PHY Security of MIMO Wiretap Channels with Generalized Selection Combining

Lucas M. Vasconcelos, Yosbel R. Ortega, Daniel B. da Costa, Rafael T. de Sousa Jr., and William F. Giozza

***Abstract*— This paper investigates the secrecy outage performance of multiple-input multiple-output (MIMO) wiretap channels, where a generalized selection combining (GSC) scheme is assumed at the legitimate receiver, while the transmitter employs a transmit antenna selection (TAS) technique and the eavesdropper adopts a maximal-ratio combining (MRC) scheme. Assuming that the eavesdropper is subject to noise and jamming, a closed-form expression for the secrecy outage probability is derived, based on which the diversity and array gains are determined after performing an asymptotic analysis. The derived expression allows for arbitrary power distributed jamming signals, and are simplified to two special cases, i.e., distinct and equal power distributed jamming signals. Some representative numerical results are depicted to show the effects of the key system parameters on the secrecy performance. Finally, the proposed analysis is corroborated through Monte Carlo simulations.**

***Keywords*— Secrecy outage performance, generalized selection combining, MIMO wiretap channels, jamming signals, transmit antenna selection.**

I. Introduction

Security has arisen as a major concern in wireless communications due to the broadcast nature of the propagation medium, which makes the communication vulnerable to attacks of malicious nodes [1]. Traditionally, security has been addressed through cryptography approaches implemented at higher levels of the protocol stack [2], [3], which rely on the limited computational capacity of the eavesdroppers. However, with the advent of infrastructureless networks, the secret key management has become a hard task. In light of this, a new approach for ensuring the information secrecy has emerged on the literature [4]–[6], called physical layer (PHY) security. As its name implies, the idea is to implement security at the PHY by exploring the spatial-temporal characteristics of the wireless channel.

Along the last years, the PHY security of wireless networks has been widely investigated from different perspectives. In particular, turning our attention to the outage performance, [7]–[11] carried out a comprehensive analysis. In [7], the authors proposed an efficient transmit antenna selection (TAS) scheme which revealed that high levels of security can be achieved when the number of antennas at the transmitter (Tx) increases, even when the eavesdropper has multiple antennas. The work of [7] was generalized in [8] assuming that all nodes are equipped with multiple antennas. In [9], the impact of antenna correlation on the secrecy outage performance was examined and insightful conclusions were drawn. For instance, it was shown that when the average signal-to-noise ratio (SNR) of the main channel is at low level, higher correlation at the eavesdropper offers more beneficial effects on secrecy than higher correlation at the legitimate receiver (Rx). In [10], assuming a multiple-input multiple-output (MISO) wiretap channel with a TAS scheme at the Tx, the effects of the outdated channel state information (CSI) on the secrecy outage performance was examined. It was shown that the expected diversity gain cannot be realized when CSI is outdated during the antenna selection process. More recently, considering an interference-limited [11] eavesdropper scenario, the secrecy performance of multiple-input multiple-output (MIMO) wiretap channels was investigated. The results revealed that the diversity gain equals to $\min(M, N_{\mathrm{A}}N_{\mathrm{B}})$, with M denoting the number of jamming signals, and N_{A} and N_{B} being, respectively, the number of antennas at the Tx and legitimate Rx. Common to the aforementioned works is that the legitimate Rx employed either a maximal-ratio combining (MRC) or a selection combining (SC) scheme. Differently from these works, [12] proposed a TAS scheme with generalized selection combining (GSC) strategy at the legitimate Rx. Basically, the system works as follows: a single antenna out of N_{A} antennas is selected at the Tx, while L_{B} antennas out of N_{B} antennas are combined at the legitimate Rx. Note that GSC can be seen as a general case of MRC ($L_{\mathrm{B}} = N_{\mathrm{B}}$) and SC ($L_{\mathrm{B}} = 1$). However, one of the drawbacks of [12] is that the eavesdropper was assumed to be subject only to additive white gaussian noise (AWGN). As we may know, in practical systems, the use of jamming signals to distract eavesdroppers reception has been widely employed.

This paper aims to generalize the results of [11] and [12] by assuming that the eavesdropper is affected by noise and jamming signals. A closed-form expression for the secrecy outage probability is derived, based on which the diversity and array gains are determined after performing an asymptotic analysis. The derived expression allows for arbitrary power distributed jamming signals. Some representative numerical results are depicted to show the effects of the key system parameters on the secrecy performance. Finally, the proposed analysis is corroborated through Monte Carlo simulations.

L. M. Vasconcelos, Y. R. Ortega, and D. B. da Costa are with the Federal University of Ceará (UFC), Brazil. E-mails:{lcvmagalhaes@gmail.com, yosbel@gtel.ufc.br, danielbcosta@ieee.org}.

R. T. de Sousa Jr. and W. F. Giozza are with the Department of Electrical Engineering, University of Brasília, Brazil. E-mails:{desousa, giozza}@unb.br.

The authors wish to thank the Brazilian research, development and innovation Agencies CAPES (Grant FORTE 23038.007604/2014-69), FAPDF (Grant 11454.54.34054.17052016), and the National Consumer Secretariat - SENACON - of the Brazilian Ministry of Justice (Project TED 001/2015), for their support to this work.

II. System Model and Useful Statistics

Let a MIMO wiretap channel composed by a Tx, called Alice, a Rx, called Bob, and an eavesdropper, called Eve, which are equipped with $N_{\rm A}$, $N_{\rm B}$ and $N_{\rm E}$ antennas, respectively. A TAS scheme is employed at Alice, a GSC scheme is adopted at Bob, and Eve uses a MRC technique. Alice sends data to Bob while Eve tries to hear the information exchange. It is assumed that Eve suffers from both AWGN component and jamming signals. As in [11] and references therein, we assume a friendly jammer which has full secure cooperation with Bob and causes interference at Eve. The Alice-Bob channel and the wiretap channel are assumed to be independent and experience Rayleigh 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 SNR of Bob. In addition, we assume that Bob holds full cooperation with the friendly jammer such that it is able to completely cancel out any jamming signal coming from friendly jammer or himself.

A. TAS at Alice and GSC at Bob

Alice selects the transmit antenna in order to maximize the received SNR at Bob, where this latter employs a GSC scheme [12] such that the $L_{\rm B}$ strongest antennas out of the $N_{\rm B}$ available ones are combined. Based on the rules of GSC, let $|h^1_{{\rm AB},k}|^2 \geq |h^2_{{\rm AB},k}|^2 \geq \ldots \geq |h^{N_{\rm B}}_{{\rm AB},k}|^2$ be the order statistics from arranging $\{|h^{l_{\rm B}}_{{\rm AB},k}|\}_{l_{\rm B}=1}^{N_{\rm B}}$ in descending order of magnitude. In this case, we denote $\mathbf{h}_{{\rm AB},k} = [h^1_{{\rm AB},k}, h^2_{{\rm AB},k} \ldots h^{N_{\rm B}}_{{\rm AB},k}]^T$ as the $N_{\rm B} \times 1$ channel vector between Bob and the kth antenna at Alice, with $(\cdot)^T$ symbolizing the transpose operation. Combining the first $L_{\rm B}$ ($1 \leq L_{\rm B} \leq N_{\rm B}$) variables in order statistics, Bob attains $\theta_k = \sum_{l_{\rm B}=1}^{L_{\rm B}} |h^{l_{\rm B}}_{{\rm AB},k}|^2$. Thus, the transmit antenna s selected by Alice is performed according to $s = \arg\max_{k\in\{1,\ldots N_{\rm A}\}}\{\theta_k\}$. Consequently, the instantaneous SNR at the GSC output is given by

$$\gamma_{{\rm B},s} = \sum_{l_{\rm B}=1}^{L_{\rm B}} \gamma_{(l_{\rm B})}, \tag{1}$$

where $\gamma_{(1)} \geq \gamma_{(2)} \geq \ldots \geq \gamma_{(N_{\rm B})}$ are the order statistics from arranging $\{\gamma_{(l_{\rm B})} = |h^{l_{\rm B}}_{{\rm AB},s}|^2 P/\sigma_b^2\}_{l_{\rm B}=1}^{N_{\rm B}}$ in descending order of magnitude. Herein, P denotes the transmit power at Alice and σ_b^2 means the variance of each noise entry pertaining to the AWGN vector arriving at Bob. From [12, Eq. (1)], the cumulative distribution function (CDF) of $\gamma_{{\rm B},s}$ can be determined as

$$F_{\gamma_{{\rm B},s}}(x) = \sum_{S_k\in S} \alpha_k x^{\beta_k} e^{\frac{-\delta_k x}{\bar{\gamma}_{\rm B}}}, \tag{2}$$

where $\bar{\gamma}_{\rm B} = P/\sigma_b^2$, $S = \left\{S_k | \sum_{n=0}^{N} n_{k,n} = N_{\rm A}\right\}, \{n_{k,n}\} \in \mathbb{Z}^+$ and, α_k, β_k, and δ_k are expressed in [12, Eqs. (2), (3), and (4)], respectively.

B. MRC at Eve

Since Eve is affected by both noise and jamming signals, its received signal can be written as

$$y_{\rm E} = \sqrt{P}\mathbf{h}_{{\rm AE,s}}x + \sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\mathbf{h}_{\rm i} + \mathbf{n}_{\rm E}, \tag{3}$$

where $\mathbf{h}_{\rm AE,s}$ represents the $N_{\rm E} \times 1$ channel vector between Eve and the selected antenna at Alice, $\mathbf{h}_i$ stands for the $N_{\rm E} \times 1$ channel vector between Eve and the ith jamming signal, $\bar{\gamma}_i$ denotes the interference power of the ith jamming signal, x stands for the signal transmitted by Alice, and $\mathbf{n}_{\rm E}$ denotes the AWGN $N_{\rm E} \times 1$ channel vector whose entries have unit variances. Following a similar rationale as employed in [11], it can be shown that the the received signal-to-interference-plus-noise ratio (SINR) at Eve can be expressed as

$$\Upsilon_{{\rm E},s} = \frac{\gamma_{{\rm E},s}}{\gamma_I + 1}, \tag{4}$$

where $\gamma_{{\rm E},s} = \bar{\gamma}_{\rm E}||\mathbf{h}_{\rm AE,s}||^2$, $\gamma_I = \sum_{i=1}^{M} \bar{\gamma}_i|\tilde{h}_i|^2$, and $\bar{\gamma}_{\rm E}$ means the channel variance, with $\tilde{h}_i = \frac{\mathbf{h}^{\dagger}_{\rm AE,s}}{\|\mathbf{h}_{\rm AE,s}\|}\mathbf{h}_i$, $||\cdot||$ indicating the Frobenius norm and $(\cdot)^{\dagger}$ denoting the conjugate transpose. In the subsequent analysis, the probability density function (PDF) of $\Upsilon_{{\rm E},s}$ is required, which can be written as

$$f_{\Upsilon_{{\rm E},s}}(x) = \frac{\partial}{\partial x}\left[\int_0^{\infty} F_{\gamma_{{\rm E},s}}(xz) f_{\gamma_I+1}(z)dz\right], \tag{5}$$

in which $F_{\gamma_{{\rm E},s}}(\cdot)$ denotes the CDF of $\gamma_{{\rm E},s}$ and $f_{\gamma_I+1}(\cdot)$ means the PDF of $\gamma_I + 1$. The former can be obtained from [11, Eq. (12)] after replacing $N_{\rm B}$ and $\bar{\gamma}_{\rm B}$ by $N_{\rm E}$ and $\bar{\gamma}_{\rm E}$, respectively, while the PDF of $\gamma_I + 1$ can be attained from [11, Eq. (19)] after performing the statistical procedure of transformation of variates, being given by

$$f_{\gamma_I+1}(z) = \sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{(j-1)!\bar{\gamma}_i^j} \sum_{k=1}^{j}\sum_{p=1}^{k} \binom{j-1}{k-1}\binom{k-1}{p-1} z^{p-1} e^{-\frac{z}{\bar{\gamma}_i}}, \tag{6}$$

where

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)!\bar{\gamma}_i^{\eta_i - j}} \frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}} \left[\prod_{k=1,k\neq i}^{t} \left(\frac{1}{1+s\bar{\gamma}_k}\right)^{\eta_k}\right]_{s=-\frac{1}{\bar{\gamma}_i}}. \tag{7}$$

Finally, after making the appropriate substitutions, a closed-form expression for the PDF of $\Upsilon_{{\rm E},s}$ can de derived as

$$\begin{aligned} f_{\Upsilon_{{\rm E},s}}(x) = &\sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \Omega_{i,j} \sum_{k=1}^{j}\sum_{p=1}^{k} (-1)^{j-k} \sum_{u=0}^{N_{\rm E}-1} \\ &\times \sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j}}{(j-k)!(k-p)!(p-1)!(u-q)!q!} \\ &\times \left(\frac{x}{\bar{\gamma}_{\rm E}}\right)^u e^{-\frac{x}{\bar{\gamma}_E}} \left[(p+q)\frac{\bar{\gamma}_i}{\bar{\gamma}_{\rm E}}\left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_{\rm E}}\right)^{-p-q-1}\right. \\ &\left. + \frac{1}{\bar{\gamma}_{\rm E}}\left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_{\rm E}}\right)^{-p-q} - ux^{-1}\left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_{\rm E}}\right)^{-p-q}\right]. \end{aligned} \tag{8}$$

III. Secrecy Outage Performance

A. Achievable Secrecy Rate

Let the capacity of the Alice-Bob (main) channel be $R_{\mathrm{B},s} = \log_2(1+\gamma_{\mathrm{B},s})$ and the capacity of the eavesdropper (wiretap) channel be $R_{\mathrm{E},s} = \log_2(1+\Upsilon_{\mathrm{E},s})$. Thus, the secrecy capacity can be defined as

$$R_S = \begin{cases} R_{\mathrm{B},s} - R_{\mathrm{E},s}, & \gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}, \\ 0, & \gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s}. \end{cases} \tag{9}$$

B. Secrecy Outage Probability

In our context, an outage event occurs when either the main channel is in outage or when Eve can intercept the information exchange between Alice and Bob. In particular, the secrecy outage probability can be defined as the probability that R_S drops below a predefined threshold rate R, being mathematically expressed as

$$\begin{aligned} P_s(R) &= \Pr(R_S < R) \\ &= \Pr\left(\frac{1+\gamma_{\mathrm{B},s}}{1+\Upsilon_{\mathrm{E},s}} < 2^R\right) \Pr\left(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}\right) \\ &\quad + \Pr\left(\gamma_{\mathrm{B},s} < \Upsilon_{\mathrm{E},s}\right), \end{aligned} \tag{10}$$

where $\Pr(\cdot)$ denotes probability. Based on [9, Eqs. (9)-(12)] and after some algebraic manipulations, (10) can be rewritten as

$$\begin{aligned} P_s(R) &= F_{\frac{1+\gamma_{\mathrm{B},s}}{1+\Upsilon_{\mathrm{E},s}}}(2^R) = \int_1^\infty F_{1+\gamma_{\mathrm{B},s}}(2^R x) f_{1+\Upsilon_{\mathrm{E},s}}(x)dx \\ &= \int_0^\infty F_{\gamma_{\mathrm{B},s}}(2^R x + 2^R - 1) f_{\Upsilon_{\mathrm{E},s}}(x)dx. \end{aligned} \tag{11}$$

By replacing (2) and (8) into (11), and performing the required integral with the help of [13, Eq. (9.211.4)], a closed-form expression for the secrecy outage probability can be derived as (13), shown at the top of the next page, where $\Psi(\cdot,\cdot,\cdot)$ denotes the Tricomi's (confluent hypergeometric) function [13, Eq. (9.211.4)] and Θ_1 is given by

$$\Theta_1 = \begin{cases} \Psi\left(u+f, u+f+1-p-q, \frac{1}{\bar{\gamma}_i} + \frac{\delta_k \bar{\gamma}_{\mathrm{E}} 2^R}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_i}\right)\Gamma(u+f) \\ \times\left(\frac{\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_i}\right)^{u+f} u, \quad u \neq 0 \\ 0, \quad u = 0 \end{cases} \tag{12}$$

Our result in (13) can be simplified to two special cases. Firstly, assuming $\bar{\gamma}_1 = \bar{\gamma}_2 = ... = \bar{\gamma}_M$, (13) can be simplified for the case of equal power distributed jamming signals as in (14), shown at the next page. Secondly, relying on the properties given in [14], (13) can be simplified for the case of distinct power distributed jamming signals as in (15), shown at the next page.

It is noteworthy that (13), (14), and (15) are new and have never been reported in the literature yet. Also, since these expressions are composed by elementary functions and finite sums, they are computationally efficient by the most popular computer softwares, such as MATHEMATICA, MAPLE, and MATLAB.

C. Asymptotic Secrecy Outage Probability

Although a closed-form expression for the secrecy outage probability is important in evaluating the exact secrecy performance, it does not directly provide much insight. Next, in order to gain further insights for the secrecy performance, an asymptotic analysis (i.e., at high SNR regions) is carried out, based on which the diversity order and the array gain of the system can be determined. Next, we assume that the Bob's average SNR is higher than Eve's SINR, i.e., $\bar{\gamma}_{\mathrm{B}} \gg \bar{\gamma}_{\mathrm{E}}/(\bar{\gamma}_I + 1)$.

Firstly, making use of the Maclaurin series to expand the exponential function of (2) and relying on [13, Eq. (1.211.1)], it can be proven[1] that the CDF of Bob can be asymptotically written as

$$F^{\infty}_{\gamma_{\mathrm{B},s}}(x) \simeq \frac{1}{L_{\mathrm{B}}^{N_{\mathrm{A}}(N_{\mathrm{B}}-L_{\mathrm{B}})}(L_{\mathrm{B}}!)^{N_{\mathrm{A}}}}\left(\frac{x}{\bar{\gamma}_{\mathrm{B}}}\right)^{N_{\mathrm{A}}N_{\mathrm{B}}}. \tag{16}$$

Now, by substituting (16) and (8) into (11), and performing the required integral, an asymptotic expression for the secrecy outage probability can be derived as

$$\begin{aligned} &P_s^{\infty}(R) \simeq \\ &\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}}\sum_{m=0}^{n}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\binom{n}{m}(-1)^{N_{\mathrm{A}}N_{\mathrm{B}}+j-k-n} \\ &\times\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j-m-u}\bar{\gamma}_E^m}{(j-k)!(k-p)!(u-q)!(p-1)!q!} \\ &\times\frac{1}{L_{\mathrm{B}}^{N_{\mathrm{A}}(N_{\mathrm{B}}-L_{\mathrm{B}})}(L_{\mathrm{B}}!)^{N_{\mathrm{A}}}} \\ &\times\Big[(p+q)\Gamma(m+u+1) \\ &\times\Psi\left(m+u+1, m+u-p-q+1, \frac{1}{\bar{\gamma}_i}\right) + \Gamma(m+u+1)\frac{1}{\bar{\gamma}_i} \\ &\times\Psi\left(m+u+1, m+u-p-q+2, \frac{1}{\bar{\gamma}_i}\right) - \Theta_2\Big]\frac{1}{\bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{A}}N_{\mathrm{B}}}}, \end{aligned} \tag{17}$$

where Θ_2 is given by

$$\Theta_2 = \begin{cases} \Psi\left(m+u, m+u-p-q+1, \frac{1}{\bar{\gamma}_i}\right) \\ \times u\Gamma(m+u), \quad u \neq 0 \\ 0, \quad u = 0 \end{cases} \tag{18}$$

From the literature, it is well-known that an asymptotic outage expression can be generally written as

$$P_s^{\infty}(R) = G_{\mathrm{A}}\left(\bar{\gamma}_{\mathrm{B}}\right)^{-G_{\mathrm{D}}} + o(\bar{\gamma}_{\mathrm{B}}^{-G_{\mathrm{D}}}), \tag{19}$$

where G_{A} and G_{D} symbolize, respectively, the array gain and the diversity gain of the system.

1) Diversity Gain: By comparing (17) and (19), it follows that G_{D} is given by

$$G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}}. \tag{20}$$

Such remark goes in contrast to the conclusion of [11], in which an interference-limited eavesdropper scenario was assumed and the diversity order was given by $G_{\mathrm{D}} = \min(M, N_{\mathrm{A}}N_{\mathrm{B}})$. Hence, when both interference and noise at Eve are considered, the diversity order is limited only by the

[1] Due to space constraints, some analytical steps have been omitted throughout the paper. However, as will be shown in the plots, the correctness of the derived expressions are confirmed through Monte Carlo simulations, in which an excellent agreement between the analytical and simulated curves is observed.

$$P_s(R) = \sum_{S_k \in S} \alpha_k e^{\frac{-\delta_k(2^R-1)}{\bar{\gamma}_{\rm B}}} \sum_{f=0}^{\beta_k} \beta_k f (2^R-1)^{\beta_k - f} 2^{Rf} \sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \Omega_{i,j} \sum_{k=1}^{j}\sum_{p=1}^{k} (-1)^{j-k} \sum_{u=0}^{N_{\rm E}-1}\sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}$$
$$\times \left(\frac{1}{\bar{\gamma}_{\rm E}}\right)^u \Bigg[\Psi\left(u+f+1, u+f+1-p-q, \frac{1}{\bar{\gamma}_i} + \frac{\delta_k \bar{\gamma}_{\rm E} 2^R}{\bar{\gamma}_{\rm B}\bar{\gamma}_i}\right) \Gamma(u+f+1) \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_i}\right)^{u+f} (p+q)$$
$$+ \Psi\left(u+f+1, u+f+2-p-q, \frac{1}{\bar{\gamma}_i} + \frac{\delta_k \bar{\gamma}_{\rm E} 2^R}{\bar{\gamma}_{\rm B}\bar{\gamma}_i}\right) \Gamma(u+f+1) \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_i}\right)^{u+f} \left(\frac{1}{\bar{\gamma}_i}\right) - \Theta_1 \Bigg]. \quad (13)$$

$$P_s(R) = \sum_{S_k \in S} \alpha_k e^{\frac{-\delta_k(2^R-1)}{\bar{\gamma}_{\rm B}}} \sum_{f=0}^{\beta_k} \beta_k f (2^R-1)^{\beta_k - f} 2^{Rf} \sum_{k=1}^{M}\sum_{p=1}^{k} (-1)^{M-k} \sum_{u=0}^{N_{\rm E}-1}\sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_1^{p+q-M}}{(M-k)!(k-p)!(u-q)!(p-1)!q!}$$
$$\times \left(\frac{1}{\bar{\gamma}_E}\right)^u \Bigg[\Psi\left(u+f+1, u+f+1-p-q, \frac{1}{\bar{\gamma}_1} + \frac{\delta_k \bar{\gamma}_{\rm E} 2^R}{\bar{\gamma}_{\rm B}\bar{\gamma}_1}\right) \Gamma(u+f+1) \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_1}\right)^{u+f} (p+q)$$
$$+ \Psi\left(u+f+1, u+f+2-p-q, \frac{1}{\bar{\gamma}_1} + \frac{\delta_k \bar{\gamma}_{\rm E} 2^R}{\bar{\gamma}_{\rm B}\bar{\gamma}_1}\right) \Gamma(u+f+1) \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_1}\right)^{u+f} \left(\frac{1}{\bar{\gamma}_1}\right) - \Theta_{1(\bar{\gamma}_i=\bar{\gamma}_1)} \Bigg]. \quad (14)$$

$$P_s(R) = \sum_{S_k \in S} \alpha_k e^{\frac{-\delta_k(2^R-1)}{\bar{\gamma}_{\rm B}}} \sum_{f=0}^{\beta_k} \beta_k f (2^R-1)^{\beta_k - f} 2^{Rf} \sum_{i=1}^{M} \bar{\gamma}_i^{M-1} \prod_{k=1, k\neq i}^{t} (\bar{\gamma}_i - \bar{\gamma}_k)^{-1} \sum_{u=0}^{N_{\rm E}-1}\sum_{q=0}^{u} \frac{\Gamma(1+q)\bar{\gamma}_i^{q}}{(u-q)!q!}$$
$$\times \left(\frac{1}{\bar{\gamma}_{\rm E}}\right)^u \Bigg[\Psi\left(u+f+1, u+f+1-p-q, \frac{1}{\bar{\gamma}_i} + \frac{\delta_k \bar{\gamma}_{\rm E} 2^R}{\bar{\gamma}_{\rm B}\bar{\gamma}_i}\right) \Gamma(u+f+1) \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_i}\right)^{u+f} (p+q)$$
$$+ \Psi\left(u+f+1, u+f+2-p-q, \frac{1}{\bar{\gamma}_i} + \frac{\delta_k \bar{\gamma}_{\rm E} 2^R}{\bar{\gamma}_{\rm B}\bar{\gamma}_i}\right) \Gamma(u+f+1) \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_i}\right)^{u+f} \left(\frac{1}{\bar{\gamma}_i}\right) - \Theta_{1(p=1)} \Bigg]. \quad (15)$$

number of antennas at Alice and Bob, regardless the number of jamming signals at Eve. Interestingly, the achieved diversity order is shown to be the same of [12], in which a GSC scheme at Bob was employed, but the analysis was carried assuming that Eve is subject only to noise. This allows us to conclude that the assumption of jamming signals at Eve does not alter the system diversity order, having effect only on the system array gain.

2) Array Gain: Again, by comparing (17) and (19), the array gain of the proposed system can de attained as

$$G_{\rm A} = \quad (21)$$
$$\sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \Omega_{i,j} \sum_{k=1}^{j}\sum_{p=1}^{k} \sum_{n=0}^{N_{\rm A}N_{\rm B}} \sum_{m=0}^{n} \binom{N_{\rm A}N_{\rm B}}{n} \binom{n}{m} (-1)^{N_{\rm A}N_{\rm B}+j-k-n}$$
$$\times \sum_{u=0}^{N_{\rm E}-1}\sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j-m-u}\bar{\gamma}_{\rm E}^{m}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}$$
$$\times \frac{1}{L_{\rm B}^{N_{\rm A}(N_{\rm B}-L_{\rm B})}(L_{\rm B}!)^{N_{\rm A}}}$$
$$\times \Big[(p+q)\Gamma(m+u+1)$$
$$\times \Psi\left(m+u+1, m+u-p-q+1, \frac{1}{\bar{\gamma}_i}\right) + \Gamma(m+u+1)\frac{1}{\bar{\gamma}_i}$$
$$\times \Psi\left(m+u+1, m+u-p-q+2, \frac{1}{\bar{\gamma}_i}\right) - \Theta_2\Big]. \quad (22)$$

IV. Numerical Results and Discussions

In this Section, representative numerical results are presented in order to evaluate the secrecy outage performance of the system under study. Also, Monte Carlo simulation are shown to validate the derived expressions. Without loss of generality, in all the plots we assume $R = 1$.

Fig. 1 plots the secrecy outage probability versus Bob's average SNR for different antenna configurations and assuming equal power distributed jamming signals. Observe that, at high SNR regions, there is a perfect agreement between the asymptotic and analytical curves, which corroborates the proposed analysis. Taking a closer look in the curves, it can be seen that the diversity order equals to $N_{\rm A}N_{\rm B}$. In particular, for the set of curves {(a), (b)}, $G_{\rm D} = 4$; for the set of curves {(c), (d), (e)}, $G_{\rm D} = 6$; and for the set of curves {(f), (g), (h), (i)}, $G_{\rm D} = 8$. Also, for each setting, $L_{\rm B}$ has been varied from 1 (SC scheme) to $N_{\rm B}$ (MRC scheme). Note that GSC brings a significant SNR advantage relative to SC, while it provides a comparable secrecy outage performance to MRC. Since GSC has a lower complexity than MRC and a higher complexity than SC, this allows us to confirm that the use of GSC at the legitimate Rx provides a cost-performance tradeoff in physical layer security enhancements.

Fig. 2 depicts the secrecy outage probability versus Bob's average SNR for different antenna configurations and distinct

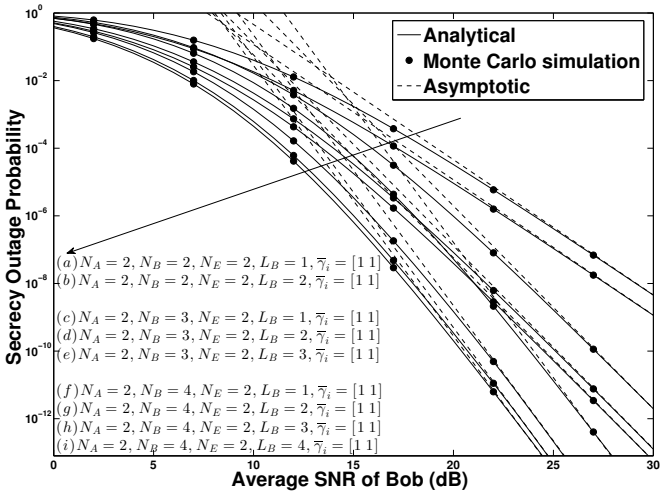

Fig. 1. Secrecy outage probability versus Bob's average SNR assuming GSC scheme at Bob. Settings: $\bar{\gamma}_{\mathrm{E}} = 4$dB; equal power distributed jamming signals.

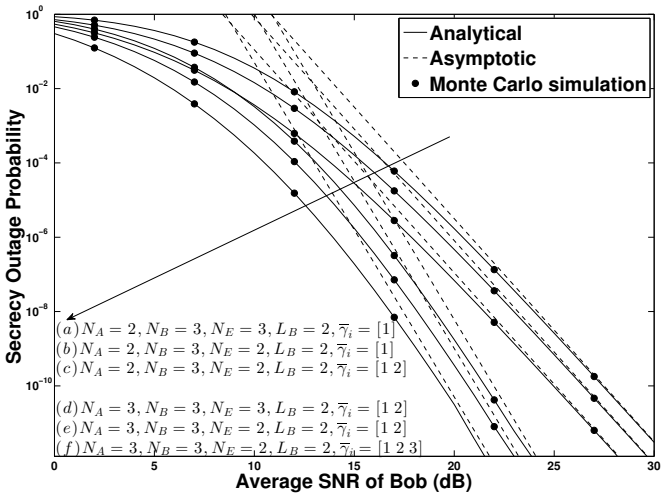

Fig. 2. Secrecy outage probability versus Bob's average SNR assuming GSC scheme at Bob. Settings: $\bar{\gamma}_{\mathrm{E}} = 4$dB; $R = 1$; distinct power distributed jamming signals.

power distributed jamming signals. We set $L_{\mathrm{B}} = 2$. Again, there is a perfect agreement between the asymptotic and analytical curves. In particular, note that the system diversity order does not change neither with N_{E} nor with M, being equal to $N_{\mathrm{A}}N_{\mathrm{B}}$, as expected.

Fig. 3 depicts the array gain versus N_{A} considering considering equal and distinct power distributed interferers. As expected, the array gain increases when N_{A} increases. However, at the same time, increasing the number of jamming signals and/or increasing L_{B} becomes the array gain improvement qualitatively less representative.

V. Conclusions

This paper investigated the secrecy outage performance of MIMO wiretap channels assuming a GSC scheme at the legitimate Rx, while the Tx employed a transmit TAS technique and the eavesdropper adopted a MRC scheme. Assuming that the eavesdropper is subject to noise and jamming, a closed-form

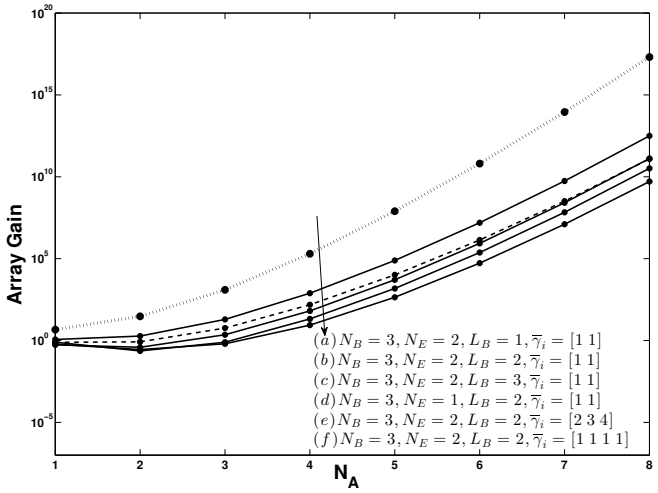

Fig. 3. Array gain versus number of antennas (N_{A}) at Alice. Settings: $N_{\mathrm{B}} = 3$; $\bar{\gamma}_{\mathrm{E}} = -5$dB.

expression for the secrecy outage probability was derived, based on which the diversity and array gains were determined. Insightful discussions were provided through the numerical examples. For instance, it was shown that the use of GSC at the legitimate Rx provides a cost-performance tradeoff in physical layer security enhancements.

References

[1] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Computer*, vol. 31, no. 9, pp. 29-33, Sep. 1998.

[2] C. Shannon, "Communication theory of secrecy systems," *Bell Systems Tech. Journ.*, 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.

[4] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, pp. 40-47, Feb. 2012.

[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, Jun. 2008.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *IEEE Int. Symp. Inf. Theory*, pp. 356-360, 2006.

[7] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372-375, Jun. 2012.

[8] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," I*EEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[9] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forens. Secur.*, vol. 8, no. 1, pp. 254-259, Jan. 2013.

[10] 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, May 2013.

[11] D. B. da Costa, N. S. Ferdinand, U. S. Dias, R. T. de Sousa Jr, and M. Latva-aho, "Secrecy outage performance of MIMO wiretap channels with multiple jamming signals," *Journ. Commun. Inf. Systems*, v. 31, p. 30-40, 2016.

[12] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna Selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1759, Sep. 2013.

[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed., San Diego, CA: Academic, 2007.

[14] 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.