Secure Spatial Modulation with A Full-Duplex Receiver

Chaowen Liu, Lie-Liang Yang, *Fellow, IEEE*, and Wenjie Wang, *Member, IEEE*

Abstract—**We propose and investigate a full-duplex receiver assisted secure spatial modulation (FDR-SSM) scheme, whose security is enhanced by the jamming sent from a full-duplexing legal receiver. In our FDR-SSM system, jamming signals are designed to allow the legal receiver free from self-interference (SI), while imposing time-varying interference on the passive eavesdropper. Therefore, the FDR-SSM scheme can maintain all the advantages of spatial modulation. In this paper, the secrecy performance of the FDR-SSM system is analyzed via analyzing its ergodic secrecy rate (ESR). Furthermore, the asymptotic ESR is analyzed, when assuming that the number of transmit antennas at the legal receiver approaches infinite. Finally, performance results are provided to demonstrate the efficiency of the FDR-SSM scheme, and to verify the analytical expressions.**

Index Terms—**MIMO, spatial modulation, full-duplex, physical layer security, artificial jamming.**

I. INTRODUCTION

AS a MIMO transmission scheme, spatial modulation (SM) exhibits a range of advantages over the other MIMO transmission schemes, and it has been recognized as a promising transmission option for MIMO systems [1]. However, due to the broadcast nature of radio signals, like the other MIMO systems, SM systems may suffer from the malicious eavesdropping conducted by unintended receivers.

In recent years, physical layer security (PLS) has widely been recognized as an attractive approach to achieve secrecy enhancement via exploiting the characteristics of wireless channels. Specifically in association with SM, several recently published references [2–5] have addressed the PLS issues in point-to-point communications scenarios. In more detail, the authors of [2] have analyzed the secrecy capacity of the space shift keying (SSK) assisted SM systems, when assuming communications over binary symmetric channels. The secrecy mutual information of SM systems has been derived in [3], when assuming that both the intended receiver and the eavesdropper employ a single antenna. Assuming underdeterminant scenarios, the authors of [4] have proposed to exploit all the transmit antennas (TAs) for joint transmission of SM signals and jamming signals, so as to enhance the secrecy performance of the SM-MIMO systems. In [5], a general SSK modulated wiretap system has been studied, and an optimal precoding scheme has been introduced to maximize the secrecy rate of the system. In the SM scenario where precoding-aided spatial modulation (PSM) [6, 7] is employed, the authors of [8] and [9] have proposed respectively the secrecy precoding and artificial noise (AN) strategies for enhancing the secrecy performance.

In the aforementioned schemes, secrecy-enhancement is typically implemented at transmitter. By contrast, the recently emerged full-duplex (FD) techniques [10] may allow a receiver to simultaneously emit jamming signals and receive information, although there are still challenges in terms of FD

C. Liu and W. Wang are with the Ministry of Education Key Laboratory for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China (E-mail: liucwhb@gmail.com, wjwang@mail.xjtu.edu.cn).

L.-L. Yang is with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK (E-mail: lly@ecs.soton.ac.uk, http://users.ecs.soton.ac.uk/lly/).

implementation [11, 12]. Hence, a FD receiver with jamming capability may be deployed to improve the secrecy performance, without imposing extra burden on the transmitter. This security-enhancement approach can also be applied to the secure SM (SSM) systems. However, to the best of our knowledge, no prior work has considered the joint of FD receiver with SSM.

With the above motivation, in this letter, we propose a novel FD receiver based secure SM (FDR-SSM) scheme to enhance the secrecy performance of SM systems. In our FDR-SSM scheme, the transmitter sends SM signals in the same way as in the conventional SM [1], while the FD receiver can simultaneously emit jamming signals and detect the SM signals sent by the transmitter. Furthermore, in order not to impose negative effect on the detection of SM signals, the jamming signals are designed to be sent in the null space of the FD receiver's self-interference channel. Hence, the FDR-SSM scheme is capable of achieving an enhanced secrecy performance, while taking the advantages of low-cost transmission/detection implementation of the conventional SM. The main contributions of this letter are summarized as follows:

1) A novel FDR-SSM scheme as above-described is proposed for enhancing the secrecy performance of SM systems, while simultaneously enjoying all the advantages of conventional SM systems.
2) The ergodic secrecy rate (ESR) of FDR-SSM systems with finite-alphabet signaling is analyzed, and a closed-form expression is derived for the asymptotic ESR of the FDR-SSM systems with the legitimate FD receiver having a large number of transmit antennas.
3) Furthermore, the secrecy performance of the FDR-SSM systems is characterized by our performance results, which are obtained from simulations or numerical evaluation of the closed-form expressions derived.

II. SYSTEM MODEL FOR THE FDR-SSM SYSTEM

The FDR-SSM system considered consists of a M_a-antenna transmitter (Alice), a M_b-antenna FD receiver (Bob), and a M_e-antenna passive eavesdropper (Eve). In order to implement the FDR, Bob's M_b antennas are divided into M_r receive antennas (RAs) and M_t TAs, satisfying $M_b = M_r + M_t$. We assume that $M_t > M_r$, so that Bob can emit AN without imposing self-interference (SI) on its receiving channels. Owing to this, Bob's receiving is not affected by the jamming signals, while Eve has no effective measures to remove the jamming signals. Consequently, the secrecy performance of the FDR-SSM system can be enhanced.

For simplicity, we let $M_a = 2^{t_a}$. Then, following the principles of SM [1], t_a binary bits per symbol period are utilized to activate one out of M_a TAs by Alice for conveying a M_m-ary amplitude-phase modulation (APM) symbol, consisting of $t_m = \log_2 M_m$ binary bits, to Bob. Consequently, a SM symbol can deliver in total $t = t_a + t_m$ bits per symbol and can be represented as

$$\boldsymbol{x}_{jk} = \boldsymbol{e}_j s_k, \qquad (1)$$

where $\boldsymbol{e}_j$ is the jth column vector of the identity matrix $\boldsymbol{I}_{M_a}$, which is selected by the t_a bits, while s_k is the kth APM symbol by the t_m bits. We assume that the APM symbol is normalized to $\mathbb{E}[|s_k|^2] = 1$, and hence, $\mathbb{E}[|\boldsymbol{x}_{jk}|^2] = 1$.

Let $\boldsymbol{E}_{SI} \in \mathbb{C}^{M_r \times M_t}$ denote Bob's SI channel. Using the singular value decomposition (SVD), we can express $\boldsymbol{E}_{SI}$ as

$$\boldsymbol{E}_{SI} = \boldsymbol{U}[\boldsymbol{\Lambda} \ \ \boldsymbol{0}][\boldsymbol{V}_S \ \ \boldsymbol{V}_\perp]^H, \tag{2}$$

where $\boldsymbol{V}_\perp \in \mathbb{C}^{M_t \times (M_t - M_r)}$ determines a null space of $\boldsymbol{E}_{SI}$. Accordingly, the jamming signals sent in the null-space by Bob can be written as

$$\boldsymbol{n} = \boldsymbol{V}_\perp \boldsymbol{\omega}, \tag{3}$$

where $\boldsymbol{\omega} \in \mathbb{C}^{(M_t - M_r) \times 1}$ stands for a random AN, whose entries are the complex Gaussian random variables distributed with zero mean and a variance of $1/(M_t - M_r)$.

Let $\boldsymbol{H} \in \mathbb{C}^{M_r \times M_a}$, $\boldsymbol{G} \in \mathbb{C}^{M_e \times M_a}$ and $\boldsymbol{F} \in \mathbb{C}^{M_e \times M_t}$ denote the channels from Alice to Bob, that from Alice to Eve and that from Bob to Eve, respectively. Then, in each transmission epoch, the signal observations obtained by Bob and Eve can be respectively expressed as

$$\boldsymbol{y}_b = \sqrt{P_a}\boldsymbol{H}\boldsymbol{x}_{jk} + \sqrt{P_b}\boldsymbol{E}_{SI}\boldsymbol{n} + \boldsymbol{z}_b$$
$$= \sqrt{P_a}\boldsymbol{H}\boldsymbol{x}_{jk} + \boldsymbol{z}_b, \tag{4}$$
$$\boldsymbol{y}_e = \sqrt{P_a}\boldsymbol{G}\boldsymbol{x}_{jk} + \sqrt{P_b}\boldsymbol{F}\boldsymbol{n} + \boldsymbol{z}_e, \tag{5}$$

where we have the second equation in (4) because of $\boldsymbol{E}_{SI}\boldsymbol{n} = \boldsymbol{E}_{SI}\boldsymbol{V}_\perp \boldsymbol{\omega} = \boldsymbol{0}$, P_a and P_b denote the transmission power at Alice and Bob, respectively. $\boldsymbol{z}_b \in \mathbb{C}^{M_r \times 1}$ and $\boldsymbol{z}_e \in \mathbb{C}^{M_e \times 1}$ represent the zero-mean complex Gaussian noise vectors at Bob and Eve, which have the covariance matrices of $\sigma_b^2 \boldsymbol{I}_{M_r}$ and $\sigma_e^2 \boldsymbol{I}_{M_e}$, respectively. Below, we analyze the secrecy rate of the FDR-SSM system by assuming that all the involved channels experience flat Rayleigh fading. Note that, it is usually reasonable to assume the Rayleigh fading for Bob's SI channel. This is because in FD, most SI is canceled in the propagation and analog domains, and only a small portion of random SI enters the digital domain.

III. ERGODIC SECRECY RATE ANALYSIS

In this section, we first analyze the ergodic secrecy rate (ESR) of the proposed FDR-SSM system. Then, by letting the number of TAs at Bob approach infinite, we analyze the asymptotic ESR of the FDR-SSM system.

A. Ergodic Secrecy Rate

Following the theory in [13], the ESR of the FDR-SSM system can be expressed as

$$R_s = [R_b - R_e]^+, \tag{6}$$

where R_b and R_e represent the ergodic rates achieved respectively by Bob and Eve.

According to (4), the communication channel from Alice to Bob is a discrete-input continuous-output memoryless channel (DCMC). Hence, with the aid of the DCMC capacity results

provided in [14], Bob's ergodic rate can be formulated as

$$R_b = \log_2(M_a M_m) - 1/(M_a M_m)$$
$$\cdot \sum_{j,k} \mathbb{E}_{\boldsymbol{H}, \boldsymbol{z}_b}\left[\log_2 \sum_{\hat{j}, \hat{k}} \exp\left(\frac{-\left\|\sqrt{P_a}\boldsymbol{H}\boldsymbol{d}_{\hat{j}\hat{k}}^{jk} + \boldsymbol{z}_b\right\|^2 + \|\boldsymbol{z}_b\|^2}{\sigma_b^2}\right)\right]$$
$$= \log_2(M_a M_m) - M_r/\ln 2$$
$$- \frac{1}{M_a M_m}\sum_{j,k}\mathbb{E}_{\boldsymbol{H}, \boldsymbol{z}_b}\left[\log_2 \sum_{\hat{j}, \hat{k}} \exp\left(-\Phi\right)\right], \tag{7}$$

where $\Phi = \|\sqrt{P_a}\boldsymbol{H}\boldsymbol{d}_{\hat{j}\hat{k}}^{jk} + \boldsymbol{z}_b\|^2/\sigma_b^2$, and $\boldsymbol{d}_{\hat{j}\hat{k}}^{jk} = \boldsymbol{x}_{jk} - \boldsymbol{x}_{\hat{j}\hat{k}}$, with $\boldsymbol{x}_{jk}$ and $\boldsymbol{x}_{\hat{j}\hat{k}}$ being any pair of SM symbols.

Let us now turn to derive the ergodic rate attainable by Eve. As shown in (5), the SM signals received by Eve is contaminated by both the time-varying AN and the thermal noise. Accordingly, the equivalent noise observed by Eve is

$$\boldsymbol{z}_v = \sqrt{P_b}\boldsymbol{F}\boldsymbol{n} + \boldsymbol{z}_e, \tag{8}$$

which is a colored Gaussian noise with zero mean and a covariance matrix of

$$\boldsymbol{\Sigma}_v = \frac{P_b}{M_t - M_r}\boldsymbol{F}\boldsymbol{V}_\perp \left(\boldsymbol{V}_\perp\right)^H \boldsymbol{F}^H + \sigma_e^2 \boldsymbol{I}_{M_e}. \tag{9}$$

Upon whitening $\boldsymbol{z}_v$ by multiplying $\boldsymbol{\Sigma}_v^{-1/2}$, we obtain

$$\boldsymbol{y}_w = \boldsymbol{\Sigma}_v^{-1/2}\boldsymbol{y}_e = \sqrt{P_a}\boldsymbol{G}_w\boldsymbol{x}_{jk} + \boldsymbol{z}_w, \tag{10}$$

where $\boldsymbol{G}_w = \boldsymbol{\Sigma}_v^{-1/2}\boldsymbol{G}$, and $\boldsymbol{z}_w = \boldsymbol{\Sigma}_v^{-1/2}\boldsymbol{z}_v$. It can be shown that after the whitening operation, $\boldsymbol{z}_w$ becomes a white Gaussian noise vector with zero mean and a covariance matrix of $\boldsymbol{I}_{M_e}$. Consequently, similar to (7), we can express the ergodic rate attainable by Eve as

$$R_e = \log_2(M_a M_m) - M_e/\ln 2$$
$$- \frac{1}{M_a M_m}\sum_{j,k}\mathbb{E}_{\boldsymbol{G}_w, \boldsymbol{z}_w}\left[\log_2 \sum_{\hat{j}, \hat{k}} \exp\left(-\Psi\right)\right], \tag{11}$$

where, by definition, $\Psi = \|\sqrt{P_a}\boldsymbol{G}_w\boldsymbol{d}_{\hat{j}\hat{k}}^{jk} + \boldsymbol{z}_w\|^2$.

Finally, the ESR of the FDR-SSM system can be obtained by substituting (7) and (11) into (6).

Note that, it is in general very hard to further simplify the results of (7) and (11), as the expectation in both the formulas contains an integration, which involves several random matrices and vectors. For this sake, we introduce the Jensen's inequality to derive a lower-bound for R_b of (7), which is stated by the following theorem.

Theorem 1: A lower-bound for R_b of the ergodic rate attained by Bob is given by

$$R_b^{\text{LB}} = \log_2(M_a M_m) + M_r - M_r/\ln 2$$
$$- \frac{1}{M_a M_m}\sum_{j,k}\log_2 \sum_{\hat{j}, \hat{k}} \left(1 + \frac{P_a}{2\sigma_b^2}D_{\hat{j}\hat{k}}^{jk}\right)^{-M_r}, \tag{12}$$

where $D_{\hat{j}\hat{k}}^{jk} = \|\boldsymbol{d}_{\hat{j}\hat{k}}^{jk}\|^2$.

Proof: Please see Appendix A. ∎

After careful analysis, we can further derive a nearly accurate approximation for R_b, which is given as follows.

Proposition 1: An approximation for R_b of the ergodic rate attained by Bob can be expressed as

$$R_b^{\text{AP}} = \log_2(M_a M_m)$$
$$- \frac{1}{M_a M_m} \sum_{j,k} \log_2 \sum_{\hat{j},\hat{k}} \left(1 + \frac{P_a}{2\sigma_b^2} D_{\hat{j}\hat{k}}^{jk}\right)^{-M_r}. \quad (13)$$

Proof: Please see Appendix B. ∎

Similarly, following the steps for deriving (12) and (13), we can obtain an approximation for R_e, which is stated by the following theorem.

Theorem 2: An approximation for R_e of the ergodic rate attainable by Eve is given by

$$R_e^{\text{AP}} = \log_2(M_a M_m) - M_e$$
$$- \frac{1}{M_a M_m} \sum_{j,k} \log_2 \sum_{\hat{j},\hat{k}} \mathbb{E}_{\boldsymbol{G}_w, \boldsymbol{z}_w} \left[\exp\left(-\Psi\right)\right]. \quad (14)$$

Proof: Following the derivations for (12), we can obtain a lower-bound for R_e as

$$R_e^{\text{LB}} = \log_2(M_a M_m) - M_e/\ln 2$$
$$- \frac{1}{M_a M_m} \sum_{j,k} \log_2 \sum_{\hat{j},\hat{k}} \mathbb{E}_{\boldsymbol{G}_w, \boldsymbol{z}_w} \left[\exp\left(-\Psi\right)\right]. \quad (15)$$

Then, as done in the Appendix B, we can obtain (14) by adding a constant of $M_e \left(1/\ln 2 - 1\right)$ to the lower-bound of (15). ∎

Consequently, an approximation to R_s can be expressed as $R_s^{\text{AP}} = [R_b^{\text{AP}} - R_e^{\text{AP}}]^+$. However, R_e^{AP} in (14) is not in closed-form. Hence, we can only find R_s^{AP} via simulations, which is prohibitive, if the number of TAs at Bob is high. Therefore, in the next subsection, we derive the closed-form formulas for R_e^{AP} and R_s^{AP}, when assuming $M_t \gg M_r, M_e$. Note that this may be the case in practice, when Bob is a full-duplex base-station.

B. Asymptotic ESR

When $M_t \to \infty$, the covariance matrix in (9) converges to

$$\boldsymbol{\Sigma} = \lim_{M_t \to \infty} \boldsymbol{\Sigma}_v = \sigma_v^2 \boldsymbol{I}_{M_e} \quad (16)$$

with $\sigma_v^2 = P_b + \sigma_e^2$. In other words, when $M_t \to \infty$, $\boldsymbol{z}_v$ converges to a white Gaussian noise vector with zero mean and a covariance matrix of $\sigma_v^2 \boldsymbol{I}_{M_e}$. In this case, the expectation in (14) can be simplified to

$$\mathbb{E}_{\boldsymbol{G}_w, \boldsymbol{z}_w} \left[\exp\left(-\Psi\right)\right]$$
$$= \mathbb{E}_{\boldsymbol{G}} \left[\mathbb{E}_{\boldsymbol{z}_v} \left[\exp\left(-\left\|\sqrt{P_a}\boldsymbol{G}\boldsymbol{d}_{\hat{j}\hat{k}}^{jk} + \boldsymbol{z}_v\right\|^2 / \sigma_v^2\right)\right]\right]$$
$$= \frac{1}{2^{M_e}} \left(1 + \frac{P_a}{2\sigma_v^2} D_{\hat{j}\hat{k}}^{jk}\right)^{-M_e}, \quad (17)$$

where the last equation is obtained due to the formulae of (57) and (63) in [15]. Substituting (17) into (14), the asymptotic ergodic rate R_e^{AP} of the eavesdropper channel is

$$\tilde{R}_e^{\text{AP}} = \log_2(M_a M_m)$$
$$- \frac{1}{M_a M_m} \sum_{j,k} \log_2 \sum_{\hat{j},\hat{k}} \left(1 + \frac{P_a}{2\sigma_v^2} D_{\hat{j}\hat{k}}^{jk}\right)^{-M_e}. \quad (18)$$

Consequently, from $R_s^{\text{AP}} = [R_b^{\text{AP}} - R_e^{\text{AP}}]^+$ we can obtain the asymptotic secrecy rate R_s^{AP}, which is expressed as

$$\tilde{R}_s^{\text{AP}} = \left[\frac{1}{M_a M_m} \sum_{j,k} \log_2 \left(\frac{\sum_{\hat{j},\hat{k}} \left(1 + \frac{P_a}{2\sigma_v^2} D_{\hat{j}\hat{k}}^{jk}\right)^{-M_e}}{\sum_{\hat{j},\hat{k}} \left(1 + \frac{P_a}{2\sigma_b^2} D_{\hat{j}\hat{k}}^{jk}\right)^{-M_r}}\right)\right]^+. \quad (19)$$

IV. SIMULATION AND NUMERICAL RESULTS

In order to demonstrate the effectiveness of Bob's transmission of AN, we set $\sigma^2 = \sigma_b^2 = \sigma_e^2$ and change the transmit power of P_a and P_b under the constraint of $P_a + P_b = 1$. Note that the average SNR per symbol shown in figures is given by $\text{SNR} = 1/\sigma^2$.

Fig. 1 depicts the ESR versus average SNR performance of the FDR-SSM systems. First, the results show that the ESR steadily increases in the low SNR region. After reaching a maximum value, the ESR decreases, when further increasing the SNR. The reason behind is that the ESR depends mainly on the Alice-Bob channel's quality in low SNR region, while depends mainly on the AN in relatively high SNR region. Second, the results with respect to P_a imply that, at a given SNR, there is an optimum power-allocation between P_a and P_b, which results in the highest ESR. Furthermore, at a given SNR, the ESR decreases as M_e increases, as Eve becomes more powerful for wiretapping when having more antennas.
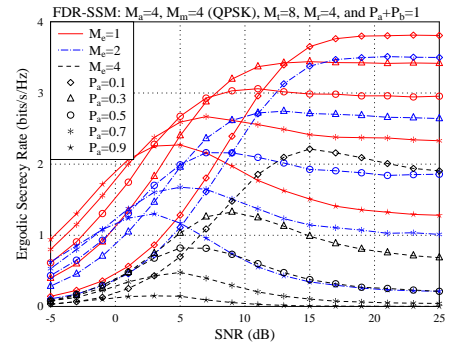

Fig. 1. Secrecy performance of the FDR-SSM systems with various system parameters and power-allocations between P_a and P_b.
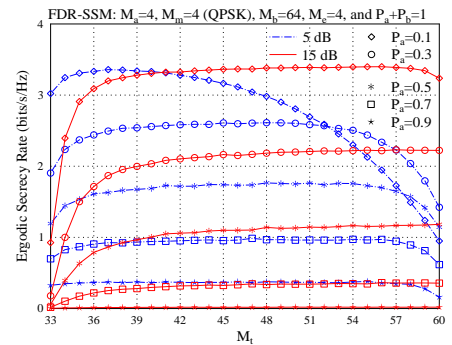

Fig. 2. Secrecy performance of the FDR-SSM systems with different pairs of (M_t, M_r) and power-allocations between P_a and P_b.

Given $M_b = 64$, Fig. 2 depicts the ESR of the FDR-SSM systems with different values of M_t and hence, different values of $M_r = 64 - M_t$. Furthermore, the effect of P_a and P_b is also considered. From the results we are implied that, at a given SNR and a given power configuration of (P_a, P_b), there exist an optimum (M_t, M_r) pair resulting in the highest
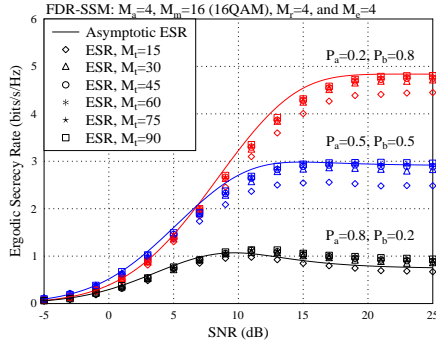
Fig. 3. Comparison between the simulated ESR and the asymptotic ESR.

secrecy rate. However, the secrecy performance is in general robust to the (M_t, M_r) values, explained by the fact that the secrecy rate is nearly flat over a big range values of (M_t, M_r). As seen in Fig. 2, the highest secrecy rate can be achieved, when Bob uses most of its power (P_b) to jam Eve's reception and, simultaneously, uses a sufficient number of receive antennas (M_r) to reliably detect the information sent by Alice. Furthermore, we can be inferred that, for a given pair of (M_t, M_r), there exists an optimum power configuration of (P_a, P_b), which yields the highest secrecy rate.

Fig. 3 shows the asymptotic ESR evaluated by (19), and the secrecy rate obtained via simulation. Explicitly, simulated ESR converges fast to the asymptotic ESR, as M_t increases, which become close provided that $M_t \geq 30$. As shown in Fig. 3, when $M_t = 90$, the difference between the asymptotic ESR and the simulated ESR is almost negligible for all the cases considered and also in both low and high SNR regions. From these results, we can be convinced that when M_t is sufficiently large, e.g., $M_t \geq 30$, the asymptotic ESR of (19) can be used to predict the achievable ESR of FDR-SSM systems.

V. CONCLUSION

A novel FDR-SSM system has been proposed and analyzed. The impacts of the number of antennas employed by Eve, Alice's transmission power and of Bob's transmission power on the secrecy performance have been investigated. Furthermore, the asymptotic ESR expression derived in Section III-B has been validated by simulations. Our studies show that the proposed FDR-SSM scheme employs all the advantages of SM, while providing significant secrecy enhancement by exploiting the full-duplexing capability of the legal receiver.

APPENDIX

A. Proof of Theorem 1

Since $\mathbb{E}_{\boldsymbol{H}, \boldsymbol{z}_b}[x] = \mathbb{E}_{\boldsymbol{H}}[\mathbb{E}_{\boldsymbol{z}_b}[x]]$, (7) can be simplified to

$$R_b = \log_2(M_a M_m) - M_r / \ln 2 - 1/(M_a M_m)$$

$$\times \sum_{j,k} \mathbb{E}_{\boldsymbol{H}}\left[\mathbb{E}_{\boldsymbol{z}_b}\left[\log_2 \sum_{\hat{j},\hat{k}} \exp\left(-\left\|\sqrt{P_a}\boldsymbol{H}\boldsymbol{d}_{\hat{j}\hat{k}}^{jk} + \boldsymbol{z}_b\right\|^2 / \sigma_b^2\right)\right]\right]$$

$$\overset{(a)}{\geq} \log_2(M_a M_m) - M_r / \ln 2 - 1/(M_a M_m)$$

$$\times \sum_{j,k} \log_2 \sum_{\hat{j},\hat{k}} \mathbb{E}_{\boldsymbol{H}}\left[\mathbb{E}_{\boldsymbol{z}_b}\left[\exp\left(-\left\|\sqrt{P_a}\boldsymbol{H}\boldsymbol{d}_{\hat{j}\hat{k}}^{jk} + \boldsymbol{z}_b\right\|^2 / \sigma_b^2\right)\right]\right]$$

$$\overset{(b)}{=} \log_2(M_a M_m) + M_r - M_r / \ln 2$$

$$- \frac{1}{M_a M_m} \sum_{j,k} \log_2 \sum_{\hat{j},\hat{k}} \left(1 + \frac{P_a}{2\sigma_b^2}\left\|\boldsymbol{d}_{\hat{j}\hat{k}}^{jk}\right\|^2\right)^{-M_r}, \quad (20)$$

where the relation (a) is obtained by applying the Jensen's inequality to the function of $\log_2(x)$, while the last equation is obtained with the aid of the formulae of (57) and (63) in [15]. Finally, by expressing $D_{\hat{j}\hat{k}}^{jk} = \|\boldsymbol{d}_{\hat{j}\hat{k}}^{jk}\|^2$ in (20), we can obtain the lower-bound of (12).

B. Proof of Proposition 1

Let $\gamma_b = 1/\sigma_b^2$ be the average receive SNR at Bob. Then, the limit of R_b can be readily obtained from (7), which is

$$\lim_{\gamma_b \to 0} R_b = 0, \text{ and } \lim_{\gamma_b \to +\infty} R_b = \log_2(M_a M_m). \quad (21)$$

Similarly, from (20), we can derive the limits of R_b^{LB} as

$$\lim_{\gamma_b \to 0} R_b^{\text{LB}} = M_r - M_r / \ln 2,$$

$$\lim_{\gamma_b \to +\infty} R_b^{\text{LB}} = \log_2(M_a M_m) + M_r - M_r / \ln 2. \quad (22)$$

By comparing the results in (21) and (22), we can know that R_b and R_b^{LB} have the same difference between the high and low SNR regions, which is $\log_2(M_a M_m)$. Moreover, both R_b and R_b^{LB} are monotonically increasing functions of γ_b. These results imply that for any given γ_b, the difference between R_b and R_b^{LB} is approximately $M_r (1/\ln 2 - 1)$, which is a constant. Therefore, we can be confident that the result in (13) represents an accurate approximation of R_b. Note that, this observation has already been reported for general MIMO channels in [15].

REFERENCES

[1] M. D. Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: Challenges, opportunities, and implementation," *Proc. IEEE*, vol. 102, no. 1, pp. 56–103, Jan. 2014.

[2] S. Sinanovic, and et.al, "Secrecy capacity of space keying with two antennas," in *Proc. of IEEE VTC (Fall)*, Sep. 2012, pp. 1–5.

[3] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *Proc. of IEEE WCSP*, Oct. 2012, pp. 1–4.

[4] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1351–1354, Aug. 2015.

[5] S. R. Aghdam and T. M. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 180–183, Apr. 2016.

[6] L.-L. Yang, "Transmitter preprocessing aided spatial modulation for multiple-input multiple-output systems," in *Proc. of IEEE 73rd VTC (Spring)*, May 2011, pp. 1–5.

[7] A. Stavridis, M. D. Renzo, and H. Haas, "Performance analysis of multistream receive spatial modulation in the MIMO broadcast channel," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 1808–1820, Mar. 2016.

[8] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[9] F. Wu, L.-L. Yang, and et.al, "Secret precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544–1547, Sep. 2015.

[10] G. Zheng, and et.al, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[11] M. Chung, and et.al, "Prototyping real-time full duplex radios," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 56–63, Sep. 2015.

[12] M. Chung, M. S. Sim, D. Kim, and C. B. Chae, "Compact full duplex MIMO radios in D2D underlaid cellular networks: From system design to prototype results," *IEEE Access*, vol. PP, no. 99, pp. 1–1, Apr. 2017.

[13] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[14] R. Zhang, L.-L. Yang, and L. Hanzo, "Error probability and capacity analysis of generalised pre-coding aided spatial modulation," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 364–375, Jan. 2015.

[15] W. Zeng, C. Xiao, M. Wang, and J. Lu, "Linear precoding for finite-alphabet inputs over MIMO fading channels with statistical CSI," *IEEE Trans. Signal Process.*, vol. 60, no. 6, pp. 3134–3148, Jun. 2012.