MIMO Wiretap Channels with Multiple Jamming Signals: A Secrecy Outage Performance Analysis

Daniel Benevides 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, a selection combining (SC) scheme is employed at the Rx, while the eavesdropper uses a maximal-ratio combining (MRC) one. The derived outage expressions hold for arbitrary power distributed jamming signals. 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.**

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

I. Introduction

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 [1]. 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 [2]. Owing to this fact, recent advances in the research have proposed to implement the security at the physical layer (PHY) [3], [4]. 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 Winer [5] and 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 [6]–[15].

Common to the works [6]–[13] is the fact that the the use of multiple antennas at the transmitter (Tx) and/or receiver (Rx) 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 (see, for instance, [14], [15]).

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, the secrecy outage performance of multiple-input multiple-output (MIMO) wiretap channels with transmit antenna selection (TAS) is investigated[1]. 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. In our analysis, a selection combining (SC) scheme is employed at Bob, while Eve uses a maximal-ratio combining (MRC) since it always provides worst secrecy performance than SC. 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) can be 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. 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 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.

II. System Model

Let 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. The friendly jammer has full secure cooperation with Bob. In this setup, Eve is operating in an interference-limited

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).

[1] Although beamforming in the direction of the legitimate user is optimal [6], the implementation complexity of beamforming is high and needs full rate feedback. Owing to this fact, the authors in [10] proposed a low-complex TAS scheme that selects a transmit antenna which maximizes the received signal-to-noise ratio (SNR) of the legitimated user. The results showed that high levels of security can be achieved when the number of antennas at Tx increases, even when the eavesdropper has multiple antennas.

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 (i.e., from Alice to Bob) is independent of the eavesdropper channel (i.e, from Alice to Eve). However, both main channel and eavesdropper channel experience slow fading with same fading block length, which is long enough to allow capacity-achieving codes within each block. Employing a TAS scheme, Alice uses the channel state information (CSI) of Bob (i.e., Eve is a passive eavesdropper) to maximize the received SNR at Bob. In our analysis, a SC scheme is employed at Bob[2], while Eve uses MRC.

Based on the system model described above, Alice selects the transmit antenna s according to the rule

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

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[3]

$$y_{\mathrm{B}} = \sqrt{P}|h_{\mathrm{AB},s}|x + n_{\mathrm{B}}, \tag{2}$$

where P denotes the transmit power at Alice, n_{B} is the additive white Gaussian noise (AWGN) component with variance n_b and

$$|h_{\mathrm{AB},s}| = \max_{m\in 1\dots,N_B} |h^m_{\mathrm{AB},s}|. \tag{3}$$

Thus, the received SNR at Bob is given by $\gamma_{B,s} = \bar{\gamma}_B|h_{\mathrm{AB},s}|^2$, with $\bar{\gamma}_B = P/n_b$.

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

$$\mathbf{y}_{\mathrm{E}} = \sqrt{P}\mathbf{h}_{\mathrm{AE,s}}x + \sum_{i=1}^{M}\sqrt{\bar{\gamma}_i}\mathbf{h}_i, \tag{4}$$

where $\mathbf{h}_{\mathrm{AE,s}}$ stands for the 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

$$\begin{aligned} y_{\mathrm{E}} &= \sqrt{P}\frac{\mathbf{h}^\dagger_{\mathrm{AE,s}}}{\|\mathbf{h}_{\mathrm{AE,s}}\|}\mathbf{h}_{\mathrm{AE,s}}x + \sum_{i=1}^{M}\sqrt{\bar{\gamma}_i}\frac{\mathbf{h}^\dagger_{\mathrm{AE,s}}}{\|\mathbf{h}_{\mathrm{AE,s}}\|}\mathbf{h}_i \\ &= \sqrt{P}\|\mathbf{h}_{\mathrm{AE,s}}\|x + \sum_{i=1}^{M}\sqrt{\bar{\gamma}_i}\tilde{h}_i, \end{aligned} \tag{5}$$

in which $(\cdot)^\dagger$ denotes conjugate transpose and $\|\cdot\|$ indicates the Frobenius norm. 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 $\mathbf{h}_i$ 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

$$\Upsilon_{E,s} = \frac{\gamma_{E,s}}{\gamma_I}, \tag{6}$$

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.

A. 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

$$R_S = \begin{cases} R_{B,s} - R_{E,s}, & \gamma_{B,s} > \Upsilon_{E,s}, \\ 0, & \gamma_{B,s} \le \Upsilon_{E,s}. \end{cases} \tag{7}$$

III. Secrecy Performance

A. Preliminaries

We assume that all channels undergo Rayleigh fading. Hence, the cumulative distribution function (CDF) of the random variable $\gamma_{B,s} = \bar{\gamma}_B|h_{\mathrm{AB},s}|^2$ is given by

$$F_{\gamma_{B,s}}(z) = \left(1 - e^{-\frac{x}{\bar{\gamma}_B}}\right)^{N_A N_B}, \tag{8}$$

where, from the binomial expansion, it follows that

$$F_{\gamma_{B,s}}(z) = 1 - \sum_{k=1}^{N_A N_B}\binom{N_A N_B}{k}(-1)^{k+1}e^{-\frac{xk}{\bar{\gamma}_B}}. \tag{9}$$

By its turn, the CDF of $\gamma_{E,s}$ can be obtained as

$$F_{\gamma_{E,s}}(z) = 1 - \frac{e^{-\frac{z}{\bar{\gamma}_E}}}{\Gamma(N_E)}\sum_{u=0}^{N_E-1}\frac{1}{u!}\left(\frac{x}{\bar{\gamma}_E}\right)^u, \tag{10}$$

with $\Gamma(\cdot)$ denoting the Gamma function [16, Eq. (8.310.1)]. Now, let $\bar{\gamma}_1, \bar{\gamma}_2, \dots \bar{\gamma}_t$ be distinct values with multiplicities $\eta_1, \eta_2, \dots \eta_t$ such that $\sum_{i=1}^{t}\eta_i = M$. Then, from [17], the probability density function (PDF) of γ_I can be written as

$$f_{\gamma_I}(z) = \sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\frac{\Omega_{i,j}}{(j-1)!\bar{\gamma}_i^j}z^{j-1}e^{-\frac{z}{\bar{\gamma}_i}}, \tag{11}$$

where

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)!\bar{\gamma}_i^{\eta_i - j}}\frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}}\left[\prod_{k=1,k\neq i}^{t}\left(\frac{1}{1+s\bar{\gamma}_k}\right)^{\eta_k}\right]_{s=-\frac{1}{\bar{\gamma}_i}}. \tag{12}$$

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

$$P_s(R) = \Pr(R_S < R), \tag{13}$$

with $\Pr(\cdot)$ denoting probability. In the sequel, the secrecy outage probability will be derived assuming arbitrary power

[2]A MRC scheme could also be employed at Bob. However, in this work, we adopt a SC scenario due to its low complexity nature. In addition, the same insights attained hereafter can also be applied if a MRC scheme were employed at Bob.

[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.

[4]We assume that the noise component at Eve can be neglected with the strong jamming signal 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: The secrecy outage probability assuming SC at Bob and MRC at Eve can be achieved as

$$P_s(R) = 1 - \sum_{k=1}^{N_A N_B} (-1)^{k+1} \binom{N_A N_B}{k} \sum_{u=0}^{N_E-1} \frac{1}{u!} \times \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!} e^{-\frac{k(2^R-1)}{\bar{\gamma}_B}} \times \left[j\Gamma(u+1)\Psi\left(u+1, -j+1; \frac{k\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_2 \right], \quad (14)$$

where

$$\Theta_2 = \begin{cases} u\Gamma(u)\Psi\left(u, -j, \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right), & u \neq 0 \\ 0, & u = 0 \end{cases}. \quad (15)$$

and $\Psi(.,.;.)$ denotes the Tricomi's (confluent hypergeometric) function [16, Eq. (9.211.4)].

Proof: Please, see Appendix.

Next, (14) will be simplified for two special cases.

Corollary 1: Relying on the properties given in [17], (14) can be simplified for the case of distinct power distributed jamming signals as

$$P_s(R) = 1 - \sum_{k=1}^{N_A N_B} \binom{N_A N_B}{k} \sum_{u=0}^{N_E-1} \sum_{i=1}^{M} \times \frac{(-1)^{k+1}\gamma_i^{M-1} e^{-\frac{k(2^R-1)}{\bar{\gamma}_B}}}{\prod_{k=1,k\neq i}^{t}(\bar{\gamma}_i - \bar{\gamma}_k)} \times \left[\Gamma(u+1)\Psi\left(u+1, 0; \frac{k\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_{21} \right], \quad (16)$$

where Θ_{21} is given in (15) by setting $j = 1$.

*Corollary 2:*Assuming $\bar{\gamma}_1 = \bar{\gamma}_2 \ldots = \bar{\gamma}_M$, (14) can be simplified for the case of equal power distributed jamming signals as

$$P_s(R) = 1 - \sum_{k=1}^{N_A N_B} (-1)^{k+1} \binom{N_A N_B}{k} \sum_{u=0}^{N_E-1} \frac{1}{u!} \frac{\Gamma(u+M)}{(M-1)!} \times e^{-\frac{k(2^R-1)}{\bar{\gamma}_B}} \times \left[M\Gamma(u+1)\Psi\left(u+1, -M+1; \frac{k\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right) - \Theta_{22} \right], \quad (17)$$

where Θ_{22} is same as Θ_2 given in (15) 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 multiple-input single-output (MISO) wiretap channel). Corollary 3 presents the secrecy outage probability for MISO wiretap channel when Eve is limited by multiple equal power distributed jamming signals.

Corollary 3: The secrecy outage probability for a MISO wiretap channel with multiple equal power interferers at eavesdropper can be obtained by setting $N_B = N_E = 1$ in (17), yielding

$$P_s(R) = 1 - \sum_{n_1=1}^{N_A} (-1)^{n_1+1} \binom{N_A}{n_1} e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}} M \times \Psi\left(1, -M+1; \frac{n_1\bar{\gamma}_E 2^R}{\bar{\gamma}_i\bar{\gamma}_B}\right). \quad (18)$$

C. Non-Zero Secrecy Rate

The probability of non-zero secrecy rate can be mathematically calculated as

$$P_r(R_S > 0) = \Pr(R_B > R_E) = \Pr(\gamma_{B,s} > \gamma_{E,s}) = \int_0^\infty \int_0^x f_{\gamma_{B,s}}(x) f_{\Upsilon_{E,s}}(y) dy dx. \quad (19)$$

From (9), the PDF of $\gamma_{B,s}$ can be easily attained. By substituting this latter and (31) into (19), and performing the required integral, a closed-form expression for the probability of non-zero secrecy rate can be derived as

$$P_r(R_S > 0) = 1 - N_A N_B \sum_{k=0}^{N_A N_B - 1} \binom{N_A N_B - 1}{k} (-1)^k \times \sum_{u=0}^{N_E-1} \frac{1}{u!} \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!} \times \Gamma(u+1) \frac{\bar{\gamma}_E}{\bar{\gamma}_B\bar{\gamma}_i} \Psi\left(u+1, 2-j; \frac{(k+1)\bar{\gamma}_E}{\bar{\gamma}_B\bar{\gamma}_i}\right). \quad (20)$$

IV. Asymptotic Secrecy Analysis

In this Section, an asymptotic analysis is carried out. For the sake of simplicity, we consider $N_E = 1$ and a uniform interference power scheme such that the derived expressions are not too long. However, for arbitrary N_E and interference power schemes, the analysis can be easily done by following the same procedure. Next, we assume that the Bob's average SNR is larger than Eve's SIR, i.e. $\bar{\gamma}_B > \bar{\gamma}_E/\bar{\gamma}_1$.

Firstly, we represent (17) in an integral form as

$$P_s(R) = 1 - \sum_{n=1}^{N_A N_B} (-1)^{n+1} \binom{N_A N_B}{n} e^{-\frac{n(2^R-1)}{\bar{\gamma}_B}} M \times \int_0^\infty \frac{e^{-\frac{n2^R\bar{\gamma}_E x}{\bar{\gamma}_1\bar{\gamma}_B}}}{(x+1)^{M+1}} dx. \quad (21)$$

Thus, making use of [16, Eq. (3.353)], it follows that

$$P_s(R) = 1 - \sum_{n=1}^{N_A N_B} \frac{(-1)^{n+1}}{(M-1)!} \binom{N_A N_B}{n} e^{-\frac{n(2^R-1)}{\bar{\gamma}_B}} \left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}\right)^M \times \left[\sum_{k=1}^{M} (k-1)!(-1)^{M-k} \left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}\right)^{-k} - (-1)^M e^{\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}} \mathrm{Ei}\left(-\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1\bar{\gamma}_B}\right) \right], \quad (22)$$

with $\mathrm{Ei}(\cdot)$ denoting the exponential integral [16, Eq. (8.211.1)]. Using the Maclaurin expansion to expand the exponential function and rewriting the exponential integral as a series

expansion [16, Eq. (8.214.1)], $P_s(R)$ can be rewritten as

$$P_s(R) = 1 - \sum_{n=1}^{N_A N_B} \frac{(-1)^{n+1}}{(M-1)!}\binom{N_A N_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M \times \left[\sum_{k=1}^{M}(k-1)!\sum_{s=0}^{\infty} n^s(2^R-1)^s(-1)^{M-k+s}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{-k} -(-1)^M\sum_{q=0}^{\infty}\frac{1}{q!}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1} - n(2^R-1)\right)^q \times\left\{\left(C+\ln\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)\right)\frac{1}{\bar{\gamma}_B^{M+q}} +\sum_{p=1}^{\infty}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^p\frac{(-1)^p}{pp!\bar{\gamma}_B^{p+q+M}}\right\}\right], \quad (23)$$

where C is the Euler constant. Finally, by considering the first non-zero order terms of (23) and after some mathematical simplifications, an asymptotic expression can be obtained as

$$P_s(R) = \begin{cases} (\psi_1\bar{\gamma}_B)^{-N_A N_B}, & N_A N_B < M \\ (\psi_2\bar{\gamma}_B)^{-M}, & N_A N_B > M \\ (\psi_3\bar{\gamma}_B)^{-N}, & N = N_A N_B = M \end{cases} \quad (24)$$

where

$$\psi_1 = \left[\sum_{n=1}^{N_A N_B}\frac{(-1)^n}{(M-1)!}\binom{N_A N_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M\sum_{k=1}^{M} \times\frac{(k-1)!(-1)^{N_A N_B-M}(n(2^R-1))^{N_A N_B-M+k}}{(N_A N_B-M+k)!} \times\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{-k}\right]^{-\frac{1}{N_A N_B}}, \quad (25)$$

$$\psi_2 = \left[\sum_{n=1}^{N_A N_B}\frac{(-1)^{n+1}}{(M-1)!}\binom{N_A N_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M \times\left(C+\ln\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)\right)\right]^{-\frac{1}{M}}, \quad (26)$$

and

$$\psi_3 = \left[\sum_{n=1}^{N_A N_B}\frac{(-1)^n}{(M-1)!}\binom{N_A N_B}{n}\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^M \times\left\{\sum_{k=1}^{M}\frac{(k-1)!(-1)^{N_A N_B-M}(n(2^R-1))^{N_A N_B-M+k}}{(N_A N_B-M+k)!} \times\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{-k} - \left(C+\ln\left(\frac{n2^R\bar{\gamma}_E}{\bar{\gamma}_1}\right)\right)\right\}\right]^{-\frac{1}{N}}. \quad (27)$$

A. Diversity Gain

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

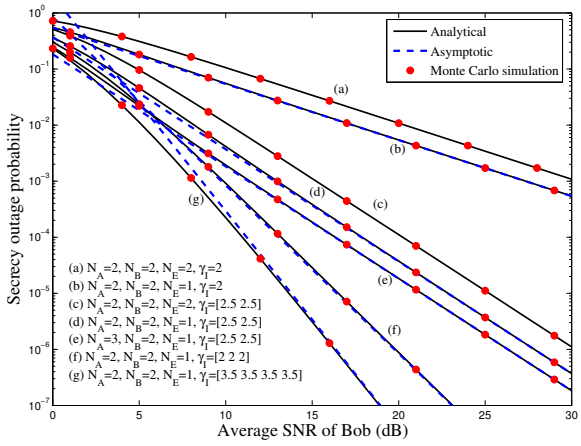

Fig. 1. Secrecy outage probability versus Bob's average SNR. $\bar{\gamma}_E = -2$dB; $R = 1$.

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. Different antenna configurations, interference powers and average SNRs are considered with the intention of studying the secrecy performance over the whole range.

Fig. 1 depicts the secrecy outage probability versus Bob's average SNR. 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 is 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 $N_A = N_B = 2$. A 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.

The probability of non-zero secrecy rate versus Bob's average SNR is plotted in Fig. 2. 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

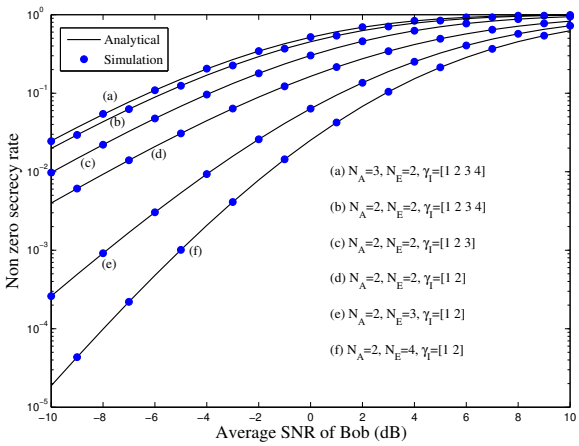

Fig. 2. Probability of non-zero secrecy rate versus Bob's average SNR. $N_B = 3$ and $\bar{\gamma}_E = 10$dB.

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 with the increase of the number of antennas at Eve.

VI. Conclusions

In this paper, we investigated the secrecy performance of MIMO wiretap channels with TAS in an interference-limited eavesdropper. Assuming a SC scheme at the legitimate user and a MRC scheme at the eavesdropper, closed-form expressions for the secrecy outage probability and non-zero secrecy rate were derived. An asymptotic analysis was carried out 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 arriving 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.

References

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

[2] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, 1998.

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

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

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

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas – Part II: The MIMOME wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5515–5532, 2010.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961–4972, 2011.

[8] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 704–716, 2012.

[9] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *Communications Letters, IEEE*, vol. 15, no. 5, pp. 509–511, 2011.

[10] H. Alves, R. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *Signal Processing Letters, IEEE*, vol. 19, no. 6, pp. 372–375, 2012.

[11] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and I. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *Communications, IEEE Transactions on*, vol. 61, no. 1, pp. 144–154, 2013.

[12] N. Yang, H. Suraweera, I. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 1, pp. 254–259, 2013.

[13] 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," *Communications Letters, IEEE*, vol. 17, no. 5, pp. 864–867, 2013.

[14] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 8, pp. 3831–3842, 2010.

[15] J. Vilela, P. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 616–627, 2011.

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

[17] N. Ferdinand and N. Rajatheva, "Unified performance analysis of two-hop amplify-and-forward relay systems with antenna correlation," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 9, pp. 3002–3011, 2011.

Appendix

The secrecy outage probability can be mathematically written as

$$P_s(R) = \Pr\left(\frac{1+\gamma_{B,s}}{1+\frac{\gamma_{E,s}}{\gamma_I}} < 2^R\right)\Pr\left(\gamma_{B,s} > \frac{\gamma_{E,s}}{\gamma_I}\right) + \Pr\left(\gamma_{B,s} < \frac{\gamma_{E,s}}{\gamma_I}\right). \quad (28)$$

Thus, by using the concepts of probability theory, (28) can be rewritten as

$$P_s(R) = F_{\frac{1+\gamma_{B,s}}{1+\frac{\gamma_{E,s}}{\gamma_I}}}(2^R) = \int_1^\infty F_{1+\gamma_{B,s}}(2^R x) f_{1+\frac{\gamma_{E,s}}{\gamma_I}}(x)dx = \int_0^\infty F_{\gamma_{B,s}}(2^R x + 2^R - 1) f_{\frac{\gamma_{E,s}}{\gamma_I}}(x)dx. \quad (29)$$

In order to provide a closed-form solution to (29), we first derive $f_{\frac{\gamma_{E,s}}{\gamma_I}}(x)$ as

$$f_{\frac{\gamma_{E,s}}{\gamma_I}}(x) = \frac{\partial}{\partial x}\left[\int_0^\infty F_{\gamma_{E,s}}(xz) f_{\gamma_I}(z)dz\right]. \quad (30)$$

Then, making use of the CDF of $\gamma_{E,s}$ and the PDF of γ_I given in (11), it follows that

$$f_{\frac{\gamma_{E,s}}{\gamma_I}}(x) = \sum_{u=0}^{N_E-1}\frac{1}{u!}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\frac{\Omega_{i,j}\Gamma(u+j)}{(j-1)!}\left(\frac{\bar{\gamma}_I}{\bar{\gamma}_E}\right)^u x^{u-1} \times \left(\frac{x\bar{\gamma}_I}{\bar{\gamma}_E}+1\right)^{-u-j-1}\left(j\frac{x\bar{\gamma}_I}{\bar{\gamma}_E}-u\right). \quad (31)$$

Now, by substituting (9) and (31) in (29), and performing the required integration with the help of [16, 9.211.4], the secrecy outage probability can be attained as in *Theorem*.