Adaptive Secure Rate Allocation via TAS/MRC under Multi-Antenna Eavesdroppers

Irfan Muhammad*, Onel L. Alcaraz López*, Hirley Alves*, Diana P. M. Osorio†, Edgar E. Benitez Olivo‡, and Matti Latva-aho*
*Centre for Wireless Communications (CWC), University of Oulu, Finland
† Federal University of São Carlos (UFSCar), São Carlos, Brazil
‡ São Paulo State University (UNESP), Campus of São João da Boa Vista, Brazil
{firstname.lastname}@oulu.fi, dianamoya@ufscar.br, edgar.olivo@unesp.br

***Abstract*—This paper investigates the secrecy outage performance of a multiple-input multiple-output and multi-antenna eavesdropper system. We consider a novel formulation for the secrecy outage probability, which is capable of quantifying reliability and secrecy separately, thus constituting a useful tool in the context of new scenarios with stringent requirements on reliability as the case of ultra-reliable low-latency communication. Our system considers a multi-antenna transmitter, Alice, that employs transmit antenna selection, a legitimate multi-antenna receiver, Bob, and a multi-antenna eavesdropper, Eve, where both employing maximal-ratio combining. For this system, exact and simpler asymptotic closed-form expressions for the conditional outage probability are provided. Moreover, for the case where channel state information is available at the three nodes, a numerical secure throughput maximization is carried out by considering quality-of-service and security constraints for an adaptive rate allocation scheme in an ON-OFF transmission. Our proposed closed-form expressions are validated via Monte Carlo simulations.**

I. Introduction

The evolution of wireless technology has revolutionized the communications industry. Wireless networks have become a vital part of our lives due to its impact in the most diverse fields. However, an inherent problem with wireless networks is information security and privacy, as wireless networks are more vulnerable to eavesdropping and denial of service (DoS) attacks, such as jamming and spoofing, when compared to a wired network, due to the broadcast nature of the wireless medium [1],

Currently, cryptographic techniques are used for security purposes, which are implemented at upper layers of the communication system by assuming eavesdropper's limited computational capabilities. Therefore, the use of lightweight cryptography along with physical-layer (PHY) security is a promising way to achieve security against any level of computational power. It is worthwhile to mention that PHY security has a pivotal role for the 5th generation of mobile wireless networks (5G) and beyond, specially for the deployment of the so-called machine-type communications (MTCs), which are intended to connect a massive number of devices with limited, low-complexity hardware resources, and severe energy constraints. Thus, providing security represents a big challenge in such a scenario [2].

In [3], Wyner introduced the wiretap channel, where it was established that secret messages can be transmitted if the eavesdropping channel is a degraded version of the legitimate channel. From Wyners remarkable studies, physical layer security has re-surged as a promising solution against eavesdropping in wireless networks, thus being extensively studied in the last decade.

In Wyner's encoding scheme, two rates are chosen by the encoder, i.e., the rate of transmitted codewords R_b, and the rate of secrecy information R_s. The capacity for the legitimate link and the eavesdropper link is given by $C_b = \log_2[1+\gamma_B]$, and $C_e = \log_2[1+\gamma_E]$, Then, $R_e = R_b - R_s$ is defined as the rate of securing the transmission against eavesdropping. Hence, Bob will correctly decode the information if $C_b > R_b$; however, it will be impossible to achieve perfect secrecy if $C_e > R_e$. As a consequence of this theory, multi-antenna diversity [4], [5], and cooperative diversity [6] have been widely studied as useful techniques to strengthen the security at the physical layer, as they can provide an enhancement of the legitimate channel over the eavesdropping channel. Particularly, the multiple-input multiple-output and multiple eavesdropper (MIMOME) scenario has been extensively investigated. In [7], the author characterized secrecy outage probability for MIMOME setup considering full channel state information (CSI) at transmitter for both main and eavesdropper channels, Also in [8] the impact of transmit antenna selection (TAS) for massive MIMO while assuming no knowledge about Eve CSI at transmitter has been analyzed. However, those works consider the classical metric of the secrecy outage probability given in [9] to evaluate the secrecy performance. Nonetheless, this formulation fails to capture the system's security level alone, because it is not possible to distinguish between reliability or secrecy outage failure. Therefore in [10], an alternative formulation is presented, conditioned upon a message actually being transmitted as a conditional probability. The new formulation provides a more thorough measure of the system's security, once it is possible to isolate security outage from transmission outage.

Inspired on [5], [10], this paper contributes on the analysis of systems with security constraints for a MIMOME scenario, by considering the new secrecy outage formulation in [10], For that purpose, we consider a three-node network, where

all nodes are multi-antenna devices and can estimate their individual CSI. In this system, the legitimate transmitter, Alice, implements TAS, while the legitimate receiver, Bob, and the eavesdropper, Eve, implement maximal-ratio combining (MRC). Under these considerations, our contributions are the following:

- Exact closed-form and simpler asymptotic closed-form expressions for the secrecy outage probability, are provided for the proposed scenario, conditioned upon a message actually being transmitted. As byproducts, closed-form expressions for the scenarios Multiple-Input Multiple-Output and Single antenna Eavesdropper (MIMOSE), Multiple-Input Single-Output and Multi-antenna Eavesdropper (MISOME), and Multiple-Input Single-Output and Single antenna Eavesdropper (MISOSE) are also provided.
- The design problem of maximizing the throughput is tackled by considering both quality-of-service (QoS) and security constraints, for an adaptive rate allocation scheme in an ON-OFF transmission.

Notation: Hereafter we denote scalar variables by italic symbols, while vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively. Given a complex vector $\mathbf{x}$, $||\mathbf{x}||$ denotes the Euclidean norm,while $(\mathbf{x})^T$ and $(\mathbf{x})^\dagger$ denote transpose and conjugate transpose operations, respectively. The $m \times m$ identity matrix is represented as $\mathbf{I}_m$. Probability density function (PDF) and cumulative distribution function (CDF) of a given random variable X are denoted as $f_X(x)$ and $F_X(x)$, respectively, while the expectation operator is denoted as $\mathbb{E}[\cdot]$. The Gamma function is denoted as $\Gamma(z)$ [11, 6, 6.1.1], while the regularized lower incomplete gamma function is denoted as $\mathrm{P}(s,z) = \frac{\gamma(s,z)}{\Gamma(z)}$ [11, 6, 6.5.1] and the regularized upper incomplete gamma function is represented as $\mathrm{Q}(s,z) = \frac{\Gamma(s,z)}{\Gamma(z)}$ [11, 26.4.19]. The Gauss hypergeometric function is denoted as ${}_2\mathrm{F}_1(a,b;c;z)$ [11, 15,15.1.1], while the inverse of the generalized regularized incomplete gamma function is represented as $\mathrm{P}^{-1}(s,z)$ [12].

II. System model

We consider a wiretap channel scenario, as depicted in Fig. 1, where a legitimate pair, Alice and Bob, communicate in the presence of an eavesdropper, Eve. In this system, all nodes are multi-antenna devices, thus N_A, N_B, and N_E are the number of antennas at Alice, Bob, and Eve, respectively. Herein, Bob and Eve are assumed to know their individual CSI perfectly, and both Bob and Alice share an open and error-free feedback channel, which is utilized to carry Alice's antenna index with the best SNR at Bob and to feedback Bob's instantaneous CSI to Alice in order to allow ON-OFF transmission. Also, it is assumed that Eve can obtain this feedback or the antenna index; however, Eve is not able to exploit such information and, therefore, it has no diversity gain. As legitimate and eavesdropper channels are not correlated, Eve is unable to manipulate diversity from Alice's antennas. All channels in this system undergo Rayleigh fading, thus h_{ij}, with $i \in \{1....N_A\}$ and $j \in \{1...N_X\}$, with $X \in \{B, E\}$, are the respective channel coefficients. Then, Alice is able to implement TAS according to the index received from Bob, which is given by

$$i^* = \arg \max_{1 \leqslant i \leqslant N_A} ||\mathbf{h}_{iB}||, \tag{1}$$

where $\mathbf{h}_{i_B} = [h_{i1}, h_{i2}, \cdots, h_{iN_B}]^T$ is the $N_B \times 1$ legitimate channel vector between the ith transmit antenna at Alice and the N_B antennas at Bob. Then, the message is encoded by Alice into a codeword $x = [x(1), x(2), \cdots, x(n))]$, using Wyner codes [13], while the transmitted codeword is assumed to be limited to an average power constraint, that is $\frac{1}{n}\sum_{j=1}^{n} \mathbb{E}\left[|x(j)|^2\right] \leqslant P_A$, where P_A is the transmit power at Alice. In turn, Bob uses MRC to combine the signals received at the N_B antennas, thus resulting in the following received signal at Bob

$$y_B = \mathbf{h}_{i_B}^\dagger \mathbf{h}_{i_B} x + \mathbf{h}_{i_B}^\dagger \mathbf{n}_{i_B}, \tag{2}$$

where $\mathbf{n}_{i_B}$ is the $N_B \times 1$ additive white Gaussian noise vector at Bob, and it is assumed that $\mathbb{E}\left[\mathbf{n}_{i_B}\mathbf{n}_{i_B}^\dagger\right] = \mathbf{I}_{i_B}\sigma_B^2$, with σ_B^2 being the noise variance at each antenna, Thus, the instantaneous SNR of the legitimate link is given by

$$\gamma_B = \frac{||\mathbf{h}_{i_B}||^2 P_A}{\sigma_B^2}, \tag{3}$$

and the corresponding PDF and CDF of which are given, respectively, by [14]

$$f_{\gamma_B}(\gamma) = \frac{N_A\ \gamma^{N_B-1}}{\Gamma(N_B)\ \overline{\gamma}_B^{N_B}} \exp\left(-\frac{\gamma}{\overline{\gamma}_B}\right) \mathrm{P}\left(N_B\,,\, \frac{\gamma}{\overline{\gamma}_B}\right)^{N_A-1}, \tag{4}$$

$$F_{\gamma_B}(\gamma) = \mathrm{P}\left(N_B\,,\, \frac{\gamma}{\overline{\gamma}_B}\right)^{N_A}. \tag{5}$$

On the other hand, Eve perceives a random TAS scheme, as the legitimate channel and the eavesdropper channel are uncorrelated. As a result, the eavesdropped signal vector using MRC is

$$y_E = \mathbf{h}_{i_E}^\dagger \mathbf{h}_{i_E} x + \mathbf{h}_{i_E}^\dagger \mathbf{n}_{i_E}, \tag{6}$$

where $\mathbf{h}_{iE}$ is the $N_E \times 1$ eavesdropper channel vector and $\mathbf{n}_{i_E}$ is the $N_E \times 1$ additive white Gaussian noise vector at Eve. We assume $\mathbb{E}\left[\mathbf{n}_{i_E}\mathbf{n}_{i_E}^\dagger\right] = \mathbf{I}_{i_E}\sigma_E^2$, with σ_E^2 being the noise variance at each antenna. Thus, the instantaneous SNR of the eavesdropper link is given by

$$\gamma_E = \frac{||\mathbf{h}_{i_E}||^2 P_A}{\sigma_E^2}, \tag{7}$$

which follows a Gamma distribution, the PDF and CDF of which are given, respectively, by [14]

$$f_{\gamma_E}(\gamma) = \frac{\gamma^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(-\frac{\gamma}{\overline{\gamma}_E}\right), \tag{8}$$

$$F_{\gamma_E}(\gamma) = \mathrm{P}\left(N_E\,,\, \frac{\gamma}{\overline{\gamma}_E}\right). \tag{9}$$

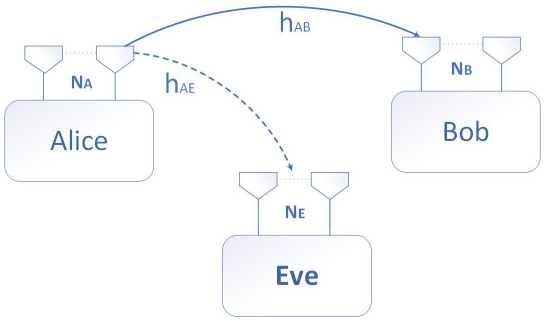

Fig. 1. Illustrative example of network deployment: Alice utilizes TAS while Bob and Eve employ MRC, But only Bob can make use of diversity from Alice's antennas. Herein, h_{AB} and h_{AE} are the channel coefficient's of legitimate and wiretap channels, The number of antennas at Alice, Bob and Eve are represented by N_A, N_B, and N_E respectively.

III. Secrecy Outage and Secure Throughput Analysis

In this section, we define and derive an expression of the secrecy outage probability for the system under study according to the formulation presented in [10], which permits to assess secrecy given that a message was actually transmitted. the probability of successful transmissions for this system is defined as the probability of γ_B being higher than a given threshold μ

$$p_s(\mu) = \Pr\left[C_b > R_b\right] = \Pr\left[\gamma_B > \mu\right] = 1 - F_{\gamma_B}(\mu) \quad (10)$$

where $F_{\gamma_B}(\cdot)$ is given as in (5) and $\mu \geqslant 2^{R_s} - 1$, since according to an ON-OFF transmission, a transmission only occurs when $C_b > R_s$. Regarding security, we resort to the secrecy outage probability metric introduced in [10], which is conditioned at a successful transmission at the legitimate channel. The secrecy outage probability can be expressed as

$$\begin{aligned} p_{(\mu,R_s)} &= \Pr\left[C_e > C_b - R_s | \gamma_B > \mu\right], \\ &\overset{(a)}{=} \frac{\Pr\left[\mu < \gamma_B < 2^{R_s}(1+\gamma_E) - 1\right]}{p_s(\mu)} \\ &\overset{(b)}{=} \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \frac{F_{\gamma_B}\left(2^{R_s}(1+\gamma_E)-1\right) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E}{1 - F_{\gamma_B}(\mu)} \\ &\quad - \frac{\left(1 - F_{\gamma_E}\left(\frac{(1+\mu)}{2^{R_s}} - 1\right)\right) F_{\gamma_B}(\mu)}{1 - F_{\gamma_B}(\mu)}, \end{aligned} \quad (11)$$

where step (a) comes from [10, Eq. (7)] and step (b) holds when assuming independent random variables. In the following, an expression for the secrecy outage probability is derived (11) for the proposed scenario

Theorem 1. *The secrecy outage probability for the MIMOME wiretap channel, where Alice employs TAS while Bob and Eve perform MRC, is given by* (12) *at the top of the next page.*

Proof. See Appendix A □

We are aware that Theorem 1 is quite intricate. Therefore, we provide simpler and easy to evaluate closed-from expression for the all variations of the MIMOME setting with respect to the number of antennas at each node.

Corollary 1. *The secrecy outage probability of the MIMOSE wiretap channel where Alice and Bob are both multiple-antenna devices, But Eve is a single-antenna, with Alice employing TAS and Bob resorting to MRC is given by*

$$\begin{aligned} p_{(\mu,R_S)} = &\sum_{k=0}^{N_A} \left[\binom{N_A}{K} \frac{(-1)^K}{p_s(\mu)} \exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right) \right. \\ &\times \frac{1}{\overline{\gamma}_E} \sum_{s_0+s_1+..s_{N_B-1}=K} \binom{K}{s_0, s_1, .., s_{N_B-1}} \\ &\times \left(\prod_{t=0}^{N_B-1} \left(\frac{1}{t!}\right)^{s_t}\right) \sum_{p=0}^{\alpha} \binom{\alpha}{p} \left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^{\alpha-p} \\ &\times \left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{p} \left(\frac{\overline{\gamma}_B\overline{\gamma}_E}{k2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B}\right)^{p+1} \\ &\times \Gamma\left[(p+1), \left(\frac{k2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B}{\overline{\gamma}_B\overline{\gamma}_E}\right)\left(\frac{\mu+1-2^{R_s}}{-2^{R_s}\overline{\gamma}_E}\right)\right] \Bigg] \\ &- \left[\frac{1}{p_s(\mu)} \exp\left(\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right) P\left(N_B, \frac{\mu}{\overline{\gamma}_B}\right)^{N_A}\right] \end{aligned} \quad (13)$$

Corollary 2. *The secrecy outage probability for the MISOME scenario, where Bob is a single-antenna device, and only the source for spatial diversity in the legitimate link comes from Alice's antennas by employing TAS, while Eve performing MRC is given by*

$$\begin{aligned} p_{(\mu,R_S)} = &\sum_{K=0}^{N_A} \left[\binom{N_A}{K} \frac{(-1)^K}{p_s(\mu)} \exp\left(-K\frac{2^{R_s}-1}{\overline{\gamma}_B}\right) \left(\frac{\overline{\gamma}_B}{\overline{\gamma}_B + K2^{R_s}\overline{\gamma}_E}\right)^{N_E} \right. \\ &\left. \times \mathrm{Q}\left(N_E, -\frac{\left(\overline{\gamma}_B + K2^{R_s}\overline{\gamma}_E\right)\left(2^{R_s}-1-\mu\right)}{2^{R_s}\overline{\gamma}_B\overline{\gamma}_E}\right) \right] - \\ &\frac{1}{1-\left(1-\exp\left(-\frac{\mu}{\overline{\gamma}_B}\right)\right)^{N_A}} \left[\left(1-\exp\left(-\frac{\mu}{\overline{\gamma}_B}\right)\right)^{N_A} \mathrm{Q}\left(N_E, -\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right)\right]. \end{aligned} \quad (14)$$

Corollary 3. *The secrecy outage probability for the MISOSE wiretap channel, where only Alice is a multiple-antenna device and performing TAS, is given by*

$$\begin{aligned} p_{(\mu,R_S)} = &\exp\left(\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right) \left[{}_2\mathrm{F}_1\left(-N_A, \frac{\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E}, 1 + \frac{\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E}, e^{-\frac{\mu}{\overline{\gamma}_B}}\right) \right. \\ &\left. - \left(1-\exp\left(-\frac{\mu}{\overline{\gamma}_B}\right)\right)^{N_A} \right] \left[\frac{1}{1-\left(1-\exp\left(-\frac{\mu}{\overline{\gamma}_B}\right)\right)^{N_A}}\right]. \end{aligned} \quad (15)$$

IV. Asymptotic Analysis

We perform the asymptotic analysis by considering the average SNR of legitimate link $\overline{\gamma}_B \to \infty$. In addition, by using the series expansion of regularized lower incomplete gamma function, and truncating the expansion to first term

$$p_{(\mu,R_S)} = \sum_{K=0}^{N_A}\left[\binom{N_A}{K}\frac{(-1)^K}{p_s(\mu)}\frac{1}{\Gamma(N_E)\overline{\gamma}_E^{N_E}}\exp\left(-K\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)\sum_{s_0+s_1+\ldots+s_{N_b-1}=K}\binom{K}{s_0,s_1,\ldots,s_{N_b-1}}\left(\prod_{t=0}^{N_b-1}\left(\frac{1}{t!}\right)^{s_t}\right)\right.$$
$$\left.\times\sum_{p=0}^{\alpha}\binom{\alpha}{p}\left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^{\alpha-p}\left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{p}\left(\frac{\overline{\gamma}_B\overline{\gamma}_E}{K2^{R_s}\overline{\gamma}_E+\overline{\gamma}_B}\right)^{p+N_E}\Gamma\left[(p+N_E),-\frac{\left(\overline{\gamma}_B+K2^{R_s}\overline{\gamma}_E\right)\left(2^{R_s}-1-\mu\right)}{2^{R_s}\overline{\gamma}_B\overline{\gamma}_E}\right]\right]$$
$$-\left[\frac{1}{p_s(\mu)}\,\mathrm{P}\left(N_B,\frac{\mu}{\overline{\gamma}_B}\right)^{N_A}\mathrm{Q}\left(N_E,-\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right)\right]. \tag{12}$$

as remaining terms has no huge impact, so the CDF of the Gamma distribution results as

$$\mathrm{P}\left(N_B\,,\,\frac{\gamma}{\overline{\gamma}_B}\right)^{N_A} \simeq \left(\frac{\gamma^{N_B}}{\overline{\gamma}_B^{N_B}N_B\Gamma(N_B)}\right)^{N_A} \tag{16}$$

By using (16) in (11), we obtained a simpler asymptotic closed form expression for MIMOME scenario in (17).

$$p_{(\mu,R_S)} = \left(\frac{\gamma^{N_B}}{\overline{\gamma}_B^{N_B}N_B\Gamma(N_B)}\right)^{N_A}\left\{\frac{1}{\Gamma(N_E)}\left(\sum_{p=0}^{N_AN_B}\right.\right.$$
$$\times\binom{N_AN_B}{p}\left(2^{R_S}-1\right)^{N_AN_B-p}\left(2^{R_S}\right)^{p}\left(\overline{\gamma}_E\right)^{p}$$
$$\left.\times\Gamma\left[(p+N_E),-\frac{\left(2^{R_s}-1-\mu\right)}{2^{R_s}\overline{\gamma}_E}\right]\right)-\left[\left(\mu^{N_AN_B}\right)\right.$$
$$\left.\left.\mathrm{Q}\left(N_E,-\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right)\right]\right\} \tag{17}$$

This is a much simpler expression for proposed scheme comparing to complicated expression in (12), and it helps the system designer to perform analysis easily.

To maximize the performance of the legitimate link, we perform throughput maximization by considering the quality of service constraints (QoS) and security constraint for adaptive rate allocation in form of an ON-OFF transmission mechanism as we shall see next.

V. Adaptive Rate Allocation and Throughput Maximization

Here, we consider an adaptive encoder that adapts the rate of the transmitted codewords, R_b, to an arbitrary value close to C_b according to the instantaneous CSI of the legitimate channel, we determine the values of μ and R_s that maximize the throughput, which is given by $T = p_{tx}(\mu)R_S$, given a QoS constraint $\sigma \in [0,1]$, and security constraint $\epsilon \in [0,1]$. Therefore, the design problem is given by

$$\begin{aligned}&\arg\max_{Rs,\mu} \quad p_{tx}(\mu)Rs,\\ &\text{s.t.} \qquad p_{so}(Rs,\mu)\leqslant\epsilon, p_{tx}(\mu)\geqslant\sigma, \mu \ \geqslant 2^{R_s}-1, R_s>0,\end{aligned}$$

We solve this problem by numerically computing the optimal value of μ for any given value of R_s. Then, from (10), we can determine the feasible range of μ that satisfies $p_{tx}(\mu)\geqslant\sigma$ as

$$\mu \in \left[2^{R_s}-1, \overline{\gamma}_B\,\mathrm{P}^{-1}\left(N_B,(1-\sigma)^{\frac{1}{N_A}}\right)\right]$$

Under these conditions, the optimization problem can be formulated as

$$\begin{aligned}&\arg\max_{Rs,\mu} \quad (1-F_{\gamma_B}(\mu))\,Rs,\\ &\text{s.t.} \qquad R_s>0, \mu \ \leqslant \overline{\gamma}_B\,\mathrm{P}^{-1}\left(N_B,(1-\sigma)^{\frac{1}{N_A}}\right),\end{aligned}$$

Due to the complexity of this optimization problem, a closed-form solution cannot be obtained, however it can be solved numerically using a computer software such as Matlab.

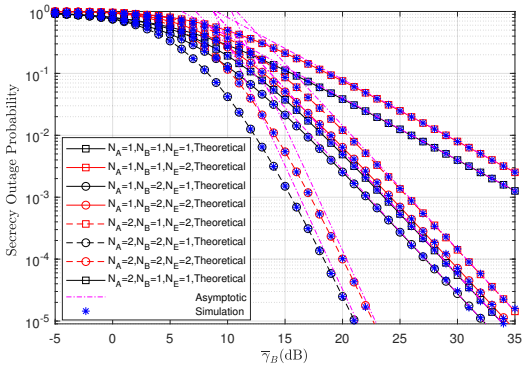

Fig. 2. New Secrecy outage probability as a function of average SNR at Bob for different number of antennas at Alice, Bob and Eve, for R_S=2 bits/s/Hz and $\overline{\gamma}_E$= 0 dB

VI. Numerical Analysis

In this section, our analytical results are validated via Monte Carlo simulations by evaluating some illustrative cases.

Fig. 2 shows the secrecy outage probability as a function of the average SNR at Bob $\overline{\gamma}_B$, for a fixed secrecy rate $R_S = 2$ bits/s/Hz, $\overline{\gamma}_E$= 0 dB, and different configurations of the number of antennas at each node. The threshold for on-off SNR is set to its minimum value of $\mu = 2^{R_s}-1$. First, notice that the simulations perfectly match with our analytical results, thus corroborating the correctness of our expressions. Note also that while an increase in N_A or N_B causes a significant decrease in the secrecy outage probability, an increase in N_E deteriorates in a lesser degree the secrecy performance of the system. This can be explained due to

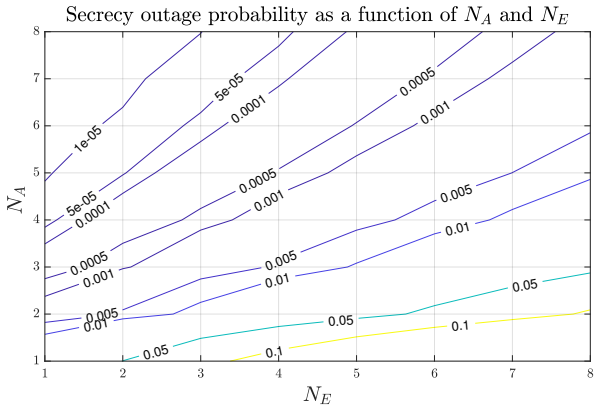

Fig. 3. Secrecy outage probability as a function of N_A and N_E for MIMOME case, $N_B = 2$, R_s= 2 bits/s/Hz, $\overline{\gamma}_B$= 15 dB, and $\overline{\gamma}_E$= 0 dB

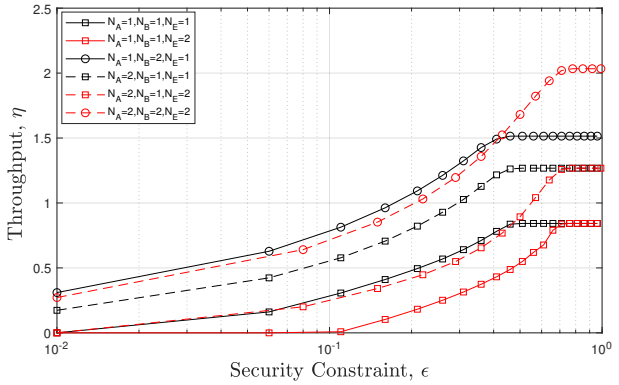

Fig. 5. Throughput of secure transmission as a function of security constraint for fixed QoS constraint $\sigma = 0.5$, $\overline{\gamma}_B$= 5 dB, and $\overline{\gamma}_E$= 0 dB

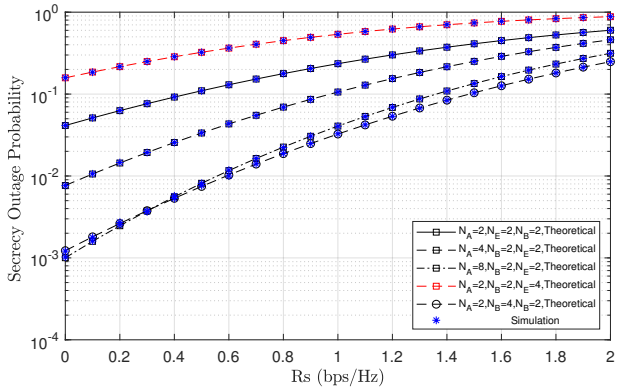

Fig. 4. New Secrecy outage formulation for MIMOME as a function of confidential rate R_S for different configurations of antennas, $\overline{\gamma}_B$= 5 dB, and $\overline{\gamma}_E$= 0 dB

the TAS technique, which prevents the eavesdropper from exploiting diversity from Alice. In addition, it can be observed that the cases of the higher number of antennas at Bob attain better performance than those of higher number of antennas at Alice. Thus, for the cases of $N_A > N_B$, it is required at least 2 dB to attain the same secrecy performance. However, the cases of $N_A = N_B$ achieve a significantly improved secrecy performance. It can also be observed that the obtained simpler asymptotic expression matches with simulated curves at high SNR, which validates the correctness of expression and corroborating the diversity order of $N_A N_B$. Moreover, notice that for the SISOSE case (12), (13), (14), and (15) reduces to the expression found in [10]. The contour plot in Fig. 3 shows the secrecy outage probability as a function of N_A and N_E. For $N_B = 2$, average SNR at Bob $\overline{\gamma}_B$ = 15 dB , and $\overline{\gamma}_E$ = 0 dB, it is observed that by increasing the average SNR between legitimate and eavesdropper channel, it is possible to achieve much lower secrecy outage probability, less than 0.1%, even if Eve has several antennas. Therefore we conclude that increasing the power ratio between legitimate and Eve's channel plays a crucial role in the performance of the network.

In Fig. 4, for an eavesdropper channel with average SNR $\overline{\gamma}_E = 0$ dB, a legitimate channel with average SNR $\overline{\gamma}_B$ of 5dB, an on-off SNR threshold $\mu = 2^{R_s} - 1$, and a particular value of secrecy outage probability, secrecy gains from 3.5 to 4.5 times can be achieved by increasing N_A or using a stronger legitimate channel of the MIMOME scenario. Also, the same level of secrecy outage probability can be observed for the cases of N_A = 8, N_B = 2, N_E = 2, and N_A = 2, N_B = 4, N_E = 2. Thus for a large number of antennas, the gain on having more antennas in Bob than Alice is significant.

In Fig. 5, the achievable throughput for the adaptive encoder design is presented as a function of the security constraint ϵ, for $N_A \in \{1, 2\}$, $N_B \in \{1, 2\}$, and $N_E \in \{1, 2\}$. We set the QoS constraint or reliability indicator to σ = 0.5, $\overline{\gamma}_B$ = 5 dB , and at $\overline{\gamma}_E$ = 0 dB. It can be observed that the throughput is higher for the MIMOME scenario, while throughput decreases if Eve has more antennas than Alice and Bob. However, a higher number of antennas at Bob has significant gains to the system throughput. We observe that the case MISOME is better than the case SISOSE for a security constraint $\epsilon > 0.5$, otherwise they have the same throughput at lower security constraint on the MIMOME and SIMOSE scenarios.

VII. Conclusion

In this work, we considered a multiple-antenna wiretap channel, where the legitimate pair, Alice and Bob, communicate in the presence of an eavesdropper who attempts to breach the transmission originating from Alice. We consider the MIMOME scenario, where Alice performs TAS, while Bob and Eve employ MRC technique. Our model is inspired by the alternative secrecy outage formulation, which provides a more thorough measure of the system's security. The conventional secrecy outage formulation fails to differentiate between the system's security and reliability level. We derived exact and simpler asymptotic closed-form expressions for the secrecy outage probability for the aforementioned scenario, and the closed-form expressions for the scenarios MIMOSE, MISOME, and MISOSE were also obtained as byproducts. Additionally, to improve the performance of a legitimate link,

a throughput maximization was performed by considering an adaptive rate, according to Bob's received SNR, subject to QoS and security constraints. Simulation results show that the number of the antenna at Bob has a significant impact on security performance compared to Alice. Furthermore, for a higher average SNR at the legitimate link, greater security is possible even if Eve has multiple antennas.

ACKNOWLEDGMENT

This research has been financially supported by Academy of Finland 6Genesis Flagship (grant 318927), EE-IoT (grant 319008), and AKProf (grant 307492), the Brazilian National Council for Scientific and Technological Development (CNPq) Project No 428649/2016-5, and the São Paulo Research Foundation (FAPESP) Project No 2017/20990-6.

APPENDIX A
PROOF OF THEOREM 1

From (11), the secrecy outage probability can be expressed as the difference of two terms, as follows

$$p_{(\mu,R_S)_1} = I_1 - \Psi_1, \tag{18}$$

where

$$\begin{aligned}
I_1 &\overset{a}{=} \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} F_{\gamma_B}\left(2^{R_s}(1+\gamma_E)-1\right) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E \\
&\overset{(b)}{=} \sum_{K=0}^{N_A}\binom{N_A}{K}(-1)^K \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right) \\
&\times \sum_{s_0+s_1+s_2+..+s_{N_B-1}=K}\binom{K}{s_0,s_1,s_2,..,s_{N_B-1}}\prod_{t=0}^{N_B-1}\left(\frac{1}{t!}\right)^{s_t} \\
&\times \left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^{s_t t} f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E \\
&\overset{(c)}{=} \sum_{K=0}^{N_A}\binom{N_A}{K}(-1)^k \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right) \\
&\times \sum_{s_0+s_1+s_2+..+s_{N_B-1}=K}\binom{K}{s_0,s_1,s_2,..,s_{N_B-1}}\left(\prod_{t=0}^{N_B-1}\left(\frac{1}{t!}\right)^{s_t}\right) \\
&\times \prod_{t=0}^{N_B-1}\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^{s_t t} f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E \\
&\overset{(d}{=} \sum_{K=0}^{N_A}\binom{N_A}{K}(-1)^k \exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right) \\
&\times \sum_{s_0+s_1+..+s_{N_B-1}=K}\binom{K}{s_0,s_1,..,s_{N_B-1}}\left(\prod_{t=0}^{N_B-1}\left(\frac{1}{t!}\right)^{s_t}\right) \\
&\times \sum_{p=0}^{\alpha}\binom{\alpha}{p}\left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^{\alpha-p}\left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{p}\frac{1}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}}\int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty}(\gamma_E)^p \\
&\times \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B}\right)\gamma_E^{N_E-1}\exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right)\mathrm{d}\gamma_E
\end{aligned} \tag{19}$$

Note that in step (b) we have applied the binomial theorem, and then we have applied the multinomial theorem, Next, after some simplifications, in step (c) we used this property $\prod_{j=0}^{J} x_j y_j = \prod_{j=0}^{J} x_j \prod_{j=0}^{J} y_j$ and $\prod_{t=0}^{N_B-1}(X)^{s_t t} = X^{s_0 0}.X^{s_1 1}.X^{s_2 2}...X^{s_{N_B-1}N_B-1} = (X)^{\sum s_t t}$, thus let $\sum s_t t = \alpha$. In step (d) we have applied the binomial expansion to $\left(\left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)+\left(\frac{2^{R_s}\gamma_E}{\overline{\gamma}_B}\right)\right)^{\alpha}$ and used (8). Next, the integral in (19) is solved as follows

$$\begin{aligned}
I_2 &= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B}\right)(\gamma_E)^{p+N_E-1}\exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right)\mathrm{d}\gamma_E \\
&= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{\gamma_E\left(K2^{R_s}\overline{\gamma}_E+\overline{\gamma}_B\right)}{\overline{\gamma}_B\overline{\gamma}_E}\right)(\gamma_E)^{p+N_E-1}\mathrm{d}\gamma_E \\
&= (\Phi)^{-p-N_E}\Gamma\left[(p+N_E)\ ,\ (\Phi)\left(\frac{\mu+1-2^{R_s}}{2^{R_s}}\right)\right]
\end{aligned} \tag{20}$$

where $\Phi = \frac{\overline{\gamma}_B\overline{\gamma}_E}{K2^{R_s}\overline{\gamma}_E+\overline{\gamma}_B}$.

$$\Psi_1 = \frac{1}{p_s(\mu)}Q\left(N_E, -\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right)P\left(N_B, \frac{\mu}{\overline{\gamma}_B}\right)^{N_A}. \tag{21}$$

By substituting (20) into (19), and putting (19), (10) and (21) into (11), we attain the secrecy outage probability of the MIMOME wiretap channel in closed form as in (12), thus concluding the proof.

REFERENCES

[1] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344 – 1371, 2013.

[2] Y.-F. Huang and H. H. Chen, "Physical layer architectures for machine type communication networks-a survey," *Wireless Communications and Mobile Computing*, vol. 16, no. 18, pp. 3269–3294, 2016.

[3] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355 –1387, 1975.

[4] H. Alves, R. Souza, and M. Debbah, "Enhanced physical layer security through transmit antenna selection," in *IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 879–883.

[5] H. Alves, R. 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.

[6] H. Alves, G. Brante, R. Souza, D. da Costa, and M. Latva-aho, "On the performance of secure full-duplex relaying under composite fading channels," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 867–870, Jul. 2015.

[7] A. S. Guerreiro, G. Fraidenraich, and R. D. Souza, "On the ergodic secrecy capacity and secrecy outage probability of the mimome rayleigh wiretap channel," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 1, p. e2924, 2017.

[8] S. Asaad, A. Bereyhi, A. M. Rabiei, R. R. Müller, and R. F. Schaefer, "Optimal transmit antenna selection for massive mimo wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 817–828, April 2018.

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

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

[11] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. Dover, 1965.

[12] Wolfram|Alpha, access October 23, 2018. [Online]. Available: http://functions.wolfram.com/GammaBetaErf/InverseGammaRegularized3/

[13] X. Tang, R. Liu, P. Spasojević, 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.

[14] H. Alves, M. D. CastroTomé, P. H. J. Nardelli, C. H. M. D. Lima, and M. Latva-Aho, "Enhanced transmit antenna selection scheme for secure throughput maximization without CSI at the transmitter," *IEEE Access*, vol. 4, pp. 4861–4873, 2016.