Linear Precoding with Friendly Jamming in Overloaded MU-MIMO Wiretap Networks

Peyman Siyari and Marwan Krunz
Department of Electrical and Computer Engineering, University of Arizona, USA
Email: {psiyari, krunz}@email.arizona.edu

***Abstract*—We consider the downlink of a multiuser MIMO (MU-MIMO) network in the presence of an external eavesdropper (Eve). No knowledge of Eve's location is assumed at the access point (Alice). The information signals for downlink users (Bobs) are accompanied by bogus signals (a.k.a. friendly jamming) that are generated from Alice. The network is studied in underloaded and overloaded conditions. In an underloaded (overloaded) network, the number of antennas at Alice is larger (smaller) than the total number of Bobs' antennas. In the overloaded setting, traditional methods of creating friendly jamming (FJ), such as zero-forcing-based methods, are infeasible. We propose a linear precoding scheme that relaxes such infeasibility in overloaded MU-MIMO networks. In the worst-case scenario where Eve has knowledge of the channels between Alice and Bobs, we show that our method imposes the most stringent condition on the number of antennas required at Eve to cancel out FJ signals. We verify our analysis with simulations. It turns out that choosing the number of data streams has an important role in achieving a tradeoff between security, reliability, and the achievable rate.**

***Index Terms*—Multiuser MIMO, linear precoding, physical-layer security, friendly jamming**

I. Introduction

With the advent of 5G and its related applications, immense amounts of sensitive and private data need to be transmitted wirelessly. The hardware used by many of these applications is too simple to execute complicated cryptographic algorithms. Alternatively, physical-layer (PHY-layer) security has a great potential in solving many new security challenges. Out of all malicious activities in a wireless network –such as jamming attacks [1], unauthenticated transmissions [2], etc.–, our main focus in this paper is on eavesdropping attacks. A widely-used PHY-layer technique for countering such attacks is *friendly jamming (FJ)* [3]. In FJ techniques, a transmitter (Alice) creates a bogus signal along with her secret message to deliberately garble the signal received at the eavesdropper (Eve) but not affect the intended recipient's (Bob's) reception.

In some designs, it has been suggested to use dedicated FJ nodes [3]. Such a method is usually referred to as *cooperative jamming (CJ)*. Despite providing security, CJ approaches face several implementation challenges related to mobility and trustworthiness. Specifically, if Bob is mobile it may be out of the reach of a stationary CJ, or if the CJ node is a malicious node itself, it may not nullify FJ at Bob.

In this paper, we focus on the application of FJ techniques in the downlink of a *broadcast network*[1]. Alice and (downlink) Bobs, all have multiple antennas, resulting in a *multiuser MIMO (MU-MIMO) network*. Linear precoding schemes, such as the ones based on *zero forcing (ZF)* and *minimum mean square error (MMSE)* [4] criteria, have been extensively used in practical realizations of MU-MIMO networks. The PHY-layer secrecy of MU-MIMO networks has also been studied in the literature, and several precoders have been designed to create FJ in such networks [5]. We are primarily interested in linear precoding design, as nonlinear designs are not practical.

In ZF-based methods for MU-MIMO networks, the number of antennas at Alice must be greater than or equal to the total number of antennas at Bobs so as to avoid inter-user interference [6]. We refer to this condition as *information rate rank constraint (IRRC)*. The case where IRRC is met is referred to as the *underloaded* scenario. If IRRC is violated, the network is *overloaded*, and hence the ZF-based and MMSE-based precoder designs are infeasible. When no information on Eve's location is known (hence FJ techniques are typically used), the ZF method requires the MU-MIMO network to be underloaded to allow for creation of FJ signals [5]. We refer to this condition as the *secrecy rank constraint (SRC)*.

To satisfy IRRC in overloaded networks, scheduling algorithms have been used to select a subset of Bobs, thus creating an underloaded network. In an extensive recent study done by Björnson et.al [7], it was shown that in MU-MIMO networks, it is more beneficial (in terms of lowering the bit-error-rate) to decrease the number of streams for each Bob and service many Bobs than to decrease the number of Bobs (by scheduling). Henceforth, we focus on schemes where the number of streams are kept low to serve more Bobs.

We propose a new linear precoding scheme for the downlink of a MU-MIMO network which uses FJ for achieving secrecy but relies on using a few streams per Bob to function in overloaded settings. To do this, we relax IRRC conditions, which allows multi-user interference (MUI) between downlink users. However, we aim to minimize MUI at each downlink user via a specific precoder design. It turns out that allowing MUI between downlink users not only enables our scheme to operate in overloaded settings, but also imposes the most stringent condition on the number of antennas that Eve requires to cancel out the FJ signals.

Notation: Boldface uppercase/lowercase letters denote matrices/vectors. $\mathbf{A}^{(:,a:b)}$ (and $\mathbf{A}^{(a:b,:)}$) denotes a matrix comprised of columns (and rows) a to b of $\mathbf{A}$. $\mathbf{I}$ and $\mathbf{0}$ denote the identity and the zero matrices. $\mathrm{E}[\bullet]$, $\bullet^{\dagger}$, $\mathrm{Tr}(\bullet)$ are respectively, the expected value, conjugate transpose, and trace operators. Lastly, $\mathbb{C}$ is the set of complex numbers.

[1]In this paper, a broadcast network refers to a network of one Alice and many Bobs, where each Bob receives his own separate message from Alice.

II. System Model

Consider a network where Alice has M antennas and communicates with Q Bobs, $Q \geq 2$. Let $\mathcal{Q} = \{1, 2, \ldots, Q\}$. Bob$_q$ has $N_q < M$ antennas, $q \in \mathcal{Q}$. Without loss of generality, assume that all Bobs have the same number of antennas, i.e., $N_q = N < M$, $\forall q \in \mathcal{Q}$. An external Eve with L antennas also exists in the range of communications[2]. The setting where $M = NQ$ is referred to as the fully-loaded scenario. When $M < NQ$, the network is overloaded, and when $M > NQ$ the network is underloaded.

Bob$_q$, $q \in \mathcal{Q}$, receives K_q independent streams from Alice, where $K_q \leq N$. Without loss of generality, assume that $K_q = K$, $\forall q \in \mathcal{Q}$. The number of streams determines how the antennas at Alice and Bobs are exploited. For example, $K = N$ indicates that the signals intended for Bobs have the maximum number of streams, thus the antennas are used to provide spatial multiplexing. In contrast, $K = 1$ signifies that the combining features of Bobs are used to increase the diversity (thus reliability) of transmissions.

A. Conventional Precoder Design

To better understand our method, we first explain the ZF method used in designing the precoding matrices[3]. The received signal at Bob$_q$, $q \in \mathcal{Q}$, can be expressed as

$$\mathbf{y}_q = \mathbf{H}_q(\mathbf{u} + \mathbf{f}) + \mathbf{n} \tag{1}$$

where $\mathbf{y}_q \in \mathbb{C}^N$, $\mathbf{H}_q \in \mathbb{C}^{N \times M}$ is the complex channel between Alice and Bob$_q$, $\mathbf{u} \in \mathbb{C}^M$ is the signal containing information from Alice, $\mathbf{f} \in \mathbb{C}^M$ is the FJ signal, and $\mathbf{n} \in \mathbb{C}^N$ is the AWGN which has i.i.d. zero-mean-circularly-symmetric-complex-Gaussian- (ZMCSCG-) distributed entries with $\mathrm{E}[\mathbf{n}\mathbf{n}^\dagger] = N_0/N\mathbf{I}$. The signal $\mathbf{u}$ is expressed as

$$\mathbf{u} \triangleq \sum_{q=1}^{Q} \mathbf{u}_q \triangleq \sum_{q=1}^{Q} \mathbf{T}_q \mathbf{s}_q \tag{2}$$

where $\mathbf{u}_q \in \mathbb{C}^M$ is the signal intended for Bob$_q$. $\mathbf{T}_q$ is the precoder that is responsible for cancelling the MUI generated from $\mathbf{u}_q$. $\mathbf{s}_q \in \mathbb{C}^K$ is the K-dimensional information signal (K streams of data) intended for Bob$_q$.

Assume that $\mathrm{E}[\mathbf{s}_q \mathbf{s}_q^\dagger] = \phi P_q / K\mathbf{I}$, where P_q is the power of Alice allocated to Bob$_q$'s signal and ϕ is the portion of Alice's total power allocated to all information signals. Let $P \triangleq \sum_{q=1}^{Q} P_q$, where P is Alice's total power. Alice allocates ϕP of her total power to all information signals. The rest of the power (i.e., $(1-\phi)P$) goes to the FJ signal.

We assume that Alice knows all $\mathbf{H}_i$, $\forall i \in \mathcal{Q}$, and Bob$_q$ only knows $\mathbf{H}_q$. In the channel estimation phase, Alice sends pilot signals to Bobs, so that Bob$_q$ can estimate $\mathbf{H}_q$ and feed it back to Alice. Substituting (2) in (1), the effective channel that Bob$_q$ sees from Alice would be $\mathbf{H}_q\mathbf{T}_q$. Hence, Alice can apply another precoder for each Bob to optimize her transmissions. Specifically, assume that $\mathbf{T}_q \in \mathbb{C}^{M \times \tau}$, $K < \tau \leq N$. Then, Alice can assign an extra precoder $\mathbf{W}_q \in \mathbb{C}^{\tau \times K}$, so that $\mathbf{y}_q$ can be written as

$$\mathbf{y}_q = \mathbf{H}_q\Big(\sum_{q=1}^{Q} \mathbf{T}_q \mathbf{W}_q \mathbf{s}_q + \mathbf{f}\Big) + \mathbf{n}. \tag{3}$$

Bob$_q$ also applies a linear combiner to estimate the transmitted information signal. In particular, Bob$_q$ applies $\mathbf{D}_q \in \mathbb{C}^{K \times N}$ to have the following estimate of $\mathbf{s}_q$:

$$\hat{\mathbf{s}}_q \triangleq \mathbf{D}_q \mathbf{y}_q = \mathbf{D}_q \left(\mathbf{H}_q\Big(\sum_{q=1}^{Q} \mathbf{T}_q \mathbf{W}_q \mathbf{s}_q + \mathbf{f}\Big) + \mathbf{n} \right). \tag{4}$$

Let $\mathbf{H}_q\mathbf{T}_q = \mathbf{U}_q\mathbf{\Sigma}_q\mathbf{V}_q^\dagger$ be the singular-value decomposition (SVD) of $\mathbf{H}_q\mathbf{T}_q$, where $\mathbf{U}_q$ and $\mathbf{V}_q$ are the unitary matrices of left and right singular vectors, and $\mathbf{\Sigma}_q$ is the matrix of singular values. Therefore, if Alice sets $\mathbf{W}_q = \mathbf{V}_q^{(:,1:K)}$ and Bob$_q$ sets $\mathbf{D}_q = {\mathbf{U}_q^{(:,1:K)}}^\dagger$, the optimal precoder/combiner duo to estimate $\mathbf{s}_q$ at Bob$_q$ can be established [5].

We now focus on the design of $\mathbf{T}_q$ and $\mathbf{f}$. The ZF method is based on nullifying both the FJ signal and MUI on unintended Bobs. Formally, the following conditions must be satisfied:

$$\mathbf{H}_r\mathbf{T}_q = \mathbf{0},\ r \neq q,\ \forall r, q \in \mathcal{Q} \tag{5a}$$

$$\mathbf{H}_q\mathbf{f} = \mathbf{0},\ \forall q \in \mathcal{Q} \tag{5b}$$

The precoder $\mathbf{T}_q$ can be determined as follows. Define $\bar{\mathbf{H}}_q \triangleq [\mathbf{H}_1^\dagger, \ldots, \mathbf{H}_{q-1}^\dagger, \mathbf{H}_{q+1}^\dagger, \ldots, \mathbf{H}_Q^\dagger]^\dagger \in \mathbb{C}^{N(Q-1) \times M}$, and let $\bar{\mathbf{H}}_q = \mathbf{L}_q\mathbf{J}_q\mathbf{R}_q$ be the SVD of $\bar{\mathbf{H}}_q$, where $\mathbf{L}_q$ and $\mathbf{R}_q$ denote the matrices of left and right singular vectors, and $\mathbf{J}_q$ denotes the matrix of singular values. Provided that $M > N(Q-1)$, $\bar{\mathbf{H}}_q$ has a nontrivial null-space, which can be exploited to meet condition (5a). Specifically, if $M > N(Q-1)$, Alice sets $\mathbf{T}_q = \mathbf{R}_q^{(:,B:B+\tau)} \in \mathbb{C}^{M \times \tau}$, where $B = N(Q-1)+1$, to satisfy (5a) for all $q \in \mathcal{Q}$. The condition

$$M \geq N(Q-1) + \tau \tag{6}$$

constitutes the IRRC in the downlink of the ZF method. The FJ signal mentioned in (1) has the following structure in the ZF method. Define $\tilde{\mathbf{H}} \triangleq [\mathbf{H}_1^\dagger, \ldots, \mathbf{H}_Q^\dagger]^\dagger \in \mathbb{C}^{NQ \times M}$. Let $\tilde{\mathbf{H}} = \mathbf{L}\mathbf{J}\mathbf{R}$ be the SVD of $\tilde{\mathbf{H}}$, where $\mathbf{L}$ and $\mathbf{R}$ denote the matrices of left and right singular vectors, and $\mathbf{J}$ denotes the matrix of singular values. To satisfy (5b), $\tilde{\mathbf{H}}$ must have a nontrivial null-space, which requires $M > NQ$. Hence, the inequality $M > NQ$ is the SRC for the ZF method. We choose $\tau = N$, as IRRC in (6) is dominated by SRC. The FJ signal is expressed as $\mathbf{f} = \mathbf{Z}\mathbf{v}$, where $\mathbf{Z}$ is the associated precoder for FJ that spans the null space of $\tilde{\mathbf{H}}$; and $\mathbf{v}$ is the vector of artificial noise that has the same characteristics of AWGN except that $\mathrm{Tr}[\mathbf{v}\mathbf{v}^\dagger] = (1-\phi)P$. If SRC is violated, the creation of FJ signal becomes infeasible.

III. Proposed Signaling scheme

In this section, we introduce our proposed signaling scheme. We first modify the signal model at Bobs in (3). Specifically, the received signal at Bob$_q$, $q \in \mathcal{Q}$ can be expressed as

$$\mathbf{y}_q = \mathbf{H}_q\mathbf{u}' + \mathbf{n} \tag{7}$$

[2]A single Eve with L antennas can also represent several multi-antenna colluding Eves.

[3]A more detailed introduction of ZF method is presented in [8, Section 2].

where $\mathbf{u}'$ is Alice's signal in our proposed signaling scheme:

$$\mathbf{u}' = \sum_{q=1}^{Q} \left(\mathbf{u}'_q + \mathbf{f}'_q\right) \tag{8}$$

where $\mathbf{u}'_q$ is the signal intended for Bob_q, $q \in \mathcal{Q}$, and $\mathbf{f}'_q$ is the FJ signal designed to protect Alice's transmissions that are intended for Bob_q. In fact, compared to (1), the main change in the signal model is the decomposition of the FJ signal (i.e., convert $\mathbf{f}$ to $\mathbf{f}'_q$, $q \in \mathcal{Q}$) in a way that each FJ signal exclusively protects the transmissions intended for one Bob.

A more detailed representation of $\mathbf{u}'$ can be given as

$$\mathbf{u}' = \sum_{q=1}^{Q} \mathbf{T}'_q(\mathbf{W}'_q\mathbf{s}_q + \mathbf{Z}'_q\mathbf{v}'_q) \tag{9}$$

with $\mathbf{u}'_q = \mathbf{T}'_q\mathbf{W}'_q\mathbf{s}_q$ and $\mathbf{f}'_q = \mathbf{T}'_q\mathbf{Z}'_q\mathbf{v}'_q$. The precoder $\mathbf{T}'_q$ is responsible for cancelling MUI and FJ on unintended Bobs, $\mathbf{W}'_q$ is the precoder to boost signal strength on Bob_q (same as $\mathbf{W}_q$ in previous section), $\mathbf{Z}'_q$ is the precoder for the FJ signal that protects Bob_q, and $\mathbf{v}'_q$ is the vector of artificial noise. As before, $\mathbf{s}_q$ is the K-stream information signal intended for Bob_q. Because precoder $\mathbf{T}'_q$ is applied to both information and FJ signals (compare (9) and (2)), we are ensured that FJ will have no effect on unintended Bobs. As in (4), a linear receiver $\mathbf{D}'_q$ is applied at Bob_q to recover $\mathbf{s}_q$. Using (7) and (9), Bob_q has the following estimate of $\mathbf{s}_q$

$$\hat{\mathbf{s}}_q \triangleq \mathbf{D}'_q\mathbf{y}_q = \mathbf{D}'_q\left(\mathbf{H}_q\Big(\sum_{q=1}^{Q} \mathbf{T}'_q(\mathbf{W}'_q\mathbf{s}_q + \mathbf{Z}'_q\mathbf{v}'_q)\Big) + \mathbf{n}\right). \tag{10}$$

The conditions for completely nullifying the MUI and FJ signals for the signal model in this section are as follows:

$$\mathbf{H}_r\mathbf{T}'_q = \mathbf{0},\ r \neq q,\ \forall r, q \in \mathcal{Q} \tag{11a}$$

$$\mathbf{D}'_q\mathbf{H}_q\mathbf{T}'_q\mathbf{Z}'_q\mathbf{v}'_q = \mathbf{0},\ \forall q \in \mathcal{Q} \tag{11b}$$

The design of $\mathbf{T}'_q$, $\mathbf{W}'_q$, and $\mathbf{D}'_q$ would be the same as those of $\mathbf{T}_q$, $\mathbf{W}_q$ and $\mathbf{D}_q$ in the previous section. Therefore, the IRRC of our method is the same as that of conventional ZF. All FJ signals are removed by a combination of (11a) and (11b). Notice that (11b) is different from (5b) in that $\mathbf{Z}'_q$ in (11b) is designed so that only $\mathbf{v}'_q$ is nullified at Bob_q with the help of $\mathbf{D}'_q$. The rest of FJ signals (i.e., $\mathbf{v}'_r,\ r \neq q$) are removed by $\mathbf{T}'_q$ that satisfies (11a). Therefore, the SRC of our method is determined by the condition that is the most dominant in (9). Due to keeping the same design of the conventional ZF method for $\mathbf{T}'_q$, the SRC is the same as IRRC in our method, i.e., $M \geq NQ$ given that $\tau = N$ (see (6)).

As mentioned earlier, because we use a different procedure to nullify the FJ signal, the design of $\mathbf{Z}'_q$ is different from $\mathbf{Z}$ of the previous section in that $\mathbf{Z}'_q$ is designed for each Bob_q. Let $\mathbf{H}_q\mathbf{T}'_q = \mathbf{U}'_q\mathbf{\Sigma}'_q{\mathbf{V}'_q}^{\dagger}$ be the SVD of $\mathbf{H}_q\mathbf{T}'_q$, where $\mathbf{U}'_q$ and $\mathbf{V}'_q$ are the unitary matrices of left and right singular vectors, and $\mathbf{\Sigma}'_q$ is the matrix of singular values. Therefore, if Alice sets $\mathbf{W}'_q = {\mathbf{V}'_q}^{(:,1:K)}$, $\mathbf{D}'_q = {\mathbf{U}'_q}^{(:,1:K)\dagger}$ (same as previous section), and $\mathbf{Z}'_q = \mathbf{V}_q^{(:,K+1:\tau)}$, then (11b) is also satisfied (compare with the design of $\mathbf{Z}$).

A. Security Analysis of the Proposed Method

The received signal at Eve can be expressed as

$$\mathbf{z} = \mathbf{G}\mathbf{u}' + \mathbf{e} = \mathbf{G}\Big(\sum_{q=1}^{Q} \left(\mathbf{u}'_q + \mathbf{f}'_q\right)\Big) + \mathbf{e} \tag{12}$$

where $\mathbf{G} \in \mathbb{C}^{L\times M}$ is the channel between Alice and Eve, and $\mathbf{e}$ has the same characteristics as $\mathbf{n}$ in (1). Eve has to first combat the MUI to be able to wiretap ongoing communications. Eve does so by applying a linear combiner. For example, to eavesdrop on signals intended for Bob_q, Eve first applies $\mathbf{A}'_q$ on the signal she receives. Define $\mathbf{z}_q \triangleq \mathbf{A}'_q\mathbf{z}$. Upon cancelling MUI with $\mathbf{A}'_q$, Eve applies $\mathbf{B}'_q$ on $\mathbf{z}_q$ to estimate $\mathbf{s}_q$. In other words, Eve's estimation from $\mathbf{s}_q$ is $\tilde{\mathbf{s}}_q = \mathbf{B}'_q\mathbf{z}_q$. We assume the worst-case scenario where Eve knows $\mathbf{G}$. For instance, Eve can use the pilot signals sent from Alice in the channel estimation phase to estimate $\mathbf{G}$. Moreover, because Bobs have to explicitly feed back the channel estimates to Alice, Eve can snoop on the channel estimation feedback from Bobs to gain knowledge of all $\mathbf{H}_q,\ \forall q \in \mathcal{Q}$. Note, however, that neither Alice nor Bobs have any knowledge of $\mathbf{G}$, i.e., Eve is a passive eavesdropper.

We now describe how Eve chooses her combiners to decode Alice's transmissions. We also show how many antennas Eve requires to decode all messages. Using (12), $\mathbf{z}_q = \mathbf{A}'_q\mathbf{z}$, and the linear estimate $\tilde{\mathbf{s}}_q = \mathbf{B}'_q\mathbf{z}_q$, we have the following

$$\tilde{\mathbf{s}}_q = \mathbf{B}'_q\mathbf{A}'_q\Big(\mathbf{G}\Big(\sum_{q=1}^{Q} \left(\mathbf{u}'_q + \mathbf{f}'_q\right)\Big) + \mathbf{e}\Big). \tag{13}$$

Eve cancels MUI by designing a combiner $\mathbf{A}'_q$ such that

$$\mathbf{A}'_q\mathbf{G}\left(\mathbf{u}'_r + \mathbf{f}'_r\right) = 0,\ r \neq q,\ \forall r, q \in \mathcal{Q} \tag{14a}$$

$$\mathbf{A}'_q\mathbf{G}\,\mathbf{f}'_q = 0,\ \forall q \in \mathcal{Q} \tag{14b}$$

Using (8), (9) and (13), Eve first constructs the following blocked matrix

$$\mathbf{G}'_q = [\mathbf{\Omega}'_1, \ldots, \mathbf{\Omega}'_{q-1}, \mathbf{\Omega}'_{q+1}, \ldots, \mathbf{\Omega}'_Q, \mathbf{\Gamma}'_q] \tag{15}$$

where $\mathbf{\Omega}'_q = \mathbf{G}\mathbf{T}'_q \in \mathbb{C}^{L\times\tau}$ and $\mathbf{\Gamma}'_q = \mathbf{G}\mathbf{T}'_q\mathbf{Z}'_q \in \mathcal{C}^{L\times\tau-K}$. Eve sets $\mathbf{A}'_q$ to be the last K columns of the matrix of left singular values of $\mathbf{G}'_q$. For such a choice of $\mathbf{A}'_q$ that allows Eve to cancel MUI and FJ, the minimum value of L is derived by counting the column of $\mathbf{G}'_q$, i.e.,

$$\Psi' = \tau(Q-1) + (\tau - K) + K = \tau Q \tag{16}$$

Setting $\tau = N$, we have $\Psi' = NQ$. The first term in the right hand side (RHS) of (16) is the number of antennas that $\mathbf{\Omega}_r,\ r \neq q,\ r \in \mathcal{Q}$ occupies in establishing $\mathbf{G}'_q$ in (15). The second term in (16) is the number of antennas that $\mathbf{\Gamma}'_q$ occupies in (15). Finally, the third term is the number of antennas that are required to recover $\mathbf{s}_q$ after nullifying MUI and FJ. The same security analysis can be done for the ZF method (see [8, Section II]), and it can be shown that if Alice uses the conventional ZF method, Eve requires at least $\Psi = M - (N-K)Q$ antennas.

B. Security Comparison Between Conventional ZF Method and the Proposed Method

We now compare required the number of Eve's antennas for both the ZF and the proposed method in underloaded scenario, i.e., we compare Ψ and Ψ' when $M > NQ$. Consider the conditions when $\Psi > \Psi'$, i.e., $M - (N-K)Q > NQ$. In other words, we examine when the ZF method is better than our approach. Clearly such a comparison depends on K, as follows:

- For $K = N$, we end up with $M > NQ$, which is always true in the underloaded scenario, so in the case of using all streams (i.e., spatial multiplexing), the ZF method imposes a more stringent condition than our method.
- For $K < N$, the simplified inequality is $2N - K < \frac{M}{Q}$. By lowering the number of streams (K), it can be deduced that the ZF method imposes more antennas on Eve than our method only when the network is *sufficiently* underloaded. To clarify, take the extreme example of $K = 1$; In this case, $M - (N-K)Q > NQ$ is reduced to $M > (2N-1)Q$ which is more demanding than an underloaded network (i.e., $M > NQ$) with $N > 1$.

Overall, when a few streams are selected for each Bob, the ZF method does not impose more antennas on Eve than our proposed method unless the network is sufficiently underloaded. Normally, a sufficiently underloaded is not preferred, as the MU-MIMO network would not be fully utilized.

IV. Proposed Precoding Method

The current precoder design for $\mathbf{T}'_q$ in our proposed signaling scheme has two issues. First, the IRRC condition is still the same as that of the conventional ZF method, which prohibits our signaling scheme from operating in overloaded scenarios. Second, after implementation of these precoders, although for $K < N$ our signaling scheme can impose more antennas on Eve to decode the ongoing messages –by adding more columns to matrix $\mathbf{G}'_q$ in (13), see Section III-B–, it turns out that the rank of $\mathbf{G}'_q$ does not increase with the added columns. Therefore, Eve can still decode the signals with fewer antennas than what our proposed signaling scheme claims. In this section, we modify the design of $\mathbf{T}'_q$ to resolve these issues. To do so, we relax condition (11a) in a way that MUI created from $\mathbf{s}_q$ inflicts the least amount of damage on the reception of other Bobs. Formally, we design the precoder $\mathbf{T}'_q$, $q \in \mathcal{Q}$ using the following optimization problem:

$$\begin{aligned} \underset{\mathbf{T}'_q}{\text{maximize}} \quad & \frac{||\mathbf{H}_q \mathbf{T}'^{(:,n)}_q||_F}{\sum_{\substack{r=1 \\ r\neq q}}^{Q} ||\mathbf{H}_r \mathbf{T}'^{(:,n)}_q||_F + \frac{N_0}{\phi P_q N}} \\ \text{s.t.} \quad & \mathbf{T}'^{(:,n)}_q \mathbf{T}'^{(:,n)\dagger}_q = \frac{1}{\tau}, \ n \in \{1, \dots, \tau\} \end{aligned} \tag{17}$$

where $||\bullet||_F$ is the Frobenius norm and $\mathbf{T}'^{(:,n)}_q$ is the nth column of $\mathbf{T}'_q$. Hence, τ problems must be solved to design $\mathbf{T}'_q$. Problem (17) states that each column of $\mathbf{T}'_q$ must be designed in a way that the interference generated from $\mathbf{s}_q$ (i.e., denominator of the objective in (17)) is minimized while the strength of $\mathbf{s}_q$ at Bob$_q$ (i.e., the numerator of the objective) is maximized. The constraint in (17) ensures that the resulting precoder does not violate the power constraint. In fact, because we assumed that $\mathrm{E}[\mathbf{s}_q \mathbf{s}_q^\dagger] = \phi P_q / K \mathbf{I}$, we must also ensure that ideally, $\mathrm{E}[\mathbf{T}'_q \mathbf{s}_q \mathbf{s}_q^\dagger \mathbf{T}'^{\dagger}_q] = \phi P_q / K \mathbf{I}$ (see (2) and description of $\mathbf{s}_q$ below it). Problem (17) is identified as a Rayleigh quotient problem [9]. The solution to (17) is given by

$$\mathbf{T}'^{*(:,n)}_q = \frac{1}{\sqrt{\tau}} \frac{\mathbf{\Delta}^{(:,n)}}{||\mathbf{\Delta}^{(:,n)}||_F} \tag{18}$$

where $\mathbf{\Delta}$ is the matrix of generalized eigenvectors corresponding to the τ non-zero generalized eigenvalues of numerator and denominator of the objective in (17), i.e.,

$$\mathbf{\Delta} \triangleq \mathrm{eig}_{max,\tau}\Big(\mathbf{H}_q^\dagger \mathbf{H}_q, \sum_{\substack{r=1 \\ r\neq q}}^{Q} \mathbf{H}_r^\dagger \mathbf{H}_r + \frac{N_0}{\phi P_q N}\Big) \in \mathbb{C}^{M \times \tau} \tag{19}$$

where $\mathrm{eig}_{max,\tau}$ is the operator for extracting τ generalized eigenvectors that correspond to τ non-zero generalized eigenvalues. From the properties of generalized eigenvalue problems, there are N eigenvectors that correspond to non-zero generalized eigenvalues in (19)[4].

In case of an underloaded network (i.e., $M > NQ$), we set $\tau = N$ (i.e., same as Section II-A and III). In case of over/fully loaded networks (i.e., $M \leq NQ$), we set $\tau = \lceil \frac{M}{Q} \rceil$, where $\lceil \bullet \rceil$ is the ceiling function to handle the case of non-integer values of τ. Notice that in an overloaded scenario, we do not decrease Q via scheduling. Instead, we have the freedom in choosing τ and still keeping all users in the network. Using the fact that $K < \tau \leq N$, we can also determine the value of K. After designing $\mathbf{T}'_q$ and determining K, the remaining matrices in our proposed method (i.e., $\mathbf{W}'_q$, $\mathbf{D}'_q$ and $\mathbf{Z}'_q$) can be designed as in Section III. Hence, all terms in (9) and (10) are defined, and our proposed precoding method is complete.

The security analysis of our method in underloaded scenarios was already done in Section III-B, where we showed Eve requires $\Psi' = \tau Q$ antennas to decode all messages. In the case of overloaded network as mentioned before, we choose $\tau = \lceil \frac{M}{Q} \rceil$. Hence, $\Psi' = \max\{\tau Q, M\}$ which is the most stringent condition on Eve's number of antennas. The conventional ZF method is not able to generate the FJ signal in an overloaded network because condition (5b) cannot be satisfied. Hence, it can be shown that Eve only requires $\Psi = KQ$ antennas to decode all messages in ZF method (see [8]). As $KQ < \max\{\tau Q, M\}$, then our method always performs better than the conventional ZF scheme in overloaded networks.

Notice that our proposed precoder design for $\mathbf{T}'_q$ in this section can also be used in the conventional ZF method to design $\mathbf{T}_q$ for overloaded scenarios and relax condition (5a). However, there will be no increase in the number of Eve's antennas required to decode Alice's messages because the design of FJ in the conventional ZF method is decoupled from the design of $\mathbf{T}_q$. Therefore, the proposed signaling scheme in Section III is essential to impose more antennas at Eve.

[4]The ZF and MMSE methods of precoding are also special cases of the optimization problem (17). See [8] for a more detailed explanation.

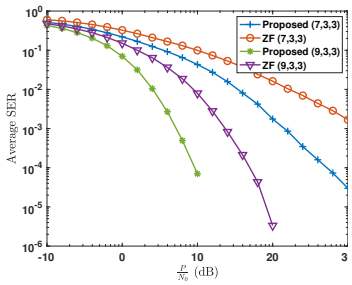

Fig. 1: Comparison of SER (Underloaded)

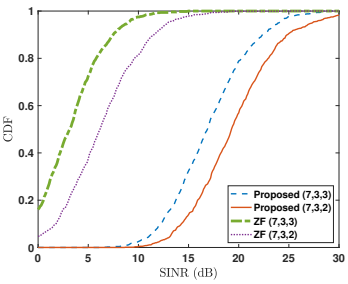

Fig. 2: Comparison of achieved SINR (Underloaded, $P = 30$ dB)

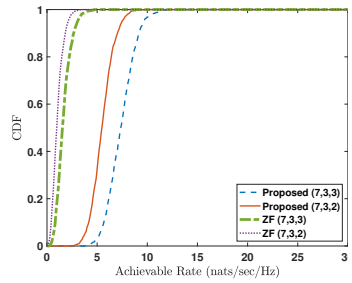

Fig. 3: Comparison of achievable rate (Underloaded)

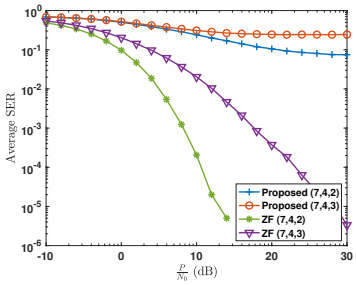

Fig. 4: Comparison of Eve's SER (Overloaded)

V. Numerical Results

We verify our theoretical analyses via simulations. All simulations are done for a network of $Q = 2$ Bobs. Similar conclusions can be drawn for networks with more Bobs and more antennas at Alice. Our *proposed method* in these simulations is the combination of the methods in Section III and Section IV, while the simulated ZF method is the scheme that we discussed in Section II-A. In our proposed method, the power allocated to Bob's message is divided equally between its associated information and FJ signals. Same is done for the ZF method. We use uncoded QPSK modulation for all simulations. For simulation that show SINR and achievable rate, we use Gaussian codebooks. The triplet (M, N, K) in all simulations denote number of Alice/Bob antennas and number of data streams[5].

Fig. 1 shows the symbol error rate (SER) of the Alice-Bob channels, averaged across all Bobs for an underloaded scenario. It can be seen that our proposed method outperforms the ZF method for both settings because our precoders are more flexible. In fact, although the precoders designed by the ZF method completely suppress MUI, they also do not contribute to the strength of the signal to the intended user.

Fig. 2 shows the CDF of the achieved SINR in an underloaded scenario. Our method achieves higher SINR compared to the ZF method. This in fact decreases the SER of our scheme as shown in Fig. 1.

Fig. 3 shows the CDF of achievable information rate. As can be seen, our method also achieves a higher rate. Therefore, our method achieves a better tradeoff between diversity (i.e., SINR in Fig. 2) and multiplexing (i.e., achievable rate in Fig. 3). Moreover, in both Figs 2 and 3, it can be seen that using a higher number of streams results in a lower SINR but higher achievable rate, and vice versa, signifying that a lower number of streams exploits the diversity of multiple antennas.

Fig. 4 shows the SER of Eve in an overloaded scenario when $L = 6$. Both $(7, 4, 3)$ and $(7, 4, 2)$ settings represent overloaded scenarios. In both settings, we set $\tau = 4$. Clearly, no FJ can be created in these settings using the ZF method. It can be seen that our method performs significantly better than the ZF scheme in both overloaded settings because our method forces Eve to have at least $\Psi' = \max\{\tau Q, M\}$ antennas to decode all messages. However, the ZF method only imposes $\Psi = KQ$ antennas in overloaded scenarios. In both of these settings, $L = 6$ antennas would be enough to decode all messages in the ZF design. It can be seen that the setting $(7, 4, 3)$ experiences more SER because more data streams are used per user, which decrease the diversity gain.

VI. Conclusions

In this paper, we proposed a novel precoding scheme that not only manages the interference in MU-MIMO networks better than the zero-forcing method, but also enables the nodes to operate in overloaded settings. Compared to the ZF method, our scheme is able to impose more stringent conditions on Eve's number of antennas in overloaded scenarios. Analysis of this scheme in massive MIMO networks, or with limited feedback from downlink users, or with in-band full-duplex capability in nodes are subjects of future research.

[5]More simulations and comparison with other methods are given in [8].

References

[1] H. Pezeshki, X. Zhou, and B. Maham, "Jamming energy allocation in training-based multiple access systems," *IEEE Commun. Letters*, vol. 17, no. 6, pp. 1140–1143, Jun. 2013.

[2] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. ACM WiSec 2010 Conf.*, 2010, pp. 89–98.

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

[4] H. Sung, S. R. Lee, and I. Lee, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3489–3499, Nov. 2009.

[5] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. Allerton Conf. Commun., Control, Computing*, Sep. 2009, pp. 1134–1141.

[6] T. M. Duman and A. Ghrayeb, *Coding for MIMO Communication Systems*. New York, NY, USA: John Wiley and Sons, Ltd, 2007.

[7] E. Bjornson, M. Kountouris, M. Bengtsson, and B. Ottersten, "Receive combining vs. multi-stream multiplexing in downlink systems with multi-antenna users," *IEEE Trans. Signal Process.*, vol. 61, no. 13, pp. 3431–3446, Jul. 2013.

[8] P. Siyari and M. Krunz, "Secure linear precoding in overloaded wiretap MU-MIMO networks," University of Arizona Department of ECE, Tech. Rep., 2019. [Online]. Available: http://wireless.ece.arizona.edu/sites/default/files/techrep_2019.pdf

[9] S. Yu, L.-C. Tranchevent, B. De Moor, and Y. Moreau, *Rayleigh Quotient-Type Problems in Machine Learning*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 27–37.