Secure Linear Precoding in Overloaded MU-MIMO Wireless Networks

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

Abstract*—We investigate signaling and linear precoding designs for secure downlink communications in a multiuser MIMO (MU-MIMO) network. The network is tapped by an external eavesdropper (Eve) who is equipped with a large number of antennas. In addition to the transmission of several (unicast) information signals to downlink users (Bobs), the transmitter (Alice) generates friendly jamming (FJ), aiming to prevent Eve from decoding Alice's signals. To mitigate both multiuser interference (MUI) and FJ on Bobs, MU-MIMO systems often rely on zero-forcing (ZF) precoders. A condition for the application of such precoders is that the network must be *underloaded*, i.e., Alice has more antennas than all Bobs combined. For *overloaded* scenarios, ZF-based precoding cannot guarantee nullification of both MUI and FJ at legitimate receivers. Accordingly, we propose a combined signaling-and-precoding scheme that can also be applied to an overloaded MU-MIMO network. In an underloaded scenario, our technique is shown to impose a more stringent antenna requirement on Eve than a classical ZF-based precoding, i.e., Eve must utilize more antennas if she is to successfully eavesdrop on Alice's transmissions. Although our scheme is comparable to antenna selection (AS) approaches in terms of Eve's antenna requirement, it incurs much less delay and complexity by avoiding frequent on/off switching of the RF chains at Bobs. For underloaded scenarios, we provide security analysis that establishes the conditions under which our scheme is superior to the ZF scheme. Using computer simulations, we validate the advantages of our design and contrast it with ZF and AS schemes in terms of the symbol error rate, the EVM, and the achievable rate in both underloaded and overloaded scenarios.

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

I. Introduction

Wireless systems constantly face serious threats related to privacy and data confidentiality. Due to the broadcast nature of the wireless medium, adversaries with modest hardware can easily eavesdrop on transmitted signals and analyze them to extract valuable information, including browsing habits [3], locations and movement [4], health data from medical devices and implantable sensors [5], etc.

Of the various malicious attacks that threaten a wireless network, we focus on *eavesdropping*. Although cryptographic techniques can adequately thwart eavesdropping on upper-layer communications, they cannot be applied to low-layer (PHY/MAC) headers and broadcast control packets. Such headers/packets must be transmitted in the clear to ensure proper protocol operation. Therefore, even with an encrypted payload, an adversary can eavesdrop on exposed headers and exploit captured information to perform malicious attacks, including traffic analysis and selective jamming [6].

Recently, researchers have started to recognize the significance of *PHY-layer security techniques*. These techniques exploit channel properties for encryption, authentication, and device fingerprinting [7]. The interest in PHY-layer security has largely been driven by its ability to support keyless confidential communications and obfuscate lower-layer headers, thereby complementing cryptography-based schemes and adding another layer of security.

In this paper, we focus on PHY-layer techniques for securing the downlink transmissions of a *multiuser MIMO (MU-MIMO)* network against a highly capable eavesdropper (Eve). From a PHY-layer security perspective, the study of MU-MIMO can be broadly classified into (see [7] for a survey):

- *MU-MIMO networks with confidential messages*, where such messages are to be kept hidden from unintended receivers (Bobs), and
- *MU-MIMO wiretap networks*, in which Bobs are not curious about each other's communications; rather, one or more external eavesdroppers (Eves) are present, and the downlink transmissions must be prevented from being captured by these Eves.

Our paper belongs to the second class of studies. Specifically, we focus on applying *friendly jamming (FJ)*, a PHY-layer security technique that has gained considerable attention. Under a *traditional* FJ approach, in addition to sending an information signal, the legitimate transmitter (Alice) also generates a bogus signal (artificial noise) that degrades the reception at Eve without impacting the quality of the received information signal at a legitimate receiver (Bob). This idea can be realized by means of MIMO precoding, whereby Alice uses its multiple antennas to transform its FJ signal so that it falls into the null space of the channel between Alice and Bob. Such a method of creating FJ is also known as *transmit-based FJ (TxFJ)*. The effectiveness of FJ was extensively analyzed (e.g., [8], [9]) and demonstrated experimentally (e.g., see [10] and references therein). FJ was also applied to other communication scenarios, including relay networks [9],

Peyman Siyari is currently with Qualcomm Technologies, San Jose, CA, USA. This work was done while he was a Ph.D. student at the University of Arizona and is based on his Ph.D. dissertation [1]. An abridged version of this paper appeared in *Proc. of the IEEE CNS 2019 Conference – Workshop on Physical-Layer Methods for Security and Privacy in 5G and the IoT* [2]. This research was supported in part by NSF and by the Broadband Wireless Access & Applications Center (BWAC). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

interference networks [8], and broadcast networks [11]. The authors in [11] introduced TxFJ techniques for MU-MIMO networks. The study of MU-MIMO networks under a massive number of antennas at Alice was done in [12]–[14]. Other interesting issues related to the secrecy performance under FJ, such as the case when spatial correlation exists between Alice's antennas and the allocation of power between FJ and information signals, were considered in [15] and [16], respectively. Lower and upper bounds on the secrecy capacity of MU-MIMO wiretap networks were derived in [17].

The application of FJ in MU-MIMO systems is intertwined with precoding design. Precoding approaches proposed over the last two decades have come close to the capacity of MU-MIMO networks. The theoretical precoding method of *dirty-paper coding* guarantees achieving such capacity [18]. However, the complicated and nonlinear structure of this method makes it impractical for commercial systems. Instead, linear precoding schemes, such as those based on *zero forcing (ZF)* and *minimum mean square error (MMSE)* [19], have been extensively used in practice.

In this work, we are primarily interested in *linear* precoding designs (e.g., ZF), as nonlinear designs are not suitable for practical implementation. In conventional ZF-based methods for MU-MIMO networks, guaranteeing interference-free communications requires the number of antennas at Alice to be greater than or equal the sum of the numbers of receive antennas at all Bobs [20]. This condition is referred to as *information rate rank constraint (IRRC)*. When IRRC is met, the network is said to be *underloaded*. Otherwise, if IRRC is violated, the network is *overloaded*, and ZF- and MMSE-based precoding become infeasible [11]. In addition to zero-forcing information signals on unintended Bobs (to meet IRRC), FJ is often nullified at all Bobs. Zero-forcing the FJ signal requires the MU-MIMO network to be underloaded to allow for the creation of TxFJ [11]; a condition referred to as the *secrecy rank constraint (SRC)*.

Antenna selection and user scheduling are two possible approaches that can be used to satisfy IRRC and/or SRC when the original network is overloaded. Specifically, selecting a subset of Bob's antennas reduces the number of data streams that Bob can receive, while scheduling links reduces the number of simultaneously serviced Bobs without removing any of their antennas/streams. It has been shown in [21] that in the case of many Bobs, the overall BER performance of the network is better (lower BER) when more Bobs with fewer spatial streams per Bob are used than when user scheduling is utilized to service fewer Bobs with a higher number of spatial streams per Bob, i.e., antenna selection is superior from a BER perspective to user scheduling. However, selecting a subset of antennas to satisfy IRRC or SRC is an integer programming problem [20] that cannot be solved in polynomial time. Antenna selection also requires RF switches, thereby increasing cost [22] and adding delay at the the receivers, especially in fast-fading channels [23]. Lastly, antenna selection may reduce the combining capabilities of Bobs. Specifically, when a receiver turns on a subset of its antennas (RF chains), it ends up with lower diversity/array gain compared to when all antennas are exploited.

The main objective of this paper is to improve upon conventional ZF-based secure precoding when applied to a MU-MIMO network that is tapped by an Eve with a large number of antennas. Our setup assumes that Alice wishes to securely communicate different unicast messages to different Bobs using MU-MIMO. Each unicast message is comprised of multiple MIMO streams. Alice, which represents the base station in a cellular system or the access point in a Wi-Fi network, uses precoded FJ signal(s) to prevent Eve from capturing its information messages to Bobs. Under conventional ZF precoding, Alice's FJ signal is precoded such that its effect on Bobs' receptions is completely nullified. However, because Eve is assumed to be equipped with many antennas, she may be able to nullify Alice's FJ signal and capture one or more of the messages intended to Bobs. Accordingly, we propose a combined signaling-and-precoding scheme that makes it harder for Eve to nullify Alice's FJ. In addition to its robustness against a well-equipped Eve, our method also enables FJ to be implemented in *overloaded scenarios* without noticeable interference on data reception at Bobs. This is an advantage over conventional ZF (secure) precoding, which does not allow for the use of FJ or the nullification of multiuser interference (MUI) in an overloaded network. Our proposed design is carried out under the assumption that for any given Bob, the number of MIMO streams that comprise his information message is smaller than the number of antennas at Bobs. This assumption is justified by the same argument, discussed before, that favors antenna selection over user scheduling.

To enable improved security against a highly capable Eve, we relax the IRRC and allow MUI not to be completely nullified by the proposed precoder. Instead, we design precoders that minimize (but not eliminate) the MUI at each Bob. This is in contrast to ZF-based precoding where the MUI is completely nullified.

The remaining sections of the paper are structured as follows. In Section II.A, we introduce the system model. In Section II.B, we revisit conventional ZF precoding and clarify the differences between this approach and our proposed precoding approach. Our proposed signaling method is presented in Section III. In contrast to the conventional ZF scheme, where only one FJ signal is used to garble all information messages at Eve, our scheme utilizes several FJ signals, each designed to protect the information signal of one Bob. In Section IV, we provide security analysis for both the proposed precoding scheme as well as the conventional ZF precoding scheme. To do that, we first model the received signal at Eve. Then, we use this model to determine how many antennas Eve is required to have if she is to succeed in intercepting the information signals under both precoding methods. Finally, in Section V, we show that despite using a new signaling scheme (presented in Section III), Eve may still be able to nullify Alice's FJ. Specifically, when the proposed signaling scheme is used in conjunction with a conventional ZF precoder, some FJ jamming signals may end up falling in the same subspace, i.e., they are not orthogonal to each other. Accordingly, in the remainder of Section V, we introduce a new precoding design that aims at enhancing the near-orthogonality of the generated

FJ signals. This is done by allowing minimal MUI at Bobs and utilizing this degree of freedom in designing a new precoder. Using simulations, we show that allowing a limited amount of MUI at various Bobs does not degrade the BER and achievable information rate metrics.

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

TABLE I: Summary of key notation

Q	Number of receivers (Bobs)
M	Number of antennas at Alice
N	Number of antennas at each Bob
K	Number of MIMO data streams per Bob
L	Number of antennas at Eve
P_q	Alice's power allocated for Bob$_q$'s signal
P	Alice's total power
$\mathbf{y}_q$	Received signal at Bob$_q$ $(q = 1, \ldots, Q)$
$\mathbf{H}_q$	Channel between Alice and Bob$_q$
$\mathbf{u}_q$	Information signal from Alice that is intended for Bob$_q$
$\mathbf{u}$	Aggregate information signal from Alice
ϕ	Alice's portion of power allocated to $\mathbf{u}$
$\mathbf{f}$	FJ signal (under ZF precoding)
$\mathbf{Z}$	Precoder to nullify FJ (under ZF precoding)
$\mathbf{v}$	Artificial noise (under ZF precoding)
$\mathbf{f}'_q$	FJ signal intended for Bob$_q$ (proposed precoder)
$\mathbf{Z}'_q$	Precoder to nullify $\mathbf{f}_q$ on Bob$_q$ (proposed precoder)
$\mathbf{v}'_q$	Artificial noise to protect Bob$_q$ (proposed precoder)
$\mathbf{n}$	Noise at each Bob
$\mathbf{e}$	Noise at Eve
$\mathbf{T}_q$	MU-MIMO precoder to cancel MUI
τ	Number of columns of $\mathbf{T}_q$
$\mathbf{s}_q$	complex modulated symbol intended for Bob$_q$
$\hat{\mathbf{s}}_q$	Bob$_q$'s estimated signal from $\mathbf{s}_q$
$\mathbf{W}_q$	Precoder to boost Bob$_q$'s signal
$\mathbf{D}_q$	Receiver combiner at Bob$_q$
$\mathbf{A}_q$	Eve's receive combiner to cancel MUI of Bob$_q$'s signal
$\mathbf{B}_q$	Eve's receive combiner to estimate Bob$_q$'s signal
$\tilde{\mathbf{s}}_q$	Eve's estimated signal from $\mathbf{s}_q$

II. Conventional Zero-Forcing-based Precoding

To better understand our proposed precoder design, we first explain the ZF method used in conventional FJ techniques.

A. System Model

Consider a transmitter Alice that has M antennas and that wishes to securely communicate Q unicast messages to Q different Bobs, where $Q \geq 2$. Let $\mathcal{Q} = \{1, 2, \ldots, Q\}$. For each $q \in \mathcal{Q}$, Bob$_q$ has $N_q < M$ antennas. Without loss of generality, we assume 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 is within Alice's communications range[1]. When $M < NQ$, the network is said to be overloaded; otherwise, it is underloaded. For $q \in \mathcal{Q}$, Bob$_q$ receives K_q *independent* streams from Alice, where $K_q \leq N$. Without loss of generality, we assume $K_q = K$, $\forall q \in \mathcal{Q}$ (our subsequent analysis can be easily extended to the case when N_q and K_q vary with q by replacing KQ and NQ with $\sum_{q=1}^{Q} K_q$ and $\sum_{q=1}^{Q} N_q$, respectively). K determines how the antennas at Alice and Bobs are exploited. For example, $K = N$ implies full exploitation of multiplexing gain, whereas $K = 1$ signifies that the combining features of each receiver are used to increase the diversity gain (thus reliability) of the transmission. An illustration of our system model is shown in Fig.1.

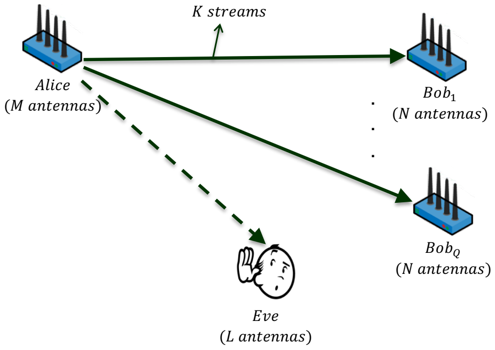

Fig. 1: System model.

B. Precoder Design

Consider the received signal at Bob$_q$, $q \in \mathcal{Q}$:

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

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 information signal from Alice, $\mathbf{f} \in \mathbb{C}^M$ is the FJ signal, and $\mathbf{n} \in \mathbb{C}^N$ is the AWGN, which is assumed to follow i.i.d. zero-mean-circularly-symmetric-complex Gaussian process with $\mathrm{E}[\mathbf{n}\mathbf{n}^{\dagger}] = N_0/N\mathbf{I}$. This means that the noise term is a complex signal; both real and imaginary components are zero-mean Gaussian random variables. Circular symmetry implies that the variance of both the real and imaginary terms are identical. The information signal $\mathbf{u}$ generated by Alice can be 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 esponsible for cancelling the MUI caused by $\mathbf{u}_q$ on other receivers Bob$_i$, $i \in \mathcal{Q}/\{q\}$, and $\mathbf{s}_q \in \mathbb{C}^K$ is the K-dimensional information signal (K streams of data) intended for Bob$_q$.

Let $\mathrm{E}[\mathbf{s}_q\mathbf{s}_q^{\dagger}] = \phi P_q/K\mathbf{I}$, where P_q is the power that Alice allocates to Bob$_q$'s signal and ϕ is the fraction of Alice's total power that is allocated to all information signals. Let $P \triangleq \sum_{q=1}^{Q} P_q$ be Alice's total power. In other words, Alice allocates ϕP of her total power to information signals and the remaining $(1 - \phi)P$ to the FJ signal. We assume that

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

Alice knows $\mathbf{H}_i$, $\forall i \in \mathcal{Q}$, but Bob$_q$ knows only $\mathbf{H}_q$. In the channel estimation phase, Alice sends pilot signals to all Bobs, allowing Bob$_q$ to estimate $\mathbf{H}_q$ and feed it back to Alice. Substituting (2) in (1), the effective channel between Alice and Bob$_q$ becomes $\mathbf{H}_q\mathbf{T}_q$.

The above treatment, however, addresses MUI but does not optimize the communication link (e.g., throughput) between Alice and Bob$_q$. To address both issues, the precoder $\mathbf{T}_q$ can be split into two precoders, one that focuses on nullifying MUI (which with some abuse of notation will be referred to as $\mathbf{T}_q$) and another that aims at optimizing the K information streams from Alice to Bob$_q$. Specifically, let the first precoder be $\mathbf{T}_q \in \mathbb{C}^{M\times\tau}$, $K \le \tau \le N$, and let the second precoder be $\mathbf{W}_q \in \mathbb{C}^{\tau\times K}$. One can view $\mathbf{H}_q\mathbf{T}_q$ as a single-link channel between Alice and Bob$_q$ for which the precoder $\mathbf{W}_q$ is designed. Accordingly, $\mathbf{y}_q$ 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$_q$ 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 obtain 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 [11].

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

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

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

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

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

is the IRRC for the downlink of the ZF method. The FJ signal in (1) has the following structure under the ZF method. Define $\tilde{\mathbf{H}} \triangleq [\mathbf{H}_1^\dagger, \dots, \mathbf{H}_Q^\dagger]^\dagger \in \mathbb{C}^{NQ\times M}$. Let $\tilde{\mathbf{H}} = \mathbf{LJR}$ 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

$$M > NQ \tag{7}$$

is the SRC under the ZF method. We choose $\tau = N$, as IRRC in (6) is dominated by SRC in (7). The FJ signal is expressed as $\mathbf{f} = \mathbf{Zv}$, where $\mathbf{Z}$ is the associated precoder for FJ, which 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 $\mathrm{Tr}[\mathbf{vv}^\dagger] = (1-\phi)P$. If SRC is violated, the FJ signal is no longer effective.

III. Proposed Signaling Method

In this section, we present the signaling part of our proposed scheme, which deals with the generation of information and FJ signals. Analogous to conditions (5a) and (5b) of Section II, we provide necessary conditions for the proposed precoding design. Our signaling design alleviates the limitations of the traditional ZF-based precoding in overloaded scenarios. Although the precoders used in this section are still the same as those of the ZF scheme, the signaling scheme that we introduce plays an important role in the design of the proposed precoders in Section V.

For the signaling scheme, we first modify the model in (1). Specifically, the received signal at Bob$_q$, $q \in \mathcal{Q}$, is now expressed as

$$\mathbf{y}_q = \mathbf{H}_q\mathbf{u}' + \mathbf{n} \tag{8}$$

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

$$\mathbf{u}' = \sum_{q=1}^{Q}\big(\mathbf{u}_q' + \mathbf{f}_q'\big). \tag{9}$$

$\mathbf{u}_q'$ is the signal intended for Bob$_q$ and $\mathbf{f}_q'$ is the FJ signal designed to protect such transmission against eavesdropping. Compared to (1), the main change in the signal model is the decomposition of the FJ signal, i.e., replacing $\mathbf{f}$ by $\mathbf{f}_q'$, $q \in \mathcal{Q}$. Such a decomposition is done in a way that each FJ signal exclusively protects the transmission intended for one Bob.

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

$$\mathbf{u}' = \sum_{q=1}^{Q}\mathbf{T}_q'(\mathbf{W}_q'\mathbf{s}_q + \mathbf{Z}_q'\mathbf{v}_q') \tag{10}$$

where $\mathbf{u}_q' = \mathbf{T}_q'\mathbf{W}_q'\mathbf{s}_q$ 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 needed to boost the information signal intended for Bob$_q$ (same as $\mathbf{W}_q$ in the previous section), $\mathbf{Z}_q'$ is the precoder for the FJ signal that protects Bob$_q$, and $\mathbf{v}_q'$ is a 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 (10) and (3)), we are assured that FJ signal $\mathbf{f}_q$, $q \in \mathcal{Q}$, 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 (8) and (10), Bob$_q$ can estimate $\mathbf{s}_q$ as follows:

$$\hat{\mathbf{s}}_q \triangleq \mathbf{D}'_q\mathbf{y}_q = \mathbf{D}'_q\left(\mathbf{H}_q\Big(\sum_{q=1}^{Q}\mathbf{T}'_q(\mathbf{W}'_q\mathbf{s}_q + \mathbf{Z}'_q\mathbf{v}'_q)\Big) + \mathbf{n}\right). \quad (11)$$

The conditions to completely nullify the MUI and FJ signals under the proposed signal model can be written as:

$$\mathbf{H}_r\mathbf{T}'_q = \mathbf{0},\ r \neq q,\ \forall r, q \in \mathcal{Q} \quad (12a)$$

$$\mathbf{D}'_q\mathbf{H}_q\mathbf{T}'_q\mathbf{Z}'_q\mathbf{v}'_q = \mathbf{0},\ \forall q \in \mathcal{Q} \quad (12b)$$

The design of $\mathbf{T}'_q$, $\mathbf{W}'_q$, and $\mathbf{D}'_q$ is similar to that of $\mathbf{T}_q$, $\mathbf{W}_q$ and $\mathbf{D}_q$ in the previous section. Therefore, the IRRC of our signaling scheme is the same as that of conventional ZF. All FJ signals are removed by a combination of (12a) and (12b), That is, an FJ signal $\mathbf{f}_q$, designed to protect Bob$_q$'s transmission, is nullified on unintended Bobs if (12a) is satisfied; furthermore, $\mathbf{f}_q$ is nullified on Bob$_q$ if (12b) is satisfied. Notice that (12b) is different from (5b) in that $\mathbf{Z}'_q$ in (12b) is designed so that only $\mathbf{v}'_q$ is nullified at Bob$_q$ with the help of $\mathbf{D}'_q$. 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., $M \geq N(Q-1)+\tau$.

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 a specific $\mathbf{Z}'_q$ is designed for each Bob$_q$. Let $\mathbf{H}_q\mathbf{T}'_q = \mathbf{U}'_q\boldsymbol{\Sigma}'_q\mathbf{V}'^{\dagger}_q$ 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 $\boldsymbol{\Sigma}'_q$ is the diagonal matrix of singular values. If Alice sets $\mathbf{W}'_q = \mathbf{V}'^{(:,1:K)}_q$, $\mathbf{D}'_q = \mathbf{U}'^{(:,1:K)^{\dagger}}_q$ (same as in the previous section), and $\mathbf{Z}'_q = \mathbf{V}^{(:,K+1:\tau)}_q$, then (12b) is satisfied (compare with the design of $\mathbf{Z}$).

IV. Security Analysis

In this section, we examine the security limitations of ZF precoding and highlight the advantages of the signaling scheme presented in the previous section in both underloaded or overloaded scenarios.

A. Zero Forcing

Consider the signal received by Eve:

$$\mathbf{z} = \mathbf{G}(\mathbf{u}+\mathbf{f}) + \mathbf{e} \quad (13)$$

where $\mathbf{G} \in \mathbb{C}^{L\times M}$ is the channel between Alice and Eve, and $\mathbf{e}$ is a noise term that has the same characteristics as $\mathbf{n}$ in (1). To eavesdrop on, say, Alice's transmission to Bob$_q$, $q \in \mathcal{Q}$, Eve must first nullify the MUI. She does that by applying a linear combiner, denoted by $\mathbf{A}_q$. 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 $\mathbf{s}_q$. Eve's estimation of $\mathbf{s}_q$ becomes:

$$\tilde{\mathbf{s}}_q = \mathbf{B}_q\mathbf{z}_q = \mathbf{B}_q\mathbf{A}_q\mathbf{z}. \quad (14)$$

We assume a worst-case scenario where Eve knows the channel matrix $\mathbf{G}$. For instance, Eve can use the pilot signals sent from Alice during 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 feedbacks 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 $\mathbf{G}$, as Eve may remain silent.

We now describe how Eve chooses her combiners to decode the transmissions of different Bobs. Combining (13) and (14), we have the following

$$\tilde{\mathbf{s}}_q = \mathbf{B}_q\mathbf{A}_q\Big(\mathbf{G}(\sum_{q=1}^{Q}\mathbf{u}_q + \mathbf{f}) + \mathbf{e}\Big) \quad (15)$$

$$= \mathbf{B}_q\mathbf{A}_q\Big(\mathbf{G}(\sum_{q=1}^{Q}\mathbf{T}_q\mathbf{W}_q\mathbf{s}_q + \mathbf{Z}\mathbf{v}) + \mathbf{e}\Big). \quad (16)$$

Eve first designs $\mathbf{A}_q$. To do that, Eve needs to satisfy the following to be able to decode the signal intended for Bob$_q$ without interference:

$$\mathbf{A}_q\mathbf{G}\,\mathbf{u}_r = \mathbf{0},\ r \neq q,\ \forall r, q \in \mathcal{Q} \quad (17a)$$

$$\mathbf{A}_q\mathbf{G}\,\mathbf{f} = \mathbf{0},\ \forall q \in \mathcal{Q}. \quad (17b)$$

Conditions (17a) and (17b) allow Eve to cancel out MUI and FJ, respectively. Define $\boldsymbol{\Omega}_q \triangleq \mathbf{G}\mathbf{T}_q\mathbf{W}_q \in \mathbb{C}^{L\times K}$ and $\boldsymbol{\Gamma} \triangleq \mathbf{G}\mathbf{Z} \in \mathbb{C}^{L\times D}$, where $D = M - NQ$ and $\mathbf{Z} \in \mathbb{C}^{M\times D}$. Let

$$\mathbf{G}_q = [\boldsymbol{\Omega}_1, \ldots, \boldsymbol{\Omega}_{q-1}, \boldsymbol{\Omega}_{q+1}, \ldots, \boldsymbol{\Omega}_Q, \boldsymbol{\Gamma}] \in \mathbb{C}^{L\times(D+K(Q-1))}. \quad (18)$$

The SVD of $\mathbf{G}_q$ is given by $\mathbf{G}_q = \mathbf{E}_q\boldsymbol{\Lambda}_q\mathbf{F}_q$. If $L > K(Q-1)+D$, Eve can cancel MUI while eavesdropping on Bob$_q$'s signal. Furthermore, Eve requires K more antennas to be able to recover $\mathbf{s}_q$. Therefore, in an *underloaded network*, Eve requires a total of

$$\Psi = D + K(Q-1) + K = M - (N-K)Q \ (\textit{Underloaded}) \quad (19)$$

antennas to nullify both MUI and FJ while eavesdropping on Bob$_q$'s signal, $q \in \mathcal{Q}$. In this case, we can increase M at Alice (while fixing N, K, and Q), which forces Eve to have more antennas if she is to achieve interference-free eavesdropping. This makes it harder for Eve to eavesdrop. In fact, by increasing M, the ZF scheme creates an FJ signal that occupies more spatial dimensions. If Eve has $L = \Psi$ antennas, she sets $\mathbf{A}_q = \mathbf{E}^{(:,\Psi-K+1:\Psi)^{\dagger}}_q$. The choice of $\mathbf{B}_q$ in (15) is simple and can be a *channel inversion* combiner or other types of linear combiners [20].

An inspection of (19) reveals that when $K = N$, Eve needs M antennas to eavesdrop successfully. However, if $K < N$, fewer antennas would be required at Eve. In an overloaded scenario (i.e., $M \leq NQ$), the SRC in (7) would be violated, thus making it infeasible to create an effective FJ signal. Hence, the additional D antennas at Eve that are needed to cancel out the FJ signal vanish (see $\boldsymbol{\Gamma}$ in (18)). With D fewer antennas subtracted from (19), Eve can cancel out MUI using only

$$\Psi = KQ \qquad (\textit{Overloaded}) \quad (20)$$

antennas, which can be significantly smaller than the total number of antennas required in (19).

B. Proposed Signaling Method

Next, we conduct the security analysis assuming the signaling scheme of Section III. The received signal at Eve can be expressed as

$$\mathbf{z} = \mathbf{G}\mathbf{u}' + \mathbf{e} = \mathbf{G}\Big(\sum_{q=1}^{Q}\big(\mathbf{u}'_q + \mathbf{f}'_q\big)\Big) + \mathbf{e}. \tag{21}$$

To eavesdrop on signals intended for Bob$_q$, Eve applies $\mathbf{A}'_q$ to its received signal. Define $\mathbf{z}_q \triangleq \mathbf{A}'_q\mathbf{z}$. Eve premultiplies $\mathbf{Z}_q$ by $\mathbf{B}'_q$ to estimate $\mathbf{s}_q$ as $\tilde{\mathbf{s}}_q \triangleq \mathbf{B}'_q\mathbf{z}_q$.

Substituting $\mathbf{z}_q = \mathbf{A}'_q\mathbf{z}$ and the RHS of (21) for $\mathbf{z}$, we end up with:

$$\tilde{\mathbf{s}}_q = \mathbf{B}'_q\mathbf{A}'_q\bigg(\mathbf{G}\Big(\sum_{q=1}^{Q}\big(\mathbf{u}'_q + \mathbf{f}'_q\big)\Big) + \mathbf{e}\bigg). \tag{22}$$

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

$$\mathbf{A}'_q\mathbf{G}\left(\mathbf{u}'_r + \mathbf{f}'_r\right) = 0,\ r \neq q,\ \forall r, q \in \mathcal{Q} \tag{23a}$$

$$\mathbf{A}'_q\mathbf{G}\,\mathbf{f}'_q = 0,\ \forall q \in \mathcal{Q} \tag{23b}$$

Using (9), (10) and (22), we see that for Eve to eavesdrop on Bob$_q$ without interference, she needs to cancel out $\mathbf{u}'_r$ and $\mathbf{f}'_r$ for $\forall r \neq q$. Hence, Eve needs to have enough antennas to concatenate the precoders used for these unintended signals in the matrix $\mathbf{G}'_q$. Therefore, she can place all $\mathbf{G}\mathbf{T}'_r\mathbf{W}'_r$ and $\mathbf{G}\mathbf{T}'_r\mathbf{Z}'_r$, $\forall r \neq q$, in the matrix $\mathbf{G}'_q$. The number of dimensions that each of these components will occupy is $K(Q-1)$ for $\mathbf{G}\mathbf{T}'_r\mathbf{W}'_r$ and $(\tau - K)(Q-1)$ for $\mathbf{G}\mathbf{T}'_r\mathbf{Z}'_r$, $\forall r \neq q$. The sum of all of these components is $\tau(Q-1)$. This is the same as setting $\mathbf{\Omega}'_q = \mathbf{G}\mathbf{T}'_q$. Hence, Eve constructs the following block matrix

$$\mathbf{G}'_q = [\mathbf{\Omega}'_1, \ldots, \mathbf{\Omega}'_{q-1}, \mathbf{\Omega}'_{q+1}, \ldots, \mathbf{\Omega}'_Q, \mathbf{\Gamma}'_q] \tag{24}$$

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 then sets $\mathbf{A}'_q$ to be the last K columns of the matrix of left singular values of $\mathbf{G}'_q$ to satisfy (23a) and (23b). 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 columns of $\mathbf{G}'_q$, i.e.,

$$\Psi' = \tau(Q-1) + (\tau - K) + K = \tau Q. \tag{25}$$

The first term in the RHS of the rightmost equality in (25) is the number of antennas that are used to establish $\mathbf{\Omega}_r,\ r \neq q,\ r \in \mathcal{Q}$. The second term is the number of antennas used to establish $\mathbf{\Gamma}'_q$ in (24). Finally, the third term is the number of antennas that are required to recover $\mathbf{s}_q$ after nullifying MUI and FJ.

Consider the underloaded scenario, i.e., $M > NQ$. We now compare our proposed method with the ZF scheme in terms of the minimum number of antennas that Eve must have for successful eavesdropping, i.e., we compare Ψ in (19) with Ψ' in (25). Let $\tau = N$ in (25). We seek the conditions under which $\Psi > \Psi'$. It is easy to see that $\Psi > \Psi'$ iff $M - (N - K)Q > NQ$, or equivalently $M > (2N-K)Q$. We examine two cases, depending on the value of K (where $K \leq N$):

- Case 1: $K = N$. In this case, $\Psi > \Psi'$ iff $M > NQ$, which is always satisfied in the underloaded scenario. In other words, if all streams are used (i.e., spatial multiplexing), the ZF method imposes a stricter requirement on Eve than our proposed scheme.
- Case 2: $K < N$. In this case, $\Psi > \Psi'$ iff $M > (2N-K)Q$. This last inequality presents a much stronger condition on network underloading than the default underloading condition $M > NQ$. In other words, the ZF method becomes superior to our proposed method only if the network is *significantly* underloaded. Cases where $\Psi > \Psi'$ (i.e., our method is superior) occur when $(2N-K)Q > M > NQ$.

V. Proposed Precoding Scheme

The precoder design for $\mathbf{T}'_q$ that we used in Section III has two issues. First, the IRRC condition is still the same as that of the conventional ZF method, which prevents our proposed signaling scheme from operating in overloaded scenarios. Second, with such a precoder design, even though our signaling scheme was shown to theoretically force Eve to have more antennas to decode Alice's messages (by adding more columns to matrix $\mathbf{G}'_q$ in (24), see Section IV-B), when we simulate this signaling scheme, we saw that the rank of $\mathbf{G}'_q$ does not increase with the added columns. Therefore, the proposed signaling scheme in Section III cannot by itself force Eve to require more antennas for interference-free eavesdropping. In this section, we modify the design of $\mathbf{T}'_q$ to resolve these issues.

To operate in overloaded scenarios, we relax condition (12a) in a way that the MUI due to $\mathbf{s}_q$ is as low as possible. Formally, we design the precoder $\mathbf{T}'_q$, $q \in \mathcal{Q}$, by solving an optimization problem. Before presenting this problem, we first formulate the ZF method as a variant of the following family of optimization problems:

$$\begin{aligned} \underset{\mathbf{T}'_q}{\text{maximize}} \quad & \frac{||\mathbf{H}_q\mathbf{T}'_q||_F}{\sum_{\substack{r=1\\ r\neq q}}^{Q} ||\mathbf{H}_r\mathbf{T}'_q||_F + \frac{NN_0}{\phi P_q}} \\ \text{s.t.} \quad & {\mathbf{T}'_q}^{\dagger}\mathbf{T}'_q = \mathbf{I} \end{aligned} \tag{26}$$

where $||\bullet||_F$ is the Frobenius norm. Problem (26) aims at selecting a precoder for Bob$_q$ such that the interference coming from $\mathbf{s}_q$ (the denominator of the objective function in (26)) is minimized while the signal strength at Bob$_q$ (the numerator of the objective function) is maximized. The constraint on $\mathbf{T}'_q$ causes the product $\mathbf{H}_q\mathbf{T}'_q$ to have the same statistical properties of $\mathbf{H}_q$. Problem (26) is identified as a Rayleigh quotient problem [24]. It is easy to see that when $N_0 \ll \phi P_q$ (i.e., high SNR regime), the solution to (26) reduces to the ZF method from the previous section because the maximum value of the objective function is reached when the denominator goes to zero, which is in line with conditions (5a) and (12a). In a moderate SNR regime, the solution to (26) reduces to MMSE-based precoding *only under an equal-power allocation strategy at all Bobs* [25]. We now examine (12a) again. This condition requires $\mathbf{H}_r\mathbf{T}'_q$ to have entries with the minimum possible value. We decompose (12a) as follows:

$$\mathbf{H}_r{\mathbf{T}'_q}^{(:,n)} = \mathbf{0},\ r \neq q,\ \forall r, q \in \mathcal{Q}\ , \forall n \tag{27}$$

where ${\mathbf{T}'_q}^{(:,n)}$ is the nth column of $\mathbf{T}'_q$. In fact, (27) is similar to (12a) but is represented on a column-by-column basis. Let $n \in \{1, \ldots, \tau\}$, where $K \leq \tau \leq N$.

Instead of (26), we propose a precoder that is obtained by solving the following optimization problem:

$$\underset{\mathbf{T}'_q}{\text{maximize}} \quad \frac{||\mathbf{H}_q{\mathbf{T}'_q}^{(:,n)}||_F}{\sum_{\substack{r=1\\r\neq q}}^{Q}||\mathbf{H}_r{\mathbf{T}'_q}^{(:,n)}||_F+\frac{NN_0}{\phi P_q\tau}}$$
$$\text{s.t.} \quad {\mathbf{T}'_q}^{(:,n)}{{\mathbf{T}'_q}^{(:,n)}}^{\dagger}=\frac{1}{\tau},\ n\in\{1,\ldots,\tau\}. \quad (28)$$

Problem (28) is still a Rayleigh quotient problem, but it differes from (26) in that in (28), the solution is obtained on a column-by-column basis. The constraint in (28) ensures that the resulting precoder does not violate the power constraint. In fact, because we assumed that $E[\mathbf{s}_q\mathbf{s}_q^{\dagger}]=\phi P_q/K\mathbf{I}$, we must also ensure that ideally, $\mathrm{Tr}[\mathbf{T}'_q\mathbf{s}_q\mathbf{s}_q^{\dagger}{\mathbf{T}'_q}^{\dagger}]=\phi P_q/K\mathbf{I}$ (see (2) and description of $\mathbf{s}_q$ below it). One can convert the above problem as follows:

$$\underset{\mathbf{T}'_q}{\text{maximize}} \quad \frac{{{\mathbf{T}'_q}^{(:,n)}}^{\dagger}\mathbf{H}_q^{\dagger}\mathbf{H}_q{\mathbf{T}'_q}^{(:,n)}}{{{\mathbf{T}'_q}^{(:,n)}}^{\dagger}\left(\sum_{\substack{r=1\\r\neq q}}^{Q}\mathbf{H}_r^T\mathbf{H}_r+\frac{\tau NN_0}{\phi P_q}\mathbf{I}\right){\mathbf{T}'_q}^{(:,n)}+}$$
$$=\frac{{{\mathbf{T}'_q}^{(:,n)}}^{\dagger}\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q{\mathbf{T}'_q}^{(:,n)}}{{{\mathbf{T}'_q}^{(:,n)}}^{\dagger}{\mathbf{T}'_q}^{(:,n)}}$$
$$\text{s.t.} \quad {\mathbf{T}'_q}^{(:,n)}{{\mathbf{T}'_q}^{(:,n)}}^{\dagger}=\frac{1}{\tau},\ n\in\{1,\ldots,\tau\} \quad (29)$$

where $\mathbf{A}^{-1}=\left(\mathbf{H}_r^T\mathbf{H}_r+\frac{\tau NN_0}{\phi P_q}\mathbf{I}\right)$. Using the method of Lagrange multipliers, we form the Lagrangian function:

$$\mathbf{L}({\mathbf{T}'_q}^{(:,n)},\lambda)={{\mathbf{T}'_q}^{(:,n)}}^{\dagger}\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q{\mathbf{T}'_q}^{(:,n)}-\lambda(||{\mathbf{T}'_q}^{(:,n)}||^2-\frac{1}{\tau}).$$

Taking the partial derivatives of the Lagrangian leads to

$$\frac{\partial\mathbf{L}}{\partial{\mathbf{T}'_q}^{(:,n)}}=2\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q{\mathbf{T}'_q}^{(:,n)}-\lambda(2{\mathbf{T}'_q}^{(:,n)})$$
$$=0\rightarrow\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q{\mathbf{T}'_q}^{(:,n)}=\lambda{\mathbf{T}'_q}^{(:,n)}$$
$$\frac{\partial\mathbf{L}}{\partial\lambda}=||{\mathbf{T}'_q}^{(:,n)}||^2-\frac{1}{\tau}=0\rightarrow||{\mathbf{T}'_q}^{(:,n)}||^2=\frac{1}{\tau}. \quad (30)$$

This implies that $({\mathbf{T}'_q}^{(:,n)},\ \lambda)$ must be an eigenpair of $\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q$, and for any solution of $\lambda=\lambda^*$ and ${\mathbf{T}'_q}^{(:,n)}={{\mathbf{T}'_q}^{(:,n)}}^*$, we have

$${{\mathbf{T}'_q}^{(:,n)}}^{\dagger*}\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q{{\mathbf{T}'_q}^{(:,n)}}^*=\lambda^*||{{\mathbf{T}'_q}^{(:,n)}}^*||^2=\frac{\lambda^*}{\tau}. \quad (31)$$

Therefore, the eignevector corresponding to the largest eigenvalue of $\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q$ is the global maximizer. Finally, the eigenvalue of $\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q$ can be simplified as follows:

$$\mathbf{A}^{-1}\mathbf{H}_q^{\dagger}\mathbf{H}_q\mathbf{v}=\lambda\mathbf{v}\Rightarrow\mathbf{H}_q^{\dagger}\mathbf{H}_q\mathbf{v}=\lambda\mathbf{A}\mathbf{v} \quad (32)$$

The right equation is called the generalized eigenvalue problem. Therefore, the solution to (28) is given by [26]:

$${\mathbf{T}'_q}^{*(:,n)}=\frac{1}{\sqrt{\tau}}\frac{\mathbf{\Delta}^{(:,n)}}{||\mathbf{\Delta}^{(:,n)}||_F} \quad (33)$$

where $\mathbf{\Delta}$ is the matrix of generalized eigenvectors corresponding to τ non-zero generalized eigenvalues of numerator and denominator of the objective in (28), i.e.,

$$\mathbf{\Delta}\triangleq\mathrm{eig}_{max,\tau}\Big(\mathbf{H}_q^{\dagger}\mathbf{H}_q,\sum_{\substack{r=1\\r\neq q}}^{Q}\mathbf{H}_r^{\dagger}\mathbf{H}_r+\frac{\tau NN_0}{\phi P_q}\mathbf{I}\Big) \quad (34)$$

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, it can be deduced that there are N eigenvectors that correspond to non-zero generalized eigenvalues in (34) [26]. Hence, $\mathbf{\Delta}\in\mathbb{C}^{M\times\tau}$.

Solving problem (28) allows us to relax the condition in (12a). Interestingly, there is no guarantee that a solution to (28) will satisfy the constraint in (26), which means that (26) and (28) are not exactly equivalent problems. Even in a high SNR regime, there is no guarantee that the two problems will lead to the same solution. In fact, the resulting precoders from (28) do not necessarily have diagonal covariance matrices to satisfy the constraint in (26). However, the constraint in (28) ensures that ${\mathbf{T}'_q}^*$ does not violate the power constraint at Alice. Furthermore, the column-by-column design strategy used in our precoders has been shown in other papers (e.g., [27]) to be superior to the original SLNR-based precoding.

For the underloaded case (i.e., $M>NQ$), we set $\tau=N$ (i.e., same as in Sections II and III). For the overloaded case, we set $\tau=\lceil\frac{M}{Q}\rceil$, where $\lceil\bullet\rceil$ is the ceiling function, which allows to consider non-integer values for 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 active. Using the fact that $K\leq\tau\leq N$, 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 (10) and (11) are defined, and our proposed precoding method is complete.

The security analysis of our method in underloaded scenarios was provided in Section IV-B, where we showed that Eve must have $\Psi'=\tau Q$ antennas to decode all information messages. In the case of an overloaded network, as mentioned earlier, we choose $\tau=\lceil\frac{M}{Q}\rceil$. Hence, $\Psi'=\max\{\tau Q,M\}$, which is the minimum number of antennas that Eve needs to have for successful eavesdropping. In contrast, it was shown in Section IV-A that under the ZF method, Eve requires only $\Psi=KQ$ antennas to decode all messages in an overloaded scenario. Because $KQ<\max\{\tau Q,M\}$, our precoder design always performs better than the conventional ZF scheme in overloaded scenarios.

Note that the proposed precoder for $\mathbf{T}'_q$ can also be used in Section II to design $\mathbf{T}_q$ in overloaded scenarios and relax condition (5a). However, this will not impact the antenna requirement at Eve for successful eavesdropping because one of the issues of using ZF-based and MMSE-based methods is that the IRRC and SRC in these methods are tied to the relation between the number of antennas at Alice (M) and the number of antennas at Bobs (N), but not the number of streams to be sent to each Bob (K).

Overall, the combination of the proposed signaling scheme in Section III and the proposed precoder in Section V not

TABLE II: Comparison of proposed method with the ZF scheme.

	The ZF Scheme	Proposed Method
MU-MIMO precoder (Mitigate MUI)	$\mathbf{T}_q,\ \forall q$	$\mathbf{T}'_q,\ \forall q$
FJ precoder	$\mathbf{f}$	$\mathbf{f}_q, \forall q$
MUI treatment (Underloaded)	Nullify MUI by $\mathbf{H}_r\mathbf{T}_q = \mathbf{0}, r \neq q,\ \forall r, q.$	$\mathbf{H}_r\mathbf{T}'_q = \mathbf{0},\ r \neq q,\ \forall r, q.$
MUI treatment (Overloaded)	If IRRC in (6) still holds, nullify MUI by $\mathbf{H}_r\mathbf{T}_q = \mathbf{0}, r \neq q, \forall r, q$. Otherwise, cannot simultaneously service all users.	Minimize MUI using (28) and (33) to simultaneously service all users.
FJ treatment (Underloaded)	Nullify FJ at all Bobs by $\mathbf{H}_q\mathbf{f} = \mathbf{0},\ \forall q.$	Nullify FJ at each Bob$_q$ by $\mathbf{D}'_q\mathbf{H}_q\mathbf{T}'_q\mathbf{f}'_q = \mathbf{0},\ \forall q.$
FJ treatment (Overloaded)	Cannot create FJ.	Nullify at each Bob$_q$ by $\mathbf{D}'_q\mathbf{H}_q\mathbf{T}'_q\mathbf{f}'_q = \mathbf{0},\ \forall q$
# antennas Eve requires for interference-free eavesdropping (Underloaded)	$M - (N - K)Q$	NQ
# antennas Eve requires for interference-free eavesdropping (Overloaded)	KQ	$\max\{\tau Q, M\},\ \tau = \lceil \frac{M}{Q} \rceil$

only handles overloaded scenarios (without scheduling or antenna selection), but also increases the rank of $\mathbf{G}'_q$ in (22), which increases the number of antennas that Eve requires to eavesdrop on Alice's transmissions.

Table II shows a summary of the main features of our proposed method alongside the ZF scheme.

VI. Antenna Selection under the Zero Forcing Scheme

In this section, we go over the well-known concept of antenna selection as another approach that facilitates MU-MIMO operation in overloaded scenarios. To compensate for the absence of FJ in overloaded scenarios, antenna selection algorithms can be used to decrease the number of functioning receive antennas at Bobs from N to N', so that SRC is satisfied, i.e., $M > N'Q$. We mainly focus on *capacity-based* antenna selection algorithms, but our analysis can be easily extended to other types of antenna selection algorithms. Suppose that $M \leq NQ$. The capacity of the channel between Alice and Bob$_q$, $q \in \mathcal{Q}$, can be expressed as[2]

$$C_q = \log\det(\mathbf{I} + \phi P_q \mathbf{H}_q \mathbf{H}_q^{\dagger}). \tag{35}$$

Using antenna selection, we are interested in employing only N' antennas of Bob$_q$, where $K \leq N' < N$, such that $M > N'Q$. Denote $\bar{\mathbf{H}}_q$ as a matrix comprised of N' columns of $\mathbf{H}_q$. Denote $\mathcal{S}(\mathbf{H}_q)$ as the set of all sub-matrices that are formed using any N' rows of $\mathbf{H}_q$. The problem of antenna selection can be formulated as:

$$\bar{\mathbf{H}}_q^* = \arg\max_{\mathcal{S}(\mathbf{H}_q)} \left(\log\det(\mathbf{I} + \phi P_q \bar{\mathbf{H}}_q \bar{\mathbf{H}}_q^{\dagger}) \right) \tag{36}$$

where $\bar{\mathbf{H}}_q^* \in \mathbb{C}^{N' \times M}$. Optimal antenna selection is a difficult integer programming problem. Thus, suboptimal algorithms such as the one in [28] can be used, which are based on minimizing the upper bounds of the capacity. After performing the antenna selection at each Bob, the SRC is expected to be met, allowing for using FJ. Hence, by replacing N with N', we can deduce from (19) that the number of antennas required at Eve to cancel out FJ and MUI under the ZF method with antenna selection[3] is $M - (N' - K)Q$.

VII. Performance Evaluation

A. Complexity Analysis

We first evaluate the worst-case computational complexity of the proposed method and contrast it with the computational complexities of the antenna selection scheme (applied in the overloaded scenario) and the ZF method (applied in the underloaded scenario). Such analysis provides theoretical insight into the computational requirements of these schemes.

The computational complexity of our method is dominated by obtaining the generalized eigenvalues in (34), which involves $O(N_r^3)$ computations. The complexity of the antenna selection method, on the other hand, is dominated by the calculation of the determinant and solving the optimization in (36). For general matrices, obtaining this determinant involves

[2] Such capacity can be achieved using dirty-paper coding, which is a nonlinear precoding method [18].

[3] Clearly, antenna selection can also be performed in situations where IRRC is violated. However, for the sake of brevity, we only apply antenna selection to satisfy SRC.

TABLE III: Comparison of Computational Complexity

	Antenna Selection Method	ZF Scheme	Proposed Method
Dominating Computation	Eq. (37)	Eq. (5a) and (5b)	Eq. (35)
Complexity	$O\left(\binom{N_r}{\tau}\tau^3\right)$	$O\left(NQM\min(NQ,M)\right)$	$O(N_r^3)$

$O(\tau^3)$ computations[4]. The determinant must be calculated $\binom{N_r}{\tau}$ times to solve the optimization problem in (36). For $\tau \neq 0$ and $\tau \neq N_r$, the antenna selection scheme must perform determinant calculation more than our proposed method. Suboptimal antenna selection schemes also need N_r^2 times to compute the determinant [20, Chapter 11.1.3], which is still higher than the number of times our method requires to calculate the precoding matrices at each Bob.

As for the traditional ZF scheme, computing the precoding matrices $\mathbf{T}_q$ and $\mathbf{f}$ that satisfy (5a) and (5b), respectively, requires SVD operations. The worst-case computation is dominated by the computation of $\mathbf{f}$ which is done in $O\left(NQM\min(NQ,M)\right)$ time.

Table III provides a comparison of the computational complexities for the proposed method, the antenna selection approach, and the ZF scheme.

B. Simulation Results

We corraborate our theoretical analyses using Matlab simulations. Our proposed method, combining the signaling method in Section III and the precoding method in Section V, is compared with the ZF scheme, discussed in Section II. For overloaded scenarios, we also compare our method with the optimal antenna selection (AS) scheme in (36) [20]. All results are based on 10^6 different realization of Rayleigh fading channels. We did not consider the effect of path loss in our simulations (e.g., by varying distances) because we did not want high/low SNR values to be a factor in studying the relative performance gain of our proposed scheme. For example, if Eve is much farther from Alice than Bobs, the received SNR at Eve will be low, and so there is no need to use FJ; hence, the methods presented in this paper (and, in general, methods for secure precoding) will be quite comparable in performance. The simulated channels realizations, however, were randomly generated to make sure that statistical analyses are meaningful. By default, we set $Q = 2$ (two Bobs). For our scheme, the total power allocated at Alice to a given Bob is split 50/50 split ($\phi = 0.5$) between the information and FJ signals associated with that Bob. This is done to simplify the treatment and focus on the effectiveness of precoding design. Optimizing ϕ requires a different treatment that takes the paper beyond its intended scope. Specifically, it is possible to maximize the secrecy sum-rate with ϕ taken as the decision variable. Such a non-convex problem has been the focus of other papers (e.g., [31], [32]). The total power allocated to a given Bob is calculated using the method in [33]. The same is done for the ZF method. We use uncoded QPSK and 16-QAM modulations in simulations. For simulations that provide SINR and achievable rate, we assume a Gaussian codebook, i.e., Gaussian random variables are used at the transmit side for all the elements of s_q, $\forall q \in Q$. This is of course an ideal scenario of primarily information-theoretic value. However, it ensures that for realistic constellations, such as QAM, the performance gain of our precoding design relative to the classical ZF precoding design is still valid [34].

Under a Gaussian codebook assumption, the CDF of the achievable rates of different precoding schemes can be obtained as follows. For the ZF method, we obtain the CDF of the following equation for many realizations of the random channel between Alice and Bobs:

$$\sum_{q=1}^{Q} C_q = \sum_{q=1}^{Q}\left(\log\det(\mathbf{I}+\phi P_q \mathbf{U}_q\mathbf{U}_q^{\dagger})\right), \tag{37}$$

where $\mathbf{U}_q \triangleq \mathbf{H}_q\mathbf{T}_q\mathbf{W}_q$.

For our proposed method, we obtain the CDF of the following equation for many realizations of the random channel between Alice and Bobs:

$$\sum_{q=1}^{Q} C_q = \sum_{q=1}^{Q}\left(\log\det(\mathbf{I}+\phi P_q \frac{\mathbf{U}_q\mathbf{U}_q^{\dagger}}{\mathbf{H}_q\left(\sum_{q\neq Q}\mathbf{Y}_q\mathbf{Y}_q^{\dagger}\right)\mathbf{H}_q^{\dagger}+\mathbf{I}})\right) \tag{38}$$

where $\mathbf{Y}_q \triangleq \mathbf{T}_q'(\mathbf{W}_q' + \mathbf{Z}_q')$.

For antenna selection, combined with ZF, we obtain the CDF of the following equation for many realizations of the channel between Alice and all Bobs:

$$\sum_{q=1}^{Q} C_q = \sum_{q=1}^{Q}\left(\log\det(\mathbf{I}+\phi P_q \bar{\mathbf{U}}_q\bar{\mathbf{U}}_q^{\dagger})\right) \tag{39}$$

where $\bar{\mathbf{U}}_q \triangleq \bar{\mathbf{H}}_q^{*}\mathbf{T}_q\mathbf{W}_q$.

In the following figures, different values for the triple (M, N, K) are selected, as indicated in the legends.

C. Underloaded Scenarios

Fig. 2 and 3 depict the symbol error rate (SER), averaged over all Bobs, versus total normalized power at Bob$_q$ for two underloaded scenarios and under, respectively, QPSK and 16-QAM modulations. Our proposed method outperforms the ZF method for all modulation schemes and all settings of (M, N, K). While exact analysis of the diversity order of our

[4] If τ is an even number, the complexity of calculating the determinant is similar to that of matrix multiplication [29]. For matrix multiplication, a naive algorithm requires $O(\tau^3)$ computations, but the faster *Strassen Algorithm* [30] can be used with complexity of $O(\tau^{2.8})$. However, Strassen algorithm is only used for very large matrix multiplication problems. Moreover, forcing τ to be an even number (to reduce the complexity of determinant calculation) may force the system to disrupt the spatial multiplexing or diversity gain. Hence, for a moderate number of antennas, we assume that determinant calculation is still done in $O(\tau^3)$ time.

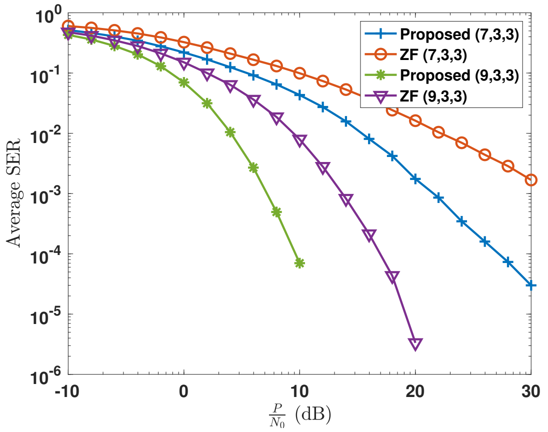

Fig. 2: SER vs. $\frac{P}{N_0}$ (QPSK, underloaded).

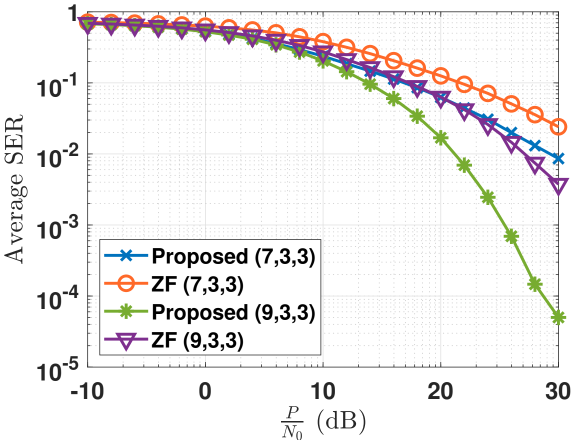

Fig. 3: SER vs. $\frac{P}{N_0}$ (16-QAM, underloaded).

scheme has not been done, the difference in the slopes of the SER curves shows that our scheme takes better advantage of antennas to achieve a higher diversity/array gain.

Fig. 4 depicts the CDF of the inverse of the *error vector magnitude* (EVM) in two underloaded scenarios. EVM (sometimes called the *relative constellation error*) is a more widely accepted measure of link performance than SINR. It is calculated by dividing the power of the constellation error in the received symbol by the power of the transmitted symbol.

We note that EVM, SINR, and BER are all metrics for measuring the quality of a communication link. It is common practice to use either BER or SNR as the main performance metric. However, determining the SNR requires knowledge of the noise floor, which can vary significantly from one receiving device to another. In addition, interference must be removed before the SNR can be determined, which requires separate techniques that would complicate the transmit/receive chains. In the case of BER, the signal must be decoded first, which in turn requires decision making at the receiver (e.g., using maximum-likelihood), thus adding complexity and/or delay. In contrast, the EVM value can be determined without decoding the received bit or symbol [35]. This can be advantageous for systems that adopt adaptive modulation. For instance, in BER-based adaptive modulation, the signal must be modulated first before updating the MCS index. In contrast, in EVM-based systems, MCS adaptation can be done without signal decoding. This advantage becomes critical when large packets are being transmitted, necessitating the implementation of intra-packet MCS adaptation. That being said, there is a relationship between EVM and BER. Studying such a relationship has been the subject of several studies (see, for example, [35]–[37]).

The inversion of the EVM is simply made to present CDF curves that are easy to analyze and compare. Our method achieves a much lower EVM than the ZF method. The reason is that although the precoders obtained using the ZF method can completely suppress MUI, they are not as effective as our scheme in contributing to the strength of the signal at the intended receiver. In contrast, our scheme does not aim for complete suppression of MUI, and instead minimizes the inevitable MUI such that the signal strength at Bobs is not decreased. The CDF of the achievable information rate is shown in Fig. 5. Our method (K) achieves a much higher information rate than ZF. It offers a better tradeoff between diversity (i.e., SER in Fig. 1 and 2) and multiplexing (i.e., achievable rate in Fig. 5). Moreover, in both Figs 4 and 5, 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 allows for exploiting the diversity gain of multiple antennas.

D. Overloaded Scenarios

Next, we study the performance of the proposed scheme in overloaded scenarios. Fig. 6 depicts the SER vs. total normalized power in two overloadeds scenario ($M = 7$, $NQ = 8$), with $K = 2$ and $K = 3$, respectively. It can be seen that the proposed method exhibits comparable SER performance to the AS scheme. However, as discussed in Section I, antenna selection methods exhibit higher overhead, e.g., require RF switches. In terms of EVM, the comparison in Fig. 7 reveals that the proposed method outperforms the AS scheme, for which the switching off of $\lceil \frac{M}{Q} \rceil$ antennas reduces the combining capabilities at each Bob.

Fig. 8 depicts the SER at Eve when $L = 5$. In both overloaded settings, having 5 antennas at Eve is enough to enable her to decode all messages when the conventional ZF design is used. In both settings, we set $\tau = 4$. Clearly, no FJ can be created in these settings using the ZF method. Our method performs significantly better than the ZF scheme because our method forces Eve to have at least $\Psi' = \max\{\tau Q, M\}$ antennas to decode all messages, compared to only $\Psi = KQ$ antennas in the ZF scheme. It can be seen that the setting $(7, 4, 3)$ experiences more SER because more data streams are used per user, which decreases the diversity gain.

In Fig. 9 we compare the achievable rate of our method in overloaded scenarios with three receivers ($Q = 3$). It can be seen that by increasing the number of spatial streams, higher achievable rates occur more often. The same is true when the number of antennas at Alice is increased from 7 to 9. However, increasing Alice's antennas results in sharper CDF

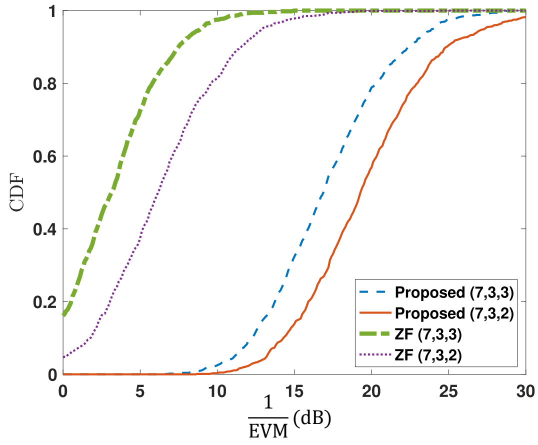

Fig. 4: CDF of inverse EVM (underloaded).

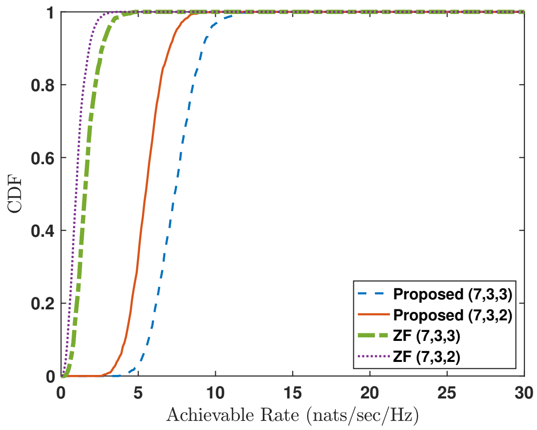

Fig. 5: CDF of achievable rate (underloaded).

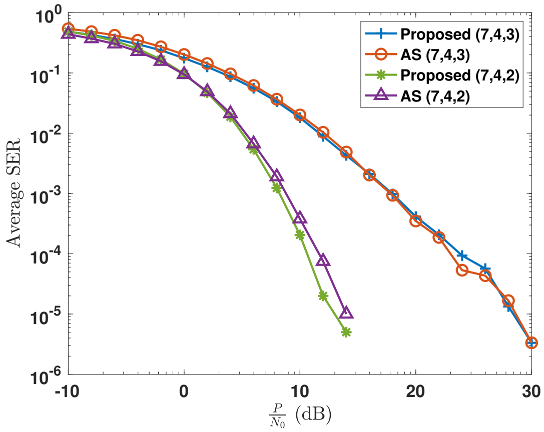

Fig. 6: SER vs. $\frac{P}{N_0}$ (overloaded).

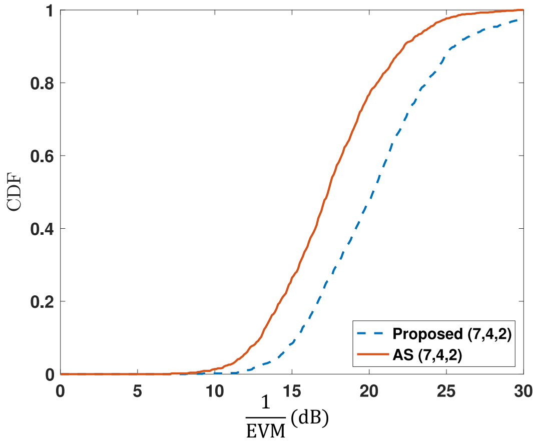

Fig. 7: CDF of the inverse EVM (overloaded).

curves, which shows that Alice is able to better manage the interference and achieve high rate more often. However, with 7 antennas at Alice, the CDF curves progresses more gradually, indicating that lower rates can occur due to tough interference conditions in the MU-MIMO network.

VIII. Conclusions

In this paper, we proposed a novel signaling-and-precoding scheme for MU-MIMO networks that not only manages the interference better than the zero-forcing method but that also enables the network to operate in overloaded settings, i.e., sum of the numbers of antennas at all bobs is larger than the number of antennas at Alice. For overloaded settings, our method is superior to the ZF method in that it requires Eve to utilize more antennas if she is to successfully eavesdrop on Alice's transmissions. Simulation results indicate that in underloaded scenarios, the proposed method is superior to ZF precoding in terms of SER, EVM, and achievable information rate. For overloaded scenarios, the ZF scheme exhibits better link performance (lower SER), but does not guarantee the secrecy of transmitted messages. A more meaningful comparison in these scenarios is between the proposed scheme and the optimal AS scheme, as both can guarantee information secrecy. For such overloaded scenarios, our simulations indicate that while both schemes achieve comparable SER, the proposed scheme exhibits lower EVM than the AS scheme, along with other advantages in terms of avoiding the extra complexity and decoding delay of AS schemes related to switching antennas on and off.

References

[1] P. Siyari, "MIMO-based friendly jamming and interference management for secure wireless communications," Ph.D. dissertation, University of Arizona, Apr. 2019.

[2] P. Siyari and M. Krunz, "Linear precoding with friendly jamming in overloaded mu-mimo wiretap networks," in *Proc. of the IEEE CNS 2019 Conf.*, 2019, pp. 1–5.

[3] C. Neumann, O. Heen, and S. Onno, "An empirical study of passive 802.11 device fingerprinting," in *Proc. of the Int. Conf. Distributed Computing Syst. Workshops*, Jun. 2012, pp. 593–602.

[4] D. Singelee and B. Preneel, "Location privacy in wireless personal area networks," in *Proc. of the ACM WiSec Conf.*, 2006, pp. 11–18.

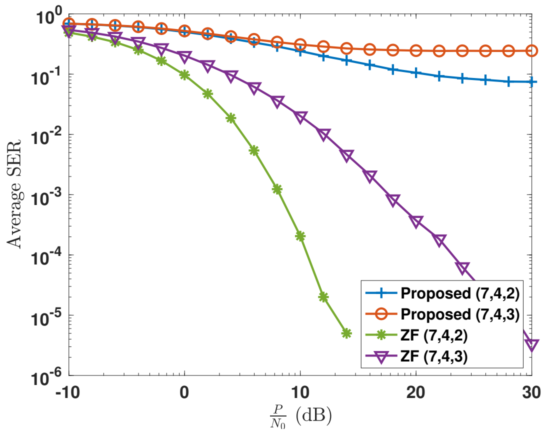

Fig. 8: Eve's SER vs. $\frac{P}{N_0}$ (overloaded).

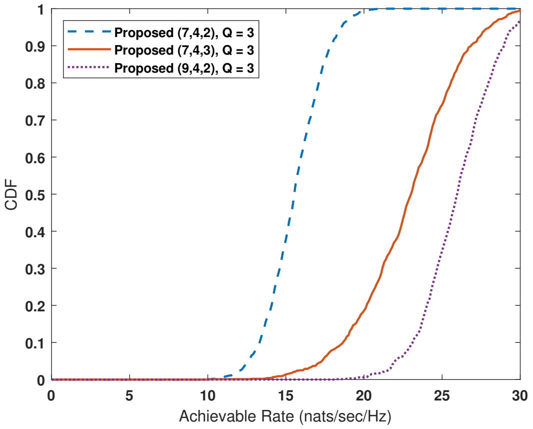

Fig. 9: CDF of achievable rate (overloaded).

[5] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *2014 IEEE Symp. Security and Privacy*, May 2014, pp. 524–539.

[6] H. Rahbari and M. Krunz, "Secrecy beyond encryption: Obfuscating transmission signatures in wireless communications," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 54–60, 2015.

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

[8] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proc. of the IEEE ISIT Conf.*, Jul. 2008, pp. 384–388.

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

[10] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using zero-forcing beamforming," in *Proc. of the IEEE INFOCOM Conf.*, Mar. 2012, pp. 720–728.

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

[12] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[13] M. Sadeghzadeh, M. Maleki, M. Salehi, and H. R. Bahrami, "Large-scale analysis of physical-layer security in multi-user wireless networks," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6450–6462, Dec. 2018.

[14] M. Sadeghzadeh, M. Maleki, and M. Salehi, "Large-scale analysis of regularized block diagonalization precoding for physical layer security of multi-user MIMO wireless networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5820–5834, Jun. 2019.

[15] N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Confidential broadcasting via linear precoding in non-homogeneous MIMO multiuser networks," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2515–2530, Jul. 2014.

[16] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation," *IEEE Trans. on Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sep. 2016.

[17] E. Ekrem and S. Ulukus, "Secure broadcasting using multiple antennas," *J. Commun. Networks*, vol. 12, no. 5, pp. 411–432, Oct. 2010.

[18] A. D. Dabbagh and D. J. Love, "Precoding for multiple antenna gaussian broadcast channels with successive zero-forcing," *IEEE Trans. Signal Process.*, vol. 55, no. 7, pp. 3837–3850, Jul. 2007.

[19] 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.

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

[21] 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.

[22] Y. Gao, H. Vinck, and T. Kaiser, "Massive MIMO antenna selection: Switching architectures, capacity bounds, and optimal antenna selection algorithms," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1346–1360, Mar. 2018.

[23] H. A. A. Saleh, A. F. Molisch, T. Zemen, S. D. Blostein, and N. B. Mehta, "Receive antenna selection for time-varying channels using discrete prolate spheroidal sequences," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2616–2627, Jul. 2012.

[24] 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.

[25] P. Patcharamaneepakorn, S. Armour, and A. Doufexi, "On the equivalence between SLNR and MMSE precoding schemes with single-antenna receivers," *IEEE Commun. Lett.*, vol. 16, pp. 1034–1037, Jul. 2012.

[26] X.-D. Zhang, *Matrix Analysis and Applications*. Cambridge, UK: Cambridge University Press, 2017.

[27] B. Ren, M. Wang, C. Yang, L. Wang, J. Zou, T. Liu, and W. Yang, "An improved leakage-based precoding scheme for multi-user MIMO systems," in *IEEE Veh. Technol. Conf.*, 2013, pp. 1–4.

[28] A. F. Molisch, M. Z. Win, Y.-S. Choi, and J. H. Winters, "Capacity of MIMO systems with antenna selection," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1759–1772, Jul. 2005.

[29] E. H. Bareiss, "Sylvester's identity and multistep integer-preserving Gaussian elimination," *Math Comp.*, vol. 22, pp. 565–578, 1968.

[30] E. W. Weisstein, Ed., *Strassen Formulas*. MathWorld–A Wolfram Web Resource.

[31] D. Park, "Weighted sum rate maximization of MIMO broadcast and interference channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1742–1753, Mar. 2016.

[32] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation," *IEEE Trans. on Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sep. 2016.

[33] B. Akgun, O. O. Koyluoglu, and M. Krunz, "Exploiting full-duplex receivers for achieving secret communications in multiuser MISO networks," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 956–968, Feb. 2017.

[34] A. Goldsmith and S.-G. Chua, "Variable-rate variable-power MQAM for fading channels," *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1218–1230, Oct. 1997.

[35] R. A. Shafik, M. S. Rahman, and A. R. Islam, "On the extended relationships among EVM, BER and SNR as performance metrics," in *2006 Int. Conf. Electrical and Comput. Eng.*, 2006, pp. 408–411.

[36] M. Oveisi and P. Heydari, "A study of BER and EVM degradation in digital modulation schemes due to PLL jitter and communication-link noise," *IEEE Trans. Circuits and Systems I: Regular Papers*, vol. 69, no. 8, pp. 3402–3415, 2022.

[37] M. D. Ardakani and S. O. Tatu, "V-Band six-port interferometer receiver: High data-rate wireless applications, BER and EVM analysis, and CFO compensation," *IEEE Access*, vol. 9, pp. 160 847–160 854, 2021.

Marwan Krunz (S'93-M'95-SM'04-F'10) is a Regents Professor at the University of Arizona. He holds the Kenneth VonBehren Endowed Professorship in ECE and is also a professor of computer science. He directs the Broadband Wireless Access and Applications Center (BWAC), a multi-university NSF/industry center that focuses on next-generation wireless technologies. He is an affiliated faculty of the UA Cancer Center. Previously, he served as the site director for the Connection One center. Dr. Krunz's research is on resource management, network protocols, and security for wireless systems. He has published more than 325 journal articles and peer-reviewed conference papers, and is a named inventor on 10 patents. His latest h-index is 60. He is an IEEE Fellow, an Arizona Engineering Faculty Fellow, and an IEEE Communications Society Distinguished Lecturer (2013-2015). He received the NSF CAREER award. He served as the Editor-in-Chief for the IEEE Transactions on Mobile Computing. He also served as editor for numerous IEEE journals. He was the TPC chair for INFOCOM'04, SECON'05, WoWMoM'06, and Hot Interconnects 9. He was the general vice-chair for WiOpt 2016 and general co-chair for WiSec'12. Dr. Krunz served as chief scientist for two startup companies that focus on 5G and beyond systems and machine learning for wireless communications.

Peyman Siyari received the B.Sc. degree from Semnan University, Iran, in 2011, and the M.Sc. degree from AmirKabir University of Technology, Iran, in 2013, all in Electrical Engineering. He received the Ph.D. degree in electrical and computer engineering from the University of Arizona in 2019. Since then, he has been with Qualcomm Inc. His research interests include physical layer security, applications of convex optimization in signal processing, and game theory.