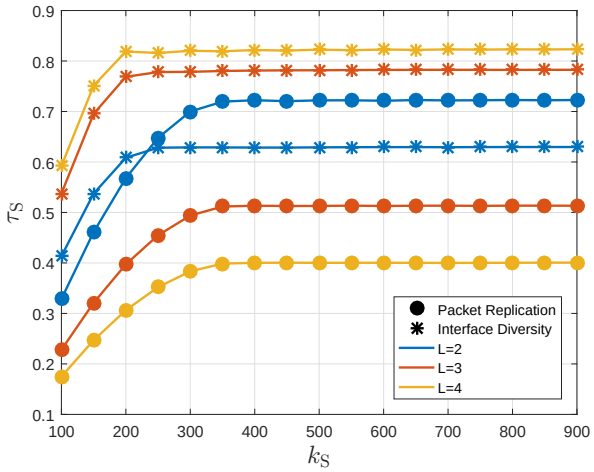

Fig. 8. Secure spectral efficiency as a function of k_S with optimal $n^\star$, $(k_B^\star,k_E^\star)$ and $P^\star$.

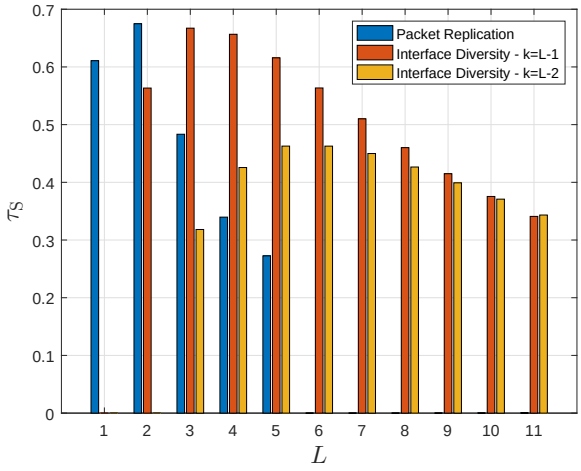

Fig. 9. Secure spectral efficiency as a function of L with optimal $n^\star$, $(k_B^\star,k_E^\star)$ and $P^\star$.

Alice constantly, which implies in an optimization performed in terms of average CSI only. In addition, the optimization considers a minimal blocklength $n_{\min} = 100$, once the approximation in (7) loses precision for $n < 100$ [37]. Furthermore, for a fair comparison between PR and ID schemes, we allow ID to use up to $n_{\max}^{(\mathrm{ID})} = k \cdot n_{\max}$ bits, recalling that k is the number of interfaces with ID, while PR is restricted to $n_{\max}$.

Next, Fig. 8 plots τ_S as a function of k_S. As we can notice, the ID scheme performs better with larger L, outperforming PR when $L \in \{3, 4\}$. This is due to the fact that the total number of channel uses $\omega^{(\mathrm{PR})}$ also increases with L, limiting the performance of the PR scheme, while $\omega^{(ID)}$ is independent of L for the ID scheme. Nevertheless, when $L = 2$ there is a trade-off between PR and ID depending on k_S, with PR performing better when $k_S \geq 250$. In addition, we also observe that the secure throughput of the schemes saturate at $k_S/\omega^{(\mathrm{sch})}$. However, this only occurs when the optimal set of parameters fills the latency requirement given by δ.

Fig. 9 corroborates with such analysis, illustrating τ_S as a function of L for PR and ID with different values for k. As we observe, $L = 2$ maximizes τ_S for PR, while the optimal L for ID depends on k. For instance, ID with $k = L - 1$ is maximized with $L = 3$, while the case with $k = L - 2$ has the optimal value in terms of τ_S with $L = 6$. Additionally, the case when $L = 1$ (no replications or a single interface) is also shown for comparison. Let us highlight that, differently from [29], in scenarios with security concerns the ID scheme achieves increased throughput when more fragments are encoded (higher k). Then, with these increase of k, a higher leakage error probability is obtained at Eve[3].

TABLE II
OPTIMAL VALUES OF POWER, BLOCKLENGTH AND (k_B,k_E) PAIR FOR THE SCENARIO OF FIG. 9

	PR			**ID with $k = L-1$**			**ID with $k = L-2$**		
L	$n^\star$	$k_B^\star$	$P^\star$	$n^\star$	$k_B^\star$	$P^\star$	$n^\star$	$k_B^\star$	$P^\star$
1	270	1000	7	100	1000	0	–	–	–
2	270	1650	12	400	1900	12	–	–	–
3	260	1750	12	500	1850	12	550	2500	12
4	250	1800	12	550	1700	12	600	2200	12
5	250	1900	12	650	1700	12	650	2050	12
6	250	1950	12	700	1650	12	700	1950	12
7	240	1950	12	800	1650	12	800	1950	12
8	240	2000	12	900	1650	12	850	1900	12
9	240	2050	12	1000	1650	12	950	1900	12
10	230	2000	12	1100	1650	12	1050	1900	12

TABLE III
LATENCY CONSTRAINT ASSOCIATED WITH THE MAXIMUM SECURE SPECTRAL EFFICIENCY

URLLC Strategy	**Latency Constraint - δ (ms)**				
-	**L=2**	**L=3**	**L=4**	**L=5**	**L=6**
PR	3.000	4.333	5.555	6.944	8.333
ID with $k = L - 1$	1.111	0.926	0.764	0.722	0.648
ID with $k = L - 2$	–	1.128	0.833	0.722	0.648

To complement the analysis, Table II shows the optimal $n^\star$, $k_B^\star$ and $P^\star$ (in dB) for different L. As we notice, the optimal blocklength decreases for PR, while it increases for ID, which is expected since a higher n consumes more channel uses in PR, decreasing τ_S. Additionally, is interesting to notice that the proposed optimization algorithm maximizes τ_S by balancing each of the system parameters, as we notice by comparing $n^\star$ and $k_B^\star$ for both transmit schemes. For instance, when increasing L we observe that $k_B^\star$ increases for PR while $n^\star$ decreases. On the other hand, an opposite behavior is observed for the ID scheme when increasing L, with $k_B^\star$ decreasing and $n^\star$ increasing.

Finally, Table III indicates the value of the latency constraint, δ, associated with the optimal values obtained for secure spectral efficiency when $k_S = 900$. As we observe, due to the increase of the replications, the PR strategy has

[3]It is worth noting that such general conclusion is also aligned with other works in the literature, as for instance [48], carried out in different contexts and meeting different requirements.

increased latency while L increases. On the other hand, the latency decreases when L increases with the ID scheme since the bandwidth also increases in this case, as in (22).

VI. Conclusions

We investigated the secure spectral efficiency of PR and ID strategies in URLLC. The impact of a finite blocklength is taken into account, as well the effects of channel uses in terms of delay. We assume no knowledge of the instantaneous channel state information available at Alice, neither with respect to Bob nor Eves, while the position of the multiple colluding eavesdroppers are specified according to a PPP over a Nakagami-m fading channel. Our results show that the proper optimization of n, k_{B} and P is crucial to maximize τ_{S}. Additionally, we also show that the increase of the number of replications/interfaces is not always beneficial for the legitimate nodes, since the eavesdroppers may also benefit from this increase. Finally, our results shown that each scheme has better performance depending of the network scenario and system parameters. Nevertheless, ID is the most advantageous scheme in general, increasing the secure spectral efficiency when L increases, while PR performs better when L is small.

References

[1] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka, H. Tullberg, M. A. Uusitalo, B. Timus, and M. Fallgren, "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 26–35, May 2014.

[2] G. Durisi, T. Koch, and P. Popovski, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proc. IEEE*, vol. 104, no. 9, pp. 1711–1726, Sept 2016.

[3] Ericsson, "Ericsson mobility report, November 2015," Tech. Rep., 2015.

[4] ——, "Cellular networks for massive IoT," Tech. Rep., 2016.

[5] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update, 2016-2021 white paper," Tech. Rep., 2017.

[6] O. N. C. Yilmaz, Y. . E. Wang, N. A. Johansson, N. Brahmi, S. A. Ashraf, and J. Sachs, "Analysis of ultra-reliable and low-latency 5G communication for a factory automation use case," in *IEEE International Conference on Communication Workshop (ICCW)*, June 2015, pp. 1190–1195.

[7] H. Tullberg, P. Popovski, Z. Li, M. A. Uusitalo, A. Hoglund, O. Bulakci, M. Fallgren, and J. F. Monserrat, "The METIS 5G system concept: Meeting the 5G requirements," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 132–139, Dec. 2016.

[8] A. Weinand, M. Karrenbauer, J. Lianghai, and H. D. Schotten, "Physical layer authentication for mission critical machine type communication using Gaussian mixture model based clustering," in *IEEE Vehicular Technology Conference*, June 2017, pp. 1–5.

[9] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, Aug 2018.

[10] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, Dec 2017.

[11] W. K. Harrison, D. Sarmento, J. P. Vilela, and M. A. C. Gomes, "Analysis of short blocklength codes for secrecy," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, oct 2018.

[12] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Block-fading channels at finite blocklength," in *IEEE 10th Int. Symp. Wireless Commun. Systems*, Aug 2013, pp. 1–4.

[13] J. Pfister, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Quantifying equivocation for finite blocklength wiretap codes," in *IEEE Int. Conf. on Commun.*, May 2017, pp. 1–6.

[14] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Secure transmission via transmit antenna selection in MIMO wiretap channels," in *IEEE Global Commun. Conf.*, Dec. 2012, pp. 789–794.

[15] C. Sun, C. She, C. Yang, T. Q. S. Quek, Y. Li, and B. Vucetic, "Optimizing resource allocation in the short blocklength regime for ultra-reliable and low-latency communications," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 402–415, Jan 2019.

[16] Y. Long, Y. Gao, and T. Yang, "Research on ultra-reliable and low-latency wireless communications in smart factory with finite blocklength," in *2018 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, Aug 2018, pp. 158–162.

[17] P. Mary, J. M. Gorce, A. Unsal, and H. V. Poor, "Finite blocklength information theory: What is the practical impact on wireless communications?" in *IEEE Globecom Workshops*, Dec 2016, pp. 1–6.

[18] H. V. Poor, M. Goldenbaum, and W. Yang, "Fundamentals for IoT networks: Secure and low-latency communications," in *Int. Conf. on Distributed Computing and Networking*, 2019, pp. 362–364.

[19] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Commun. Magazine*, vol. 54, no. 6, pp. 152–158, June 2016.

[20] J. Farhat, G. Brante, and R. D. Souza, "Secure throughput optimization of selective decode-and-forward with finite blocklength," in *IEEE 87th Vehicular Technology Conference (VTC Spring)*, June 2018, pp. 1–5.

[21] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 6–11, October 2019.

[22] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[23] W. Yang, R. F. Schaefer, and H. V. Poor, "Finite-blocklength bounds for wiretap channels," in *IEEE Int. Symp. Inf. Theory*, July 2016, pp. 3087–3091.

[24] H. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2019.

[25] S. Tomasin, "HARQ with quantized 1-bit CSI feedback for block fading wiretap channels," in *2016 IEEE Globecom Workshops (GC Wkshps)*, Dec 2016, pp. 1–5.

[26] J. Choi, "On channel-aware secure HARQ-IR," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 351–362, Feb 2017.

[27] M. Le Treust, L. Szczecinski, and F. Labeau, "Rate adaptation for secure HARQ protocols," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 2981–2994, Dec 2018.

[28] T. Ssettumba, A. H. A. El-Malek, M. Elsabrouty, and M. Abo-Zahhad, "Physical layer security enhancement for internet of things in the presence of co-channel interference and multiple eavesdroppers," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[29] J. J. Nielsen, R. Liu, and P. Popovski, "Optimized interface diversity for ultra-reliable low latency communication (URLLC)," in *IEEE Global Commun. Conf.*, Dec 2017, pp. 1–6.

[30] P. Popovski, . Stefanović, J. J. Nielsen, E. de Carvalho, M. Angjelichinoski, K. F. Trillingsgaard, and A. Bana, "Wireless access in ultra-reliable low-latency communication (URLLC)," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5783–5801, 2019.

[31] D. S. Michalopoulos, I. Viering, and L. Du, "User-plane multi-connectivity aspects in 5G," in *Int. Conf. Telecommun.*, May 2016, pp. 1–5.

[32] J. J. Nielsen and P. Popovski, "Latency analysis of systems with multiple interfaces for ultra-reliable M2M communication," in *IEEE Int. Workshop on Signal Processing Advances in Wireless Commun.*, July 2016, pp. 1–6.

[33] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 616–627, Sep. 2011.

[34] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

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

[36] G. Brante, H. Alves, R. Souza, and M. Latva-aho, "Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1330–1342, Apr. 2015.

[37] B. Makki, T. Svensson, and M. Zorzi, "Wireless energy and information transmission using feedback: Infinite and finite block-length analysis," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5304–5318, Dec. 2016.

[38] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel, "On optimal scheduling in duty-cycled industrial IoT applications using IEEE802.15.4e TSCH," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3655–3666, Oct 2013.

[39] S. R. Meraji, "Performance analysis of transmit antenna selection in Nakagami-m fading channels," *Wirel. Pers. Commun.*, vol. 43, no. 2, pp. 327–333, Oct. 2007.

[40] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover Publications, Inc., 1974.

[41] G. Chen and J. P. Coon, "Secrecy outage analysis in random wireless networks with antenna selection and user ordering," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 334–337, June 2017.

[42] J. P. B. Nadas, O. Onireti, R. D. Souza, H. Alves, G. Brante, and M. A. Imran, "Performance analysis of hybrid ARQ for ultra-reliable low latency communications," *IEEE Sensors Journal*, vol. 19, no. 9, pp. 3521–3531, May 2019.

[43] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes 3rd Edition: The Art of Scientific Computing*, 3rd ed. New York, NY, USA: Cambridge University Press, 2007.

[44] M. T. Heath and E. M. Munson, *Scientific Computing: An Introductory Survey*, 2nd ed. McGraw-Hill Higher Education, 1996.

[45] T. Renk, D. Iankov, and F. K. Jondral, "Adaptive resource allocation in wireless relay networks," in *IEEE Vehicular Technology Conference*, April 2009, pp. 1–5.

[46] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: A Bradford Book, 2018.

[47] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Prentice-Hall, 2002.

[48] 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, Apr. 2009.