On the Security Gap of Convolutional-Coded Transmit Antenna Selection Systems

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

***Abstract*— In this work we evaluate the security gap of a network composed of two legitimate nodes and one passive eavesdropper, all of them provided with multiple antennas. We consider that transmit antenna selection (TAS) along with frame scrambling is adopted at the transmitter node, while both legitimate and malicious receivers operate under the maximum ratio combining (MRC) protocol. By considering a quasi-static fading scenario, we evaluate (analytically and through numerical results) the security gap in terms of both outage probability and frame error rate (when using convolutional codes), showing that in both situations 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 that allows eavesdroppers to potentially intercept any transmission. Information theoretic secrecy, introduced by Shannon in 1949 [1], is a promising approach towards increasing communication security complementing classical cryptography techniques. In [2], 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 an eavesdropper (Eve). Recent works have applied concepts of information theoretic secrecy to wireless communications, showing that the randomness inherent to wireless channels can improve the secrecy of the network [3]–[5].

However, the design of practical wiretap codes with feasible block lengths is general unknown for many scenarios of interest, as is the case of quasi-static fading wireless channel [6]. A more practical security metric was introduced in [7]. In the so-called security gap, the security is 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. That is, 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 [8], the authors resort to a technique referred to as frame scrambling, where several independent frames are mixed aiming at decreasing the security gap by boosting the propagation of residual errors. The idea behind scrambling is that a single residual bit error in one of several scrambled frames is sufficient to maximize the uncertainty of the decoding process, leading to a scenario where half of the bits are incorrectly decoded. 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 [9], 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 [10]–[12].

Some preliminary results on the outage probability-based security gap in a MIMO scenario, where Alice adopts the transmit antenna selection (TAS) scheme [13], [14] while both Bob and Eve operate under the maximum ratio combining (MRC) scheme [13], are presented in [15] 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 [14].

In this work, under the same framework as [15], 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 [15]. Moreover, we also evaluate the performance of the proposed scheme by adopting a more realistic FER-based security gap formulation, which is calculated supposing the use of convolutional codes. Our results 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 possible even if the channel between Alice and Eve is in better conditions, in average, than the channel between Alice and Bob.

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.

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).

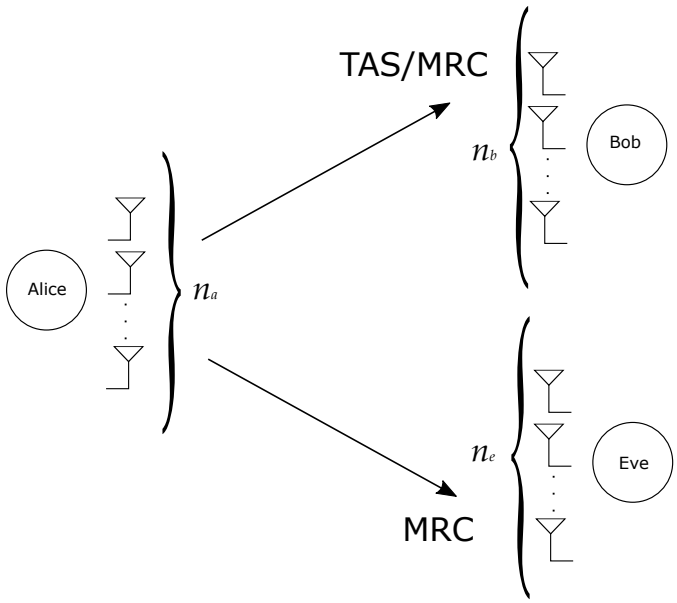

Fig. 1. System model. Alice is equipped with n_A antennas using TAS to transmit, while Bob and Eve are using respectively n_B and n_E antennas, operating under MRC [13].

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 [13]. This is illustrated in Fig. 1.

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

$$\mathbf{y}_j^i = \sqrt{P d_j^{-\alpha}}\, h_j^i\, \mathbf{x} + \mathbf{n}_j^i, \tag{1}$$

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

The instantaneous SNR can be expressed as $\gamma_j = \bar{\gamma}_j \left|h_j^i\right|^2$, where $\bar{\gamma}_j = P d_j^{-\alpha}$ corresponds to the average SNR. Thus, the outage probability under Rayleigh fading becomes [13]

$$\mathcal{O}\left(\mathcal{R}, \gamma_j\right) \triangleq \Pr[\gamma_j < \beta] = 1 - \exp\left(-\frac{\beta}{\bar{\gamma}_j}\right), \tag{2}$$

where $\beta = 2^{\mathcal{R}} - 1$ and $\mathcal{R}$ is the spectral efficiency in bits per channel use (bpcu).

[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.

B. Frame Error Rate

In this paper, we also adopt the frame error rate (FER) as the reliability performance metric, when considering the class of (n, k, K) convolutional codes 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 bit error rate (BER) as [16]

$$P_b^{\mathsf{AWGN}}\left(\bar{\gamma}\right) \leq \frac{1}{k} \sum_{\delta=\delta_{\text{free}}}^{\infty} \beta_\delta\, P_2(\delta), \tag{3}$$

where β_δ corresponds to the information weight of the codeword that is at a distance δ of the all zero codeword, δ_{free} is the minimum distance of the code and

$$P_2(\delta) = \begin{cases} \displaystyle\sum_{i=\frac{\delta+1}{2}}^{\delta} \binom{\delta}{i} \frac{p^i}{(1-p)^{i-\delta}} & \text{, if } \delta \text{ is odd;} \\ \displaystyle\sum_{i=\frac{\delta}{2}+1}^{\delta} \binom{\delta}{i} \frac{p^i}{(1-p)^{i-\delta}} + \binom{\delta}{\delta/2} \frac{(1/2)\, p^{\delta/2}}{(1-p)^{-\delta/2}} & \text{, if } \delta \text{ is even,} \end{cases} \tag{4}$$

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 can write $p = \frac{1}{2}\text{erfc}\left(\sqrt{\bar{\gamma}}\right)$, being erfc the complementary error function.

From (3), the upper bound for the FER of a convolutional code with frame length given by N can be obtained as

$$P_f^{\mathsf{AWGN}}(\bar{\gamma}) \leq 1 - \left[1 - P_b^{\mathsf{AWGN}}(\bar{\gamma})\right]^N. \tag{5}$$

Note that (5) is restricted to an AWGN channel. Then, in order to obtain the average FER of a channel subjected to fading, one must calculate [13, Eq. 6.50]

$$P_f\left(\bar{\gamma}\right) = \int_0^\infty f_\gamma\left(\gamma\right) P_f^{\mathsf{AWGN}}\left(\gamma\right) \mathrm{d}\gamma, \tag{6}$$

where $f_\gamma\left(\gamma\right)$ corresponds to the the probability density function (pdf) of the random variable γ, which for Rayleigh fading is exponential distributed with pdf $f_\gamma(\gamma) = (1/\bar{\gamma}) \exp\left(-\gamma/\bar{\gamma}\right)$.

C. Frame Scrambling

In [8], the authors proposed a non-systematic method of transmission, where the bits within a frame (or several consecutive frames) 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 leading to a non-systematic transmission. Under the assumption of perfect scrambling [8] and considering scrambling in a single frame, just a bit error ensures that half of information are in error after descrambling. In our case, one single bit error in any one of Z frames ensures that, after descrambling, half of the bits throughout all the frames are incorrectly decoded. In practice, according to [8], perfect scrambling can be approached by using a scrambling

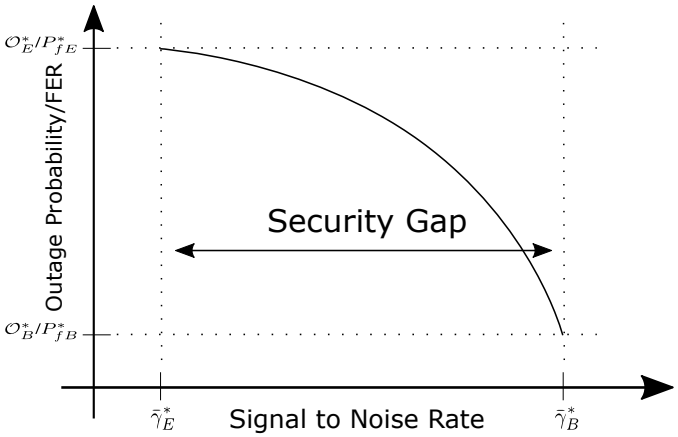

Fig. 2. Outage probability/FER versus SNR showing the bound of security concerning Secrecy ($\mathcal{O}_E/P_{fE} > \mathcal{O}_E^*/P_{fE}^*$) and Reliability ($\mathcal{O}_B/P_{fB} < \mathcal{O}_B^*/P_{fB}^*$). Thus, from (11), the security gap is $\gamma_B^* - \gamma_E^*$. This figure is based on [7].

matrix S with a dense inverse, that is, with a high density of 1s. Consequently, considering $\mathcal{O}$ to be the outage probability of a single frame, the outage probability of Z scrambled frames, $\mathcal{O}_Z^*$, can be calculate [8] as

$$\mathcal{O}_Z^* = 1 - (1 - \mathcal{O})^Z . \tag{7}$$

Thus, from (7), one can obtain the outage probability of a single frame as

$$\mathcal{O} = 1 - (1 - \mathcal{O}_Z^*)^{1/Z} . \tag{8}$$

Likewise, the FER of a single frame P_f is obtained as

$$P_f = 1 - \left(1 - P_{fZ}^*\right)^{1/Z} , \tag{9}$$

where P_{fZ}^* represents the FER of Z scrambled frames.

D. 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 [8], [17], [18]. 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 Fig. 2. The security gap is then defined as [7]

$$\Delta \triangleq \frac{\bar{\gamma}_B^*}{\bar{\gamma}_E^*}, \tag{10}$$

where $\bar{\gamma}_E^*$ and $\bar{\gamma}_B^*$ represent respectively the average SNR at Eve and Bob necessary to achieve a target outage probability or FER. Alternatively, the security gap in dB is

$$\Delta \triangleq \bar{\gamma}_B^* - \bar{\gamma}_E^* \qquad \text{(dB)}. \tag{11}$$

From the definition of the security gap, we can see that the smaller the gap, the better the performance in terms of physical layer security.

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

As presented in [13] the outage probability of a receiver operating under the MRC scheme can be expressed as

$$\mathcal{O}_{\text{MRC}}\left(n_r\right) = \Gamma\left(n_r, \frac{\beta}{\bar{\gamma}}\right), \tag{12}$$

where n_r is the number of receiving antennas and $\Gamma(a, b)$ corresponds to the incomplete gamma function, defined as

$$\Gamma(a, b) = \frac{\int_0^b \exp\left(-t\right) t^{a-1}\, \mathrm{d}t}{\Gamma(a)}. \tag{13}$$

When the transmitter applies TAS among its n_t transmit antennas along with the MRC adopted at the receiver side, the end-to-end outage probability becomes [19], [20]

$$\mathcal{O}_{\text{TAS/MRC}}\left(n_t, n_r\right) = \Gamma\left(n_r, \frac{\beta}{\bar{\gamma}}\right)^{n_t} . \tag{14}$$

After applying scrambling, we have from (8) that the outage probability of a single frame at Bob and Eve, when taking into account the outage probabilities from (14) and (12), are given respectively by

$$\mathcal{O}_B^* = 1 - \left[1 - \mathcal{O}_{\text{TAS/MRC}}\left(n_A, n_B\right)\right]^Z , \tag{15a}$$

$$\mathcal{O}_E^* = 1 - \left[1 - \mathcal{O}_{\text{MRC}}\left(n_E\right)\right]^Z . \tag{15b}$$

From (10), it can be seen that one needs to isolate the SNR from the outage probability equation in order to obtain the security gap. When isolating $\bar{\gamma}_E^*$ and $\bar{\gamma}_B^*$ respectively from (15b) and (15b), and then applying the result in (10), the outage probability-based security gap in this scenario yields

$$\Delta = \frac{\Gamma^{-1}\left(\left[1 - (1 - \mathcal{O}_E^*)^{1/Z}\right], n_E\right)}{\Gamma^{-1}\left(\left[1 - (1 - \mathcal{O}_B^*)^{1/Z}\right]^{1/n_A}, n_B\right)}, \tag{16}$$

where $\Gamma^{-1}(y, a)$ is the inverse incomplete gamma function[2], corresponding to the inverse of (13).

When $\bar{\gamma} \gg 1$, the incomplete gamma function can be approximated as $\Gamma(n_r, \frac{\beta}{\bar{\gamma}}) \approx \left(1/\Gamma\left(n_r + 1\right)\right)\left(\beta/\bar{\gamma}\right)^{n_r}$, which enables us to obtain a high-SNR approximation for the security gap from (16) as

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

[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.

It may be of practical interest to have the number of transmit antennas necessary to achieve a predefined target security gap, which is obtained by isolating n_A in (16) as

$$n_A = \left\lceil \frac{\log\left(1-\left(1-\mathcal{O}_B^*\right)^{1/Z}\right)}{\log\left(\Gamma\left(\frac{\Gamma^{-1}\left(1-\left[1-\mathcal{O}_E^*\right]^{1/Z}, n_E\right)}{\Delta}, n_B\right)\right)} \right\rceil, \tag{18}$$

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

Note that the case without frame scrambling is obtained from (16)-(18) by properly substituting $Z = 1$.

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 (referred to as P_{fB}) and Eve (P_{fE}). This can be done by solving (6), 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. According to this approach, the instantaneous overall SNR γ for Bob (which results from the TAS/MRC operation) and Eve (after MRC) are obtained from the upper bound on the FER for the AWGN channel, after averaging the probability of error for each channel realization.

The security gap based on the FER is then 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 (10), the FER-based security gap can be finally written as

$$\Delta = \frac{P_{fB}^{-1}\left(1-\left(1-P_{fB}^*\right)^{\frac{1}{Z}}\right)}{P_{fE}^{-1}\left(1-\left(1-P_{fE}^*\right)^{\frac{1}{Z}}\right)}. \tag{19}$$

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 a numerical analysis. Finally, again it is worthy noting that the case without frame scrambling is obtained by making $Z = 1$.

IV. Simulations

In this section, we present some numerical results in order to evaluate the accuracy of the analysis presented previously. Unless stated otherwise, in the following results we assume $n_B = n_E = 2$, reliability constraint at Bob (P_{fB}^* or $\mathcal{O}_B^*$) equal to 0.01, while the minimum allowed reliability level at Eve (P_{fE}^* or $\mathcal{O}_E^*$) is set to 0.9. We also consider that $N = 256$ bits and $\mathcal{R} = 1$ bpcu. We also adopt the NASA-Standard Convolutional Code $(1, 2, 7)$, with generator polynomial in octal $[133, 171]$ and whose $\delta_{\text{free}} = 10$ [16, Table 8-2-1].

Figure 3 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 (12), while for Bob it is given by (14). The upper bound FER is calculated by simulating the effect of (6) (referred to as "semi-analytical" approach). From the figure, we can see that Eve is not affected by n_A, since the legitimate and malicious channels are independent, because TAS always chooses the best antenna for Bob, which seems a random choice for Eve. 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.

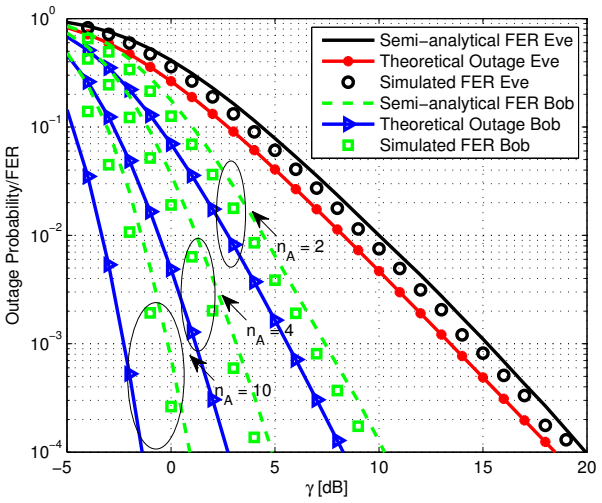

Fig. 3. Comparison between outage probability and upper bound FER for Eve and Bob considering $n_A \in [2, 4, 10]$.

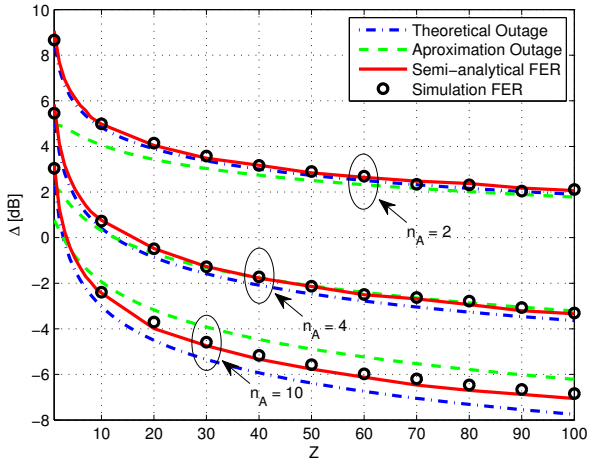

Fig. 4. Security gap calculated by theoretical equation using outage probability, approximation from [15], semi-analytical approach using FER of Standard NASA convolutional code with rate $1/2$ (constraint length 7 and generator polynomial in octal $[133, 171]$) and $N = 256$ bits, and the simulation of this same code. Considering $n_A \in [2, 4, 10]$.

In Figure 4, we present both the outage-based (16), approximated (17) and FER-based security gap, with the frame scrambling operation obtained according to (8) and (9), respectively. 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.

We can observe that the difference between the two predictions of the security gap based on outage probability (exact

and approximation) grow up as n_A increases. For $n_A = 2$, we see that the approximate result tends to the exact one as Z increases. However, this is not true when we consider $n_A = 10$. This behavior can be explained analyzing the approximate equation which is only valid to $\bar{\gamma} \gg 1$ [15]. As n_A 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 [15].

In Tables I and II we present the number of transmit antennas n_A necessary to achieve a gap equal to 0 dB, for different target outage probabilities (Table I, obtained according to (18)) and FER (Table II, obtained numerically) at Eve, when adopting a target outage probability/FER at Bob equal to 0.01.

TABLE I

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 II

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 Tables I and II, 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. When $Z = 100$, for example, 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. 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.

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.

REFERENCES

[1] C. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

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

[3] 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.

[4] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 356–360.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] S. Sanayei and A. Nosratinia, "Antenna selection in mimo systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68–73, Oct 2004.

[15] M. A. Chiodi-Jr., 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.

[16] J. G. Proakis, *Digital Communications*. McGraw-Hill, 2001.

[17] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *Information Theory Workshop (ITW), 2010 IEEE*, 2010, pp. 1–5.

[18] 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.

[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.

[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.