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

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 Wyner’s remarkable studies, physical layer security has re-surfaced 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 \( R_e \). 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 (MISOE) 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 \( x \), \( ||x|| \) denotes the Euclidean norm, while \( (x)^T \) and \( (x)\) denote transpose and conjugate transpose operations, respectively. The \( m \times n \) identity matrix is represented as \( I_n \). 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 \( E[\cdot] \). The Gamma function is denoted as \( \Gamma(x) \) [11, 6.1.1], while the regularized lower incomplete gamma function is denoted as \( P(s, z) = \frac{\gamma(s, z)}{\Gamma(s)} \) [11, 6.5.1] and the regularized upper incomplete gamma function is represented as \( Q(s, z) = \frac{\Gamma(z)}{\Gamma(s)} \) [11, 6.5.11]. The Gauss hypergeometric function is denoted as \( _2F_1(a, b; c; z) \) [11, 15.15.1.1], while the inverse of the generalized regularized incomplete gamma function is represented as \( P^{-1}(s, z) \) [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

\[
i^* = \text{arg} \max_{i \in N_A} ||h_{IB}||,
\]

where \( h_{ib} = [h_{i1}, h_{i2}, \ldots, h_{iN_B}]^T \) is the \( N_B \times 1 \) legitimate channel vector between the \( i \)th transmit antenna at Alice and the \( N_B \) antennas at Bob. Then, the message is encoded by Alice into a codeword \( x = [x(1), x(2), \ldots, x(n)] \), using Wyner codes [13], while the transmitted codeword is assumed to be limited to an average power constraint, that is

\[
\frac{1}{N_A} \sum_{j=1}^N ||x(j)||^2 \leq P_A,
\]

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

\[
y_B = h_{1b}^T h_{ib} x + h_{1b}^T n_{ib},
\]

where \( n_{ib} \) is the \( N_B \times 1 \) additive white Gaussian noise vector at Bob, and it is assumed that \( E[n_{ib} h_{ib}^T] = I_B \sigma_B^2 \), with \( \sigma_B^2 \) being the noise variance at each antenna. Thus, the instantaneous SNR of the legitimate link is given by

\[
\gamma_B = \frac{||h_{ib}||^2 P_A}{\sigma_B^2},
\]

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

\[
F_{\gamma_B}(\gamma) = \frac{N_A}{\Gamma(N_B)} \gamma_B^{N_A-1} \exp\left(-\frac{\gamma}{\gamma_B}\right) P\left(N_B, \frac{\gamma}{\gamma_B}\right)^{N_A-1},
\]

\[
F_{\gamma_B}(\gamma) = \frac{N_B}{\Gamma(N_B)} \left(\frac{\gamma}{\gamma_B}\right)^{N_A}.
\]

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

\[
y_E = h_{1e}^T h_{iei} x + h_{1e}^T n_{ixe},
\]

where \( h_{ie} \) is the \( N_E \times 1 \) eavesdropper channel vector and \( n_{ie} \) is the \( N_E \times 1 \) additive white Gaussian noise vector at Eve. We assume \( E[n_{ie} h_{ie}^T] = I_E \sigma_E^2 \), with \( \sigma_E^2 \) being the noise variance at each antenna. Thus, the instantaneous SNR of the eavesdropper link is given by

\[
\gamma_E = \frac{||h_{ie}||^2 P_A}{\sigma_E^2},
\]

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

\[
F_{\gamma_E}(\gamma) = \frac{\gamma^{N_E-1}}{\Gamma(N_E)} \gamma_E^{N_E} \exp\left(-\frac{\gamma}{\gamma_E}\right),
\]

\[
F_{\gamma_E}(\gamma) = \frac{N_E}{\Gamma(N_E)} \left(\frac{\gamma}{\gamma_E}\right)^{N_E}.
\]
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 $\gamma_B$ being higher than a given threshold $\mu$.

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

where $F_{\gamma_B}(\cdot)$ is given as in (5) and $\mu \geq 2^{R_b} - 1$, since according to an ON-OFF transmission, a transmission only occurs when $C_b > R_b$. 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

$$p_s(\mu) = \Pr[C_e > C_b - R_b | \gamma_B > \mu] = (a) \Pr[\gamma_B < 2^{R_b}(1 + \gamma_E) - 1]$$

$$= \sum_{K=0}^{N_A} \left( \frac{(N_A)}{K} \right) \frac{(-1)^K}{p_s(\mu)} \exp \left( -K(2^{R_b} - 1) \frac{\gamma_E}{\gamma_B} \right) \frac{1}{\gamma_B^{K+1}}$$

$$\times \left( \prod_{t=0}^{K-1} \left( \frac{\gamma_E}{\gamma_B} \right) \right) \sum_{p=0}^{\alpha} \left( \frac{\alpha}{p} \right) \left( \frac{2^{R_b} - 1}{\gamma_B} \right)^{p+1}$$

$$\times \Gamma \left( (p+1), \left( \frac{k2^{R_b} \gamma_E}{\gamma_B} \right) \right) \exp \left( 2^{R_b} - 1 - \mu \right) P \left( N_B, \frac{\mu}{\gamma_B} \right)$$

$$= 1 - \exp \left( -\mu \frac{2^{R_b} - 1 - \mu}{\gamma_B} \right) P \left( N_B, \frac{\mu}{\gamma_B} \right)$$  \hspace{1cm} (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, 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 MIMOME wiretap channel where Alice and Bob are both multiple-antenna devices, But Eve is a single-antenna device, with Alice employing TAS and Bob resorting to MRC is given by

$$p_{(\mu,R_s)} = \sum_{k=0}^{N_A} \left( \frac{(N_A)}{K} \right) \frac{(-1)^K}{p_s(\mu)} \exp \left( -K(2^{R_b} - 1) \frac{\gamma_E}{\gamma_B} \right) \frac{1}{\gamma_B^{K+1}}$$

$$\times \left( \prod_{t=0}^{K-1} \left( \frac{\gamma_E}{\gamma_B} \right) \right) \sum_{p=0}^{\alpha} \left( \frac{\alpha}{p} \right) \left( \frac{2^{R_b} - 1}{\gamma_B} \right)^{p+1}$$

$$\times \Gamma \left( (p+1), \left( \frac{k2^{R_b} \gamma_E}{\gamma_B} \right) \right) \exp \left( 2^{R_b} - 1 - \mu \right) P \left( N_B, \frac{\mu}{\gamma_B} \right)$$

$$= 1 - \exp \left( -\mu \frac{2^{R_b} - 1 - \mu}{\gamma_B} \right) P \left( N_B, \frac{\mu}{\gamma_B} \right)$$  \hspace{1cm} (13)

**Corollary 2.** The secrecy outage probability for the MISO-ME 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

$$p_{(\mu,R_s)} = \sum_{K=0}^{N_A} \left( \frac{(N_A)}{K} \right) \frac{(-1)^K}{p_s(\mu)} \exp \left( -K(2^{R_b} - 1) \frac{\gamma_E}{\gamma_B} \right) \frac{1}{\gamma_B^{K+1}}$$

$$\times \left( \prod_{t=0}^{K-1} \left( \frac{\gamma_E}{\gamma_B} \right) \right) \sum_{p=0}^{\alpha} \left( \frac{\alpha}{p} \right) \left( \frac{2^{R_b} - 1}{\gamma_B} \right)^{p+1}$$

$$\times \Gamma \left( (p+1), \left( \frac{k2^{R_b} \gamma_E}{\gamma_B} \right) \right) \exp \left( 2^{R_b} - 1 - \mu \right) P \left( N_B, \frac{\mu}{\gamma_B} \right)$$

$$= 1 - \exp \left( -\mu \frac{2^{R_b} - 1 - \mu}{\gamma_B} \right) P \left( N_B, \frac{\mu}{\gamma_B} \right)$$  \hspace{1cm} (14)

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

$$p_{(\mu,R_s)} = \exp \left( -\mu \frac{2^{R_b} - 1 - \mu}{\gamma_B} \right) P \left( N_A, \frac{\gamma_B}{2^{R_b} \gamma_E} e^{2^{R_b} - 1} \right)$$

$$- \left( 1 - \exp \left( -\mu \frac{2^{R_b} - 1 - \mu}{\gamma_B} \right) \right) P \left( N_A, \frac{\gamma_B}{2^{R_b} \gamma_E} e^{2^{R_b} - 1} \right)$$  \hspace{1cm} (15)

IV. ASYMPTOTIC ANALYSIS

We perform the asymptotic analysis by considering the average SNR of legitimate link $\gamma_B \rightarrow \infty$. In addition, by using the series expansion of regularized lower incomplete gamma function, and truncating the expansion to first term.
As remaining terms has no huge impact, so the CDF of the Gamma distribution results as

\[
P(N_B, \frac{\gamma}{\tau_B}) = \left(\frac{\gamma_{NB}}{\tau_{NB}}\right)^{N_A} \frac{1}{\Gamma(N_B)} \operatorname{P}(\sum_{p=0}^{N_A} N_{B}^p \frac{2^{R_s}}{\tau_B} \left(\frac{2^{R_s} - 1 - \mu}{2^{R_s} - 1}\right)^p \frac{\gamma_{NB}^{N_B}}{\tau_{NB}^{N_B}} \left(\gamma_{NB} \right)^{N_B})
\]

(16)

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

\[
P(\mu, R_s) = \left(\frac{\gamma_{NB}}{\tau_{NB}}\right)^{N_A} \frac{1}{\Gamma(N_B)} \operatorname{P}(\sum_{p=0}^{N_A} N_{B}^p \frac{2^{R_s}}{\tau_B} \left(\frac{2^{R_s} - 1 - \mu}{2^{R_s} - 1}\right)^p \frac{\gamma_{NB}^{N_B}}{\tau_{NB}^{N_B}} \left(\gamma_{NB} \right)^{N_B})
\]

\[
\times \left(\frac{\gamma_{NB}}{\tau_{NB}}\right)^{N_A} \frac{1}{\Gamma(N_B)} \operatorname{P}(\sum_{p=0}^{N_A} N_{B}^p \frac{2^{R_s}}{\tau_B} \left(\frac{2^{R_s} - 1 - \mu}{2^{R_s} - 1}\right)^p \frac{\gamma_{NB}^{N_B}}{\tau_{NB}^{N_B}} \left(\gamma_{NB} \right)^{N_B})
\]

\[
\times \Gamma(p + N_E, \frac{2^{R_s} - 1 - \mu}{2^{R_s} - 1 - \mu}) - \left(\mu^{N_A N_B}\right)
\]

\[
Q\left(N_E, \frac{2^{R_s} - 1 - \mu}{2^{R_s} - 1 - \mu}\right)
\]

(17)

This is a much simpler expression for proposed scheme compared 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, \(R_s\), to an arbitrary value close to \(C_0\) according to the instantaneous CSI of the legitimate channel, we determine the values of \(\mu\) 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

\[
\arg \max_{R_s, \mu} \quad p_{tx}(\mu)R_s,
\]

s.t. \(p_{so}(R_s, \mu) \leq \epsilon, p_{tx}(\mu) \geq \sigma, \mu \geq 2^{R_s} - 1, R_s > 0,\)

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

\[
\mu \in \left[2^{R_s} - 1, \frac{2^{R_s} - 1}{\tau_B} P^{-1}\left(N_B, (1 - \sigma)^{\frac{1}{\gamma}}\right)\right]
\]

(12)

Under these conditions, the optimization problem can be formulated as

\[
\arg \max_{R_s, \mu} \quad (1 - F_{\mu}(\mu)) R_s,
\]

s.t. \(R_s > 0, \mu \leq \frac{2^{R_s} - 1}{\tau_B} P^{-1}\left(N_B, (1 - \sigma)^{\frac{1}{\gamma}}\right)\).

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.

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 average SNR at Bob for different number of antennas at Alice, Bob and Eve, for \(R_s=2\) bits/s/Hz and \(\tau_{BE}=0\) dB.
the TAS technique, which prevents the eavesdropper from exploiting diversity from Alice. In addition, it can be observed that the cases of more 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 $\gamma_B = 15$ dB, and $\gamma_E = 0$ 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 $\gamma_E = 0$ dB, a legitimate channel with average SNR $\gamma_B$ of 5dB, an on-off SNR threshold $\mu = 2^{\epsilon_1} - 1$, 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 $N_A = 2, N_B = 2$, $N_A = 2, N_B = 4$, $N_E = 2$. 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 $\epsilon$, 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 $\sigma = 0.5$, $\tau_B = 5$ dB, and at $\tau_E = 0$ 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 AKPro (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

\[ P(\mu, R_{E}) = I_1 - \Psi_1, \]  

where

\[ I_1 = \int_{\frac{2\mu R_{E}}{\gamma} - 1}^{\infty} F_{\gamma} \left( \frac{2R_{E}(1 + \gamma E) - 1}{\gamma} \right) \gamma E d\gamma E \]

\[ = \left. \frac{K}{s_{1}t} \left( \frac{2R_{E}(1 + \gamma E) - 1}{\gamma} \right) \right|_{s_{0} = 1}^{s_{N_{B} - 1}} \sum_{t=0}^{s_{N_{B} - 1}} \left( \frac{K}{s_{t}} \right) \left( \frac{2R_{E}(1 + \gamma E) - 1}{\gamma} \right) \left( \frac{N_{B} - 1}{s_{t}} \right) \left( \frac{1}{s_{t}} \right) \]  

\[ = \left. \frac{K}{s_{1}t} \left( \frac{2R_{E}(1 + \gamma E) - 1}{\gamma} \right) \right|_{s_{1} = 1}^{s_{N_{B} - 1}} \sum_{t=0}^{s_{N_{B} - 1}} \left( \frac{K}{s_{t}} \right) \left( \frac{2R_{E}(1 + \gamma E) - 1}{\gamma} \right) \left( \frac{N_{B} - 1}{s_{t}} \right) \left( \frac{1}{s_{t}} \right) \]

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**


