On Countermeasures of Pilot Spoofing Attack in Massive MIMO Systems: A Double Channel Training Based Approach

Wei Wang, Nan Cheng, *Member, IEEE*, Kah Chan Teh, *Senior Member, IEEE*, Xiaodong Lin, *Fellow, IEEE*, Weihua Zhuang, *Fellow, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—In this paper, we investigate secure communication in a massive multiple-input multiple-output (MIMO) system with multiple users and multiple eavesdroppers (Eve) under both pilot spoofing attack (PSA) and uplink jamming. Specifically, Eve impairs the normal channel estimation by sending identical pilot sequences with the legitimate users. Based on the impaired channel estimation, the base station adopts linear processing schemes for uplink data reception, which is jammed by Eve, and downlink confidential information transmission. We first evaluate the impact of the PSA on the achievable rate with linear processing, and then propose a double channel training based scheme to combat PSA. By using the channel estimation difference in two training phases, the presence of the PSA can be detected and accurate legitimate channel estimation can be obtained by removing the effect of Eve's channel. Furthermore, we analyze the channel estimation errors and derive a closed-form expression of the minimum mean square error precoding scheme to maximize the minimum achievable secrecy rate, which outperforms the conventional linear precoding counterparts.**

***Index Terms*—Massive MIMO, pilot spoofing attack, double channel training, downlink precoding, secrecy rate.**

I. Introduction

BY EXPLOITING the large spatial degrees of freedom (DoF), massive multiple-input multiple-output (MIMO) can provide improved spectral and energy efficiency, and has been regarded as a promising solution for future wireless communication systems [1], [2]. It has been reported that 64-antenna base stations (BSs) have been commercially deployed in LTE-Advanced networks [3]. Particularly, channel vectors of different users become asymptotically orthogonal by expanding the size of the antenna array, which greatly facilitates the intra-cell interference management. More importantly, near-optimal performance can be achieved through linear precoding and detection. Thus, plenty of research has been conducted to investigate various problems in massive MIMO systems over the past years [4]–[9].

On the other hand, wireless communications are vulnerable to external eavesdropping and jamming due to the open nature of wireless medium. Therefore, providing security is of paramount importance for wireless communication systems [10]–[13]. By utilizing the intrinsic characteristics of wireless channels, physical layer security can achieve secure transmission without using upper layer cryptographic protocols and avoid complicated secret key generation and management [14]. Hence, physical layer security provides essential advantages in future large-scale and heterogeneous networks, such as the space-air-ground integrated networks, and has received intensive research attention recently [15]–[20].

With a large antenna array at BSs, information transmission can be focused in the direction where the users are located with a sharp beam, and information leakage to unknown eavesdroppers (Eves) can be significantly reduced; thus massive MIMO can effectively boost physical layer security [11], [21]. Due to the increased antenna gain and reduced inter-user interference, the secrecy capacity can be increased by adding more antennas [11]. Considering inter-cell interference in multi-cell systems, positive ergodic secrecy rate is achievable with proper artificial noise (AN) injection, and the achievable secrecy rate with random AN transmission is shown to be close to that of the conventional null-space based AN transmission [21].

To fully exploit benefits of massive MIMO, accurate channel state information (CSI) is a prerequisite. Inaccurate CSI based precoding not only introduces more inter-user interference, but also incurs more information leakage to the Eves. In time-division-duplex (TDD) massive MIMO systems, the downlink CSI is acquired through reverse channel training. In this case, smart Eves may jam such channel training process to manipulate the channel estimation, such that the achievable secrecy performance is severely deteriorated. Specifically, a smart Eve may send an identical training sequence with the legitimate user, resulting in an contaminated channel estimation at the BS [22]. Moreover, the Eve can flexibly change the transmission power to control the eavesdropping rate. Such an attack is usually termed

Manuscript received January 27, 2019; revised April 24, 2019; accepted May 6, 2019. Date of publication May 10, 2019; date of current version July 16, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 91638204 and in part by the Natural Sciences and Engineering Research Council of Canada. The review of this paper was coordinated by Dr. A.-C. Pang. *(Corresponding author: Nan Cheng.)*

W. Wang, N. Cheng, W. Zhuang, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L3G1, Canada (e-mail: wei.wang1@uwaterloo.ca; n5cheng@uwaterloo.ca; wzhuang@uwaterloo.ca; sshen@uwaterloo.ca).

K. C. Teh is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: ekcteh@ntu.edu.sg).

X. Lin is with the School of Computer Science, University of Guelph, Guelph, ON N1G 2W1, Canada (e-mail: xlin08@uoguelph.ca).

Digital Object Identifier 10.1109/TVT.2019.2916209

as pilot spoofing attack (PSA) [23] or pilot contamination attack [24], [25], and has been investigated in single-cell system [26]–[31], multi-cell system [24], [25], and cell-free system [32], respectively. It is proved that the secure DoF reduces to zero under PSA [26], and the achievable secrecy rate does not monotonically increase with the signal-to-noise ratio (SNR) [24].

To combat PSA, effective attack detection and channel estimation are crucial. An energy ratio based detector is proposed in [23], and PSA can be detected by comparing the received signal power between Alice and Bob. PSA can also be detected with the minimum description length (MDL) criterion [27] and the source enumeration approach [28]. Legitimate channel and Eve channel estimation and secure beamforming are discussed in [28] by using the temporal subspace property of the pilot signal. A jamming resistant receiver scheme is proposed for an uplink massive MIMO system in [29], where the jamming channel is estimated by exploiting the unused pilot sequence. To combat PSA and jamming attack, a random training scheme is proposed in [30], where each legitimate user is allocated with multiple pilot sequences (PSs) and the user randomly selects one PS each time to confuse the Eves. The transmitted PS of the legitimate user can be identified based on the channel observations. However, most of the aforementioned works are suitable only for single user and single Eve cases, since the energy ratio detector [23] and the random training sequences [27], [28] cannot deal with the inter-user interference in a multi-user case. Moreover, multiple training sequences are required for each user in the random training scheme [30], which greatly limits the applications in practice. The PSA in the presence of multiple collaboratively Eves is discussed from the perspective of Eves in [31], and thus the schemes cannot be directly applied for PSA detection and channel estimation at the BS.

In this paper, we consider both PSA and uplink jamming in a general but challenging scenario with multiple users and multiple Eves, which can be regarded as an extension of [28] and [30]. We first evaluate the effect of PSA on the uplink and downlink achievable rates, and then propose a double channel training based scheme to detect the presence of PSA and to estimate the legitimate channels by cancelling out the components of the eavesdropping channels. Based on the estimated channels, a minimum mean square error (MMSE) based precoding scheme is proposed to maximize the minimum achievable downlink secrecy rate. The contributions of this paper are summarized as follows:

- We derive the lower bounds of the downlink achievable secrecy rate and uplink achievable rate with linear processing under both PSA and uplink jamming, and obtain the sufficient condition for achieving a positive secrecy rate. The power allocation between PSA and uplink jamming is also analyzed from the perspective of Eve;
- We propose a double channel training based scheme to combat PSA. Based on the difference of the channel estimations in two training phases, the presence of PSA can be detected and the eigenspace of the eavesdropping channel can be estimated. Then, an eigenvalue decomposition (EVD) based channel estimation scheme is adopted to estimate the legitimate channel by removing the contamination of the eavesdropping links. It shows that the downlink achievable secrecy rate can be improved significantly for both matched filter (MF) and zero-forcing (ZF) precoding schemes based on the obtained channel estimations;
- We analyze the channel estimation errors arising from both limited samples and limited number of antennas, and derive a closed-form expression of the MMSE precoding for minimum achievable downlink secrecy rate maximation, which outperforms the MF and ZF precoding schemes.

The remainder of this paper is organized as follows. We describe the system model in Section II. The achievable uplink and downlink rates with linear precoding and the power allocation of Eves are analyzed in Sections III. The double channel training based scheme, PSA detection, and EVD based channel estimation are presented in Section IV, and the MMSE precoding design for downlink secrecy rate maximization is given in Section V. Lastly, we demonstrate the simulation results in Section VI and draw the conclusion of this study in Section VII.

II. System Model

Consider downlink secure communications in a single-cell massive MIMO system, where the N-antenna BS intends to transmit confidential information to multiple single-antenna users. Each user is assumed to be eavesdropped by a single Eve, and each Eve can launch PSA and intentional jamming in the uplink training and data transmission phases, respectively. All the channels experience large-scale path loss as well as small-scale fading. Specifically, for the kth user, the channel to the BS is denoted by $\sqrt{\beta_{u_k}}\mathbf{h}_k$, where β_{u_k} and $\mathbf{h}_k \in \mathbb{C}^{1\times N}$ denote the path loss and small-scale Rayleigh fading with $\mathbf{h}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$, respectively. Similar definition applies to the lth Eve with channel $\sqrt{\beta_{e_l}}\mathbf{g}_l$ and $\mathbf{g}_l \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$.

Remark 1: Each user may be eavesdropped by all the Eves, and each Eve may launch PSA by combining all the training sequences in the uplink training phase. Note that when each Eve combines all the training sequences for PSA, the effect of PSA on the channel estimation of a certain user is similar to the case with a single virtual Eve. To facilitate the subsequent theoretical analysis, we consider only the case that each user is eavesdropped by a single Eve.

A. Uplink Channel Training

Consider the uplink pilot-based channel training for downlink CSI acquisition in TDD massive MIMO systems, after perfect synchronization between the BS and UEs. Each Eve is synchronized with the BS to launch PSA. The K users use orthogonal pilot sequences for channel training, and such sequences are known to Eves and thus each Eve sends identical PS with the legitimate user in the uplink training phase. The BS observes a combined baseband signal[1] given by

$$\mathbf{Y}_p = \sum_{k=1}^{K}\left(\sqrt{P_u\beta_{u_k}}\mathbf{h}_k^H\mathbf{s}_k + \sqrt{P_{e_k}\beta_{e_k}}\mathbf{g}_k^H\mathbf{s}_k\right) + \mathbf{N} \quad (1)$$

where P_u and P_{e_k} are the uplink transmission power levels of the legitimate user and Eve, respectively, and $\mathbf{s}_k$ is the PS of the

[1]Since the channel is independent over each coherent interval, we omit the time instant for simplicity.

kth user with length τ_p. Note that $\mathbf{s}_k\mathbf{s}_l^H = \delta_{kl}\tau_p$ with $\delta_{kl} = 1$ when $k = l$ and $\delta_{kl} = 0$ otherwise, and $\mathbf{N}$ is the additive white Gaussian noise (AWGN) at the BS following $\mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_N)$. By correlating $\mathbf{Y}_p$ with $\mathbf{s}_k$, we have

$$\mathbf{y}_k = \frac{\mathbf{s}_k\mathbf{Y}_p^H}{\tau_p} = \sqrt{P_u\beta_{u_k}}\mathbf{h}_k + \sqrt{P_{e_k}\beta_{e_k}}\mathbf{g}_k + \mathbf{n}_k \quad (2)$$

where $\mathbf{n}_k \sim \mathcal{CN}(\mathbf{0}, \frac{\sigma^2}{\tau_p}\mathbf{I}_N)$. The MMSE estimation of the legitimate channel is given by [33]

$$\begin{aligned}\widehat{\mathbf{h}}_k &= \frac{\sqrt{P_u\beta_{u_k}}}{\Sigma}\mathbf{y}_k \\ &= \frac{P_u\beta_{u_k}}{\Sigma_k}\mathbf{h}_k + \frac{\sqrt{P_uP_{e_k}\beta_{u_k}\beta_{e_k}}}{\Sigma_k}\mathbf{g}_k + \frac{\sqrt{P_u\beta_{u_k}}}{\Sigma_k}\mathbf{n}_k\end{aligned} \quad (3)$$

where $\Sigma_k = P_u\beta_{u_k} + P_{e_k}\beta_{e_k} + \frac{\sigma^2}{\tau_p}$. The channel error can be expressed as

$$\widetilde{\mathbf{h}}_k = \mathbf{h}_k - \widehat{\mathbf{h}}_k \sim \mathcal{CN}\left(\mathbf{0}, (1-\eta_{u_k})\mathbf{I}_N\right) \quad (4)$$

where $\eta_{u_k} = \frac{P_u\beta_{u_k}}{\Sigma_k}$.

B. Uplink Data Transmission

During the uplink data transmission phase, users transmit payload data to the BS and Eves transmit jamming signal to degrade the reception at the BS. The received signal at the BS is given by

$$\mathbf{y}_u = \sum_{k=1}^{K}\left(\sqrt{p_k\beta_{u_k}}\mathbf{h}_k u_k + \sqrt{q_k\beta_{e_k}}\mathbf{g}_k a_k\right) + \mathbf{n}_u \quad (5)$$

where p_k and q_k denote the uplink transmission power levels of the kth user and the kth Eve, respectively, with u_k and a_k being the corresponding transmitted signals. $\mathbf{n}_u \sim (\mathbf{0}, \sigma^2\mathbf{I}_N)$ is the AWGN.

C. Downlink Data Transmission

In the downlink transmission phase, the BS delivers data to the users using the precoding vector based on the estimated channels, which is eavesdropped by the corresponding Eve. To enhance the secrecy rate, AN is injected [34]. Thus, the transmitted signal is given by

$$\mathbf{x} = \mathbf{WPm} + \sqrt{\phi_0 P}\mathbf{V}\mathbf{n}_a \quad (6)$$

where $\mathbf{P} = \text{diag}[\phi_1 P, \ldots, \phi_K P]$, $\mathbf{W} = [\mathbf{w}_1, \ldots, \mathbf{w}_K]$, and $\mathbf{m} = [m_1, \ldots, m_K]^H$, with ϕ_k, $\mathbf{w}_k \in \mathbb{C}^{N\times 1}$, and m_k being the power allocation, beamforming vector, and intended message to the kth user. In addition, P is the downlink transmission power, ϕ_0 is the power allocated to AN, $\mathbf{V}$ is the weighting matrix for AN which is usually orthogonal with $\widehat{\mathbf{H}}$ where $\widehat{\mathbf{H}} = [\widehat{\mathbf{h}}_1^H, \ldots, \widehat{\mathbf{h}}_K^H]^H \in \mathbb{C}^{K\times N}$, and $\mathbf{n}_a \sim \mathcal{CN}(\mathbf{0}, \frac{1}{N-K}\mathbf{I}_{N-K})$ is the transmitted AN signal. The received signal at the kth user is

$$\begin{aligned}y_k = &\sqrt{\phi_k P\beta_{u_k}}\mathbf{h}_k\mathbf{w}_k m_k + \sum_{l\neq k}^{K}\sqrt{\phi_l P\beta_{u_l}}\mathbf{h}_k\mathbf{w}_l m_l \\ &+ \sqrt{\phi_0 P}\mathbf{h}_k\mathbf{V}\mathbf{n}_a + n_k\end{aligned} \quad (7)$$

where $n_k \sim \mathcal{CN}(0, \sigma^2)$. Similarly, the received signal at the kth Eve is

$$\begin{aligned}y_{e_k} = &\sqrt{\phi_k P\beta_{e_k}}\mathbf{g}_k\mathbf{w}_k m_k + \sum_{l\neq k}^{K}\sqrt{\phi_l P\beta_{e_l}}\mathbf{g}_k\mathbf{w}_l m_l \\ &+ \sqrt{\phi_0 P}\mathbf{g}_k\mathbf{V}\mathbf{n}_a + n_{e_k}\end{aligned} \quad (8)$$

where $n_{e_k} \sim \mathcal{CN}(0, \sigma^2)$.

III. Achievable Secrecy Rate With Linear Processing

The BS adopts linear processing for both uplink reception and downlink transmission, with MF and ZF precoding/detection schemes given by $\mathbf{W}^{\text{MF}} = \widehat{\mathbf{H}}^H / \left\|\widehat{\mathbf{H}}^H\right\|$ and $\mathbf{W}^{\text{ZF}} = \widehat{\mathbf{H}}^H(\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H)^{-1}$, respectively. In this section, we first analyze the uplink and downlink achievable rate under both PSA and uplink jamming, respectively. Then, the optimal power allocation of Eve for PSA and uplink jamming is discussed.

A. Downlink Achievable Secrecy Rate

In the absence of downlink channel training, statistical CSI is used by each user for signal detection [33], [35]. The achievable rate of the kth user is lower bounded by [33]

$$R_k = \frac{\tau_{dl}}{\tau_c}\log_2(1 + \text{SINR}_k) \quad (9)$$

where τ_c is the coherent interval, τ_{dl} is the allocated downlink data transmission time, and the effective signal-to-interference-plus-noise ratio (SINR) is given by (10), shown at the bottom of this page. Similarly, the eavesdropping rate of the kth Eve is lower bounded by

$$R_{e_k} = \frac{\tau_{dl}}{\tau_c}\log_2(1 + \text{SINR}_{e_k}) \quad (11)$$

where SINR_{e_k} is given by (12), shown at the bottom of the page. Then, the achievable secrecy rate defined as the difference

$$\text{SINR}_k = \frac{\phi_k P\beta_{u_k}\left|\mathbb{E}[\mathbf{h}_k\mathbf{w}_k]\right|^2}{\phi_k P\beta_{u_k}\text{var}(\mathbf{h}_k\mathbf{w}_k) + \sum_{l\neq k}^{K}\phi_l P\beta_{u_k}\mathbb{E}[|\mathbf{h}_k\mathbf{w}_l|^2] + \frac{\phi_0 P}{N-K}\left\|\mathbf{h}_k\mathbf{V}\right\|^2 + 1} \quad (10)$$

$$\text{SINR}_{e_k} = \frac{\phi_k P\beta_{e_k}\left|\mathbb{E}[\mathbf{g}_k\mathbf{w}_k]\right|^2}{\phi_k P\beta_{e_k}\text{var}(\mathbf{g}_k\mathbf{w}_k) + \sum_{l\neq k}^{K}\phi_l P\beta_{e_k}\mathbb{E}[|\mathbf{g}_k\mathbf{w}_l|^2] + \frac{\phi_0 P}{N-K}\left\|\mathbf{g}_k\mathbf{V}\right\|^2 + 1} \quad (12)$$

between the rate of the legitimate user and that of the Eve can be derived as follows.

Theorem 1: The downlink achievable secrecy rate with MF precoding under PSA is approximated by

$$R_{sec,k}^{\mathrm{MF}} \approx \frac{\tau_{dl}}{\tau_c}\left[\log_2(1+\mathrm{SINR}_k^{\mathrm{MF}}) - \log_2(1+\mathrm{SINR}_{e_k}^{\mathrm{MF}})\right]^+ \tag{13}$$

where

$$\mathrm{SINR}_k^{\mathrm{MF}} = \frac{C_N^2\phi_k\eta_{u_k}}{\phi_k\zeta_{u_k} + \sum_{l\neq k}^{K}\phi_l + \phi_0 + \frac{\sigma^2}{\beta_{u_k}P}} \tag{14}$$

$$\mathrm{SINR}_{e_k}^{\mathrm{MF}} = \frac{C_N^2\phi_k\eta_{e_k}}{\phi_k\zeta_{e_k} + \sum_{l\neq k}^{K}\phi_l + \phi_0 + \frac{\sigma^2}{\beta_{e_k}P}}. \tag{15}$$

Note that $[x]^+ = \max(x,0)$, and we use $\zeta_{u_k} = V_n\eta_{u_k} + (1-\eta_{u_k}), \zeta_{e_k} = V_n\eta_{e_k} + (1-\eta_{e_k}), \eta_{e_k} = \frac{P_{e_k}\beta_{e_k}}{\Sigma_k}, V_n = N - C_N^2$, $C_N = \frac{\Gamma(N+\frac{1}{2})}{\Gamma(N)}$.

Please see Appendix A for proof.

Based on Theorem 1, the sufficient condition to achieve a positive secrecy rate under PSA can be obtained, which is given by the following corollary.

Corollary 1: For the kth user, a positive secrecy rate is achievable when $\eta_{u_k} \geq \eta_{e_k}$.

The proof is omitted here.

Corollary 1 indicates that, as long as the effective training power (i.e., the product of transmission power and the path loss) of the legitimate user is larger than that of the Eve, the legitimate channel capacity is larger than that of the eavesdropping channel, since the beamforming vector will be closer to the user's channel. Following the same procedure, we can derive the achievable secrecy rate without PSA.

Proposition 1: In absence of PSA, the downlink achievable secrecy rate with MF precoding is approximated by

$$\bar{R}_{sec,k} \approx \frac{\tau_{dl}}{\tau_c}\left[\log_2\left(1+\overline{\mathrm{SINR}}_k^{\mathrm{MF}}\right) - \log_2\left(1+\overline{\mathrm{SINR}}_{e_k}^{\mathrm{MF}}\right)\right]^+ \tag{16}$$

where

$$\overline{\mathrm{SINR}}_k^{\mathrm{MF}} = \frac{C_N^2\phi_k\bar{\eta}_{u_k}}{\phi_k\bar{\zeta}_{u_k} + \sum_{l\neq k}^{K}\phi_l + \phi_0 + \frac{\sigma^2}{\beta_{u_k}P}} \tag{17}$$

$$\overline{\mathrm{SINR}}_{e_k}^{\mathrm{MF}} = \frac{\phi_k}{\phi_k V_n + \sum_{l\neq k}^{K}\phi_l + \phi_0 + \frac{\sigma^2}{\beta_{e_k}P}}. \tag{18}$$

Note that $\bar{\zeta}_{u_k} = V_n\bar{\eta}_{u_k} + (1-\bar{\eta}_{u_k})$ and $\bar{\eta}_{u_k} = \frac{P_u\beta_{u_k}}{P_u\beta_{u_k}+\frac{\sigma^2}{\tau_p}}$.

Based on Theorem 1 and Proposition 1, we can derive the achievable secrecy rate loss, which is given by the following corollary.

Corollary 2: When $N\to\infty$ and $N \gg K$, the downlink achievable secrecy rate loss due to PSA is approximated by

$$R_{\mathrm{loss},k}^{\mathrm{DL,MF}} \approx \frac{\tau_{dl}}{\tau_c}\log_2\left(\frac{C_N^2\phi_k\eta_{e_k}}{\eta_{u_k}\sum_{l=0}^{K}\phi_l}\right). \tag{19}$$

Proof: When N approaches infinity and PSA is absent, the SINR of the legitimate user is much larger than that of Eve and the secrecy rate approaches to the main channel capacity, which reveals the inherent anti-eavesdropping capability of massive MIMO [11]. However, both capacities of legitimate user and Eve increase with N without PSA. Hence, the secrecy rate loss can be approximated by

$$\begin{aligned}\bar{R}_{s,k} - R_{s,k} &\approx \frac{\tau_{dl}}{\tau_c}\left[\log_2\left(\overline{\mathrm{SINR}}_k^{\mathrm{MF}}\right) - \log_2\left(\frac{\mathrm{SINR}_k^{\mathrm{MF}}}{\mathrm{SINR}_{e_k}^{\mathrm{MF}}}\right)\right] \\ &= \frac{\tau_{dl}}{\tau_c}\log_2\left(\frac{\overline{\mathrm{SINR}}_k^{\mathrm{MF}}\mathrm{SINR}_{e_k}^{\mathrm{MF}}}{\mathrm{SINR}_k^{\mathrm{MF}}}\right) \\ &\approx \frac{\tau_{dl}}{\tau_c}\log_2\left(\frac{C_N^2\phi_k\eta_{e_k}}{\eta_{u_k}(\sum_{l\neq k}^{K}\phi_l + V_n\phi_k)}\right).\end{aligned} \tag{20}$$

This completes the proof. ■

Similar to the MF scheme, for ZF precoding, the achievable secrecy rate can be obtained, which is given by the following theorem.

Theorem 2: The downlink achievable secrecy rate with ZF precoding in the presence of PSA is approximated by

$$R_{sec,k}^{\mathrm{ZF}} \approx \frac{\tau_{dl}}{\tau_c}\left[\log_2(1+\mathrm{SINR}_k^{\mathrm{ZF}}) - \log_2(1+\mathrm{SINR}_{e_k}^{\mathrm{ZF}})\right]^+ \tag{21}$$

where

$$\mathrm{SINR}_k^{\mathrm{ZF}} = \frac{C_{N-K+1}^2\phi_k\eta_{u_k}}{\phi_k\zeta_{u_k} + \sum_{l\neq k}^{K}\phi_l(1-\eta_{u_k}) + \phi_0 + \frac{\sigma^2}{\beta_{u_k}P}} \tag{22}$$

$$\mathrm{SINR}_{e_k}^{\mathrm{ZF}} = \frac{C_{N-K+1}^2\phi_k\eta_{e_k}}{\phi_k\zeta_{e_k} + \sum_{l\neq k}^{K}\phi_l(1-\eta_{e_k}) + \phi_0 + \frac{\sigma^2}{\beta_{e_k}P}}. \tag{23}$$

The proof is similar to Appendix A and is omitted here for brevity.

B. Uplink Achievable Rate

Similar to the downlink beamforming, the BS uses linear MF or ZF detection for the uplink received signal based on the estimated channels. The uplink achievable rate of the kth user is lower bounded by

$$R_{ul,k}^{\mathrm{s}} = \frac{\tau_{ul}}{\tau_c}\log_2(1+\mathrm{SINR}_{ul,k}^{\mathrm{s}}), \mathrm{s}\in\{\mathrm{MF},\mathrm{ZF}\} \tag{24}$$

where $\mathrm{SINR}_{ul,k}^{\mathrm{s}}$ is given by (25) and (26), shown at the bottom of the next page, for MF and ZF detection, respectively, τ_{ul} is the time allocated for uplink data transmission.

When N approaches infinity, we can observe from (25) and (26) that the interference from Eve who launches the PSA approaches infinity, which makes the SINR saturate to a constant

given by

$$\mathrm{SINR}_{ul,k}^{\mathrm{s}} \to \frac{p_k \beta_{u_k} \eta_{u_k}}{q_k \beta_{e_k} \eta_{e_k}}. \tag{27}$$

We can conclude from (27) that the MF and ZF detection can achieve the same performance in the presence of PSA and uplink jamming. For the MF detection scheme, from (25) we can obtain that, when the uplink jamming is absent, i.e. $q_k = 0$, the achievable SINR approaches to

$$\overline{\mathrm{SINR}}_{ul,k}^{\mathrm{MF}} \approx \frac{C_N^2 p_k \beta_{u_k} \eta_{u_k}}{p_k \beta_{u_k} \zeta_{u_k} + \sum_{l \neq k} p_l \beta_{u_l}}. \tag{28}$$

Hence, the achievable rate loss caused by the uplink jamming can be approximated by

$$R_{\mathrm{loss},k}^{\mathrm{UL,MF}} \approx \frac{\tau_{ul}}{\tau_c} \log_2 \left(\frac{C_N^2 q_k \beta_{e_k} \eta_{e_k}}{p_k \beta_{u_k} \zeta_{u_k} + \sum_{l \neq k} p_l \beta_{u_l}} \right). \tag{29}$$

We observe that both the uplink capacity and downlink capacity can be severely degraded by the PSA due to the inaccurate channel estimation. Thus, effective PSA detection and channel estimation are required to improve the secrecy rate, as discussed in the next section.

C. Power Allocation of Eves

Considering that each Eve can launch both PSA and uplink jamming, from the perspective of Eve, the power allocated for PSA and jamming signal needs to be optimized to maximize the weighted sum rate loss of a legitimate user in both uplink and downlink. Note that maximizing the rate loss is equivalent to minimize the achievable secrecy rate in the downlink and minimize the achievable rate in the uplink. The problem can be formulated as

$$\begin{aligned} \mathrm{P1}: \quad & \max_{P_{e_k}, q_k} \quad w_k R_{\mathrm{loss},k}^{\mathrm{DL,MF}} + v_k R_{\mathrm{loss},k}^{\mathrm{UL,MF}} \\ & \text{s.t.} \quad \mathrm{SINR}_{ul,k}^{\mathrm{MF}} \geq \Gamma_k \\ & \qquad \tau_p P_{e_k} + \tau_{ul} q_k \leq E_k \end{aligned} \tag{30}$$

where w_k and v_k are the weighting factors for the kth user, Γ_k is the uplink SINR threshold, E_k is the power constraint of each Eve. Note that the uplink SINR constraint in P1 is used to hide the presence of PSA. When the uplink SINR is too low, the BS may infer the presence of the PSA and may take countermeasure approaches to make it ineffective. Accordingly, we obtain the following lemma.

Lemma 1: At the optimal point, at least one of the constraints in P1 holds with equality.

Proof: From (19) and (29), we observe that the objective function is a monotonically increasing function of P_{e_k} and q_k. Following that, we can prove Lemma 1 by contradiction [36].■

To facilitate the analysis, we substitute the uplink SINR by its asymptotic form in (27). Then, the SINR constraint can be transformed to

$$\frac{p_k \beta_{u_k} \eta_{u_k}}{q_k \beta_{e_k} \eta_{e_k}} \geq \Gamma_k. \tag{31}$$

For each fixed variable, it is straightforward to show that the constraints in P1 are convex. Hence, the optimal solution can be obtained through the alternate optimization algorithm [37].

Remark 2: Even thought the optimization in Subsection III-C is based on MF precoding, it is also applicable to ZF precoding.

IV. PSA Detection and Channel Estimation

In this section, we propose an uplink data aided double channel training scheme, which can accurately detect the presence of PSA and estimate the legitimate channels.

A. Double Channel Training Scheme

In addition to the normal training as discussed in Subsection II-A, another training process is conducted during the uplink training phase. Specifically, the kth user combines the normal training sequence with a random sequence as

$$\mathbf{s}_{b,k} = \xi_k (\sqrt{\alpha_k} \mathbf{s}_{n,k} \mathbf{P}_k^{\perp} + \sqrt{1-\alpha_k} \mathbf{s}_k e^{j\varphi_k}) \tag{32}$$

where $\mathbf{P}_k^{\perp} = \mathbf{I} - \bar{\mathbf{S}}_k^H (\bar{\mathbf{S}}_k \bar{\mathbf{S}}_k^H)^{-1} \bar{\mathbf{S}}_k$ denotes the nullspace of $\bar{\mathbf{S}}_k$, with $\bar{\mathbf{S}}_k = [\mathbf{s}_1, \ldots, \mathbf{s}_{k-1}, \mathbf{s}_{k+1}, \ldots, \mathbf{s}_{\tau_p}]^H$, $\mathbf{s}_{n,k}$ the random training sequence for the kth user in the second phase training, α_k the power allocation between the random training sequence and the normal training sequence, and ξ_k the power scaling factor.

We assume that Eve can also conduct random training with a training sequence given by

$$\mathbf{s}_{e,k} = \sqrt{\alpha_{e,k}} \tilde{\mathbf{s}}_{n,k} + \sqrt{(1-\alpha_{e,k})} \mathbf{s}_k \tag{33}$$

where $\alpha_{e,k}$ is the power allocation between the random training sequence and the normal training sequence for Eve. The received signal in the second training phase is given by

$$\tilde{\mathbf{Y}}_p = \sum_{k=1}^{K} \left(\sqrt{P_u \beta_{u_k}} \mathbf{h}_k^H \mathbf{s}_{b,k} + \sqrt{P_{e_k} \beta_{e_k}} \mathbf{g}_k^H \mathbf{s}_{e,k} \right) + \tilde{\mathbf{N}} \tag{34}$$

$$\mathrm{SINR}_{ul,k}^{\mathrm{MF}} = \frac{C_N^2 p_k \beta_{u_k} \eta_{u_k}}{p_k \beta_{u_k} \zeta_{u_k} + \sum_{l \neq k} (p_l \beta_{u_l} + q_l \beta_{e_l}) + q_k \beta_{e_k} (C_N^2 \eta_{e_k} + \zeta_{e_k}) + \sigma^2}, \tag{25}$$

$$\mathrm{SINR}_{ul,k}^{\mathrm{ZF}} = \frac{C_{N-K+1}^2 p_k \beta_{u_k} \eta_{u_k}}{p_k \beta_{u_k} \zeta_{u_k} + \sum_{l \neq k} (p_l \beta_{u_l} (1-\eta_{u_k}) + q_l \beta_{e_l} (1-\eta_{e_k})) + q_k \beta_{e_k} (C_{N-K+1}^2 \eta_{e_k} + \zeta_{e_k}) + \sigma^2}. \tag{26}$$

where $\tilde{\mathbf{N}}$ is the AWGN with each element following $\mathcal{CN}(0,\sigma^2)$. By correlating $\tilde{\mathbf{Y}}_p$ with $\mathbf{s}_k$, we have

$$\begin{aligned}\tilde{\mathbf{y}}_k &= \mathbf{s}_k\tilde{\mathbf{Y}}_p^H \\ &= \sqrt{P_u\beta_{u_k}}\mathbf{h}_k\mathbf{s}_k\mathbf{s}_{b,k}^H + \sqrt{(1-\alpha_e)P_e\beta_{e_k}}\mathbf{g}_k\mathbf{s}_k\mathbf{s}_k^H \\ &\quad + \sum_{i=1}^{K}\sqrt{\alpha_eP_e\beta_{e_i}}\mathbf{g}_i\mathbf{s}_k\tilde{\mathbf{s}}_{n,i}^H + \tilde{\mathbf{n}}_k\end{aligned} \tag{35}$$

where $\tilde{\mathbf{n}}_k \sim \mathcal{CN}(\mathbf{0},\sigma^2\tau_p\mathbf{I})$. Note that, with the random training sequence, the mutual orthogonal property among different sequences of Eves does not hold anymore and the estimated channel is contaminated by all the other eavesdropping channels. By using the least square (LS) estimation method, we can obtain

$$\begin{aligned}\hat{\mathbf{h}}_{2,k} &= \frac{\tilde{\mathbf{y}}_k}{\sqrt{P_u\beta_{u_k}}\mathbf{s}_k\mathbf{s}_{b,k}^H} \\ &= \mathbf{h}_k + \frac{\sqrt{(1-\alpha_{e,k})P_{e_k}\beta_{e_k}}}{\sqrt{P_u\beta_{u_k}}}\frac{\mathbf{s}_k\mathbf{s}_{e,k}^H}{\mathbf{s}_k\mathbf{s}_{b,k}^H}\mathbf{g}_k \\ &\quad + \sum_{i=1}^{K}\frac{\sqrt{\alpha_{e,k}P_{e_k}\beta_{e_i}}\mathbf{s}_k\tilde{\mathbf{s}}_{n,i}^H}{\mathbf{s}_k\mathbf{s}_{b,k}^H}\mathbf{g}_i + \frac{\tilde{\mathbf{n}}_k}{\sqrt{P_u\beta_{u_k}}\mathbf{s}_k\mathbf{s}_{b,k}^H}.\end{aligned} \tag{36}$$

From (36), to estimate the channel, prior information about $\mathbf{s}_{b,k}$ or $\mathbf{s}_{b,k}^H\mathbf{s}_k$ at the BS is required. In practice, each user can adaptively change parameters such as α_k and φ_k to satisfy $\mathbf{s}_{b,k}^H\mathbf{s}_k = \bar{\alpha}\tau_p e^{j\omega_k}$, where $\bar{\alpha}$ and ω_k can be determined based on its large scale fading coefficient β_{u_k}, which is unknown to Eves. From (2), with the LS estimation method, we have

$$\hat{\mathbf{h}}_{1,k} = \frac{\mathbf{y}_k}{\sqrt{P_u\beta_{u_k}}} = \mathbf{h}_k + \frac{\sqrt{P_{e_k}\beta_{e_k}}}{\sqrt{P_u\beta_{u_k}}}\mathbf{g}_k + \frac{1}{\sqrt{P_u\beta_{u_k}}}\mathbf{n}_k. \tag{37}$$

Following that, we can obtain

$$\mathbf{z}_k = \hat{\mathbf{h}}_{1,k} - \hat{\mathbf{h}}_{2,k} = \mathbf{g}_E + \mathbf{n}_z \tag{38}$$

where

$$\mathbf{g}_E = \sqrt{\frac{P_e\beta_{e_k}}{P_u\beta_{u_k}}}\left(1 - \frac{\mathbf{s}_k\mathbf{s}_{e,k}^H}{\mathbf{s}_k\mathbf{s}_{b,k}^H}\right)\mathbf{g}_k - \sum_{i=1}^{K}\sqrt{\alpha_eP_e\beta_{e_i}}\frac{\mathbf{s}_k\tilde{\mathbf{s}}_{n,i}^H}{\mathbf{s}_k\mathbf{s}_{b,k}^H}\mathbf{g}_i \tag{39}$$

and $\mathbf{n}_z$ is the AWGN which follows $\mathcal{CN}(0,\sigma_N^2\mathbf{I})$ with $\sigma_N^2 = \frac{\sigma^2}{\tau_pP_u\beta_{u_k}}(1+\frac{1}{\bar{\alpha}^2})$. Note that the eavesdropping channel components exist only in the difference of estimated channels. Thus, the difference of channel estimations can be used to detect the presence of PSA, which is discussed in the next subsection.

B. PSA Detection

To detect the presence of PSA, we first define two hypotheses, H_0 and H_1, H_0- there is no active Eve conducting the PSA and H_1- the pilot training of each user will be attacked by an active Eve. The estimated channel difference for the kth user in the two training phases is

$$\begin{aligned}H_0 &: \mathbf{z}_k = \mathbf{n}_z \sim (0,\sigma_N^2\mathbf{I}) \\ H_1 &: \mathbf{z}_k = \mathbf{g}_E + \mathbf{n}_z \sim (\mathbf{g}_E,\sigma_N^2\mathbf{I}).\end{aligned} \tag{40}$$

Since $\mathbf{g}_E$ is unknown to the BS, we adopt a generalized logarithm likelihood test, given by

$$T(\mathbf{z}_k) = \ln\frac{\max\limits_{\mathbf{g}_E} f(\mathbf{z}_k \mid H_1,\mathbf{g}_E)}{f(\mathbf{z}_k \mid H_0)} = \frac{\|\mathbf{z}_k\|^2}{\sigma_N^2} \underset{H_0}{\overset{H_1}{\gtrless}} \bar{T} \tag{41}$$

where $\bar{T}$ is the test threshold determined by a predefined false alarm probability. Under hypothesis H_0, $\|\mathbf{z}_k\|^2$ follows a Gamma distribution with shape and scale parameters N and σ_N^2, respectively. Then, the false alarm probability can be calculated by

$$P_{fa} = \mathbb{P}(\|\mathbf{z}_k\|^2 > \sigma_N^2\bar{T} \mid H_0) = \Gamma(\bar{T},N). \tag{42}$$

For a given false alarm rate, ϵ, the threshold can be calculated by $\bar{T} = \Gamma^{-1}(\epsilon,N)$.

After the PSA is detected, we proceed to estimate legitimate channel and the eavesdropping channel to recover the secure transmission. In the next subsection, we adopt the EVD based channel estimation scheme to estimate the legitimate channel.

C. EVD Based Channel Estimation

The received signal in the uplink data transmission phase in (5) can be rewritten as

$$\mathbf{y}_u = \mathbf{u}\mathbf{D}_u^{1/2}\mathbf{H} + \mathbf{a}\mathbf{D}_e^{1/2}\mathbf{G} + \mathbf{n} \tag{43}$$

where $\mathbf{D}_u = \text{diag}\{p_1\beta_{u_1}, p_2\beta_{u_2},\ldots,p_K\beta_{u_K}\}$, and $\mathbf{D}_e = \text{diag}\{q_1\beta_{e_1}, q_2\beta_{e_2},\ldots,q_K\beta_{e_K}\}$, $\mathbf{u} = [u_1,\ldots,u_K]$. The covariance matrix of the received data signal can be calculated by

$$\mathbf{R}_\mathbf{y} = \mathbb{E}[\mathbf{y}_u^H\mathbf{y}_u] = \mathbf{H}^H\mathbf{D}_u\mathbf{H} + \mathbf{G}\mathbf{D}_e^H\mathbf{G} + \sigma^2\mathbf{I}_N. \tag{44}$$

When N approaches infinity, we have

$$\frac{\mathbf{h}_l\mathbf{h}_k^H}{N} = \delta_{lk}. \tag{45}$$

Following that, we can obtain

$$\mathbf{R}_\mathbf{y}\mathbf{H}^H = \mathbf{H}^H(N\mathbf{D}_u + \sigma^2\mathbf{I}_K) \tag{46}$$

and

$$\mathbf{R}_\mathbf{y}\mathbf{G}^H = \mathbf{G}^H(N\mathbf{D}_e + \sigma^2\mathbf{I}_K). \tag{47}$$

For a large N, the columns of $\mathbf{H}^H$ and $\mathbf{G}^H$ are pairwisely orthogonal, and $N\mathbf{D}_u + \sigma^2\mathbf{I}_K$ and $N\mathbf{D}_e + \sigma^2\mathbf{I}_K$ are diagonal matrices. As a result, the kth columns of $\mathbf{H}^H$ and $\mathbf{G}^H$ are the eigenvectors corresponding to the eigenvalues of $Np_k\beta_{u_k} + \sigma^2$ and $Nq_k\beta_{e_k} + \sigma^2$, respectively. Hence, both $\mathbf{H}$ and $\mathbf{G}$ can be estimated from the eigenvectors of $\mathbf{R}_\mathbf{y}$ [38].

However, since the transmission power for PSA and the distance to each Eve are unknown to the BS, it is difficult to match the eigenvalue with the corresponding eigenvector. On the other hand, when the effective transmission power of Eve is very close to that of the legitimate user, the EVD based channel estimation

has a large estimation error. Since each $\mathbf{z}_k$ only contains the Eves' channel information, we can estimate the eigenspace of the Eves' channel based on the EVD method. From (38), when PSA is present, we have

$$\mathbf{R}_{\mathbf{z}} = \sum_{k=1}^{K} \mathbb{E}[\mathbf{z}_k^H \mathbf{z}_k] \to \sum_{k=1}^{K}\sum_{i=1}^{K} c_{ki}^2 \mathbf{g}_i^H \mathbf{g}_i, \text{as } N \to \infty. \quad (48)$$

The eigenspace of the Eve channels can be estimated by the eigenvector corresponding to the K largest eigenvalues of $\mathbf{R}_{\mathbf{z}}$. Denote $\mathbf{U}_{\mathbf{g}}$ as the eigenspace of the Eve channels, by projecting the received uplink data signal into the null space of $\mathbf{U}_{\mathbf{g}}$ space,i.e., $\tilde{\mathbf{y}}_u^H = (\mathbf{I}_N - \mathbf{P}_{\mathbf{g}})\mathbf{y}_u^H$ with $\mathbf{P}_{\mathbf{g}} = \mathbf{U}_{\mathbf{g}}(\mathbf{U}_{\mathbf{g}}^H\mathbf{U}_{\mathbf{g}})^{-1}\mathbf{U}_{\mathbf{g}}^H$, the jamming signal can be cancelled out. Following the EVD channel estimation procedure, the eigenspace of the legitimate channels can be obtained from the eigenvector of the covariance matrix of $\tilde{\mathbf{y}}_u$. In practice, the covariance matrix can be estimated based on the received uplink data, i.e.,

$$\hat{\mathbf{R}}_{\tilde{\mathbf{y}}} = \frac{1}{\tau_{ul}} \sum_{t=1}^{\tau_{ul}} \mathbb{E}[\tilde{\mathbf{y}}_u^H(t)\tilde{\mathbf{y}}_u(t)]. \quad (49)$$

Note that $\tilde{\mathbf{y}}_u(t)$ denotes the tth received symbol in the uplink transmission phase. Denoting the set of eigenvectors of $\hat{\mathbf{R}}_{\tilde{\mathbf{y}}}$ corresponding to the K largest eigenvalues by $\mathbf{U} = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K]$, the channel estimates can be founded as

$$\hat{\mathbf{h}}_k^H = \mathbf{P}_{\mathbf{u}}\hat{\mathbf{h}}_{1,k}^H \quad (50)$$

where $\mathbf{P}_{\mathbf{u}} = \mathbf{U}(\mathbf{U}^H\mathbf{U})^{-1}\mathbf{U}^H$. Moreover, when the transmit power of each Eve and its path loss coefficient are available, the eavesdropping channel can be estimated as

$$\hat{\mathbf{g}}_k = \mathbf{P}_{\mathbf{g}}\hat{\mathbf{g}}_{LS,k} \quad (51)$$

where $\hat{\mathbf{g}}_{LS,k}$ is the LS estimation of the eavesdropping channel.

Remark 3: The proposed training scheme can be applied to the multi-user case since the training sequences sent from the users remain orthogonal with each other. Moreover, for the case that each Eve employs a random training sequence in both training phases, the proposed double training scheme is still applicable, but the eavesdropping channel cannot be accurately estimated.

Remark 4: For the case without uplink jamming, we can employ the EVD approach to estimate the eigenspace of the legitimate channels, and accurate channel estimation can be obtained without double channel training.

V. MMSE-Based Precoding for Secrecy Rate Maximization

In this section, we aim to design the beamforming vector based on the obtained channel estimation to maximize the achievable secrecy rate. For the users, we define $\Lambda_u = \text{diag}\{\phi_1 P\beta_{u_1}, \ldots, \phi_K P\beta_{u_K}\}$, $\mathbf{F}_U = \Lambda_u^{\frac{1}{2}}\mathbf{H}$, $\hat{\mathbf{F}}_U = \Lambda_u^{\frac{1}{2}}\hat{\mathbf{H}}$, and $\tilde{\mathbf{F}}_U = \mathbf{F}_U - \hat{\mathbf{F}}_U$. Similarly, for Eves, we define $\Lambda_e = \text{diag}\{\phi_1 P\beta_{e_1}, \ldots, \phi_K P\beta_{e_K}\}$, $\mathbf{F}_E = \Lambda_e^{\frac{1}{2}}\mathbf{G}$, $\hat{\mathbf{F}}_E = \Lambda_e^{\frac{1}{2}}\hat{\mathbf{G}}$, and $\tilde{\mathbf{F}}_E = \mathbf{F}_E - \hat{\mathbf{F}}_E$. Since the secrecy rate is determined by both the main channel capacity and the eavesdropping capacity, based on (7), the downlink secrecy rate maximization problem can be equivallently formulated as:

$$\begin{aligned} \text{P2:} \quad \min_{\mathbf{W}} \quad & \mathbb{E}_{\tilde{\mathbf{F}}_U, \tilde{\mathbf{F}}_E, \mathbf{m}} \Big[\|\alpha(\mathbf{F}_U\mathbf{W}\mathbf{m} + \mathbf{n}) - \mathbf{m}\|^2 \\ & + \|\xi\alpha\mathbf{F}_E\mathbf{W}\mathbf{m}\|^2 \Big| \hat{\mathbf{F}}_U, \hat{\mathbf{F}}_E \Big] \\ \text{s.t.} \quad & \text{trace}(\mathbf{W}^H\mathbf{W}) = 1. \end{aligned} \quad (52)$$

In (52), ξ is used for information leakage control and α is a power scaling factor to satisfy the power constraint.

Remark 5: Otimization problem P2 contains the eavesdropping channel and thus requires the information of large-scale path loss of Eves to be available at the BS. When such information is not available, we can remove the second part in the objective function by setting ξ to zero.

To solve P2, we first investigate the channel estimation errors arising from inaccurate subspace estimation due to the limited number of antennas and limited samplings.

Lemma 2: The covariance of the channel estimation error can be approximated by

$$\mathbb{E}\left[\tilde{\mathbf{F}}_\nu^H\tilde{\mathbf{F}}_\nu \mid \hat{\mathbf{F}}_\nu\right] \approx \delta_\nu \mathbf{I}_N, \nu \in \{U, E\} \quad (53)$$

where $\delta_\nu = \frac{\sum_{i=1}^{K}\phi_i P\beta_{\nu_i}\sum_{l\neq k}\phi_l^2\beta_{\nu_l}^2}{N\phi_k^2\beta_{\nu_k}^2}$.

Please see Appendix B for proof.

Then, the optimal precoding vector can be obtained based on Lemma 2, which is given as follows.

Theorem 3: For a fixed power allocation, the optimal downlink beamforming vector is given by

$$\mathbf{W}^\star = \alpha\left(\hat{\mathbf{F}}^H\hat{\mathbf{F}} + \xi^2\hat{\mathbf{F}}_E^H\hat{\mathbf{F}}_E + \kappa\mathbf{I}_N\right)^{-1}\hat{\mathbf{F}}^H. \quad (54)$$

where $\kappa = \delta_U + \xi^2\delta_E + K\sigma^2$

Please see Appendix C for proof.

It is worth noting that, similar to the multi-cell precoding in [33] where the inter-cell interference is taken into account for precoding design, the information leakage to Eve is incorporated in the proposed MMSE precoding. However, when all the users are allocated with equal power, the precoding scheme only maximizes the minimum achievable secrecy rate among all the users. To maximize the achievable sum secrecy rate, optimal power allocation among different users requires further investigation.

VI. Numerical Results

In this section, the downlink achievable secrecy rate and uplink achievable rate under PSA are evaluated through simulations to verify the analysis. The path loss follows $\beta = C_0 r^{-4}$, with $C_0 = -38.46$ dB. The users are uniformly distributed in a circular region with BS located at the center and the inner and outer radiuses of 100 m and 120 m, respectively. Without loss of generality, we assume that each Eve experiences the same path loss with the corresponding legitimate user. The uplink transmitting power levels for pilot and data of the users are

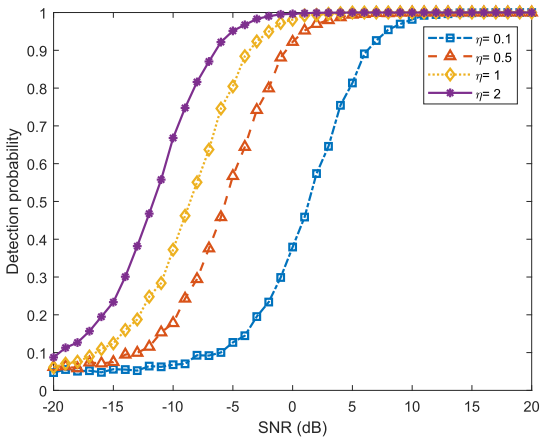

Fig. 1. The PSA detection probability, with $N = 64$, $K = 4$, and $\epsilon = 5\%$.

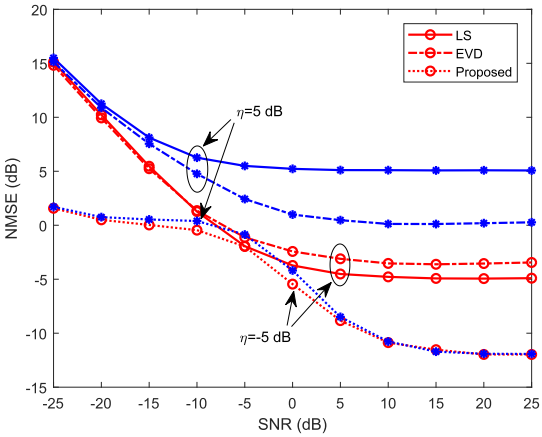

Fig. 2. The NMSE of different channel estimation schemes, where $N = 64$ and $K = 4$.

$P_u = 30$ dBm and $p_1 = \cdots = p_K = 30$ dBm, respectively, unless otherwise specified, and the downlink transmission power of the BS is 40 dBm. The transmission power for PSA is set to be the same for all Eves, and $q_1 = \cdots = q_K = P_{e_k}$ unless otherwise specified. For notation simplicity, we use $\eta = P_{e_k}/P_u$ to denote the transmission power for PSA. The channel coherent inteval is set to be $\tau_c = 1000$ samples for a low mobility environment (corresponding to a coherent time 50 ms and coherent bandwidth 200 kHz) [39], the uplink training length is $\tau_p = K$ samples, and the uplink data transmission length is $\tau_{ul} = 200$ samples. For each simulated point in the curves, 10000 Monte Carlo simulations are conducted.

We evaluate the PSA detection performance with the proposed double channel training scheme, as shown in Fig. 1. For a given false alarm probability, the detection probability increases with the SNR and approaches to one in high the SNR region. Moreover, the detection probability increases with the transmission power of PSA, which infers that Eve should properly control its transmission power to hide its presence. We evaluate the channel estimation performance with different channel estimation schemes, and use the normalized mean square error (NMSE) ($\|\mathbf{h}_k - \hat{\mathbf{h}}_k\|^2/\|\mathbf{h}_k\|^2$) as the performance metric, in Fig. 2. The NMSE of the proposed scheme is much lower than that of the

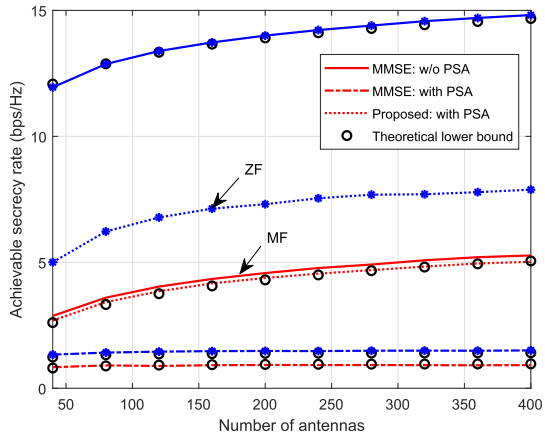

Fig. 3. The downlink achievable secrecy rate with different channel estimation and precoding schemes, where $K = 4$, $\phi = 0.8$, and $\eta = 0.5$ for all Eves. Note that the marked lines denote the results for ZF scheme and the black circles are theoretical lower bound for the MMSE based channel estimations with or without PSA.

LS scheme and the conventional EVD based channel estimation scheme, especially in the high SNR region. This is because the LS estimation scheme cannot distinguish between the user's channel and the eavesdropping channel due to the PSA. In addition, since the Eves are assumed to experience the same path loss as the corresponding users, the EVD based scheme has a large error in subspace estimation.

The downlink achievable secrecy rate under both MF precoding and ZF precoding schemes are shown in Fig. 3. We observe that the achievable secrecy rate is severely degraded by the PSA for both precoding schemes due to the inaccurate channel estimation. In addition, the achievable secrecy rate monotonically increases with the number of antennas when PSA is absent, whereas it remains invariant under PSA since both the SINRs of the legitimate user and Eve increase with the number of antennas. For the MF precoding scheme with the proposed channel estimation, the achievable secrecy rate approaches to that of the perfect CSI case, which shows the effectiveness of the proposed scheme. However, for the ZF precoding scheme, even though the secrecy rate can be significantly improved with the proposed scheme, there exists a large gap as compared to the perfect CSI case. This is because the ZF precoding scheme relies on very accurate channel estimation, and more inter-user interference occurs under channel estimation errors. Moreover, the lower bound is very tight as compared with the simulation results, which validates the theoretical analysis.

The uplink achievable rate under PSA and uplink jamming is shown in Fig. 4 with different channel estimation and MF/ZF detection schemes. Similar to the downlink case, we can observe that the uplink achievable rate is significantly degraded by PSA. It approaches to a constant value when N is very large, which verifies the analysis in Subsection III-B. The uplink achievable rate with the proposed channel estimation scheme outperforms that with the conventional scheme. This is because the uplink jamming can be cancelled out, since the proposed channel estimation lies in the nullspace of the eavesdropping channel. We then analyze the impact of power allocation between PSA and

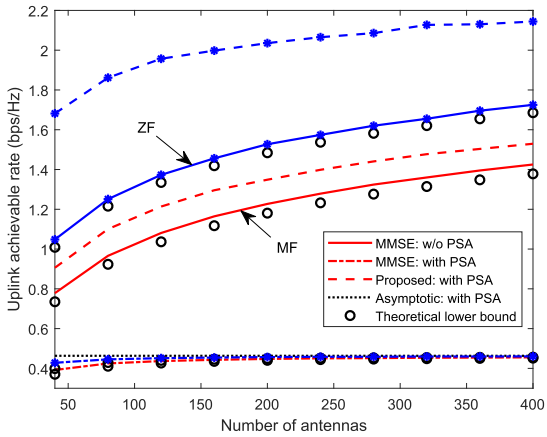

Fig. 4. The uplink achievable rate vs. the number of antennas with different schemes, where $K = 4$ and $\eta = 0.5$ for all Eves. Note that the marked lines denote the results for ZF scheme and the black circles are theoretical lower bound for the MMSE based channel estimations with or without PSA.

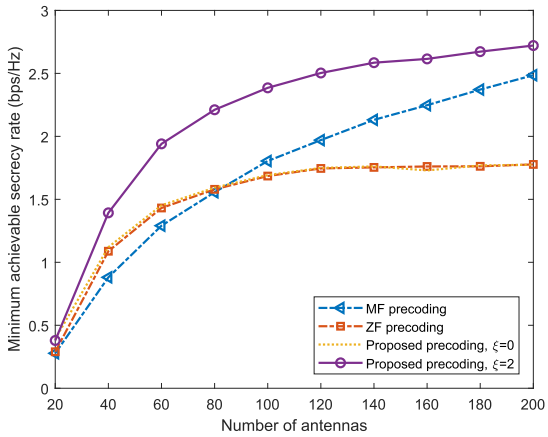

Fig. 6. The minimum achievable secrecy rate among all the users with different precoding schemes based on the proposed channel estimation, where $N = 64$, $K = 8$, $\phi = 0.9$, $\eta = -5$ dB for all Eves.

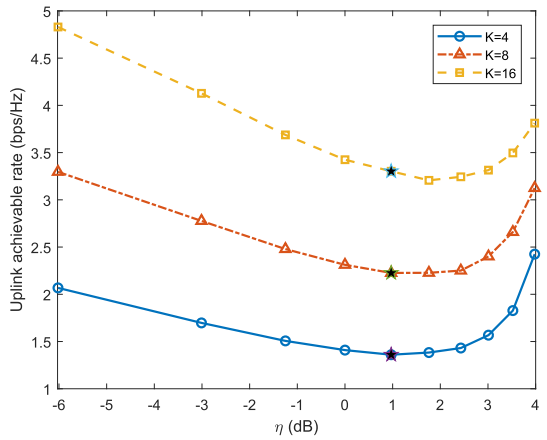

Fig. 5. The uplink achievable sum rate vs. the transmission power of PSA, where $N = 64$, $P_u = 30$ dBm, the total energy of each Eve is 0.1 J. Note that the approximated optimal solution with P1 is denoted by the solid star.

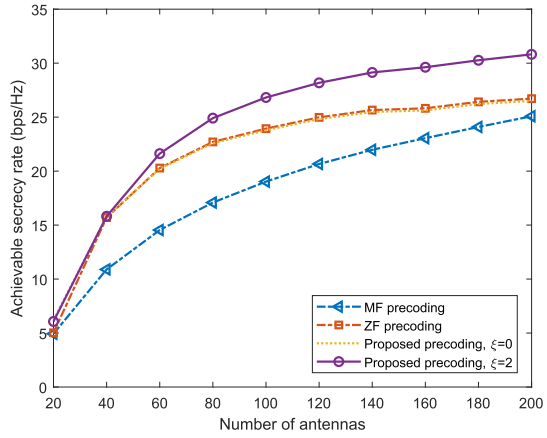

Fig. 7. The downlink achievable sum secrecy rate with different precoding schemes based on the proposed channel estimation, where $N = 64$, $K = 8$, $\phi = 0.9$, and $\eta = -5$ dB for all Eves.

uplink jamming of Eve on the uplink achievable rate in Fig. 5. It can be seen that the uplink achievable rate is a convex function of the transmission power for PSA and the obtained solution of PSA power with P1 in Subsection III-C approaches to the optimal value.

Lastly, we compare the downlink achievable secrecy rates for different precoding schemes based on the proposed channel estimation in Fig. 6. The minimum achievable secrecy rate among all the users can be significantly improved with the proposed MMSE precoding scheme, since the information leakage to Eve has been reduced by the proposed scheme. Moreover, the achievable secrecy rate with the MF precoding scheme increases with N, and is larger than that of the ZF scheme when N is very large. This is because the channel estimation error decreases with N, and thus the achievable secrecy rate will be improved. Since the channel estimation errors arising from the limited antennas cannot vanish [40], and the ZF precoding scheme is very sensitive to CSI errors, the achievable secrecy rate with ZF precoding is asymptotically approach to a constant, as shown in Fig. 6. The achievable sum secrecy rate with AN is evaluated, as shown in Fig. 7, which demonstrates that the proposed precoding scheme outperforms both the MF and the ZF schemes.

VII. Conclusion

In this paper, we have evaluated the effect of PSA on the achievable rate in a single-cell massive MIMO system. It has been shown that both the uplink achievable rate and the downlink achievable secrecy rate can be degraded severely by PSA, and downlink positive secrecy rate is achievable as long as the effective transmission power of Eve is less than that of the legitimate user. To improve the secrecy rate, a double channel training based scheme has been proposed, and the eigenspace of Eve channels can be estimated based on the channel estimation difference. It has been shown that the PSA can be detected and the legitimate channel can be estimated accurately with the proposed scheme. Based on the estimated channels, an MMSE precoding scheme has been presented to maximize the downlink achievable secrecy rate. To facilitate the analysis, we consider

only the single-cell case in this study. Extension to a multi-cell case requires further investigation in the future considering both the conventional pilot contamination and pilot spoofing attack.

APPENDIX

A. Proof of Theorem 1

Based on the lower bound of the achievable rate in (9) and (11), the achievable secrecy rate is approximated by

$$R_{sec,k} \approx [R_k - R_{e_k}]^+. \tag{55}$$

Based on (3) and MF precoding, we have

$$|\mathbb{E}[\mathbf{h}_k \mathbf{w}_k]|^2 = \left| \mathbb{E}\left[\frac{\mathbf{h}_k \widehat{\mathbf{h}}_k^H}{\left\| \widehat{\mathbf{h}}_k^H \right\|} \right] \right|^2 = \mathbb{E}\left[\left\| \widehat{\mathbf{h}}_k \right\|^2 \right] \overset{(a)}{=} C_N^2 \eta_{u_k}$$

where (a) holds because $\|\widehat{\mathbf{h}}_k\|$ follows a chi-square distribution with $2N$ DoF. Similarly,

$$\begin{aligned} \text{var}(\mathbf{h}_k \mathbf{w}_k) &= \mathbb{E}[(\mathbf{h}_k \mathbf{w}_k)^2] - \mathbb{E}^2[\mathbf{h}_k \mathbf{w}_k] \\ &\overset{(b)}{=} \mathbb{E}\left[\left| \widetilde{\mathbf{h}}_k \mathbf{w}_k \right|^2 \right] + \mathbb{E}\left[\left| \widehat{\mathbf{h}}_k \mathbf{w}_k \right|^2 \right] - \mathbb{E}^2[\widehat{\mathbf{h}}_k \mathbf{w}_k] \\ &\overset{(c)}{=} 1 - \eta_{u_k} + \text{var}(\widehat{\mathbf{h}}_k \mathbf{w}_k) \\ &= 1 - \eta_{u_k} + V_n \eta_{u_k}, \end{aligned}$$

where (b) holds since $\widehat{\mathbf{h}}_k$ and $\widetilde{\mathbf{h}}_k$ are independent of each other, and (c) holds since $\widetilde{\mathbf{h}}_k$ and $\mathbf{w}_k$ are uncorrelated. Substituting the above results into (9), we can obtain the lower bound of the achievable rate for the kth user. Similarly, we can derive the achievable rate for the kth Eve as shown in (11).

B. Proof of Lemma 2

The channel estimation error comes from the subspace estimation error of eavesdropping channel due to the finite N and limited number of samples. It has been proved that the effect of limited number of samples on the channel estimation vanishes as the number of samples increases. Since the length of the uplink data is usually much larger than the number of users, channel estimation errors resulting from limited samples can be ignored. From [40], we know that the channel estimation error arising from a limited number of antennas is given by

$$\tilde{\mathbf{h}}_k = \frac{\sum_{l \neq k} p_l \beta_{u_l} \mathbf{h}_l \mathbf{h}_k^H \mathbf{h}_l}{N p_k \beta_{u_k}} \tag{56}$$

and the covariance of the channel estimation error can be calculated by

$$\tilde{\mathbf{h}}_k^H \tilde{\mathbf{h}}_k \approx \frac{\sum_{l \neq k} \phi_l^2 \beta_{s_l}^2}{N \phi_k^2 \beta_{s_k}^2} \mathbf{I}_N. \tag{57}$$

Similarly, we can derive the covariance for the eavesdropping channel.

C. Proof of Theorem 3

The objective function of P2 can be expressed as

$$\begin{aligned} &J(\mathbf{W}) \\ &= \mathbb{E}\left[\|\alpha(\mathbf{F}_U \mathbf{W}\mathbf{m} + \mathbf{n}) - \mathbf{m}\|^2 + \|\xi \alpha \mathbf{F}_E \mathbf{W}\mathbf{m}\|^2 \Big| \hat{\mathbf{F}}_U, \hat{\mathbf{F}}_E \right] \\ &= \mathbb{E}\left[\|(\alpha \mathbf{F}_U \mathbf{W} - \mathbf{I}_K)\mathbf{m}\|^2 + \|\xi \alpha \mathbf{F}_E \mathbf{W}\mathbf{m}\|^2 \Big| \hat{\mathbf{F}}_U, \hat{\mathbf{F}}_E \right] + \alpha^2 K \\ &= \text{trace}\left(\mathbb{E}\left[(\alpha \mathbf{F}_U \mathbf{W} - \mathbf{I}_K)^H (\alpha \mathbf{F}_U \mathbf{W} - \mathbf{I}_K) \right.\right. \\ &\left.\left. + \alpha^2 \xi^2 \mathbf{W}^H \mathbf{F}_E^H \mathbf{F}_E \mathbf{W} | \hat{\mathbf{F}}_U, \hat{\mathbf{F}}_E \right] \right) + \alpha^2 K \\ &= \text{trace}\Big(\alpha^2 \mathbf{W}^H \mathbb{E}[\mathbf{F}_U^H \mathbf{F}_U | \hat{\mathbf{F}}_U] \mathbf{W} - \alpha \mathbf{W}^H \mathbf{F}_U^H - \alpha \hat{\mathbf{F}}_U \mathbf{W} \\ &+ \alpha^2 \xi^2 \mathbf{W}^H \mathbb{E}[\mathbf{F}_E^H \mathbf{F}_E | \hat{\mathbf{F}}_E] \mathbf{W} \Big) + (\alpha^2 + 1) K \\ &\overset{(d)}{=} \text{trace}\Big(\alpha^2 \mathbf{W}^H \Big(\hat{\mathbf{F}}_U^H \hat{\mathbf{F}}_U + \xi^2 \hat{\mathbf{F}}_E^H \hat{\mathbf{F}}_E + (\delta_U + \xi^2 \delta_E) \mathbf{I}_N \Big) \mathbf{W} \\ &- \alpha \mathbf{W}^H \hat{\mathbf{F}}_U^H - \alpha \hat{\mathbf{F}}_U \mathbf{W} \Big) + (\alpha^2 + 1) K, \end{aligned} \tag{58}$$

where (d) follows from Lemma 2. The Lagrangian function of P2 can be expressed as

$$L(\mathbf{W}, \lambda) = J(\mathbf{W}) + \lambda(\text{trace}(\mathbf{W}^H \mathbf{W}) - 1) \tag{59}$$

where λ is the Lagrangian multiplier. Define

$$\mathbf{R} = \hat{\mathbf{F}}_U^H \hat{\mathbf{F}}_U + \xi^2 \hat{\mathbf{F}}_E^H \hat{\mathbf{F}}_E + \left(\delta_U + \xi^2 \delta_E + \frac{\lambda}{\alpha^2} \right) \mathbf{I}_N \tag{60}$$

we have

$$L(\mathbf{W}, \lambda) = \|\Theta - \Xi\|^2 - \hat{\mathbf{F}}_U \mathbf{R}^{-1} \hat{\mathbf{F}}_U^H + (\alpha^2 + 1) K - \lambda \tag{61}$$

where $\Theta = \alpha \mathbf{R}^{\frac{1}{2}} \mathbf{W}$, and $\Xi = \mathbf{R}^{-\frac{1}{2}} \hat{\mathbf{F}}_U^H$. It can be seen that $L(\mathbf{W}, \lambda)$ is minimized when $\Theta = \Xi$. Thus, the optimal solution can be obtained as

$$\mathbf{W}^\star = \frac{1}{\alpha} \mathbf{R}^{-1} \hat{\mathbf{F}}_U^H. \tag{62}$$

We then have

$$L(\mathbf{W}^\star, \lambda) = -\hat{\mathbf{F}}_U \mathbf{R}^{-1} \hat{\mathbf{F}}_U^H + (\alpha^2 + 1) K - \lambda. \tag{63}$$

Similar to the proof in [33], we can solve the optimal value of λ given by $\lambda^\star = \alpha^2 K$. This completes the proof.

REFERENCES

[1] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surv. Tuts.*, vol. 20, no. 4, pp. 2714–2741, Oct.–Dec. 2018.

[2] F. Rusek *et al.*, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.

[3] "Sprint unveils six 5G-ready cities; significant milestone toward launching first 5G mobile network in the U.S.," 2018. [Online]. Available: http://newsroom.sprint.com/sprint-unveils-5g-ready-massive-mimo-markets.htm

[4] A. Khansefid and H. Minn, "Achievable downlink rates of MRC and ZF precoders in massive MIMO with uplink and downlink pilot contamination," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 4849–4864, Dec. 2015.

[5] O. Elijah, C. Y. Leow, T. A. Rahman, S. Nunoo, and S. Z. Iliya, "A comprehensive survey of pilot contamination in massive MIMO-5G system," *IEEE Commun. Surv. Tuts.*, vol. 18, no. 2, pp. 905–923, Apr.–Jun. 2016.

[6] J. Zuo, J. Zhang, C. Yuen, W. Jiang, and W. Luo, "Multicell multiuser massive MIMO transmission with downlink training and pilot contamination precoding," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6301–6314, Aug. 2016.

[7] H. V. Cheng, E. Björnson, and E. G. Larsson, "Optimal pilot and payload power control in single-cell massive MIMO systems," *IEEE Trans. Signal Process.*, vol. 65, no. 9, pp. 2363–2378, May 2017.

[8] W. Wu, X. Gao, Y. Wu, and C. Xiao, "Beam domain secure transmission for massive MIMO communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7113–7127, Aug. 2018.

[9] J. Li, D. Wang, P. Zhu, J. Wang, and X. You, "Downlink spectral efficiency of distributed massive MIMO systems with linear beamforming under pilot contamination," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1130–1145, Feb. 2018.

[10] Z. M. Fadlullah, C. Wei, Z. Shi, and N. Kato, "GT-QoSec: A game-theoretic joint optimization of QoS and security for differentiated services in next generation heterogeneous networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1037–1050, Feb. 2017.

[11] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[12] Z. M. Fadlullah, C. Wei, Z. Shi, and N. Kato, "Joint optimization of QoS and security for differentiated applications in heterogeneous networks," *IEEE Wireless Commun.*, vol. 23, no. 3, pp. 74–81, Jun. 2016.

[13] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "Healthdep: An efficient and secure deduplication scheme for cloud-assisted ehealth systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4101–4112, Sep. 2018.

[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 3, pp. 1550–1573, Jul.–Sep. 2014.

[15] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4265–4276, Aug. 2015.

[16] M. Alageli, A. Ikhlef, and J. Chambers, "SWIPT massive MIMO systems with active eavesdropping," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 233–247, Jan. 2019.

[17] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, Nov. 2013.

[18] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 1, pp. 347–376, Jan.–Mar. 2017.

[19] X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, and X. Shen, "On physical layer security: Weighted fractional Fourier transform based user cooperation," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5498–5510, Aug. 2017.

[20] W. Wang, K. C. Teh, and K. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[21] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[22] 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.

[23] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 5, pp. 932–940, May 2015.

[24] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[25] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6437–6449, Dec. 2018.

[26] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Physical-layer security in TDD massive MIMO," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7359–7380, Nov. 2018.

[27] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 525–528, Oct. 2015.

[28] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2093–2106, May 2018.

[29] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 1, pp. 210–223, Jan. 2018.

[30] H.-M. Wang, K.-W. Huang, and T. A. Tsiftsis, "Multiple antennas secure transmission under pilot spoofing and jamming attack," *IEEE J Sel. Areas Commun.*, vol. 36, no. 4, pp. 860–876, Apr. 2018.

[31] K.-W. Huang, H.-M. Wang, Y. Wu, and R. Schober, "Pilot spoofing attack by multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6433–6447, Oct. 2018.

[32] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive mimo networks: Optimal power control against active eavesdropping," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4724–4737, Oct. 2018.

[33] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2640–2651, Aug. 2011.

[34] W. Wang, K. C. Teh, K. H. Li, and S. Luo, "On the impact of adaptive eavesdroppers in multi-antenna cellular networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 269–279, Feb. 2018.

[35] J. Hoydis, S. Ten Brink, and M. Debbah, "Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?" *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 160–171, Feb. 2013.

[36] H. Ju and R. Zhang, "Optimal resource allocation in full-duplex wireless-powered communication network," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3528–3540, Oct. 2014.

[37] L. Grippo and M. Sciandrone, "On the convergence of the block nonlinear Gauss–Seidel method under convex constraints," *Operations Res. Lett.*, vol. 26, no. 3, pp. 127–136, 2000.

[38] H. Q. Ngo and E. G. Larsson, "EVD-based channel estimation in multicell multiuser MIMO systems with very large antenna arrays," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, 2012, pp. 3249–3252.

[39] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. Cambridge, U.K.: Cambridge Univ. Press, 2016.

[40] W. Xu, W. Xiang, Y. Jia, Y. Li, and Y. Yang, "Downlink performance of massive-MIMO systems using EVD-based channel estimation," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3045–3058, Apr. 2017.

Wei Wang (S'14) received the B.Eng. degree in information countermeasure technology and the M.Eng. degree in signal and information processing from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2018. He is currently a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include wireless communications, space-air-ground integrated networks, wireless security, and physical layer security. He received the IEEE Student Travel Grants for IEEE ICC'17, and the Chinese Government Award for Outstanding Self-financed Students Abroad in 2019.

Nan Cheng (M'16) received the B.E. and M.S. degrees from Tongji University, Shanghai, China, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada. He is currently a Joint Professor with the School of Telecommunication, Xidian University. He is also a Joint Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, and with the Department of Electrical and Computer Engineering, University of Waterloo. His research interests include performance analysis, MAC, opportunistic communication for vehicular networks, unmanned aerial vehicles, and application of artificial intelligence for wireless networks.

Kah Chan Teh (S'96–M'99–SM'07) received the B. Eng. and Ph.D. degrees in electrical engineering from Nanyang Technological University (NTU), Singapore, in 1995 and 1999, respectively. Since July 1999, he has been with NTU where he is currently an Associate Professor with the School of Electrical and Electronic Engineering. His research interests include signal processing for communications, performance evaluations of interference suppression for spread-spectrum communication systems, multiuser detection in CDMA systems, cognitive radios, cooperative communication systems and radar. He received the Best Teacher of the Year Award from NTU in 2005 and 2014.

Xiaodong Lin (M'09–SM'12–F'17) received the Ph.D. degree in information engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 1998, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently a tenured Associate Professor with the School of Computer Science, College of Engineering and Physical Sciences, University of Guelph, Ontario, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. He received the Outstanding Achievement in Graduate Studies Award from the University of Waterloo. He received the Canada Graduate Scholarship for Doctoral Award from the Natural Sciences and Engineering Research Council of Canada and the best paper awards of the 18th International Conference on Computer Communications and Networks in 2009, the 5th International Conference on Body Area Networks in 2010, and the IEEE International Conference on Communications in 2007.

Weihua Zhuang (M'93–SM'01–F'08) has been with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, since 1993, where she is a Professor and a Tier I Canada Research Chair in Wireless Communication Networks. She is the recipient of 2017 Technical Recognition Award from IEEE Communications Society Ad Hoc & Sensor Networks Technical Committee, one of 2017 ten N2Women (Stars in Computer Networking and Communications), and a co-recipient of several best paper awards from IEEE conferences. She was the Editor-in-Chief of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (2007–2013), Technical Program Chair/Co-Chair of IEEE VTC Fall 2017 and Fall 2016, and the Technical Program Symposia Chair of the IEEE GLOBECOM 2011. She is a fellow of the Royal Society of Canada, the Canadian Academy of Engineering, and the Engineering Institute of Canada. She is an elected member in the Board of Governors and VP Publications of the IEEE Vehicular Technology Society. She was an IEEE Communications Society Distinguished Lecturer (2008–2011).

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree in electrical engineering from Dalian Maritime University, Dalian, China, in 1982, and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1987 and 1990, respectively. He is currently a university Professor and an Associate Chair for graduate studies with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include resource management, wireless network security, social networks, smart grids, and vehicular ad hoc and sensor networks. He is a registered Professional Engineer of ON, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He was an Elected Member of the IEEE ComSoc Board of Governor and the Chair of the Distinguished Lecturers Selection Committee. He was a recipient of the Excellent Graduate Supervision Award in 2006. He received the Premiers Research Excellence Award from the Province of Ontario, Canada, in 2003. He served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom16, Infocom14, IEEE VTC10 Fall, and Globecom07, the Symposia Chair for IEEE ICC10, the Tutorial Chair for IEEE VTC11 Spring and IEEE ICC08, the General Co-Chair for ACM Mobihoc15, Chinacom07, and QShine06, and the Chair for the IEEE Communications Society, Technical Committee on Wireless Communications and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for the IEEE INTERNET OF THINGS JOURNAL, IEEE Network, *Peer-to-Peer Networking and Application*, and *IET Communications*; a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Networks*, and *ACM/Wireless Networks*; and the Guest Editor for IEEE JSAC, IEEE WIRELESS COMMUNICATIONS, IEEE Communications Magazine, and *ACM Mobile Networks and Applications*.