Deterministic Pilot Jamming Symbol Design for Enhanced Physical Layer Secrecy

Sungjun Ahn, Wonju Lee, *Kwang Eog Lee, and Joonhyuk Kang
Korea Advanced Institute of Science and Technology, Daejeon, Korea
*Agency for Defense Development, Daejeon, Korea
Email : {sungjunahn, wonjulee}@kaist.ac.kr, *kelee@add.re.kr, jhkang@ee.kaist.ac.kr

***Abstract*—Tackling the physical layer secrecy issue, existing studies on cooperative jamming generally assume the persistent jamming and perfect channel estimation at the receiver side. However, these two assumptions are incompatible since jamming signals can corrupt the pilot symbols. In addition, due to the energy budget limitation, persistent jamming is burdensome to the cooperative jammers. To address these issues, we propose a cooperative jamming strategy that designs the jamming symbols aiming only at the pilot signals to attain security improvement by manipulating the channel estimations at the authorized receiver and the eavesdropper simultaneously. Via computer simulations, we compare the performance of the proposed strategy with that of a conventional persistent artificial noise-aided strategy, and these results demonstrate that the proposed strategy achieves substantial secrecy rate gain in wide region, especially at the low data transmission power regime and at the rank-deficient environment.**

***Index Terms*—Physical layer secrecy, channel estimation, cooperative jamming, pilot jamming.**

I. Introduction

It is a vital issue in wireless communication systems to cope with adversarial eavesdroppers due to the broadcast nature of the wireless medium. As a promising technology to resolve the security issue, information theoretic approaches at the physical layer have been recently investigated [1]-[4]. In particular, artificial noise-aided cooperative jamming strategies have been intensively examined [5]-[7], since the data symbols are unknown in general and introducing artificial noise is proven to be optimal in this case [8]. These works emphasize that the artificial noise, which is generated from the legitimate transmitter or external cooperative jammers degrades the eavesdropping channel and hence deprives the opportunity to restore a desired message from the eavesdropper. Furthermore, so as to introduce artificial noise to the eavesdropper more destructively, beamformers have been designed in spatially correlated fashion [9].

While cooperative jamming has been examined to provide substantial theoretic gain on security, it is still controversial in practicality. One questionable point of the previous literature on cooperative jamming is the simultaneous assumption of perfect channel estimation and persistent jamming. To remark that the persistent jamming covers the pilot transmission phase, the channel estimation at the receiver side is ruined by undesired jamming signals. On the other hand, the authors of [10] criticize the availability of the perfect channel knowledge at the transmitter side by introducing the uplink pilot contamination attack from an active eavesdropper, and verify that the impact of pilot corruption is critical to security. Motivated from this result, in this paper, we claim that the cooperative jamming deserves to be addressed in an extended perspective, providing a precise description of channel mismeasure effect. Moreover, we reveal an opportunity to improve physical layer secrecy, which can be obtained by disrupting the channel estimation at the eavesdropper.

In addition to the channel estimation issue, an energy budget issue arises from the persistent cooperative jamming. In general, the cooperative jammers are inherently energy-limited since they mainly pursue a reliable communication of their own network [11], [12], or are empowered by constrained power sources such as battery or energy harvesting [13]. It emphasizes that the cooperative jamming ought to be carried out efficiently in light of energy burden reduction. Hence, the constant transmission at the cooperative jammer is inadequate. In this context, along with extending the cooperative jamming-assisted physical layer secrecy system to include the pilot transmission phase, it is worth mentioning about the temporal cooperative jamming upon pilot signals in terms of energy efficiency.

In this paper, we propose a cooperative jamming-assisted secure communication scheme that targets solely on the pilot transmission phase. Unlike the conventional persistent jamming schemes, we deliver jamming signals periodically in concern of energy efficiency. Where the pilot sequence can be publicly known from its finite and standardized characteristic, we introduce a deterministic design of pilot jamming symbols which provides substantial secrecy rate gain. Furthermore, we provide a performance comparison between the proposed technique and the persistent artificial noise-aided scheme through simulations.

The rest of the paper is organized as follows. Section II describes the system model throughout this work. In Section III, we investigate the cooperative pilot jamming symbol design, pursuing the physical layer secrecy enhancement. The numerical results are provided in Section IV. Lastly, Section V concludes the paper.

Notation: Boldface lowercase and uppercase letters denote vectors and matrices, respectively; $[\cdot]^H$, $[\cdot]^{-1}$, and $[\cdot]^\dagger$ denote complex transpose, inverse, and pseudo-inverse, respectively; $[\cdot]^+$ denote the function $\max(0,\cdot)$; $\mathrm{diag}\{\mathbf{x}\}$ stands for a

978-1-5090-3781-9/16/$31.00 ©2016 IEEE

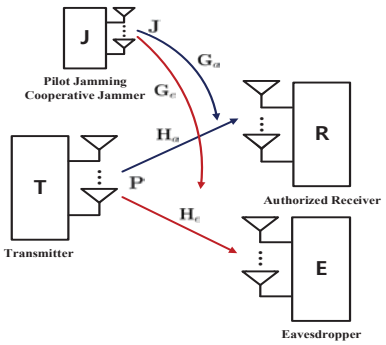

Fig. 1. MIMO wiretap channel with pilot jamming cooperative jammer

diagonal matrix with the elements of $\mathbf{x}$ in diagonal entries; $|\mathbf{A}|$ and $\mathrm{tr}\{\mathbf{A}\}$ are the determinant and the trace of a square matrix $\mathbf{A}$, respectively; $||\mathbf{A}||_{\mathrm{F}} = \sqrt{\mathrm{tr}\{\mathbf{A}\mathbf{A}^H\}}$ represents the Frobenius norm of $\mathbf{A}$; $\mathrm{span}(\mathbf{A})$ and $\mathrm{span}^{\perp}(\mathbf{A})$ represent the space spanned by the column vectors of matrix $\mathbf{A}$ and the null-space of it, respectively; $\mathbf{I}$ is the identity matrix; $\Pi_{\mathbf{A}} \triangleq \mathbf{A}(\mathbf{A}^H\mathbf{A})^{-1}\mathbf{A}^H$ and $\Pi_{\mathbf{A}}^{\perp} \triangleq \mathbf{I} - \Pi_{\mathbf{A}}$ are the orthogonal projection and the orthogonal complement onto the column space of $\mathbf{A}$ and onto the orthogonal complement of the column space of $\mathbf{A}$, respectively.

II. System Model

We consider a $N_T \times N_R$ MIMO wiretap channel in the presence of an eavesdropper with N_R antennas and a cooperative jammer with N_T antennas as depicted in Fig. 1. The channel from the transmitter to the authorized receiver and the eavesdropper are denoted as $\mathbf{H}_{\mathrm{a}} \in \mathbb{C}^{N_R \times N_T}$ and $\mathbf{H}_{\mathrm{e}} \in \mathbb{C}^{N_R \times N_T}$, respectively. The channels from the cooperative jammer to the authorized receiver and the eavesdropper are $\mathbf{G}_{\mathrm{a}} \in \mathbb{C}^{N_R \times N_T}$ and $\mathbf{G}_{\mathrm{e}} \in \mathbb{C}^{N_R \times N_T}$, respectively. We assume the cooperative jammer has full channel state information (CSI)[1] while the receiving terminals estimate the respective reception channels $\mathbf{H}_{\mathrm{a}}$ and $\mathbf{H}_{\mathrm{e}}$ with regard to the given knowledge of pilot symbols.

To enable the channel estimation at the authorized receiver, a sufficient number of pilot symbols is required in each frame, i.e., N_T pilot symbols are required at least. Therefore, transmission is composed into two distinct phases: a pilot transmission phase and a subsequent data transmission phase. Here, without loss of generality, we assign N_T slots to the pilot transmission phase in which each antenna sends one symbol per slot. We assume that the ith antenna transmits a pilot symbol p_i at the ith slot of the pilot transmission phase for $i = 1, 2, ..., N_T$, and we denote pilot symbol matrix by $\mathbf{P} = \mathrm{diag}\{[p_1, p_2, ..., p_{N_T}]^T\} \in \mathbb{C}^{N_T}$. Being aware of $\mathbf{P}$, the cooperative jammer inserts pilot jamming signals into the sounding signals in order to ruin the channel estimation at the eavesdropper and not to disrupt the channel estimation at the authorized receiver simultaneously. As written in [15], the consequent received channel sounding signal at the eavesdropper $\mathbf{S}_{\mathrm{e}} \in \mathbb{C}^{N_R \times N_T}$ can be expressed as

$$\mathbf{S}_{\mathrm{e}} = \mathbf{H}_{\mathrm{e}}\mathbf{P} + \mathbf{G}_{\mathrm{e}}\mathbf{J} + \mathbf{N}_{\mathrm{e}}, \tag{1}$$

where $\mathbf{J} \in \mathbb{C}^{N_T}$ is a pilot jamming symbol matrix which is denoted as $[\mathbf{j}_1, \mathbf{j}_2, ..., \mathbf{j}_{N_T}]$. Here, the ith column vector $\mathbf{j}_i$ implies the jamming symbol vector transmitted at the ith pilot transmission slot. The noise that the eavesdropper received in pilot transmission phase is denoted by $\mathbf{N}_{\mathrm{e}} \in \mathbf{C}^{N_R \times N_T}$, and is assumed to have i.i.d. circularly symmetric complex Gaussian entries with zero-mean and unit variance. The equivalent signal model can be established for the authorized receiver as $\mathbf{S}_{\mathrm{a}} = \mathbf{H}_{\mathrm{a}}\mathbf{P} + \mathbf{G}_{\mathrm{a}}\mathbf{J} + \mathbf{N}_{\mathrm{a}}$. Hereafter, we denote the equivalent terms for the authorized receiver and the eavesdropper by subscripts a and e, respectively.

We suppose here to accomplish channel estimation by least-square estimation. The estimated channel at the eavesdropper is given by

$$\hat{\mathbf{H}}_{\mathrm{e}} = \mathbf{H}_{\mathrm{e}} + \mathbf{G}_{\mathrm{e}}\mathbf{J}\mathbf{P}^{-1} + \mathbf{N}_{\mathrm{e}}\mathbf{P}^{-1}. \tag{2}$$

In turn, the received signal in data phase is written as

$$\begin{aligned} \mathbf{y}_{\mathrm{e}} &= \mathbf{H}_{\mathrm{e}}\mathbf{x} + \mathbf{n}_{\mathrm{e}} \\ &= (\hat{\mathbf{H}}_{\mathrm{e}} + \mathbf{E}_{\mathrm{e}})\mathbf{x} + \mathbf{n}_{\mathrm{e}}, \end{aligned} \tag{3}$$

where $\mathbf{x} \in \mathbb{C}^{N_T \times 1}$ denotes the transmitted data signal, $\mathbf{E}_{\mathrm{e}} = \mathbf{H}_{\mathrm{e}} - \hat{\mathbf{H}}_{\mathrm{e}}$ is a channel error matrix, and $\mathbf{n}_{\mathrm{e}}$ is the noise vector at the eavesdropper. The elements of $\mathbf{x}$ and $\mathbf{n}_{\mathrm{e}}$ are assumed to be zero-mean circularly symmetric Gaussian random variables with covariances $\gamma/N_T\mathbf{I}$ and $\mathbf{I}$, respectively, where γ represents a data transmission power normalized to a noise power.

Since the cooperative jammer aims reliable communication of legitimate pair and security concurrently, it intends to design proper pilot jamming signal that maximizes the achievable secrecy rate, which is given by a solution of the following problem:

$$\begin{aligned} &\max_{\mathbf{J}} \; R_{\mathrm{sec}}(\mathbf{J}) \\ &\text{s.t. } ||\mathbf{J}||_{\mathrm{F}}^2 \le P_J, \end{aligned} \tag{4}$$

where the approximated expression of the achievable secrecy rate motivated by [16], with Gaussian data signal inputs, is given as follows:

$$\begin{aligned} R_{\mathrm{sec}}(\mathbf{J}) &= [I_{\mathrm{a}}(\mathbf{J}) - I_{\mathrm{e}}(\mathbf{J})]^+ \\ &\approx \left[\log \left| \mathbf{I} + \frac{\gamma}{N_T}\hat{\mathbf{H}}_{\mathrm{a}}\hat{\mathbf{H}}_{\mathrm{a}}^H \left(\mathbf{I} + \frac{\gamma}{N_T}\mathbf{E}_{\mathrm{a}}\mathbf{E}_{\mathrm{a}}^H \right)^{-1} \right| \right. \\ &\quad \left. - \log \left| \mathbf{I} + \frac{\gamma}{N_T}\hat{\mathbf{H}}_{\mathrm{e}}\hat{\mathbf{H}}_{\mathrm{e}}^H \left(\mathbf{I} + \frac{\gamma}{N_T}\mathbf{E}_{\mathrm{e}}\mathbf{E}_{\mathrm{e}}^H \right)^{-1} \right| \right]^+, \end{aligned} \tag{5}$$

with mutual information of the transmitter-to-legitimate receiver link $I_{\mathrm{a}}(\mathbf{J})$ and of the transmitter-to-eavesdropper link $I_{\mathrm{e}}(\mathbf{J})$.

[1]It is widely assumed that the cooperative jammer has the information of the eavesdropper's channels, in physical layer secrecy literature (see [7], [11], [12]). Specifically, in [14], this issue is well justified by dealing with the internal eavesdroppers.

$$\mathbf{J} = \sqrt{P}\frac{\lambda\left(\alpha\Pi_{\mathbf{G}_{\mathrm{e}}^H} + (1-\alpha)\,\Pi^{\perp}_{\mathbf{G}_{\mathrm{e}}^H}\right)\mathbf{G}_{\mathrm{a}}^{\dagger}\mathbf{H}_{\mathrm{a}}\mathbf{P} - (1-\lambda)\left(\beta\Pi_{\mathbf{G}_{\mathrm{a}}^H} + (1-\beta)\,\Pi^{\perp}_{\mathbf{G}_{\mathrm{a}}^H}\right)\mathbf{G}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\mathbf{P}}{\left|\left|\lambda\left(\alpha\Pi_{\mathbf{G}_{\mathrm{e}}^H} + (1-\alpha)\,\Pi^{\perp}_{\mathbf{G}_{\mathrm{e}}^H}\right)\mathbf{G}_{\mathrm{a}}^{\dagger}\mathbf{H}_{\mathrm{a}}\mathbf{P} - (1-\lambda)\left(\beta\Pi_{\mathbf{G}_{\mathrm{a}}^H} + (1-\beta)\,\Pi^{\perp}_{\mathbf{G}_{\mathrm{a}}^H}\right)\mathbf{G}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\mathbf{P}\right|\right|_{\mathrm{F}}} \tag{6}$$

III. Deterministic pilot jamming symbol design at cooperative jammer

In this section, we aim at designing the pilot jamming symbols to achieve secret and reliable communication between legitimate terminal pair. We remark that since the data symbol interpretation at the legitimate receiver and the eavesdropper is controlled by the preceding channel estimation, the proposed pilot selective jamming strategy is expected to offer a feasible security performance.

Clearly, the problem (4) is non-concave due to the negative term of (5). Even though the non-concave maximization problems have been generally solved by convex semidefinite programming (SDP) technique with linear relaxation such as difference-of-convex (DC) algorithm, due to its dependency of $\mathbf{J}$ on $\mathbf{H}_{\mathrm{a}}$ and $\mathbf{H}_{\mathrm{e}}$ in problem (4), it is cumbersome to directly obtain $\mathbf{J}$ from (4). Therefore, we alternatively introduce a parametric form of pilot jamming symbols and reformulate problem (4) into the optimal parameter searching problem.

Our idea proceeds in three parts: (i) to find the sub-solutions that respectively improve and degrade the channel estimation derived from $\mathbf{S}_{\mathrm{a}}$ and $\mathbf{S}_{\mathrm{e}}$; (ii) to transform the sub-solutions into the mediatable forms, which can control the spatial components with respect to the authorized channel and the eavesdropping channel; and (iii) to combine the modified sub-solutions with the optimal parameters pursuing the achievable secrecy rate maximization.

We focus on the fact that wiping out the pilot at the eavesdropper induces the eavesdropper to fail decoding and to regard the received signals solely as noise. On the contrary, when an appropriate pilot amplification is provided, the quality of service at the authorized receiver is improved. Therefore, we get two distinct sub-solutions; the eavesdropper pilot nulling symbol $\mathbf{J}^{(\mathrm{PN,e})} = -\mathbf{G}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\mathbf{P}$ and the legitimate pilot amplifying symbol $\mathbf{J}^{(\mathrm{PA,a})} = \mathbf{G}_{\mathrm{a}}^{\dagger}\mathbf{H}_{\mathrm{a}}\mathbf{P}$. By noting that jamming signals orthogonal to the row space of $\mathbf{G}_{\mathrm{a}}$ yield no interference to the authorized receiver, we split $\mathbf{J}^{(\mathrm{PN,e})}$ into two components, projected onto span$(\mathbf{G}_{\mathrm{a}}^H)$ and onto span$^{\perp}(\mathbf{G}_{\mathrm{a}}^H)$. Since $\mathbf{J}^{(\mathrm{PA,a})}$ is already mapped into a space span$(\mathbf{G}_{\mathrm{a}}^H)$, so there is no need to project it onto the dual space span$^{\perp}(\mathbf{G}_{\mathrm{a}}^H)$. Similarly, $\mathbf{J}^{(\mathrm{PA,a})}$ is split into span$(\mathbf{G}_{\mathrm{e}}^H)$ component and span$^{\perp}(\mathbf{G}_{\mathrm{e}}^H)$ component. Combining the sub-solutions, the mediation among $\Pi_{\mathbf{G}_{\mathrm{e}}^H}\mathbf{J}^{(\mathrm{PA,a})}$, $\Pi^{\perp}_{\mathbf{G}_{\mathrm{e}}^H}\mathbf{J}^{(\mathrm{PA,a})}$, $\Pi_{\mathbf{G}_{\mathrm{a}}^H}\mathbf{J}^{(\mathrm{PN,e})}$, and $\Pi^{\perp}_{\mathbf{G}_{\mathrm{a}}^H}\mathbf{J}^{(\mathrm{PN,e})}$ comes up with the pilot jamming symbol (6), where λ, α, and β are mediation factors which indicate the weighting ratio on sub-solution terms, P is the power coefficient which satisfies the power constraint. In consequence, we reformulate problem (4) into the following form

$$\begin{aligned}&\max_{\lambda,\alpha,\beta,P}\; R_{\mathrm{sec}}(\lambda,\alpha,\beta,P)\\ &\quad\text{s.t. } 0\le\lambda,\alpha,\beta\le 1 \text{ and } 0\le P\le P_J,\end{aligned} \tag{7}$$

which is a real-valued scalar parameter searching problem.

To offer an insight on symmetric full-rank case, we now consider a system that all nodes are equipped with same number of antennas, i.e., $N_T = N_R$. Increase of N_R provides a degree-of-freedom (DoF) gain on legitimate terminal pair, but also gives better chance to the eavesdropper to overhear. Moreover, it degrades the jamming performance since there is no more extra dimensionality to exploit. In detail, $\mathbf{G}_{\mathrm{a}}$ and $\mathbf{G}_{\mathrm{e}}$ becomes full-rank matrix, and consequently the respective null-spaces of $\mathbf{G}_{\mathrm{a}}$ and $\mathbf{G}_{\mathrm{e}}$ are reduced to zero. Thus, dropping α and β out, (6) is reduced into

$$\mathbf{J} = \sqrt{P}\frac{\lambda\mathbf{G}_{\mathrm{a}}^{-1}\mathbf{H}_{\mathrm{a}}\mathbf{P} - (1-\lambda)\,\mathbf{G}_{\mathrm{e}}^{-1}\mathbf{H}_{\mathrm{e}}\mathbf{P}}{\left|\left|\lambda\mathbf{G}_{\mathrm{a}}^{-1}\mathbf{H}_{\mathrm{a}}\mathbf{P} - (1-\lambda)\,\mathbf{G}_{\mathrm{e}}^{-1}\mathbf{H}_{\mathrm{e}}\mathbf{P}\right|\right|_{\mathrm{F}}}. \tag{8}$$

Remark 1: Note that $\mathbf{J}^{(\mathrm{PA,a})}$ and $\mathbf{J}^{(\mathrm{PN,e})}$ can be highly correlated due to the full-rank channel condition. From this aspect, we can infer that λ will increase at higher power regime in data transmission. In case of high power transmission, it is beyond hope to disturb the eavesdropper without significant deterioration of the authorized user rate. In turn, the cooperative jammer would focus on raising $I_{\mathrm{a}}(\mathbf{J})$ as the transmitter expenses more power.

IV. Numerical Results

In this section, we evaluate the performance of the proposed cooperative pilot jamming strategy for a MIMO wiretap channel. The channels $\mathbf{H}_{\mathrm{a}}$, $\mathbf{G}_{\mathrm{a}}$, $\mathbf{H}_{\mathrm{e}}$, and $\mathbf{G}_{\mathrm{e}}$ are generated from the i.i.d. circularly symmetric complex Gaussian distribution with zero-mean and unit variance. The pilot signal power is given 3dB higher than the data signal power, where the data transmission power of legitimate transmitter varies from -5 dB to 30 dB, and the jamming power constraint on the cooperative jammer is set to 5 dB. The frame consists of 21 slots.

To offer an appropriate comparison, a cooperative jammer with persistent artificial noise transmission is investigated as a reference curve. Where the persistent jamming covers the pilot phase undiscriminatingly, pilot tone jamming is attained in identical fashion to data phase jamming. Jamming power is allocated uniformly over 21 slots and thus the jamming power affects on single slot is limited up to $P_J/21$. In a spatially selective manner, a proper beamformer is deployed to maximize the achievable secrecy rate. To make it clear, in this case, the cooperative jammer keeps transmitting artificial noise in both pilot transmission phase and data transmission phase, maintaining the same beamforming matrix and jamming power. The persistent artificial noise-aided jamming filtered by a beamforming matrix $\mathbf{W}\in\mathbb{C}^{N_T}$ comes up with the achievable secrecy rate (9), where γ_p is SNR of pilot symbols. Coping with the non-concavity of (9), the optimal beamforming matrix is found from a DC algorithm with a relaxation which is

$$R_{\text{sec}}(\mathbf{W}) = \left[\log \left| \mathbf{I} + \frac{\gamma}{N_T} \left(\mathbf{H}_{\text{a}} \mathbf{H}_{\text{a}}^H + \frac{N_T}{\gamma_p} \mathbf{G}_{\text{a}} \mathbf{W} \mathbf{W}^H \mathbf{G}_{\text{a}}^H + \frac{N_T}{\gamma_p} \mathbf{I} \right) \left(\left(1 + \frac{\gamma}{\gamma_p} \right) \left(\mathbf{I} + \mathbf{G}_{\text{a}} \mathbf{W} \mathbf{W}^H \mathbf{G}_{\text{a}}^H \right) \right)^{-1} \right| \right.$$
$$\left. - \log \left| \mathbf{I} + \frac{\gamma}{N_T} \left(\mathbf{H}_{\text{e}} \mathbf{H}_{\text{e}}^H + \frac{N_T}{\gamma_p} \mathbf{G}_{\text{e}} \mathbf{W} \mathbf{W}^H \mathbf{G}_{\text{e}}^H + \frac{N_T}{\gamma_p} \mathbf{I} \right) \left(\left(1 + \frac{\gamma}{\gamma_p} \right) \left(\mathbf{I} + \mathbf{G}_{\text{e}} \mathbf{W} \mathbf{W}^H \mathbf{G}_{\text{e}}^H \right) \right)^{-1} \right| \right]^+ \quad (9)$$

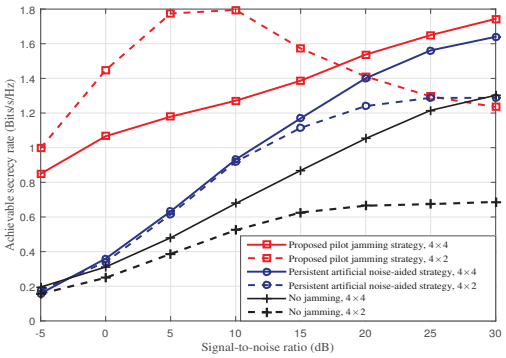

Fig. 2. Achievable secrecy rate comparison between the proposed cooperative pilot jamming strategy and the persistent artificial noise-aided strategy ($(N_T, N_R) = \{(4,4),(4,2)\}$, $P_J = 5$ dB, and 3 dB pilot power offset).

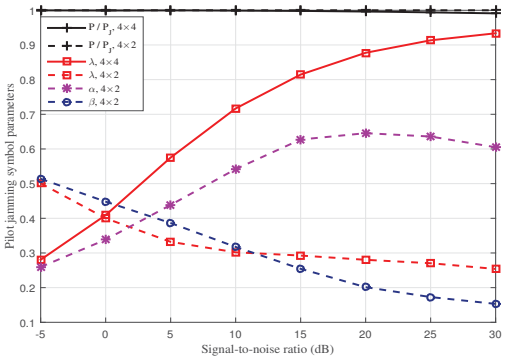

Fig. 3. Mediation parameters of pilot jamming symbols and jamming power usage ($(N_T, N_R) = \{(4,4),(4,2)\}$, $P_J = 5$ dB, and 3 dB pilot power offset).

accomplished by first-order Taylor expansion.

In Fig. 2, we present the achievable secrecy rate of the proposed pilot jamming strategy with respect to the data transmission power, when $(N_T, N_R) = (4,4)$ and $(N_T, N_R) = (4,2)$, respectively. We compare the proposed strategy with the persistent artificial noise-aided strategy which is stated above. Subject to the jamming power constraint, it is shown that the proposed strategy outperforms the persistent artificial noise-aided strategy in wide region, especially in low SNR regime. In particular, for SNR = 0 dB in case of 4×2, we attain 426% secrecy rate gain compared to the persistent jamming strategy. Furthermore, we observe the drastic increase of the achievable secrecy rate in 4×2 case. This is because, the rank deficiency of the channel matrix $\mathbf{G}_{\text{a}}$ provides an extra opportunity to utilize channel spaces more efficiently. Meanwhile, in the regime of high SNR, since the increase of the pilot signal power mitigates the channel estimation error, it is observed that the persistent jamming strategy can be more preferred than the proposed pilot jamming strategy especially for rank-deficient environment, e.g., in 4×2 case.

The mediation factors and jamming power usage over SNR of the data signal are illustrated in Fig. 3. Probing the behavior of λ, which implies the weighting on $\mathbf{J}^{(\text{PA,a})}$ that amplifies pilot at the authorized receiver, we observe the contradictory aspects between 4×4 and 4×2 cases. While the cooperative jammer in 4×4 system more concentrates on $\mathbf{J}^{(\text{PA,a})}$ at the higher SNR regime as we expected in Section III, the cooperative jammer expenses more jamming power to the pilot nulling at the eavesdropper as the SNR gets higher in 4×2 case. This difference comes with the existence of $\text{span}^{\perp}(\mathbf{G}_{\text{a}}^H)$. From the plot of β according to 4×2 system, we notice that the cooperative jammer attempts to deliver the eavesdropper pilot nulling signal more undetectable to the authorized receiver, when the data transmission power is high. Therefore, we conclude that the direct link between the cooperative jammer and the eavesdropper is the mostly intended channel to deliver the jamming signal. In the same vein, we can take an account of the power usage falloff at high data transmission power regime. To remark that the excessive pilot amplifying rather bothers the legitimate communication, we attempt to deliver the optimal pilot amplification to the authorized receiver. However, the impact of the channel estimation error is intensified as the transmitter expenses more power and therefore, the authorized receiver requires less pilot amplification as the data transmission power increases. In this sense, the correlation between $\mathbf{J}^{(\text{PA,a})}$ and $\mathbf{J}^{(\text{PN,e})}$ is critical to $I_{\text{a}}(\mathbf{J})$. Especially in 4×4 case, as we mentioned previously, we cannot avoid the significant noise enhancement at the authorized receiver which is entailed by $\mathbf{J}^{(\text{PN,e})}$. Thus, with sufficient degradation of the eavesdropper overhearing, there is no need to exploit extra jamming power. In consequence, the jamming power usage is reduced in the high SNR regime.

V. Conclusion

This paper reveals an opportunity of information-theoretic security improvement which come with an imperfect channel estimation, dealing with an energy-limited cooperative jammer. In the light of energy efficiency, we have tackled the scenario with the cooperative jammer which introduces pilot jamming signals periodically. In this regard, we have designed pilot jamming symbols which manipulate the channel estimations at the authorized receiver and at the eavesdropper. Due to the difficulty of the direct design of the optimal pilot jamming symbol, we have hence introduced the parametric form of

the pilot jamming symbol and reformulated the problem into the optimal parameter searching problem. For an appropriate comparison, the artificial noise-aided persistent cooperative jamming scheme was revised to involve the impact of channel estimation error. As shown via simulations, the proposed strategy achieves substantial secrecy rate gain, especially at the low data transmission power regime. Moreover, an additional secrecy rate gain was highly exhibited at the rank-deficient environment.

ACKNOWLEDGEMENT

This work has been supported by the National GNSS Research Center program of Defense Acquisition Program Administration of Agency for Defense Development.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, Vol. 28, No. 4, pp. 656-715, Oct. 1949.

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

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[4] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Tech.*, vol. 61, pp. 2599-2612, Jul. 2012.

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

[6] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, pp.2735-2751, Jun. 2008.

[7] E. A. Jorswieck, "Secrecy capacity of single- and multi-antenna channels with simple helpers," in *Proc. IEEE SCC*, Miami, FL, USA, Jan. 2010.

[8] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 152-157, Jan. 1983.

[9] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704-2717, May 2013.

[10] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903-907, Mar. 2012.

[11] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134-144, Jan. 2013.

[12] K. Lee, C. B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Tech.*, vol. 62, no. 9, pp. 4672-4678, Nov. 2013.

[13] H. Kim, J. Kang, S. Jeong, K. E. Lee, and J. Kang, "Secure beamforming and self-energy recycling with full-duplex wireless-powered relay," in *Proc. IEEE CCNC*, Las Vegas, NV, USA, Jan. 2016.

[14] S. Jeong, K. Lee, J. Kang, Y. Baek, and B. Koo, "Cooperative jammer design in cellular network with internal eavesdroppers," in *Proc. IEEE MILCOM*, Orlando, FL, USA, Oct. 2012.

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

[16] T. -Y. Liu, S. -C. Lin, T. -H. Chang, and Y. -W. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in *Proc. IEEE ICC*, Ottawa, ON, Canada, Jun. 2012.