Performance of Transmit Antenna Selection Physical Layer Security Schemes

Hirley Alves, Richard Demo Souza, Mérouane Debbah, Mehdi Bennis

Performance of Transmit Antenna Selection Physical Layer Security Schemes

Hirley Alves, Richard Demo Souza, Mérouane Debbah and Mehdi Bennis

***Abstract*—We analyze the physical layer (PHY) security of a communication scheme consisting of a multiple antenna transmitter with a single radio frequency (RF) chain using transmitter antenna selection (TAS) and a single antenna receiver, in the presence of a sophisticated multiple antenna eavesdropper. We develop closed-form expressions for the analysis of the secrecy outage probability, and we show that the PHY security can be considerably enhanced when multiple antennas are available at the legitimate transmitter. Moreover, a single RF chain multiple antenna transmitter reduces cost, complexity, size and power consumption at the expense of a slight loss in performance with respect to a multiple RF chain transmitter.**

I. Introduction

Recently, securing the communication over the wireless medium at the physical layer (PHY) has gained considerable attention [1]–[6]. A pioneering work on PHY security is that of Wyner in [7], where it was proved that there are codes for the wire-tap channel that guarantee both low error probabilities and a certain degree of confidentiality. The wire-tap channel is composed of two legitimate users, commonly known as Alice and Bob, communicating in the presence of an eavesdropper, known as Eve. Alice and Bob communicate through the main channel while Eve observes through the eavesdropper channel a degraded version of the message seen by Bob. Later, in [8] it was demonstrated that the secrecy capacity on a Gaussian wire-tap channel can be defined as the difference between the capacity of the main channel and the eavesdropper channel, being the capacity of the former greater than the latter.

In [1], [2] PHY security for a quasi-static Rayleigh fading wire-tap channel with single antenna devices was investigated. A different scenario was analyzed in [4] in which only the eavesdropper has multiple antennas and the channels are subject to quasi-static Rayleigh fading. The authors in [4] have shown that when Selection Combining (SC) is used one multiple antenna eavesdropper causes the same effect as of multiple single antenna eavesdroppers. Moreover, it was shown that the secrecy outage probability rises as the number of the eavesdropper's antennas increases. The authors also compared SC to Maximal Ratio Combining (MRC) at the eavesdropper. Their results show that MRC is more efficient than SC from the point of view of the eavesdropper. Furthermore, in [5] both Bob and Eve are assumed to have multiple antennas while Alice is a single antenna device. The authors developed closed-form expressions for the secrecy outage probability, considering that the receivers employ MRC. The results show that the use of multiple receive antennas can enhance security, and that the secrecy outage probability is a function of the ratio between the number of receive antennas at Bob and Eve.

Wireless systems with multiple antennas are conceived to increase reliability on account of diversity or to achieve high data rates due to the presence of multiplexing gains [9]. In the context of PHY security the multiple-input multiple-output (MIMO) wire-tap channel is known as MIMOME channel [3], once all nodes have multiple antennas. For instance, in [3] secrecy capacity expressions were derived for the Gaussian MIMO wire-tap channel, while in [6] the authors derived secrecy outage probability expressions for a codebook based beamforming on the Rayleigh MISOME channel (Bob is a single antenna device). The authors proposed a codebook based beamforming, which means that the transmitter is using a predefined codebook known to both transmitter and receiver and that a feedback channel is required. However, the gains obtained through MIMO do not come for free. The front-end architecture is highly complex and the hardware of the radio frequency (RF) section is expensive, while complexity and cost increase with the number of antennas [9]–[11]. Alternatively, transmit antenna selection (TAS) [10] uses a single RF chain instead of several parallel RF sections, reducing cost, complexity, power consumption and size at the expense of a generally acceptable loss in performance [9]–[11].

In this work we assume a reasonable practical scenario in which only Alice and Eve have multiple antennas while Bob is a single antenna device. Alice could be seen as a base station in a cellular network and Bob as regular mobile user, while Eve is a more sophisticated device than Bob, and therefore more likely to obtain private information. Alice employs TAS on the main channel, which is a low cost and complexity method for exploiting spatial diversity in multiple antenna settings [10]–[12], while Eve employs optimum MRC. Moreover, we consider that Bob informs Alice of the best antenna index through an open (non-secure) and low rate return channel. Although Eve is able to access the open return channel, the eavesdropper will not be able to exploit this information since Eve has access uniquely to the antenna index, and has no channel state information (CSI) of the main channel. Furthermore, such an antenna index is optimum for the main channel only. Therefore, Eve is not able to exploit any additional diversity from the multiple transmit antennas at Alice. The main contribution of this paper is to show that PHY security can be considerably enhanced using a low cost and complexity single RF chain transmitter, even if the eavesdropper is more sophisticated than the legitimate receiver.

H. Alves and M. Bennis are with the Centre for Wireless Communications, University of Oulu, Oulu, P.O. Box 4500, FI-90014, Finland. Email:{halves,bennis}@ee.oulu.fi.

R. D. Souza is with CPGEI, Federal University of Technology - Paraná (UTFPR), Curitiba, PR 80230-901, Brazil. Email:richard@utfpr.edu.br. H. Alves is also with CPGEI, UTFPR, Brazil.

M. Debbah is with the Alcatel-Lucent Chair on Flexible Radio, SUPELEC, 3 rue Joliot-Curie, Gif-sur-Yvette, 91192, France. Email: merouane.debbah@supelec.fr

The rest of this paper is organized as follows. Section II introduces the system model. In Section III the secrecy outage probability is derived. Section IV presents the numerical results, while Section V concludes the paper.

II. System Model

We consider that Alice and Eve have N_A and N_E antennas, respectively, while Bob is a single antenna device. We assume quasi-static Rayleigh fading channels, zero-mean complex Gaussian noise and that nodes have low mobility. The receivers have full CSI of their own channels [1]. Bob and Alice exchange the index of Alice's antenna with the best SNR at Bob through an open return channel. Alice uses this index in a TAS scheme, allowing Bob to achieve N_A diversity order. From Eve's point of view the optimum TAS scheme for Bob is a random TAS scheme, as the main channel and the eavesdropper channel are uncorrelated. Thus, Eve cannot exploit any additional spatial diversity from Alice's antennas. After TAS, Alice sends the message x to Bob. The signal y received by Bob can be written as:

$$y = \sqrt{P\kappa_M}\; h_M\, x + n_M, \tag{1}$$

where P is the average transmit power, $E[|x|^2] \leq P$, $\kappa_M = d_M^{-\alpha}$ is the path loss of the main channel, d_M is the distance between Alice and Bob, α is the path loss exponent, h_M is the Rayleigh fading coefficient of the channel between the selected antenna from Alice and the receive antenna at Bob, while n_M is complex Gaussian noise with zero mean and power N_M.

Eve is capable of eavesdropping the signal sent by Alice. As Eve uses multiple antennas, the received signal vector $\mathbf{z} = [z_1 z_2 ... z_{N_E}]^T$ at Eve is:

$$\mathbf{z} = \sqrt{P\kappa_W}\; \mathbf{h}_W\, x + \mathbf{n}_W, \tag{2}$$

where $\kappa_W = d_W^{-\alpha}$ is the path loss of the eavesdropper's channel, d_W is the distance between Alice and Eve, $\mathbf{h}_W = [h_{W,1} h_{W,2} ... h_{W,N_E}]^T$ is the fading between Alice's transmit antenna and Eve's receive antennas, $\mathbf{n}_W = [n_{W,1} n_{W,2} ... n_{W,N_E}]^T$ is a vector of complex Gaussian noise samples, where each $n_{W,i}$ has zero mean and power N_W.

The instantaneous SNR at Bob is $\gamma_M = \frac{P\,\kappa_M |h_M|^2}{N_M}$, while the average SNR is $\overline{\gamma}_M = \frac{P\,\kappa_M E[|h_M|^2]}{N_M}$. As Eve applies MRC among the receive antennas, we have $\gamma_W = \frac{P\kappa_W \sum_{i=1}^{N_E} |h_{W,i}|^2}{N_W}$, and $\overline{\gamma}_W = \frac{P\,\kappa_W E[\sum_{i=1}^{N_E} |h_{W,i}|^2]}{N_W}$.

The probability density function (pdf) of γ_M is [12]:

$$f_{\gamma_M}(\gamma_M) = \frac{N_A}{\overline{\gamma}_M} \cdot \exp\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right) \cdot \left[1 - \exp\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right)\right]^{N_A - 1}, \tag{3}$$

and the pdf of γ_W is [1]:

$$f_{\gamma_W}(\gamma_W) = \frac{\gamma_W^{N_E - 1}}{(N_E - 1)!\,\overline{\gamma}_W^{N_E}} \cdot \exp\left(-\frac{\gamma_W}{\overline{\gamma}_W}\right), \tag{4}$$

The instantaneous secrecy capacity can be defined as [1]:

$$C_s = [C_M - C_W]^+, \tag{5}$$

where

$$C_M = \log(1 + \gamma_M) \quad \text{and} \quad C_W = \log(1 + \gamma_W), \tag{6}$$

are respectively the instantaneous capacity of the main and eavesdropper's channel. Based on the non-negativity of the channel capacity, we can rewrite the secrecy capacity as

$$C_s = \begin{cases} \log(1 + \gamma_M) - \log(1 + \gamma_W) & \gamma_M > \gamma_W \\ 0 & \gamma_M \leq \gamma_W \end{cases} \tag{7}$$

Considering the independence between the main channel and the eavesdropper's channel, we can derive the probability of the existence of a non-zero secrecy capacity as:

$$\begin{aligned} \Pr[C_s > 0] &= \Pr[\gamma_M > \gamma_W] \\ &= \int_0^\infty \int_0^{\gamma_M} f_{\gamma_M \gamma_W}(\gamma_M, \gamma_W) d\gamma_W d\gamma_M \\ &= \int_0^\infty \int_0^{\gamma_M} f_{\gamma_M}(\gamma_M) f_{\gamma_W}(\gamma_W) d\gamma_W d\gamma_M \\ &= 1 - \sum_{k=0}^{N_A} \binom{Na}{k} (-1)^k \left(1 + k\frac{\overline{\gamma}_W}{\overline{\gamma}_M}\right)^{-N_E}, \end{aligned} \tag{8}$$

where $\Pr[\theta]$ is the probability of the event θ, and $f_{\gamma_M \gamma_W}(\gamma_M, \gamma_W) = f_{\gamma_M}(\gamma_M) f_{\gamma_W}(\gamma_W)$ is the joint pdf of γ_M and γ_W. For further details see Appendix A.

When legitimate and eavesdropper nodes are all single antenna devices (8) reduces to [1]:

$$\Pr[C_s > 0] = \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_W}. \tag{9}$$

Due to the fact that Alice has not perfect channel knowledge about Bob and Eve, secrecy capacity can not be guaranteed in this scenario. It is only possible to perform a probabilistic treatment of secrecy capacity, by means of the so called secrecy outage probability, as we do next.

III. Secrecy Outage Probability

The outage probability can be defined as [2]:

$$\begin{aligned} \mathcal{O}(\mathcal{R}_s) &= \Pr[C_s < \mathcal{R}_s] \\ &= \Pr[C_s < \mathcal{R}_s \mid \gamma_M > \gamma_W] \Pr[\gamma_M > \gamma_W] \\ &+ \Pr[C_s < \mathcal{R}_s \mid \gamma_M \leq \gamma_W] \Pr[\gamma_M \leq \gamma_W], \end{aligned} \tag{11}$$

where $\mathcal{R}_s > 0$ is the secrecy rate [1], [5]. Note that, $C_s = 0$ when $\gamma_M \leq \gamma_W$ and $\mathcal{R}_s > 0$, therefore $\Pr[C_s < \mathcal{R}_s \mid \gamma_M \leq \gamma_W] = 1$. In (8) we defined $\Pr[\gamma_M > \gamma_W]$, consequently:

$$\begin{aligned} \Pr[\gamma_M \leq \gamma_W] &= 1 - \Pr[\gamma_M > \gamma_W] \\ &= \sum_{k=0}^{N_A} \binom{Na}{k} (-1)^k \left(1 + k\frac{\overline{\gamma}_W}{\overline{\gamma}_M}\right)^{-N_E}. \end{aligned} \tag{12}$$

Next, we determine $\Pr[\theta = C_s < \mathcal{R}_s \mid \gamma_M > \gamma_W]$, which is given by (13) where $y = 2^{\mathcal{R}_s}(1 + \gamma_W) - 1$. The detailed solution of (13) is presented in Appendix B. Finally, using (8), (12) and (13) into (11) we obtain the secrecy outage probability for our proposed scheme, which is given by (14). When $N_A = 1$ (14) reduces to:

$$\mathcal{O}(\mathcal{R}_s) = 1 - \frac{\overline{\gamma}_M}{\overline{\gamma}_M + 2^{\mathcal{R}_s}\overline{\gamma}_W} \exp\left(-\frac{2^{\mathcal{R}_s} - 1}{\overline{\gamma}_M}\right), \tag{15}$$

which is the same result as that in [1], where the authors consider that Alice, Bob and Eve are single antenna devices.

IV. Numerical Results

Figure 1 shows the probability of existence of secrecy capacity $\Pr[C_s > 0]$ for different values of N_A, N_E, $\overline{\gamma}_W = 0$ dB and $\mathcal{R}_s = 1$ bits/s/Hz. Moreover, throughout this paper we assume $d_M = d_W = 1$, $\alpha = 4$ and $N_M = N_W = 1$. From the figure we can see that the probability of existence decreases

$$\Pr[\theta] = \int_0^{\infty}\int_{\gamma_W}^{y} \frac{f_{\gamma_M}(\gamma_M) f_{\gamma_W}(\gamma_W)}{\Pr[\gamma_M > \gamma_W]} d\gamma_M d\gamma_W = \frac{\sum_{k=0}^{N_A} \binom{Na}{k} (-1)^k \left[e^{\left(-k\frac{2^{\mathcal{R}_s}-1}{\overline{\gamma}_M}\right)} \left(1 + k\frac{2^{\mathcal{R}_s}\overline{\gamma}_W}{\overline{\gamma}_M}\right)^{-N_E} - \left(1 + k\frac{\overline{\gamma}_W}{\overline{\gamma}_M}\right)^{-N_E} \right]}{1 - \sum_{k=0}^{N_A} \binom{Na}{k} (-1)^k \left(1 + k\frac{\overline{\gamma}_W}{\overline{\gamma}_M}\right)^{-N_E}}. \quad (13)$$

$$\mathcal{O}(\mathcal{R}_s) = \sum_{k=0}^{N_A} \binom{Na}{k} (-1)^k \exp\left(-k\frac{2^{\mathcal{R}_s}-1}{\overline{\gamma}_M}\right) \left(1 + k\frac{2^{\mathcal{R}_s}\overline{\gamma}_W}{\overline{\gamma}_M}\right)^{-N_E}. \quad (14)$$

with the increase in the number of the eavesdropper antennas. The loss can be partially recovered by increasing the number of antennas at Alice, and the gains in terms of SNR are around 2dB when we compare $N_A = 1, N_E = 2$ to $N_A = 2, N_E = 2$ at $\Pr[C_s > 0] = 0.1$. Monte Carlo simulations are also shown.

Figure 2 shows the probability of existence of secrecy capacity as a function of the number of antennas at Eve (N_E), where $r = \frac{\overline{\gamma}_W}{\overline{\gamma}_M}$, $\overline{\gamma}_W = 0$ dB and $\overline{\gamma}_M \in \{3; 0; -3\}$ dB. We can see that the probability of existence decreases with the increase of N_E. On the other hand, it increases with the increase of N_A or $\overline{\gamma}_M$ and also with the decrease of N_E. Figure 3 shows the secrecy outage probability as a function of $\overline{\gamma}_M$, $N_A \in \{1; 2\}$ and $N_E \in \{1; 2; 4\}$. The closed-form expression and MC simulations match very well. From Fig. 3 we can notice that the outage probability reduces with the increase of N_A. On the other hand, it increases with N_E. Therefore, even with a more powerful eavesdropper than Bob, our proposed scheme can considerably enhance PHY security.

Figure 4 compares the proposed scheme to the schemes in [5], [6], assuming a fixed secrecy rate $\mathcal{R}_S = 1$ bits/s/Hz and

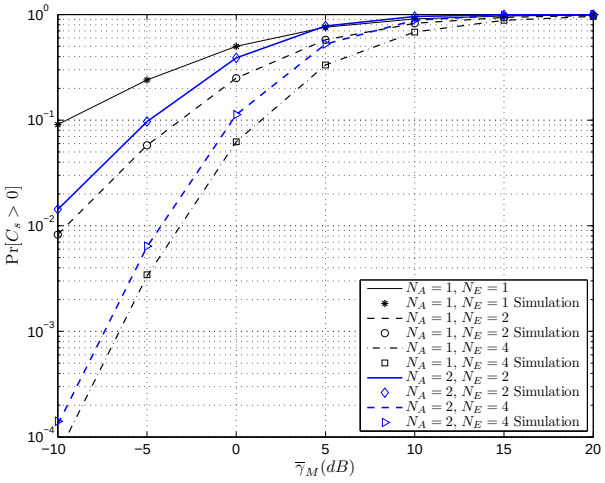

Fig. 1. Probability of existence of secrecy capacity as a function of $\overline{\gamma}_M$ when $\mathcal{R}_s = 1$ bits/s/Hz, $\overline{\gamma}_W = 0$ dB, $N_A \in \{1; 2\}$ and $N_E \in \{1; 2; 4\}$.

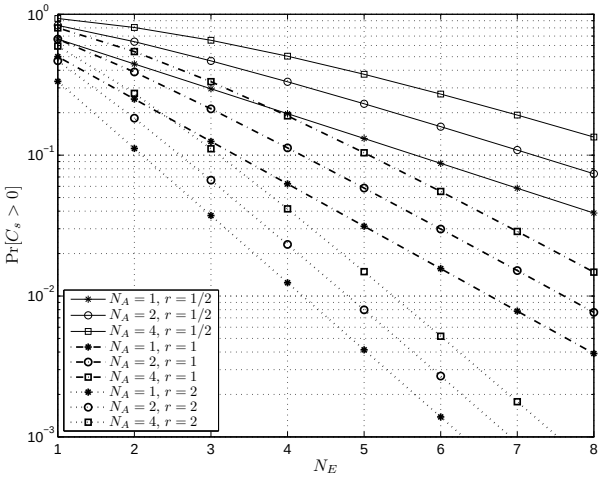

Fig. 2. Probability of existence of secrecy capacity as a function of N_E when $\mathcal{R}_s = 1$ bits/s/Hz and $N_A \in \{1; 2; 4\}$. Note that $r = \frac{\overline{\gamma}_W}{\overline{\gamma}_M}$, $\overline{\gamma}_W = 0$ dB and $\overline{\gamma}_M \in \{3; 0; -3\}$ dB.

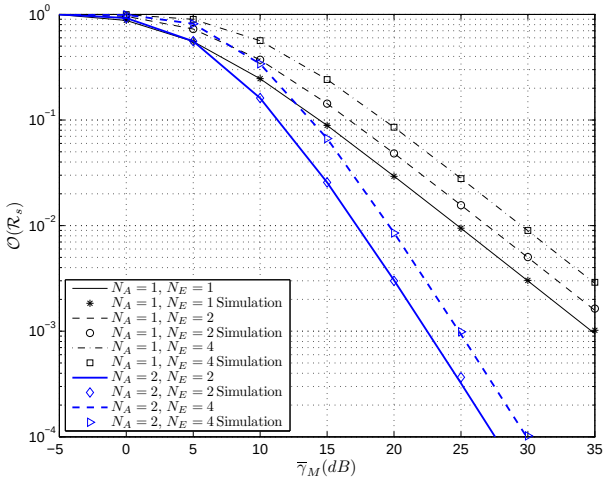

Fig. 3. Secrecy Outage Probability as a function of $\overline{\gamma}_M$ when $\mathcal{R}_s = 1$ bits/s/Hz, $\overline{\gamma}_W = 0$ dB, $N_A \in \{1; 2\}$ and $N_E \in \{1; 2; 4\}$.

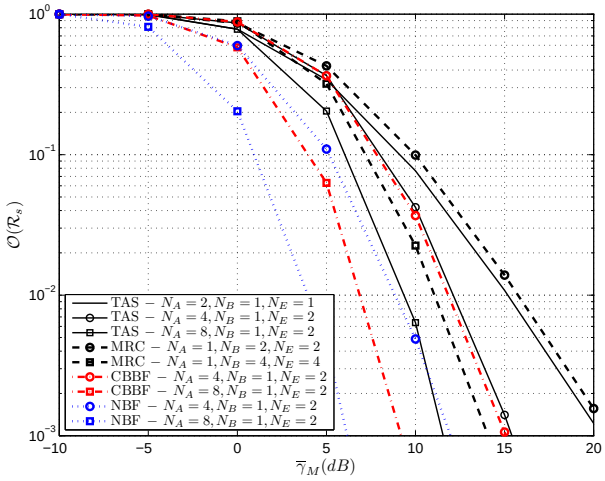

Fig. 4. Secrecy Outage Probability as a function of $\overline{\gamma}_M$ when $\mathcal{R}_s = 1$ bits/s/Hz, $\overline{\gamma}_W = 0$ dB, $N_A \in \{1; 2\}$ and $N_E \in \{1; 2; 4\}$.

$$\begin{aligned}\Pr[C_s>0] &= \int_0^\infty \left\{ \frac{N_A \cdot e^{\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right)}}{\overline{\gamma}_M} \cdot \left[1-e^{\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right)}\right]^{N_A-1} - \frac{N_A \cdot e^{\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right)} \cdot \Gamma\left(N_E, \frac{\gamma_M}{\overline{\gamma}_W}\right)}{\Gamma(N_E)\,\overline{\gamma}_M} \cdot \left[1-e^{\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right)}\right]^{N_A-1} \right\} d\gamma_M \\ &= 1 - I_1. \end{aligned} \tag{16}$$

$$\begin{aligned}\Pr[\theta] &= \mathcal{A} \cdot \int_0^\infty \left\{ e^{\left(-\frac{\gamma_W}{\overline{\gamma}_W}\right)} \cdot \left[1-e^{\left(-\frac{2^{\mathcal{R}_s}(\gamma_W+1)-1}{\overline{\gamma}_M}\right)}\right]^{N_A} \cdot \gamma_W^{N_E-1} - e^{\left(-\frac{\gamma_W}{\overline{\gamma}_W}\right)} \cdot \left[1-e^{\left(-\frac{\gamma_W}{\overline{\gamma}_M}\right)}\right]^{N_A} \cdot \gamma_W^{N_E-1} \right\} d\gamma_W, \\ &= \mathcal{A} \cdot \left[f\left(N_E-1, N_A, \frac{1}{\overline{\gamma}_W}, \frac{2^{\mathcal{R}_s}}{\overline{\gamma}_M}, -e^{\left(-\frac{2^{\mathcal{R}_s}-1}{\overline{\gamma}_M}\right)}\right) - f\left(N_E-1, N_A, \frac{1}{\overline{\gamma}_W}, \frac{1}{\overline{\gamma}_M}, -1\right)\right], \quad \mathcal{A} = \frac{\overline{\gamma}_W^{N_E}}{\Gamma(N_E)\cdot\Pr[\gamma_M>\gamma_W]} \end{aligned} \tag{22}$$

$\overline{\gamma}_W = 0$ dB. In [5], Eve and Bob have multiple antennas and apply MRC, while Alice is a single antenna device. The authors in [6] proposed a codebook based beamforming (CBBF) and also analyze the naive beamforming (NBF) scheme. In CBBF the amount of information that has to be sent from Bob to Alice is limited and depends on the size of the codebook, while in NBF Bob transmits to Alice the complete CSI, requiring in theory an unlimited and unrealistic amount of feedback. From the figure we can see that the proposed scheme performs close to CBBF[1] and outperforms the MRC scheme. The conclusions hold for different values of $\mathcal{R}_s$ and $\overline{\gamma}_W$. Furthermore, we emphasize that TAS requires only a single RF chain which considerably reduces cost, complexity, power consumption and size [9], while CBBF and NBF utilize N_A RF chains. Moreover, our proposed scheme requires only a low rate return channel once few bits have to be fed back ($\lceil \log(N_A) \rceil$ bits).

V. Conclusion

We analytically investigated the secrecy when Alice is a multiple antenna transmitter with single RF chain, Bob is a single antenna device, and Eve is a sophisticated multiple antenna device. We developed closed-form expressions for the secrecy outage probability. Our results show that high levels of security can be achieved when the number of antennas at Alice increases, even when Eve has multiple antennas. The proposed TAS scheme requires only a single RF chain which considerably reduces cost, complexity, power consumption and size at the expense of a very small loss in performance when compared to a multiple RF chain scheme.

Appendix A
Probability of Existence

Consider $\Pr[C_s>0]$ in (16), where I_1 can be rewritten as:

$$I_1 = \frac{\int_0^\infty \exp\left(-\frac{\gamma_M}{\overline{\gamma}_W}\right) \cdot \left[1-\exp\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right)\right]^{N_A} \cdot \gamma_M^{N_E-1} d\gamma_M}{\overline{\gamma}_W^{N_E}\Gamma(N_E)}, \tag{17}$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function [13, Chap. 6]. Now let $f(\cdot) = f(n,m,p,q,a)$ be:

$$\begin{aligned} f(\cdot) &= \int_0^\infty \exp(-p\,t)\cdot[1+a\,\exp(-q\,t)]^m \cdot t^n dt & (18)\\ &= \sum_{k=0}^{m}\binom{m}{k} a^k \int_0^\infty \exp\left(-t\,(p+kq)\right)\cdot t^n dt & (19)\\ &= \sum_{k=0}^{m}\binom{m}{k} a^k \frac{\Gamma(n+1)}{(p\,+\,kq)^{n+1}}. & (20)\end{aligned}$$

[1]We assume a coding design criteria $\delta = \frac{1}{2}$ for CBBF [6].

For obtaining (20) we first expand the binomial term in (18), then we apply a variable substitution $v = t(p+kq)$, which results in the Gamma function [13, Chap. 6]. Thus, applying (20) in (17) yields:

$$\begin{aligned} I_1 &= \frac{\overline{\gamma}_W^{-N_E}}{\Gamma(N_E)} \cdot f(N_E-1, N_A, \frac{1}{\overline{\gamma}_W}, \frac{1}{\overline{\gamma}_M}, -1) \\ &= \sum_{k=0}^{N_A}\binom{Na}{k}(-1)^k \left(1+k\frac{\overline{\gamma}_W}{\overline{\gamma}_M}\right)^{-N_E}. \end{aligned} \tag{21}$$

Finally, taking the result of (21) and putting it into (16) we have the probability of existence as shown in (8).

Appendix B

Here we analyze $\Pr[\theta = C_s < \mathcal{R}_s \mid \gamma_M > \gamma_W]$, which is given by (13). We can rewrite the integral in (13) as (22), then resorting to (20) and after a few algebraic manipulations we have the solution for $\Pr[\theta]$ as shown in (13).

References

[1] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *ISIT'06*, 2006, pp. 356 –360.

[2] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. on Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[3] A. Khisti and G. Wornell, "Secure transmission with multiple antennas - part ii: The mimome wiretap channel," *IEEE Trans. on Inf. Theory*, vol. 56, no. 11, pp. 5515 –5532, 2010.

[4] V. Prabhu and M. Rodrigues, "On wireless channels with m-antenna eavesdroppers: Characterization of the outage probability and outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, no. 99, 2011.

[5] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Comm. Letters*, vol. 15, no. 5, 2011.

[6] S. Bashar, Z. Ding, and G. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. on Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, 2011.

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

[8] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. on Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[9] A. Mohammadi and F. Ghannouchi, "Single rf front-end mimo transceivers," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 104–109, 2011.

[10] S. Sanayei and A. Nosratinia, "Antenna selection in mimo systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68–73, 2004.

[11] S. Prakash and I. McLoughlin, "Effects of channel prediction for transmit antenna selection with maximal-ratio combining in rayleigh fading," *IEEE Trans. Veh. Technol.*, vol. 60, no. 6, pp. 2555–2568, 2011.

[12] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 4, pp. 1312–1321, 2005.

[13] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 10th ed. Dover Publications, 1972.