Secrecy Outage Performance of MIMO Wiretap Channels with Multiple Jamming Signals

Daniel B. da Costa, Nuwan S. Ferdinand, Ugo S. Dias, Rafael T. de Sousa Jr., and Matti Latva-aho

***Abstract*—In this paper, assuming an interference-limited eavesdropper scenario, the secrecy outage performance of multiple-input multiple-output wiretap channels with transmit antenna selection is investigated. Considering that the transmitter (Tx) and the receiver (Rx) are equipped with N_A and N_B antennas, respectively, while the passive eavesdropper is set with N_E antennas, closed-form expressions for the secrecy outage probability and non-zero secrecy rate are derived. In our analysis, both maximal-ratio combining (MRC) and selection combining (SC) are employed at the Rx, while the eavesdropper uses a MRC scheme. The derived outage expressions hold for arbitrary power distributed jamming signals and some of their special cases (i.e., distinct power distributed and equal power distributed jamming signals) are presented. An asymptotic analysis is carried out to show the impact of the number of jamming signals and number of antennas on the secrecy outage performance. Interestingly, our results show that the diversity order equals to $\min(M, N_A N_B)$, with M denoting the number of jamming signals. This allows us to conclude that the number of jamming signals at the eavesdropper limits the secrecy performance via diversity such that a high number of antennas does not imply necessarily in a performance improvement, unless for a large number of jamming signals.**

***Index Terms*—Jamming, MIMO wiretap channels, outage probability, secrecy performance.**

I. Introduction

The broadcast nature of the wireless medium makes the communication process vulnerable to eavesdroppers which are in the coverage area of the transmission. Thus, security issues play an important role in wireless networks. Diverse strategies to ensure the information privacy have been proposed in the literature. Traditionally, the security is addressed via cryptographic approaches implemented at higher layers of the protocol stack [2], [3]. Cryptography-based security aims to design a protocol such that it is computationally prohibitive for the eavesdropper to decode the information. The idea behind of this approach relies on the limited computational power of the eavesdroppers. However, with the advent of infrastructureless networks, the secret key management may be vulnerable to attacks of malicious users [4]. Owing to this fact, recent advances in the research have proposed to implement the security at the physical layer (PHY) [5]–[7]. The key principle behind this strategy is to exploit the spatial-temporal characteristics of the wireless channel to guarantee secure data transmission. A seminal work was proposed by Wyner [8], where the wiretap channel was introduced. In [8], using the information theory approach, it was shown that the communication can be performed with non-zero rate if the transmitter-eavesdropper channel is a degraded version of the transmitter-receiver channel. Since then, from different perspectives, PHY security has received a considerable attention from the wireless community as a way to ensure perfect secrecy along the communication process [9]–[29]. These works are briefly discussed next.

Employing an information-theoretic approach, [9] considered a Gaussian multiple-input single-output (MISO) channel. For these channel inputs, and under different channel fading assumptions, optimal transmission strategies were proposed. Later, in two independent works [10], [11], the secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel under the average total power constraint was characterized using a Sato-like argument and matrix analysis tools. The authors in [12] presented an alternative characterization of the secrecy capacity of the multiple-antenna wiretap channel under a more general matrix constraint on the channel input using a channel-enhancement argument. In [13], the secrecy outage in MISO systems was investigated assuming that the transmitter has only partial information about the channel to the eavesdropper. In this case, the outage probability of secure transmission was minimized under single-stream beamforming and the use of artificial noise in the null space of the main channel. Robust beamforming methods were proposed in [15] to combat the imperfect channel estimates and improve the secrecy in MIMO wiretap channels. Assuming a cooperative diversity scenario, the authors in [16] addressed the robust relay beamforming problem for the relay-eavesdropper network, in which perfect channel state information (CSI) of legitimate channels was known to all nodes, whereas only imperfect CSI of the eavesdropper's channel was available to legitimate nodes.

Different from the aforementioned works, researchers also have investigated the analytical secrecy outage performance of wiretap channels. In [17], a method of utilizing channel diversity to increase secrecy capacity in wireless transmissions was proposed, in which it was shown that an intended receiver can achieve a relatively high secrecy capacity even at low signal-to-noise ratio (SNR) regions. In [18], it was considered that a single-antenna transmitter communicates with a single-antenna receiver in the presence of an eavesdropper equipped

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

D. B. da Costa is with the Federal University of Ceará (UFC), Campus Sobral, Ceará, Brazil (e-mail: danielbcosta@ieee.org).

N. S. Ferdinand and M. Latva-aho are with the Centre for Wireless Communications, University of Oulu, Finland (e-mail: {nuferdin,matla}@ee.oulu.fi).

U. S. Dias and R. T. de Sousa Júnior are with the Department of Electrical Engineering, University of Brasília, Brazil (email: {udias,desousa}@unb.br).

The authors wish to thank the Brazilian research, development and innovation Agencies CAPES (Grant FORTE 23038.007604/2014-69), FINEP (Grant RENASIC/PROTO 01.12.0555.00), CNPq (Grant 304301/2014-0), and the National Consumer Secretariat (SENACON) of the Brazilian Ministry of Justice, for their support to this work.

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.2016.2

with multiple antennas, which employs either a maximal-ratio combining (MRC) or a selection combining (SC) technique. Closed-form expressions for the secrecy-outage probability were derived for both combining techniques. The work in [19] investigated the transmission of confidential messages through Nakagami-m fading channel in the presence of multiple eavesdroppers. In this case, the probability of non-zero secrecy capacity, outage secrecy probability, outage secrecy capacity, and ergodic secrecy capacity were characterized.

Although beamforming in the direction of legitimate user is optimal [9], the implementation complexity of beamforming is high and needs full rate feedback. Hence, authors in [20] proposed a low-complexity transmit antenna selection (TAS) scheme that selects a transmit antenna which maximizes the received SNR of the legitimate user. The results showed that high levels of security can be achieved when the number of antennas at transmitter (Tx) increases, even when the eavesdropper has multiple antennas. This work was generalized in [21], where the secrecy outage performance was examined for the scenario with all nodes being multiple-antenna terminals. In this case, the receiver (Rx) and eavesdropper employed either SC or MRC to combine the received signals. More recently, assuming a TAS wiretap channel, the impact of antenna correlation at the receiver and eavesdropper sides on the secrecy performance was studied in [22]. The Tx experienced independent fading and employed a TAS scheme, while MRC was applied at the Rx and eavesdropper. Finally, in [23], the effects of outdated CSI on the secrecy performance was investigated. It was observed that the expected diversity gain cannot be realized when CSI is outdated during the antenna selection process.

All the above works showed that multiple antennas increase the PHY security. However, numerous researchers have looked into another dimension to enhance it further, i.e., the use of jamming signals to distract eavesdroppers reception or, equivalently, the use of interference or artificial noise to confuse the eavesdropper. Along the last years, considerable works have been proposed to address the jamming in wiretap channels, and some of them can be found in [24]–[29]. The overall concept is to have a helping jammer that sends codewords which are independent of the source message at an appropriate rate [24]. In [24], the authors considered all possible interference patterns and designed the corresponding achievable coding scheme at the legitimate transmitter based on the coding rate of the interference codebook. This work was extended for multiple access and broadcast channels by using cooperative jamming in [25], [26]. In [27], secure communication in wiretap fading channels was analyzed (in terms of ergodic secrecy capacity) in the presence of non-colluding or colluding eavesdroppers. In that analysis, the transmitter was equipped with multiple antennas and was able to simultaneously transmit an information signal to the intended receiver and artificial noise to confuse the eavesdroppers. Authors in [28] analyzed the benefits of jamming on secure communications based on the density of jammers and eavesdroppers and the choice of active jammers. Finally, power allocation scheme has been proposed in [29], where both the destination and relay cooperates with the source to jam the eavesdropper without creating interference at the destination.

Although the concept of using a friendly jammer has been considered in the literature, as far as the authors are aware, the *secrecy outage analysis* of wiretap channels in an interference-limited eavesdropper scenario has not been carried out in the technical literature yet. In this paper, assuming an interference-limited eavesdropper scenario[1], the secrecy outage performance of MIMO wiretap channels with TAS is investigated. Considering that the Tx, called Alice, and the Rx, called Bob, are equipped with N_A and N_B antennas, respectively, while the passive eavesdropper, called Eve, is set with N_E antennas, closed-form expressions for the secrecy outage probability and non-zero secrecy rate are derived for different receive antenna configurations. In our analysis, both MRC and SC are employed at Bob to combine the received signals. On the other hand, Eve uses only MRC since this is the worst case from a secrecy point of view[2]. The derived outage expressions hold for arbitrary power distributed jamming signals, in which some special cases (i.e., distinct power distributed and equal power distributed jamming signals) are attained. An asymptotic analysis is carried out to show the impact of the number of jamming signals and number of antennas on the secrecy outage performance. Insightful conclusions are achieved from our results. For instance, it is shown that the diversity order equals to $\min(M, N_A N_B)$, with M denoting the number of jamming signals. This allows us to conclude that the number of jamming signals arriving at Eve limits the secrecy performance via diversity such that a high number of antennas does not necessarily imply in a performance improvement, unless for a large number of jamming signals. This remark has not been reported in previous works yet, being of paramount importance for the system design of MIMO wiretap channels in an interference-limited eavesdropper scenario.

II. System Model

We consider a MIMO wiretap channel where the transmitter Alice communicates with a legitimate receiver Bob while an eavesdropper Eve hears the transmitted signal by Alice. We consider a friendly jammer which causes interference at Eve. As shown in Fig. 1, the friendly jammer has full secure cooperation with Bob. Indeed, when Bob is a full-duplex node, the friendly jammer is Bob himself who sends jamming signals to eavesdropper. In this setup, Eve is operating in an interference-limited environment, in which a general model with M arbitrary power distributed jamming signals is adopted. All terminals are equipped with multiple antennas, with N_A, N_B, and N_E denoting the number of antennas at Alice, Bob, and Eve, respectively. The main channel is independent of the eavesdropper's channel. However, both main channel and eavesdropper's channel experience slow fading with the same fading block length, which is long enough to allow capacity-achieving codes within each block. Employing a TAS scheme, Alice uses the CSI of Bob (i.e., Eve is a passive eavesdropper) to maximize the received signal to noise ratio (SNR) of Bob. This system setup naturally forced us to consider two receiver combining schemes at Bob: MRC to higher secrecy performance gain with higher complexity

[1]It is considered that a friendly jammer causes interference at the eavesdropper. The jamming signals can arise in several practical schemes: (a) if the Rx is a full-duplex node, these signals can be deployed by the Rx with the single purpose of jamming potential eavesdroppers; (b) A friendly jammer who transmit jamming signals to the eavesdropper without causing interference to Rx.

[2]Note that employing MRC at Eve always provides worst secrecy performance than SC.

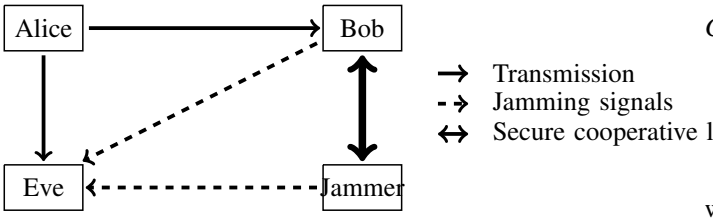

Fig. 1. System model.

and SC to have low complexity with slightly less secrecy performance gain. On the other hand, Eve uses only MRC since this is the worst case from a secrecy point of view.

A. MRC at Bob

Alice selects the transmit antenna s according to the rule

$$s = \arg \max_{k \in \{1,\dots N_A\}} \|\mathbf{h}_{\mathrm{AB},k}\|, \tag{1}$$

where $\|\cdot\|$ indicates the Frobenius norm and $\mathbf{h}_{\mathrm{AB},k} = [h^1_{\mathrm{AB},k} h^2_{\mathrm{AB},k} \dots h^{N_B}_{\mathrm{AB},k}]^T$ denotes the $N_B \times 1$ channel vector between the k^{th} antenna at Alice and Bob, with $(\cdot)^T$ representing the transpose operation. Then, Alice transmits its signal x using the selected antenna s and the received signal at Bob is[3]

$$\mathbf{y}_{\mathrm{B}} = \sqrt{P}\mathbf{h}_{\mathrm{AB},s} x + \mathbf{n}_{\mathrm{B}}, \tag{2}$$

where P denotes the transmit power at Alice, $\mathbf{h}_{\mathrm{AB},s}$ stands for the $N_B \times 1$ channel vector from the selected antenna at Alice to Bob, and $\mathbf{n}_{\mathrm{B}}$ is the additive white Gaussian noise (AWGN) $N_B \times 1$ channel vector with entries having variance n_b. Bob uses a MRC scheme to combine the received signals, in which the MRC weight vector is given by $\mathbf{w}_{\mathrm{B}} = \frac{\mathbf{h}^\dagger_{\mathrm{AB},s}}{\|\mathbf{h}_{\mathrm{AB},s}\|}$, with $(\cdot)^\dagger$ denoting conjugate transpose. Thus, the signal at the combiner output can be written as

$$y_{\mathrm{B}} = \sqrt{P}\|\mathbf{h}_{\mathrm{AB},s}\| x + \mathbf{w}_{\mathrm{B}}\mathbf{n}_{\mathrm{B}}. \tag{3}$$

The received SNR at Bob is given by $\gamma^{mrc}_{B,s} = \bar{\gamma}_B \|\mathbf{h}_{\mathrm{AB},s}\|^2$, with $\bar{\gamma}_B = P/n_b$.

B. SC at Bob

In this case, Alice selects the transmit antenna s according to the rule

$$s = \arg \max_{k \in \{1,\dots N_A\}} |h^m_{\mathrm{AB},k}|, \quad \forall m \in \{1, \dots N_B\}, \tag{4}$$

where $h^m_{\mathrm{AB},k}$ represents the channel coefficient between the Alice's k^{th} antenna and the Bob's m^{th} antenna. Then, Bob uses a SC scheme to select an antenna that maximizes the instantaneous SNR such that its combined signal is given by

$$y_{\mathrm{B}} = \sqrt{P}|h_{\mathrm{AB},s}| x + n_{\mathrm{B}}, \tag{5}$$

where n_{B} is AWGN component with variance n_b and

$$|h_{\mathrm{AB},s}| = \max_{m \in 1\dots,N_B} |h^m_{\mathrm{AB},s}|. \tag{6}$$

Thus, the received SNR at Bob is given by $\gamma^{sc}_{B,s} = \bar{\gamma}_B |h_{\mathrm{AB},s}|^2$.

[3]Since Bob has full cooperation with the friendly jammer, we assume that it can completely cancel the jamming signals coming from jammer or itself.

C. MRC at Eve subject to Jamming Signals

The received signal at Eve can be written as[4]

$$\mathbf{y}_{\mathrm{E}} = \sqrt{P}\mathbf{h}_{\mathrm{AE,s}} x + \sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\mathbf{h}_i, \tag{7}$$

where $\mathbf{h}_{\mathrm{AE,s}}$ stands for channel component from the selected antenna at Alice to Eve, $\mathbf{h}_i$ denotes the $N_B \times 1$ channel vector between the i^{th} jamming signal and Eve, and $\bar{\gamma}_i$ represents the interference power of the i^{th} jamming signal. Eve performs MRC such that the signal at the combiner output is given by

$$\begin{aligned} y_{\mathrm{E}} &= \sqrt{P}\frac{\mathbf{h}^\dagger_{\mathrm{AE,s}}}{\|\mathbf{h}_{\mathrm{AE,s}}\|}\mathbf{h}_{\mathrm{AE,s}} x + \sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\frac{\mathbf{h}^\dagger_{\mathrm{AE,s}}}{\|\mathbf{h}_{\mathrm{AE,s}}\|}\mathbf{h}_i \\ &= \sqrt{P}\|\mathbf{h}_{\mathrm{AE,s}}\| x + \sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\tilde{h}_i. \end{aligned} \tag{8}$$

It can be proved that $\tilde{h}_i = \frac{\mathbf{h}^\dagger_{\mathrm{AE,s}}}{\|\mathbf{h}_{\mathrm{AE,s}}\|}\mathbf{h}_i$ follows the same distribution as element of $\mathbf{h}_i$ when $\mathbf{h}_i$ and $\mathbf{h}_{\mathbf{AE,s}}$ are independent. Based on above, the received signal-to-interference ratio (SIR) at Eve can be expressed as

$$\Upsilon_{E,s} = \frac{\gamma_{E,s}}{\gamma_I}, \tag{9}$$

where $\gamma_{E,s} = \bar{\gamma}_E \|\mathbf{h}_{\mathrm{AE,s}}\|^2$, $\gamma_I = \sum_{i=1}^{M} \bar{\gamma}_i |\tilde{h}_i|^2$, and $\bar{\gamma}_E$ means the channel variance.

D. Achievable Secrecy Rate

Let the capacity of the main channel be $R_{B,s} = \log_2(1 + \gamma_{B,s})$ and the capacity of the eavesdropper channel be $R_{E,s} = \log(1 + \Upsilon_{E,s})$. Thus, the secrecy capacity can be defined as[5]

$$R_S = \begin{cases} R_{B,s} - R_{E,s}, & \gamma_{B,s} > \Upsilon_{E,s}, \\ 0, & \gamma_{B,s} \le \Upsilon_{E,s}. \end{cases} \tag{10}$$

III. Secrecy Performance

A. Preliminaries

We assume that all channels undergo Rayleigh fading. Hence, the probability density function (PDF) and cumulative distribution function (CDF) of the random variable $\gamma^{mrc}_{B,k} = \bar{\gamma}_B \|\mathbf{h}_{\mathrm{AB},k}\|^2$ are given

$$f_{\gamma^{mrc}_{B,k}}(z) = \frac{z^{N_B - 1} e^{-\frac{z}{\bar{\gamma}_B}}}{\bar{\gamma}_B^{N_B}\Gamma(N_B)}, \tag{11}$$

$$F_{\gamma^{mrc}_{B,k}}(z) = 1 - e^{-\frac{z}{\bar{\gamma}_B}} \sum_{u=0}^{N_B - 1} \frac{1}{u!}\left(\frac{z}{\bar{\gamma}_B}\right)^u, \tag{12}$$

with $\Gamma(\cdot)$ denoting the Gamma function [30, Eq. (8.310.1)]. Then, using the concepts of probability theory and considering statistically independent Rayleigh fading, the CDF of $\gamma^{mrc}_{B,s}$ can be written as

$$F_{\gamma^{mrc}_{B,s}}(z) = \left[F_{\gamma^{mrc}_{B,k}}(z)\right]^{N_A}. \tag{13}$$

[4]We assume that the noise component at Eve can be neglected with the strong jamming signal power.

[5]Depending on the combining scheme employed at Bob, note that $\gamma_{B,s}$ can be either $\gamma^{mrc}_{B,s}$ or $\gamma^{sc}_{B,s}$.

Now, by substituting (12) into (13) and making use of the multinomial theorem, followed by mathematical simplifications, the CDF of $\gamma_{B,s}^{mrc}$ can be rewritten as

$$F_{\gamma_{B,s}^{mrc}}(z) = \sum_{n_1=0}^{N_A} (-1)^{n_1} \binom{N_A}{n_1} \sum_{N_B,n_1} \left(\frac{z}{\bar{\gamma}_B}\right)^{\beta} e^{-\frac{n_1 z}{\bar{\gamma}_B}}, \quad (14)$$

where the following notation is adopted

$$\sum_{N_B,n_1} = \sum_{n_2=0}^{n_1} \sum_{n_3=0}^{n_2} \cdots \sum_{n_{N_B}=0}^{n_{N_B-1}} \prod_{i=0}^{N_B-1} \left(\frac{1}{i!}\right)^{n_{i+1}-n_{i+2}} \binom{n_{i+1}}{n_{i+2}}, \quad (15)$$

and $\beta = \sum_{j=0}^{N_B-1} j(n_{j+1} - n_{j+2})$, with $n_{N_B+1} = 0$. The derivation is taken to obtain PDF of $\gamma_{B,s}^{mrc}$ as

$$f_{\gamma_{B,s}^{mrc}}(z) = \frac{N_A}{\Gamma(N_B)} \sum_{n_1=0}^{N_A-1} (-1)^{n_1} \binom{N_A-1}{n_1} \times \sum_{N_B,n_1} \frac{z^{N_B+\beta-1}}{\bar{\gamma}_B^{N_B+\beta}} e^{-\frac{(n_1+1)z}{\bar{\gamma}_B}}, \quad (16)$$

By its turn, the CDF of $\gamma_{B,s}^{sc}$ can be derived as

$$F_{\gamma_{B,s}^{sc}}(z) = \left(1 - e^{-\frac{z}{\bar{\gamma}_B}}\right)^{N_A N_B}, \quad (17)$$

where, from the binomial expansion, it follows that

$$F_{\gamma_{B,s}^{sc}}(z) = 1 - \sum_{k=1}^{N_A N_B} \binom{N_A N_B}{k} (-1)^{k+1} e^{-\frac{zk}{\bar{\gamma}_B}}. \quad (18)$$

The CDF of γ_E can be obtained replacing N_B and $\bar{\gamma}_B$ by N_E and $\bar{\gamma}_E$, respectively, in (12). Let $\bar{\gamma}_1, \bar{\gamma}_2, \ldots \bar{\gamma}_t$ be the distinct values with multiplicities $\eta_1, \eta_2, \ldots \eta_t$ such that $\sum_{i=1}^{t} \eta_i = M$. Then, from [31], the PDF of γ_I can be written as

$$f_{\gamma_I}(z) = \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{(j-1)!\bar{\gamma}_i^j} z^{j-1} e^{-\frac{z}{\bar{\gamma}_i}}, \quad (19)$$

where

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)!\bar{\gamma}_i^{\eta_i - j}} \frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}} \left[\prod_{k=1,k\neq i}^{t} \left(\frac{1}{1+s\bar{\gamma}_k}\right)^{\eta_k}\right]_{s=-\frac{1}{\bar{\gamma}_i}}. \quad (20)$$

B. Secrecy Outage Probability

It is defined as the probability that R_S drops below a predefined threshold rate R and it can be mathematically expressed as

$$P_s(R) = \Pr(R_S < R), \quad (21)$$

with $\Pr(\cdot)$ denoting probability. In the sequel, the secrecy outage probability will be derived assuming either MRC or SC at Bob as well as arbitrary power distributed jamming signals. Afterwards, the general expressions will be reduced for two special cases, i.e., distinct power distributed jamming signals and equal power distributed jamming signals.

Theorem 1: The secrecy outage probability assuming MRC at Bob can be derived as

$$P_s^{mrc}(R) = 1 - \sum_{n_1=1}^{N_A} \binom{N_A}{n_1} \sum_{N_B,n_1} \sum_{u=0}^{N_E-1} \frac{(-1)^{n_1+1}}{u!} \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \times \frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!\bar{\gamma}_B^{\beta}} \sum_{p=0}^{\beta} \binom{\beta}{p} \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i}\right)^p (2^R-1)^{\beta-p} 2^{Rp} e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}} \times \left[j\Gamma(p+u+1)\Psi\left(p+u+1, p-j+1, \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_1\right], \quad (22)$$

where

$$\Theta_1 = \begin{cases} u\Gamma(p+u)\Psi\left(p+u, p-j, \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right), & u \neq 0 \\ 0, & u = 0 \end{cases}, \quad (23)$$

and $\Psi(.,.;.)$ denotes the Tricomi's (confluent hypergeometric) function [30, Eq. (9.211.4)], with $\sum_{N_B,n_1}$ and β being defined as in (15).

Proof: Please, see Appendix A.

Next, (22) will be simplified for two special cases.

Corollary 1.1: Relying on the properties given in [31], (22) can be simplified for the case of distinct power distributed jamming signals as

$$P_s^{mrc}(R) = 1 - \sum_{n_1=1}^{N_A} \binom{N_A}{n_1} \sum_{N_B,n_1} \sum_{u=0}^{N_E-1} (-1)^{n_1+1} \sum_{i=1}^{M} \bar{\gamma}_i^{M-1} \times \prod_{k=1,k\neq i}^{t} (\bar{\gamma}_i - \bar{\gamma}_k)^{-1} \frac{1}{\bar{\gamma}_B^{\beta}} \sum_{p=0}^{\beta} \binom{\beta}{p} \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i}\right)^p (2^R-1)^{\beta-p} 2^{Rp} \times e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}} \left[\Gamma(p+u+1)\Psi\left(p+u+1, p, \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_{11}\right], \quad (24)$$

where Θ_{11} equals to Θ_1 given in (23) by setting $j = 1$.

Corollary 1.2: Assuming $\bar{\gamma}_1 = \bar{\gamma}_2 \ldots = \bar{\gamma}_M$, (22) can be simplified for the case of equal power distributed jamming signals as

$$P_s^{mrc}(R) = 1 - \sum_{n_1=1}^{N_A} \binom{N_A}{n_1} \sum_{N_B,n_1} \sum_{u=0}^{N_E-1} \frac{(-1)^{n_1+1}}{u!} \frac{\Gamma(u+M)}{(M-1)!\bar{\gamma}_B^{\beta}} \times \sum_{p=0}^{\beta} \binom{\beta}{p} \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_1}\right)^p (2^R-1)^{\beta-p} 2^{Rp} e^{-\frac{n_1(z-1)}{\bar{\gamma}_B}} \times \left[M\Gamma(p+u+1)\Psi\left(p+u+1, p-M+1, \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_1\bar{\gamma}_B}\right) - \Theta_{12}\right], \quad (25)$$

where Θ_{12} equals to Θ_1 given in (23) by setting $j = M$.

Theorem 2: The secrecy outage probability assuming SC at Bob can be achieved as

$$P_s^{sc}(R) = 1 - \sum_{k=1}^{N_A N_B} (-1)^{k+1} \binom{N_A N_B}{k} \sum_{u=0}^{N_E-1} \frac{1}{u!} \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \times \frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!} e^{-\frac{k(2^R-1)}{\bar{\gamma}_B}} \left[j\Gamma(u+1)\Psi\left(u+1, -j+1; \frac{k\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_2\right], \quad (26)$$

where

$$\Theta_2 = \begin{cases} u\Gamma(u)\Psi\left(u, -j, \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right), & u \neq 0 \\ 0, & u = 0 \end{cases}. \quad (27)$$

Proof: Please, see Appendix A.

Similarly to the MRC scheme, the secrecy outage probability in (26) will be particularized to two special cases.

Corollary 2.1: Assuming distinct power distributed jamming signals at Bob, (26) can be written as

$$P_s^{sc}(R) = 1 - \sum_{k=1}^{N_A N_B} \binom{N_A N_B}{k} \sum_{u=0}^{N_E-1} \sum_{i=1}^{M} \times \frac{(-1)^{k+1}\gamma_i^{M-1} e^{-\frac{k(2^R-1)}{\bar{\gamma}_B}}}{\prod_{k=1,k\neq i}^{t}(\bar{\gamma}_i - \bar{\gamma}_k)} \left[\Gamma(u+1)\Psi\left(u+1, 0; \frac{k\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_{21}\right], \quad (28)$$

where Θ_{21} is given in (27) by setting $j = 1$.

Corollary 2.2: For the case of equal power distributed jamming signals at Bob, (26) reduces to

$$P_s^{sc}(R) = 1 - \sum_{k=1}^{N_A N_B} (-1)^{k+1}\binom{N_A N_B}{k} \sum_{u=0}^{N_E-1} \frac{1}{u!}\frac{\Gamma(u+M)}{(M-1)!} \times e^{-\frac{k(2^R-1)}{\bar{\gamma}_B}} \left[M\Gamma(u+1)\Psi\left(u+1, -M+1; \frac{k\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_{22}\right], \quad (29)$$

where Θ_{22} is same as Θ_2 given in (27) by setting $j = M$.

In order to gain further insights for the secrecy performance, it would be interesting to consider the case when both Bob and Eve are single-antenna devices (i.e., a MISO wiretap channel). Hence, Corollary 3 presents secrecy outage for MISO wiretap channel when Eve is limited by multiple equal power distributed jamming signals.

Corollary 3: The secrecy outage for MISO wiretap channel with multiple equal power interference at eavesdropper can be obtained using $N_B = N_E = 1$ in (25) or (29) as

$$P_s^{miso}(R) = -\sum_{n_1=1}^{N_A} (-1)^{n_1+1}\binom{N_A}{n_1} e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}} M \times \Psi\left(1, -M+1; \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right). \quad (30)$$

C. Non-Zero Secrecy Rate

Now, the probability of non-zero secrecy rate is studied in which closed-form expressions for this metric are derived assuming both MRC and SC techniques at Bob. The probability of nonzero secrecy rate can be mathematically represented as

$$\begin{aligned} P_r(R_S > 0) &= \Pr(R_B > R_E) \\ &= \Pr(\gamma_{B,s} > \gamma_{E,s}) \\ &= \int_0^\infty \int_0^x f_{\gamma_{B,s}}(x) f_{\Upsilon_{E,s}}(y) dy dx. \end{aligned} \quad (31)$$

1) MRC at Bob: An exact closed-form expression for the probability of non-zero rate is derived by substituting (16) and (51) into (31), and performing the required integral, yielding

$$P_r^{mrc}(R_S > 0) = 1 - \frac{N_A}{\Gamma(N_B)} \sum_{n_1=0} N_A - 1(-1)^{n_1}\binom{N_A-1}{n_1} \times \sum_{N_B,n_1} \sum_{u=0}^{N_E-1} \frac{1}{u} \sum_{i=1} t \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!}\Gamma(N_B+\beta+u) \times \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_B\bar{\gamma}_i}\right)^{N_B+\beta} \Psi\left(N_B+\beta+u, N_B+\beta-j+1; \frac{(n_1+1)\bar{\gamma}_E}{\bar{\gamma}_B\bar{\gamma}_i}\right). \quad (32)$$

2) SC at Bob: Similarly, an exact closed-form expression is derived using the PDFs of $\gamma_{B,s}^{sc}$ and $\Upsilon_{E,s}$ in (31), i.e.,

$$P_r^{sc}(R_S > 0) = 1 - N_A N_B \sum_{k=0}^{N_A N_B - 1} \binom{N_A N_B - 1}{k}(-1)^k \times \sum_{u=0}^{N_E-1} \frac{1}{u!} \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!}\Gamma(u+1)\frac{\bar{\gamma}_E}{\bar{\gamma}_B\bar{\gamma}_i} \times \Psi\left(u+1, 2-j; \frac{(k+1)\bar{\gamma}_E}{\bar{\gamma}_B\bar{\gamma}_i}\right). \quad (33)$$

IV. Asymptotic Secrecy Analysis

In this Section, to gain further insights for the secrecy performance, an asymptotic analysis (i.e., at high SNR regions) is now carried out from which the diversity order is attained. For the sake of simplicity, we consider $N_E = 1$ such that the derived expressions are not too long. However, for arbitrary N_E, the analysis can be easily done following the same procedure. Next, we assume that the Bob's average SNR is larger than Eve's SIR, i.e., $\bar{\gamma}_B > \bar{\gamma}_E/\bar{\gamma}_1$.

A. Asymptotic Secrecy Outage for MRC at Bob

Firstly, representing (22) in integral form, it follows

$$P_s^{mrc}(R) = 1 - \sum_{n_1=1}^{N_A}\binom{N_A}{n_1} \sum_{N_B,n_1} (-1)^{n_1+1} \sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{\bar{\gamma}_B^{\beta}} \times \sum_{p=0}^{\beta}\binom{\beta}{p}\left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i}\right)^p (2^R-1)^{\beta-p} 2^{Rp} e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}} j \times \int_0^\infty x^p e^{-\frac{n_1 2^R x\bar{\gamma}_E}{\bar{\gamma}_B\bar{\gamma}_i}} (x+1)^{-j-1} dx. \quad (34)$$

After some mathematical manipulations and using the binomial expansion, the integral in (34) can be solved, yielding

$$P_s^{mrc}(R) = 1 - \sum_{n_1=1}^{N_A}\binom{N_A}{n_1} \sum_{N_B,n_1} (-1)^{n_1+1} \sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{\bar{\gamma}_B^{\beta}} \times \sum_{p=0}^{\beta}\binom{\beta}{p}\left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i}\right)^p (2^R-1)^{\beta-p} 2^{Rp} \times e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}} e^{\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}} j \sum_{q=0}^{p}\binom{p}{q}(-1)^{p-q}\Psi, \quad (35)$$

where, for $q - j - 1 \geq 0$, we have

$$\Psi = e^{-\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}} \sum_{r=0}^{q-j-1} \frac{(q-j-q)!}{r!}\left(\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}\right)^{j-q+r}, \quad (36)$$

and, for $q-j-1<0$,

$$\Psi=\frac{1}{(j-q)!}\left[-\left(-\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}\right)^{j-q}\mathrm{Ei}\left(-\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}\right)+e^{-\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}}\sum_{r=0}^{j-q-1}\left(-\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}\right)^{r}(j-q-1-r)!\right], \tag{37}$$

with $\mathrm{Ei}(\cdot)$ denoting the exponential integral [30, Eq. (8.211.1)]. Now, using the Maclaurin expansion to expand the exponential function, rewriting the exponential integral as a series expansion [30, Eq. (8.214.1)], and considering the first non-zero order terms of (35), and after some mathematical simplifications, an asymptotic expression is obtained as

$$P_s^{mrc,\infty}(R)=\left[\sum_{n_1=1}^{N_A}\binom{N_A}{n_1}\sum_{N_B,n_1}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\sum_{p=0}^{\beta}\sum_{q=0}^{p}\Omega_{i,j}\binom{\beta}{p}\times(2^R-1)^{\beta-p}2^{Rp}j\binom{p}{q}(-1)^{n_1+p-q}\Lambda\right]\bar{\gamma}_B^{-G}+o(\bar{\gamma}_B^{-G-1}), \tag{38}$$

where, for $q-j-1\geq 0$, we have (39), given at the top of the next page, and, for $q-j-1<0$,

$$\Lambda=\sum_{r=0}^{j-q-1}\frac{(j-q-1-r)!(-1)^{G-\beta}\bar{\gamma}_E^{p+r}(n_1(2^R-1))^{G-\beta-r}}{\bar{\gamma}_i^{p+r}(j-q)!(n_1 2^R)^{-r}(G-\beta-r)!}-\frac{\bar{\gamma}_E^{p+j-q}\left(\frac{n_1 2^R\bar{\gamma}_E}{\bar{\gamma}_i}-n_1(2^R-1)\right)^{G-\beta-j+q}}{(j-q)!(-n_1 2^R)^{j-q}\bar{\gamma}_i^{p+j-q}(G-\beta-j+q)!}\times\left(C+\ln\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}\right)\right). \tag{40}$$

From above, note that the diversity order equals to $G=\min(N_AN_B,M)$.

B. Asymptotic Secrecy Outage for SC at Bob

Now, we derive an asymptotic expression for the secrecy outage probability considering a SC technique at Bob. To gain further insight and to obtain a more simplified expression, we consider a uniform interference power scheme. It is worth noting that, for a non-uniform interference power scheme, the same conclusions hold. Firstly, in order to derive an asymptotic expression, we represent (29) in an integral form (by setting $N_E=1$) as

$$P_s^{sc}(R)=1-\sum_{n=1}^{N_AN_B}(-1)^{n+1}\binom{N_AN_B}{n}e^{-\frac{n(2^R-1)}{\bar{\gamma}_B}}M\times\int_0^\infty\frac{e^{-\frac{n2^R\bar{\gamma}_Ex}{\bar{\gamma}_1\bar{\gamma}_B}}}{(x+1)^{M+1}}dx. \tag{41}$$

Thus, making use of [30, Eq. (3.353)], it follows that

$$P_s^{sc}(R)=1-\sum_{n=1}^{N_AN_B}\frac{(-1)^{n+1}}{(M-1)!}\binom{N_AN_B}{n}e^{-\frac{n(2^R-1)}{\bar{\gamma}_B}}\times\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}\right)^M\left[\sum_{k=1}^{M}(k-1)!(-1)^{M-k}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}\right)^{-k}-\chi\right], \tag{42}$$

where $\chi=(-1)^Me^{\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}}\mathrm{Ei}\left(-\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}\right)$. Using the Maclaurin expansion to expand the exponential function and rewriting the exponential integral as a series expansion [30, Eq. (8.214.1)], an asymptotic expression can be attained as

$$P_s^{sc,\infty}(R)=1-\sum_{n=1}^{N_AN_B}\frac{(-1)^{n+1}}{(M-1)!}\binom{N_AN_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M\times\left[\sum_{k=1}^{M}(k-1)!\sum_{s=0}^{\infty}n^s(2^R-1)^s(-1)^{M-k+s}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{-k}\times-(-1)^M\sum_{q=0}^{\infty}\frac{1}{q!}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}-n(2^R-1)\right)^q\times\left\{\left(C+\ln\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)\right)\frac{1}{\bar{\gamma}_B^{M+q}}+\sum_{p=1}^{\infty}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^p\times\frac{(-1)^p}{pp!\bar{\gamma}_B^{p+q+M}}\right\}\right], \tag{43}$$

where C is the Euler constant. Finally, by considering the first non-zero order terms of (43) and after some mathematical simplifications, an asymptotic expression can be obtained as

$$P_s^{sc,\infty}(R)=\begin{cases}(\psi_1\bar{\gamma}_B)^{-N_AN_B}, & N_AN_B<M\\(\psi_2\bar{\gamma}_B)^{-M}, & N_AN_B>M\\(\psi_3\bar{\gamma}_B)^{-N}, & N=N_AN_B=M\end{cases} \tag{44}$$

where

$$\psi_1=\left[\sum_{n=1}^{N_AN_B}\frac{(-1)^n}{(M-1)!}\binom{N_AN_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M\sum_{k=1}^{M}\times\frac{(k-1)!(-1)^{N_AN_B-M}(n(2^R-1))^{N_AN_B-M+k}}{(N_AN_B-M+k)!}\times\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{-k}\right]^{-\frac{1}{N_AN_B}}, \tag{45}$$

$$\psi_2=\left[\sum_{n=1}^{N_AN_B}\frac{(-1)^{n+1}}{(M-1)!}\binom{N_AN_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M\times\left(C+\ln\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)\right)\right]^{-\frac{1}{M}}, \tag{46}$$

and

$$\psi_3=\left[\sum_{n=1}^{N_AN_B}\frac{(-1)^n}{(M-1)!}\binom{N_AN_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M\times\left\{\sum_{k=1}^{M}\frac{(k-1)!(-1)^{N_AN_B-M}(n(2^R-1))^{N_AN_B-M+k}}{(N_AN_B-M+k)!}\times\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{-k}-\left(C+\ln\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)\right)\right\}\right]^{-\frac{1}{N}}. \tag{47}$$

C. Diversity Gain

From the previous subsection, note that the diversity gain equals to $G_D=\min(M,N_AN_B)$. This is a very interesting result as it shows that the diversity is limited by the number of

$$\Lambda = \sum_{r=0}^{q-j-1} \frac{(q-j-1)!(-1)^{G-\beta+q-j-r}\bar{\gamma}_E^{p-q+j+r}(n_1(2^R-1))^{G-\beta+q-j-r}}{\bar{\gamma}_i^{p-q+j+r} r!(n_1 2^R)^{q-j-r}(G-\beta+q-j-r)!}. \quad (39)$$

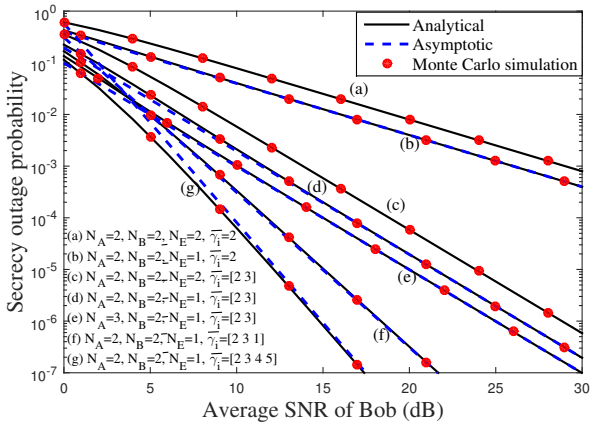

Fig. 2. Secrecy outage probability versus Bob's average SNR assuming MRC scheme at Bob ($\bar{\gamma}_E = -2$dB; $R = 1$).

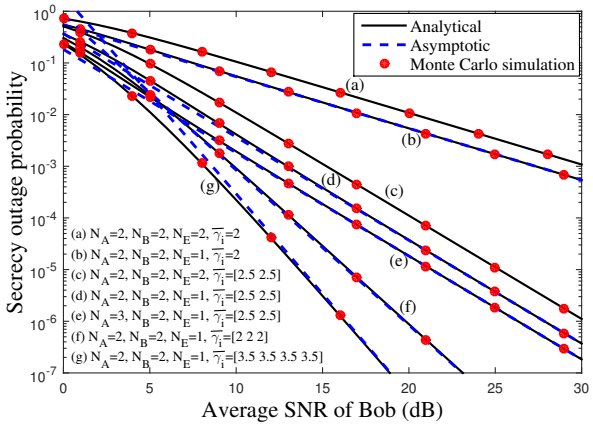

Fig. 3. Secrecy outage probability versus Bob's average SNR assuming SC scheme at Bob ($\bar{\gamma}_E = -2$dB; $R = 1$).

jamming signals at Eve. In other words, regardless the number of antennas at Alice and Bob, the diversity is limited by the number of jamming signals at Eve. Hence, we can conclude that interference at Eve is not always beneficial for the secrecy performance unless the number of jamming signals are higher than or equal to the product of the number of antennas at Alice and Bob. It is noteworthy that, although the analysis was carried assuming $N_E = 1$, it will be observed in the next section that this behavior is maintained for general cases such that the diversity gain remains to be $G_D = \min(M, N_A N_B)$.

V. Numerical Results and Discussions

In this Section, representative numerical results are presented in order to evaluate the performance of the proposed scenario. Our analysis is corroborated by means of Monte Carlo simulations[6]. Different antenna configurations, interference powers and average SNRs are considered with the intention of studying the secrecy performance over the whole range. In all the plots, we assume $R = 1$.

Figs. 2 and 3 depict the secrecy outage probability versus Bob's average SNR assuming MRC and SC at Bob, respectively. Observe that both MRC and SC schemes follow the same behavior, however the former scheme outperforms the second one. In fact, it is noticed that the MRC scheme has approximately 1dB gain over SC scheme at 10^{-6}. Focusing on Fig. 2, remarks regarding the secrecy outage performance and diversity order will be provided[7]. Firstly, it is observed from curves (a) and (b) that the diversity gain equals to 1 due to the fact that number of jamming signals are equal to one. One can also notice that curve (a) is plotted for $N_E = 2$ and curve (b) assumes $N_E = 1$, which shows that the diversity gain is not effected by N_E, although we observe a secrecy outage probability improvement with the decrease of N_E. The curves (c), (d) and (e) are plotted for different antenna configuration, while fixing the number of jamming signals to two, which results in diversity gain to be equal to 2. Note also that just increasing N_A does not increase the diversity gain, as seen in curve (e). In curves (f) and (g), we set the number of jamming signals to 3 and 4, respectively, while keeping $N_A = N_B = 2$. Note that the diversity gain of 3 is observed for curve (f) and a diversity gain of 4 for curve (g), as expected since the diversity gain expression was determined as $\min(N_A N_B, M)$.The diversity gain claims are also verified by plotting asymptotic curves which show to be compatible with the analytical ones. In addition, Monte Carlo simulations are performed to corroborate the accuracy of our analytical results.

Fig. 4 shows the secrecy outage probability versus Bob's average SNR, highlighting the effect of different jamming signals arriving at Eve. We set $N_A = 2$, $N_B = 2$, and $N_E = 1$. Both MRC and SC cases are plotted and, as expected, MRC scheme outperforms the latter one. Equal power jamming signals and distinct power jamming signals are plotted. It is noticed that both equal power and distinct power distribution of interference have the same performance when they have the same number of jamming signals and when the sum of the average interference powers are equal. This observation is of paramount importance and it allows us to conclude that, for a given general system, we can use the simplified equal power distributed interference scenario for evaluating the secrecy performance. Again, Monte Carlo simulations are coincident with the analytical curves, which corroborate our results.

In order to show the diversity gain variation in different configurations, Fig. 5 plots the ratio D =

[6]We consider $\mathbf{h}_{\mathrm{AB},k}$ to be a N_B dimensional random variable vector and we modeled each random variable using Rayleigh fading distribution in our simulations. Similarly, elements of $\mathbf{h}_{\mathrm{AB},s}$ vector is modeled as Rayleigh distributed random variables. Further, elements of γ_I is obtained by arbitrary weighted gamma distribution. By obtaining these random values, the Monte Carlo simulations were performed for large number iterations to get accurate results.

[7]Nonetheless, it is noteworthy that these observations can also be applied for the SC case (shown in Fig. 3).

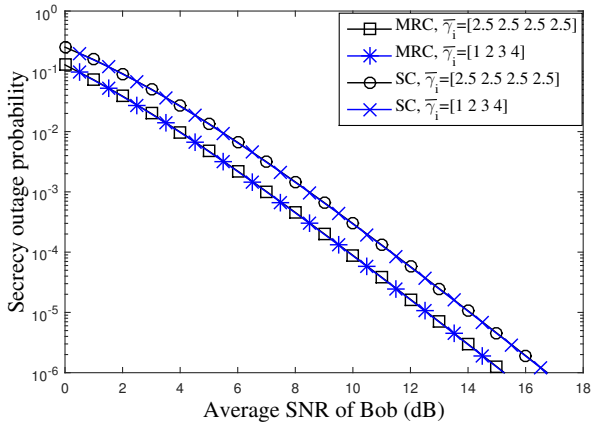

Fig. 4. Secrecy outage probability versus Bob's average SNR for different combining schemes and interference configurations ($\bar{\gamma}_E = -2$dB and $R = 1$).

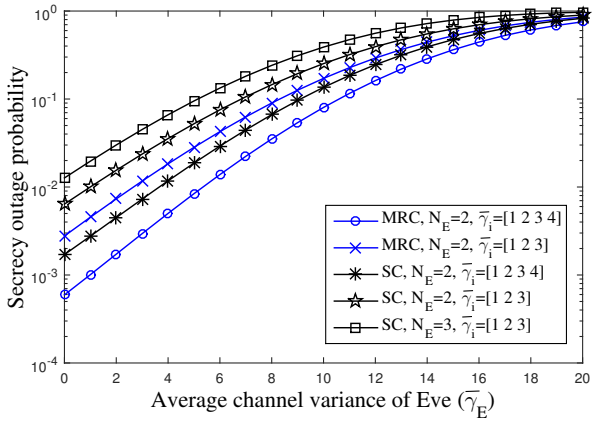

Fig. 6. Secrecy outage probability versus average channel variance of Eve ($N_A = N_B = 2$ and $\bar{\gamma}_B = 10$dB).

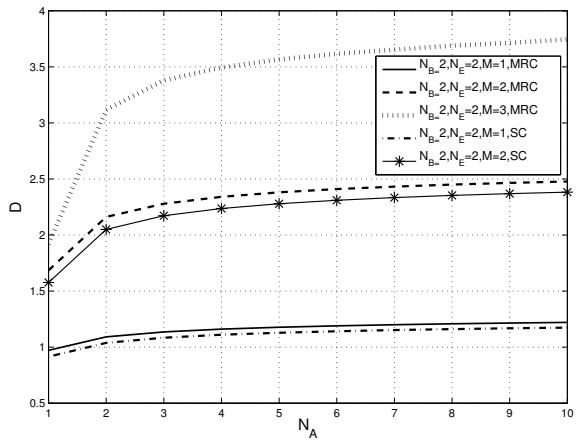

Fig. 5. The ratio of $D = -\log_{10}(P_s(R))/\log_{10}(\bar{\gamma}_B)$ versus the number of antennas at Alice to illustrate the diversity. $\bar{\gamma}_B = 25$dB; $\bar{\gamma}_E = -5$dB; $R = 1$; for $M = 1, 2, 3$, we used $\bar{\gamma}_i = \{(0.3), (0.3, 0.4), (0.3, 0.4, 0.2)\}$dB, respectively.

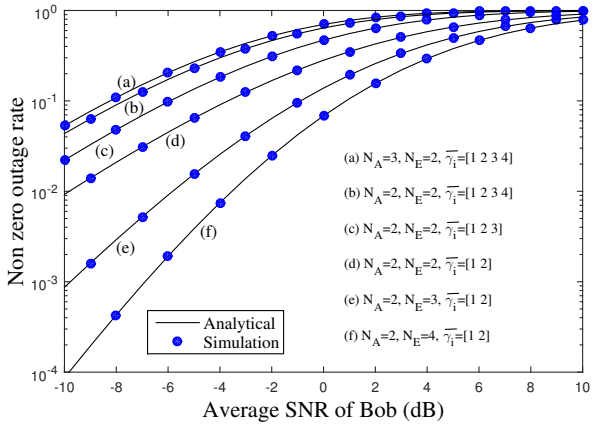

Fig. 7. Probability of non-zero secrecy rate versus Bob's average SNR for MRC scheme ($N_B = 3$ and $\bar{\gamma}_E = 10$dB).

$-\log_{10}(P_s(R))/\log_{10}(\bar{\gamma}_B)$ versus N_A. Both MRC and SC schemes are considered and the higher coding gain in MRC scheme than SC can be easily seen. Importantly, we notice that although N_A increases, the ratio D saturates to one level. From the bottom most curve, note that the diversity gain equals 1 due to the fact that $M = 1$, although $N_A N_B$ increases. The additional loss at low N_A and the additional gain at high N_A are due to the array gain. Similar observations can be acquired in the middle plots ($N_B = 2, M = 2$) in which the diversity gain remains 2 with the increase of N_A. It is noteworthy that the topmost curve has a diversity gain of 2 when $N_A = 1$ and it increases to 3 when N_A increases. This is due to the fact that, when $N_A = 1$ we have $N_A N_B = 2$ and $M = 3$, hence the diversity equals to 2. However, when N_A increases, the diversity is governed by M such that it remains 3.

Fig. 6 plots the secrecy outage probability versus average channel variance of Eve for both MRC and SC schemes. As expected, we observe an increase of secrecy performance when: (a) the number of jamming signals increases; (b) the Eve's average SNR decreases; and/or (c) the number of antennas at Eve decreases. Furthermore, one can notice that the secrecy outage probability converges to 1 when Eve's average SNR increases beyond Bob's average SNR (which is fixed to 10dB).

The probability of non-zero secrecy rate versus Bob's average SNR is plotted in Figs. 7 and 8 for MRC and SC schemes, respectively. Apart from larger non-zero secrecy rate probability for the MRC scheme, as seen by comparing Figs. 7 and 8, the performance follows the same behavior. In addition, from curves (a) and (b), it is observed that the decrease of N_A implies in a decrement of the non-zero secrecy rate probability, however this gap is rather small when compared to the case where the number of jamming signals decreases, as seen in curve (c). By fixing the number of jamming signals to 2, we plot the curve (d), (e) and (f) for different N_E. From these three curves, observe a significant decrease of non-zero secrecy rate probability with the increase of number of antennas at Eve.

VI. Conclusions

We have investigated the secrecy performance of MIMO wiretap channels with TAS in an interference-limited eavesdropper. Two receiver combining schemes, i.e. MRC and SC, were considered at the legitimate user, while only a

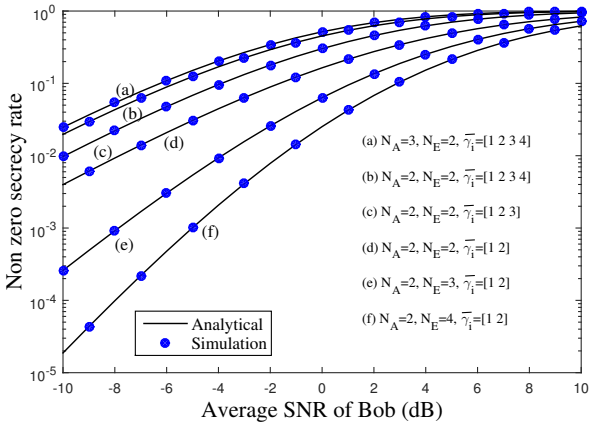

Fig. 8. Probability of non-zero secrecy rate versus Bob's average SNR for SC scheme ($N_B = 3$ and $\bar{\gamma}_E = 10$dB).

MRC scheme was employed at the eavesdropper. Closed-form expressions for the secrecy outage probability and nonzero secrecy rate were derived and they allowed for arbitrary power distributed jamming signals. An asymptotic analysis was carried and our results showed that the diversity order equals to $\min(M, N_A N_B)$. This allowed us to conclude that the number of jamming signals arrived at the eavesdropper limits the secrecy performance via diversity such that a higher number of antennas does not necessarily imply in a diversity improvement, unless for a large number of jamming signals.

APPENDIX A

The secrecy outage probability can be mathematically written as

$$P_s(R) = \Pr\left(\frac{1+\gamma_B}{1+\frac{\gamma_E}{\gamma_I}} < 2^R\right) \Pr\left(\gamma_B > \frac{\gamma_E}{\gamma_I}\right) + \Pr\left(\gamma_B < \frac{\gamma_E}{\gamma_I}\right). \quad (48)$$

Thus, by using the concepts of probability theory, (48) can be rewritten as

$$P_s(R) = F_{\frac{1+\gamma_B}{1+\frac{\gamma_E}{\gamma_I}}}(2^R) = \int_1^\infty F_{1+\gamma_B}(2^R x) f_{1+\frac{\gamma_E}{\gamma_I}}(x)dx = \int_0^\infty F_{\gamma_B}(2^R x + 2^R - 1) f_{\frac{\gamma_E}{\gamma_I}}(x)dx. \quad (49)$$

In order to provide a closed-form solution to (49), we first derive $f_{\frac{\gamma_E}{\gamma_I}}(x)$ as

$$f_{\frac{\gamma_E}{\gamma_I}}(x) = \frac{\partial}{\partial x}\left[\int_0^\infty F_{\gamma_E}(xz) f_{\gamma_I}(z)dz\right]. \quad (50)$$

Then, making use of the CDF of γ_E and the PDF of γ_I given in (19), it follows that

$$f_{\frac{\gamma_E}{\gamma_I}}(x) = \sum_{u=0}^{N_E-1} \frac{1}{u!} \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!} \left(\frac{\bar{\gamma}_I}{\bar{\gamma}_E}\right)^u x^{u-1} \times \left(\frac{x\bar{\gamma}_I}{\bar{\gamma}_E} + 1\right)^{-u-j-1} \left(j\frac{x\bar{\gamma}_I}{\bar{\gamma}_E} - u\right). \quad (51)$$

Now, by substituting (14) and (51) in (49), and performing the required integration with the help of [30, 9.211.4], the secrecy outage probability for MRC scheme can be attained as in *Theorem 1*. Similarly, we use the CDF of γ_B^{sc} and $f_{\frac{\gamma_E}{\gamma_I}}(x)$ to derive the secrecy outage probability for the SC scheme, as given in *Theorem 2*.

REFERENCES

[1] D. B. da Costa, N. S. Ferdinand, U. S. Dias, R. T. de Sousa Jr, and M. Latva-aho, "MIMO wiretap channels with multiple jamming signals: a secrecy outage performance analysis," in *XXXIII Brazilian Telecommun. Symp. (SBrT'15)*, Sep. 2015, pp. 1–5.

[2] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[3] E. Silva, A. Dos Santos, L. Albini, and M. Lima, "Identity-based key management in mobile ad hoc networks: techniques and applications," *IEEE Wireless Commun.*, vol. 15, no. 5, pp. 46–52, 2008, doi: 10.1109/MWC.2008.4653131.

[4] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, 1998, doi: 10.1109/2.708447.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008, doi: 10.1109/TIT.2008.921908.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Int. Symp. Inform. Theory*, 2006, pp. 356–360, doi: 10.1109/ISIT.2006.261613.

[7] R. Liu, I. Maric, P. Spasojević, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008, doi: 10.1109/TIT.2008.921879.

[8] A. D. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[9] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *IEEE Int. Symp. Inf. Theory*, 2007, pp. 2466–2470, doi: 10.1109/ISIT.2007.4557589.

[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas – Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010, doi: 10.1109/TIT.2010.2068852.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011, doi: 10.1109/TIT.2011.2158487.

[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, 2009, doi: 10.1109/TIT.2009.2018322.

[13] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forens. Secur.*, vol. 7, no. 2, pp. 704–716, 2012, doi: 10.1109/TIFS.2011.2181946.

[14] J. Li and A. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, 2011, doi: 10.1109/TWC.2011.011811.100356.

[15] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, 2011, doi: 10.1109/TSP.2010.2078810.

[16] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Techcnol.*, vol. 62, no. 5, pp. 2140–2155, 2013, doi: 10.1109/TVT.2012.2230657.

[17] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, 2011, doi: 10.1109/LCOMM.2011.030911.102343.

[18] V. Prabhu and M. Rodrigues, "On wireless channels with m-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forens. Sec.*, vol. 6, no. 3, pp. 853–860, 2011, doi: 10.1109/TIFS.2011.2159491.

[19] M. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *43rd Asilomar Conf. Sig. Comp.*, 2009, pp. 829–833, doi: 10.1109/ACSSC.2009.5469979.

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

[21] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and I. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, 2013, doi: 10.1109/TCOMM.2012.12.110670.

[22] N. Yang, H. Suraweera, I. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forens. Sec.*, vol. 8, no. 1, pp. 254–259, 2013, doi: 10.1109/TIFS.2012.2223681.

[23] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, 2013, doi: 10.1109/LCOMM.2013.040213.122696.
[24] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, 2011, doi: 10.1109/TIT.2011.2121450.
[25] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008, doi: 10.1109/TIT.2008.921680.
[26] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *IEEE Int. Symp. Inf. Theory*, 2008, pp. 2217–2221, doi: 10.1109/ISIT.2008.4595384.
[27] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, 2010, doi: 10.1109/TVT.2010.2059057.
[28] J. Vilela, P. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Trans. Inf. Forens. Sec.*, vol. 6, no. 3, pp. 616–627, 2011, doi: 10.1109/TIFS.2011.2142305.
[29] Y. Liu and A. Petropulu, "Destination assisted cooperative jamming for wireless physical layer security," in *IEEE Int. Work. Inf. Forens. Sec.(WIFS)*, 2012, pp. 282–287, doi: 10.1109/WIFS.2012.6412663.
[30] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed., San Diego, CA: Academic, 2007.
[31] N. Ferdinand and N. Rajatheva, "Unified performance analysis of two-hop amplify-and-forward relay systems with antenna correlation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3002–3011, 2011, doi: 10.1109/TWC.2011.072511.101783.

Daniel Benevides da Costa was born in Fortaleza, Ceará, Brazil, in 1981. He received the B.Sc. degree in Telecommunications from the Military Institute of Engineering, Rio de Janeiro, Brazil, in 2003 and the M.Sc. and Ph.D. degrees in Telecommunications from the University of Campinas, Campinas, Brazil, in 2006 and 2008, respectively. His Ph.D. dissertation was awarded the Best Ph.D. Thesis in Electrical Engineering by the Brazilian Ministry of Education (CAPES) at the 2009 CAPES Thesis Contest. From 2008 to 2009, he was a Postdoctoral Research Fellow with INRS-EMT, University of Quebec, Montreal, QC, Canada. At that time, he was the recipient of two scholarships: 1) the Merit Scholarship Program for Foreign Students in Quebec and 2) the Natural Sciences and Engineering Research Council of Canada Postdoctoral Scholarship. Since 2010, he has been with the Federal University of Ceará, Brazil, where he is currently an Assistant Professor.

Prof. da Costa has authored or coauthored more than 70 journal papers, more than 50 papers in international conferences, and 2 book chapters. His research interests lie in the area of wireless communications and include channel modeling and characterization, relaying/multihop/mesh networks, cooperative systems, cognitive radio networks, physical layer security, energy harvesting systems, free-space optical communications, and performance analysis/design of multiple-input multiple-output systems. He is currently an Editor of the IEEE Communications Letters, IEEE Transactions on Vehicular Technology, EURASIP Journal on Wireless Communications and Networking, and the KSII Transactions on Internet and Information Systems. He has also served as Associate Technical Editor for the IEEE Communications Magazine. In the past, he served as the Lead Guest Editor for EURASIP Journal on Wireless Communications and Networking in the Special Issue on "Cooperative Cognitive Networks", Lead Guest Editor for KSII Transactions on Internet and Information Systems in the Special Issue on "Cognitive Radio Networks: Survey, Tutorial, and New Introduction", and a Guest Editor for IET Communications in the Special Issue on "Secure Physical Layer Communications". Also, he was the Workshop Chair of the 2nd International Conference on Computing, Management and Telecommunications (ComManTel 2014) and he served as the TPC chair for the IEEE GLOBECOM 2013, Workshop on "Trusted Communications with Physical Layer Security". Currently, he serves as the Lead Guest Editor for IEEE Access Journal in the Special Issue on "Security in Wireless Communications and Networking". He also acts as a reviewer for major international journals of the IEEE and IET, and he has been Member of the Technical Program Committee of several international conferences, such as ICC, WCNC, GLOBECOM, PIRMC, and VTC. He is currently a Scientific Consultant of the National Council of Scientific and Technological Development (CNPq), Brazil, and of the Brazilian Ministry of Education (CAPES). He is also a Productivity Research Fellow of CNPq. From 2010 to 2012, he was a Productivity Research Fellow of the Ceará Council of Scientific and Technological Development (FUNCAP). Currently, he is a member of the Advisory Board of FUNCAP, Area: Telecommunications. Prof. da Costa is the recipient of three conference paper awards: one at the 2009 IEEE International Symposium on Computers and Communications, one at the 13th International Symposium on Wireless Personal Multimedia Communications in 2010, and another at the XXIX Brazilian Telecommunications Symposium in 2011. In 2013, he received the Exemplary Reviewer Certificate of the IEEE Wireless Communications Letters and the Certificate of Appreciation of Top Associate Editor for outstanding contributions to IEEE Transactions on Vehicular Technology. He is a Senior Member of IEEE, Member of IEEE Communications Society, IEEE Vehicular Technology Society, and Brazilian Telecommunications Society.

Nuwan Suresh Ferdinand received the B.Sc. degree in electronics and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2009 and the M.Eng. degree from Asian Institute of Technology, Thailand, in 2011. He is currently pursuing the Ph.D. degree at the Centre for Wireless Communications, University of Oulu, Finland. His research interests are communication theory, information theory, coding theory and their applications to wireless communication.

Ugo Silva Dias was born in Belém, Brazil, in 1981. He obtained the B.S. degree in Electrical Engineering from the Federal University of Para, Brazil. He received the M.Sc. and Ph.D. degrees in Electrical Engineering from the State University of Campinas, Brazil, in 2006 and 2010, respectively. From 2004 to 2010, he was a member of the Wireless Technology Laboratory (WissTek), where he worked researching advanced mobile systems, field measurements, and generalized fading channels. Besides the academic experience, Dr. Dias also worked in several companies in the ICT industry. Since March 2010, Ugo Dias is Professor at University of Brasilia (UnB), Brazil. He is a faculty member of the Department of Electrical Engineering and Latitude Lab. His research interest include fading channels, field measurements, cell networks, and wireless technologies in general. Prof. Dias is also chair of IEEE ComSoc Chapter of Centro-Norte Brasil Section, IT director of Brazilian Telecommunications Society, and Advisor of Brazilian Internet Steering Committee.

Rafael Timóteo de Sousa Júnior was born in Campina Grande - PB, Brazil, on June 24, 1961. He graduated in Electrical Engineering from the Federal University of Paraíba - UFPB, Campina Grande - PB, Brazil, 1984, and got his Doctorate Degree in Telecommunications from the University of Rennes 1, Rennes, France, 1988. He worked as a software and network engineer in the private sector from 1989 to 1996. Since 1996, he is a Network Engineering Professor in the Electrical Engineering Department, at the University of Brasília, Brazil. From 2006 to 2007, he took a sabbatical year in the Group for the Security of Information Systems and Networks, at Ecole Superiéure d´Electricité, Rennes, France. He is a member of the Post-Graduate Program on Electrical Engineering (PPGEE) and supervises the Decision Technologies Laboratory (LATITUDE) of the University of Brasília. His field of study is distributed systems, network management and information security.

Matti Latva-aho was born in Kuivaniemi, Finland in 1968. He received the M.Sc., Lic.Tech. and Dr. Tech (Hons.) degrees in Electrical Engineering from the University of Oulu, Finland in 1992, 1996 and 1998, respectively. From 1992 to 1993, he was a Research Engineer at Nokia Mobile Phones, Oulu, Finland. During the years 1994 - 1998 he was a Research Scientist at Telecommunication Laboratory and Centre for Wireless Communications (CWC) at the University of Oulu. Prof. Latva-aho was Director of Centre for Wireless Communications (CWC) at the University of Oulu during the years 1998-2006. He is Professor of Digital Transmission Techniques at the University of Oulu since 2000 and currently Director of CWC Radio Technologies research unit. His research interests are related to mobile broadband communication systems and currently his group focuses on 5G systems research. Prof. Latva-aho has published 300+ conference or journal papers in the field of wireless communications. He has been TPC Chairman for PIMRC'06, TPC Co-Chairman for ChinaCom'07 and General Chairman for WPMC'08, CROWNCOM'14 and will be organizer for EUCNC'17 in Oulu. He acted as the Chairman and vice-chairman of IEEE Communications Finland Chapter in 2000 - 2003. Prof. Latva-aho has received the following prizes: 2015 Nokia Foundation Award, 2003 IEE Mountbatten Premium Award, 2000 Electrical Engineering Foundation Finland (EIS) Award, 1998 Best doctoral thesis prize of technical sciences in Finland. Prof. Latva-aho is a member of Finnish Academy of Technology since 2011.