Beam-Domain Anti-Jamming Transmission for Downlink Massive MIMO Systems: A Stackelberg Game Perspective

Zhexian Shen, Kui Xu, *Member, IEEE*, and Xiaochen Xia

***Abstract*— In this paper, beam-domain (BD) anti-jamming transmission in a downlink massive multiple-input multiple-output (MIMO) system is investigated. A smart jammer with multiple antennas attempts to interfere with the signal reception of users with the desired energy efficiency (EE), whereas a base station (BS) tries to minimize the transmission cost while ensuring uninterrupted communication. A Bayesian Stackelberg game between the BS and jammer, where the jammer is the follower and the BS acts as the leader, is modeled. In the follower subgame, the optimal jamming precoding with a closed-form power solution is introduced. The optimal jamming power is proportional to the transmission power in the downlink, and thus, for the BS, the strategy of suppressing malicious attacks by increasing the transmission power fails. In the leader subgame, generalized zero-forcing (ZF), whose closed-form power solution constitutes the unique Stackelberg equilibrium (SE) with that of the jammer, is found to be the optimal anti-jamming precoding for robust transmission. The results show that there always exists a precoding solution for the BS that ensures reliable transmission when the SE is obtained. A proper increase in the minimum signal-to-interference-and-noise ratio (SINR) threshold or the BD channel approximation error helps the BS save power during the resistance against the jammer. Then, a simplified power solution without the instantaneous channel state information (CSI) of jamming channels is further introduced for practical implementation. Numerical results are provided to verify the proposed solutions.**

***Index Terms*— Massive MIMO, jamming defense, Stackelberg game, beam domain.**

I. Introduction

A. Motivation

THE physical layer security of massive multiple-input multiple-output (massive MIMO) systems has been widely investigated in the research community. Based on the attacking mode, the security issues include active/passive eavesdropping and jamming. In Wyner's pioneering work [1], a nonzero secrecy capacity is obtained if the legitimate channel is superior to the eavesdropping channel. To improve the secrecy of transmission, S. Goel *et al* first proposed a method of broadcasting artificial noise (AN) within the null space of user channels [2]. Since no information about eavesdropping channels is needed, many secure transmission schemes expanding AN injection have been proposed [3]–[6]. A large number of researchers also concentrate on the study of jamming defense. Instead of pursuing the secrecy of communication, the anti-jamming issue mainly focuses on the robustness of transmission. In addition to typical solutions, e.g., frequency hopping [7] and the direction-sequence spread spectrum (DSSS) [8], many solutions have been proposed against different attacking patterns. Specifically, when a jammer attempts to disturb the base station (BS) beamforming through pilot contamination in the uplink [9], [10], jamming detection schemes [11]–[13] along with the high degrees of freedom (DoF) from high-dimensional channels can be applied to suppress the pilot contamination and ensure the accurate beamforming [14]. In our previous work, a spatial sparsity based secure transmission scheme was proposed to defend against simultaneous eavesdropping and jamming attacks [15]. A beam extraction method was introduced to eliminate pilot contamination, from which a grouping based receiving scheme was proposed along with a joint power and combining matrix optimization algorithm to improve the secrecy of transmission. In another case where a jammer tries to interfere with the downlink transmission so as to avoid being detected by the BS and improve the energy efficiency (EE) [16], a set of methods involving the jamming power estimation [17], the game theory based decision making [18] and the anti-jamming beamforming reconfiguration [19] can be coordinated to defend against the malicious jamming attacks. Nevertheless, it is still challenging to address this issue, especially for a downlink massive MIMO system. On the one hand, the transmission in the downlink is more vulnerable than that in the uplink because of the limited number of antennas and signal processing capacity on the user side. In contrast, the jamming precoding can be designed in multi-domains, e.g., the power-domain and the spatial-domain, to achieve stronger attacks with less power consumption [16], [20]. On the other hand, the intelligence can be achieved by a jammer to adjust the jamming strategy according to the variation of the precoding on the BS side.

Manuscript received July 3, 2020; revised November 20, 2020 and February 4, 2021; accepted February 14, 2021. Date of publication March 2, 2021; date of current version April 1, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 62071485, Grant 61901519, and Grant 61771486; in part by the Basic Research Project of Jiangsu Province under Grant BK20192002; and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20201334 and Grant BK20181335. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Stefano Tomasin. *(Corresponding author: Kui Xu.)*

The authors are with the College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China (e-mail: lgdxszx@sina.com; lgdxxukui@sina.com).

Digital Object Identifier 10.1109/TIFS.2021.3063632

Under this condition, the fixed anti-jamming solutions fail and there exists a game between the BS and jammer. It is unknown whether there exists a closed-form precoding solution where the BS can achieve long-term advantages in the game. All these issues should be investigated.

B. Related Works

The physical layer security of massive MIMO systems has increasingly raised concerns. Although the high-dimensional channels are spatially sparse and can be used for designing directional beamforming through beam-domain (BD) or angle-domain (AD) transmission schemes to improve the security [21]–[25], owing to the open and shared nature of the wireless medium, the transmission in massive MIMO systems is extremely vulnerable to malicious attacks. The gain of beamforming depends on the accurate estimation of channels. Unfortunately, a smart jammer may actively attack the training for the purpose of inducing pilot contamination and directing the BS beamforming to the disadvantage of users [26]. Alternatively, a powerful jammer may be equipped with a large-scale antenna array to disturb the data transmission and deteriorate the receiving signal-to-interference-and-noise ratio (SINR) [20].

There have been many works studying different types of jammers. Based on the mechanism of disruption, jammers can be classified into four categories: constant jammers, intermittent jammers, reactive jammers, and adaptive jammers.[1] A constant jammer continuously transmits jamming signals with constrained power and limited bandwidth, while an intermittent jammer transmits for a certain time slot and then goes dormant for the remaining time [27]. Both of these types of jammers suffer from low EE and high probability of being detected since the statistical characteristics of legitimate signals, such as the received signal strength, carrier sensing time and packet error rate, are changed [28], [29]. A reactive jammer remains quiet most of the time and corrupts the signal reception only when the legitimate channel is found to be busy [30], [31], which is more energy efficient and hard to detect. However, an accurate sensing method should be designed to determine the status of legitimate nodes. An adaptive jammer takes similar steps to a reactive jammer and further constructs a precise power solution according to the variation in the wireless channel between legitimate nodes [32]. Since more intelligent design is achieved, the adaptive jammer is also called the "smart jammer" and is considered to provide an upper bound of the jamming performance. This is, however, challenging to realize in practice because the wireless channel varies quickly and the perfect channel state information (CSI) of legitimate nodes is usually unknown to the jammer [33], [34].

Efforts have been made to fight against jamming attacks. From the perspective of engineering, the anti-jamming communication cycle mainly consists of three steps: jamming cognition, anti-jamming decision-making and beamforming design [18]. First, the cognitive radio technologies, along with machine learning and range based methods, are employed to detect jamming attacks and acquire the location of jammers [35]. Then, based on game theory, the specific anti-jamming decisions are made, which guide the beamforming design in multi-domains. Specifically, in spectrum-domain, frequency hopping and DSSS [8] technologies are adopted to defend against constant/intermittent jamming attacks. The cost is the requirement for a wide band and the loss of spectral efficiency, and this kind of method is ineffective for defending against a reactive/adaptive jammer without the assistance of advanced jamming detection and a faster hopping rate [36]. In power and spatial domain, the power and the configuration of the beamforming are designed separately to suppress the jamming signals from the direction of jammers [10], [14]. The main challenge is that the statistics of the jamming channel should be available for the legitimate nodes, which may be infeasible in practice. When making anti-jamming decisions, various game theory-based solutions have been proposed [18], [37]–[42]. Through the modeling and analysis of the interactions among players with different attributes, sequential decisions are made for jamming defense in wireless networks [43]. In [37], the Markov game framework was modeled, and a collaborative multiagent reinforcement learning method was employed to obtain the optimal anti-jamming strategy. In [38], Li. Y *et al.* considered security issues in the remote state estimation of cyber-physical systems containing an energy constrained sensor-jammer pair. A zero-sum game framework was formulated to search for the optimal strategies on both sides. Among the game models, the Stackelberg game stands out for capturing the hierarchical interactions between legitimate users and jammers, which has recently been of increasing concern. Based on the Stackelberg game framework, the anti-jamming power solutions were investigated in [33], [40]–[43], and the channel selection scheme was proposed in [44]. Some of the schemes took the incomplete information of the jammers into consideration and formulated a game model with statistics. Nevertheless, it is still challenging to address this issue in wireless communication systems, especially in a downlink massive MIMO system. On the one hand, the transmission in the downlink is more vulnerable than that in the uplink because of the limited number of antennas and signal processing capacity on the user side. It is much easier for a multi-antenna jammer to achieve stronger attacks with higher EE when facing users [16], [20]. On the other hand, there is no way for the BS to obtain the knowledge of the jamming channel directly, if the jamming attacks occur in the downlink. Under this condition, it is unknown whether there exists a precoding solution where the BS can ensure the long-term robust transmission.

C. Contributions

In this paper, we consider the jamming defense in a downlink massive MIMO system, where a smart jammer equipped with a large-scale antenna array attempts to interfere with the reception of users and the BS has to ensure reliable transmission by dynamically adjusting the precoding. A Bayesian Stackelberg game is used to model the hierarchical interaction

[1]The jamming attacks in other layers, such as medium access control (MAC) and network layers, are out of the scope of this paper.

between the BS and jammer. Inspired by [22]–[24], BD signal processing is applied by both the BS and jammer to get the optimal precoding strategies with closed-form power solutions. The main contributions of this paper are as follows:

- Two cases of the game are considered. In case 1, the BD channels of the BS or the jammer are approximately orthogonal, whereas in case 2, the correlation of the BD channels is considered. Based on this, an optimization of the jammer's precoding that aims to achieve the target jamming EE with minimum power consumption is introduced in the follower subgame, and then, the optimal power solution in a closed form is proposed. The result shows that the optimal jamming power is proportional to that of the BS. Simply increasing the transmission power does not help the system defend against malicious attacks. Instead, the feasibility of the jammer's optimization is improved.
- An optimization of the anti-jamming precoding at the BS is introduced in the leader subgame for the purpose of ensuring uninterrupted communication in the downlink. We prove that the generalized zero-forcing (ZF) becomes the optimal configuration for jamming defense. To minimize the cost fighting against the jammer, the optimal power solution in a closed form is given in case 1, and an approach to obtaining the numerical power solution is introduced in case 2.
- We prove that there exists a unique Stackelberg equilibrium (SE) between the BS and jammer in case 1. The proposed strategy pair considering the absence of the instantaneous CSI of the jammer constitutes a good approximation of the equilibrium. When the SE is obtained, there always exists a precoding solution for the BS that ensures reliable transmission. An interesting result is that a proper increase in the SINR threshold or the BD channel approximation error is conducive to reducing the power consumption of the BS, which is different from the result in a typical massive MIMO system without a jammer. The cost of this, however, is a higher probability of the optimization being infeasible.

The remainder of this paper is organized as follows. Section II introduces the system model and the formulation of problems. Section III presents the analysis of the follower subgame. In section IV, the leader subgame is discussed. In section V, the numerical simulation results are given. Finally, the conclusion is presented in section VI.

Notation: Boldface uppercase letters $\mathbf{A}$ and lowercase letters $\mathbf{a}$ are used to denote matrices and column vectors. $\mathbf{A}_{p,q}$ and $(\mathbf{A})_{,q}$ are used to denote the elements in the p-th row and q-th column and the q-th column of the matrix, respectively. $(\mathbf{a})_m$ stands for the m-th element of the vector $\mathbf{a}$, and $|\mathbf{a}|$ and $\|\mathbf{a}\|$ are the modulus and Euclidean norm of $\mathbf{a}$, respectively. The superscripts $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$ represent transpose, conjugate and conjugate-transpose operations, respectively. In addition, $\succcurlyeq$, $(\cdot)^\dagger$ and $\mathbb{E}\{\cdot\}$ are the positive semidefinite, pseudoinverse and expectation operations of matrices. We use $\mathcal{Z}\sim\mathcal{N}_{\mathbb{C}}\left(\mu,\sigma^2\right)$ to denote a circularly symmetric complex-Gaussian distribution with a mean of μ and variance of σ^2.

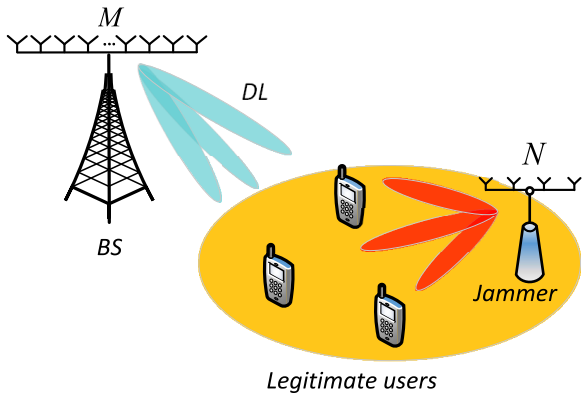

Fig. 1. Downlink transmission in massive MIMO systems against multi-antenna jammer.

II. System Model And Problem Formulations

A. System Model

We consider a downlink massive MIMO system consisting of K single-antenna users that are arbitrarily distributed over the coverage area. The BS and jammer are equipped with uniform linear arrays (ULA) with M and N elements, respectively, to implement BD transmissions. In order to design the jamming precoding, we assume that the jammer eavesdrops on the pilot signals in the uplink and obtains the CSI of jamming channels [16]. An illustration of the system is shown in Fig. 1. Based on the ray-tracing based narrowband model [45], [46], the downlink channel from BS to user k is[2]

$$\mathbf{h}_k = \frac{1}{\sqrt{L}}\sum_{l=1}^{L}\alpha_{k,l}\mathbf{a}\left(\theta_{k,l}\right), \tag{1}$$

where L is the number of paths, $\alpha_{k,l}$ is the complex gain distributed as $\alpha_{k,l}\sim\mathcal{N}_{\mathbb{C}}\left(0,\sigma_{k,l}^2\right)$. The steering vector $\mathbf{a}\left(\theta_{k,l}\right)$ for path l is

$$\mathbf{a}\left(\theta_{k,l}\right) = \left[1, e^{j\frac{2\pi d\cos\left(\theta_{k,l}\right)}{\lambda}}, \cdots, e^{j\frac{2\pi d(M-1)\cos\left(\theta_{k,l}\right)}{\lambda}}\right]^T, \tag{2}$$

where $\theta_{k,l}$ is the angle of departure (AOD) for path l, d is the antenna spacing, and λ is the wavelength. On the jammer side, a channel condition that is beneficial to the jammer is considered, where the jammer is elevated and a model similar to $\mathbf{h}_k$ is employed.[3] The jamming channel $\mathbf{g}_k\in\mathbb{C}^{N\times 1}$ from jammer to user k is

$$\mathbf{g}_k = \frac{1}{\sqrt{Q}}\sum_{q=1}^{Q}\beta_{k,q}\mathbf{a}\left(\omega_{k,q}\right), \tag{3}$$

[2]The model is simple as compared to the typical correlated Rayleigh fading model [47] but captures key characteristics and has an intuitive structure parameterizing the spatial sparsity by the direction of paths [48]. Therefore, the model is appropriate for both the line-of-sight (LoS) and NLoS cases and can be simply turned into other models, e.g., one-ring model [49] and ray-cluster based model [50].

[3]Compared to the model where the jammer is fixed on the ground, more spatial sparsity is obtained to help design the directional jamming that is more threatening and energy efficient [19], [51]. In addition, from the perspective of a smart jammer, it may not be a good idea to install the jammer in a rich-scattering place, since more transmission power will be consumed.

where Q is the number of jamming paths, $\omega_{k,q}$ is the AOD for path q, and the complex gain $\beta_{k,q}$ is distributed as $\beta_{k,q} \sim \mathcal{N}_{\mathbb{C}}\left(0, \sigma_{k,q,j}^2\right)$.

In massive MIMO systems with finite antenna elements, perfect orthogonality of the channels is unachievable. An alternative solution is to perform transmission in the BD [22]–[25]. The first step is to make a normalized discrete Fourier transform (DFT), i.e. $\tilde{\mathbf{h}}_k = \mathbf{F}\mathbf{h}_k$, where $\tilde{\mathbf{h}}_k$ is the BD expression of the channel and $\mathbf{F} \in \mathbb{C}^{M\times M}$ is the normalized DFT matrix with $\mathbf{F}_{p,g} = e^{-j\frac{2\pi}{M}(p-1)(q-1)}/\sqrt{M}$, $\forall p, q \in \{1, \cdots M\}$. Let $\text{asinc}_M(x) = \frac{\sin(M\pi x)}{M\sin(\pi x)}$ denote the aliased sinc function, and the m-th element of $\tilde{\mathbf{h}}_k$ is

$$\left(\tilde{\mathbf{h}}_k\right)_m = \sum_{l=1}^{L}\sqrt{\frac{M}{L}}\alpha_{k,l}e^{j\pi(M-1)\left[\frac{d}{\lambda}\cos\left(\theta_{k,l}\right)-\frac{m-1}{M}\right]} \times \text{asinc}_M\left(\frac{d}{\lambda}\cos\left(\theta_{k,l}\right) - \frac{m-1}{M}\right). \quad (4)$$

Under the conditions of $M \to \infty$, $\text{asinc}_M(x) \overset{M\to\infty}{\to} \delta(x)$, then we derive that for each path, $\tilde{\mathbf{h}}_k$ obtains a unique non-zero value when $m = 1 + \frac{Md}{\lambda}\cos\left(\theta_{k,l}\right), \forall l \in \{1, \cdots L\}$. Since the AODs of any two paths are different, $\tilde{\mathbf{h}}_k$ obtains the total L non-zero elements, and each beam index m points in the direction of a scattering path. In this paper, we define the set $\{B_k\}$ as the active beam set (ABS) of the downlink channel, which is given by $\{B_k\} \overset{M\to\infty}{\to} \left\{m \,|m = 1 + \frac{Md}{\lambda}\cos\left(\theta_{k,l}\right), \forall l \in \{1, \cdots, L\}\right\}$. However, in practice the number of antennas is large but finite, and for most cases, $\frac{Md}{\lambda}\cos\left(\theta_{k,l}\right)$ is not a integer, leading to power leakage in other DFT points [23]. To solve this issue, we relax the definition of the ABS by searching for the indexes meeting the following conditions:

$$\min_{\{B_k\}} |\{B_k\}| \quad s.t. \sum_{m\in\{B_k\}} \left|\left(\tilde{\mathbf{h}}_k\right)_m\right|^2 / \left\|\tilde{\mathbf{h}}_k\right\|^2 \geq \eta, \quad (5)$$

where η is the threshold of the approximation determined by the channel gain and thermal noise, which is generally $0.9 < \eta < 1$. Then, the BD channel is approximated as

$$\hat{\mathbf{h}}_k = \mathbf{F}\sum_{m\in\{B_k\}}\left(\tilde{\mathbf{h}}_k\right)_m \mathbf{f}_m^*. \quad (6)$$

Note that the perfect CSI is unknown and the minimum mean-square-error (MMSE) estimation of $\tilde{\mathbf{h}}_k$ is [52]

$$\tilde{\mathbf{h}}_k^{\text{MMSE}} = \mathbf{F}\mathbf{R}_k\left(\mathbf{R}_k + \frac{\sigma^2}{\tau p_\tau}\mathbf{I}\right)^{-1}\mathbf{y}_k^{pilot}, \quad (7)$$

where $\mathbf{R}_k \in \mathbb{C}^{M\times M}$ is the correlation matrix of the channel, and $\mathbf{y}_k^{pilot} = \mathbf{h}_k + \tau^{-1}p_\tau^{-1/2}\mathbf{N}_s\Xi_k^H$ is the least squares (LS) estimation of the channel involving the thermal noise $\mathbf{N}_s \in \mathbb{C}^{M\times\tau}$ and the pilot sequence $\Xi_k \in \mathbb{C}^{\tau\times 1}$. σ^2, τ and p_τ are the noise variance, length and symbol power of pilot sequences, respectively. Through the substitution of (7) into (6), $\hat{\mathbf{h}}_k$ is rewritten as $\hat{\mathbf{h}}_k = \mathbf{F}\sum_{m\in\{B_k\}}\left(\tilde{\mathbf{h}}_k^{\text{MMSE}}\right)_m \mathbf{f}_m^*$, and the error vector containing the estimation and approximation error is

$$\delta_k = \tilde{\mathbf{h}}_k - \hat{\mathbf{h}}_k, \quad \|\delta_k\| \leq \varepsilon_k. \quad (8)$$

In the same way, BD transmission is performed by a jammer. The ABS of the jamming channel is $\{J_k\}$, and the error vector is $\delta_{k,j} = \tilde{\mathbf{g}}_k - \hat{\mathbf{g}}_k$, $\|\delta_{k,j}\| \leq \nu_k$.

In this paper, we consider the game under two cases. In case 1, the ABSs of any two channels do not overlap; i.e., both $\{B_k\} \cap \{B_{k'}\} = \varnothing$ and $\{J_k\} \cap \{J_{k'}\} = \varnothing$ hold for $\forall k \neq k'$. Based on (6), we derive

$$\forall k \neq k', \quad \begin{cases}\hat{\mathbf{h}}_k^H\hat{\mathbf{h}}_{k'} = 0\\ \hat{\mathbf{g}}_k^H\hat{\mathbf{g}}_{k'} = 0.\end{cases} \quad (9)$$

This occurs when the directions of the users are non-overlapping. Usually, the AODs toward the users in the same cluster are correlated, and a grouping scheme assigning users from different clusters to a group is necessary to help realize the transmission in case 1. Typical grouping and precoding approaches have been investigated in [23], [24]. In contrast, $\{B_k\} \cap \{B_{k'}\} \neq \varnothing$ and $\{J_k\} \cap \{J_{k'}\} \neq \varnothing$, $\exists k \neq k'$ are considered in case 2. Similarly, the solutions applied for case 2, e.g, joint spatial division and multiplexing (JSDM) and hybrid beamforming, can be found in [22], [25], [47].

The downlink signal to user k is given by

$$y_k = \tilde{\mathbf{h}}_k^H\mathbf{s}_k x_k + \sum_{i=1,i\neq k}^{K}\tilde{\mathbf{h}}_k^H\mathbf{s}_i x_i + \sum_{i=1}^{K}\tilde{\mathbf{g}}_k^H\mathbf{w}_i u_i + n_k, \quad (10)$$

where $\mathbf{s}_k$ is the BD precoding vector at the BS with $\|\mathbf{s}_k\|^2 = p_k$, $\mathbf{w}_i$ is the jamming precoding vector with $\|\mathbf{w}_i\|^2 = p_{i,j}$, and $n_k \sim \mathcal{N}_{\mathbb{C}}\left(0, \sigma_k^2\right)$ is the thermal noise. Both the power of the downlink symbol x_i and jamming symbol u_i are normalized. Let $\mathbf{S} = [\mathbf{s}_1, \cdots, \mathbf{s}_K]$, $\mathbf{W} = [\mathbf{w}_1, \cdots, \mathbf{w}_K]$, then, the received SINR at user k is given by

$$\chi_k(\mathbf{S}, \mathbf{W}) = \frac{\left\|\tilde{\mathbf{h}}_k^H\mathbf{s}_k\right\|^2}{\sum_{i\neq k}\left\|\tilde{\mathbf{h}}_k^H\mathbf{s}_i\right\|^2 + \sum_{n=1}^{K}\left\|\tilde{\mathbf{g}}_k^H\mathbf{w}_n\right\|^2 + \sigma_k^2}. \quad (11)$$

Note that both the BS and jammer has incomplete information of (11). Specifically, the BS has no knowledge of the instantaneous jamming channel $\tilde{\mathbf{g}}_k$ and the precoding matrix $\mathbf{W}$. In contrast, the instantaneous downlink channel $\tilde{\mathbf{h}}_k$ and the precoding matrix $\mathbf{S}$ are unknown to the jammer.

B. Problem Formulation

We consider a smart jammer intending to interfere with signal reception with the desired EE. The strategy matrix is $\mathbf{W}$, and the EE for attacking user k is defined as

$$\Delta_k = \frac{\chi_k(\mathbf{S}, \mathbf{0}) - \chi_k(\mathbf{S}, \mathbf{W})}{\|\mathbf{w}_k\|^2}. \quad (12)$$

The transmission cost is denoted by $P_j = \|\mathbf{W}\|^2 = \sum_{k=1}^{K}\|\mathbf{w}_k\|^2$, and the utility function U_j is the inverse of P_j, i.e., $U_j P_j = 1$.

With the EE threshold γ_j, the optimization problem of the jammer is formulated as

$$\begin{aligned} &\min_{\mathbf{W}} \ P_j \\ &s.t. \ \Delta_k \geq \gamma_j \\ &\quad k = 1, 2, \cdots, K. \end{aligned} \tag{13}$$

For jamming defense, the tenacity of the downlink beamforming is considered. Specifically, a robust precoding should be designed with the goal of ensuring uninterrupted communication with users even under the worst conditions where $\mathbf{W}_j$ is optimized. Therefore, an anti-jamming Bayesian Stackelberg game is formulated. The jammer is assumed to be the follower and the BS is the leader. Assume that the downlink signals can be decoded successfully by users when the received SINR is no less than the minimum threshold γ_d. Then, the strategy for the BS is to design $\mathbf{S}$ thereby minimizing the cost of realizing $\chi_k(\mathbf{S}, \mathbf{W}) \geq \gamma_d$. The transmission cost is $P_d = \|\mathbf{S}\|^2 = \sum_{k=1}^{K} \|\mathbf{s}_k\|^2$, and the utility function is set to be $U_d = P_d^{-1}$. Let $\mathbf{W}^{\star}(\mathbf{S})$ be the solution of (13), which is a function of $\mathbf{S}$. Then the optimization problem is formulated as

$$\begin{aligned} &\min_{\mathbf{S}} \ P_d \\ &s.t. \ \chi_k\left(\mathbf{S}, \mathbf{W}^{\star}(\mathbf{S})\right) \geq \gamma_d \\ &\quad k = 1, 2, \cdots, K. \end{aligned} \tag{14}$$

III. Analysis of the Follower Subgame

Let $\mathbf{J}$ denote the problem (13). For the smart jammer, the challenge of solving $\mathbf{J}$ is two-fold. First, the configuration of $\mathbf{W}$ is unknown, and thus $\mathbf{J}$ is NP-hard [53]. Second, the jammer has no knowledge of either the CSI $\mathbf{h}_k$ or the strategy matrix $\mathbf{S}$ on the BS side. To make $\mathbf{J}$ feasible, we notice that when jamming users, it is unnecessary to focus on the inter-user interference caused by the power leakage of the precoding. Therefore, we refer to the typical matched filtering (MF) scheme and assume that the precoding model is

$$\mathbf{w}_k = \sqrt{p_{k,j}} \frac{\hat{\mathbf{g}}_k}{\left\|\hat{\mathbf{g}}_k\right\|}, \quad k = 1, 2 \cdots, K. \tag{15}$$

Then $\mathbf{J}$ is turned into a power optimization problem. Furthermore, we utilize the so-called use-and-then-forget method that is widely used in massive MIMO [48], i.e., $\tilde{\mathbf{h}}_k$ and $\mathbf{s}_k$ are known only during the process of solving $\mathbf{J}$. Let $d_k = \left\|\tilde{\mathbf{h}}_k^H \mathbf{s}_k\right\|^2$ and $m_k = \sum_{i \neq k} \left\|\tilde{\mathbf{h}}_k^H \mathbf{s}_i\right\|^2$ denote the desired signal and inter-user interference, respectively. Based on (11), the constrains in $\mathbf{J}$ are rewritten as

$$\begin{aligned} &\tilde{\mathbf{g}}_k^H \left[d_k - \gamma_j \left(m_k + \sigma_k^2\right) p_{k,j}\right] \left(\sum_{n=1}^{K} \mathbf{w}_n \mathbf{w}_n^H\right) \tilde{\mathbf{g}}_k \\ &\quad - \gamma_j \left(m_k + \sigma_k^2\right)^2 p_{k,j} \geq 0, \quad k = 1, 2, \cdots, K \end{aligned} \tag{16}$$

To simplify the expression, let $\mathbf{Y}_k = \left[d_k - \gamma_j \left(m_k + \sigma_k^2\right) p_{k,j}\right] \sum_{n=1}^{K} \mathbf{w}_n \mathbf{w}_n^H$, which is a Hermitian matrix, $c_k = \hat{\mathbf{g}}_k^H \mathbf{Y}_k \hat{\mathbf{g}}_k - \gamma_j \left(m_k + \sigma_k^2\right)^2 p_{k,j}$. Then, (16) is simplified to $\tilde{\mathbf{g}}_k^H \mathbf{Y}_k \tilde{\mathbf{g}}_k + c_k - \hat{\mathbf{g}}_k^H \mathbf{Y}_k \hat{\mathbf{g}}_k \geq 0$. Since $\tilde{\mathbf{g}}_k = \hat{\mathbf{g}}_k + \delta_{k,j}$, $\left\|\delta_{k,j}\right\| \leq \nu_k$, (16) is further reformulated as

$$\begin{aligned} &\begin{bmatrix} \delta_{k,j} \\ 1 \end{bmatrix}^H \begin{bmatrix} \mathbf{Y}_k & \mathbf{Y}_k \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H \mathbf{Y}_k & c_k \end{bmatrix} \begin{bmatrix} \delta_{k,j} \\ 1 \end{bmatrix} \geq 0 \\ &\quad \begin{bmatrix} \delta_{k,j} \\ 1 \end{bmatrix}^H \begin{bmatrix} -\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \nu_k^2 \end{bmatrix} \begin{bmatrix} \delta_{k,j} \\ 1 \end{bmatrix} \geq 0 \\ &\quad k = 1, 2 \cdots, K. \end{aligned} \tag{17}$$

Lemma 1: S-Procedure [54]: For n-order complex Hermitian matrices $\mathbf{A}, \mathbf{B}$*, complex vectors* $\mathbf{a}_1 \in \mathbb{C}^{n \times 1}, \mathbf{b}_1 \in \mathbb{C}^{n \times 1}$*, and* $a_2, b_2 \in \mathbb{R}$*, define* $f_A(\mathbf{x})$ *and* $f_B(\mathbf{x})$ *as*

$$\begin{aligned} f_A(\mathbf{x}) &= \begin{bmatrix} \mathbf{x} \\ 1 \end{bmatrix}^H \begin{bmatrix} \mathbf{A} & \mathbf{a}_1 \\ \mathbf{a}_1^H & a_2 \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ 1 \end{bmatrix} \\ f_B(\mathbf{x}) &= \begin{bmatrix} \mathbf{x} \\ 1 \end{bmatrix}^H \begin{bmatrix} \mathbf{B} & \mathbf{b}_1 \\ \mathbf{b}_1^H & b_2 \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ 1 \end{bmatrix} \end{aligned} \tag{18}$$

When $f_A(\mathbf{x}) \geq 0$*, the condition* $f_B(\mathbf{x}) \geq \rho f_A(\mathbf{x}) \geq 0$ *holds true if and only if*

$$\begin{bmatrix} \mathbf{B} & \mathbf{b}_1 \\ \mathbf{b}_1^H & b_2 \end{bmatrix} - \rho \begin{bmatrix} \mathbf{A} & \mathbf{a}_1 \\ \mathbf{a}_1^H & a_2 \end{bmatrix} \succcurlyeq \mathbf{0}, \tag{19}$$

where $\rho \geq 0$.

Based on *Lemma 1*, the constrains (17) is equivalent to

$$\begin{bmatrix} \mathbf{Y}_k + \rho_k \mathbf{I} & \mathbf{Y}_k \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H \mathbf{Y}_k & c_k - \rho_k \nu_k^2 \end{bmatrix} \succcurlyeq 0, \tag{20}$$

where $\rho_k \geq 0$. Let $\{\rho_k\}$ denote the set of $\rho_k, \forall k \in \{1, \cdots K\}$. Then, $\mathbf{J}$ can be equivalently modeled as

J-E:

$$\begin{aligned} &\min_{\mathbf{W}, \{\rho_k\}} \sum_{k=1}^{K} Tr(\mathbf{W}_k) \\ &s.t. \ \begin{bmatrix} \mathbf{Y}_k + \rho_k \mathbf{I} & \mathbf{Y}_k \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H \mathbf{Y}_k & c_k - \rho_k \nu_k^2 \end{bmatrix} \succcurlyeq 0 \\ &\quad \mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H \\ &\quad \rho_k \geq 0, \quad k = 1, 2, \cdots, K \end{aligned} \tag{21}$$

A. Case 1

In case 1, $\{J_k\} \cap \{J_{k'}\} = \varnothing$ holds for $\forall k \neq k'$. Based on (9) and (15), we derive that for $\forall k \in \{1, \cdots, K\}$, $\mathbf{w}_k / \sqrt{p_{k,j}}$ is the eigenvector of $\mathbf{Y}_k$, which spans the subspace $\mathbf{W}_k$. Thus $Rank(\mathbf{W}_k) = 1$, and the equality constrains in (21) can be simplified to $\mathbf{W}_k \succcurlyeq \mathbf{0}$. Moreover, $\rho_k > 0$ holds for $\forall k \in \{1, \cdots, K\}$, which can be proven from the contradiction. Specifically, we assume that there exists $\rho_k = 0$ for some k. By left and right multiplying both sides of (20) by $\left[-\hat{\mathbf{g}}_k^H \ 1\right]$ and $\left[-\hat{\mathbf{g}}_k^H \ 1\right]^H$, we have

$$-\gamma_j \left(m_k + \sigma_k^2\right)^2 p_{k,j} > 0, \tag{22}$$

which is not true. Therefore, $\rho_k > 0$ holds for $\forall k \in \{1, \cdots, K\}$.

Based on this finding, **J-E** is turned into a semi-definite programming (SDP) problem and can be solved with CVX tools [53]. However, the numerical solution does not help

explain the interaction between the BS and jammer. Thereby, a solution in a closed-form is needed. To solve this issue, we refer to the beamforming optimization method intended for a typical massive MIMO system in [24], and use Lemma 2 to simplify the matrix optimization to a standard convex optimization of the jamming power.

Lemma 2: Generalized Schur's Complement [55]: Let $\mathbf{M} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^H & \mathbf{C} \end{bmatrix}$ *denote a Hermitian matrix.* $\mathbf{M} \succcurlyeq \mathbf{0}$ *holds true if and only if the following conditions stand*:

$$(i)\ \ \mathbf{C} - \mathbf{B}^H \mathbf{A}^\dagger \mathbf{B} \succcurlyeq \mathbf{0}$$
$$(ii)\ \ \left(\mathbf{I} - \mathbf{A}\mathbf{A}^\dagger\right)\mathbf{B} = \mathbf{0}$$
$$(iii)\ \ \mathbf{A} \succcurlyeq \mathbf{0}$$

Based on Lemma 2, the semi-definite constrain (20) is decomposed into

$$c_k - \rho_k v_k^2 - \hat{\mathbf{g}}_k^H \mathbf{Y}_k (\mathbf{Y}_k + \rho_k \mathbf{I})^\dagger \mathbf{Y}_k \hat{\mathbf{g}}_k \succcurlyeq 0 \tag{23}$$
$$\left[\mathbf{I} - (\mathbf{Y}_k + \rho_k \mathbf{I})(\mathbf{Y}_k + \rho_k \mathbf{I})^\dagger\right] \mathbf{Y}_k \hat{\mathbf{g}}_k = \mathbf{0} \tag{24}$$
$$\mathbf{Y}_k + \rho_k \mathbf{I} \succcurlyeq 0. \tag{25}$$

Note that (24) is guaranteed when (25) holds true. To simplify the problem, we may first assume that (25) holds, and later verify the solution under this constrain. We define the eigenvalue decomposition (EVD) of $\mathbf{Y}_k$ as

$$\begin{aligned} \mathbf{Y}_k &= \xi_k \mathbf{U}_j \mathbf{\Lambda}_j \mathbf{U}_j^H, \\ \mathbf{\Lambda}_j &= diag\left(\underbrace{p_{1,j}, \cdots, p_{K,j}}_{K}, \underbrace{0, \cdots, 0}_{N-K}\right), \\ \mathbf{U}_j &= \left[\frac{\mathbf{w}_1}{\sqrt{p_{1,j}}}, \cdots, \frac{\mathbf{w}_K}{\sqrt{p_{K,j}}}, \mathbf{u}_{K+1,j}, \cdots \mathbf{u}_{N,j}\right], \\ \xi_k &= d_k - \gamma_j \left(m_k + \sigma_k^2\right) p_{k,j}. \end{aligned} \tag{26}$$

Through the substitution of (26) into (23), the semi-definite constrain (20) is relaxed to

$$\frac{\xi_k p_{k,j} \rho_k}{\xi_k p_{k,j} + \rho_k} \left\|\hat{\mathbf{g}}_k\right\|^2 - \gamma_j \left(m_k + \sigma_k^2\right)^2 p_{k,j} - \rho_k v_k^2 \geq 0. \tag{27}$$

Let $\left\{p_{k,j}\right\}$ denote the set of the jamming power. Then **J-E** is simplified to

J1:

$$\begin{aligned} \min_{\{p_{k,j}\},\{\rho_k\}} \ & Tr\left(\mathbf{\Lambda}_j\right) \\ s.t.\ & \frac{\xi_k p_{k,j} \rho_k}{\xi_k p_{k,j} + \rho_k} \left\|\hat{\mathbf{g}}_k\right\|^2 \\ & - \gamma_j \left(m_k + \sigma_k^2\right)^2 p_{k,j} - \rho_k v_k^2 \geq 0 \\ & \rho_k > 0,\ \ p_{k,j} > 0,\ \ k = 1, 2, \cdots, K. \end{aligned} \tag{28}$$

Theorem 1: In case 1, the following must be true.

(a) ***J1*** *is convex. The Karush-Kuhn-Tucker (KKT) solution is*

$$p_{k,j}^\star = \frac{d_k}{\left(m_k + \sigma_k^2\right)\gamma_j} - \frac{m_k + \sigma_k^2}{\left(\left\|\hat{\mathbf{g}}_k\right\| - v_k\right)^2}; \tag{29}$$

(b) The optimal solution of ***J1*** *and* ***J-E*** *is*

$$\begin{aligned} \left[\mathbf{W}^\star(\mathbf{S})\right]_{,k} &= \mathbf{w}_k^\star \\ &= \sqrt{p_{k,j}^\star} \frac{\hat{\mathbf{g}}_k}{\left\|\hat{\mathbf{g}}_k\right\|}, \quad k = 1, \cdots, K. \end{aligned} \tag{30}$$

Proof: See Appendix A. ∎

According to *Theorem 1*, a proper γ_j should be selected to ensure $p_{k,j}^\star > 0$. When trying to enhance the EE of the jammer, the infeasibility probability of **J1** is increased. We notice that although $p_{k,j}^\star$ is obtained, the optimal solution is still infeasible for practical implementation, since the jammer has no knowledge of d_k and m_k, both of which are determined by the CSI $\mathbf{h}_k$ and strategy matrix $\mathbf{S}$ on the BS side. Instead, we consider the upper bound of (29). On the one hand, $p_{k,j}^\star$ is the decreasing function of m_k;Then, $p_{k,j}^\star$ obtains the maximal value when $m_k = 0$, which implies that more power is consumed at the jammer when the inter-user interference caused by $\mathbf{S}$ is eliminated. On the other hand, we derive from the Cauchy-Schwarz inequality that $d_k = \left\|\tilde{\mathbf{h}}_k^H \mathbf{s}_k\right\|^2 \leq p_k \left\|\tilde{\mathbf{h}}_k\right\|^2$. Then we derive $p_{k,j}^\star \leq \frac{p_k \left\|\tilde{\mathbf{h}}_k\right\|^2}{\sigma_k^2 \gamma_j} - \frac{\sigma_k^2}{\left(\left\|\hat{\mathbf{g}}_k\right\| - v_k\right)^2}$. Moreover, the statistical CSI $\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}$ is obtained to replace the instantaneous gain $\left\|\tilde{\mathbf{h}}_k\right\|^2$.

Proposition 1: The expectation of $\left\|\tilde{\mathbf{h}}_k\right\|^2$ *is*

$$\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\} = \sum_{m=1}^{M} \sum_{l=1}^{L} \frac{M \sigma_{k,l}^2}{L} \operatorname{asinc}_M^2 \left(\frac{d}{\lambda} \cos\theta_{k,l} - \frac{m-1}{M}\right). \tag{31}$$

Proof: The m-th element of $\tilde{\mathbf{h}}_k$ is given by (4). Due to the circular symmetry of the complex gain distributed as $\alpha_{k,l} \sim \mathcal{N}_{\mathbb{C}}\left(0, \sigma_{k,l}^2\right), \forall l \in \{1, \cdots, L\}$, the BD complex gain of the m-th element for path l is distributed as $\mathcal{N}_{\mathbb{C}}\left(0, \sigma_{k,l,BD}^2\right)$, where $\sigma_{k,l,BD} = \sqrt{\frac{M}{L}} \sigma_{k,l} \operatorname{asinc}_M\left(\frac{d}{\lambda}\cos\theta_{k,l} - \frac{m-1}{M}\right)$. Based on the independence among paths, we derive $\left(\tilde{h}_k\right)_m \sim \mathcal{N}_{\mathbb{C}}\left(0, \sum_{l=1}^{L} \sigma_{k,l,BD}^2\right)$. Then (31) is verified. ∎

According to *Proposition 1*, the statistical CSI of the user channel is mainly determined by three factors, i.e., the antenna number of the BS, the direction of the BS-user channel, and the path loss determined by the transmission distance, all of which can be pre-obtained by the jammer. Specifically, taking the jammer as the coordinate origin and the line between the BS and jammer as the coordinate axis, the mean direction of the jammer-user channel can be obtained by using ULA based phase rotation schemes [25] or typical direction estimation methods, such as multiple signal classification (MUSIC) algorithm [56] and the estimation of signal parameters via rotational invariance techniques (ESPRIT) algorithm [57]. Meanwhile, the distance from the BS/user to the jammer can be measured by using the signal strength. Based on this, the geometric method, e.g., the law of cosines, can be used

to estimate the direction and distance from the BS to user k. Then, (31) can be obtained by the jammer.

Let $\hat{p}_k$ denote the estimation of $\|\mathbf{s}_k\|^2$; then, the feasible solution of $\mathbf{J}$ is

$$p_{k,j}^{\star} = \left(\frac{\hat{p}_k \mathbb{E}\left\{ \left\| \tilde{\mathbf{h}}_k \right\|^2 \right\}}{\sigma_k^2 \gamma_j} - \frac{\sigma_k^2}{\left(\left\| \hat{\mathbf{g}}_k \right\| - \nu_k \right)^2} \right)^+, \tag{32}$$

where $(\cdot)^+ \triangleq \max(\cdot, 0)$.

B. Case 2

In case 2, the orthogonality of the BD channels no longer holds for $\forall k \neq k'$. Instead, $\{J_k\} \cap \{J_{k'}\} \neq \varnothing, \exists k' \neq k$ is considered. Without loss of generality, we assume that there exists $\{J_1\} \cap \{J_2\} \neq \varnothing$, s.t. $\hat{\mathbf{g}}_1^H \hat{\mathbf{g}}_2 \neq 0$, whereas the orthogonality shown in (9) holds for $\forall k \neq k', k, k' \in \{1, 3, \cdots, K\}$ and $k, k' \in \{2, 3, \cdots, K\}$.

In this case, the EVD of $\mathbf{Y}_k$ is given by $\mathbf{Y}_k = \mathbf{U}_j \mathbf{\Lambda}_{k,j} \mathbf{U}_j^H$, where $\mathbf{U}_j = \left[\mathbf{u}_{1,j}, \cdots, \mathbf{u}_{N,j} \right]$ is the eigenmatrix and $\mathbf{\Lambda}_{k,j} = diag\left(q_{k,1}, \cdots, q_{k,N} \right)$ is the eigenvalue matrix. Based on *Lemma 2*, (23)-(25) still hold, where (23) is rewritten as

$$\rho_k \sum_{i=1}^{N} \frac{q_{k,i}}{q_{k,i} + \rho_k} \left| \hat{\mathbf{g}}_k^H \mathbf{u}_{i,j} \right|^2 - \gamma_j \left(m_k + \sigma_k^2 \right)^2 p_{k,j} - \rho_k \nu_k^2 \geq 0. \tag{33}$$

Since both $q_{k,i}$ and $\mathbf{u}_{i,j}$ are unknown to the jammer, meanwhile the equality constrain $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$ involves the non-convex rank-one constrain, i.e., $Rank\left(\mathbf{W}_k\right) = 1$, **J-E** is NP-hard. We notice that $\{J_1\} \cap \{J_2\} \neq \varnothing$ indicates the angular correlation between $\hat{\mathbf{g}}_1$ and $\hat{\mathbf{g}}_2$. Inspired by the JSDM scheme in [47], we assign these two users into a group whose external CSI is $\hat{\mathbf{g}}_{sum} = \hat{\mathbf{g}}_1 + \hat{\mathbf{g}}_2$. Then, the precoding model is denoted by

$$\mathbf{w}_k = \begin{cases} \sqrt{p_{k,j}} \dfrac{\hat{\mathbf{g}}_{sum}}{\left\| \hat{\mathbf{g}}_{sum} \right\|}, \forall k \in \{1, 2\} \\ \sqrt{p_{k,j}} \dfrac{\hat{\mathbf{g}}_k}{\left\| \hat{\mathbf{g}}_k \right\|}, \forall k \in \{3, \cdots, K\} \end{cases}. \tag{34}$$

Since $\hat{\mathbf{g}}_{sum}^H \hat{\mathbf{g}}_k = 0$ holds for $\forall k \in \{3 \cdots K\}$, the normalized version of (34) acts as the eigenvector of $\mathbf{Y}_k$, which spans the positive semi-definite subspace $\mathbf{W}_k$. Thus, the grouping based optimization problem in case 2 is turned into the SDP problem in case 1, and can be solved by taking similar steps. Under this condition, **J-E** is rewritten as

J2:

$$\min_{\{p_{k,j}\}, \{\rho_k\}} \sum_{k=1}^{K} p_{k,j}$$

$$s.t.\ c_1 : \frac{\rho_k \xi_k \sum_{i=1}^{2} p_{i,j}}{\xi_k \sum_{i=1}^{2} p_{i,j} + \rho_k} \left| \hat{\mathbf{g}}_k^H \hat{\mathbf{g}}_{sum} \right|^2 / \left\| \hat{\mathbf{g}}_{sum} \right\|^2 - \gamma_j p_{k,j} \left(m_k + \sigma_k^2 \right)^2 - \rho_k \nu_k^2 \geq 0, \quad \forall k \in \{1, 2\}$$

$$c_2 : \frac{\rho_k \xi_k p_{k,j}}{\xi_k p_{k,j} + \rho_k} \left\| \hat{\mathbf{g}}_k \right\|^2 - \rho_k \nu_k^2 - \gamma_j p_{k,j} \left(m_k + \sigma_k^2 \right)^2 \geq 0, \quad \forall k \in \{3, \cdots, K\}$$

$$c_3 : \rho_k > 0, \ p_{k,j} > 0, \quad \forall k \in \{1, \cdots, K\} \tag{35}$$

Similarly, **J2** is convex and the KKT solution is

$$p_{k,j}^{\star} = \begin{cases} \dfrac{d_1}{\left(m_1 + \sigma_1^2 \right) \gamma_j} - \dfrac{m_1 + \sigma_1^2}{(1 + \psi) \left(\frac{\left| \hat{\mathbf{g}}_1^H \hat{\mathbf{g}}_{sum} \right|}{\left\| \hat{\mathbf{g}}_{sum} \right\|} - \nu_1 \right)^2}, k = 1 \\ \psi p_{1,j}^{\star}, k = 2 \\ \dfrac{d_k}{\left(m_k + \sigma_k^2 \right) \gamma_j} - \dfrac{m_k + \sigma_k^2}{\left(\left\| \hat{\mathbf{g}}_k \right\| - \nu_k \right)^2}, \forall k \in \{3, \cdots, K\}, \end{cases} \tag{36}$$

where $\psi > 0$ is the factor determined by

$$\frac{\psi}{1 + \psi} = \left[\frac{d_2}{\gamma_j \left(m_2 + \sigma_2^2 \right)^2} - \frac{\beta p_{1,j}^{\star}}{\left(m_2 + \sigma_2^2 \right)} \right] (r_2 - \nu_2)^2, \tag{37}$$

and $r_2 = \left| \hat{\mathbf{g}}_2^H \hat{\mathbf{g}}_{sum} \right|^2 \left\| \hat{\mathbf{g}}_{sum} \right\|^{-2}$. It is shown that for $\forall k \in \{3, \cdots, K\}$, the optimal power solution in case 2 is the same as that in case 1; thus, (32) also provides a feasible solution for **J2**. $p_{1,j}^{\star}$ and $p_{2,j}^{\star}$, however, are infeasible for practical implementation. One reason is that ψ cannot be obtained by solving (37), which requires an unknown CSI and precoding matrix on the BS side. Another is that $p_{1,j}^{\star}$ and $p_{2,j}^{\star}$ are increasing functions of ψ, and the asymptotic case occurs when $p_{1,j}^{\star} \overset{\psi \to \infty}{\to} d_1 \left(m_1 + \sigma_1^2 \right)^{-1} \gamma_j^{-1}$, $p_{2,j}^{\star} \overset{\psi \to \infty}{\to} \infty$. It is impossible to obtain a relaxed and feasible solution by dropping ψ. Therefore, from a game point of view, a tradeoff should be made between the feasibility and optimality.

IV. Analysis of the Leader SubGame

Let $\mathbf{P}$ denote the problem (14). The main challenge of solving $\mathbf{P}$ is two-fold. First, $\mathbf{W}^{\star}(\mathbf{S})$ is a function of $\mathbf{S}$, and the optimal jamming power varies with the change in the precoding at the BS. Therefore, an equilibrium of the game should be found. Second, the BS has no knowledge of the jamming channel $\tilde{\mathbf{g}}_k$ or the strategy matrix $\mathbf{W}^{\star}(\mathbf{S})$ on the jammer side. To make $\mathbf{P}$ solvable, we adopt the use-and-then forget solution again; i.e., $\tilde{\mathbf{g}}_k$ and $p_{k,j}^{\star}$ are only known during the process of solving $\mathbf{P}$. We show that the generalized ZF precoding is the optimal anti-jamming precoding model for both cases and that a specific solution in closed form that constitutes the SE together with $\mathbf{W}^{\star}(\mathbf{S})$ can be obtained in case 1.

By substituting (30) into (14), we rewrite the constrains of $\mathbf{P}$ as

$$\tilde{\mathbf{h}}_k^H \left(\frac{\mathbf{S}_k}{\gamma_d} - \sum_{\substack{i=1 \\ i \neq k}}^{K} \mathbf{S}_i \right) \tilde{\mathbf{h}}_k - \sigma_k^2 - \sum_{n=1}^{K} l_{k,n} p_{n,j}^{\star} \geq 0 - \delta_k^H \delta_k + \varepsilon_k^2 \geq 0, \ \forall k \in \{1, \cdots, K\}, \tag{38}$$

where $\mathbf{S}_k$ is the subspace spanned by $\mathbf{S}_k = \mathbf{s}_k\mathbf{s}_k^H$, $l_{k,n} = \left(\frac{\tilde{\mathbf{g}}_k^H\hat{\mathbf{g}}_n}{\|\hat{\mathbf{g}}_n\|}\right)^2$. For simplicity, let $\mathbf{X}_k = \mathbf{S}_k\gamma_d^{-1} - \sum_{i\neq k}\mathbf{S}_i$, $I_k = \sum_{n=1}^{K} l_{k,n}p_{n,j}^{\star}$. Based on *Lemma 1*, (38) is equivalent to

$$\begin{bmatrix} \mathbf{X}_k + \mu_k\mathbf{I} & \mathbf{X}_k\hat{\mathbf{h}}_k \\ \hat{\mathbf{h}}_k^H\mathbf{X}_k & \hat{\mathbf{h}}_k^H\mathbf{X}_k\hat{\mathbf{h}}_k - \sigma_k^2 - I_k - \mu_k\varepsilon_k^2 \end{bmatrix} \succcurlyeq \mathbf{0}, \quad (39)$$

where $\mu_k \geq 0$. Let $\{\mu_k\}$ denote the set of $\mu_k, \forall k \in \{1, \cdots K\}$; then, $\mathbf{P}$ is transformed to

P-E:

$$\begin{aligned} \min_{\mathbf{S},\{\mu_k\}} \ & \sum_{k=1}^{K} Tr\left(\mathbf{S}_k\right) \\ s.t. \ & \begin{bmatrix} \mathbf{X}_k + \mu_k\mathbf{I} & \mathbf{X}_k\hat{\mathbf{h}}_k \\ \hat{\mathbf{h}}_k^H\mathbf{X}_k & \hat{\mathbf{h}}_k^H\mathbf{X}_k\hat{\mathbf{h}}_k - \sigma_k^2 - I_k - \mu_k\varepsilon_k^2 \end{bmatrix} \succcurlyeq \mathbf{0} \\ & \mathbf{S}_k = \mathbf{s}_k\mathbf{s}_k^H \\ & \mu_k \geq 0, \quad \forall k \in \{1, \cdots K\} \end{aligned} \quad (40)$$

Note that the equality constrain in (40) is composed of (a) $\mathbf{S}_k \succcurlyeq \mathbf{0}$ and (b) $Rank\left(\mathbf{S}_k\right) = 1$. **P-E** is NP-hard.

Theorem 2: Let $\hat{\mathbf{H}} = \left[\hat{\mathbf{h}}_1, \cdots, \hat{\mathbf{h}}_K\right]$. *The solution of* ***P-E*** *is denoted by* $\mathbf{S}^{\star} = \left[\mathbf{s}_1^{\star}, \cdots, \mathbf{s}_K^{\star}\right]$, $\left\|\mathbf{s}_k^{\star}\right\|^2 = p_k^{\star}, \forall k \in \{1, \cdots K\}$. *When* ***P-E*** *is feasible, we must have*

$$\mathbf{s}_k^{\star} = \sqrt{p_k^{\star}}\frac{\hat{\mathbf{H}}\left(\hat{\mathbf{H}}^H\hat{\mathbf{H}}\right)^{-1}_{,k}}{\sqrt{\left(\hat{\mathbf{H}}^H\hat{\mathbf{H}}\right)^{-1}_{k,k}}}, \quad \forall k \in \{1, \cdots, K\}. \quad (41)$$

Proof: See Appendix B. ∎

Theorem 2 shows that the generalized ZF is the optimal configuration for jamming defense in both cases. Interestingly, similar results were found in [24] and [10], where the regularized ZF (RZF) is optimal for jamming resistance in uplink massive MIMO systems [10] and the typical ZF-type precoding is optimal for robust beamforming in downlink beam division multiple access (BDMA) massive MIMO systems without malicious attack [24]. Note that *Theorem 2* expands the results to a more complex scenario and (41) is a necessary condition of $\mathbf{s}_k^{\star}$ but not sufficient. The transmission power should be optimized for both cases.

A. Case 1

In case 1, $\{B_k\} \cap \{B_{k'}\} = \varnothing$ holds for $\forall k \neq k'$. Due to the orthogonality of the BD channels, (41) can be simplified to $\mathbf{s}_k^{\star} = \sqrt{p_k^{\star}}\frac{\hat{\mathbf{h}}_k}{\|\hat{\mathbf{h}}_k\|}, \forall k \in \{1, \cdots, K\}$. We notice that $\mathbf{s}_k^{\star}$ has the same model as that of the jamming precoding and that for $\forall k \in \{1, \cdots, K\}$, $\mathbf{u}_k = \mathbf{s}_k^{\star}/\sqrt{p_k^{\star}}$ is the eigenvector of $\mathbf{X}_k$, which spans the subspace $\mathbf{S}_k$.[4] Since $\mathbf{X}_k = \mathbf{S}_k\gamma_d^{-1} - \sum_{i\neq k}\mathbf{S}_i$, the EVD of $\mathbf{X}_k$ is given by

$$\begin{aligned} \mathbf{X}_k &= \mathbf{U}_k\mathbf{\Lambda}_k\mathbf{U}_k^H, \\ \mathbf{U}_k &= \left[\mathbf{u}_k, \mathbf{u}_1, \cdots, \mathbf{u}_{k-1}, \mathbf{u}_{k+1}, \cdots, \mathbf{u}_M\right], \\ \mathbf{\Lambda}_k &= diag\left(\frac{p_k^{\star}}{\gamma_d}, -p_1^{\star}, \cdots, -p_{k-1}^{\star}, -p_{k+1}^{\star}, \cdots, \mathbf{0}_{M-K}^T\right). \end{aligned} \quad (42)$$

Based on *Lemma 2*, the semi-definite constrain (39) is decomposed into

$$\hat{\mathbf{h}}_k^H\mathbf{X}_k\hat{\mathbf{h}}_k - \sigma_k^2 - I_k - \mu_k\varepsilon_k^2 - \hat{\mathbf{h}}_k^H\mathbf{X}_k\left(\mathbf{X}_k + \mu_k\mathbf{I}\right)^{\dagger}\mathbf{X}_k\hat{\mathbf{h}}_k \geq 0, \quad (43)$$

$$\left[\mathbf{I} - \left(\mathbf{X}_k + \mu_k\right)\left(\mathbf{X}_k + \mu_k\right)^{\dagger}\right]\mathbf{X}_k\hat{\mathbf{h}}_k = \mathbf{0}, \quad (44)$$

$$\mathbf{X}_k + \mu_k\mathbf{I} \succcurlyeq \mathbf{0}, \quad (45)$$

where (44) is guaranteed when (45) holds true. Similar to the steps of solving *J-E*, we first drop (45) and later verify the solution under this constrain. By substituting (32) and (42) into (43), we relax the semi-definite constrain (39) to

$$\begin{aligned} &\frac{\mu_k p_k^{\star}}{p_k^{\star} + \gamma_d\mu_k}\left\|\hat{\mathbf{h}}_k\right\|^2 - \sigma_k^2 - \mu_k\varepsilon_k^2 \\ &\quad - \sum_{n=1}^{K} l_{k,n}\left(\frac{p_n^{\star}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_n\right\|^2\right\}}{\sigma_n^2\gamma_j} - \frac{\sigma_n^2}{\left(\left\|\hat{\mathbf{g}}_n\right\| - \nu_n\right)^2}\right) \geq 0. \end{aligned} \quad (46)$$

We derive from (46) that $\mu_k > 0$ since $\mu_k = 0$ leads to a negative value on the left side of (46). Furthermore, the Hessian matrix of (46) is $\frac{-2\gamma_d}{\left(p_k^{\star}+\gamma_d\mu_k\right)^3}\left[-p_k^{\star}, \mu_k\right]^H\left[-p_k^{\star}, \mu_k\right] \prec \mathbf{0}$; thus, (46) is concave. Then, **P-E** is transformed into a convex optimization problem as follows:

P1:

$$\begin{aligned} \min_{\{\mu_k\},\{p_k^{\star}\}} \ & \sum_{k=1}^{K} p_k^{\star} \\ s.t. \ & \frac{\mu_k p_k^{\star}}{p_k^{\star} + \gamma_d\mu_k}\left\|\hat{\mathbf{h}}_k\right\|^2 - \sigma_k^2 - \mu_k\varepsilon_k^2 \\ & \quad - \sum_{n=1}^{K} l_{k,n}\left(\frac{p_n^{\star}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_n\right\|^2\right\}}{\sigma_n^2\gamma_j} - \frac{\sigma_n^2}{\left(\left\|\hat{\mathbf{g}}_n\right\| - \nu_n\right)^2}\right) \geq 0 \\ & \mu_k > 0, \ p_k^{\star} > 0, \quad k = 1, 2\cdots, K. \end{aligned} \quad (47)$$

The KKT solution of **P1** is given by

$$p_k^{\star} = \frac{\sigma_k^4\gamma_d\gamma_j}{\left(\left\|\hat{\mathbf{g}}_k\right\| - \nu_k\right)^2}\frac{\vartheta_{k,j}}{\vartheta_k}, \quad (48)$$

where $\vartheta_k = \left(\left\|\hat{\mathbf{h}}_k\right\| - \varepsilon_k\right)^2\sigma_k^2\gamma_j - \sum_{n=1}^{K} l_{n,k}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}\gamma_d$, $\vartheta_{k,j} = \left(\left\|\hat{\mathbf{g}}_k\right\| - \nu_k\right)^2 - \sum_{n=1}^{K} l_{n,k}$. The steps of solving **P1** are given in Appendix C. Note that $l_{n,k}|_{n=k} = \left\|\hat{\mathbf{g}}_k\right\|^2 > \left(\left\|\hat{\mathbf{g}}_k\right\| - \nu_k\right)^2$ leads to $\vartheta_{k,j} < 0$. To make $p_k^{\star} > 0$, we must

[4] In this case, the generalized ZF precoding is equivalent to the MF scheme, and the performance of the precoding is mainly determined by the BD channel approximation error.

have $\vartheta_k < 0$, i.e., $\frac{\gamma_d}{\gamma_j} > \frac{\left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)^2\sigma_k^2}{\sum_{n=1}^{K} l_{n,k}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}}$. Additionally, we recall from (32) that the positive constrain of $p_{k,j}^{\star}$ is $p_k^{\star} > \frac{\sigma_k^4\gamma_j}{\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}\left(\|\hat{\mathbf{g}}_k\|-\nu_k\right)^2}$, which can be rewritten as $\frac{\gamma_d}{\gamma_j} < \frac{\left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)^2\sigma_k^2}{\left(\|\hat{\mathbf{g}}_k\|-\nu_k\right)^2\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}}$ with the help of (48). Then we derive

$$\frac{\left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)^2\sigma_k^2}{\sum_{n=1}^{K} l_{n,k}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}} < \frac{\gamma_d}{\gamma_j} < \frac{\left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)^2\sigma_k^2}{\left(\|\hat{\mathbf{g}}_k\|-\nu_k\right)^2\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}}. \quad (49)$$

This indicates that proper thresholds must be chosen by both the BS and jammer to match the channel sparsity and thus ensure positive solutions. Otherwise, **P1** and **J1** will be infeasible.

Now, we verify the solution under the constrain (45). Substituting (42) into (45), we derive $\mu_k \geq p_i^{\star}, \forall i \neq k$, which can be rewritten as $\frac{p_k^{\star}}{p_i^{\star}} \geq \frac{\varepsilon_k\gamma_d}{\left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)}, \forall i \neq k$ with the help of (80). Similarly, $\frac{p_i^{\star}}{p_k^{\star}} \geq \frac{\varepsilon_i\gamma_d}{\left(\left\|\hat{\mathbf{h}}_i\right\|-\varepsilon_i\right)}$ can be obtained. Therefore, the solution is subject to constrain (45) if, and only if, $\gamma_d^2 \leq \frac{\left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)\left(\left\|\hat{\mathbf{h}}_i\right\|-\varepsilon_i\right)}{\varepsilon_k\varepsilon_i}, \forall i \neq k$. This can be guaranteed because both the communication threshold γ_d and the channel approximation error ε_k are under the control of the BS.

As we mentioned in the beginning of this section, the information of the jamming channel involving $\left\|\hat{\mathbf{g}}_k\right\|$ and ν_k is unknown to the BS; thus, the ideal solution (48) is infeasible in practice. To solve this issue, we consider the worst condition where $p_k^{\star}$ is maximized. Let $L_k = \sum_{n=1}^{K} l_{n,k}$ denote the interference from jammer to user k. The derivation of (48) with respect to L_k is given by

$$\frac{\partial p_k^{\star}}{\partial\left(L_k\right)} = \frac{\gamma_d\gamma_j\sigma_k^4}{\left(\left\|\hat{\mathbf{g}}_k\right\|-\nu_k\right)^2\vartheta_k^2} \cdot\left[\left(\left\|\hat{\mathbf{g}}_k\right\|-\nu_k\right)^2\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}\gamma_d - \left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)^2\sigma_k^2\gamma_j\right]. \quad (50)$$

Substituting (49) into (50), we derive $\frac{\partial p_k^{\star}}{\partial(L_k)} < 0, \forall k \in \{1,\cdots,K\}$, and $p_k^{\star}$ is a decreasing function of L_k. Therefore, the first step of turning (48) into a feasible solution is constructing min $L_k = l_{k,k} = \left\|\hat{\mathbf{g}}_k\right\|^2$ to obtain the maximum power. Then, we recall from (6), (7) and (8) that $\hat{\mathbf{g}}_k^H\delta_{k,j} \approx 0, \forall k \in \{1,\cdots,K\}$, and the perfect orthogonality holds when the estimation error of the jamming channel is eliminated. Usually, this is negligible in BD massive MIMO transmission compared to the artificial channel approximation error (8). For simplicity, we assume that $\hat{\mathbf{g}}_k^H\delta_{k,j}=0, \forall k \in \{1,\cdots,K\}$, which leads to $\|\tilde{\mathbf{g}}_k\|^2 = \left\|\hat{\mathbf{g}}_k\right\|^2 + \nu_k^2$. Here we set $r_j = \nu_k^2/\|\tilde{\mathbf{g}}_k\|^2$ where $r_j < 0.5$ denotes the ratio of the approximation error to the channel gain. The last step is taken by replacing $\|\tilde{\mathbf{g}}_k\|^2$ with $\mathbb{E}\left\{\|\tilde{\mathbf{g}}_k\|^2\right\}$ according to *Proposition 1*. Then, the feasible solution of **P1** is given by

$$p_k^{\star} = \left[\frac{1-r_j}{\left(\sqrt{1-r_j}-\sqrt{r_j}\right)^2} - 1\right] \cdot \frac{\sigma_k^4\gamma_d\gamma_j}{\mathbb{E}\left\{\|\tilde{\mathbf{g}}_k\|^2\right\}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}\left(1-r_j\right)\gamma_d - \left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)^2\sigma_k^2\gamma_j} \quad (51)$$

B. Case 2

In case 2, $\{B_k\}\cap\{B_{k'}\} \neq \varnothing, \exists k' \neq k$. In the analysis of the follower subgame, we show that only sub-optimal solutions can be designed by the jammer to interfere with spatially correlated users. Therefore, the jamming power $p_{k,j}^{\star}, \forall k \in \{1,2\}$ is a "black box" to the BS, and a closed-form power solution such as (48) cannot be obtained in case 2. Based on (74), **P** is rewritten as

P2:

$$\begin{aligned} &\min_{\{p_k^{\star}\}} \sum_{k=1}^{K} p_k^{\star} \\ &s.t.\ \frac{\left\|\mathbf{w}_k^{GZF}\right\|^2}{\left\|\tilde{\mathbf{h}}_k^H\mathbf{w}_k^{GZF}\right\|^2}\gamma_d\left(p_k^{\star}\right)^{-1} \\ &\quad\cdot\left(\sum_{i\neq k}\frac{\left\|\tilde{\mathbf{h}}_k^H\mathbf{w}_i^{GZF}\right\|^2}{\left\|\mathbf{w}_i^{GZF}\right\|^2}p_i^{\star} + I_k + \sigma_k^2\right) \leq 1 \\ &\quad p_k^{\star} > 0, \forall k \in \{1,\cdots,K\}. \end{aligned} \quad (52)$$

It is shown that for a given I_k, **P2** becomes standard geometric programming (GP) and can be solved by using CVX tools [53]. The numerical solution, however, cannot be obtained in practice because I_k is unknown to the BS. One way to address this issue is to estimate I_k in the free time slots and feed this information back to the BS. Another way is to assign correlated users into orthogonal time/frequency blocks to turn both **P2** and **J2** into **P1** and **J1**. Then, a similar power solution such as (48) can be obtained, which helps establish an equilibrium for the game between the BS and jammer. Note that the cost of both of these schemes is a decrease in the spectral efficiency.

C. Existence and Uniqueness of the SE

In (13) and (14), the constrains of **J** and **P** are determined by the strategy matrices **S** and **W**, and the utility functions are given by $U_j(\mathbf{S},\mathbf{W}) = \left(\sum_{k=1}^{K}\|\mathbf{w}_k\|^2\right)^{-1}$ and $U_d(\mathbf{S},\mathbf{W}) = \left(\sum_{k=1}^{K}\|\mathbf{s}_k\|^2\right)^{-1}$, respectively, both of which obtain the maximum value when **J** and **P** are optimized.

We define that the optimal strategy pair $(\mathbf{S}^{\star},\mathbf{W}^{\star})$ constitutes the SE of the proposed anti-jamming Bayesian Stackelberg game if the following conditions are satisfied [58]:

$$U_j\left(\mathbf{S}^{\star},\mathbf{W}^{\star}\right) \geq U_j\left(\mathbf{S}^{\star},\mathbf{W}\right), \quad (53)$$

$$U_d\left(\mathbf{S}^\star, \mathbf{W}^\star\right) \geq U_d\left(\mathbf{S}, \mathbf{W}^\star\right). \tag{54}$$

Theorem 3: There exists a unique SE for the proposed anti-jamming Bayesian Stackelberg game in case 1.

Proof: According to (53) and (54), the BS and jammer achieve an SE when both players believe they have achieved the highest returns. Given the precoding matrix $\mathbf{S}$ at the BS, the proposed game reduces to a non-cooperative game and **J1** is convex. Specifically, the strategy space consisting of (15) is a convex and compact subspace of Euclidean space, and the utility function $U_j(\mathbf{S}, \mathbf{W})$ is a convex function of $\mathbf{W}$ for a given $\mathbf{S}$. Based on [59], there exists at least one Nash equilibrium (NE) in the follower subgame, and the unique NE for a given $\mathbf{S}$ is $(\mathbf{S}, \mathbf{W}^\star(\mathbf{S}))$. Then, the conditions of the SE can be rewritten as

$$U_d\left(\mathbf{S}^\star, \mathbf{W}^\star\left(\mathbf{S}^\star\right)\right) \geq U_d\left(\mathbf{S}, \mathbf{W}^\star(\mathbf{S})\right). \tag{55}$$

In case 1, **P1** is convex and the KKT solution (48) associated with *Theorem 2* forms a unique strategy pair $(\mathbf{S}^\star, \mathbf{W}^\star(\mathbf{S}^\star))$ with that of the jammer, which satisfies (55) and thus becomes the SE of the proposed game. In case 2, there also exists a unique NE for a given $\mathbf{S}$ in the follower subgame, whereas the condition (53) cannot be satisfied because the theoretical optimal precoding vectors toward the correlated users cannot be obtained by the jammer. Therefore, the SE does not exist in case 2. ■

Note that the proposed strategy pair based on (32) and (51) is an effective approximation of the perfect SE obtained from (29) and (48) by considering the precoding implementation in practice. Additionally, the condition necessary for the establishment of the SE is that (49) holds. This implies that the BS can always find a feasible power solution to ensure uninterrupted communication with users at the equilibrium point.

We derive from (51) that $\frac{\partial p_k^\star}{\partial r_j} > 0$, $r_j < 0.5$. Therefore, the jammer can force the BS to raise the transmission power in the game by simply increasing r_j. Similarly, the same result occurs if the jamming EE threshold γ_j is raised. The cost of this, however, is two-fold. First, $p_{k,j}^\star, \forall k \in \{1, \cdots, K\}$ is correlated with $p_k^\star$ according to (32). The strategy of increasing r_j or γ_j inversely aggravates the jamming power. Second, the feasibility probability of **J1** declines according to (49). Therefore, it is better for the jammer to reduce r_j to make precise attacks, and the meaning of this is to make full use of the spatial DoF of channels to transmit jamming signals through all paths.

From the perspective of the BS, let $r_k = \varepsilon_k^2 / \left\|\tilde{\mathbf{h}}_k\right\|^2$ denote the ratio of the approximation error to the channel gain on the BS side. It is shown from (51) that both $\frac{\partial p_k^\star}{\partial r_k} < 0$ and $\frac{\partial p_k^\star}{\partial \gamma_d} < 0$ hold for $\forall k \in \{1, \cdots, K\}$. Thus, the BS can reduce the power consumption by increasing r_k or raising the SINR threshold γ_d. Interestingly, this is in contrast to the results in [24], which say that r_k or γ_d must be reduced to decrease the power of the robust beamforming in a typical BDMA massive MIMO system without jammers. The intuitive explanation from a game perspective is that the optimal power solutions of the BS and jammer are positive correlated. During the game with the jammer, the BS only achieves the advantage on the path with stronger gain. By dropping weak paths and focusing the power on main paths, it s easier for the BS to achieve the equilibrium of the game with less power consumption. It should be noticed that **P1** has no solutions if γ_d or r_k is too large since the constrain of positive solutions (49) is not satisfied. Under this condition, only the suboptimal solutions can be designed by the BS and jammer, and the SE does not exist. This is not favorable for the BS because the attack pattern of the jammer will be unpredictable when the SE cannot be obtained, and the BS will have no knowledge of whether there exists a robust beamforming configuration ensuring uninterrupted communication with users. To avoid this, proper values of γ_d and r_k should be selected. The details of the proposed scheme are shown in Algorithm 1.

Algorithm 1 Beam-Domain Anti-Jamming Transmission Strategy Based On Stackelberg Game

1. Initialization:
- Choose ε_k, ν_k. Obtain $\tilde{\mathbf{h}}_k, \hat{\mathbf{h}}_k, \tilde{\mathbf{g}}_k, \hat{\mathbf{g}}_k$ by using (4), (5), (6),(7).
- Define $\mathbf{S}, \mathbf{W}$ as the strategy matrices. Define U_d, U_j as the utility functions.
- Obtain $\chi_k(\mathbf{S}, \mathbf{W})$ and Δ_k according to (11),(12), respectively.

2. For the follower subgame:

if case 1 occurs
- Compute the KKT solution $p_{k,j}^\star$ by using (29).
- Compute the feasible solution (32) by replacing $\left\|\tilde{\mathbf{h}}_k\right\|^2$ with $\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}$.

else
- Select a proper value of ψ according to (37).
- Compute the KKT solution $p_{k,j}^\star$ by using (36).

3. For the leader subgame:

if case 1 occurs
- Compute the KKT solution $p_k^\star$ by using (48).
- Compute the feasible solution (51) by replacing $\|\tilde{\mathbf{g}}_k\|^2$ with $\mathbb{E}\left\{\|\tilde{\mathbf{g}}_k\|^2\right\}$.

else
- Obtain the numerical results by solving GP in (52).

V. Numerical Results

Numerical results are provided in this section to evaluate the proposed anti-jamming transmission. We consider a simulation scenario where $K = 8$ users are independently and uniformly distributed over the coverage area. The BS with $M = 128$ antennas is installed in the center of the cell and the smart jammer with $N = 128$ antennas is randomly placed at high places. We use the 3GPP spatial channel model for the MIMO simulation in an urban environment [60]. The center frequency and bandwidth are set to 2.4GHz and 20 MHz, respectively. The path loss is given by $30.18 + 26\log 10\,(d)$[dB], where the mean distance from the BS to users is $d = 400$m. The bulk normal shadowing applied to the sub-paths has a standard

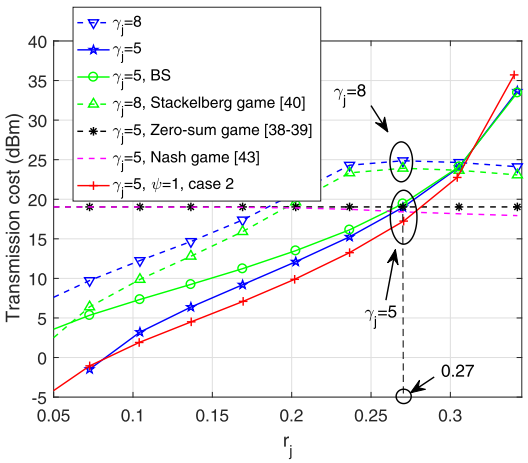

Fig. 2. Transmission cost of the jammer (P_j). $\gamma_d = 1$. $\gamma_j = 5$ *or* 8 mW^{-1}. In case 2, the central AODs of $\mathbf{g}_1$ and $\mathbf{g}_2$ are set to 30° and 33°, respectively.

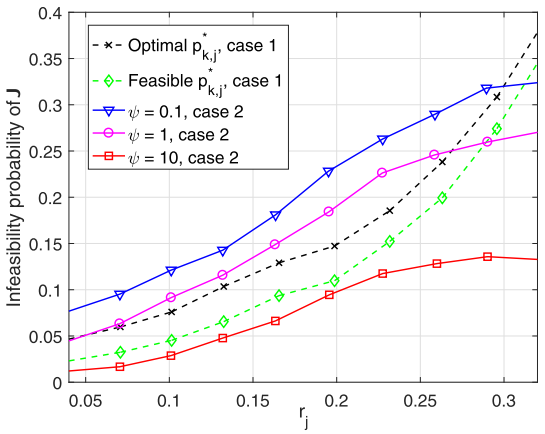

Fig. 3. Infeasibility probability of $\mathbf{J}$ (F_j). $\gamma_j = 5$ mW^{-1}. In case 2, the central AODs of $\mathbf{g}_1$ and $\mathbf{g}_2$ are set to 30° and 33°, respectively.

deviation of 4 dB. The channel parameters of the jammer is set to be the same as user channels. The thermal noise density is set to -174 dBm/Hz. The maximum transmission power of the BS and jammer are set to 10 dBm/user. Assume that the downlink signals can be correctly decoded by users when $\gamma_d \geq 1$. The value of γ_j is calculated based on (49).

In this section, we use four indicators to evaluate the impact of the game on the downlink transmission. (a) As introduced in section II, the transmission costs of the BS and jammer are given by $P_d = \sum_{k=1}^{K} \|\mathbf{s}_k\|^2$ and $P_j = \sum_{k=1}^{K} \|\mathbf{w}_k\|^2$, respectively, to evaluate the power consumption on both sides. (b) The infeasibility probability of $\mathbf{J}$ is denoted by $F_j = \Pr\left\{p_{k,j}^{\star} < 0, \exists k\right\}$. (c) The outage probability of the downlink transmission associated with the proposed scheme is defined as the probability that $p_k^{\star} < 0$ or the semi-definite constrain (45) is not satisfied; i.e., $F_d = 1 - \Pr\left\{p_k^{\star} > 0,\ \mathbf{X}_k + \mu_k \mathbf{I} \succcurlyeq \mathbf{0}, \forall k\right\}$. (d) The ergodic EE of the downlink transmission is given by $E_d = \mathbb{E}\left\{\sum_{k=1}^{K} \log_2\left(1 + \chi_k\left(\mathbf{S}, \mathbf{W}\right)\right)/P_d\right\}$. In addition, we compare the proposed scheme with three solutions: the typical Stackelberg game framework with perfect information [40], the zero-sum game framework which aims to optimize the throughput [38], [39] and the Nash game framework involving sequential actions [43]. The simulation results are averaged over 10k Monte Carlo runs.

Fig. 2 shows the transmission cost of the jammer. The first observation is that the jamming power increases with increasing γ_j or r_j. This indicates that the precise precoding with proper jamming threshold helps save the transmission power. Meanwhile, for $r_j < 0.27$, the jammer needs less power than the BS under the same channel conditions. This verifies the threat of the smart jammer to the system. The second observation is that the performance of the jammer is almost not influenced by r_j under zero-sum game and Nash game framework, and the reason is that full power is transmitted under both game models. Therefore, more power is used when $r_j < 0.27$.

Fig. 3 shows the infeasibility probability of $\mathbf{J}$ in two cases. In case 1, we notice that the infeasibility probability of the optimal solution given by *Theorem 1* is higher than that of the approximated solution (32), and increases exponentially with increasing r_j. However, the probability tends to converge with the high r_j condition of case 2. Based on the results in Fig. 2, this occurs when large jamming power is used. Therefore it is better for the jammer to reduce r_j so as to avoid both high power consumption and infeasibility probability. It is also shown that a proper ψ should be selected in case 2, since a large value helps to reduce the infeasibility probability of the optimization.

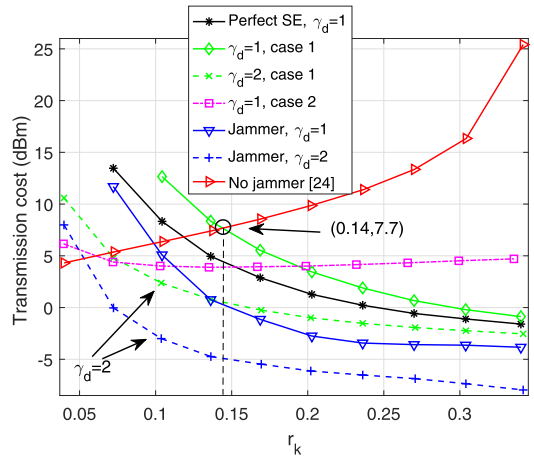

Fig. 4. Transmission cost of the BS (P_d). $r_j = 0.1$, $\gamma_j = 10$ mW^{-1}. $r_k = \varepsilon_k^2 / \left\|\tilde{\mathbf{h}}_k\right\|^2$. $\gamma_d = 1$ *or* 2.

Fig. 4 shows the transmission cost of the BS. For comparison, the performance of the jammer and the BD precoding solution without jamming attacks [24] are also presented in the figure. It is shown that both P_j and P_d are reduced by increasing r_k or γ_d, which verifies the discussion of $p_k^{\star}$ in (51). In contrast, the transmission power of the BS without jamming attacks increases exponentially by raising r_k and is larger than the power for jamming defense when $r_k > 0.14$. The reason is that the large channel approximation error results in serious inter-user interference. Moreover, we notice that $P_d > P_j$ holds in all conditions, and the performance gap is inversely

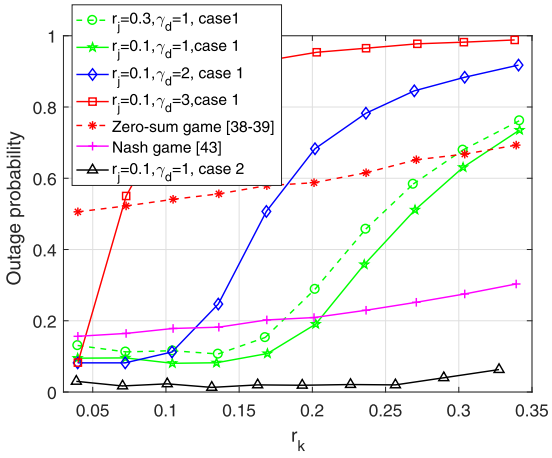

Fig. 5. Outpage probability of the downlink tranmission (F_d). $r_j = 0.1$ *or* 0.3, $\gamma_j = 10$ mW^{-1}.

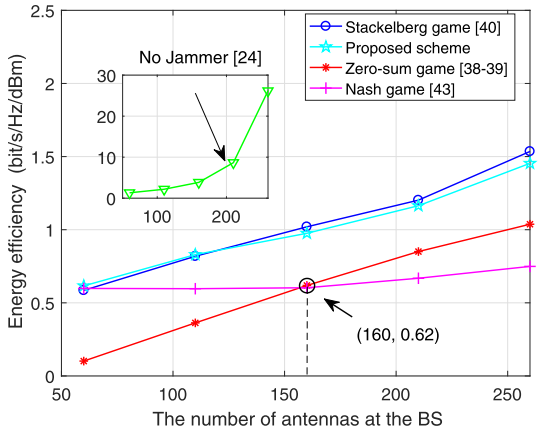

Fig. 6. Ergodic EE of the downlink transmission (E_d). $r_j = 0.1$, $\gamma_j = 10$ mW^{-1}. $r_k = 0.1$. $\gamma_d = 1$. $N = 128$.

proportional to r_k, which is consistent with the observation in Fig. 2.

Fig. 5 shows the outage probability of the downlink transmission. We notice that F_d increases rapidly and converges to 1 when $r_k > 0.17$, $\gamma_d = 1$ or $r_k > 0.1$,$\gamma_d = 2$. Therefore, it is infeasible to reduce the transmission power by increasing the channel approximation error or the threshold without limitation. Based on the results in Fig. 4 and Fig. 5, we conclude that it is more likely for the BS to achieve the equilibrium with jammer under low γ_d and r_k conditions. Nevertheless, proper values of γ_d and r_k can be selected to save the power consumption while ensuring reliable signal reception of users. The second observation is that the zero-sum game based scheme aiming to maximize the throughput obtains the highest outage probability when $\gamma_d = 1$, $r_k < 0.33$, which implies that it is difficult for the BS to guarantee the efficiency and robustness of transmission simultaneously. In contrast, the Nash game based solution obtains the best performance in the high r_k conditions where $r_k > 0.2$. The cost, however, is the long time consumption for the convergence of game. Moreover, we derive from Fig. 4 and Fig. 5 that under the high r_k conditions of case 2, the BS obtains the lowest outage probability at the cost of using more power.

Fig. 6 shows the ergodic EE of the downlink transmission. The first observation is that the performance of the proposed scheme is close to that of the Stackelberg game based solution with perfect information, which provides the upper bound of EE. In contrast, the zero-sum game based solution provides the poorest performance when $M < 160$, since the antennas number of the BS is less than that of the jammer. Similarly, the Nash game based solution gets the lowest EE under the conditions of $M > 160$, and the reason is that the sequential decisions making often produces a situation where full power is transmitted while the game cannot converge to the equilibrium point. The second observation is that all these schemes obtain much lower performance than the precoding scheme without jamming attacks, and this proves again the threats of the smart jammer to the system.

VI. Conclusions

In this paper, we proposed an anti-jamming transmission scheme for downlink massive MIMO systems. A Bayesian Stackelberg game was modeled to investigate the hierarchical interactions between the BS and jammer. The optimal jamming precoding with a closed-form power solution was proposed in the follower subgame and was converted into a solution for practical implementation. It was shown that a precise attack with the power proportional to the transmission power of the BS could maximize the jamming effect. In the leader subgame, we proved that the generalized ZF was the optimal configuration for jamming defense and that the closed-form power solution constituted the unique SE with that of the jammer. A simplified power solution without knowledge of the instantaneous jamming channel was further introduced for practical implementation. We proved that the BS was more likely to reach the SE with a jammer under low SINR threshold conditions, where uninterrupted communication with users was ensured. A proper increase in the channel approximation

$$
\begin{aligned}
\mathbf{H}(f_k) &= \frac{-2}{\left(\xi_k p_{k,j} + \rho_k\right)^3}\begin{bmatrix} p_{k,j}^2\xi_k^2 & -\xi_k p_{k,j}\rho_k\left(2\xi_k - d_k\right) \\ -\xi_k p_{k,j}\rho_k\left(2\xi_k - d_k\right) & \rho_k^2\left[\left(d_k - \xi_k\right)\left(\xi_k p_{k,j} + \rho_k\right) + \left(2\xi_k - d_k\right)^2\right]\end{bmatrix} \\
&\prec \frac{-2}{\left(\xi_k p_{k,j} + \rho_k\right)^3}\begin{bmatrix} p_{k,j}^2\xi_k^2 & -\xi_k p_{k,j}\rho_k\left(2\xi_k - d_k\right) \\ -\xi_k p_{k,j}\rho_k\left(2\xi_k - d_k\right) & \rho_k^2\left(2\xi_k - d_k\right)^2\end{bmatrix} \\
&= \frac{-2}{\left(\xi_k p_{k,j} + \rho_k\right)^3}\begin{bmatrix} -p_{k,j}\xi_k \\ \rho_k\left(2\xi_k - d_k\right)\end{bmatrix}\cdot\begin{bmatrix} -p_{k,j}\xi_k \\ \rho_k\left(2\xi_k - d_k\right)\end{bmatrix}^H \prec \mathbf{0}
\end{aligned} \tag{56}
$$

error was conducive to reducing the power consumption of the precoding in the defense against a jammer.

APPENDIX

A. Proof of Theorem 1

Let $f_k\left(\rho_k, p_{k,j}\right) = \frac{\xi_k p_{k,j}\rho_k}{\xi_k p_{k,j}+\rho_k}\left\|\hat{\mathbf{g}}_k\right\|^2$, whose Hessian matrix is shown at the bottom of the precious page. $\mathbf{H}\left(f_k\right) \prec \mathbf{0}$ implies that constrain (27) is concave; thus, **J1** is a convex optimization problem. Let $\left\{\lambda_{k,j}\right\}$, $\left\{\tau_{k,j}\right\}$, and $\left\{\phi_{k,j}\right\}$ denote the sets of nonnegative multipliers, and the Lagrangian of **J1** is

$$\begin{aligned}&\mathcal{L}\left(\left\{p_{k,j}\right\},\{\rho_k\},\left\{\lambda_{k,j}\right\},\left\{\phi_{k,j}\right\},\left\{\tau_{k,j}\right\}\right)\\&=\sum_{k=1}^{K} p_{k,j}-\sum_{k=1}^{K}\phi_{k,j}\rho_k-\sum_{k=1}^{K}\tau_{k,j}p_{k,j}\\&\quad-\sum_{k=1}^{K}\lambda_{k,j}\left[f_k\left(\rho_k, p_{k,j}\right)-\gamma_j\left(m_k+\sigma_k^2\right)^2 p_{k,j}-\rho_k v_k^2\right],\end{aligned} \tag{57}$$

and the KKT conditions are

$$\frac{\partial\mathcal{L}}{\partial\rho_k}=-\lambda_{k,j}\left[\frac{\xi_k^2 p_{k,j}^2}{\left(\xi_k p_{k,j}+\rho_k\right)^2}\left\|\hat{\mathbf{g}}_k\right\|^2-v_k^2\right]-\phi_{k,j}=0, \tag{58}$$

$$\begin{aligned}\frac{\partial\mathcal{L}}{\partial p_{k,j}}&=-\lambda_{k,j}\left[\frac{\rho_k^2\left(2\xi_k-d_k\right)}{\left(\xi_k p_{k,j}+\rho_k\right)^2}\left\|\hat{\mathbf{g}}_k\right\|^2-\gamma_j\left(m_k+\sigma_k^2\right)^2\right]\\&\quad+1-\tau_{k,j}=0,\end{aligned} \tag{59}$$

$$\lambda_{k,j}\left[f_k\left(\rho_k, p_{k,j}\right)-\gamma_j\left(m_k+\sigma_k^2\right)^2 p_{k,j}-\rho_k v_k^2\right]=0, \tag{60}$$

$$\phi_{k,j}\rho_k=0,\quad \tau_{k,j}p_{k,j}=0,\ k=1,2,\cdots,K. \tag{61}$$

Since $\rho_k > 0$, $p_{k,j} > 0$, we derive from the complementary slackness condition (61) that $\phi_{k,j}=0$, $\tau_{k,j}=0$. By substituting $\tau_{k,j}=0$ into (59), we derive $\lambda_{k,j} > 0$. Furthermore, by substituting $\phi_{k,j}=0$ and $\lambda_{k,j} > 0$ into (58), the relationship between ρ_k and $p_{k,j}$ is given by

$$\xi_k p_{k,j}\left(\left\|\hat{\mathbf{g}}_k\right\|-v_k\right)=v_k\rho_k. \tag{62}$$

Based on (60) and (62), the KKT solution of **J1** is obtained.

Now, we verify the solution under the constrain (25). According to (29), $p_{k,j}^{\star} < \frac{d_k}{(m_k+\sigma_k^2)\gamma_j}$, i.e., $\xi_k > 0$. Then we derive $\xi_k p_{k,j}^{\star}+\rho_k > 0$, $\forall k \in \{1,\cdots K\}$. This means that the eigenvalues of $\mathbf{Y}_k+\rho_k\mathbf{I}$ are positive and that $\mathbf{Y}_k+\rho_k\mathbf{I}\succcurlyeq 0$ holds true. Therefore, $p_{k,j}^{\star}$ is the optimal power solution of both **J1** and **J**. Based on (15), (30) is obtained.

B. Proof of Theorem 2

To simplify the problem, we first assume that $Rank\left(\mathbf{S}_k\right)=1$ holds and later verify the solution under this constrain. We define $\mathbf{\Psi}_k=\begin{bmatrix}\mathbf{Z}_k & \mathbf{r}_k\\ \mathbf{r}_k^H & \eta_k\end{bmatrix}\succcurlyeq 0$, $\mathbf{\Phi}_{s,k}\succcurlyeq\mathbf{0}$, and $\phi_{\mu,k}\geq 0$ as the multipliers of (39), $\mathbf{S}_k$ and μ_k,respectively; then, the Lagrangian of **P-E** is given by

$$\begin{aligned}&\mathcal{L}\left(\left\{\mathbf{S}_k\right\},\left\{\mu_k\right\},\left\{\mathbf{\Psi}_k\right\},\left\{\mathbf{\Phi}_{s,k}\right\},\left\{\phi_{\mu,k}\right\}\right)\\&=\sum_{k=1}^{K} Tr\left(\mathbf{S}_k\right)-\sum_{k=1}^{K} Tr\left(\mathbf{\Phi}_{s,k}\mathbf{S}_k\right)-\sum_{k=1}^{K}\phi_{\mu,k}\mu_k\\&\quad-\sum_{k=1}^{K}\mathbf{\Psi}_k\begin{bmatrix}\mathbf{X}_k+\mu_k\mathbf{I} & \mathbf{X}_k\hat{\mathbf{h}}_k\\ \hat{\mathbf{h}}_k^H\mathbf{X}_k & \hat{\mathbf{h}}_k^H\mathbf{X}_k\hat{\mathbf{h}}_k-\sigma_k^2-I_k-\mu_k\varepsilon_k^2\end{bmatrix}.\end{aligned} \tag{63}$$

In case 1, (32) is substituted into (63) to obtain

$$\begin{aligned}&\mathcal{L}\left(\left\{\mathbf{S}_k\right\},\left\{\mu_k\right\},\left\{\mathbf{\Psi}_k\right\},\left\{\mathbf{\Phi}_{s,k}\right\},\left\{\phi_{\mu,k}\right\}\right)\\&=\sum_{k=1}^{K} Tr\left(\mathbf{B}_k\mathbf{S}_k\right)-\sum_{k=1}^{K}\left[\phi_{\mu,k}+Tr\left(\mathbf{Z}_k\right)-\eta_k\varepsilon_k^2\right]\mu_k\\&\quad+\sum_{k=1}^{K}\eta_k\left[\sigma_k^2-\sum_{n=1}^{K}\frac{l_{k,n}\sigma_n^2}{\left(\left\|\hat{\mathbf{g}}_n\right\|-v_n\right)^2}\right],\end{aligned} \tag{64}$$

where $\mathbf{B}_k=\left(1+\sum_{n=1}^{K}\eta_n\frac{l_{k,n}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_n\right\|^2\right\}}{\sigma_n^2\gamma_j}\right)\mathbf{I}-\frac{\mathbf{A}_k}{\gamma_d}+\sum_{\substack{i=1\\ i\neq k}}^{K}\mathbf{A}_i-\mathbf{\Phi}_{s,k}$, $\mathbf{A}_k=\mathbf{Z}_k+\mathbf{r}_k\hat{\mathbf{h}}_k^H+\hat{\mathbf{h}}_k\mathbf{r}_k^H+\eta_k\hat{\mathbf{h}}_k\hat{\mathbf{h}}_k^H$. Then the KKT condition about $\{\mathbf{S}_k\}$ is

$$\frac{\partial\mathcal{L}}{\partial\mathbf{S}_k^*}=\frac{\partial Tr\left(\mathbf{B}_k\mathbf{S}_k\right)}{\partial\mathbf{S}_k^*}=0, \tag{65}$$

and the solution of (65) is given by

$$\mathbf{\Phi}_{s,k}^{\star}=\left(1+\sum_{n=1}^{K}\eta_n\frac{l_{k,n}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_n\right\|^2\right\}}{\sigma_n^2\gamma_j}\right)\mathbf{I}-\frac{\mathbf{A}_k}{\gamma_d}+\sum_{\substack{i=1\\ i\neq k}}^{K}\mathbf{A}_i. \tag{66}$$

Since $\mathbf{A}_k\succcurlyeq\mathbf{0}$ and $\gamma_d,\gamma_j > 1$ hold for $\forall k\in\{1,\cdots,K\}$, we derive that for $\forall k\neq i$,

$$\begin{aligned}&\mathbf{\Phi}_{s,k}^{\star}+\mathbf{\Phi}_{s,i}^{\star}\\&\succ 2\mathbf{I}+\left(1-\frac{1}{\gamma_d}\right)\mathbf{A}_k+\left(1-\frac{1}{\gamma_j}\right)\mathbf{A}_i+2\sum_{n\neq k,i}\mathbf{A}_n\\&\succ\mathbf{0}.\end{aligned} \tag{67}$$

In case 2, (63) is rewritten as

$$\begin{aligned}&\mathcal{L}\left(\left\{\mathbf{S}_k\right\},\left\{\mu_k\right\},\left\{\mathbf{\Psi}_k\right\},\left\{\mathbf{\Phi}_{s,k}\right\},\left\{\phi_{\mu,k}\right\}\right)\\&=\sum_{k=1}^{K} Tr\left(\mathbf{B'}_k\mathbf{S}_k\right)-\sum_{k=1}^{K}\left[\phi_{\mu,k}+Tr\left(\mathbf{Z}_k\right)-\eta_k\varepsilon_k^2\right]\mu_k\\&\quad+\sum_{k=1}^{K}\eta_k\left[\sigma_k^2+I_k\right],\end{aligned} \tag{68}$$

where $\mathbf{B'}_k=\mathbf{I}-\frac{\mathbf{A}_k}{\gamma_d}+\sum_{i\neq k}\mathbf{A}_i-\mathbf{\Phi}_{s,k}$. The KKT condition about $\{\mathbf{S}_k\}$ is given by

$$\mathbf{\Phi}_{s,k}^{\star}=\mathbf{I}-\frac{\mathbf{A}_k}{\gamma_d}+\sum_{i\neq k}\mathbf{A}_i. \tag{69}$$

Similar to (67), we derive that $\mathbf{\Phi}^{\star}_{s,k}+\mathbf{\Phi}^{\star}_{s,i}\succ\mathbf{0}$. This implies that $Rank\left(\mathbf{\Phi}^{\star}_{s,k}+\mathbf{\Phi}^{\star}_{s,i}\right)=M$ holds for both cases. Let $\left\{\mathbf{u}_{s,k}\right\}$ and $\left\{\mathbf{u}_{s,i}\right\}$ denote the set of eigenvectors of $\mathbf{\Phi}^{\star}_{s,k}$ and $\mathbf{\Phi}^{\star}_{s,i}$, respectively. Let $\mathbf{I}_M=[\mathbf{e}_1,\cdots,\mathbf{e}_M]$. Then the full-rank property leads to

$$Span\left\{\left\{\mathbf{u}_{s,k}\right\}\cup\left\{\mathbf{u}_{s,i}\right\}\right\}=Span\left\{\mathbf{e}_1,\cdots,\mathbf{e}_M\right\}. \tag{70}$$

Furthermore, the complementary slackness of (63) is

$$\mathbf{\Phi}^{\star}_{s,k}\mathbf{S}^{\star}_k=\mathbf{0},\quad \forall k\in\{1,\cdots,K\}. \tag{71}$$

When $\mathbf{S}^{\star}_k\neq\mathbf{0}$, we must have $Rank\left(\mathbf{\Phi}^{\star}_{s,k}\right)<M$ and $\mathbf{S}_k$ is in the null space of $\mathbf{\Phi}^{\star}_{s,k}$, i.e., $\mathbf{S}^{\star}_k\perp Span\left\{\mathbf{u}_{s,k}\right\}$; then, we have

$$\mathbf{S}^{\star}_k\subseteq Span\left\{\mathbf{u}_{s,i}\right\},\quad \forall i\neq k. \tag{72}$$

Since $\mathbf{S}^{\star}_i\perp Span\left\{\mathbf{u}_{s,i}\right\}$ also holds true, we derive

$$\mathbf{S}^{\star}_k\mathbf{S}^{\star}_i=\mathbf{0},\quad \forall i\neq k. \tag{73}$$

This implies that the optimal anti-jamming precoding has the same model as the generalized ZF precoding in both cases, which is given by $\mathbf{w}^{GZF}_k=\sqrt{p^{GZF}_k}\hat{\mathbf{H}}\left(\hat{\mathbf{H}}^H\hat{\mathbf{H}}\right)^{-1}_{,k},\forall k\in\{1,\cdots,K\}$. Since $\left\|\mathbf{s}^{\star}_k\right\|^2=p^{\star}_k$, the optimal anti-jamming precoding can be modeled as

$$\mathbf{s}^{\star}_k=\sqrt{p^{\star}_k}\frac{\mathbf{w}^{GZF}_k}{\left\|\mathbf{w}^{GZF}_k\right\|},\quad \forall k\in\{1,\cdots,K\}. \tag{74}$$

Then (41) is obtained, meanwhile the solution satisfies $Rank\left(\mathbf{S}^{\star}_k\right)=1$.

C. Proof of (48)

We define $\{\lambda_k\}$ and $\{\tau_k\}$ as the sets of nonnegative multipliers. The Lagrangian of **P1** is

$$\begin{aligned}&\mathcal{L}\left(\{\tau_k\},\left\{\phi_{\mu,k}\right\},\{\lambda_k\}\right)\\&=\sum_{k=1}^{K}p^{\star}_k-\sum_{k=1}^{K}\phi_{\mu,k}\mu_k-\sum_{k=1}^{K}\tau_k p^{\star}_k\\&\quad-\sum_{k=1}^{K}\lambda_k\left(\frac{\mu_k p^{\star}_k}{p^{\star}_k+\gamma_d\mu_k}\left\|\hat{\mathbf{h}}_k\right\|^2-\sigma^2_k-\mu_k\varepsilon^2_k\right)\\&\quad+\sum_{k=1}^{K}\sum_{n=1}^{K}\lambda_k l_{k,n}\left(\frac{p^{\star}_n\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_n\right\|^2\right\}}{\sigma^2_n\gamma_j}-\frac{\sigma^2_n}{\left(\left\|\hat{\mathbf{g}}_n\right\|-\nu_n\right)^2}\right),\end{aligned} \tag{75}$$

and the KKT conditions are given by

$$\frac{\partial\mathcal{L}}{\partial\mu_k}=-\lambda_k\left[\frac{p^{\star}_k\left\|\hat{\mathbf{h}}_k\right\|^2}{\left(p^{\star}_k+\gamma_d\mu_k\right)^2}-\varepsilon^2_k\right]-\phi_{\mu,k}=0, \tag{76}$$

$$\begin{aligned}\frac{\partial\mathcal{L}}{\partial p^{\star}_k}&=1-\tau_k-\frac{\lambda_k\gamma_d\mu^2_k}{\left(p^{\star}_k+\gamma_d\mu_k\right)^2}+\sum_{n=1}^{K}\lambda_n\frac{l_{n,k}\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_k\right\|^2\right\}}{\sigma^2_k\gamma_j}\\&\quad-\sum_{n=1}^{K}\lambda_k l_{k,n}\left(\frac{p^{\star}_n\mathbb{E}\left\{\left\|\tilde{\mathbf{h}}_n\right\|^2\right\}}{\sigma^2_n\gamma_j}-\frac{\sigma^2_n}{\left(\left\|\hat{\mathbf{g}}_n\right\|-\nu_n\right)^2}\right)\\&=0,\end{aligned} \tag{77}$$

$$\lambda_k\left(\frac{\mu_k p^{\star}_k}{p^{\star}_k+\gamma_d\mu_k}\left\|\hat{\mathbf{h}}_k\right\|^2-\sigma^2_k-\mu_k\varepsilon^2_k\right)=0, \tag{78}$$

$$\phi_{\mu,k}\mu_k=0,\quad \tau_k p^{\star}_k=0,\ \forall k\in\{1,\cdots,K\}. \tag{79}$$

Since $\mu_k>0$ and $p_k>0$ hold for $\forall k\in\{1,\cdots,K\}$, we derive from the complementary slackness condition (79) that $\phi_k=0$, $\tau_k=0$. Furthermore, by substituting $\tau_k=0$ into (77), we derive $\lambda_k>0$. Then (76) can be simplified into

$$\mu_k=\frac{p^{\star}_k\left(\left\|\hat{\mathbf{h}}_k\right\|-\varepsilon_k\right)}{\varepsilon_k\gamma_d}. \tag{80}$$

Based on (78) and (80), (48) is obtained.

REFERENCES

[1] A. D. Wyner, "The wiretap channel" *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975

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

[3] 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.

[4] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[5] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 2001–2016, Mar. 2017.

[6] J. Zhu, W. Xu, and N. Wang, "Secure massive MIMO systems with limited RF chains," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5455–5460, Jun. 2017.

[7] H. Wang, L. Zhang, T. Li, and J. Tugnait, "Spectrally efficient jamming mitigation based on code-controlled frequency hopping," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 728–732, Mar. 2011.

[8] B. Gopalakrishnan and M. A. Bhagyaveni, "Random codekey selection using codebook without pre-shared keys for anti-jamming in WBAN," *Comput. Electr. Eng.*, vol. 51, pp. 89–103, Apr. 2016.

[9] B. Akgun, M. Krunz, and O. O. Koyluoglu, "Pilot contamination attacks in massive MIMO systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Las Vegas, NV, USA, Oct. 2017, pp. 1–9.

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

[11] 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.

[12] J. Vinogradova, E. Bjornson, and E. G. Larsson, "Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory," in *Proc. IEEE 17th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Edinburgh, U.K., Jul. 2016, pp. 1–5.

[13] H. Akhlaghpasand, S. M. Razavizadeh, E. Bjornson, and T. T. Do, "Jamming detection in massive MIMO systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 2, pp. 242–245, Apr. 2018.

[14] 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.

[15] Z. Shen, K. Xu, X. Xia, W. Xie, and D. Zhang, "Spatial sparsity based secure transmission strategy for massive MIMO systems against simultaneous jamming and eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3760–3774, 2020.

[16] D. Rathore, S. Kashyap, and A. Rajesh, "On the efficacy of antenna selection at the massive antenna jammer," in *Proc. Int. Conf. Signal Process. Commun. (SPCOM)*, Bangalore, India, Jul. 2020, pp. 1–5.

[17] A. Sheikhi, S. M. Razavizadeh, and I. Lee, "A comparison of TDD and FDD massive MIMO systems against smart jamming," *IEEE Access*, vol. 8, pp. 72068–72077, 2020.

[18] L. Jia, Y. Xu, Y. Sun, S. Feng, and A. Anpalagan, "Stackelberg game approaches for anti-jamming defence in wireless networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 120–128, Dec. 2018.
[19] Z. Xiao, B. Gao, S. Liu, and L. Xiao, "Learning based power control for mmWave massive MIMO against jamming," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.
[20] N.-P. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and D. B. da Costa, "Full-duplex cyber-weapon with massive arrays," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5544–5558, Dec. 2017.
[21] C. Sun, X. Gao, S. Jin, M. Matthaiou, Z. Ding, and C. Xiao, "Beam division multiple access transmission for massive MIMO communications," *IEEE Trans. Commun.*, vol. 63, no. 6, pp. 2170–2184, Jun. 2015.
[22] X. Xia, K. Xu, D. Zhang, Y. Xu, and Y. Wang, "Beam-domain full-duplex massive MIMO: Realizing co-time co-frequency uplink and downlink transmission in the cellular system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 8845–8862, Oct. 2017.
[23] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3170–3184, Apr. 2017.
[24] F. Zhu, F. Gao, S. Jin, H. Lin, and M. Yao, "Robust downlink beamforming for BDMA massive MIMO system," *IEEE Trans. Commun.*, vol. 66, no. 4, pp. 1496–1507, Apr. 2018.
[25] H. Lin, F. Gao, S. Jin, and G. Y. Li, "A new view of multi-user hybrid massive MIMO: Non-orthogonal angle division multiple access," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2268–2280, Oct. 2017.
[26] 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.
[27] O. Besson, P. Stoica, and Y. Kamiya, "Direction finding in the presence of an intermittent interference," *IEEE Trans. Signal Process.*, vol. 50, no. 7, pp. 1554–1564, Jul. 2002.
[28] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2nd Quart., 2011.
[29] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Urbana-Champaign, IL, USA, 2005, pp. 46–57.
[30] Y. Liu and P. Ning, "BitTrickle: Defending against broadband and high-power reactive jamming attacks," in *Proc. 31st Annu. IEEE Int. Conf. Comput. Commun.*, Orlando, FL, USA, Mar. 2012, pp. 909–917.
[31] E. Lance and G. K. Kaleh, "A diversity scheme for a phase-coherent frequency-hopping spread-spectrum system," *IEEE Trans. Commun.*, vol. 45, no. 9, pp. 1123–1129, Sep. 1997.
[32] H. Pirzadeh, S. M. Razavizadeh, and E. Bjornson, "Subverting massive MIMO by smart jamming," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 20–23, Feb. 2016.
[33] L. Jia, F. Yao, Y. Sun, Y. Niu, and Y. Zhu, "Bayesian Stackelberg game for antijamming transmission with incomplete information," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 1991–1994, Oct. 2016.
[34] Y. E. Sagduyu, R. Berry, and A. Ephremides, "MAC games for distributed wireless network security with incomplete information of selfish and malicious user types," in *Proc. GameNets*, 2009, pp. 39–130.
[35] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, pp. 197–215, Dec. 2014.
[36] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[37] F. Yao and L. Jia, "A collaborative multi-agent reinforcement learning anti-jamming algorithm in wireless networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1024–1027, Aug. 2019.
[38] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.
[39] X. Song, P. Willett, S. Zhou, and P. B. Luh, "The MIMO radar and jammer games," *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 687–699, Feb. 2012.
[40] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A stackelberg game approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 4038–4047, Aug. 2013.
[41] L. Xiao, T. Chen, J. Liu, and H. Dai, "Anti-jamming transmission stackelberg game with observation errors," *IEEE Commun. Lett.*, vol. 19, no. 6, pp. 949–952, Jun. 2015.
[42] L. Jia, F. Yao, Y. Sun, Y. Xu, S. Feng, and A. Anpalagan, "A hierarchical learning solution for anti-jamming stackelberg game with discrete power strategies," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 818–821, Dec. 2017.
[43] F. Slimeni *et al.*, "Optimal power allocation over parallel Gaussian channels in cognitive radio and jammer games," *IET Commun.*, vol. 10, no. 8, pp. 980–986, Feb. 2016.
[44] F. Yao, L. Jia, Y. Sun, Y. Xu, S. Feng, and Y. Zhu, "A hierarchical learning approach to anti-jamming channel selection strategies," *Wireless Netw.*, vol. 25, no. 1, pp. 201–213, 2017.
[45] J.-A. Tsai, R. M. Buehrer, and B. D. Woerner, "The impact of AOA energy distribution on the spatial fading correlation of linear antenna array," in *Proc. IEEE 55th Veh. Technol. Conf.*, Birmingham, AL, USA, May 2002, pp. 933–937.
[46] H. Yin, D. Gesbert, M. Filippou, and Y. Liu, "A coordinated approach to channel estimation in large-scale multiple-antenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 264–273, Feb. 2013.
[47] A. Adhikary, J. Nam, J.-Y. Ahn, and G. Caire, "Joint spatial division and multiplexing—The large-scale array regime," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6441–6463, Oct. 2013.
[48] E. Bjornson, J. Hoydis, and L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency, foundations and trends," *Signal Process.*, vol. 11, nos. 3–4, pp. 154–655, 2017.
[49] J. Nam, A. Adhikary, J.-Y. Ahn, and G. Caire, "Joint spatial division and multiplexing: Opportunistic beamforming, user grouping and simplified downlink scheduling," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 876–890, Oct. 2014.
[50] J. Singh and S. Ramakrishna, "On the feasibility of codebook-based beamforming in millimeter wave systems with multiple antenna arrays," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2670–2683, May 2015.
[51] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.
[52] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.
[53] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[54] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory* (Studies in Applied Mathematics). Philadelphia, PA, USA: SIAM, 1994.
[55] R. A. Horn and C. R. Johnson, *Matrix Analysis*. New York, NY, USA: Cambridge Univ. Press, 1985.
[56] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Trans. Antennas Propag.*, vol. 34, no. 3, pp. 276–280, Mar. 1986.
[57] A. J. Weiss and M. Gavish, "Direction finding using ESPRIT with interpolated arrays," *IEEE Trans. Signal Process.*, vol. 39, no. 6, pp. 1473–1478, Jun. 1991.
[58] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjrungnes, *Game Theory in Wireless and Communication Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[59] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, Jul. 1965.
[60] *Spatial Channel Model for Multiple Input Multiple Output (MIMO) Simulations*, document 3GPP TR 25.996, version 13.0.0, Release 13, Jan. 2016.

Zhexian Shen received the B.S. degree from the Nanjing University of Posts and Telecommunications in 2016, and the M.S. degree from PLA Army Engineering University in 2018. He is currently pursuing the Ph.D. degree with the Institution of Communications Engineering, PLA Army Engineering University. His research interests include signal processing in massive MIMO systems, millimeter-wave, physical-layer security, and heterogenous network. He received the 2018 excellent master's degree dissertation award of the PLA Army Engineering University. He serves as the Reviewer for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICLE TECHNOLOGY, the IEEE SYSTEMS JOURNAL.

Kui Xu (Member, IEEE) was born in 1982. He received the B.S. degree in wireless communications and the Ph.D. degree in software-defined radio from the PLA University of Science and Technology, Nanjing, China, in 2004 and 2009, respectively. He is currently an Associate Professor with the College of Communications Engineering, Army Engineering University of PLA. Since 2013, he has been a Post-Doctoral Fellow with the PLA University of Science and Technology. His research interests include massive MIMO, energy harvesting, signal processing for communications, network coding, and wireless communication networks. He has authored about 50 papers in refereed journals and conference proceedings and holds five patents in China. He received the URSI Young Scientists Award in 2014 and the 2010 Ten Excellent Doctor Degree Dissertation Award of PLAUST. He also serves as the Reviewer of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATION, the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICLE TECHNOLOGY.

Xiaochen Xia was born in 1987. He received the B.S. degree in electronic science and technology from Tianjin University (TJU) in 2010, and the M.S. and Ph.D. degrees in communication and information system from the Army Engineering University of PLA in 2013. His research interests include signal processing in MIMO systems, machine learning for communications, cooperative networks, and full-duplex communications. He received the 2013 excellent master degree dissertation awards of Jiangsu Province, China, and the Army Engineering University of PLA. He also received the 2018 excellent doctor degree dissertation awards of the Chinese Institute of Command and Control (CICC) and the Army Engineering University of PLA. He serves as a Reviewer for the IEEE WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICLE TECHNOLOGY.