IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2020, accepted March 28, 2020, date of publication April 13, 2020, date of current version April 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987606

A Comparison of TDD and FDD Massive MIMO Systems Against Smart Jamming

ASHKAN SHEIKHI[1], (Member, IEEE),
S. MOHAMMAD RAZAVIZADEH[1], (Senior Member, IEEE),
AND INKYU LEE[2], (Fellow, IEEE)
[1]School of Electrical Engineering, Iran University of Science and Technology, Tehran 16844, Iran
[2]School of Electrical Engineering, Korea University, Seoul 02841, South Korea

Corresponding authors: S. Mohammad Razavizadeh (smrazavi@iust.ac.ir) and Inkyu Lee (inkyu@korea.ac.kr)

This work was supported by the National Research Foundation through the Ministry of Science, ICT, and Future Planning (MSIP), Korean Government, under Grant 2017R1A2B3012316.

ABSTRACT Frequency division duplex (FDD) massive multiple-input multiple-output (MIMO) systems introduce a large overhead in downlink channel estimation in contrast to the time division duplex (TDD) mode. This overhead results in a considerable spectral efficiency (SE) gap between the FDD and TDD modes. In this paper, we consider the performance of the TDD and FDD massive MIMO systems with a spatially correlated channel in the presence of jamming in the network. We show how a smart jammer can effectively design its attack signal to degrade the network performance in terms of the downlink SE. Since the jammer can obtain different information about the channels in the TDD and FDD modes, two distinct jamming strategies are proposed for each mode. In the numerical results, the performance of both the TDD and FDD modes under the optimized jamming designs are evaluated and compared. Our results show that despite more attention to the TDD mode in current massive MIMO systems, it is more vulnerable to smart jamming attacks compared to the FDD mode which results in a smaller SE-gap between the modes. Furthermore, a countermeasure technique is proposed to combat this jamming attack in both the TDD and FDD modes by estimating the jamming power, grouping users, and allocating power among them. The numerical results demonstrate the effectiveness of the proposed countermeasure techniques in both the TDD and FDD modes.

INDEX TERMS Frequency division duplex (FDD), massive MIMO, physical layer security, smart jamming, time division duplex (TDD).

I. INTRODUCTION

Massive multiple input multiple output (MIMO) technique is one of the main solutions to meet the huge capacity demands in 5G networks. In massive MIMO systems, a large number of antennas are used at the base stations (BSs) that serve low-complexity user equipments (UEs) [1]. By adopting this technology, a remarkable improvement in the network spectral efficiency (SE) can be achieved even with linear processing and non-ideal hardware [2]. To get these advantages, it is crucial to acquire accurate channel state information (CSI) at the BS [3], [4]. Massive MIMO can be deployed in time division duplex (TDD) and frequency division duplex (FDD) modes. Taking advantage of channel reciprocity in the TDD systems, the channel estimation process can be much simpler than the FDD systems, and hence the TDD mode is often preferred in implementing massive MIMO systems. Obtaining the downlink CSI in the FDD massive MIMO systems may incur a huge training overhead which reduces the SE of the network. However, most of the current wireless networks are working in the FDD mode and it is still favored by network operators. Recently, many researches have been conducted on adopting FDD for massive MIMO systems by reducing the downlink training and feedback overhead, e.g. [5]–[8].

On the other hand, security has always been an important concern in wireless networks. Eavesdropping and jamming, which are two major security issues in wireless systems, can endanger confidentiality and reliability of such systems. The security issues can be studied in all layers of the network. Physical layer security is known as an efficient approach to deal with the security problems in wireless channels [9]–[11]. Recently, the physical layer security has been investigated extensively in the massive MIMO systems [12]–[21].

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

Massive MIMO has been shown to be resilient against passive eavesdropping due to high degree of freedom. However, an active eavesdropper that attacks the training phase can introduce pilot contamination in the network and drastically degrades the system performance [12], [13]. In [12], the secrecy rate analysis of massive MIMO systems in the presence of the pilot contamination attack was addressed. The authors in [13] considered power allocation for a smart jammer who tries to attack both training and data phases in the uplink of a TDD massive MIMO network. A multi-cell TDD massive MIMO was studied in [14] with a passive eavesdropper in the network. An information theoretic analysis was conducted to assess the secrecy rate and the outage probability by adopting matched filter precoding and artificial noise generation at the BS. An active eavesdropper was examined in [15] for the same scenario as in [14] and the asymptotic results were derived under a pilot contamination attack. The maximum secure degree of freedom of a TDD massive MIMO with pilot contamination attack was investigated in [16]. An advanced adversary with a full-duplex large-scale array was analyzed in [17] for a TDD massive MIMO network, and the achievable ergodic secrecy rate of the system was derived. The authors in [18] presented a robust receiver scheme in the uplink of a TDD massive MIMO to make the system resilient against jamming attacks. In [19], a jamming detection method for the TDD massive MIMO systems was illustrated by exploiting unused pilots in the training phase. A jamming suppression method was proposed in [20] for TDD massive MIMO systems. Note that almost all of the previous works on the physical layer security of massive MIMO systems have considered the TDD mode, and to the best of our knowledge, the FDD mode has not been studied before in the literature.

In this paper, we address the problem of physical layer security in massive MIMO networks in both the TDD and FDD modes. In particular, we examine a multi-user massive MIMO system with spatially correlated channels where there is a multi-antenna smart jammer who aims to degrade the data transfer from the BS to the UEs. This problem is investigated from two points of view. First, from the jammer's perspective, we design optimal jamming attack strategies for each of the TDD and FDD modes. Then, we develop a countermeasure method to suppress the jamming effect and improve the network SE. The main contributions of this paper can be summarized as follows.

- Two smart jamming schemes are introduced to attack the downlink of massive MIMO systems with spatially correlated channels for each of the TDD and FDD modes.
- A countermeasure technique is proposed for both the TDD and FDD massive MIMO systems to improve the network SE under the jamming attacks. By adopting our proposed countermeasure, the BS can use its transmit power efficiently to suppress the jamming effect on network SE.
- A comparison between the TDD and FDD massive MIMO systems under the smart jamming attacks is conducted. We show that the TDD mode is more vulnerable against a smart jamming attack compared to the FDD mode, because the smart jammer can obtain more information about the channels in the TDD mode. As a result, the SE gap between the TDD and FDD modes in massive MIMO systems can become quite small.

The rest of this paper is organized as follows: In Section II, the system model and channel structure are introduced. Section III presents the proposed jamming strategies and the signal design problems. We propose the countermeasure in Section IV. Section V illustrates the simulation results and finally, Section VI concludes the paper.

Throughout the paper, we use boldface uppercase, boldface lowercase and italic letters to denote matrices, vectors and scalars, respectively. The notation $(.)^H$ indicates conjugate transpose and $\boldsymbol{A}(i:j)$ represents a matrix containing columns i through j of a matrix $\boldsymbol{A}$. The expectation operator is expressed by $\mathbb{E}\{.\}$ and $\boldsymbol{v} \sim CN(0, \boldsymbol{R})$ stands for circularly symmetric complex Gaussian random vectors with zero mean and covariance matrix $\boldsymbol{R}$. An $L \times L$ identity matrix is defined by $\boldsymbol{I}_L$. The covariance matrix of two random vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ is denoted by $\boldsymbol{C}_{\boldsymbol{x},\boldsymbol{y}}$. We indicate the inner product of two matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ by $\langle \boldsymbol{A}, \boldsymbol{B} \rangle$. The subspace which spans the vectors $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_K$ is represented by $Span(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_K)$.

II. SYSTEM AND CHANNEL MODEL

We consider a multi-user network consisting of a large-scale BS using $M \gg 1$ antennas to serve K single-antenna UEs. There is a smart jammer in the network equipped with N antennas who intends to degrade the network SE as much as possible. Fig. 1 illustrates the system model. The block fading channel model is assumed in which the channels are constant in the time-frequency plane in each block, defined by the coherence bandwidth and the coherence time of the channels, and change independently between different blocks. We also assume that the channels are spatially correlated which is a more realistic model. The fading channel from the BS and the jammer to the k'th UE are modeled as $\boldsymbol{h}_k \in \mathbb{C}^{M\times 1}$ and $\boldsymbol{g}_k \in \mathbb{C}^{N\times 1}$, respectively, where $\boldsymbol{h}_k \sim CN(0, \boldsymbol{\Gamma}_k)$ and $\boldsymbol{g}_k \sim CN(0, \boldsymbol{R}_k)$ with $\boldsymbol{\Gamma}_k$ and $\boldsymbol{R}_k$ being the covariance matrices of the channels. In addition, the path-loss plus shadowing in the channels from the BS and the jammer to the k'th UE are defined by η_k and β_k, respectively. The k'th UE receives a composition of the signals transmitted by the BS and the jammer as

$$y_k = \sqrt{P_k \eta_k}\boldsymbol{h}_k^H \boldsymbol{w}_k s_k + \sqrt{\beta_k}\boldsymbol{g}_k^H \boldsymbol{z} + \sum_{i=1, i\neq k}^{K} \sqrt{P_i \eta_k}\boldsymbol{h}_k^H \boldsymbol{w}_i s_i + n_k, \quad (1)$$

where $\boldsymbol{z}$ is the signal transmitted by the jammer, P_i, $\boldsymbol{w}_i \in \mathbb{C}^{M\times 1}$, and s_i represent the transmit power, the precoding vector, and the data symbol intended for the i'th UE, respectively, and $n_k \sim CN(0, \sigma_k^2)$ indicates the additive white Gaussian noise (AWGN) at the k'th UE.

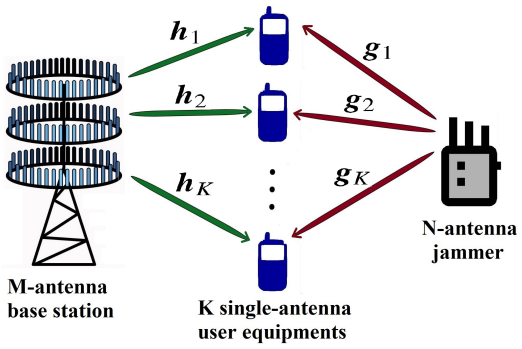

FIGURE 1. System model.

By employing the channel covariance matrix, the channel vector $\boldsymbol{h}_k$ can be decomposed as

$$\boldsymbol{h}_k = \sqrt{M}\boldsymbol{\Gamma}_k^{1/2}\boldsymbol{x}_k, \tag{2}$$

where $\boldsymbol{x}_k \sim CN(0, \frac{1}{M}\boldsymbol{I}_M)$. Since we intend to study the massive MIMO system performance under a jamming attack in the downlink data phase of both the TDD and FDD modes, we adopt a flexible model for the estimated channel that can be used irrespective of the duplex mode of the system.

The estimated channel at the BS is modeled as [22]–[25]

$$\hat{\boldsymbol{h}}_k = \sqrt{M}\boldsymbol{\Gamma}_k^{1/2}\left(\sqrt{1-\tau_k^2}\boldsymbol{x}_k + \tau_k\boldsymbol{e}_k\right), \tag{3}$$

where $\boldsymbol{e}_k \sim CN(0, \frac{1}{M}\boldsymbol{I}_M)$ is a random vector independent of $\boldsymbol{x}_k$ to model the channel estimation error and $\tau_k \in [0, 1]$ accounts for the accuracy of the estimation. The regulating parameter τ_k can take into account the difference in estimation errors between the TDD and FDD modes, due to distinct downlink channel estimation approaches. Smaller values of τ_k correspond to more accurate estimation of the channel. The value of τ_k depends on many factors including the length and power of training sequences, pilot contamination effects, and the quality of the CSI feedback links. In general, in the TDD mode, the minimum length of the training sequences is $L = K$ while in the FDD mode it is $L = M$. However, by exploiting the spatial correlation of the channels, the length of the pilot sequences in the FDD mode can be chosen much smaller than M [5]–[8]. In this paper, we assume $L = \alpha M$ for the FDD mode where $\alpha \leq 1$ determines the training overhead.

By assuming uniform distribution of the scatters in the environment and linear uniform arrays at both the BS and the jammer, we use the one-ring model to describe the spatial correlation between the channel coefficients as [26]

$$[\boldsymbol{R}]_{i,j} = \frac{1}{2\Delta}\int_{-\Delta+\theta}^{\Delta+\theta} e^{-j2\pi D(i-j)sin\alpha}d\alpha, \tag{4}$$

where Δ represents the angular spread, θ indicates the azimuth angle of the UE, and D is the antenna spacing.

III. JAMMING ATTACK DESIGN

For a smart jamming signal design, we propose the jamming signal to be modeled as a zero-mean complex Gaussian random vector $\boldsymbol{z} \sim CN(0, \boldsymbol{R}_z)$ with covariance matrix $\boldsymbol{R}_z = \mathbb{E}(\boldsymbol{z}\boldsymbol{z}^H)$, where $\boldsymbol{R}_z$ is the matrix to be designed. To this end, we first use eigenvalue decomposition of $\boldsymbol{R}_z$ as $\boldsymbol{R}_z = \boldsymbol{U}_z\boldsymbol{D}_z\boldsymbol{U}_z^H$ where $\boldsymbol{D}_z = diag(\lambda_{z_1}, \lambda_{z_2}, \ldots, \lambda_{z_N})$ is a diagonal matrix containing the eigenvalues of $\boldsymbol{R}_z$ in decreasing order and $\boldsymbol{U}_z$ denotes a unitary matrix consisting of the corresponding eigenvectors. The matrix $\boldsymbol{U}_z$ determines the subspace of the jamming signal. To design the jamming signal, the jammer selects the best eigenvalues (and corresponding eigenvectors) by exploiting its information about the legitimate system and considering a utility function.

As we assume that the jammer cannot acquire any information about the channels between the BS and the UEs, it is also not possible for the jammer to estimate the network SE or the received signal-to-interference-plus-jamming and noise ratio (SIJNR) at the UEs. Therefore, a smart strategy at the jammer is to maximize its jamming power at the UEs during the downlink data transmission. This power depends on the channels from the UEs to the jammer in each coherence block.

The average jamming power Q_k received at the k'th UE in each realization of the channels is

$$Q_k = \mathbb{E}_z\left[\left|\sqrt{\beta_k}\boldsymbol{g}_k^H\boldsymbol{z}\right|^2\right] = \beta_k\boldsymbol{g}_k^H\boldsymbol{R}_z\boldsymbol{g}_k = \langle\boldsymbol{R}_z, \beta_k\boldsymbol{g}_k\boldsymbol{g}_k^H\rangle, \tag{5}$$

where the last equality results from the cyclic property of inner product. Depending on the operation mode of the massive MIMO system, the smart jammer may adopt different strategies to maximize the jamming powers at the UEs. This is related to different information that the jammer can acquire in the two modes.

A. TDD MODE

In the TDD mode, because of the reciprocity property,[1] the BS can estimate the downlink CSI directly from the uplink CSI using the pilots transmitted by the UEs in the uplink training phase. It is beneficial as the uplink training overhead is independent of the number of BS antennas. In a similar way, a smart jammer who knows the pilots used in the system, can take advantage of this reciprocity and exploit the pilots transmitted by the UEs to estimate the instantaneous channels between the jammer and UEs. We will show how it can jeopardize the TDD massive MIMO systems against downlink jamming attacks.

In the uplink training phase, the UEs transmit orthogonal pilots $\boldsymbol{\phi}_i$ $(i = 1, 2, \ldots, K)$ and the jammer receives the signal $\boldsymbol{Y}_j$ which can be expressed as

$$\boldsymbol{Y}_j = \sum_{k=1}^{K}\sqrt{\beta_k\rho}\boldsymbol{g}_k\boldsymbol{\phi}_k + \boldsymbol{N}_j \tag{6}$$

[1]It should be noted that in practical systems, calibration on the estimated channels is needed, which has been investigated well in the massive MIMO literature.

where ρ is the uplink training power of the UEs, $\boldsymbol{\phi}_k \in \mathbb{C}^{1\times L}$ represents the normalized pilot sequence of length L, i.e. $\boldsymbol{\phi}_k\boldsymbol{\phi}_k^H = L$, assigned to the k'th UE, and $\boldsymbol{N}_j \in \mathbb{C}^{N\times L}$ indicates the AWGN at the jammer with entries of zero-mean and variance σ_j^2.

Using the orthogonality of the pilots, the jammer computes

$$\tilde{\boldsymbol{y}}_k = \frac{1}{\sqrt{\beta_k\rho}L}\boldsymbol{Y}_j\boldsymbol{\phi}_k^H = \boldsymbol{g}_k + \tilde{\boldsymbol{n}}_j \tag{7}$$

where $\tilde{\boldsymbol{n}}_j = \frac{\boldsymbol{N}_j\boldsymbol{\phi}_k^H}{\sqrt{\beta_k\rho}L} \sim CN(0, \frac{\sigma_j^2}{\beta_k\rho L}\boldsymbol{I}_N)$. Therefore, the jammer can exploit the channel reciprocity in the TDD mode and apply $\tilde{\boldsymbol{y}}_k$ to estimate the channels from the jammer to the UEs $\boldsymbol{g}_k$. In a worst-case scenario, the jammer may have access to the channel correlation matrices of the UEs and adopt a minimum mean square error (MMSE) estimator to find $\boldsymbol{g}_k$ with high accuracy. After estimating $\boldsymbol{g}_k$, the jammer can obtain the received jamming power Q_k at the k'th UE. Then the jammer chooses $\boldsymbol{U}_z$ and $\boldsymbol{D}_z$ based on the values of Q_k. Here, the jammer can employ two approaches for designing $\boldsymbol{R}_z$ as follows.

1) MAXIMIZING SUM OF THE JAMMING POWER AT THE UEs (MaxSum)

An efficient strategy that the jammer can follow for designing its attack signal is to deliver as much power as possible to all the UEs. By using this strategy, the jammer affects some specific UEs which are more vulnerable to the jamming attack. This is suitable for the cases where the jammer has low transmission power. To this end, the optimization problem for jamming design is formulated as

$$\begin{aligned}\max_{\boldsymbol{R}_z}\ & \sum_{k=1}^{K} Q_k = \langle \boldsymbol{R}_z, \sum_{k=1}^{K}\beta_k\boldsymbol{g}_k\boldsymbol{g}_k^H\rangle\\ \text{s.t. } & tr(\boldsymbol{R}_z) \le P_j\\ & \boldsymbol{R}_z = \boldsymbol{R}_z^H\\ & \boldsymbol{R}_z \succeq 0\end{aligned} \tag{8}$$

where P_j is the maximum transmission power at the jammer. This is a convex optimization problem [27] and the following lemma gives its closed-form solution.

Lemma 1: Defining $\boldsymbol{G} = \sum_{k=1}^{K}\beta_k\boldsymbol{g}_k\boldsymbol{g}_k^H$, the optimal matrix $\boldsymbol{R}_z^*$ that solves the problem in (8) is

$$\boldsymbol{R}_z^* = P_j\boldsymbol{u}_{\boldsymbol{G}_1}\boldsymbol{u}_{\boldsymbol{G}_1}^H \tag{9}$$

where $\boldsymbol{u}_{\boldsymbol{G}_1}$ is the eigenvector corresponding to the largest eigenvalue of the matrix $\boldsymbol{G}$.

Proof: See Appendix. ∎

The optimal solution (9) states that the jammer should generate its attack signal in the one-dimensional subspace aligned with the dominant eigenvector of the matrix $\boldsymbol{G}$. A closer look at $\boldsymbol{G}$ reveals that it is the summation of K rank-1 matrices, and thus its rank is $min(N, K)$. Although the dominant eigenvector of $\boldsymbol{G}$ is determined by the channel gains of all the UEs, i.e. $\beta_k\|\boldsymbol{g}_k\|_2^2$ $(k = 1, 2, \ldots, K)$, the UEs with larger channel gains have more contributions. Consequently, the *MaxSum* design generates more jamming power at these UEs. Therefore, if the channel gains have large variations, e.g. when the jammer is very close to one UE and far from other UEs, this design may neglect the UEs with weaker channel gains and only a small portion of the UEs will be under attack.

2) MAXIMIZING PRODUCT OF THE JAMMING POWER AT THE UEs (MaxProd)

When the jamming power is sufficient, the jammer can follow another approach to affect a larger number of the UEs and degrade the network SE more severely. In fact, the jammer must select a cost function to deliver high jamming power to a larger group of the UEs. We propose a scheme which maximizes the product of the jamming powers $\prod_{k=1}^{K} Q_k$. In fact, to maximize this cost function, the jamming power at the UEs should be close to each other. Therefore, a large number of UEs will be affected by the jamming attack. In this approach, the optimization problem for jamming design becomes

$$\begin{aligned}\max_{\boldsymbol{R}_z}\ & \prod_{k=1}^{K} Q_k = \prod_{k=1}^{K}\langle \boldsymbol{R}_z, \beta_k\boldsymbol{g}_k\boldsymbol{g}_k^H\rangle\\ \text{s.t. } & tr(\boldsymbol{R}_z) \le P_j\\ & \boldsymbol{R}_z = \boldsymbol{R}_z^H\\ & \boldsymbol{R}_z \succeq 0.\end{aligned} \tag{10}$$

Based on the solution of (8), we conclude that the subspace of the matrix $\boldsymbol{R}_z$ must be the same as the orthogonal subspace which spans all the channel vectors $\boldsymbol{g}_k$. We define this subspace as

$$\boldsymbol{V} = Span\left(\frac{\boldsymbol{g}_1}{\|\boldsymbol{g}_1\|_2}, \frac{\boldsymbol{g}_2}{\|\boldsymbol{g}_2\|_2}, \ldots, \frac{\boldsymbol{g}_K}{\|\boldsymbol{g}_K\|_2}\right). \tag{11}$$

By representing each orthonormal basis of this subspace by $\boldsymbol{v}_i$, the optimal matrix $\boldsymbol{R}_z^*$ is selected as

$$\boldsymbol{R}_z^* = \sum_{i=1}^{r} p_i\boldsymbol{v}_i\boldsymbol{v}_i^H, \tag{12}$$

where p_i is the eigenvalue corresponding to $\boldsymbol{v}_i$, to be optimized. Note that $r \le min(N, K)$.

Assuming this structure for $\boldsymbol{R}_z^*$, the optimization problem in (10) can be converted to

$$\begin{aligned}\max_{p_1,\ldots,p_r}\ & \prod_{k=1}^{K}\langle \sum_{i=1}^{r} p_i\boldsymbol{v}_i\boldsymbol{v}_i^H, \beta_k\boldsymbol{g}_k\boldsymbol{g}_k^H\rangle\\ \text{s.t. } & \sum_{i=1}^{r} p_i = P_j,\\ & p_i \ge 0 \quad i = 1, \ldots, r.\end{aligned} \tag{13}$$

Because of the non-convex cost function in (13), this problem is non-convex and cannot be solved efficiently in the current form. However, it can be transformed to a convex problem by defining

$$\prod_{k=1}^{K}\langle \sum_{i=1}^{r} p_i\boldsymbol{v}_i\boldsymbol{v}_i^H, \beta_k\boldsymbol{g}_k\boldsymbol{g}_k^H\rangle = \prod_{k=1}^{K}\boldsymbol{b}_k^T\boldsymbol{p}, \tag{14}$$

where $\boldsymbol{b}_k = \left[\langle \boldsymbol{v}_1 \boldsymbol{v}_1^H, \beta_k \boldsymbol{g}_k \boldsymbol{g}_k^H \rangle, \ldots, \langle \boldsymbol{v}_r \boldsymbol{v}_r^H, \beta_k \boldsymbol{g}_k \boldsymbol{g}_k^H \rangle\right]^T$ and $\boldsymbol{p} = [p_1, p_2, \ldots, p_r]^T$. Instead of maximizing $\prod_{k=1}^{K} \boldsymbol{b}_k^T \boldsymbol{p}$, we can maximize its logarithm. Therefore, the optimization problem in (13) is equivalent to

$$\begin{aligned} \max_{\boldsymbol{p}} \ & \sum_{k=1}^{K} log \boldsymbol{b}_k^T \boldsymbol{p} \\ \text{s.t. } & \mathbf{1}^T \boldsymbol{p} = P_j, \\ & p_i \geq 0, \quad i = 1, \ldots, r, \end{aligned} \tag{15}$$

where $\mathbf{1}$ represents a vector whose elements are all one. The problem (15) is convex and can be efficiently solved by using the available numerical methods [27].

B. FDD MODE

In the FDD mode, the uplink and downlink channels operate in separate frequency bands. Therefore, the reciprocity property does not hold and the BS has to transmit pilot signals to the UEs so that each UE estimates its own downlink channel gain and feeds back it to the BS. In contrast to the TDD mode, the jammer cannot exploit the pilots transmitted by the UEs to estimate the channels from the jammer to the UEs. However, the jammer can acquire the channels from the UEs to the jammer using the pilots transmitted by the UEs. Then, the jammer can exploit this information to obtain second-order statistics of the channels.

In our proposed jamming method in the FDD mode, the jammer first estimates the correlation matrix of the channels from the UEs to the jammer. Then, it should convert this matrix to the reverse direction channel correlation matrix, i.e. $\boldsymbol{R}_k$. Many techniques have been developed in the multi-user MIMO systems which can be used for this purpose, e.g. [28]–[32]. We consider a worst-case scenario where the jammer has obtained perfect estimation of the correlation matrices $\boldsymbol{R}_k$ $(k = 1, 2, \ldots, K)$. Note that these matrices vary slowly over time and once the jammer estimates them, they can be used for a period of time without being outdated.

Apparently, the jammer cannot compute the received jamming power Q_k at the UEs in each realization of the channel. However, since the jammer knows the correlation matrices $\boldsymbol{R}_k$, it can obtain the average received jamming power at each UE as

$$\overline{Q}_k = \mathbb{E}\left[Q_k\right] = \mathbb{E}\left[\beta_k \boldsymbol{g}_k^H \boldsymbol{R}_z \boldsymbol{g}_k\right] \tag{16}$$

$$= tr\left(\boldsymbol{R}_z \mathbb{E}\left[\beta_k \boldsymbol{g}_k \boldsymbol{g}_k^H\right]\right) = \langle \boldsymbol{R}_z, \beta_k \boldsymbol{R}_k \rangle. \tag{17}$$

Similar to the TDD mode, the jammer has two options to design its attack signal.

1) MAXIMIZING SUM OF THE AVERAGE JAMMING POWER AT THE UEs (MaxSum)

In this case, the optimization problem for jamming design becomes

$$\max_{\boldsymbol{R}_z} \sum_{k=1}^{K} \overline{Q}_k = \langle \boldsymbol{R}_z, \sum_{k=1}^{K} \beta_k \boldsymbol{R}_k \rangle$$

$$\begin{aligned} \text{s.t. } & tr(\boldsymbol{R}_z) \leq P_j \\ & \boldsymbol{R}_z = \boldsymbol{R}_z^H \\ & \boldsymbol{R}_z \succeq 0. \end{aligned} \tag{18}$$

This problem is similar to (8) and its solution can be found by Lemma 1 with selecting $\boldsymbol{G} = \sum_{k=1}^{K} \beta_k \boldsymbol{R}_k$. Here, the dominant eigenvector of the matrix $\boldsymbol{G}$ is associated with the UEs with larger values of $tr(\beta_k \boldsymbol{R}_k)$, i.e. the UEs with larger values of β_k and eigenvalues. Therefore, when some particular UEs have significantly better long-term statistical channel conditions, the *MaxSum* jamming design would not affect all the UEs, and a large portion of them may be immune to this jamming. Note that in contrast to the TDD mode, the jammer does not need to update the attack signal in each realization of the channel, since the design is based on the long-term statistics of the channel.

2) MAXIMIZING PRODUCT OF THE AVERAGE JAMMING POWER AT THE UEs (MaxProd)

The same analysis as in the TDD mode holds here, except that the jammer uses $\beta_k \boldsymbol{R}_k$ instead of $\beta_k \boldsymbol{g}_k \boldsymbol{g}_k^H$ in (10), and the optimal subspace of $\boldsymbol{R}_z$ should be constructed based on the eigenvectors of all the UEs as

$$\boldsymbol{V} = Span\left[\boldsymbol{u}_{1_1}, \boldsymbol{u}_{2_1}, \ldots, \boldsymbol{u}_{K_1}\right] \tag{19}$$

where $\boldsymbol{u}_{k_1}$ is the dominant eigenvector of $\boldsymbol{R}_k$. With this definition, the jammer obtains $\boldsymbol{R}_z^*$ similar to (12) - (15) by replacing $\beta_k \boldsymbol{g}_k \boldsymbol{g}_k^H$ with $\beta_k \boldsymbol{R}_k$ for each UE.

Remark 1: It is interesting to note the difference between the TDD and FDD modes when dealing with the jamming attacks. In the TDD mode, the jammer adjusts its jamming signal subspace continuously based on the instantaneous CSI. In contrast, in the FDD mode, the jammer selects $\boldsymbol{R}_z$ based on the long-term behavior of the channel, i.e. second-order statistics. Therefore, the TDD jamming design demands more computational complexity compared to the FDD mode.

IV. COUNTERMEASURE AGAINST JAMMING

In the previous section, we have discussed the optimal strategies for a jammer to effectively degrade the massive MIMO system's performance in both the TDD and FDD modes. Now in this section, we will propose a countermeasure technique at the BS against the jamming attacks. We present a three-step method to suppress the jamming impact on the system. Our proposed countermeasure is mainly a smart power allocation method based on the received jamming power at the UEs. One should note that because of the channel hardening property in massive MIMO systems [2], the BS can rely on the large-scale variations of the channel for downlink power allocation. The signal to interference plus jamming and noise ratio (SIJNR) $\widetilde{\Psi}_k$ is derived as (20), as shown at the bottom of the next page. Then, A lower bound for the k'th UE's SE can be derived as [2]

$$SE_k \geq \left(1 - \tfrac{L}{T_c}\right) \log_2\left(1 + \widetilde{\Psi}_k\right), \tag{21}$$

where L is the number of symbols dedicated to the channel estimation and T_c represents the size of a channel coherence block.

The BS has several options to select the power allocation cost function, e.g. sum-SE, max-min-SE, and SINR product of the UEs [2]. In [2], it was shown that if the product of the SINR of the UEs is adopted as the power allocation cost function, all the UEs are likely to experience high SE and this approach would result in better fairness in comparison to other power allocation schemes. However, in the presence of a jammer, some particular UEs located near the jammer may suffer from severe jamming interference. For such UEs, allocating more transmit power has negligible effect on their SE and this power is wasted without improving the system performance. In fact, if the product of $\widetilde{\Psi}_k$ for all the UEs is employed, these severely jammed UEs make the BS allocate more transmit power to them so that the fairness holds for all the UEs. Therefore, a more efficient approach for the BS in this scenario is to apply the summation of UEs' SE as the power allocation criterion. The sum-SE maximization problem is non-convex and cannot be solved effectively. Also, aside from the severely jammed UEs, the sum-SE as the power allocation may lead to unfairness among the remaining UEs. Therefore, we propose that the power allocation is performed in the following three steps.

A. JAMMING POWER ESTIMATION

In order to perform the power allocation with a cost function based on (21), the BS needs to have an estimation of the average jamming power received at each UE in advance. To do so, we propose that for a period of $C \ll T_c$ channel uses in n_t consecutive blocks, the BS does not transmit any signal in the downlink data phase. Therefore, in this period, each UE receives

$$y_{k_{c,n}} = \sqrt{\beta_k}\boldsymbol{g}_{k_{c,n}}^H \boldsymbol{z}_{k_{c,n}} + n_{k_{c,n}} \tag{22}$$

where $y_{k_{c,n}}$ is the signal received at the k'th UE in the c'th channel use of the n'th block. Then, the UEs compute an estimation of their received jamming power as

$$\hat{\overline{Q}}_k = \frac{1}{n_t C}\sum_{n=1}^{n_t}\sum_{c=1}^{C} y_{k_{c,n}} y_{k_{c,n}}^*. \tag{23}$$

Each UE quantizes the computed value and feeds back it to the BS. After n_t blocks, the BS has an estimation of the jamming power and can apply this information in the power allocation of the future blocks.

B. USER GROUPING

In this step, the BS assesses the received jamming power fed back from the UEs and groups the UEs into two different sets based on their jamming condition. We define Υ_J as a set containing the jammed UEs and Υ_S as a set including the safe UEs. For the k'th UE, if $\hat{\overline{Q}}_k \geq \chi \frac{P_0}{K}\theta_k \left|\mathbb{E}\left[\boldsymbol{h}_k^H \boldsymbol{w}_k\right]\right|^2$, the UE will be in the jammed group, otherwise the UE will be in the safe group. The parameter χ is a positive scalar and determines the threshold of the grouping. Selecting a large value for χ may result in including some severely jammed UEs in the safe set, which degrades the countermeasure performance. On the other hand, smaller values of χ can cause a large number of UEs to be designated as jammed UEs, which is not favorable for the network performance as described in the next step.

C. POWER ALLOCATION

After grouping the UEs in the previous step, the BS allocates its downlink power among the UEs by considering the grouping information. The UEs in the jammed group are severely affected by the jamming attack and increasing their power cannot improve their SE significantly. Thus, the BS power will be wasted without increasing the network SE. Therefore, for that group the BS sets the jammed UEs' power to zero, i.e. $P_k = 0$, for $k \in \Upsilon_J$, and serves only the safe group UEs by considering the following optimization problem

$$\begin{aligned} &\max_{P_k,\ k\in\Upsilon_S} \prod_{k\in\Upsilon_S} \widetilde{\Psi}_k \\ &\text{s.t.} \sum_{k\in\Upsilon_S} P_k = P_0, \\ &\quad P_k \geq 0 \quad \textit{for} \ \ k \in \Upsilon_S. \end{aligned} \tag{24}$$

This problem can be converted to a geometric programming optimization problem easily by defining an auxiliary variable and then it can be solved by numerical tools [27].

The proposed countermeasure can be adopted in both the TDD and FDD modes. However, one should note that in the FDD mode, the jammer designs $\boldsymbol{R}_z$ based on the correlation matrices of $\boldsymbol{g}_k$. Therefore, the jammer does not update $\boldsymbol{R}_z$ during n_t blocks. In contrast, in the TDD mode, this matrix is selected based on the instantaneous values of $\boldsymbol{g}_k$ and varies with time during n_t blocks. Thus, the jamming power estimation in (23) can be performed with better accuracy in the FDD mode.

V. SIMULATION RESULTS

For numerical validation of the proposed jamming attacks and the countermeasure, we consider a massive MIMO network consisting of a BS with M antennas which serves $K = 10$ single antenna UEs in a cell with the radius of 500 m. Also, there is a jammer with $N = 16$ antennas located at a distance of 250 m from the BS. The UEs are uniformly and randomly

$$\widetilde{\Psi}_k = \frac{P_k\theta_k \left|\mathbb{E}\left[\boldsymbol{h}_k^H \boldsymbol{w}_k\right]\right|^2}{\sum_{i=1}^{K} P_i\theta_k \mathbb{E}\left[\left|\boldsymbol{h}_k^H \boldsymbol{w}_i\right|^2\right] - P_k\theta_k \left|\mathbb{E}\left[\boldsymbol{h}_k^H \boldsymbol{w}_k\right]\right|^2 + \beta_k \mathbb{E}\left[\boldsymbol{g}_k^H \boldsymbol{R}_z \boldsymbol{g}_k\right] + \sigma_k^2}. \tag{20}$$

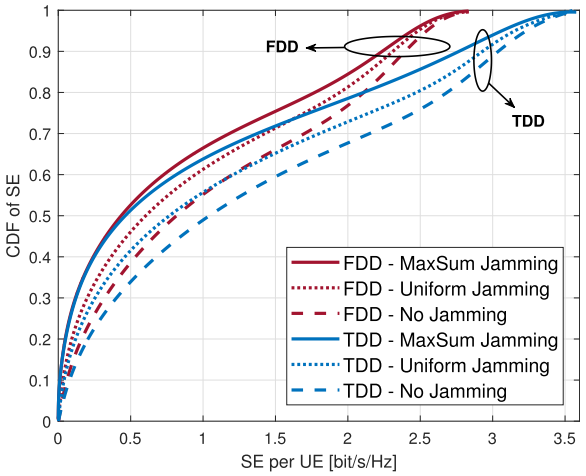

FIGURE 2. The CDF of the SE for one UE in the network with MRT.

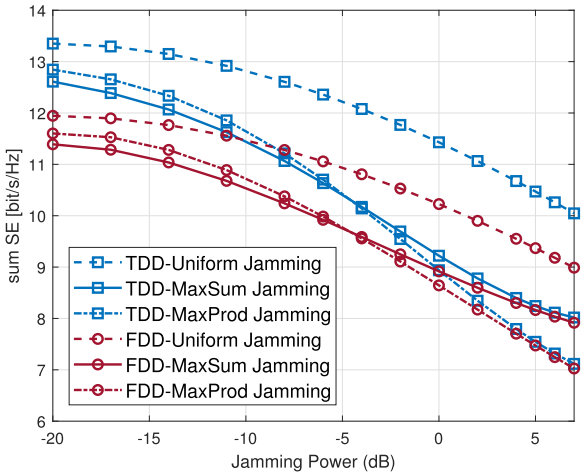

FIGURE 3. Sum SE with respect to jamming power for the proposed jamming designs with RZF precoder.

distributed in the cell with a minimum distance of 50 m to both the BS and the jammer. The path-loss exponent and the shadowing standard deviation are $n_l = 3.76$ and $\sigma_{sh} = 10$ dB, respectively. The central frequency equals $f_c = 2$ GHz and the uniform linear arrays with the antenna spacing of $D = \lambda/2$ are assumed at the BS and the jammer. The angular spread is set to $\Delta = 10°$ and the azimuth angle of the UEs, θ, is uniformly distributed in $[-60°, 60°]$. The estimation error parameter τ_k in (3) is assumed to be identical for all the UEs. We assume $\tau = 0.3$ and $\tau = 0.5$ for the TDD mode and the FDD mode, respectively. The FDD mode overhead coefficient is fixed at $\alpha = 0.5$ and the grouping threshold is assumed to be $\chi = 5$. All the figures are derived with 1500 different random setups of UEs locations.

First, we evaluate the performance of the smart jamming designs proposed in Section III in the TDD and the FDD modes. Then, we assess the performance of the proposed countermeasure on the jamming scenarios. To see the impact of the smart jamming design, we consider a naive jammer with the uniform jamming signal covariance matrix $\boldsymbol{R}_z$ as

$$\boldsymbol{R}_z^{uni} = \frac{P_j}{N}\boldsymbol{I}_N. \tag{25}$$

Fig. 2 compares the cumulative distribution function (CDF) of SE for one UE in the network under different jamming scenarios when the BS adopts maximum ratio transmission (MRT). As we see, when there is no jamming in the network, the TDD outperforms the FDD drastically due to high downlink overhead in the FDD mode. For the uniform jamming case, the same difference holds as expected. However, when our smart jamming designs proposed in Section III are employed, the TDD performance degrades more than the FDD. This difference can compensate the overhead effect such that the FDD mode performance gets close to the TDD mode with a high probability.

Fig. 3 presents the sum SE of all the UEs for different values of the jamming power when the BS adopts the regularized zero forcing (RZF) precoder. As we see, the proposed

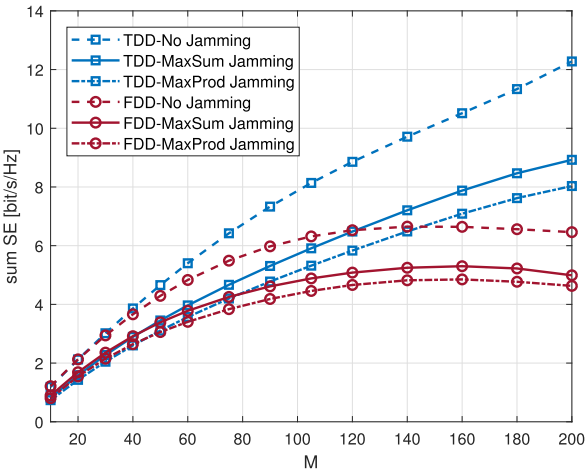

FIGURE 4. Sum SE with respect to the number of BS antennas for the proposed jamming designs with MRT.

MaxSum and *MaxProd* jamming attacks outperform the uniform jamming attack remarkably. However, for the TDD mode, by increasing the jamming power, the smart jamming designs have more severe impact on the SE and make the sum SE of the TDD become close to that of the FDD mode in the high jamming power environments. Also, as expected, the *MaxProd* jamming design works better than the *MaxSum* design for higher jamming power, because the *MaxProd* can affect more UEs. On the contrary, when the jamming power is not large enough, the *MaxSum* design would be a better choice for the jammer.

Figures 4 and 5 illustrate the sum-SE for different numbers of BS antennas with MRT and RZF precoding, respectively. When there is no jammer in the network, the TDD outperforms the FDD with increasing the number of antennas. However, when there is a smart jammer in the network, the TDD performance becomes close to the FDD up to around 100 antennas, which is a typical number in practical massive MIMO scenarios.

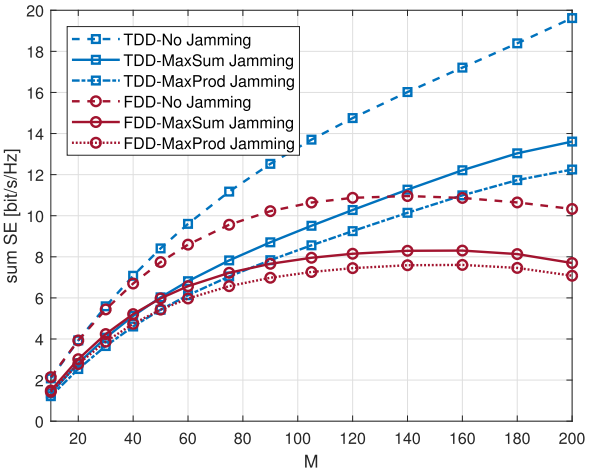

FIGURE 5. Sum SE with respect to the number of BS antennas for the proposed jamming designs with RZF precoder.

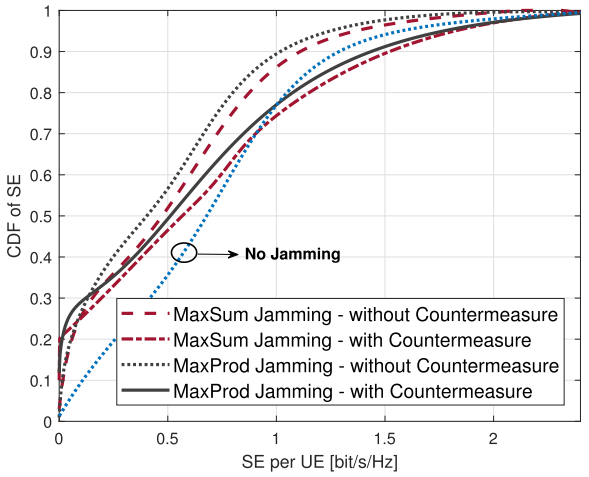

FIGURE 6. The CDF of SE for one UE in the FDD mode with MRT.

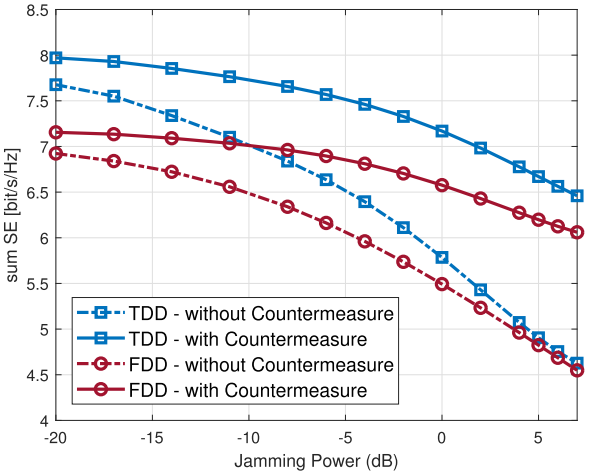

FIGURE 7. Sum SE with respect to jamming power with MaxProd jamming and MRT.

For the evaluation of the proposed countermeasure, Fig. 6 presents the CDF of SE for one UE in the FDD mode with MRT. The system performance without countermeasure and the case with no jammer in the network are also plotted

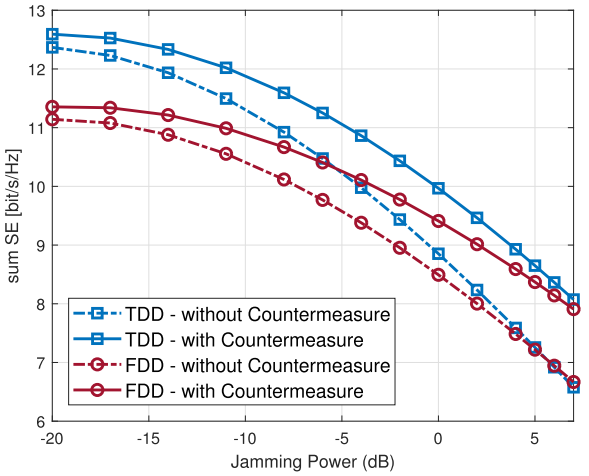

FIGURE 8. Sum SE with respect to jamming power with MaxProd jamming and RZF precoder.

for comparison. In the no jamming case, the BS is assumed to adopt equal power allocation. Apparently, the system performance without the countermeasure has a significant gap with the no jamming scenario. By applying our proposed countermeasure, this gap narrows and the probability of having a higher SE for the UEs improves remarkably. In addition, the SE for the UEs in the safe group can even outperform the no jamming case which is due to the merit of non-equal power allocation in the countermeasure.

Fig. 7 shows the effect of the proposed countermeasure on the sum SE of the system under different jamming attacks for the TDD and the FDD mode with MRT. As expected, this countermeasure can provide significant gains in the sum SE, because it prevents wasting the power on the severely jammed UEs. Even at high jamming power, our proposed countermeasure works well. Fig. 8 exhibits the results with RZF precoding. In this regard, the countermeasure can bring the tremendous improvement in sum SE again. By comparing Figures 7 and 8, one should note that in the high jamming power regime, adopting the proposed countermeasure with MRT case can result in the same performance as the case with RZF precoding without any countermeasure.

VI. CONCLUSION

In this paper, we have studied the impact of smart data jamming attacks on massive MIMO systems in the TDD and FDD modes. We have shown that the TDD massive MIMO system is more vulnerable to smart data jamming attacks compared to the FDD mode because the smart jammer can acquire more information about the channels in the TDD mode. Based on the difference in the channel information acquisition in the two modes, we have proposed two smart jamming designs. Simulation results have demonstrated that the SE-gap between the TDD and FDD modes becomes remarkably narrow in the presence of the smart jammers, due to more vulnerability of the TDD mode. Then, we have proposed a jamming countermeasure at the BS against such smart jamming attacks. This approach consists of three steps:

jamming power estimation, user grouping, and power allocation at the BS. Simulation results have proven that by using this countermeasure, the BS can improve the network SE against the smart jamming attacks significantly.

APPENDIX

The optimization problem in (8) is convex and can be solved using the Lagrangian method. Denoting the eigenvalue decomposition of $\boldsymbol{G}$ as $\boldsymbol{G} = \boldsymbol{U}_G \boldsymbol{D}_G \boldsymbol{U}_G^H$ and defining $\boldsymbol{X} = \boldsymbol{U}_G^H \boldsymbol{R}_z^* \boldsymbol{U}_G$, this problem is equivalent to maximizing the cost function $\langle \boldsymbol{D}_G, \boldsymbol{X} \rangle$ under the same constraints where $\boldsymbol{R}_z^* = \boldsymbol{U}_z^H \boldsymbol{D}_z \boldsymbol{U}_z$ is the optimal solution to this problem. The Lagrangian is computed as

$$\mathbb{L} = -\langle \boldsymbol{D}_G, \boldsymbol{X} \rangle + \nu \left(\langle \boldsymbol{I}_N, \boldsymbol{X} \rangle - P_j \right) - \langle \boldsymbol{V}, \boldsymbol{X} \rangle, \tag{26}$$

where ν and $\boldsymbol{V}$ are Lagrangian multipliers. Then, Karush-Kuhn-Tucker (KKT) conditions [27] are expressed as

$$\langle \nu \boldsymbol{I}_N - \boldsymbol{D}_G \, , \boldsymbol{X} \rangle = 0, \tag{27}$$

$$\nu \boldsymbol{I}_N - \boldsymbol{D}_G \succeq 0, \tag{28}$$

$$tr(\boldsymbol{X}) = P_j, \tag{29}$$

$$\boldsymbol{X} \succeq 0, \tag{30}$$

$$\nu \geq 0, \tag{31}$$

where inequality (28) implies that $\nu \geq \lambda_{\boldsymbol{G}_1}$. We can rewrite (27) as

$$\langle \nu \boldsymbol{I}_N - \boldsymbol{D}_G \, , \boldsymbol{X} \rangle = \sum_{i=1}^{N} (\nu - \lambda_{\boldsymbol{G}_i}) \boldsymbol{X}_{ii} = 0, \tag{32}$$

where $\boldsymbol{X}_{ii}$ represents the i'th diagonal entry of $\boldsymbol{X}$. As $\nu \geq \lambda_{\boldsymbol{G}_1}$, we conclude that $(\nu - \lambda_{\boldsymbol{G}_i}) \geq 0$ for $i = 1, \ldots, N$. Therefore, the only case where the above equality holds occurs when $(N-1)$ diagonal entries of $\boldsymbol{X}$ are zero, and the non-zero entry $\nu = \lambda_{\boldsymbol{G}_i}$ makes the above summation equal to zero. Thus, we have $\nu = \lambda_{\boldsymbol{G}_1}$. Based on (29), it follows

$$\boldsymbol{X} = \boldsymbol{U}_G^H \boldsymbol{U}_z \boldsymbol{D}_z \boldsymbol{U}_z^H \boldsymbol{U}_G = diag\left(P_j, 0, \ldots, 0\right), \tag{33}$$

which results in $\boldsymbol{U}_z = \boldsymbol{U}_G$ and $\boldsymbol{D}_z = diag\left(P_j, 0, \ldots, 0\right)$. Therefore, the optimal $\boldsymbol{R}_z^*$ equals (9).

REFERENCES

[1] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.
[2] E. Björnson, J. Hoydis, and L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency," *Found. Trends Signal Process.*, vol. 11, nos. 3–4, pp. 154–655, 2017, doi: 10.1561/2000000093.
[3] F. Rusek, D. Persson, B. Kiong Lau, E. G. Larsson, T. L. Marzetta, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.
[4] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.
[5] J. Choi, D. J. Love, and P. Bidigare, "Downlink training techniques for FDD massive MIMO systems: Open-loop and closed-loop training with memory," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 802–814, Oct. 2014.
[6] B. Lee, J. Choi, J.-Y. Seol, D. J. Love, and B. Shim, "Antenna grouping based feedback compression for FDD-based massive MIMO systems," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3261–3274, Sep. 2015.
[7] J. Fang, X. Li, H. Li, and F. Gao, "Low-rank covariance-assisted downlink training and channel estimation for FDD massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1935–1947, Mar. 2017.
[8] Z. Jiang, A. F. Molisch, G. Caire, and Z. Niu, "Achievable rates of FDD massive MIMO systems with spatial channel correlation," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2868–2882, May 2015.
[9] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.
[10] J. Moon, S. H. Lee, H. Lee, and I. Lee, "Proactive eavesdropping with jamming and eavesdropping mode selection," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3726–3738, Jul. 2019.
[11] J. Moon, H. Lee, C. Song, S. Lee, and I. Lee, "Proactive eavesdropping with full-duplex relay and cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6707–6719, Oct. 2018.
[12] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
[13] 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.
[14] 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.
[15] 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.
[16] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Physical-layer security in TDD massive MIMO," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7359–7380, Nov. 2018.
[17] 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.
[18] 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.
[19] 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.
[20] H. Akhlaghpasand, E. Bjornson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 1, pp. 182–186, Jan. 2020.
[21] M. A. Sheikhi and S. Mohammad Razavizadeh, "Security vulnerability of FDD massive MIMO systems in downlink training phase," in *Proc. 9th Int. Symp. Telecommun. (IST)*, Dec. 2018, pp. 492–496.
[22] C. Wang and R. D. Murch, "Adaptive downlink multi-user MIMO wireless systems for correlated channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2435–2446, Sep. 2006.
[23] M. Ding and S. D. Blostein, "MIMO minimum total MSE transceiver design with imperfect CSI at both ends," *IEEE Trans. Signal Process.*, vol. 57, no. 3, pp. 1141–1150, Mar. 2009.
[24] B. Nosrat-Makouei, J. G. Andrews, and R. W. Heath, Jr., "MIMO interference alignment over correlated channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2783–2794, Jun. 2011.
[25] S. Wagner, R. Couillet, M. Debbah, and D. T. M. Slock, "Large system analysis of linear precoding in correlated MISO broadcast channels under limited feedback," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4509–4537, Jul. 2012.
[26] D.-S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Kahn, "Fading correlation and its effect on the capacity of multielement antenna systems," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 502–513, Mar. 2000.
[27] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.
[28] H. Xie, F. Gao, S. Jin, J. Fang, and Y.-C. Liang, "Channel estimation for TDD/FDD massive MIMO systems with channel covariance computing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 4206–4218, Jun. 2018.
[29] B. K. Chalise, L. Haering, and A. Czylwik, "Robust uplink to downlink spatial covariance matrix transformation for downlink beamforming," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2004, pp. 3010–3014.
[30] K. Upadhya and S. A. Vorobyov, "Covariance matrix estimation for massive MIMO," *IEEE Signal Process. Lett.*, vol. 25, no. 4, pp. 546–550, Apr. 2018.

[31] M. Jordan, X. Gong, and G. Ascheid, "Conversion of the spatio-temporal correlation from uplink to downlink in FDD systems," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2009, pp. 1–6.
[32] A. Decurninge, M. Guillaud, and D. T. M. Slock, "Channel covariance estimation in massive MIMO frequency division duplex systems," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2015, pp. 1–6.

ASHKAN SHEIKHI (Member, IEEE) received the B.Sc. and M.Sc. (Hons.) degrees in electrical engineering—communication systems from the Iran University of Science and Technology (IUST), Tehran, Iran, in 2016 and 2019, respectively. He is currently pursuing the Ph.D. degree in wireless communication with the Department of Electrical and Information Technology (EIT), Lund University, Sweden. His research interests are mainly in the areas of wireless communication and signal processing techniques for the next generations of communication networks with a focus on the implementation challenges of massive MIMO systems and beyond.

S. MOHAMMAD RAZAVIZADEH (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Iran University of Science and Technology (IUST), in 1997, 2000, and 2006, respectively. He is currently an Associate Professor and the Head of the Communications Group, School of Electrical Engineering, Iran University of Science and Technology (IUST). He is also serving as the Director of the 5G Research Center (5GRC), IUST. Before joining IUST, in 2011, he was a Research Assistant Professor with the Iran Telecomm Research Center (ITRC), from 2006 to 2011. He has held several visiting positions at the University of Waterloo, Korea University, and the Chalmers University of Technology. His research interests are mainly in the area of wireless communication systems and wireless signal processing.

INKYU LEE (Fellow, IEEE) received the B.S. degree (Hons.) in control and instrumentation engineering from Seoul National University, Seoul, South Korea, in 1990, and the M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, USA, in 1992 and 1995, respectively.

From 1995 to 2001, he was a member of the Technical Staff with Bell Laboratories, Lucent Technologies, where he studied high-speed wireless system designs. From 2001 to 2002, he was a Distinguished Member of the Technical Staff with Agere Systems (formerly the Microelectronics Group, Lucent Technologies), Murray Hill, NJ, USA. Since 2002, he has been with Korea University, Seoul, South Korea, where he is currently the Department Head of the School of Electrical Engineering. In 2009, he was a Visiting Professor with the University of Southern California, Los Angeles. He has authored or coauthored more than 180 journal papers in IEEE publications and holds 30 U.S. patents granted or pending. His research interests include digital communications, signal processing, and coding techniques applied for next-generation wireless systems. He was elected as a member of the National Academy of Engineering in Korea, in 2015. He is also a Distinguished Lecturer of the IEEE. He was a recipient of the IT Young Engineer Award at the IEEE/IEEK Joint Award, in 2006, and the Best Paper Award at the Asia-Pacific Conference on Communications, in 2006, the IEEE Vehicular Technology Conference, in 2009, the IEEE International Symposium on Intelligent Signal Processing and Communication Systems, in 2013, the Best Research Award from the Korean Institute of Communications and Information Sciences (KICS), in 2011, the Best Young Engineer Award from the National Academy of Engineering in Korea, in 2013, and the Korea Engineering Award from the National Research Foundation of Korea, in 2017. He served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, from 2001 to 2011, and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, from 2007 to 2011. He was also a Chief Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (special issue on 4G wireless systems), in 2006. He currently serves as the Co-Editor-in-Chief of the *Journal of Communications and Networks*.