Security Gap of Coded Transmit Antenna Selection Systems with Frame Scrambling

Marco Antônio Chiodi Junior, João Luiz Rebelatto, Richard Demo Souza and Glauber Brante

***Abstract*—In this work, we consider a network composed of two legitimate nodes and one passive eavesdropper, all of them provided with multiple antennas. We also consider the transmit antenna selection (TAS) scheme along with frame scrambling at the transmitter to provide an instantaneous advantage for the legitimate users over the eavesdropper, while both legitimate and malicious receivers operate under maximum ratio combining (MRC). By considering a quasi-static fading scenario, we evaluate (analytically and through numerical results) the physical layer security through the security gap in terms of both outage probability and convolutional coding-based frame error rate (FER), as a function of the number of antennas at each node. Our results show that, either adopting the FER or the outage probability as the performance metric, it is possible to achieve negative security gaps using a feasible number of antennas.**

***Keywords*—physical-layer security, security gap, frame scrambling, TAS/MRC.**

I. Introduction

Information security is a major concern in wireless communications, due to the broadcast nature of the wireless medium which allows eavesdroppers to potentially intercept any transmission. Information theoretic secrecy, introduced by Shannon in 1949 [2], is a promising approach towards increasing communication security complementing classical cryptography techniques. In [3], Wyner elaborated on the work of Shannon by introducing the so-called wiretap channel, which is composed of a pair of legitimate nodes (usually referred to as Alice and Bob) communicating in the presence of a passive eavesdropper (Eve). Recent works have applied concepts of information theoretic secrecy to wireless communications, showing that the randomness inherent to wireless channels can be helpful towards increasing the security of the legitimate channel over the eavesdropper channel [4]–[6].

However, the design of practical wiretap codes with feasible block lengths is usually known just for few scenarios of interest, which do not include the case of quasi-static fading wireless channels [7]. In [8], the authors proposed the use of a more practical metric to evaluate security: the so-called security gap, which represents the difference (gap) of channel quality experienced between Bob and Eve [9]. That is, under this metric security can be measured in terms of the ratio between the signal-to-noise ratios (SNR) required at Bob and Eve to achieve reliable communication for Bob while achieving a sufficient level of physical layer security. Considering a quasi-static fading channel, one must ensure *i) secrecy*, by guaranteeing that the outage probability/frame error rate (FER) experienced at Eve is above a given target value; and *ii) reliability*, by guaranteeing that Bob operates at an outage probability/FER below a required threshold.

In [10], the authors resort to a technique referred to as frame scrambling, which consists of the concatenation and scrambling of several independent frames. The goal of frame scrambling is to spread a single residual bit error from the several scrambled frames to maximize the uncertainty of the decoding process, *i.e.*, the security gap is decreased by boosting the propagation of residual errors. Moreover, multiple-input multiple-output (MIMO) is a feature initially proposed to combat the fading inherent to the wireless channels and consequently to increase its capacity [11], being currently widely adopted. Recent works have also evaluated the potential of MIMO towards increasing the physical-layer security, showing that the use of multiple antennas is an effective way of increasing the secrecy capacity of wireless transmissions [12]–[14].

Some preliminary results on the outage probability-based security gap in a MIMO scenario, where Alice adopts the transmit antenna selection (TAS) scheme [15], [16] while both Bob and Eve operate under the maximum ratio combining (MRC) scheme [15], are presented in [1], [17] showing the benefits of employing TAS along with scrambling towards reducing the security gap. One important feature of TAS is that it requires a minimal amount of feedback (just the index of the best antenna). Moreover, even if Eve is capable of accessing the feedback message, the selected antenna is only optimum to Bob since the channels between Alice and Bob and between Alice and Eve are independent. Another aspect of TAS is that it employs only one radio frequency (RF) chain instead of many parallel RF chains as other MIMO techniques. Such characteristic reduces cost, complexity, consumption and size at the expense of a small loss in performance [16].

In [1], under the same framework as [17], we resort to the inverse gamma function to obtain an exact expression to the outage probability-based security gap, in order to validate the accuracy of the approximation introduced in [17]. Moreover, we also evaluate the performance of the proposed scheme by adopting a more realistic FER-based security gap formulation,

The Associate Editors coordinating the review of this manuscript and approving it for publication were Profs. Cecílio Pimentel and Marcelo da Silva Pinho.

Marco Antônio Chiodi Junior, João Luiz Rebelatto, Richard Demo Souza and Glauber Brante¸ CPGEI, Federal University of Technology - Parana, Av. Sete de Setembro, 3165, Rebouças, Curitiba, PR, 80230-901, Brazil. E-mails: marco@radioenge.com.br, {jlrebelatto, richard, gbrante}@utfpr.edu.br.

This work was partially supported by Fundação Araucária, CAPES and CNPq (Brazil).

A preliminary version of this paper was presented in XXXIII Simpósio Brasileiro de Telecomunicações (SBrT'15), Juiz de Fora, MG, Brazil, September 1-4, 2015 [1].

Digital Object Identifier: 10.14209/jcis.2016.12.

which is calculated supposing the use of convolutional codes. The results in [1] confirm that, either considering outage probability or FER as the reliability metric, it is possible to achieve a security gap lower than 0 dB under feasible scrambling depths and using practical number of antennas, which means that secure communication is feasible even if the channel between Alice and Eve is in better conditions, in average, than the channel between Alice and Bob.

This work aims at presenting an extension of [17] and [1], including further analysis and discussions about both the perfect and more practical scrambling-based scenarios, as well as a more detailed mathematical analysis regarding the convolutional codes. Our results show that the perfect scrambling-based security gap presents a very similar result to the practical case, while being much easier to be calculated. Moreover, a more detailed set of results is presented, where the influence in the security gap of the number of antennas among all the nodes in the network is evaluated, as well as other system parameters such as the target reliability constraint and the distance among the nodes.

The rest of this paper is organized as follows. Section II presents the system model and some important preliminary results. Section III proposes and evaluates the scrambler-aided TAS/MRC scheme. Numerical results are given in Section IV in order to evaluate the accuracy of our analyses and, finally, Section V concludes the paper.

II. Preliminaries

A. System Model

We consider a wireless network composed of one transmitter, Alice (A), communicating with a legitimate receiver, Bob (B), in the presence of an eavesdropper, Eve (E). Alice is equipped with n_A antennas and uses TAS to transmit, while Bob and Eve have respectively n_B and n_E receive antennas, applying MRC [15]. The system model is illustrated in Figure 1.

Thus, the frame transmitted by Alice and received by the i-th antenna of node $j \in \{B, E\}$ is

$$\mathbf{y}_j^i = \sqrt{P_t \kappa_j}\, h_j^i\, \mathbf{x} + \mathbf{n}_j^i, \tag{1}$$

being P_t the overall transmit power[1], κ_j the path loss, h_j^i the block-fading coefficient, whose envelop is modeled as a Rayleigh independent identically distributed random variable and which changes independently between frames, $\mathbf{x} \in \mathbb{C}^{1\times M}$ is the average unity energy transmitted frame from Alice, with M the encoded frame length, and $\mathbf{n}_j^i$ is the zero-mean complex Gaussian noise with variance σ_j^2. The path loss κ_j between Alice and the j-th node is modeled as [15]

$$\kappa_j = \frac{\lambda^2}{(4\pi) d_j^{\alpha}}, \tag{2}$$

being d_j the distance between Alice and the j-th node, α the path loss exponent and $\lambda = \frac{3\cdot 10^8}{f_c}$ the carrier wavelength, where

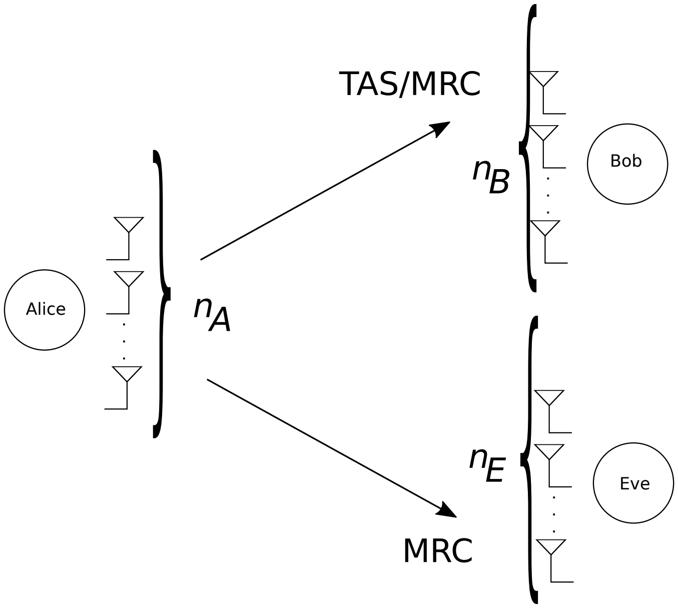

Fig. 1. System model. Alice is equipped with n_A antennas using TAS to transmit, while Bob and Eve are using respectively n_B and n_E antennas, operating under MRC [15].

f_c is the carrier frequency. The instantaneous SNR is then expressed as

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

where $\bar{\gamma}_j = \frac{P_t \kappa_j}{N_0 B}$ corresponds to the average SNR, N_0 the power spectral density and B the bandwidth.

B. Frame Error Rate

In this paper, we adopt the FER as the reliability performance metric, when considering convolutional code with constraint length K and rate R as the error correcting code. Since it is hard (if possible) to obtain a closed-form equation to the FER, we resort to an upper bound, which represents a pessimistic result. In order to obtain such bound, one first needs to upper bound the BER as [18]

$$P_b^{\mathsf{UB}}(\bar{\gamma}) \leq \frac{1}{k} \sum_{\delta=\delta_{\text{free}}}^{\infty} \Lambda_\delta\, P_2(\delta), \tag{4}$$

where k is the number of input bits to encoder (it is a parameter of the code), Λ_δ corresponds to the information weight of the codeword that is at a Hamming distance δ of the all zero codeword, δ_{free} is the minimum Hamming distance of the code

[1] Note that, under the TAS scheme, all the transmit power is allocated to the transmit antenna that maximizes the SNR at Bob and whose index is informed to Alice by a public feedback channel.

and

$$P_2(\delta) = \begin{cases} \displaystyle\sum_{i=\frac{\delta+1}{2}}^{\delta} \binom{\delta}{i} \frac{p^i}{(1-p)^{i-\delta}} & \text{, if } \delta \text{ is odd;} \\ \displaystyle\sum_{i=\frac{\delta}{2}+1}^{\delta} \binom{\delta}{i} \frac{p^i}{(1-p)^{i-\delta}} + \binom{\delta}{\delta/2} \frac{(1/2)\, p^{\delta/2}}{(1-p)^{-\delta/2}} & \text{, if } \delta \text{ is even,} \end{cases} \tag{5}$$

where p is the BER of an additive white Gaussian noise (AWGN) channel without channel coding and depends on the employed modulation. For instance, considering BPSK, we have that $p = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\bar{\gamma}}{R}}\right)$ [10], being erfc the complementary error function.

From (4), one can upper bound the FER of a convolutional code with uncoded frame length N as

$$P_f^{\mathsf{UB}}(\bar{\gamma}) \leq 1 - \left[1 - P_b^{\mathsf{UB}}(\bar{\gamma})\right]^N, \tag{6}$$

being $M = \frac{N}{R}$.

Note that (6) is restricted to an AWGN channel. Then, in order to obtain the average FER of a channel subjected to fading, one must calculate [15, Eq. 6.50]

$$P_f(\bar{\gamma}) = \int_0^\infty f_\gamma(\gamma)\, P_f^{\mathsf{UB}}(\gamma)\, \mathrm{d}\gamma, \tag{7}$$

where $f_\gamma(\gamma)$ corresponds to the the probability density function (pdf) of the random variable γ, which for Rayleigh fading can be written considering MRC or TAS/MRC as shown in Table I [15].

TABLE I. PROBABILITY DENSITY FUNCTION FOR MRC AND TAS/MRC

MRC	$f_\gamma(\gamma) = \frac{\gamma^{n_E-1}\exp\left(\frac{-\gamma}{\bar{\gamma}}\right)}{\bar{\gamma}^{n_E}(n_E-1)!}$
TAS/MRC	$f_\gamma(\gamma) = \frac{n_A}{\Gamma(n_B)}\Gamma\left(n_B, \frac{\gamma}{\bar{\gamma}}\right)^{n_A-1}\left[\left(\frac{\gamma}{\bar{\gamma}}\right)^{n_B-1}\exp\left(-\frac{\gamma}{\bar{\gamma}}\right)\right]$

C. Outage Probability

The outage probability corresponds to the probability that the transmission cannot be decoded with negligible error probability, and can be viewed as an lower bound to the FER [15]. In practice, the outage probability is defined as the probability that the instantaneous SNR γ falls below a target value $\beta = 2^{\mathcal{R}} - 1$, with $\mathcal{R}$ being the spectral efficiency in bits per channel use (bpcu), that is [15]:

$$\mathcal{O}(\bar{\gamma}, \beta) \triangleq \Pr[\gamma < \beta] = \int_0^\beta f_\gamma(\gamma)\, \mathrm{d}\gamma. \tag{8}$$

Thus, after applying the pdfs from Table I in (8), one can show that the outage probability of a system operating under the MRC scheme (which holds to Eve in the system model adopted in this work) becomes [15]:

$$\mathcal{O}_{\mathrm{MRC}}(\bar{\gamma}, \beta) = \Gamma\left(n_r, \frac{\beta}{\bar{\gamma}}\right), \tag{9}$$

where n_r is the number of receiving antennas and $\Gamma(a, b)$ corresponds to the incomplete gamma function, defined as $\Gamma(a,b) = \frac{\int_0^b \exp(-t) t^{a-1}\, \mathrm{d}t}{\Gamma(a)}$. When the transmitter applies TAS among its n_t transmit antennas along with the MRC adopted at the receiver side (which is the case of Bob in our work), the end-to-end outage probability becomes [19], [20]

$$\mathcal{O}_{\mathrm{TAS/MRC}}(\bar{\gamma}, \beta) = \Gamma\left(n_r, \frac{\beta}{\bar{\gamma}}\right)^{n_t}. \tag{10}$$

D. Frame Scrambling

In [10], the authors proposed a non-systematic method of transmission, where the bits within a frame are scrambled before encoding, aiming at increasing security. In this work, we propose the use of an inter-frame scrambling, which performs the scrambling operation among a set of Z frames. Under the assumption of perfect scrambling [10], and considering scrambling in a single frame, a single bit error ensures that half of information are in error after descrambling. In our case, considering frame scrambling, the occurrence of a decoding error in a single frame among the Z scrambled frames ensures that, after descrambling, all the frames will be incorrectly decoded. In practice, according to [10], perfect scrambling can be approached by using a scrambling matrix S with a dense inverse, that is, with a high density of 1s.

In order to calculate the BER and the FER in a system adopting frame scrambling, it is necessary to solve the scrambling within a single frame first. Thus, following [10] and considering that an error will be spread within the frame it belongs to, one can represent the scrambled-based FER within a single frame as

$$P_f^{\mathsf{S}}(\bar{\gamma}) = P_f^{\mathbf{UB}}(\bar{\gamma}). \tag{11}$$

When considering perfect scrambling, each frame in error results in half of information in error. From (11), the BER of a scrambling-aided convolutional code can be estimated as

$$P_b^{\mathsf{S}} = \frac{1}{2} P_f^{\mathsf{S}}, \tag{12}$$

where we drop the index $(\bar{\gamma})$ to lighten the notation.

From (11) and (12), one is then able to calculate the BER and the FER of frame-scrambled convolutional coding, which has been adopted in this work due to its peculiarity of enabling flexible frame lengths, which is an important feature for frame scrambling. After descrambling, each received bit can be seen as a sum of bits from all the Z frames. Thus, the frame scrambling BER is [10]

$$P_b^{\mathsf{ZS}} = \sum_{\substack{i=1 \\ \text{i odd}}}^{Z} \binom{Z}{i} \left(P_b^{\mathsf{S}}\right)^i \left(1 - P_b^{\mathsf{S}}\right)^{Z-i}, \tag{13}$$

and, as one wrong frame leads to an error in each one of the Z frames, the FER can be written as

$$P_f^{\text{ZS}} = 1 - \left(1 - P_f^{\text{S}}\right)^Z . \tag{14}$$

Figures 2 and 3 present a comparison between simulated and theoretical values for the BER and the FER over wireless Rayleigh channel, respectively, considering a convolutional code (with $N = 256$ and $k = 1$) with perfect frame scrambling using the upper bounds from (13) and (14). The difference between theoretical and simulated values can be explained by the use of the upper bound from (4). However, one can see that the analysis supports the simulated results with good precision. Furthermore, since the security gap that we adopt as the performance metric corresponds to the difference between two SNRs, such difference caused by employing the upper bound is minimal in the final results, as will be presented latter.

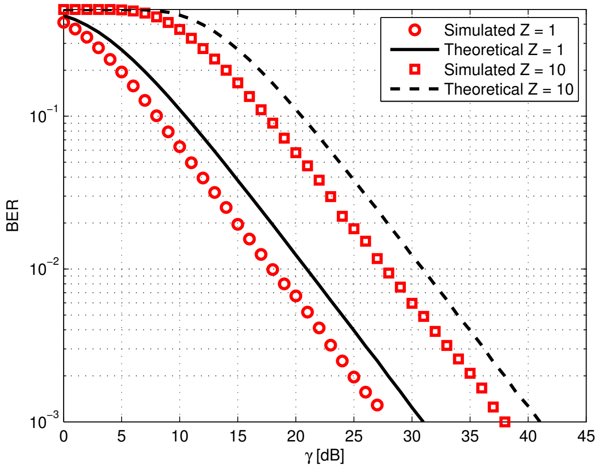

Fig. 2. BER with frame scrambling considering Rayleigh channel, $N = 256$ and perfect scrambling.

E. Security Gap

The security gap is a performance metric defined as the ratio between the SNR required at Bob and Eve to achieve reliable communication for Bob while achieving a sufficient level of physical layer security [9], [10], [21]. In other words, when considering a block fading channel, one must ensure *i) secrecy*, by guaranteeing that the outage probability (or FER) experienced at Eve is above a given target $\mathcal{O}_E^*$ (or P_{fE}^*); and *ii) reliability*, by guaranteeing that Bob operates at an outage probability below a required target $\mathcal{O}_B^*$ (or P_{fB}^*). This is illustrated in Figure 4.

The security gap is then defined as [8]

$$\Delta \triangleq \frac{\bar{\gamma}_B^*}{\bar{\gamma}_E^*}, \tag{15}$$

where $\bar{\gamma}_E^*$ and $\bar{\gamma}_B^*$ represent respectively the average SNR at Eve and Bob necessary to achieve the corresponding target outage probabilities or FERs.

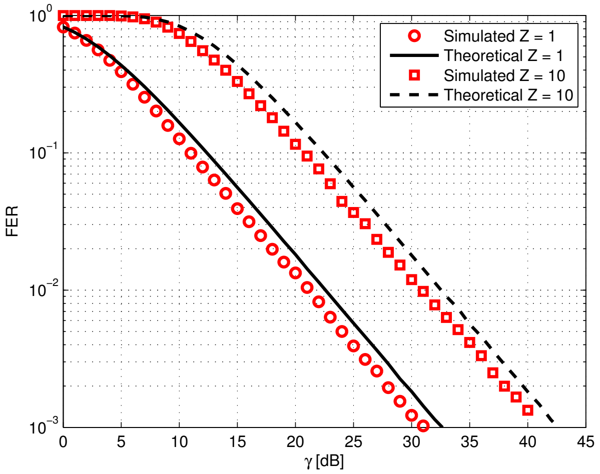

Fig. 3. FER with frame scrambling considering Rayleigh channel, $N = 256$ and perfect scrambling.

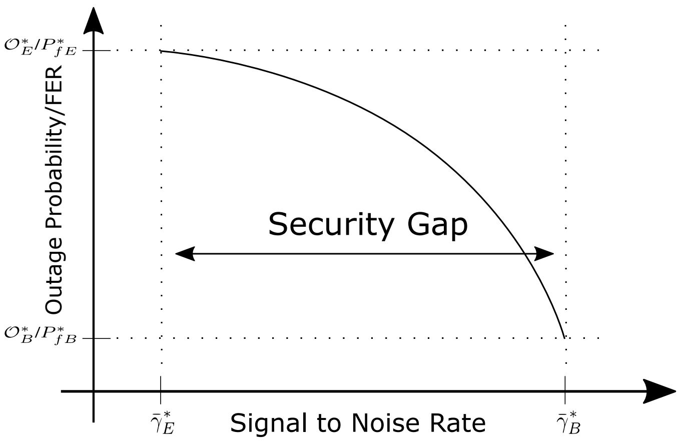

Fig. 4. Outage probability/FER versus SNR showing the bound of security concerning Secrecy ($\mathcal{O}_E/P_{fE} > \mathcal{O}_E^*/P_{fE}^*$) and Reliability ($\mathcal{O}_B/P_{fB} < \mathcal{O}_B^*/P_{fB}^*$). Thus, from (15), the security gap is $\gamma_B^* - \gamma_E^*$. This figure is based on [8].

From (1) and (15), we can notice that smaller the security gap, smaller the distance between Alice and Eve considering a secure communication into the legitimate channel. This effect of the security gap in the distance of Eve and Bob is illustrated in Figure 5.

III. Security Gap of TAS/MRC with Frame Scrambling

In what follows we present the development of the security gap based on outage probability and FER for the scheme adopted in this work, which considers TAS at the transmitter and MRC at both legitimate and malicious receivers.

A. Gap Based on Outage Probability

The main feature of frame scrambling is to spread the error from a single frame to all the Z frames. Thus, considering that

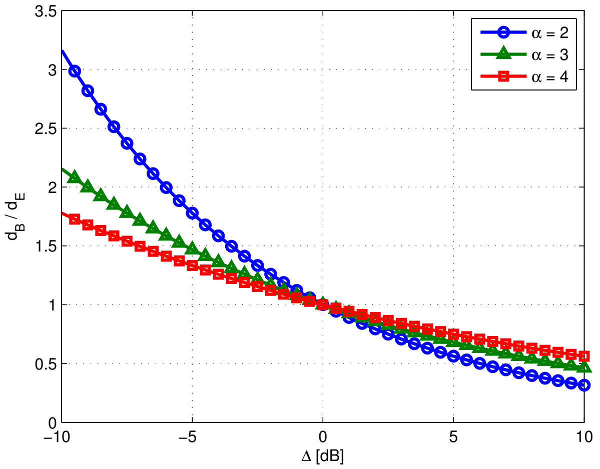

Fig. 5. Effect of α and Δ in the distances of Bob and Eve from Alice.

Bob operates under TAS/MRC and Eve, under MRC, we can write the frame scrambling-aided outage probability of Bob and Eve as

$$\mathcal{O}_B^* = 1 - \left[1 - \mathcal{O}_{\text{TAS/MRC}}\left(n_A, n_B\right)\right]^Z, \tag{16a}$$

$$\mathcal{O}_E^* = 1 - \left[1 - \mathcal{O}_{\text{MRC}}\left(n_E\right)\right]^Z. \tag{16b}$$

From (15), it can be seen that one needs to isolate the SNR from the outage probability in order to obtain the security gap. When isolating $\bar{\gamma}_E^*$ and $\bar{\gamma}_B^*$ respectively from (16a) and (16b), and then applying the result in (15), the outage probability-based security gap in this scenario yields

$$\Delta = \frac{\Gamma^{-1}\left(\left[1 - \left(1 - \mathcal{O}_E^*\right)^{1/Z}\right], n_E\right)}{\Gamma^{-1}\left(\left[1 - \left(1 - \mathcal{O}_B^*\right)^{1/Z}\right]^{1/n_A}, n_B\right)}, \tag{17}$$

where $\Gamma^{-1}(y, a)$ is the inverse incomplete gamma function[2], corresponding to the inverse of $\Gamma(a, b)$.

When $\bar{\gamma} \gg 1$, the incomplete gamma function can be approximated as [19]

$$\Gamma(n_r, \frac{\beta}{\bar{\gamma}}) \approx \frac{\left(\frac{\beta}{\bar{\gamma}}\right)^{n_r}}{\Gamma\left(n_r + 1\right)}, \tag{18}$$

which enables us to obtain a high-SNR approximation for the security gap from (17) as

$$\Delta_{\mathsf{app}} = \frac{\left[\left(1 - \left[1 - \mathcal{O}_E^*\right]^{1/Z}\right)\Gamma\left(n_E + 1\right)\right]^{1/n_E}}{\left[\left(1 - \left[1 - \mathcal{O}_B^*\right]^{1/Z}\right)\Gamma\left(n_B + 1\right)^{n_A}\right]^{1/(n_A n_B)}}. \tag{19}$$

It may be of practical interest to know the number of transmit antennas necessary to achieve a predefined target security gap, which is obtained by isolating n_A in (17) as

$$n_A = \left\lceil \frac{\log\left(1 - \left(1 - \mathcal{O}_B^*\right)^{1/Z}\right)}{\log\left(\Gamma\left(\frac{\Gamma^{-1}\left(1 - \left[1 - \mathcal{O}_E^*\right]^{1/Z}, n_E\right)}{\Delta}, n_B\right)\right)} \right\rceil, \tag{20}$$

where $\lceil\cdot\rceil$ corresponds to the ceil operation.

B. Gap Based on FER

In order to calculate the security gap based on the FER, one first needs to obtain the FER to both Bob (P_{fB}) and Eve (P_{fE}). This can be done by solving (7), which is a hard (if possible) task. Alternatively, one can resort to a semi-analytical approach that simulates the fading effect through Monte Carlo integration [22], [23] by creating several channel realizations satisfying the probability density function presented in Table I and, using theoretical equations with these values, calculate the BER and the FER. This process can be simpler than a real simulation, which is to create a bit array, modulate it and then calculate the performance in the channel. According to this approach, the instantaneous overall SNR γ for Bob (after TAS/MRC operation) and Eve (after MRC) are obtained from the upper bound on the FER for the AWGN channel, after averaging the error probability from the ensemble of individual channel realizations.

If a target FER of P_{fB}^* for Bob and P_{fE}^* for Eve is required at the destination, one must have a single frame error probability

$$P_{fB} = 1 - \left(1 - P_{fB}^*\right)^{\frac{1}{Z}}, \tag{21a}$$

$$P_{fE} = 1 - \left(1 - P_{fE}^*\right)^{\frac{1}{Z}}. \tag{21b}$$

Then, the security gap based on the FER is achieved after obtaining the inverse functions of P_{fB} and P_{fE}, that is, representing $\bar{\gamma}$ as a function of P_{fB} and P_{fE}. Thus, from (15), (21a) and (21b), the FER-based security gap can be finally written as

$$\Delta = \frac{P_{fB}^{-1}\left(1 - \left(1 - P_{fB}^*\right)^{\frac{1}{Z}}\right)}{P_{fE}^{-1}\left(1 - \left(1 - P_{fE}^*\right)^{\frac{1}{Z}}\right)}. \tag{22}$$

Unlike the outage-based scenario, it is not possible to obtain the number of transmit antennas necessary to achieve a given security gap in a closed-form equation. However, note that such value can be easily obtained through an exhaustive search. These numerical analysis introduce an error, which must be set in the project. This error is defined as the gap between the results of two consecutive iterations [22], [23].

[2] Note that, even tough this is not actually a closed-form result, the inverse incomplete gamma function is already available in several programming softwares, such as the `gammaincinv` function in Matlab®, for instance.

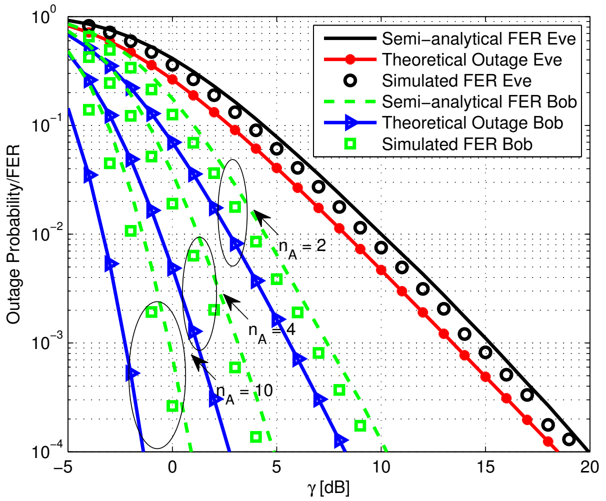

Fig. 6. Comparison between outage probability and the FER for Eve and Bob considering $n_A \in [2, 4, 10]$, $N = 256$.

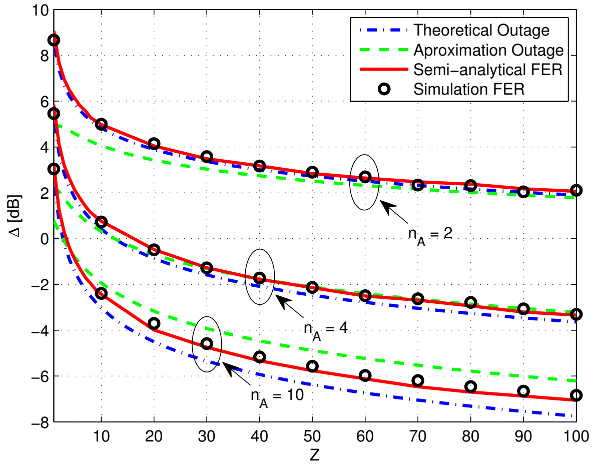

Fig. 7. Security gap calculated by the theoretical equation using outage probability (17), approximation (19) from [17] and the semi-analytical approach to solve (22) using the FER of Standard NASA convolutional code with rate $1/2$ (constraint length 7 and generator polynomial in octal [133, 171]), $k = 1$ and $N = 256$ bits', and the simulation of this same code. Considering $n_A \in [2, 4, 10]$ and $n_B = n_E = 2$.

IV. Simulations

In this section, we present some numerical results in order to evaluate the accuracy of the analysis presented in the previous sections. Unless stated otherwise, in the following we assume a reliability constraint at Bob (P^*_{fB} or $\mathcal{O}^*_B$) equal to 0.01, while the minimum allowed error level at Eve (P^*_{fE} or $\mathcal{O}^*_E$) is set to 0.9 and $\mathcal{R} = 1$ bpcu. We also adopt the NASA-Standard Convolutional Code $(1, 2, 7)$, with generator polynomials in octal [133, 171], $k = 1$ and whose $\delta_{\text{free}} = 10$ [18, Table 8-2-1].

Figure 6 presents the individual outage probability and FER of both Bob and Eve, without frame scrambling ($Z = 1$), obtained from the analyses and validated by simulations/numerical results. The analytical outage probability from Eve is obtained from (9), while for Bob it is given by (10). The upper bound FER is calculated by simulating the effect of (7) (referred to as "semi-analytical" approach). In this figure, we plotted just one set of curves of Eve, because she is not affected by n_A. It happens as an effect of TAS, which makes Alice always chooses the best antenna for Bob which is not necessarily the best for Eve, since the legitimate and malicious channels are independent. This leads to an improved performance at Bob as n_A increases. Moreover, one can also notice that the analytical results match the simulations with good accuracy. Another important remark is that, even considering infinite frame length, the obtained values from outage probability are very close to the FER-based results, which consider finite frame length and codes that do not achieve the channel capacity. We can observe that the larger the parameter δ_{free} of the code, the smaller the upper bound BER from (4) and consequently the smaller the upper bound FER from (6). However, as security gap is calculated as the difference between two values of SNR, the gap is weakly affected by this parameter.

A. Security Gap as a Function of Z

In Figure 7 we present both the outage-based (17), approximated (19) and FER-based security gaps, with the frame scrambling operation and assuming $n_B = n_E = 2$. We can see that, either employing the outage or the FER as the metric, one can predict security gaps smaller than zero when the scrambling depth Z and the number of transmit antennas n_A increases.

Moreover, we can observe that the difference between the two predictions of the security gap based on outage probability (exact and approximation) increase as n_A increases. For $n_A = 2$, we see that the accuracy of the approximation increases as Z increases. It happens, because, when Z increases, more link quality is needed, getting better the accuracy of the approximation. However, the opposite occurs when we consider $n_A = 10$, for the reason that increasing the number of antennas in Alice makes the SNR decreases, which decreases the accuracy of the approximation consequently.

It is also worthy mentioning that the decoding delay is increased with the increase of Z, establishing a trade-off. Thus, the choice of the optimum value of Z must also take into account the delay requirements of the network.

B. Security Gap as a Function of n_A, n_B and n_E

Next we investigate the behavior of the security gap as a function of the number of antennas in Alice and Eve. Figures 8, 9 and 10 plot the security gap as a function of n_A and n_E considering, respectively, the exact outage probability from (17), the approximate outage probability from (19), and the FER. All of them considering the use of frame scrambling with depth $Z = 10$ frames.

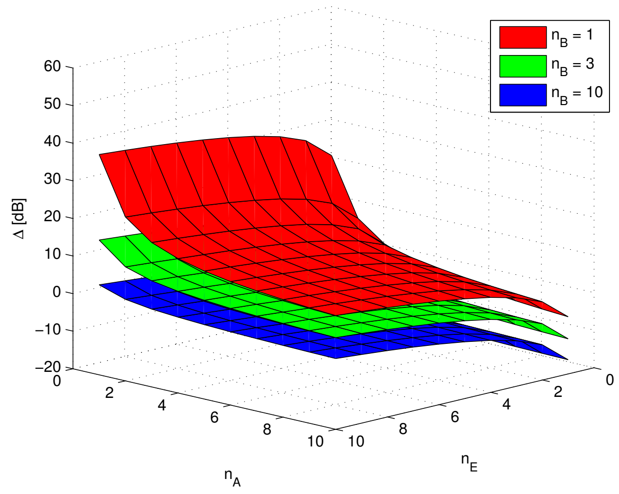

Fig. 8. Security gap based on exact outage probability as a function of n_A and n_E considering $n_B \in [1, 3, 10]$.

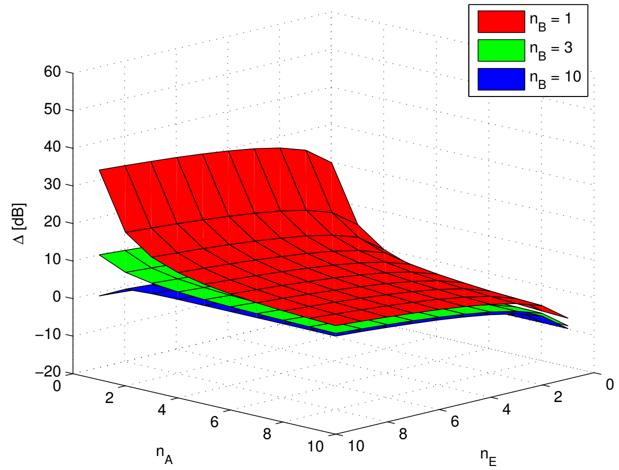

Fig. 9. Security gap based on approximate outage probability as a function of n_A and n_E considering $n_B \in [1, 3, 10]$.

Comparing Figures 8 and 9 we observe that the difference between exact and approximate curves increases with n_A and n_B, as also observed in Figure 7. This behavior can be explained by the high-SNR approximation used in (18). As n_A or n_B increases, less link quality is needed to achieve the same performance, making the approximation to be less accurate. That means that the actual results (in terms of required security gap) can be even smaller than those found in [17]. The results in Figure 10, which consider a real code that does not achieve channel capacity, show security gap values better than those presented in Figure 8. This implies that legitimate channel can be in a much worse condition when compared to illegitimate one than we previously calculated.

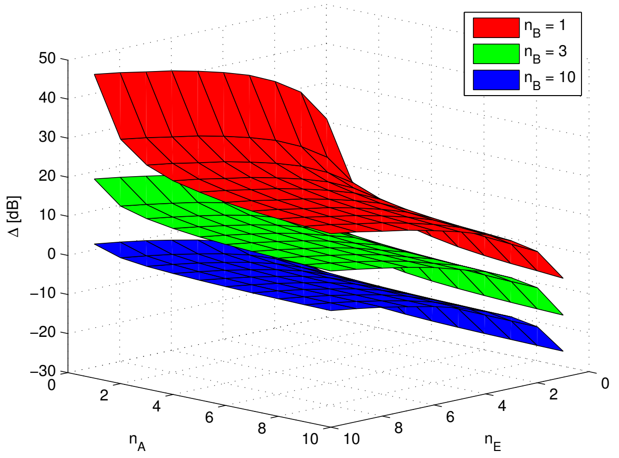

Fig. 10. Security gap based on FER as a function of n_A and n_E considering $n_B \in [1, 3, 10]$.

C. Number of Antennas in Alice

Tables II and III present the number of transmit antennas n_A necessary to achieve a gap equal to 0 dB, for different target outage probabilities (obtained according to (20)) and FER (obtained numerically) at Eve, when adopting a target outage probability/FER at Bob equal to 0.01.

TABLE II. n_A AS FUNCTION OF Δ, $\mathcal{O}_E^*$ AND Z, FOR $\mathcal{O}_B^* = 0.01$ AND $n_B = n_E = 2$.

Z	$\mathcal{O}_E^*$				
	0.1	0.3	0.5	0.7	0.9
1	2	4	7	13	44
10	2	3	3	4	5
100	2	2	2	3	3

TABLE III. n_A AS FUNCTION OF Δ, FER$_E^*$ AND Z, FOR $P_{fB}^* = 0.01$, $N = 256$ AND $n_B = n_E = 2$.

Z	P_{fE}^*				
	0.1	0.3	0.5	0.7	0.9
1	3	5	8	18	94
10	2	3	3	4	5
100	2	2	2	3	3

From these tables, one can see that, in the absence of frame scrambling, the number of transmit antennas necessary to achieve a security gap equal to 0 dB is in general larger when adopting the FER as the performance metric than when adopting the outage-probability. However, when the scrambling depth increases, both scenarios (FER and outage) present the same behavior. For instance, when $Z = 100$, it is possible to achieve a security gap equal to zero, with Bob (resp. Eve) operating at a FER/outage of 0.01 (resp. 0.9) with a practical and feasible number of three transmit antennas. For $Z = 10$, one would need a similar number of antennas at Alice to achieve the same result as $Z = 100$, however, the delay would be considerably decreased.

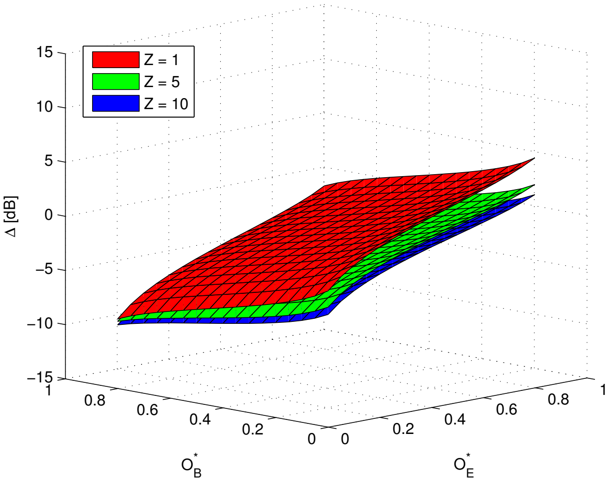

Fig. 11. Security gap based on exact outage probability as a function of $\mathcal{O}_B^*$ and $\mathcal{O}_E^*$ considering $Z \in [1, 5, 10]$ and $n_A = n_B = n_E = 2$.

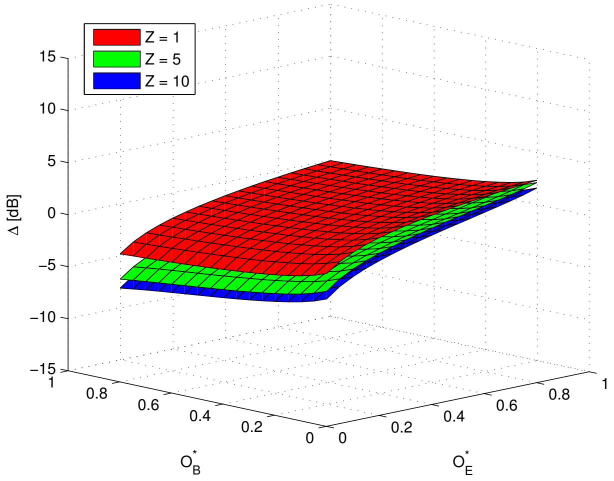

Fig. 12. Security gap based on approximate outage probability as a function of $\mathcal{O}_B^*$ and $\mathcal{O}_E^*$ considering $Z \in [1, 5, 10]$ and $n_A = n_B = n_E = 2$.

Therefore, we may say that the theoretical prediction of the required security gap provided by the outage probability formulation is accurate enough to give a very reasonable approximation of the true security gap, specially for large frame scrambling depths, what is a desirable result as larger frame scrambling depths increase the physical layer security of the proposed approach.

D. Security Gap as a Function of the Outage/FER Targets

Here we evaluate the influence of the Outage/FER target values for Bob and Eve in the security gap. We consider all nodes with two antennas and frame scrambling with depth $Z \in [1, 5, 10]$. Figures 11, 12 and 13 plot the respective cases with exact outage probability, approximate outage probability and FER.

In the three cases we can observe that the security gap increases considerably as the target for Eve increases, while and opposite behavior is observed if the target for Bob increases. This behavior can be explained due to the fact that large target values for Eve lead to more errors in Eve and consequently less channel quality, increasing the security gap. The same happens to Bob. In addition, a final observation when comparing Figures 11 and 12 concerns the outage approximation in (19) for small values of Z. Notice that when $Z = 1$ the approximation is not very accurate, once the gap presented in Figure 11 is much smaller than that in Figure 12. However, the accuracy of the approximation increases when Z increases. Finally, one can see that Figures 11 and 13 are in good agreement, and that, the security gap based on outage probability is an alternative to estimate security in a real scenario in order to skip numerical solutions.

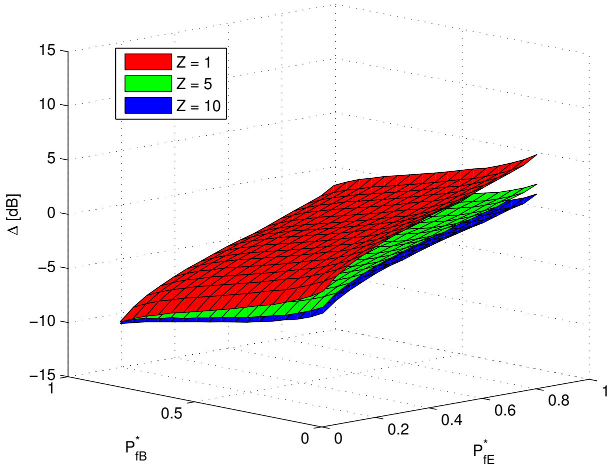

Fig. 13. Security gap based on FER as a function $\mathcal{O}_B^*$ and $\mathcal{O}_E^*$ considering $Z \in [1, 5, 10]$ and $n_A = n_B = n_E = 2$.

V. Final Comments

We evaluated the security gap of a network composed of two legitimate nodes and one passive eavesdropper, being all of them provided with multiple antennas, communicating under quasi-static Rayleigh fading. We consider the use of TAS and frame scrambling at Alice, with both receiver nodes operating under the MRC protocol. We showed that it is possible to achieve negative security gaps with a feasible number of antennas at the legitimate transmitter and receiver nodes. Moreover, we showed that the required security gap to guarantee a set of target outage probabilities can be well predicted by both a FER based formulation and a theoretical outage probability analysis, and that the accuracy of the outage based formulation increases with the frame scrambling depth. Finally, we also showed that the approximation for the outage probability can be used to estimate the number of antennas to achieve a given desired security gap when frame scrambling with $Z \geq 10$ is employed.

References

[1] M. A. Chiodi Junior, J. L. Rebelatto, R. Demo Souza, and G. Brante, "On the Security Gap of Convolutional-Coded Transmit Antenna Selection Systems," in *XXXIII Simpósio Brasileiro de Telecomunicações 2015 (SBrT2015)*, Juiz de Fora, Brazil, September 2015.

[2] C. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, October 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x

[3] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975. doi: 10.1002/j.1538-7305.1975.tb02040.x

[4] P. K. Gopala, L. Lai, and H. E. Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, 2008. doi: 10.1109/TIT.2008.928990

[5] J. Barros and M. Rodrigues, "Secrecy Capacity of Wireless Channels," in *Information Theory, 2006 IEEE International Symposium on*, July 2006. doi: 10.1109/ISIT.2006.261613 pp. 356–360.

[6] 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, April 2009. doi: 10.1109/TIT.2009.2013043

[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, C. U. Press, Ed. Cambridge University Press, 2011.

[8] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian Wiretap Channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 532 – 540, 2011. doi: 10.1109/TIFS.2011.2134093

[9] M. Baldi, M. Bianchi, N. Maturo, and F. Chiaraluce, "A practical viewpoint on the performance of LDPC codes over the fast Rayleigh Fading Wire-Tap Channel," *IEEE Symposium on Computers and Communications*, pp. 000 287 – 000 292, 2013. doi: 10.1109/ISCC.2013.6754961

[10] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analisys," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 883 – 894, 2012. doi: 10.1109/TIFS.2012.2187515

[11] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Communications*, vol. 6, pp. 311–335, 1998. doi: 10.1023/A:1008889222784

[12] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009. doi: 10.1109/TIT.2009.2018322

[13] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, June 2012. doi: 10.1109/LSP.2012.2195490

[14] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, January 2013. doi: 10.1109/TCOMM.2012.12.110670

[15] A. Goldsmith, *Wireless Communications*, C. U. Press, Ed. Cambridge University Press, 2005.

[16] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68–73, October 2004. doi: 10.1109/MCOM.2004.1341263

[17] M. A. Chiodi Junior, J. L. Rebelatto, R. D. Souza, and G. G. O. Brante, "Achieving Negative Security Gap with Transmit Antenna Selection and Frame Scrambling in Quasi-Static Fading Channels," *Electronics Letters*, vol. 51, pp. 200,202, 2015. doi: 10.1049/el.2014.3244

[18] J. Proakis, *Digital Communications*, ser. Electrical engineering series. McGraw-Hill, 2001.

[19] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of Transmit Antenna Selection/Maximal-Ratio Combining in Rayleigh Fading Channels," *IEEE Trans. Veh. Commun.*, vol. 54, pp. 1312 – 1321, 2005. doi: 10.1109/TVT.2005.851319

[20] C.-Y. Chen, A. Sezdin, J. M. Cioffi, and A. Paulraj, "Antenna Selection in Space-Time Block Coded Systems: Performance Analysis and Low-Complexity Algorithm," *IEEE Trans. Signal Process.*, vol. 56, pp. 3303 – 3314, 2008. doi: 10.1109/TSP.2008.917856

[21] M. Baldi, M. Bianchi, N. Maturo, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *Information Theory Workshop (ITW), 2010 IEEE*, 2010. doi: 10.1109/CIG.2010.5592833 pp. 1–5.

[22] P. K. MacKeown, *Stochastic simulation in physics*. Singapore ; New York : Springer, 1997.

[23] J. Chen and L. Feng, "Using Lower and Upper Bounds to Increase the Computing Accuracy of Monte Carlo Method," in *Computational and Information Sciences (ICCIS), 2010 International Conference on*, December 2010. doi: 10.1109/ICCIS.2010.159 pp. 630–633.

Marco Antônio Chiodi Junior was born in Apiaí-SP, Brazil, in 1991. He received the BSc. degree (2014) in Electrical Engineering (Emphasis in Electronics and Telecommunications) and the MSc. Degree in Electrical Engineering in 2016, both from Federal University of Technology — Paraná (UTFPR), Curitiba, Brazil. He has been working on telemetry and wireless communications since 2014.

João Luiz Rebelatto was born in Lapa-PR, Brazil, in 1984. He received the B.Sc. degree from the Federal University of Technology - Paraná (UTFPR), Curitiba, Brazil, in 2006 and the D.Sc. degree from the Federal University of Santa Catarina (UFSC), Florianópolis, Brazil, in 2010, both in electrical engineering. From September 2009 to August 2010 he was a Visiting Ph.D. Student at the University of Sydney, Australia. From February 2011 to January 2012 he held a Post-Doctoral position at the UFSC. Since June 2011 he has been with the Department of Electronics, UTFPR, where he is currently an Assistant Professor. His research interests are in the area of coding and information theory, with applications to wireless communications systems.

Richard Demo Souza was born in Florianópolis, Brazil. He received the B.Sc. and the D.Sc. degrees in Electrical Engineering from the Federal University of Santa Catarina (UFSC), Brazil, in 1999 and 2003, respectively. From March 2003 to November 2003, he was a Visiting Researcher in the Department of Electrical and Computer Engineering at the University of Delaware, USA. Since April 2004 he has been with the Federal University of Technology - Paraná (UTFPR), Brazil, where he is now an Associate Professor. His research interests are in the areas of wireless communications and signal processing. He is a Senior Member of the IEEE and of the Brazilian Telecommunications Society (SBrT) and has served as Associate Editor for the IEEE Communications Letters, the EURASIP Journal on Wireless Communications and Networking, and the IEEE Transactions on Vehicular Technology. He is a co-recipient of the 2014 IEEE/IFIP Wireless Days Conference Best Paper Award and the supervisor of the awarded 2013 Best PhD Thesis in Electrical Engineering in Brazil.

Glauber Brante was born in Arapongas-PR, Brazil, in 1983. He received the B.Sc., M.Sc. and D.Sc. degrees in Electrical Engineering from the Federal University of Technology - Paraná (UTFPR), Curitiba-, Brazil, in 2007, 2010 and 2013, respectively. He is currently an Assistant Professor at the same University. From January to September 2012 he was a Visiting Researcher at the Institute of Information and Communication Technologies, Electronics and Applied Mathematics (ICTEAM) at the Catholic University of Louvain, Belgium. His research interests include cooperative communications, HARQ, energy efficiency and physical layer security.