IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 4, 2016, accepted October 3, 2016, date of publication March 21, 2017, date of current version April 24, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2684901

A Lower Bound on Secrecy Capacity for MIMO Wiretap Channel Aided by a Cooperative Jammer With Channel Estimation Error

SHUNYA IWATA[1], (Student Member, IEEE), TOMOAKI OHTSUKI[1], (Senior Member, IEEE), AND POOI-YUEN KAM[2], (Fellow, IEEE)

[1]Graduate School of Science and Technology, Keio University, Yokohama 223-8522, Japan
[2]Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117576

Corresponding author: S. Iwata (iwata@ohtsuki.ics.keio.ac.jp)

ABSTRACT We consider a multiple-input multiple-output wiretap channel with one transmitter, one receiver, one cooperative jammer, and one eavesdropper whereby each node is equipped with multiple antennas. Eigenbeam-space division multiplexing (E-SDM) and cooperative jamming are known as techniques for improving secrecy rate. E-SDM enables the transmitter and the legitimate receiver to communicate with each other in parallel using channel state information known to them to maximize the legitimate receiver's mutual information. On the other hand, cooperative jamming is to jam only the eavesdropper to degrade the eavesdropper's mutual information. However, co-channel interference and residual interference from the cooperative jammer are caused by channel estimation errors, which degrade the legitimate receiver's mutual information. How these interferences affect the secrecy capacity has not been clarified. In this paper, we derive a lower bound on secrecy capacity using the legitimate receiver's mutual information in the presence of channel estimation errors and the mutual information of the eavesdropper who uses a minimum mean square error receiver. We analyze the effect of co-channel interference and residual interference from the cooperative jammer on the secrecy rate.

INDEX TERMS MIMO wiretap channel, channel estimation error, physical layer security, cooperative jamming, secrecy rate.

I. INTRODUCTION

The broadcast nature of wireless channels allows unauthorized users to overhear the transmitted signal. Traditionally, security in wireless communication has been realized by employing a cryptographic method implemented at upper layer, which is based on computational complexity to decode. However, this method in general requires intended user to share secret keys, which is difficult to realize in terms of key distribution and management. The security also depends on eavesdropper's ability to decode. Therefore, a rapid advance in computing power and resources make it feasible for eavesdropper to decode the encrypted wireless signal. Recently, instead of the method based on computational complexity in [1], physical layer security based on information security has been developed [2]. It enhances security by exploiting the physical characteristics of wireless channel, e.g., fading, noise, and diversity. It has much attention in the field of upcoming the fifth generation (5G) network. In particular, the internet of things (IoT) which is a key component of 5G is expected to enable any devices to interact with each other in sensor network. However, irrespective of being exposed to eavesdropper, it is more challenging to implement a cryptographic method in IoT systems, because IoT has the complexity and energy constraints. Physical layer security is expected to be a promising secure method to be replaced with cryptographic method in IoT systems [3]–[5].

Wyner, who is a pioneer in information theoretic security, introduced the wiretap channel in which a transmitter (say Alice) transmits the intended signal to intended user (say Bob) while unauthorized user (say Eve) eavesdrops it [6] assuming that the Eve's channel is worse than Bob's one. In this model, secrecy capacity was given as the performance metric of security, which is the maximal achievable rate by Eve without any information. In [7], this model is extended to the general non-degraded broadcast channel with confidential messages (BCC), where Alice has a common message

to Bob and Eve but a confidential message to only Bob. Then, Leung-Yan-Cheong and Hellman [8] generalized this work and determined secrecy capacity for wiretap channel with additive white Gaussian noise (AWGN). Furthermore, the secrecy capacity with various antenna configurations and various channel conditions were studied [9]–[12]. Ergodic secrecy rate of fading channels was derived in [9]. The secrecy capacity of single-input multiple-output (SIMO) [10], multiple-input single-output (MISO) [11], and MIMO wiretap channel was derived in [12].

To enhance the security in wireless communication, various techniques were known, one of which is cooperative jamming that degrades Eve's mutual information using a cooperative node who transmits jamming signal nulled only at Bob side in [13]. Multiple cooperative jamming node have been considered in [14]. The authors of [15] and [16] addressed the secrecy rate optimization and provided robust beamforming technique, considering the cooperative jamming nodes. In addition, an artificial noise (AN) is known as the similar technique which uses a null-space jamming signal with the intended signal [17] simultaneously. Moreover, the relay-eavesdropper channels with cooperative jamming scheme have been studied [18]. In MIMO system, Alice may transmit multiple-streams to Bob, which forces Alice and Bob to have to remove inter-stream interference to realize the achievable channel capacity. Eigenbeam-space division multiplexing (E-SDM) is known as a technique that enables to transmit information signal without interference between streams in [19] using both CSI. In physical layer security, this technique was used to realize Bob's achievable capacity by choosing Alice's transmit covariance matrix based on water-filling solution without considering Eve's channel [20]. The co-channel interference such as mixing unintended signals sent in K-user interference channel acts as effective noise, which is exploited to prevent the unintended users from eavesdropping the signals for the other intended users. The work exploiting the technique that aligns the multiple interference into a subspace at every receiver by coordination between transmitters are known to enhance secrecy [21]–[23]. Another different approach is to exploit artificial fading that increases channel uncertainty, which helps improve secure communications [24].

The assumption that channel state information (CSI) is perfect or imperfect, at which terminal it is available, and the available CSI from which terminal to which terminal is very important for deciding the system model. In [13], the lower and upper bounds of the secrecy capacity were derived in wiretap channel aided by a cooperative jammer, which consists of Alice and Bob with single antenna, Eve and jammer with multiple antennas under the assumption that all nodes can use perfect CSI of its channel. Also, secrecy capacity with channel estimation error has been analyzed in various models. In [25], the authors derived the upper bound on secrecy capacity in single-input single-output (SISO) wiretap channel, which consists of Alice, Bob, and Eve, with imperfect channel estimation between Alice-Bob channel. In [26], the authors were devoted to analyzing the secrecy capacity in presence of channel estimation errors on AN using maximum ratio transmission (MRT) and maximum ratio combining (MRC) with Alice, Bob, and Eve. This work only clarified the effect of main channel estimation error on secrecy capacity in the conventional three node model. In [27], secrecy rate optimization in MIMO wiretap channel with Alice, Bob, a cooperative jammer, and an eavesdropper was investigated assuming that Alice and the jammer know the channels to Bob and Eve and share them with each other, while Eve knows the channels to Alice and the jammer, which showed the optimized secrecy rate when the channel estimation error is considered only in the Alice-Eve channel and the jammer-Eve channel. However, to the best of our knowledge, the secrecy rate of MIMO wiretap channel aided by a cooperative jammer has not been clarified when both Alice-Bob channel and the jammer-Bob channel are imperfect.

In this paper, we first derive a lower bound on ergodic secrecy capacity of MIMO wiretap channel aided by a cooperative jammer in the presence of the channel estimation errors in Alice-Bob channel and the jammer-Bob channel by lower-bounding Bob's mutual information, assuming that Eve uses a linear minimum mean-squared error (MMSE) receiver. We then evaluate the effects of co-channel interference and residual interference from the cooperative jammer on ergodic secrecy rate through numerical results. Please note that we do not optimize the power allocation so as to maximize secrecy rate but analyze the secrecy rate when the power allocation schemes described in Section II are given.

The remainders of this paper are organized as follows. In Section II, the system model is introduced. In Section III, lower bound on ergodic secrecy capacity under channel estimation error in MIMO wiretap channel is derived. The numerical results and simulation are included in Section IV. Finally, conclusions are presented in Section V.

Notation: We use the upper case boldface letters for matrices and lower case boldface letters for vectors. $|(\cdot)|$ denotes the determinant of a matrix. $\mathrm{Tr}(\cdot)$ denotes the trace of a matrix. $()^H$ denotes conjugate transpose. $(\cdot)^{-1}$ denotes the inverse of a matrix. $\mathbb{E}[\cdot]$ denotes the statistical expectation of random variables. $\mathbf{I}_d$ denotes $d \times d$ the identity matrix. $I(\mathbf{X}; \mathbf{Y})$ and $\mathrm{Cov}(\mathbf{X}, \mathbf{Y})$ denote the mutual information and the covariance of two random variables $\mathbf{X}$ and $\mathbf{Y}$, respectively. $\mathbf{X}(:, i{:}j)$ denotes the columns from i to j of $\mathbf{X}$. We also define the conditional mutual information $I(\mathbf{X}; \mathbf{Y}|\mathbf{Z})$ as $\mathbb{E}_{\mathbf{Z}}[I(\mathbf{X}; \mathbf{Y})|\mathbf{Z}]$, following the notation in [28].

II. SYSTEM MODEL AND TRANSMISSION SCHEME

A. SYSTEM MODEL

We consider a MIMO wiretap channel consisting of a transmitter (Alice), an intended user (Bob), a cooperative jammer, and a passive eavesdropper (Eve), with N_A, N_B, N_J, and N_E antennas, respectively. The system model is shown in Fig. 1. Let $\mathbf{H}_{BA}$, $\mathbf{H}_{EA}$, $\mathbf{H}_{BJ}$, and $\mathbf{H}_{EJ}$ denote $N_B \times N_A$, $N_E \times N_A$, $N_B \times N_J$, $N_E \times N_J$ channel matrices between

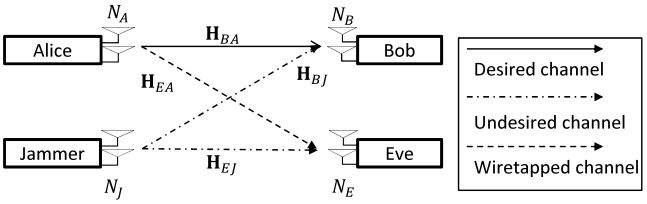

FIGURE 1. A system model in this paper.

Alice and Bob, between Alice and Eve, between the jammer and Bob, and between the jammer and Eve, respectively. Also, we assume that the elements of all channel matrices are independently distributed zero-mean circularly symmetric complex Gaussian (ZMCSCG) with unit variance. Alice transmits the intended signal to Bob while the jammer transmits the jamming signal nulled at Bob but harmful to Eve. Alice and Bob estimate $\mathbf{H}_{BA}$, and jammer and Bob estimate $\mathbf{H}_{BJ}$ imperfectly, respectively. On the contrary, we assume that Eve knows $\tilde{\mathbf{H}}_{EA}, \tilde{\mathbf{H}}_{EJ}$, which are defined as the weighted channel in III-B. The assumption of the system model is summarized as follows.

1) Alice has the imperfect knowledge of the channel $\mathbf{H}_{BA}$ denoted by $\widehat{\mathbf{H}}_{BA}$ and transmits the intended signal precoded by the right singular value $\widehat{\mathbf{V}}$ of $\widehat{\mathbf{H}}_{BA}$.
2) Bob has the imperfect knowledge of the channel $\mathbf{H}_{BA}$, $\mathbf{H}_{BJ}$ denoted by $\widehat{\mathbf{H}}_{BJ}$ and processes the received signal by multiplying with the left singular value $\widehat{\mathbf{U}}$ of $\widehat{\mathbf{H}}_{BA}$.
3) Jammer has the imperfect knowledge of the channel $\mathbf{H}_{BJ}$ and transmits the jamming signal so that it is nulled at Bob.
4) Eve has the perfect knowledge of the weighted channel $\tilde{\mathbf{H}}_{EA}, \tilde{\mathbf{H}}_{EJ}$ given in Subsection III-B and intercepts the intended signal using MMSE filter.

We also assume that the number of intended information and jamming signal streams are d_1, d_2, respectively, where $d_1 = \min(N_A, N_B)$. Note that N_J must be more than $N_B + d_2$ so that the jamming signal is nulled at Bob. Thus, we assume that $N_J \geq N_B + d_2$. Further, we assume $N_E \leq d_2$ so that Eve can not remove the jamming signals by utilizing the remaining available dimensions of her antennas. Also, let P_A and P_J denote Alice's total transmit power and the jammer's total transmit power, respectively.

B. TRANSMISSION SCHEME

Alice transmits the intended signal $\mathbf{x}$ expressed as,

$$\mathbf{x} = \widehat{\mathbf{V}}\mathbf{\Lambda}\mathbf{s} \tag{1}$$

where $\mathbf{s}$ is the $d_1 \times 1$ information signal vector consisting of Gaussian inputs whose elements are i.i.d. ZMCSCG random variables with unit variance, $\mathbf{\Lambda}$ is the $d_1 \times d_1$ diagonal matrix that decides how much transmit power is allocated to each signal, $\widehat{\mathbf{V}}$ is the $N_A \times d_1$ weighting matrix. In our model, $\mathbf{\Lambda}$ is determined by the water-filling solution based on the estimated channel. In addition, $\mathbf{H}_{BA}$ is, in the presence of channel estimation error $\mathbf{E}_{BA}$, using the estimated channel $\widehat{\mathbf{H}}_{BA}$, expressed as,

$$\mathbf{H}_{BA} = \widehat{\mathbf{H}}_{BA} + \mathbf{E}_{BA} \tag{2}$$

where the elements of $\widehat{\mathbf{H}}_{BA}$ are i.i.d. ZMCSCG random variables with variance $1 - \sigma_A^2$. Also, the elements of $\mathbf{E}_{BA}$ are i.i.d. ZMCSCG random variables with variance σ_A^2 [29], [30]. We obtain the weighting matrix $\widehat{\mathbf{V}}$ by using the singular value decomposition (SVD) of $\widehat{\mathbf{H}}_{BA}$ expressed as,

$$\widehat{\mathbf{H}}_{BA} = \widehat{\mathbf{U}}\widehat{\mathbf{\Sigma}}\widehat{\mathbf{V}}^H \tag{3}$$

where $\widehat{\mathbf{U}}$, $\widehat{\mathbf{V}}$ are respectively $N_B \times d_1$ and $N_A \times d_1$ unitary matrices, and $\widehat{\mathbf{\Sigma}} = \mathrm{diag}\{\sqrt{\lambda_1}, \sqrt{\lambda_2}, \cdots, \sqrt{\lambda_{d_1}}\}$ with singular values in the decreasing order of size. The jammer transmits the jamming signal $\mathbf{z}_J$, which is expressed as,

$$\mathbf{z}_J = \widehat{\mathbf{W}}_J \mathbf{\Lambda}_J \boldsymbol{v}_J \tag{4}$$

where $\boldsymbol{v}_J$ is the $d_2 \times 1$ artificial noise vector whose elements are i.i.d. ZMCSCG random variables with unit variance, $\mathbf{\Lambda}_J$ is the $d_2 \times d_2$ diagonal matrix that decides how much transmit power is allocated to each jamming signal, $\widehat{\mathbf{W}}_J$ is the $N_J \times d_2$ weighting matrix. In our model, we adopt equal power allocation for $\mathbf{\Lambda}_J$. $\mathbf{H}_{BJ}$ is, in the presence of channel estimation error $\mathbf{E}_{BJ}$, using the estimated channel $\widehat{\mathbf{H}}_{BJ}$, expressed as,

$$\mathbf{H}_{BJ} = \widehat{\mathbf{H}}_{BJ} + \mathbf{E}_{BJ} \tag{5}$$

where the elements of $\widehat{\mathbf{H}}_{BJ}$ are i.i.d. ZMCSCG random variables with variance $1 - \sigma_J^2$, and the elements of $\mathbf{E}_{BJ}$ are i.i.d. ZMCSCG random variables with variance σ_J^2. The jammer designs the weighting matrix $\widehat{\mathbf{W}}_J$ so that the jamming signal lies in the null space of $\widehat{\mathbf{H}}_{BJ}$.

$$\widehat{\mathbf{W}}_J = \mathrm{null}(\widehat{\mathbf{H}}_{BJ}) \tag{6}$$

where $\mathrm{null}(\cdot)$ denotes a null space of vector or matrix. To realize (6), $\widehat{\mathbf{H}}_{BJ}$ is decomposed, then we substitute the null space of $\widehat{\mathbf{H}}_{BJ}$ into $\widehat{\mathbf{W}}_J$ as follows.

$$\widehat{\mathbf{H}}_{BJ} = \widehat{\mathbf{U}}^{(J)}[\widehat{\mathbf{\Sigma}}^{(J)}\ \mathbf{0}_{N_B \times (N_J - N_B)}][\widehat{\mathbf{V}}_1^{(J)}\ \widehat{\mathbf{V}}_0^{(J)}]^H, \tag{7}$$

$$\widehat{\mathbf{W}}_J = \widehat{\mathbf{V}}_0^{(J)}(:, 1 : d_2). \tag{8}$$

Also, we assume that Alice's and Jammer's total average transmit powers are constrained by P_A and P_J, respectively, as follows.

$$\mathrm{Tr}(\mathbf{Q}_A) \leq P_A \tag{9}$$

$$\mathrm{Tr}(\mathbf{Q}_J) \leq P_J \tag{10}$$

where $\mathbf{Q}_A = \mathbb{E}[\mathbf{\Lambda}\mathbf{s}\mathbf{s}^H\mathbf{\Lambda}^H]$, $\mathbf{Q}_J = \mathbb{E}[\mathbf{\Lambda}_J \boldsymbol{v}_J \boldsymbol{v}_J^H \mathbf{\Lambda}_J^H]$. As mentioned previously, we adopt water-filling solution scheme for $\mathbf{Q}_A$ and equal power allocation scheme for $\mathbf{Q}_J$, respectively. Therefore, the ith diagonal element of $\mathbf{Q}_A$ [28] and $\mathbf{Q}_J$ are given by,

$$\mathbf{Q}_{A,ii} = \left(\mu - \frac{1}{\lambda_i}\right)^+, \quad i = 1, \cdots, d_1 \tag{11}$$

$$\mathbf{Q}_J = \frac{P_J}{d_2}\mathbf{I}_{d_2} \tag{12}$$

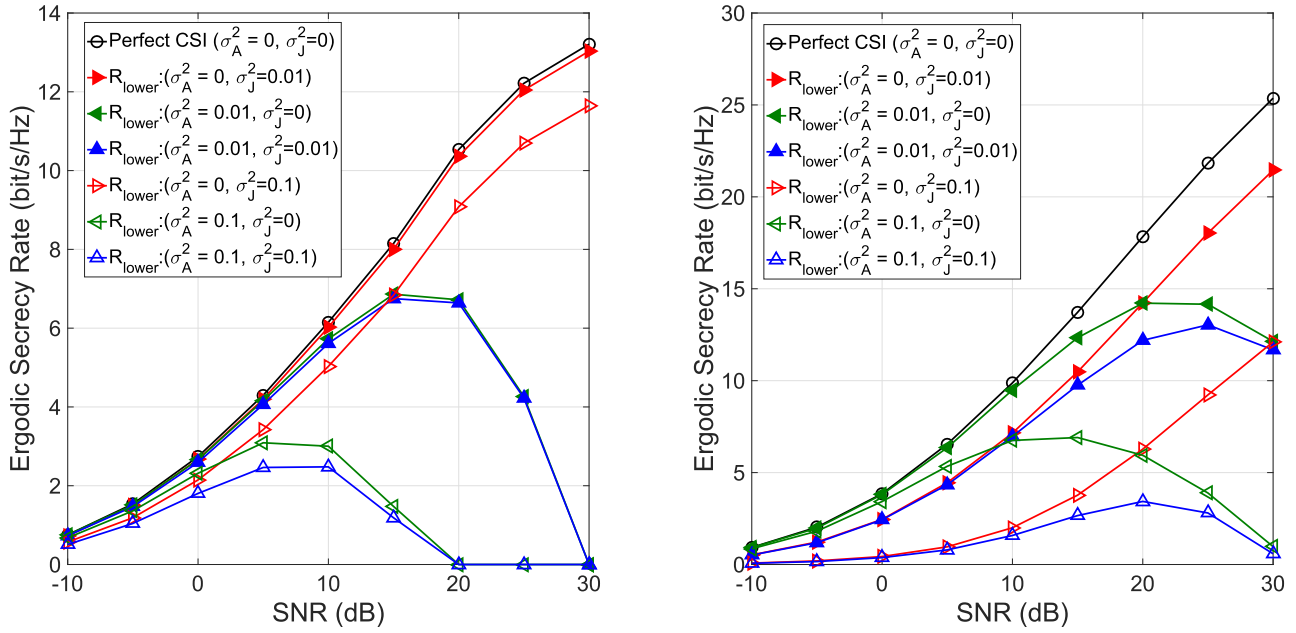

FIGURE 2. $R_{\mathbf{lower}}$ versus SNR for a fixed $N_E = 4$. (a) $P_J = 5$ dB. (b) $P_J = 20$ dB.

where μ is chosen to satisfy $\sum_{i=1}^{d_1} \mathbf{Q}_{A,ii} = P_A$. The signal vector received by Bob $\mathbf{y}'_B$ is given by

$$\begin{aligned}\mathbf{y}'_B &= \mathbf{H}_{BA}\mathbf{x} + \mathbf{H}_{BJ}\mathbf{z}_J + \mathbf{n}_B \\ &= (\widehat{\mathbf{H}}_{BA} + \mathbf{E}_{BA})\widehat{\mathbf{V}}\mathbf{\Lambda}\mathbf{s} + \mathbf{E}_{BJ}\widehat{\mathbf{W}}_J\mathbf{\Lambda}_J\boldsymbol{\nu}_J + \mathbf{n}_B \end{aligned} \quad (13)$$

where $\mathbf{n}_B$ is the $N_B \times 1$ noise vector at Bob whose elements are i.i.d. ZMCSCG random variables with variance σ^2_{Bob}. Multiplied by $\widehat{\mathbf{U}}$, (13) can be re-expressed as,

$$\begin{aligned}\widehat{\mathbf{U}}^H\mathbf{y}'_B = (\widehat{\mathbf{\Sigma}} + \widehat{\mathbf{U}}^H\mathbf{E}_{BA}\widehat{\mathbf{V}})\mathbf{\Lambda}\mathbf{s} + \widehat{\mathbf{U}}^H\mathbf{E}_{BJ}\widehat{\mathbf{W}}_J\mathbf{\Lambda}_J\boldsymbol{\nu}_J \\ + \widehat{\mathbf{U}}^H\mathbf{n}_B. \end{aligned} \quad (14)$$

Defining $\tilde{\mathbf{E}}_{BA} = \widehat{\mathbf{U}}^H\mathbf{E}_{BA}\widehat{\mathbf{V}}$, $\tilde{\mathbf{E}}_{BJ} = \widehat{\mathbf{U}}^H\mathbf{E}_{BJ}\widehat{\mathbf{W}}_J$, and $\mathbf{n}'_B = \widehat{\mathbf{U}}^H\mathbf{n}_B$, (14) is re-expressed as,

$$\begin{aligned}\mathbf{y}_B &= \widehat{\mathbf{U}}^H\mathbf{y}'_B \\ &= (\widehat{\mathbf{\Sigma}} + \tilde{\mathbf{E}}_{BA})\mathbf{\Lambda}\mathbf{s} + \tilde{\mathbf{E}}_{BJ}\mathbf{\Lambda}_J\boldsymbol{\nu}_J + \widehat{\mathbf{U}}^H\mathbf{n}_B \\ &= (\widehat{\mathbf{\Sigma}} + \underbrace{\tilde{\mathbf{E}}_{BA}}_{\text{co-channel}})\mathbf{\Lambda}\mathbf{s} + \underbrace{\tilde{\mathbf{E}}_{BJ}\mathbf{\Lambda}_J\boldsymbol{\nu}_J}_{\text{residual}} + \mathbf{n}'_B \end{aligned} \quad (15)$$

where the elements of $\tilde{\mathbf{E}}_{BA}$, $\tilde{\mathbf{E}}_{BJ}$, $\mathbf{n}'_B$ are also i.i.d. ZMCSCG random variables with variance 1, 1, and σ^2_{Bob}, respectively, due to the fact that to be multiplied by unitary matrix does not change its distribution [24]. On the other hand, the signal vector received by Eve $\mathbf{y}_E$ is given by,

$$\begin{aligned}\mathbf{y}_E &= \mathbf{H}_{EA}\mathbf{x} + \mathbf{H}_{EJ}\mathbf{z}_J + \mathbf{n}_E \\ &= \mathbf{H}_{EA}\widehat{\mathbf{V}}\mathbf{\Lambda}\mathbf{s} + \mathbf{H}_{EJ}\widehat{\mathbf{W}}_J\mathbf{\Lambda}_J\boldsymbol{\nu}_J + \mathbf{n}_E \\ &= \tilde{\mathbf{H}}_{EA}\mathbf{\Lambda}\mathbf{s} + \tilde{\mathbf{H}}_{EJ}\mathbf{\Lambda}_J\boldsymbol{\nu}_J + \mathbf{n}_E \end{aligned}$$

where $\mathbf{n}_E$ is $N_E \times 1$ noise vector at Eve whose elements are i.i.d. ZMCSCG random variables with variance σ^2_{Eve}. Also, we define $\tilde{\mathbf{H}}_{EA} = \mathbf{H}_{EA}\widehat{\mathbf{V}}$ and $\tilde{\mathbf{H}}_{EJ} = \mathbf{H}_{EJ}\widehat{\mathbf{W}}_J$.

III. ERGODIC SECRECY RATE WITH IMPERFECT CSI AND MUTUAL INFORMATION AT BOB AND EVE

In this section, we formulate the lower bound on ergodic secrecy capacity in MIMO wiretap channel, and then derive Bob's and Eve's mutual information in the next subsection. First of all, MIMO secrecy capacity C_S has been analyzed in [12] and [31], which is defined as the maximum of the difference of mutual information between Bob and Eve:

$$C_S = \max_{\{\mathbf{Q}_A, \mathbf{Q}_J\} \succeq 0} I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B) - I_{\text{Eve}}(\mathbf{x}; \mathbf{y}_E) \quad (16)$$

where $I_{Bob}(\mathbf{x}; \mathbf{y}_B)$ denotes the mutual information between Alice and Bob, $I_{Eve}(\mathbf{x}; \mathbf{y}_E)$ denotes the mutual information between Alice and Eve, and the maximum is taken over all the possible input covariance matrices. In general, since we must average (16) by the distribution or channel realization in considering available CSI, we need consider ergodic secrecy capacity instead of (16). The ergodic secrecy capacity given CSI is expressed as in [32],

$$\mathbb{E}[C_S] = \max_{\{\mathbf{Q}_A, \mathbf{Q}_J\} \succeq 0} \mathbb{E}_{\mathbf{H}}\Big[[I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B) - I_{\text{Eve}}(\mathbf{x}; \mathbf{y}_E)]^+\Big] \quad (17)$$

where $\mathbf{H} \triangleq \{\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}, \tilde{\mathbf{H}}_{EA}, \tilde{\mathbf{H}}_{EJ}\}$ and $[\cdot]^+$ denotes $\max(\cdot, 0)$. This expression is intractable to analyze. Therefore, in order to make it tractable to analyze, we resort to a lower bound on secrecy capacity expressed as

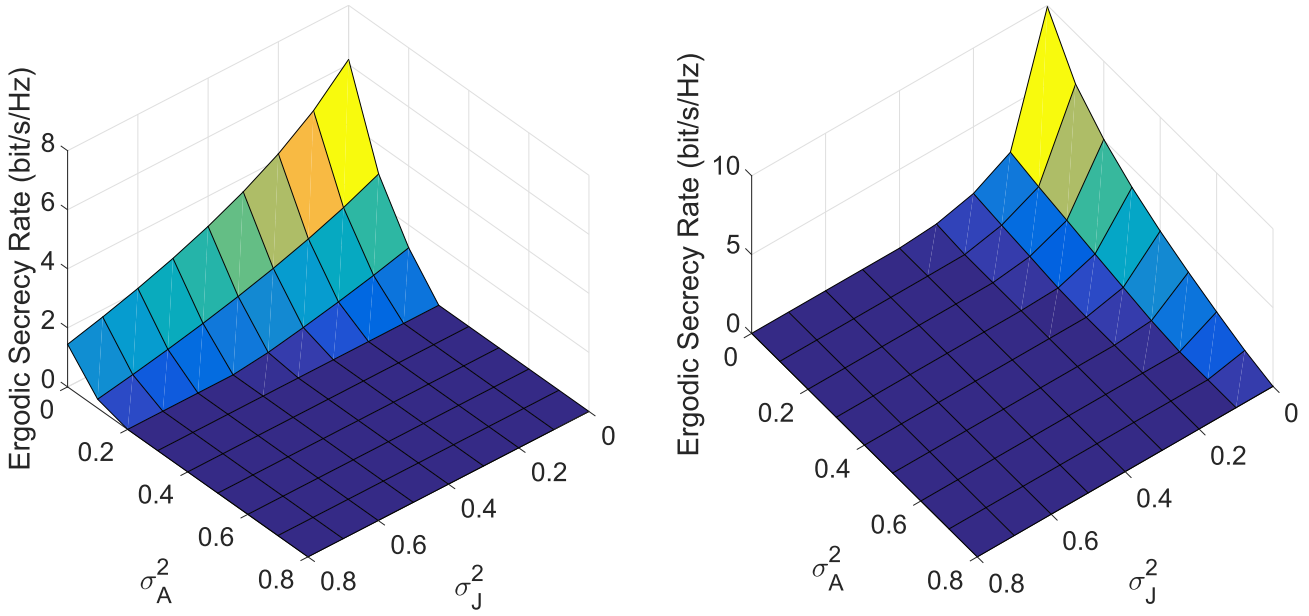

FIGURE 3. R_{lower} versus σ_A^2 and σ_J^2 (SNR= 10 dB, $N_E = 4$). $P_J = 5$ dB. (b) $P_J = 20$ dB.

in [20], [32], [33],

$$\mathbb{E}[C_S] = \max_{\{\mathbf{Q}_A, \mathbf{Q}_J\} \succeq 0} \mathbb{E}_{\mathbf{H}}\Big[[I_{Bob}(\mathbf{x}; \mathbf{y}_B) - I_{Eve}(\mathbf{x}; \mathbf{y}_E)]^+\Big] \quad (18)$$

$$\geq \Big[\mathbb{E}_{\mathbf{H}}[I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B) - I_{\text{Eve}}(\mathbf{x}; \mathbf{y}_E)]\Big]^+ \quad (19)$$

$$= \Big[I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) - I_{\text{Eve}}(\mathbf{x}; \mathbf{y}_E|\tilde{\mathbf{H}}_{EA}, \tilde{\mathbf{H}}_{EJ})\Big]^+. \quad (20)$$

This expression used in (19) is also called Secrecy Rate [32]. Furthermore, using a lower bound on $I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})$ presented in the next subsection, the lower bound on the ergodic secrecy capacity R_{lower} can be:

$$R_{\text{lower}} \triangleq \Big[I_{\text{Bob,lower}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) - I_{\text{Eve}}(\mathbf{x}; \mathbf{y}_E|\mathbf{H}_{EA})\Big]^+ \quad (21)$$

where $I_{\text{Bob,lower}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})$ denotes a lower bound on $I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})$.

A. LOWER BOUND ON BOB'S MUTUAL INFORMATION

In this subsection, we provide a lower bound on Bob's mutual information. Taking the similar steps as in [34]–[36] and performing some mathematical calculations, then we obtain

$$I_{\text{Bob,lower}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) = \mathbb{E}_{\widehat{\mathbf{H}}_{BA}}\Big[\log_2\Big|\mathbf{I}_{d_1} + \frac{1}{\sigma_A^2 P_A + \sigma_J^2 P_J + \sigma_{Bob}^2}\widehat{\mathbf{\Sigma}}^H\widehat{\mathbf{\Sigma}}\mathbf{Q}_A\Big|\Big]. \quad (22)$$

The derivation of (22) is given in Appendix.

B. EVE'S MUTUAL INFORMATION

Eve decouples the received signal by MMSE filter. The corresponding signal to noise plus interference ratio (SINR) γ_i of the output stream i is expressed as in [37],

$$\gamma_i = \mathbf{h}_i^H\Big(\tilde{\mathbf{H}}_{EA}\mathbf{Q}_A\tilde{\mathbf{H}}_{EA}^H - \mathbf{h}_i\mathbf{h}_i^H + \tilde{\mathbf{H}}_{EJ}\mathbf{Q}_J\tilde{\mathbf{H}}_{EJ}^H + \sigma_{Eve}^2\mathbf{I}_{N_E}\Big)^{-1}\mathbf{h}_i \quad (23)$$

where $\mathbf{h}_i$ is the ith column of $\tilde{\mathbf{H}}_{EA}\mathbf{\Lambda}$. Thus, $I_{\text{Eve}}(\mathbf{x}; \mathbf{y}_E|\tilde{\mathbf{H}}_{EA}, \tilde{\mathbf{H}}_{EJ})$ is expressed as in [38], [39].

$$I_{\text{Eve}}(\mathbf{x}; \mathbf{y}_E|\tilde{\mathbf{H}}_{EA}, \tilde{\mathbf{H}}_{EJ}) = \mathbb{E}_{\tilde{\mathbf{H}}_{BA}, \tilde{\mathbf{H}}_{EJ}}\Big[\sum_{i=1}^{d_1}\log_2(1+\gamma_i)\Big]. \quad (24)$$

IV. NUMERICAL AND SIMULATION RESULTS

In this section, numerical results and Monte Carlo simulations are presented to see that how those channel estimation errors affect on secrecy rate in terms of low or high power jamming, magnitude of the channel estimation error, and signal to noise ratio (SNR). Monte Carlo simulations are carried out by generating 1000 realizations of channel, and table 1 lists simulation parameters used through all the figures. All the channels are assumed to be flat Rayleigh fading and distance attenuation is not considered. We define SNR as the ratio of total transmit power to Bob's noise power, that is, $\text{SNR} = \dfrac{P_A}{\sigma_{Bob}^2}$.

Fig. 2(a) and 2(b) show ergodic secrecy rate as the function of SNR in the case where the values of σ_A^2 and σ_J^2 are changed

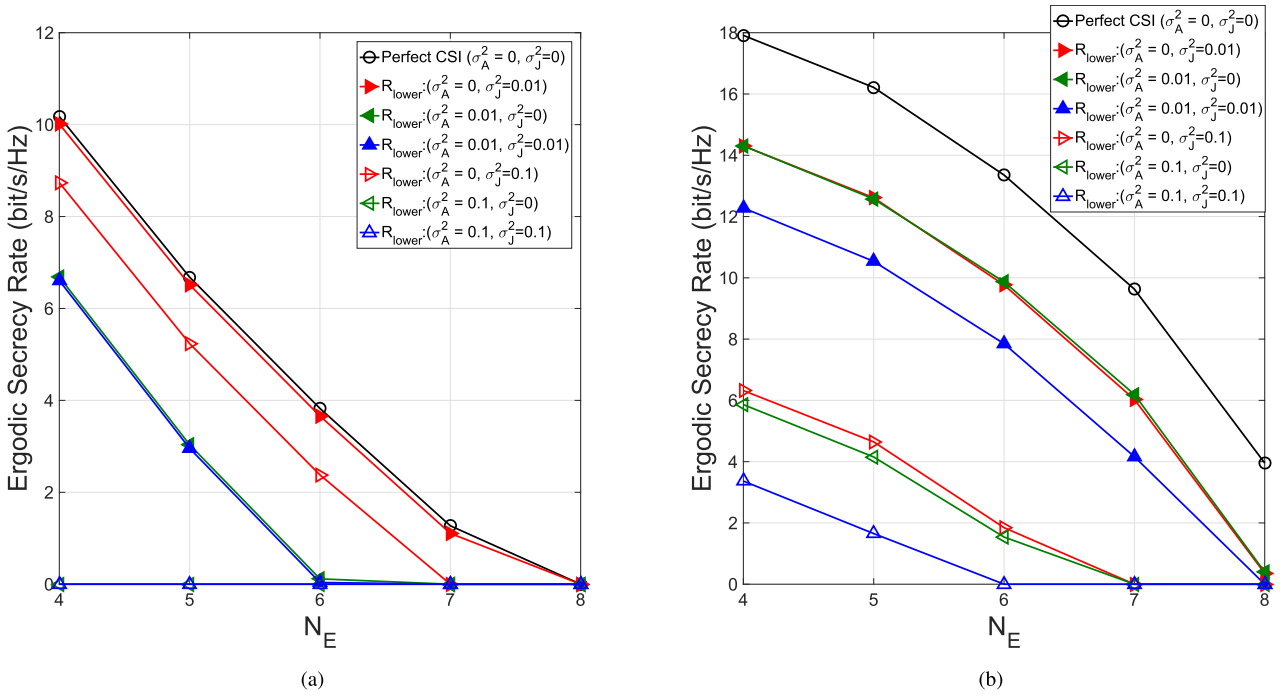

FIGURE 4. R_{lower} versus N_E when SNR = 20 dB. (a) $P_J = 5$ dB. (b) $P_J = 20$ dB.

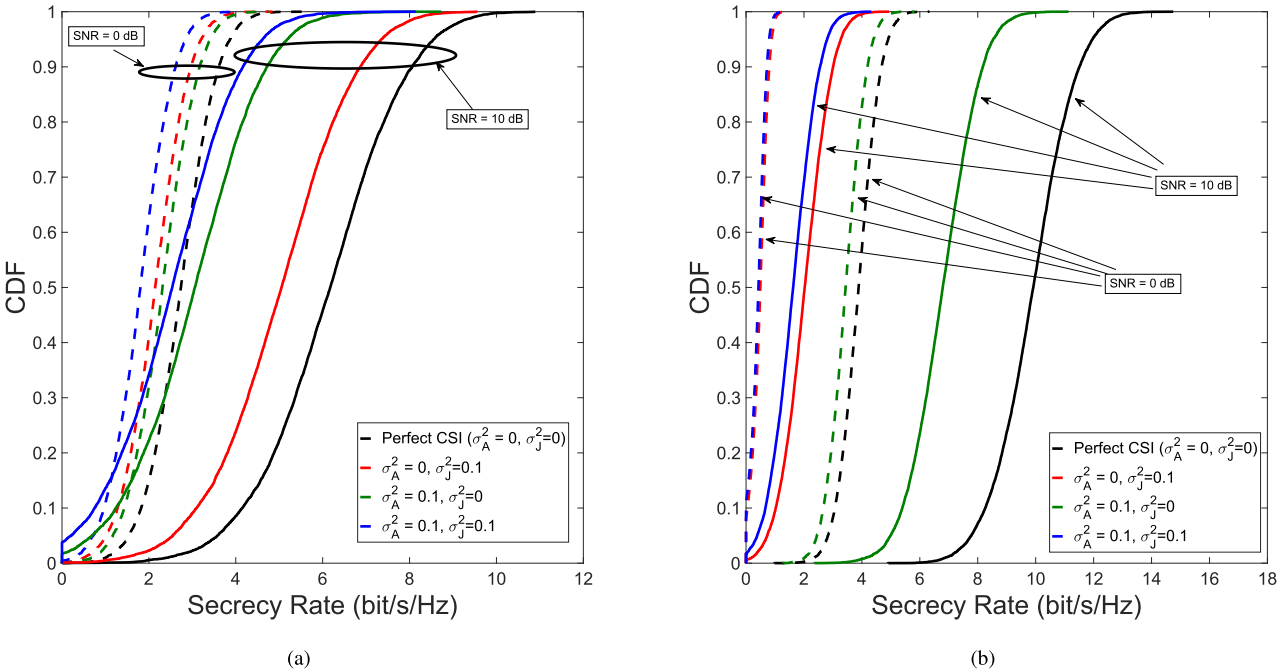

FIGURE 5. Empirical CDF in (17) ($N_E = 4$). (a) $P_J = 5$ dB. (b) $P_J = 20$ dB.

independently to 0, 0.01, and 0.1 when $P_J = 5$ and 20 dB, respectively, for a fixed $N_E = 4$.

As can be seen from these figures, the secrecy rate is degraded by channel estimation error, and the magnitude of the degradation in secrecy rate increases as the value of the channel estimation error increases. It is seen that when the impact of σ_A^2 exists, secrecy rate improves to some extent as SNR increases. Then secrecy rate begins to degrade at an SNR without depending on the magnitude of jamming power. This is because improvement of E-SDM by increasing SNR is saturated at an SNR, which leads to the saturation of Bob's mutual information, even though improvement of the Eve's

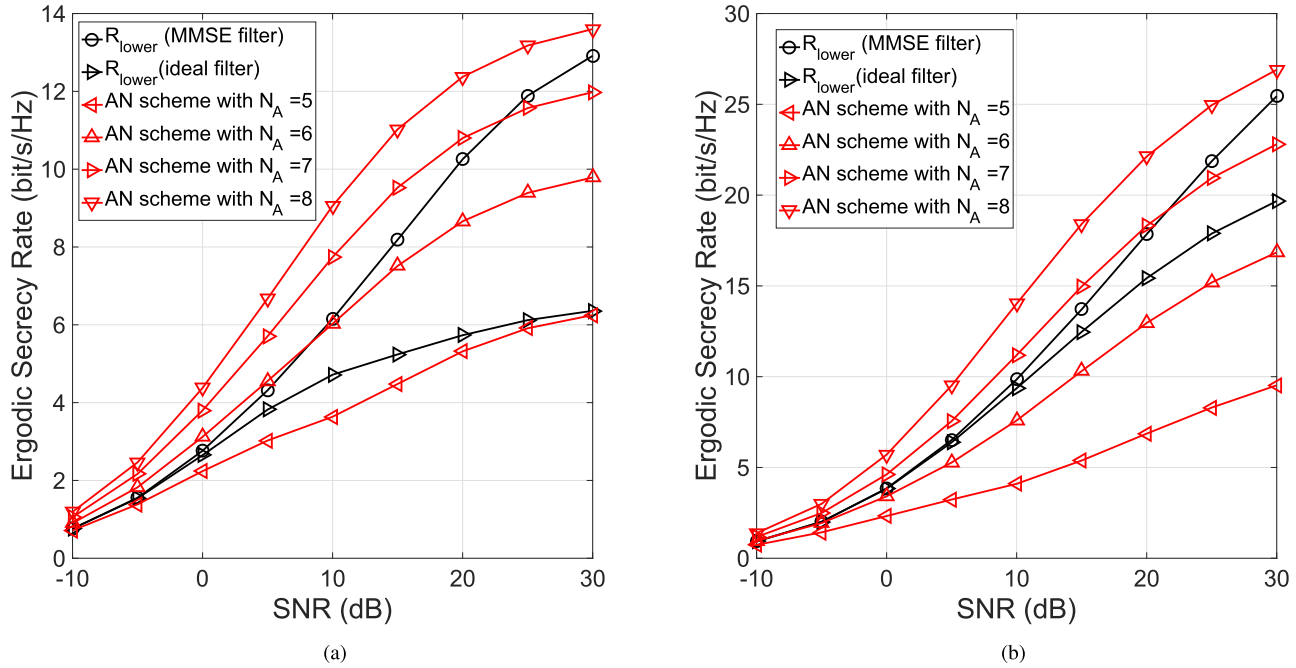

FIGURE 6. Ergodic secrecy rate vs SNR compared with the existing AN scheme and our transmission scheme ($N_E = 4$). (a) $P_J = 5$ dB. (b) $P_J = 20$ dB.

TABLE 1. Simulation parameters.

Assumption of all channels	Rayleigh fading
Variance of the elements of $\mathbf{E}_{BA}$	σ_A^2
Variance of the elements of $\mathbf{E}_{BJ}$	σ_J^2
Alice's transmit power	P_A
Jammer's transmit power	P_J
Number of Alice's antennas N_A	4
Number of Bob's antennas N_B	4
Number of Eve's antennas	N_E
Number of jammer's antennas N_J	8
Number of streams d_1 and d_2	4
Bob's noise power σ_{Bob}^2	1
Eve's noise power σ_{Eve}^2	1

mutual information is not saturated. On the contrary, when the impact of σ_J^2 exists, secrecy rate degrades compared with that in the case of no channel estimation error, but secrecy rate improves and are not saturated as SNR increases. Also, comparing Fig. 2(a) with Fig. 2(b), the impact of σ_J^2 on secrecy rate increases as P_J increases.

Fig. 3(a) and 3(b) shows ergodic secrecy rate versus σ_A^2 and σ_J^2 when $P_J = 5, 10$ dB, respectively, for a fixed SNR $= 10$ dB and $N_E = 4$. Compared Fig. 3(a) with Fig. 3(b), the impact of σ_J^2 on R_{lower} remains small even when σ_J^2 increases, because P_J is small in Fig. 3(a). On the contrary, in Fig. 3(b), it is noticed that the impact of σ_J^2 on R_{lower} increases as σ_J^2 increases. Compared Fig. 3(a) and 3(b), it is also observed that the impact of σ_A^2 on R_{lower} is mitigated by using high power jamming in the regime where σ_J^2 is small.

Fig. 4(a) and 4(b) shows ergodic secrecy rate versus N_E when $P_J = 5$ and 10 dB respectively, with SNR$=$ 20 dB. As the value of N_E increases, the secrecy rate is degraded. This is because Eve's mutual information increases due to spatial receiver that utilizes available diversity. Especially, channel estimation error helps secrecy rate to be 0, which reduces Eve's antennas so that secrecy rate is 0. For example, it can be observed that R_{lower} with $\sigma_A^2 = 0.1$ and $\sigma_J^2 = 0.1$ in Fig. 4(b) becomes 0 by changing from $N_E = 5$ to 6.

In Fig. 5(a) and 5(b), the empirical cumulative distribution function (CDF) in (17) for the case of SNR $= 0, 10$ dB is presented when $P_J = 5$ and 10 dB, respectively, for a fixed $N_E = 4$. It is noted that Fig. 5 represents CDF when we use both transmit covariance matrices (9) and (10) for one channel realization, instead of when (17) is maximized with respect to $\mathbf{Q}_A, \mathbf{Q}_J$. In the case of SNR $= 0$ dB, it is observed that there are few differences among the results in Fig. 5(a), while in Fig. 5(b), there is much difference between the ones with $\sigma_J^2 = 0.1$ and the others, since high power jamming signal in the presence of channel estimation error impairs Bob's received signal greatly. On the other hand, in the case of SNR $= 10$ dB, it is observed that the results with $\sigma_A^2 = 0.1$ in Fig. 5(a) degrades more greatly compared with perfect CSI case. However, in Fig. 5(b), there is the large gap between the results with $\sigma_J^2 = 0.1$ and perfect CSI case.

Fig. 6(a) and 6(b) shows ergodic secrecy rate against SNR with $P_J = 5, 10$ dB for $N_E = 4$ and the other same parameters except for N_A and d_2, respectively, in order to compare the existing AN transmission scheme which consists of Alice, Bob, and Eve in [20] and our transmission scheme when no channel estimation errors exist. It is noted that when we use [20], P_J is equivalent to the power for artificial noise

and d_2 is set as $N_A - d_1$, namely which is $N_A - 4$. That is why we assume that $N_A > 4$ for the AN transmission scheme. Besides, to compare the difference of secrecy rate between the filter that Eve uses, we add the case where Eve uses ideal receiver such as Maximum Likelihood Detection (MLD) to obtain the Eve's capacity in [20], which is described as R_{lower} with ideal filter in Fig. 6. It is observed that the secrecy rate of both AN transmission scheme and our transmission scheme decreases as SNR increases. It is also observed that secrecy rate of AN transmission scheme increases as N_A increases. This is because the increase of N_A that leads to the increase of magnitude of eigenvalues contributes to the improvement of Bob's mutual information. In particular, the AN scheme with $N_A = 8$ achieves the highest secrecy rate in the region below SNR $= 30$ dB in both Fig. 6(a) and 6(b). It is observed that R_{lower} with MMSE filter exceeds R_{lower} with ideal filter. The reason is that Eve's mutual information is larger with ideal filter than that with MMSE filter.

V. CONCLUSION AND FUTURE WORK

In this paper, we have derived and investigated the lower bound on the ergodic secrecy capacity in multiple-input multiple-output (MIMO) wiretap channel aided by a cooperative jammer with channel estimation errors both in Alice-Bob channel and Jammer-Bob channel, which leads to co-channel interference and residual interference, respectively. Numerical and simulation results have shown how those channel estimation errors affected the secrecy rate in terms of low or high power jamming, magnitude of the channel estimation error, and SNR. It has been seen that as the magnitude of the channel estimation errors increases, the more secrecy rate degrades. It has been also observed that when co-channel interference exists, secrecy rate improves to some extent as SNR increases, and then secrecy rate begins to degrade at an SNR without depending on the magnitude of jamming power. Moreover, it has been observed that residual interference also degrades secrecy rate more greatly as jamming transmit power and the magnitude of the channel estimation error in Jammer-Bob channel increase. These results have been observed in terms of not only ergodic capacity but also CDF.

As mentioned in the Introduction, exploiting the co-channel interference is promising for enhancing security. Although there are some works addressing K user interference channel and X network, no works have considered the means of enhancement for security by exploiting the co-channel such as inter-stream interference. Therefore, we treat it as our future work.

APPENDIX
DERIVATION OF (22)

The Bob's mutual infomation $I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})$ is expressed as in [34], [36], [40],

$$I_{\text{Bob}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) = h(\mathbf{x}|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) - h(\mathbf{x}|\mathbf{y}_B, \widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}). \quad (25)$$

$h(\mathbf{x})$ denotes the differential entropy of a complex random vector $\mathbf{x}$. The first term $h(\mathbf{x}|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})$ in (25) is expressed as in [41].

$$\begin{aligned} h(\mathbf{x}|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) &= \log_2 |\pi e \cdot \text{Cov}(\mathbf{x}, \mathbf{x}|\widehat{\mathbf{H}}_{BA})| \\ &= \log_2 |\pi e \cdot \mathbf{Q}_A|. \end{aligned} \quad (26)$$

To obtain $I_{\text{Bob,lower}}(\mathbf{x}; \mathbf{y}_B|\widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})$, we use the upper bound on $h(\mathbf{x}|\mathbf{y}_B, \widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})$, which is given by

$$\begin{aligned} &h(\mathbf{x}|\mathbf{y}_B, \widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) \\ &= h(\mathbf{x} - \widehat{\mathbf{x}}|\mathbf{y}_B, \widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) \\ &\le \log_2 |\pi e \cdot \text{Cov}(\mathbf{x} - \widehat{\mathbf{x}}, \mathbf{x} - \widehat{\mathbf{x}}|\mathbf{y}_B, \widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ})| \end{aligned} \quad (27)$$

where (27) follows the fact that the LHS is upper bounded by the entropy of Gaussian random variables with the same covariance as the mean square error of the liner MMSE estimate $\widehat{\mathbf{x}}$ of $\mathbf{x}$ given $\mathbf{y}_B$, $\widehat{\mathbf{H}}_{BA}$, and $\widehat{\mathbf{H}}_{BJ}$ as in [36], [42], and [43]. The weighting matrix of $\widehat{\mathbf{x}}$ is given by $\text{Cov}(\mathbf{x}, \mathbf{y}_B)\text{Cov}(\mathbf{y}_B, \mathbf{y}_B)^{-1}$ in [36]. $\text{Cov}(\mathbf{y}_B, \mathbf{y}_B)$ is expressed as follows,

$$\begin{aligned} \text{Cov}(\mathbf{y}_B, \mathbf{y}_B) &= \mathbb{E}[\mathbf{y}_B\mathbf{y}_B^H] \\ &= \widehat{\boldsymbol{\Sigma}}\mathbf{Q}_A\widehat{\boldsymbol{\Sigma}}^H + \mathbb{E}[\tilde{\mathbf{E}}_{BA}\boldsymbol{\Lambda}\mathbf{s}\mathbf{s}^H\boldsymbol{\Lambda}^H\tilde{\mathbf{E}}_{BA}] \\ &\quad + \mathbb{E}[\tilde{\mathbf{E}}_{BJ}\boldsymbol{\Lambda}_J\boldsymbol{v}_J\boldsymbol{v}_J^H\boldsymbol{\Lambda}_J^H\tilde{\mathbf{E}}_{BJ}^H] + \mathbb{E}[\mathbf{n}_B'\mathbf{n}_B'^H]. \end{aligned} \quad (28)$$

Furthermore, second, third, and fourth terms in (28), respectively, are expressed as in [35],

$$\begin{aligned} &\mathbb{E}[\tilde{\mathbf{E}}_{BA}\boldsymbol{\Lambda}\mathbf{s}\mathbf{s}^H\boldsymbol{\Lambda}^H\tilde{\mathbf{E}}_{BA}^H] \\ &= \mathbb{E}_{\tilde{\mathbf{E}}_{BA},\boldsymbol{\Lambda},\mathbf{s}}[\tilde{\mathbf{E}}_{BA}\boldsymbol{\Lambda}\mathbf{s}\mathbf{s}^H\boldsymbol{\Lambda}^H\tilde{\mathbf{E}}_{BA}^H] \\ &= \sigma_A^2\mathbb{E}_{\boldsymbol{\Lambda},\mathbf{s}}[\text{Tr}(\boldsymbol{\Lambda}\mathbf{s}\mathbf{s}^H\boldsymbol{\Lambda}^H)]\mathbf{I}_{d_1} \\ &= \sigma_A^2\text{Tr}(\mathbf{Q}_A)\mathbf{I}_{d_1} \\ &= \sigma_A^2 P_A\mathbf{I}_{d_1} \end{aligned} \quad (29)$$

and

$$\begin{aligned} &\mathbb{E}[\tilde{\mathbf{E}}_{BJ}\boldsymbol{\Lambda}_J\boldsymbol{v}_J\boldsymbol{v}_J^H\boldsymbol{\Lambda}_J^H\tilde{\mathbf{E}}_{BJ}^H] \\ &= \mathbb{E}_{\tilde{\mathbf{E}}_{BJ},\boldsymbol{\Lambda}_J,\boldsymbol{v}_J}[\tilde{\mathbf{E}}_{BJ}\boldsymbol{\Lambda}_J\boldsymbol{v}_J\boldsymbol{v}_J^H\boldsymbol{\Lambda}_J^H\tilde{\mathbf{E}}_{BJ}^H] \\ &= \sigma_J^2\mathbb{E}_{\boldsymbol{\Lambda}_J,\boldsymbol{v}_J}[\text{Tr}(\boldsymbol{\Lambda}_J\boldsymbol{v}_J\boldsymbol{v}_J^H\boldsymbol{\Lambda}_J^H)]\mathbf{I}_{d_1} \\ &= \sigma_J^2\text{Tr}(\mathbf{Q}_J)\mathbf{I}_{d_1} \\ &= \sigma_J^2 P_J\mathbf{I}_{d_1} \end{aligned} \quad (30)$$

and

$$\mathbb{E}[\mathbf{n}_B'\mathbf{n}_B'^H] = \sigma_{Bob}^2\mathbf{I}_{d_1}. \quad (31)$$

Using (29), (30), and (31), $\text{Cov}(\mathbf{y}_B, \mathbf{y}_B)$ is finally expressed as,

$$\begin{aligned} &\text{Cov}(\mathbf{y}_B, \mathbf{y}_B) \\ &= \widehat{\boldsymbol{\Sigma}}\mathbf{Q}_A\widehat{\boldsymbol{\Sigma}}^H + (\sigma_A^2 P_A + \sigma_J^2 P_J + \sigma_{Bob}^2)\mathbf{I}_{d_1}. \end{aligned} \quad (32)$$

Moreover, $\text{Cov}(\mathbf{x}, \mathbf{y_B})$ is expressed as,

$$\begin{aligned} \text{Cov}(\mathbf{x}, \mathbf{y_B}) &= \mathbb{E}[\mathbf{x}\mathbf{y}_B^H] \\ &= \mathbf{Q}_A\widehat{\boldsymbol{\Sigma}}^H. \end{aligned} \quad (33)$$

Therefore, $\widehat{\mathbf{x}}$ is given by,

$$\begin{aligned} \widehat{\mathbf{x}} &= \text{Cov}(\mathbf{x}, \mathbf{y}_B)\text{Cov}(\mathbf{y}_B, \mathbf{y}_B)^{-1}\mathbf{y}_B \\ &= \mathbf{Q}_A\widehat{\boldsymbol{\Sigma}}^H\left(\widehat{\boldsymbol{\Sigma}}\mathbf{Q}_A\widehat{\boldsymbol{\Sigma}}^H + (\sigma_A^2 P_A + \sigma_J^2 P_J + \sigma_{Bob}^2)\cdot\mathbf{I}_{d_1}\right)^{-1}\mathbf{y}_B. \end{aligned} \quad (34)$$

Substituting $\widehat{\mathbf{x}}$ into the corresponding covariance in (27), we have

$$\begin{aligned}
&\mathrm{Cov}(\mathbf{x}-\widehat{\mathbf{x}}, \mathbf{x}-\widehat{\mathbf{x}}|\mathbf{y}_B, \widehat{\mathbf{H}}_{BA}, \widehat{\mathbf{H}}_{BJ}) \\
&\quad = \mathbb{E}[(\mathbf{x}-\widehat{\mathbf{x}})(\mathbf{x}-\widehat{\mathbf{x}})^H] \\
&\quad = \mathbb{E}[\mathbf{x}(\mathbf{x}-\widehat{\mathbf{x}})^H] \qquad (35) \\
&\quad = \mathbf{Q}_A - \mathbf{Q}_A^H \widehat{\boldsymbol{\Sigma}}^H \Big(\widehat{\boldsymbol{\Sigma}} \mathbf{Q}_A \widehat{\boldsymbol{\Sigma}}^H + \Big(\sigma_A^2 P_A \\
&\qquad\qquad + \sigma_J^2 P_J + \sigma_{Bob}^2 \Big) \mathbf{I}_{d_1} \Big)^{-1} \widehat{\boldsymbol{\Sigma}} \mathbf{Q}_A \qquad (36)
\end{aligned}$$

where (35) follows the orthogonality that satisfies $\mathbb{E}[\widehat{\mathbf{x}}(\mathbf{x}-\widehat{\mathbf{x}})^H] = 0$. Moreover, applying the matrix inversion lemma to (36) leads to (22).

REFERENCES

[1] N. Sklavos and X. Zhang, *Wireless Security Cryptography: Specifications Implementations*, 1st ed. Boca Raton, FL, USA: CRC Press, 2007.

[2] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[4] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[5] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

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

[7] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[10] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 2152–2155.

[11] Z. Haiyang and W. Bao-yun, "The achievable secrecy rate of MISO wiretap channels," in *Proc. 2011 Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nov. 2011, pp. 1–4.

[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[13] L. Lingxiang, C. Zhi, and F. Jun, "On secrecy capacity of Gaussian wiretap channel aided by a cooperative jammer," *IEEE Signal Process. Lett.*, vol. 21, no. 11, pp. 1356–1360, Nov. 2014.

[14] S. Liu, Y. Hong, and E. Viterbo, "Cooperative jamming for MIMO wiretap channels," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Oct. 2014, pp. 388–392.

[15] Z. Chu, M. Johnston, and S. L. Goff, "Alternating optimization for mimo secrecy channel with a cooperative jammer," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC)*, May 2015, pp. 1–5.

[16] Z. Chu, M. Johnston, and S. Le Goff, "Robust beamforming techniques for miso secrecy communication with a cooperative jammer," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC)*, May 2015, pp. 1–5.

[17] S. Ma, M. Hempel, Y. L. Yang, and H. Sharif, "An approach to secure wireless communications using randomized eigenvector-based jamming signals," in *Proc. Int. Wireless Commun. Mobile Comput. Conf.*, 2010, pp. 1172–1176.

[18] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[19] H. P. Bui, Y. Ogawa, T. Nishimura, and T. Ohgane, "Performance evaluation of a multi-user MIMO system with prediction of time-varying indoor channels," *IEEE Trans. Antennas Propag.*, vol. 61, no. 1, pp. 371–379, Jan. 2013.

[20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[21] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[22] L. Li, A. P. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1433–1448, Dec. 2016.

[23] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810–3823, Jul. 2015.

[24] 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.

[25] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652–3664, Oct. 2014.

[26] J. M. Taylor, M. Hempel, H. Sharif, S. Ma, and Y. Yang, "Impact of channel estimation errors on effectiveness of eigenvector-based jamming for physical layer security in wireless networks," in *Proc. IEEE 16th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Jun. 2011, pp. 122–126.

[27] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[28] İ. E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, 1999.

[29] M. D. Larsen and A. L. Swindlehurst, "MIMO SVD-based multiplexing with imperfect channel knowledge," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Mar. 2010, pp. 3454–3457.

[30] E. K. S. Au, S. Jin, M. R. McKay, W. H. Mow, X. Gao, and I. B. Collings, "BER analysis of MIMO-SVD systems with channel estimation error and feedback delay," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2007, pp. 4375–4380.

[31] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[32] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2537–2551, Apr. 2016.

[33] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[34] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.

[35] L. Musavian, M. R. Nakhai, M. Dohler, and A. H. Aghvami, "Effect of channel uncertainty on the mutual information of MIMO fading channels," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 2798–2806, Sep. 2007.

[36] M. Médard, "The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 933–946, May 2000.

[37] R. Couillet, M. Debbah, and J. W. Silverstein, "Asymptotic capacity of multi-user MIMO communications," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2009, pp. 16–20.

[38] C. Artigue and P. Loubaton, "On the ergodic capacity and precoder design of flat fading MIMO systems equipped with MMSE receivers," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2009, pp. 1095–1099.

[39] C. Zhong and T. Ratnarajah, "Ergodic sum rate analysis of Rayleigh product MIMO channels with linear MMSE receiver," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2011, pp. 2607–2611.

[40] T. Yoo and A. Goldsmith, "Capacity of fading MIMO channels with channel estimation error," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 2. Jun. 2004, pp. 808–813.

[41] G. Taubock, "Complex-valued random vectors and channels: Entropy, divergence, and capacity," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2729–2744, May 2012.

[42] H. Farhadi, M. N. Khormuji, C. Wang, and M. Skoglund, "Ergodic interference alignment with noisy channel state information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 584–588.

[43] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.

SHUNYA IWATA received the B.E. degree in information engineering from Keio University, Yokohama, Japan, in 2015. He is currently pursuing the M.E. degree with Keio University. His research interests include physical-layer security.

TOMOAKI OHTSUKI received the B.E., M.E., and Ph.D. degrees in electrical engineering from Keio University, Yokohama, Japan, in 1990, 1992, and 1994, respectively. From 1993 to 1995, he was a Special Researcher of Fellowships of the Japan Society for the Promotion of Science for Japanese Junior Scientists. From 1994 to 1995, he was a Post-Doctoral Fellow and a Visiting Researcher in electrical engineering with Keio University. From 1995 to 2005, he was with the Science University of Tokyo. From 1998 to 1999, he was with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, CA, USA. In 2005, he joined Keio University, where he is currently a Professor. He is involved in research on wireless communications, optical communications, signal processing, and information theory. He received the 1997 Inoue Research Award for Young Scientist, the 1997 Hiroshi Ando Memorial Young Engineering Award, the Ericsson Young Scientist Award 2000, the 2002 Funai Information and Science Award for Young Scientist, the IEEE 1st Asia-Pacific Young Researcher Award 2001, the 5th International Communication Foundation Research Award, the 2011 IEEE SPCE Outstanding Service Award, the 28th TELECOM System Technology Award, the ETRI Journal's 2012 Best Reviewer Award, and the 9th International Conference on Communications and Networking in China 2014 Best Paper Award.

POOI-YUEN KAM was born in Ipoh, Malaysia. He received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1972, 1973, and 1976, respectively.

From 1976 to 1978, he was a member of the Technical Staff at the Bell Telephone Laboratories, Holmdel, NJ, USA, where he was involved in packet network studies. Since 1978, he has been with the Department of Electrical and Computer Engineering, National University of Singapore, where he is currently a Professor. From 2000 to 2003, he served as the Deputy Dean of Engineering and the Vice Dean for Academic Affairs with the Faculty of Engineering, National University of Singapore. His research interests are in the communication sciences and information theory and their applications to wireless and optical communications. He was on sabbatical leave at the Tokyo Institute of Technology, Tokyo, Japan, from 1987 to 1988, under the sponsorship of the Hitachi Scholarship Foundation. In 2006, he was invited to the School of Engineering Science, Simon Fraser University, Burnaby, BC, Canada, as the David Bested Fellow. He was appointed as a Distinguished Guest Professor (Global) at the Graduate School of Science and Technology, Keio University, Tokyo, from 2015 to 2017.

Dr. Kam is a member of Eta Kappa Nu, Tau Beta Pi, and Sigma Xi. He was an Elected Fellow of the IEEE for his contributions to receiver design and performance analysis for wireless communications. He received the Best Paper Award at the IEEE VTC2004-Fall, at the IEEE VTC2011-Spring, at the IEEE ICC2011, and at the IEEE/CIC ICCC2015. Since 2011, he has been a Senior Editor of the IEEE Wireless Communications Letters. From 1996 to 2011, he served as the Editor for Modulation and Detection for Wireless Systems of the IEEE Transactions on Communications. From 2007 to 2012, he served on the Editorial Board of PHYCOM, the *Journal of Physical Communications of Elsevier*. He was a Co-Chair of the Communication Theory Symposium of IEEE Globecom 2014.