Secrecy Analysis of A MIMO Full-Duplex Active Eavesdropper with Channel Estimation Errors

Conference Paper · September 2016

DOI: 10.13140/RG.2.1.1247.0003

5 authors, including:

Jiguang He
University of Oulu
21 PUBLICATIONS **62** CITATIONS
SEE PROFILE

Georges Kaddoum
École de Technologie Supérieure
129 PUBLICATIONS **1,000** CITATIONS
SEE PROFILE

Satyanarayana Vuppala
University of Luxembourg
40 PUBLICATIONS **76** CITATIONS
SEE PROFILE

Lin Wang
Xiamen University
160 PUBLICATIONS **1,512** CITATIONS
SEE PROFILE

Secrecy Analysis of A MIMO Full-Duplex Active Eavesdropper with Channel Estimation Errors

Long Kong*, Jiguang He‡, Georges Kaddoum*, Satyanarayana Vuppala+, Lin Wang†,
*Department of Electrical Engineering, Universite du Quebec, ETS, Montreal, Canada
‡Centre for Wireless Communications, FI-90014, University of Oulu, Oulu, Finland
+IDCOM, school of Engineering, University of Edinburgh, Edinburgh, United Kingdom
†Department of Communication Engineering, Xiamen University, Xiamen, P.R. China
Email: long.kong.1@ens.etsmtl.ca, jhe@ee.oulu.fi, georges.kaddoum@etsmtl.ca, S.Vuppala@ed.ac.uk, wanglin@xmu.edu.cn

***Abstract*—In this paper, we investigate the secrecy performance of the multiple-input multiple-output (MIMO) wiretap channels in the presence of an active full-duplex eavesdropper with consideration of channel estimation error at the legitimate destination and eavesdropper. For this purpose, the probability density functions (PDFs) and cumulative density functions (CDFs) of the receive signal-to-interference-plus-noise ratio (SINR) at the destination and eavesdropper are given by conducting the singular value decomposition (SVD) on the estimated channel coefficient matrices. Consequently, the closed-form expressions for the probability of positive secrecy capacity and secrecy outage probability over Rayleigh fading channels are derived. Finally, the Monte-Carlo simulation results are presented to validate the accuracy of our theoretical analysis.**

***Index Terms*—Physical layer security, channel estimation error, the MIMO full-duplex active eavesdropper.**

I. Introduction

Due to the broadcast nature of wireless channels, security issues are increasingly becoming one of the top critical concerns of wireless network. Currently, the traditional cryptography technique widely used in the upper-layer of wireless networks faces big challenges because of the high computational complexity of the communication devices. Fortunately, unlike the traditional methods, a complement or alternative appealing approach termed as physical layer security was emerged to achieve secure wireless transmission, which is based on Shannon theory [1] using the physical characteristics (i.e. noise, fading, interference) of wireless channels. The main philosophy of physical layer security is to achieve perfect secrecy capacity from the information-theoretic perspective, which is defined as the maximization of wireless transmission rate while achieving perfect secure transmission [2]. In other words, it can be further explained as that eavesdroppers can not do better than the legitimate destinations [3]. Against this background, some promising techniques, such as multiple antennas, cooperative jamming/relay [2]–[6], are exploited to degrade the capability of either active attacker or passive eavesdroppers so as to ease the information leakage.

Multiple antenna technique, as an effective approach, is widely used toward improving the secrecy rate. The literature using MIMO technique in the filed of physical layer security demonstrated its capability of boosting secrecy performance [4], [7]–[11]. In particular, the secrecy performance of single-input multiple-output (SIMO) [10], multiple-input single-output (MISO) [12] and multiple-input multiple-output (MIMO) [8] were widely studied from the information-theoretic viewpoint. Shafiee. *et. al* investigated the existence of a computable expression for the secrecy capacity of a 2-2-1 MIMO wiretap channel [7]. Yan. *et. al* investigated the classical three-player MIMO wiretap scenario that Alice firstly selects two strongest transmitter antennas from its multiple antenna set based on the channel gain for the sake of maximizing the instantaneous signal-to-noise ratio (SNR) and then performs Alamouti coding over the selected antennas, afterwards, the closed-form expression of secrecy outage probability for the proposed scheme was derived [4]. In [9], an optimal jamming policy for a full-duplex active eavesdropper to minimize the secrecy rate of the Alice-Bob-Eve MIMO wiretap channel was examined. The authors of [10] analyzed the secrecy performance of a SIMO wiretap channel with channel estimation errors available at the legitimate receiver and eavesdropper, its conclusion suggests that there exists error floor of secrecy outage probability caused by the imperfect channel estimation.

Motivated by these studies, it is so far that there is no previous work that studied the secrecy performance of a 2-2-2 MIMO wiretap channel with consideration of channel estimation error whilst in the presence of an active full-duplex eavesdroppers. To this end, the contribution of this paper lies in the investigation of the secrecy performance of the 2-2-2 MIMO wiretap channel, including the probability of positive secrecy capacity and secrecy outage probability, over Rayleigh fading in the presence of an active full-duplex eavesdropper with channel estimation errors at the legitimate receiver and eavesdropper side. First, the probability density functions (PDFs) and cumulative density functions (CDFs) of the signal-to-interference-plus-noise ratios (SINRs) of Bob's and Eve's received signals are given. Second, the closed-form expressions for the secrecy metrics are derived, and the Monte-Carlo simulation are presented to examine our theoretical analysis.

The remainder of this paper is organized as follows. System model and problem formulation are outlined in Section II. In the Section III, secrecy performance, including the probability of positive secrecy capacity and secrecy outage probability,

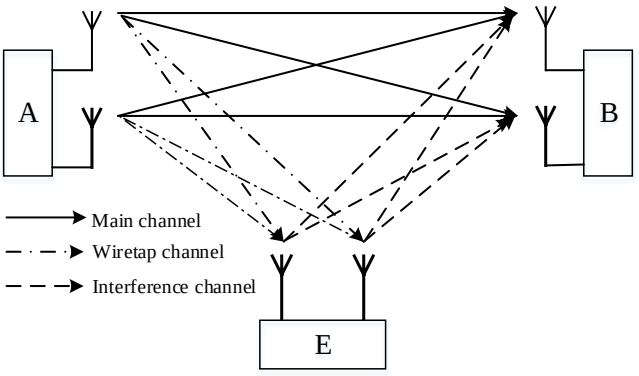

Fig. 1. System model

are derived with closed-form expressions, followed by the comparison of theoretical analysis and numerical simulations given in Section IV. Finally, concluding remarks are given in Section V.

Notations: In this paper, matrices and vectors are separately presented by boldfaced uppercase (e.g., $\mathbf{X}$) and lowercase (e.g., $\mathbf{x}$) letters. Moreover, we use $\mathbf{X}^H$ to denote the Hermitian transpose of the matrix $\mathbf{X}$, $Tr(\cdot)$ to the trace operator, $\mathbf{E}(\cdot)$ to the expectation operator, $\mathbf{I}_m$ the identity matrix of m dimension, $\mathbf{y} \sim \mathcal{CN}(\mu,\sigma^2\mathbf{I})$ to denote that y is the complex Gaussian random variable, having a μ-mean and σ^2-variance.

II. System model and problem formulation

A. System Model

The Alice-Bob-Eve classic model shown in Fig. 1 is used here to illustrate a wireless network with a potential active eavesdropper, where all the users are equipped with 2 antennas. In such a wiretap channel model, the transmitter Alice (A) wishes to send secret messages to the intended receiver Bob (B) in the presence of an active eavesdropper Eve (E); the link between Alice and Bob is called the main channel, whereas the one between Alice and Eve is named as the wiretap channel, and the one between Eve and Bob is termed as interference channel. It is assumed that all links are independent and undergoing quasi-static Rayleigh fading. The fading coefficients of the links $i \to j$ are denoted as $\mathbf{H}_{ij}$, $i, j \in \{A, B, E\}$. In addition, assuming Eve operates in the full-duplex mode, it means that she can listen to data transmission of main channel whilst transmitting jamming signals to Bob. Additionally, it is assumed that Bob and Eve have imperfect channel state information (CSI) of their links, and Alice and Bob have no knowledge of the CSI of the wiretap links.

Then, the received signal at Bob and Eve can be expressed as

$$\mathbf{r}_B = \mathbf{H}_{\mathrm{AB}}\mathbf{x}_A + \mathbf{H}_{\mathrm{EB}}\mathbf{x}_E + \mathbf{n}_B, \tag{1}$$

$$\mathbf{r}_E = \mathbf{H}_{\mathrm{AE}}\mathbf{x}_A + \mathbf{H}_{\mathrm{EE}}\mathbf{x}_E + \mathbf{n}_E, \tag{2}$$

where $\mathbf{x}_A$ and $\mathbf{x}_E$ are the 2×1 transmit signal vector from Alice and jamming signal vector from Eve, respectively. Alice's transmit power is assumed to be fixed to $Tr\{E[\mathbf{x}_A\mathbf{x}_A^H]\} = P_A$. Likewise, Eve's jamming power is subject to $Tr\{E[\mathbf{x}_E\mathbf{x}_E^H]\} = P_E$. Each entry of $\mathbf{H}_{ij}$ follows independent identically distributed (i.i.d.) Gaussian distribution with zero mean and unit variance, denoted by $\mathbf{H}_{ij}(m,n) \sim \mathcal{CN}(0,1)$ for $m, n \in \{1, 2\}$. $\mathbf{n}_B$ and $\mathbf{n}_E$ are the zero mean additive white Gaussian noise (AWGN) distributed with $\mathcal{CN}(0, \boldsymbol{\sigma}_B^2\mathbf{I})$ and $\mathcal{CN}(0, \boldsymbol{\sigma}_E^2\mathbf{I})$, respectively.

B. Problem Formulation

Due to the characteristic of wireless channel, a practical imperfect channel estimator is frequently exploited at the legitimate receivers. The following model is broadly used throughout this paper for the estimated channel $\hat{\mathbf{H}}_{ij}$ [10],

$$\mathbf{H}_{ij} = \sqrt{1-\epsilon_{ij}^2}\hat{\mathbf{H}}_{ij} + \epsilon_{ij}\mathbf{V}_{ij}, \tag{3}$$

where each entry of $\mathbf{V}_{ij}$ follows $\mathcal{CN}(0, \mathbf{I})$, $\mathbf{V}_{ij}$ is independent of $\mathbf{H}_{ij}$, and $\epsilon_{ij} \in [0, 1]$ is used to measure the accuracy of the channel estimation.

Setting $\mathbf{H}_{\mathrm{B}} = \hat{\mathbf{H}}_{\mathrm{AB}}\hat{\mathbf{H}}_{\mathrm{AB}}^H$, $\mathbf{H}_{\mathrm{B}}$ can be decomposed as $\mathbf{H}_{\mathrm{B}} = \mathbf{W}_{\mathrm{B}}\Lambda\mathbf{W}_{\mathrm{B}}^H$ by using the singular value decomposition (SVD), where $\Lambda = \mathrm{diag}(\lambda_1, \lambda_2)$ and $\lambda_1 \geq \lambda_2 \geq 0$. $\mathbf{W}_{\mathrm{B}}$ is an unitary matrix, i.e., $\mathbf{W}_{\mathrm{B}}\mathbf{W}_{\mathrm{B}}^H = \mathbf{I}$. Based on the above description, we choose $\mathbf{W}_B$ as the combiner matrix at user B. Similarly, $\mathbf{W}_E$ can be constructed in the same way as $\mathbf{W}_B$, and then is used as the combining matrix at user E. Consequently, while taking consideration of channel estimation error, the combined signals at Bob and Eve are given by

$$\begin{aligned}\mathbf{Y}_B &= \mathbf{W}_{\mathrm{B}}^H\mathbf{r}_B \\ &= \sqrt{1-\epsilon_{AB}^2}\mathbf{W}_{\mathrm{B}}^H\hat{\mathbf{H}}_{\mathrm{AB}}\mathbf{x}_A + \epsilon_{AB}\mathbf{W}_{\mathrm{B}}^H\mathbf{V}_{\mathrm{AB}}\mathbf{x}_A + \\ &\quad \mathbf{W}_{\mathrm{B}}^H\left(\mathbf{H}_{\mathrm{BE}}\mathbf{x}_E + \mathbf{n}_B\right),\end{aligned} \tag{4}$$

$$\begin{aligned}\mathbf{Y}_E &= \mathbf{W}_{\mathrm{E}}^H\mathbf{r}_E \\ &= \sqrt{1-\epsilon_{AE}^2}\mathbf{W}_{\mathrm{E}}^H\hat{\mathbf{H}}_{\mathrm{AE}}\mathbf{x}_A + \epsilon_{AE}\mathbf{W}_{\mathrm{E}}^H\mathbf{V}_{\mathrm{AE}}\mathbf{x}_A + \\ &\quad \mathbf{W}_{\mathrm{E}}^H\left(\mathbf{H}_{\mathrm{EE}}\mathbf{x}_E + \mathbf{n}_E\right).\end{aligned} \tag{5}$$

Therefore, the average SINR of the combined signal at Bob's side γ_B is given by

$$\gamma_{\mathrm{B}} = \Omega_B Tr(\mathbf{W}_B^H\hat{\mathbf{H}}_{\mathrm{AB}}\hat{\mathbf{H}}_{\mathrm{AB}}^H\mathbf{W}_B), \tag{6}$$

where $\Omega_B = \frac{P_A(1-\epsilon_{AB}^2)}{2\epsilon_{AB}^2P_A+\sigma_B^2+2P_E} = \frac{\Phi_B(1-\epsilon_M^2)}{2\epsilon_M^2\Phi_B+1+2\Phi_J}$. Herein, $\Phi_B = P_A/\sigma_B^2$, $\Phi_J = P_E/\sigma_B^2$. For convenience, $\epsilon_{AB}^2 = \epsilon_M^2$.

Obviously, the denominator is constant while the numerator is equal to the sum of the eigenvalues of the Wishart matrix $\hat{\mathbf{H}}_{\mathrm{AB}}\hat{\mathbf{H}}_{\mathrm{AB}}^H$. Based on the random matrix theory, the joint PDF of the ordered eigenvalues of $\mathbf{H}_{\mathrm{B}}$ can be expressed as [13]

$$p(\lambda_1, \lambda_2) = (\lambda_2 - \lambda_1)^2 e^{-\lambda_1-\lambda_2}. \tag{7}$$

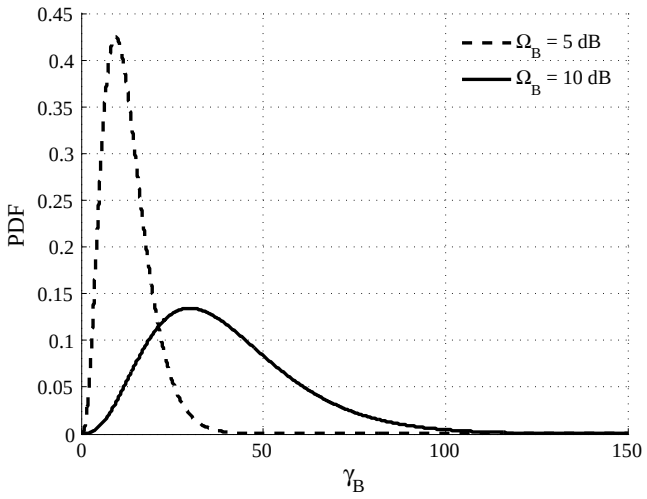

Fig. 2. The PDFs of γ_B when Ω_B are 5 dB and 10 dB, respectively.

Let $\lambda = \lambda_1 + \lambda_2$, then $\gamma_B = \Omega_B \lambda$. The CDF of γ_B can be expressed as

$$\begin{aligned} F_{\gamma_B}(\gamma_B) &= Pr\left(\Omega_B\left(\lambda_1+\lambda_2\right) \le \gamma_B\right) \\ &= \int_0^{\frac{\gamma_B}{2\Omega_B}} \int_{\lambda_2}^{\frac{\gamma_B}{\Omega_B}-\lambda_2} p(\lambda_1,\lambda_2) d\lambda_1 d\lambda_2 \\ &= 1 - \left[(\frac{\gamma_B}{\Omega_B})^3 + 3(\frac{\gamma_B}{\Omega_B})^2 + 6(\frac{\gamma_B}{\Omega_B}) + 6\right] \frac{e^{-\frac{\gamma_B}{\Omega_B}}}{6}. \end{aligned} \tag{8}$$

Differentiating (8) with regard to γ_B, the PDF of γ_B is established as follows

$$\begin{aligned} f_{\gamma_B}(\gamma_B) &= \frac{dF_{\gamma_B}(\gamma_B)}{d\gamma_B} \\ &= \frac{\gamma_B^3}{6\Omega_B^4} e^{-\frac{\gamma_B}{\Omega_B}}. \end{aligned} \tag{9}$$

Fig. 2 shows the PDFs of γ_B with respect to different values of Φ_B.

It is assumed that perfect self-interference cancellation can be performed at the Eve's side. Likewise, we have the received average SINR at Eve

$$\gamma_{\mathrm{E}} = \Omega_E Tr(\mathbf{W}_E^H \hat{\mathbf{H}}_{\mathrm{AB}} \hat{\mathbf{H}}_{\mathrm{AB}}^H \mathbf{W}_E), \tag{10}$$

where $\Omega_E = \frac{(1-\epsilon_{AE}^2)P_A}{2\epsilon_{AE}^2 P_A + \sigma_E^2} = \frac{(1-\epsilon_W^2)\Phi_E}{2\epsilon_W^2\Phi_E+1}$, $\Phi_E = P_A/\sigma_E^2$, and $\epsilon_{AE}^2 = \epsilon_W^2$.

The CDF and PDF of γ_E are

$$F_{\gamma_E}(\gamma_E) = 1 - \left[(\frac{\gamma_E}{\Omega_E})^3 + 3(\frac{\gamma_E}{\Omega_E})^2 + 6(\frac{\gamma_E}{\Omega_E}) + 6\right] \frac{e^{-\frac{\gamma_E}{\Omega_E}}}{6}, \tag{11}$$

and

$$f_{\gamma_E}(\gamma_E) = \frac{\gamma_E^3}{6\Omega_E^4} e^{-\frac{\gamma_E}{\Omega_E}}, \tag{12}$$

respectively.

III. Secrecy performance analysis

A. Probability of Positive Secrecy Capacity

According to [2], the secrecy capacity for the MIMO wiretap channel over Rayleigh fading is defined as the difference between the main channel capacity $C_M = \log_2(1+\gamma_B)$ and the wiretap channel capacity $C_W = \log_2(1+\gamma_E)$ as the following form,

$$C_s = \begin{cases} C_M - C_W, & \gamma_B > \gamma_E \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

Therefore, the probability of positive secrecy capacity refers to the event that the secrecy capacity can be achieved, i.e. $Pr(C_s > 0)$, thus with regard to its definition, (13) can be further rewritten as follows,

$$\begin{aligned} Pr(C_s > 0) &= Pr(\gamma_B > \gamma_E) \\ &= \int_0^{\infty} \int_0^{\gamma_B} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_E d\gamma_B \\ &= \int_0^{\infty} f_{\gamma_B}(\gamma_B) F_{\gamma_E}(\gamma_B) d\gamma_B. \end{aligned} \tag{14}$$

Substituting (9) and (11) into (14), we use the equation (15) [14, Eq. (3.351.3)],

$$\int_0^{\infty} x^n e^{-\mu x} dx = \begin{cases} n!\mu^{-n-1}, & \text{if n = 0,1,2,}\cdots\text{, } \mu > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

then we have the closed-form expression for the probability of positive secrecy capacity in (16) shown on the top of next page.

B. Secrecy Outage Probability

The outage probability of the secrecy capacity is defined as the probability that the secrecy capacity C_s falls below the target secrecy rate R_s, i.e.,

$$P_{out}(R_s) = Pr(C_s < R_s). \tag{17}$$

Secrecy outage probability can be conceptually explained as two cases: (i) $C_s < R_s$ whilst positive secrecy capacity is guaranteed; (ii) $P_{out}(R_s)$ definitely happens when the secrecy capacity is non-positive. (17) can thus be rewritten as follows [10]

$$\begin{aligned} P_{out}(R_s) &= Pr(C_s < R_s | \gamma_B > \gamma_E) Pr(\gamma_B > \gamma_E) \\ &\quad + Pr(\gamma_B < \gamma_E) \\ &= \int_0^{\infty} \int_{\gamma_E}^{\gamma_0} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_B d\gamma_E \\ &\quad + \int_0^{\infty} \int_0^{\gamma_E} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_B d\gamma_E \\ &= \int_0^{\infty} f_{\gamma_E}(\gamma_E) \left[\int_0^{\gamma_0} - \int_0^{\gamma_E}\right] f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E \\ &\quad + \int_0^{\infty} \int_0^{\gamma_E} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_B d\gamma_E \\ &= \int_0^{\infty} F_{\gamma_B}(\gamma_0) f_{\gamma_E}(\gamma_E) d\gamma_E, \end{aligned} \tag{18}$$

$$Pr(C_s > 0) = 1 - \frac{1}{\Omega_B^4 \Omega_E^3} \left[20(\frac{1}{\Omega_B} + \frac{1}{\Omega_E})^{-7} + 10\Omega_E(\frac{1}{\Omega_B} + \frac{1}{\Omega_E})^{-6} + \Omega_E^2(\frac{1}{\Omega_B} + \frac{1}{\Omega_E})^{-5} + \Omega_E^3(\frac{1}{\Omega_B} + \frac{1}{\Omega_E})^{-4} \right]. \quad (16)$$

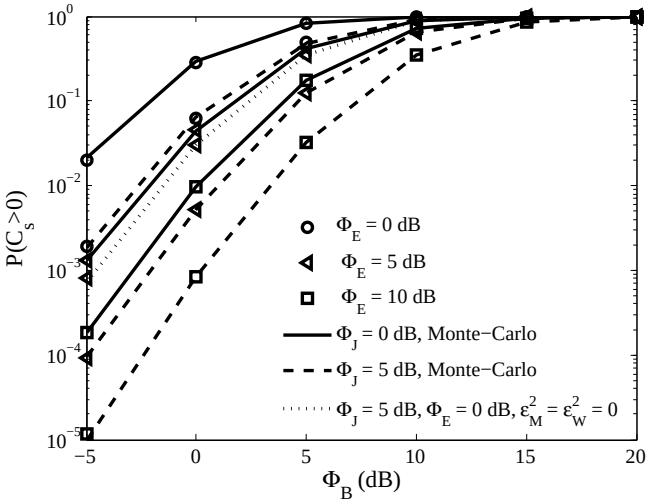

Fig. 3. Probability of positive secrecy capacity against Φ_B for selected values of Φ_E for the case of Φ_J = 0 dB and Φ_J = 5 dB whilst $\epsilon_M^2 = 0.01$, $\epsilon_W^2 = 0.1$.

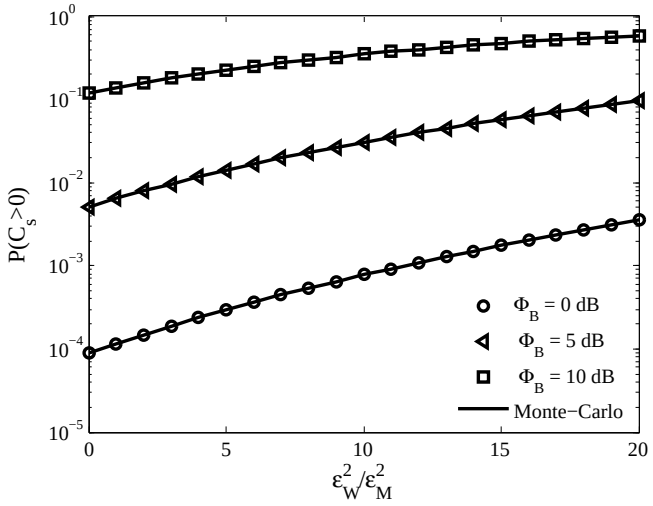

Fig. 4. Probability of positive secrecy capacity against $\epsilon_W^2/\epsilon_M^2$ for selected values of Φ_B while $\epsilon_M^2 = 0.01$, Φ_J = 5 dB and Φ_E = 5 dB.

where $\gamma_0 = M(1+\gamma_E) - 1$, $M = 2^{R_s}$.

Similarly, substituting (8) and (12) into (18) using (15), the closed-form expression for secrecy outage probability can be eventually derived as in (19) shown on the top of next page.

IV. Numerical Results and discussions

In this section, we perform the Monte-Carlo simulation to validate the accuracy of the closed-form expressions for probability of positive secrecy capacity and secrecy outage probability. In the following figures, the curves only using markers are the theoretical results, while the ones in lines are the Monte-Carlo simulation results.

Fig. 3 shows the simulation and analytic results of the probability of positive secrecy capacity against Φ_B for selected values of Φ_E when $\epsilon_M^2 = 0.01$ and $\epsilon_W^2 = 0.1$ for the cases: (i) Φ_J = 0 dB, (ii) Φ_J = 5 dB. One can observe that the numerical results are in perfect match with our analytical results. Notably, we can obtain the conclusions below: (i) Pr($C_s > 0$) increases with Φ_B for a fixed Φ_E. (ii) The higher Φ_E, the lower of probability of positive secrecy capacity. (iii) More importantly, the jamming power Φ_J has a critical role to play in the probability of positive secrecy capacity for fixed γ_E. The larger values of Φ_J, the worse of Pr($C_s > 0$). (iv) Additionally, there exists secrecy loss of imperfect CSI compared with the case of perfect channel estimation (ϵ_M^2 = 0 and ϵ_W^2 = 0) at receiver sides.

Fig. 4 explores the relationship of probability of positive secrecy capacity against the ratio of ϵ_W^2 and ϵ_M^2 whilst $\epsilon_M^2 = 0.01$, Φ_J = 5 dB and Φ_E = 5 dB for selected values of Φ_B. It is saying that the higher the ratio, the much probable the event that the positive secrecy capacity can be achieved.

Similarly, Fig. 5 and Fig. 6 examine the simulation and analysis results of the secrecy outage probability of physical layer security with regard to two cases: (i) fixed ϵ_M^2 and ϵ_W^2 whilst varying Φ_B and Φ_E; (ii) changing the ratio of ϵ_B^2 and ϵ_W^2 while fixing Φ_J = 5 dB and Φ_E = 5 dB for selected values of Φ_B, namely, 10 dB, 15 dB and 25 dB. Notably, we can easily draw the same conclusion about the accuracy of our derived expression with Monte-Carlo simulation results.

Additionally, as shown in Fig. 5, the secrecy outage probability degrades with the increase of Φ_B for specific values Φ_E and Φ_J. More importantly, there exists an error floor due to the imperfect channel estimation at the receiver sides in comparison with the case, i.e., ϵ_M^2 = 0 and ϵ_W^2 = 0. As Φ_B is much larger than Φ_J regarding a fixed Φ_E, Ω_B converges to the same value for different Φ_J with a limited value, which consequently makes their secrecy outage probabilities converge to the error floor.

When it comes to Fig. 6, the secrecy outage probability witnesses a completely opposite trend compared with that of the probability of positive secrecy capacity, shown in Fig. 4. Furthermore, the larger of the gap between Φ_B and Φ_E, the less likely the secrecy outage probability.

V. Conclusion

In this paper, we have analyzed secrecy performance of the MIMO wiretap channel with channel estimation errors at the legitimate destination and eavesdropper's receivers whilst in the presence of an active eavesdropper. The probability of

$$P_{out}(R_s) = 1 - \frac{exp(\frac{1-M}{\Omega_B})}{6\Omega_B^3\Omega_E^4}\Bigg[120M^3(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-7} + 60M^2\left(\Omega_B - 1 + M\right)(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-6}$$
$$+ 12M\left(1 - 2\Omega_B + 2\Omega_B^2 - 2M + 2\Omega_B M + M^2\right)(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-5} \quad (19)$$
$$+ \left(-1 + 6\Omega_B^3 + 3\Omega_B - 6\Omega_B^2 + 3M - 6\Omega_B M + 6\Omega_B^2 M - 3M^2 + 3\Omega_B M^2 + M^3\right)(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-4}\Bigg].$$

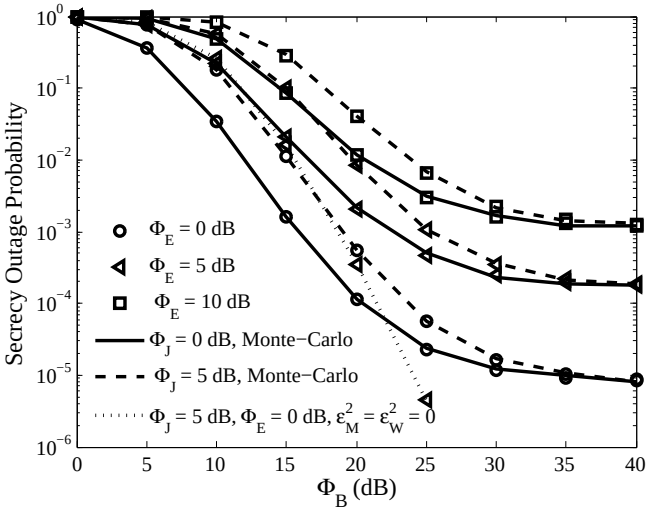

Fig. 5. Secrecy outage probability against Φ_B for selected values of Φ_E for the case of Φ_J = 0 dB and Φ_J = 5 dB whilst $\epsilon_M^2 = 0.01$, $\epsilon_W^2 = 0.1$ and $R_s = 0.5$ [bits/s/Hz].

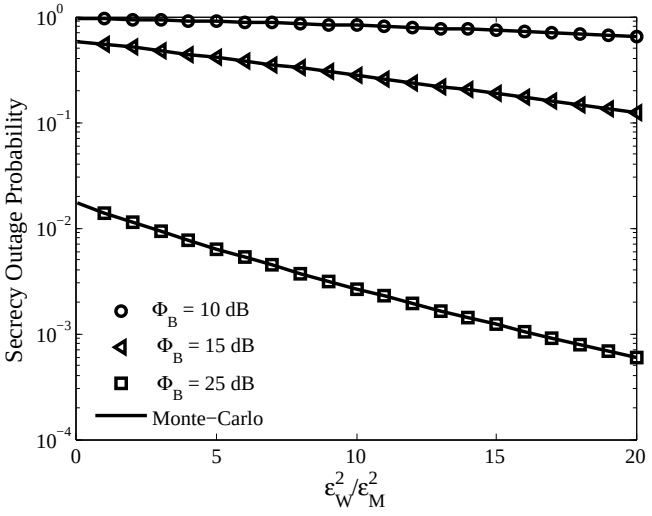

Fig. 6. Secrecy outage probability against $\epsilon_W^2/\epsilon_M^2$ for selected values of Φ_B while $\epsilon_M^2 = 0.01$, Φ_J = 5 dB, Φ_E = 5 and $R_s = 0.5$ [bits/s/Hz].

positive secrecy capacity and secrecy outage probability were derived with closed-form expressions through the PDFs and CDFs of the receive SINRs. Finally, the theoretical analysis are confirmed by the Monte-Carlo simulation results by comparing the secrecy performances with different levels of channel estimation errors, received SINRs and jamming signals.

ACKNOWLEDGMENT

This work has been supported by the ETS' research chair of physical layer security in wireless networks.

REFERENCES

[1] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[2] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.
[3] W. Saad, X. Zhou, M. Debbah, and H. Poor, "Wireless physical layer security: Part 1 [guest editorial]," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 15–15, Jun. 2015.
[4] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.
[5] T. Allen and N. Al-Dhahir, "Performance analysis of a secure STBC with coherent and differential detection," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, Mar. 2015, pp. 522–527.
[6] M. Atallah, G. Kaddoum, and L. Kong, "A survey on cooperative jamming applied to physical layer security," in *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, Oct. 2015, pp. 1–5.
[7] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.
[8] 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, Nov. 2010.
[9] A. Mukherjee and A. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov. 2011, pp. 265–269.
[10] K. S. Ahn, S.-W. Choi, and J.-M. Ahn, "Secrecy performance of maximum ratio diversity with channel estimation error," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2167–2171, Nov. 2015.
[11] F. Oggier and B. Hassibi, "A perspective on the MIMO wiretap channel," *Proc. IEEE*, vol. 103, no. 10, pp. 1874–1882, Oct. 2015.
[12] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[13] I. E. Telatar *et al.*, "Capacity of multi-antenna gaussian channels," *European transactions on telecommunications*, vol. 10, no. 6, pp. 585–595, 1999.
[14] D. Zwillinger, *Table of integrals, series, and products*. Elsevier, 2014.