Multiuser Diversity for Secrecy Communications Using Opportunistic Jammer Selection – Secure DoF and Jammer Scaling Law

Jung Hoon Lee, *Student Member, IEEE*, and Wan Choi, *Senior Member, IEEE*

Abstract

In this paper, we propose opportunistic jammer selection in a wireless security system for increasing the secure degrees of freedom (DoF) between a transmitter and a legitimate receiver (say, Alice and Bob). There is a jammer group consisting of S jammers among which Bob selects K jammers. The selected jammers transmit independent and identically distributed Gaussian signals to hinder the eavesdropper (Eve). Since the channels of Bob and Eve are independent, we can select the jammers whose jamming channels are aligned at Bob, but not at Eve. As a result, Eve cannot obtain any DoF unless it has more than KN_j receive antennas, where N_j is the number of jammer's transmit antenna each, and hence KN_j can be regarded as defensible dimensions against Eve. For the jamming signal alignment at Bob, we propose two opportunistic jammer selection schemes and find the scaling law of the required number of jammers for target secure DoF by a geometrical interpretation of the received signals.

Index Terms

Physical layer security, secure DoF, multiuser diversity, opportunistic jammer selection

A part of this paper has been presented in *IEEE Global Commun. Conf. (Globecom)*, Anaheim, CA, Dec. 2012.

J. H. Lee and W. Choi are with Department of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 305-701, Korea (e-mail: tantheta@kaist.ac.kr wchoi@ee.kaist.ac.kr).

I. INTRODUCTION

Wireless communication systems are vulnerable to eavesdropping because transmitted signals are broadcasted over the air. Privacy and security start being treated as important issues. Traditionally, security in wireless communications has mainly been addressed in upper layers and focused on computational security such as cryptography. Recently, information-theoretic security in physical layer has received great attentions because it enables perfect secrecy without the aid of encryption/decryption keys.

A typical model of a security communication system consists of three nodes – a transmitter (Alice), a legitimate receiver (Bob), and a passive eavesdropper (Eve). Information theoretic security study was opened by Shannon [1] with the notion of perfect secrecy. The wiretap channel model was first introduced by Wyner [2] and *secrecy capacity* is defined in [3] as the maximum achievable rate of Bob preventing Eve from obtaining any information. Positive secrecy capacity was shown to be achieved when Bob's channel is less noisy than Eve's. For guaranteeing positive secrecy rate, artificial noise was additionally transmitted from the transmitter [4]. The authors in [5] showed that the artificial noise can enlarge the secrecy rate region in a symmetric interference channel. The secrecy issues were also studied in cooperative relay systems [6]–[8]. In [7], [8], joint selection of relays and jammers was studied and opportunistic jamming and relay chatting was proposed.

As an alternative measure to secrecy capacity, secure degrees of freedom (DoF) have popularly been investigated. In [9], the secure DoF was found in an X network. For N-user Gaussian interference channels, an interference channel with confidential message and an interference channel with an external eavesdropper were studied in [10], [11], respectively. The secure DoFs for those cases were shown to be $\frac{N-2}{2N-2}$ and $\frac{N-2}{2N}$, respectively, while a half DoF per orthogonal dimension is to be achievable via the *interference alignment* (IA) scheme [12], [13] in the absence of the secrecy constraint.

The multiuser diversity, exploiting multiuser dimensions by serving the selected users with good channel conditions, can enhance the performance of wireless communication systems [14]–[19]. In many cases, the multiuser diversity asymptotically achieves the optimal performance with considerably reduced channel

feedback overhead. Recently, the opportunistic interference alignment (OIA) has been proposed by the authors in order to resolve the difficulties of IA implementation [20]–[22]. In the OIA scheme, user dimensions are exploited to align interfering channels; each transmitter has multiple users and selects a single user having the most aligned interfering channels. The OIA scheme does not require the global channel state information (CSI) and large computational complexity for precoding/postprocessing design. A bit surprisingly, the achieved DoF by OIA was shown to be higher than that of conventional IA thanks to multiuser dimensions. This result motivates new applications using the concept of OIA for security communication systems.

In this paper, we propose opportunistic jammer selection (OJS) schemes for secure DoF. The basic idea of OJS is to align jamming signals at Bob's receiver via jammer selection, while the jamming signals are not aligned at Eve. There is a jammer group consisting of S jammers, and Bob selects $K(\geq 2)$ jammers among them whose jamming signals are most aligned. Since we use jamming subspaces formed by jammers, the selected jammers simply use independent and identically distributed (i.i.d) Gaussian signals independent of Eve's CSI as well as Alice's. Denoting the numbers of antennas at Alice, Bob, and Eve by N_t, N_r, and N_e, respectively, we focus on the cases that $N_t + N_j \leq N_r < N_t + KN_j$ because these cases require the jamming signal alignment at Bob's receiver.

Although the jamming signals from the selected jammers can be aligned at Bob's receiver, they are randomly given to Eve and hence span KN_j-dimensional subspace at Eve's receiver. Because Eve requires more than KN_j receive antennas to obtain non-zero DoF[1], we can regard KN_j as *defensible dimensions* of the system. For any number of Eve's receive antennas, we can make Eve's DoF zero by increasing either the number of selected jammers K or the number of each jammer's antennas N_j. On the contrary, the jamming signals from the selected jammers can be aligned in N_j-dimensional subspace at Bob's receiver if the number of jammers goes to infinity. In this case, Bob needs only $N_t + N_j$ receive antennas to obtain DoF of N_t while Eve needs $N_t + KN_j$ receive antennas.

[1]Eve's DoF is defined by $\lim_{P\to\infty} (\mathcal{C}_{\text{Eve}}/\log_2 P)$ where $\mathcal{C}_{\text{Eve}}$ is Eve's channel capacity.

Although both OIA and OJS exploit multiuser (or multiple jammer) dimensions to align interfering (or jamming) signals, the problems are quite different. In OIA, each user in N-transmitter IC has $N-1$ interfering channels jointly determined for each channel realization. Thus, the OIA problem is to measure how much the $N-1$ interfering channels are aligned at the selected user when each user has $N-1$ random interfering channels. However, because Bob chooses K jammers among total S jammers in OJS, the problem is changed to how much we can align the K jamming signals by directly picking each jamming signal among S jamming signals.

There have been many studies on utilizing jammers for increasing secure DoF [23], [24], [26]. In [23], cooperative jamming with structured jamming signals based on lattice coding was proposed for a Gaussian wiretap channel. In multiple access fading channels, [24] proposed two ergodic alignment schemes for secrecy communications – scaling based alignment (SBA) and ergodic secret alignment (ESA). In SBA, users repeatedly transmit their symbols with proper scaling over several consecutive time slots. Then, the signals are aligned at eavesdropper's receiver and hence Eve's DoF becomes zero. In ESA, the concept of ergodic IA [25] was extended to secrecy communications. In [26], cooperative jammers were exploited to increase secure DoF in a Gaussian wiretap channel, where transmitter and cooperative jammers send jointly designed signals according to channel conditions. Contrary to the previous works, in our proposed OJS schemes, the selected jammers adopt i.i.d Gaussian signals oblivious to CSI. Furthermore, any precoding design at Alice is not required for the proposed scheme. Because the role of CSI is only for constructing the wiretap code, the proposed OJS scheme does not suffer from secure DoF degradation even with only Bob's CSI, which is a practical advantage of the proposed OJS scheme.

Our contributions are summarized below.

- Using a geometrical interpretation of jamming signals, we define an *alignment measure* representing how well the selected jamming signals are aligned at Bob's receiver and quantify the achievable alignment measure via jammer selection for the total number of jammers.
- To obtain the secure DoF, we propose two jammer selection schemes – the minimum DoF loss

jammer selection and the subspace-based jammer selection. Using the proposed jammer selection schemes, we show that Bob can achieve the secure DoF of $d \in (0, N_t]$ when the number of jammers is scaled by $S \propto P^{dN_j/2}$ where P is transmit power.

- We show that the same secure DoF is achievable with secrecy outage probability ϵ by the proposed OJS with only Bob's CSI.

The rest of the paper is organized as follows. Section II presents the system model. The achievable secure DoF via opportunistic jammer selection is analyzed in Section III. We geometrically interpret the jamming channels in Section IV, and propose opportunistic jammer selection schemes in Section V. In Section VI, we derive the scaling laws of the required number of jammers for target secure DoF. Numerical results are presented in Section VII, followed by concluding remarks in Section VIII.

II. System Model

Our system model is depicted in Fig. 1. Alice wants to send secret messages to Bob, and a passive eavesdropper, Eve, overhears the secret messages. The numbers of antennas at Alice, Bob, and Eve are denoted by N_t, N_r, and N_e, respectively. To prevent Eve's eavesdropping, there is a jammer group consisting of S jammers with N_j antennas each, and Bob selects K $(K \geq 2)$ jammers among them. The selected jammers simultaneously transmit i.i.d. Gaussian signals independent of Alice's message so that the jamming signals interfere with Bob as well as Eve.

We assume that Alice and the selected jammers fully utilize their antenna dimensions, i.e., Alice and each selected jammer transmit N_t and N_j streams, respectively. We also assume that Eve has more antennas than each jammer, i.e., $N_e > N_j$, and Bob selects K jammers such that $KN_j \geq N_e$. We consider the cases that Bob has N_r receive antennas such that $N_t + N_j \leq N_r < N_t + KN_j$. If Bob has a less number of receive antennas than the total number of antennas at Alice and a jammer, i.e., $N_r < N_t + N_j$, Bob cannot obtain DoF of N_t; otherwise, if the number of Bob's antennas is larger than or equal to the total number of Alice and all selected jammers' antennas, i.e., $N_r \geq N_t + KN_j$, Bob can easily achieve DoF of N_t with zero-forcing like schemes.

Since Bob knows the jamming channel from each jammer, we assume that Bob selects K jammers in the jammer group with only its own CSI. It is also assume that Eve has its own CSI from the selected jammers, which is independent of Bob's CSI. For wiretap code construction at Alice, we firstly assume that Alice knows Bob's achievable rate and Eve's channel capacity after Bob's jammer selection. Then, in Section VI-A we show that the required jammer scaling for the target secure DoF is the same even in practical scenarios that Alice has no information about Eve.

In this paper, we adopt the quasi-static fading channel model [27], where the coherent interval is longer than the jammer selection procedure and the length of a codeword. That is, the channel coefficients remain constant over the transmission of an entire codeword but each codeword suffers from an independent channel.

Let $s_1, \ldots, s_K$ be the indices of the K selected jammers in the jammer group. Then, the received signal of Bob, $\mathbf{y} \in \mathbb{C}^{N_r \times 1}$, is given by

$$\mathbf{y} = \mathbf{H}_0 \mathbf{x}_0 + \sum_{k=1}^{K} \mathbf{H}_{s_k} \mathbf{x}_{s_k} + \mathbf{n}, \tag{1}$$

where $\mathbf{H}_0 \in \mathbb{C}^{N_r \times N_t}$ is the channel matrix from Alice to Bob, and $\mathbf{H}_{s_k} \in \mathbb{C}^{N_r \times N_j}$ is the channel matrix from the s_kth jammer to Bob. We assume that all elements of the channel matrices are i.i.d. complex Gaussian random variables with zero mean and unit variance. The vectors $\mathbf{x}_0 \in \mathbb{C}^{N_t \times 1}$ and $\mathbf{x}_{s_k} \in \mathbb{C}^{N_j \times 1}$ are the transmit signal from Alice and the s_kth jammer, respectively, satisfying $\mathbb{E}[\mathbf{x}_0 \mathbf{x}_0^\dagger] = (P/N_t)\mathbf{I}_{N_t}$ and $\mathbb{E}[\mathbf{x}_{s_k} \mathbf{x}_{s_k}^\dagger] = (P/N_j)\mathbf{I}_{N_j}$, where $(\cdot)^\dagger$ denotes conjugate transpose, P is total transmit power budget at each node, and $\mathbf{I}_{N_t}$ is an $N_t \times N_t$ identity matrix. $\mathbf{n} \in \mathbb{C}^{N_r \times 1}$ is a circularly symmetric complex Gaussian noise vector such that $\mathbf{n} \sim \mathcal{CN}(0, \mathbf{I}_{N_r})$.

From (1), the capacity of Bob becomes

$$\mathcal{C}_{\text{Bob}} \triangleq \log_2 \left| \mathbf{I}_{N_r} + \frac{P}{N_t} \mathbf{H}_0 \mathbf{H}_0^\dagger \left(\mathbf{I}_{N_r} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{H}_{s_k} \mathbf{H}_{s_k}^\dagger \right)^{-1} \right|.$$

In this paper, we assume that Bob uses the postprocessing matrix $\mathbf{V}^\dagger \in \mathbb{C}^{N_t \times N_r}$ such that $\mathbf{V}^\dagger \mathbf{V} = \mathbf{I}_{N_t}$ to

suppress the jamming signals. After postprocessing, the received signal at Bob is given by

$$\mathbf{V}^\dagger \mathbf{y} = \mathbf{V}^\dagger \mathbf{H}_0 \mathbf{x}_0 + \sum_{k=1}^{K} \mathbf{V}^\dagger \mathbf{H}_{s_k} \mathbf{x}_{s_k} + \mathbf{V}^\dagger \mathbf{n},$$

and the achievable rate of Bob becomes

$$\mathcal{R}_{\text{Bob}} \triangleq \log_2 \frac{\left| \mathbf{I}_{N_t} + \mathbf{V}^\dagger \left(\frac{P}{N_t} \mathbf{H}_0 \mathbf{H}_0^\dagger + \sum_{k=1}^{K} \frac{P}{N_j} \mathbf{H}_{s_k} \mathbf{H}_{s_k}^\dagger \right) \mathbf{V} \right|}{\left| \mathbf{I}_{N_t} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{V}^\dagger \mathbf{H}_{s_k} \mathbf{H}_{s_k}^\dagger \mathbf{V} \right|}.$$

On the other hand, the received signal at Eve denoted by $\bar{\mathbf{y}} \in \mathbb{C}^{N_e \times 1}$ becomes

$$\bar{\mathbf{y}} = \mathbf{G}_0 \mathbf{x}_0 + \sum_{k=1}^{K} \mathbf{G}_{s_k} \mathbf{x}_{s_k} + \bar{\mathbf{n}},$$

where $\mathbf{G}_0 \in \mathbb{C}^{N_e \times N_t}$ and $\mathbf{G}_{s_k} \in \mathbb{C}^{N_e \times N_j}$ are the channel matrices from Alice and from the selected jammer s_k, respectively, whose elements are i.i.d. complex Gaussian random variables with zero mean and unit variance. Also, $\bar{\mathbf{n}} \in \mathbb{C}^{N_e \times 1}$ is a circularly symmetric complex Gaussian noise vector such that $\bar{\mathbf{n}} \sim \mathcal{CN}(0, \mathbf{I}_{N_e})$. Thus, the channel capacity of Eve is given by

$$\mathcal{C}_{\text{Eve}} \triangleq \log_2 \left| \mathbf{I}_{N_e} + \frac{P}{N_t} \mathbf{G}_0 \mathbf{G}_0^\dagger \left(\mathbf{I}_{N_e} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{G}_{s_k} \mathbf{G}_{s_k}^\dagger \right)^{-1} \right|. \tag{2}$$

Therefore, the secrecy rate $[\mathcal{R}_{\text{Bob}} - \mathcal{C}_{\text{Eve}}]^+$ is achievable at Bob for each channel realization through the Wyner's encoding scheme [2], [28] with nested code structure, where $[\cdot]^+$ denotes $\max(\cdot, 0)$. In an average sense, we obtain the secrecy rate and the secure DoF given, respectively, by

$$\begin{aligned} \text{Secrecy rate} &= \mathbb{E}\left\{ [\mathcal{R}_{\text{Bob}} - \mathcal{C}_{\text{Eve}}]^+ \right\}, \\ \text{Secure DoF} &= \mathbb{E}\left\{ \lim_{P \to \infty} \frac{[\mathcal{R}_{\text{Bob}} - \mathcal{C}_{\text{Eve}}]^+}{\log_2 P} \right\}. \end{aligned} \tag{3}$$

III. Achievable Secure DoF via Opportunistic Jammer Selection

A. The Concept of Opportunistic Jammer Selection

The purpose of the opportunistic jammer selection is to obtain the secure DoF between Alice and Bob. To hinder Eve's eavesdropping, Bob selects K jammers among S jammers in the jammer group. Since the jamming signals also interfere with Bob, appropriate jammers should be selected from the jammer group. Using the IA concept, the subspace spanned by multiple N_j-dimensional signals can be reduced

minimally in the N_j-dimensional subspace. It was also shown in [20]–[22] that interference alignment can be achieved by opportunistic user selection if the number of users goes to infinity.

Since each jammer has N_j transmit antennas, each jamming signal spans N_j-dimensional subspace in $\mathbb{C}^{N_r}$ at Bob's receiver. Thus, opportunistically selected jamming signals can be aligned in N_j-dimensional subspace if the selection pool size S goes to infinity. If the jamming signals are aligned in $(N_r - N_t)$-dimensional subspace at Bob's receiver, Bob can use the residual N_t dimensions for Alice's signals. The concept of the opportunistic jammer selection is illustrated in Fig. 2. In the jammer group, Bob selects K jammers whose channels are most aligned. When there are an infinite number of jammers (i.e., $S = \infty$), the jamming signals can be perfectly aligned in N_j-dimensional subspace at Bob's receiver by proper jammer selection. In this case, $N_t + N_j$ antennas are enough for Bob to achieve DoF of N_t. At Eve's receiver, on the other hand, the jamming signals are not aligned and span KN_j-dimensional subspace. This is because the jammer selection of Bob is independent of Eve so that it corresponds to a random jammer selection to Eve. Since KN_j-dimensional subspace at Eve's receiver is corrupted by the jamming signals from the selected K jammers, KN_j can be interpreted as *defensible dimensions* of the security system against eavesdropping. If the number of Eve's receive antenna is less than KN_j, Eve cannot achieve any DoF; Eve needs $N_t + KN_j$ receive antennas for DoF of N_t. Thus, the jamming system is designed according to the target defensible dimensions. Since Eve has N_e antennas, we require the defensible DoF larger than or equal to N_e, i.e., $KN_j \geq N_e$ to yield the zero DoF at Eve.

B. Secure DoF via Opportunistic Jammer Selection

In this section, we find the achievable secure DoF via OJS. We recall the channel capacity of Eve given in (2):

$$\mathcal{C}_{\text{Eve}} \triangleq \log_2 \left| \mathbf{I}_{N_e} + \frac{P}{N_t} \mathbf{G}_0 \mathbf{G}_0^{\dagger} \left(\mathbf{I}_{N_e} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{G}_{s_k} \mathbf{G}_{s_k}^{\dagger} \right)^{-1} \right|.$$

Then, it can be decomposed into $\mathcal{C}_{\text{Eve}}^{+}$ and $\mathcal{C}_{\text{Eve}}^{-}$ such that $\mathcal{C}_{\text{Eve}} = \mathcal{C}_{\text{Eve}}^{+} - \mathcal{C}_{\text{Eve}}^{-}$ given by

$$\mathcal{C}_{\text{Eve}}^{+} \triangleq \log_2 \left| \mathbf{I}_{N_e} + \frac{P}{N_t} \mathbf{G}_0 \mathbf{G}_0^{\dagger} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{G}_{s_k} \mathbf{G}_{s_k}^{\dagger} \right|$$
$$\mathcal{C}_{\text{Eve}}^{-} \triangleq \log_2 \left| \mathbf{I}_{N_e} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{G}_{s_k} \mathbf{G}_{s_k}^{\dagger} \right|.$$

In the above equations, the matrix $\sum_{k=1}^{K} \mathbf{G}_{s_k} \mathbf{G}_{s_k}^{\dagger} (= [\mathbf{G}_{s_1}, \ldots, \mathbf{G}_{s_K}][\mathbf{G}_{s_1}, \ldots, \mathbf{G}_{s_K}]^{\dagger})$ becomes an $N_e \times N_e$ Wishart matrix with KN_j $(\geq N_e)$ DoF, and hence it has N_e non-zero eigenvalues with probability one. From this fact, we can easily show that Eve's DoF becomes zero for each channel realization such that

$$\lim_{P \to \infty} \frac{\mathcal{C}_{\text{Eve}}}{\log_2 P} = \lim_{P \to \infty} \frac{\mathcal{C}_{\text{Eve}}^{+} - \mathcal{C}_{\text{Eve}}^{-}}{\log_2 P} = N_e - N_e = 0. \tag{4}$$

This implicates that the achievable DoF at Bob directly becomes the secure DoF.

To find the secure DoF at Bob, we decompose the average achievable rate at Bob, i.e., $\mathbb{E}\left[\mathcal{R}_{\text{Bob}}\right]$, into $\mathcal{R}_{\text{Bob}}^{+}$ and $\mathcal{R}_{\text{Bob}}^{-}$ such that $\mathbb{E}\left[\mathcal{R}_{\text{Bob}}\right] = \mathcal{R}_{\text{Bob}}^{+} - \mathcal{R}_{\text{Bob}}^{-}$, which are given, respectively, by

$$\mathcal{R}_{\text{Bob}}^{+} = \mathbb{E} \log_2 \left| \mathbf{I}_{N_t} + \mathbf{V}^{\dagger} \left(\frac{P}{N_t} \mathbf{H}_0 \mathbf{H}_0^{\dagger} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{H}_{s_k} \mathbf{H}_{s_k}^{\dagger} \right) \mathbf{V} \right|$$
$$\mathcal{R}_{\text{Bob}}^{-} = \mathbb{E} \log_2 \left| \mathbf{I}_{N_t} + \frac{P}{N_j} \sum_{k=1}^{K} \mathbf{V}^{\dagger} \mathbf{H}_{s_k} \mathbf{H}_{s_k}^{\dagger} \mathbf{V} \right|.$$

Then, similar to (4), the achievable DoF of Bob becomes

$$\begin{aligned} \mathbb{E}\left\{ \lim_{P \to \infty} \frac{\mathcal{R}_{\text{Bob}}}{\log_2 P} \right\} &= \lim_{P \to \infty} \frac{\mathcal{R}_{\text{Bob}}^{+} - \mathcal{R}_{\text{Bob}}^{-}}{\log_2 P} \\ &= N_t - \lim_{P \to \infty} \frac{\mathcal{R}_{\text{Bob}}^{-}}{\log_2 P}. \end{aligned} \tag{5}$$

In (4), we show that Eve's DoF becomes zero for each channel realization. By plugging (4) and (5) in (3), we obtain the achievable secure DoF via opportunistic jammer selection:

$$\boxed{\text{Secure DoF} = N_t - \lim_{P \to \infty} \frac{\mathcal{R}_{\text{Bob}}^{-}}{\log_2 P}.} \tag{6}$$

Therefore, the achievable secure DoF depends on how much the DoF loss from jamming signals is reduced at Bob. In the latter part of the paper, we set the target secure DoF $d \in (0, N_t]$ and find the number of required jammers to obtain the target secure DoF.

IV. Geometric Interpretations

A. Geometric Interpretations of Jamming Channels

The Grassmann manifold $\mathcal{G}_{N_r,N_j}(\mathbb{C})$ is set of all N_j-dimensional subspaces in $\mathbb{C}^{N_r}$ [33]–[35]. Since each jammer and Bob have N_j and N_r antennas, respectively, the channel matrix from each jammer to Bob constructs an N_j-dimensional subspace in $\mathbb{C}^{N_r}$. Let H_k be the subspace formed by the channel matrix from the kth jammer to Bob, i.e., $\mathbf{H}_k$. Then, it belongs to the Grassmann manifold $\mathcal{G}_{N_r,N_j}(\mathbb{C})$, i.e., $\mathsf{H}_k \in \mathcal{G}_{N_r,N_j}(\mathbb{C})$. Each subspace can be represented by the *generator matrix* whose columns are orthonormal and span the same subspace. If we denote the generator matrix of H_k by $\tilde{\mathbf{H}}_k \in \mathbb{C}^{N_r \times N_j}$, it is satisfied that $\tilde{\mathbf{H}}_k^\dagger \tilde{\mathbf{H}}_k = \mathbf{I}_{N_j}$ and $\mathrm{span}(\tilde{\mathbf{H}}_k) = \mathrm{span}(\mathbf{H}_k) = \mathsf{H}_k$. Since Bob has more antennas than Alice, Bob can partly suppress the jamming signals using the residual antenna dimensions. In our case, the N_j-dimensional jamming signals should be aligned in $(N_r - N_t)$-dimensional subspace to obtain the secure DoF of N_t.

The distance between two subspaces can be defined in many ways. The *chordal distance* is one of the most widely used ones. Let $\mathsf{Q} \in \mathcal{G}_{N_r,N_r-N_t}(\mathbb{C})$ be an arbitrary $(N_r - N_t)$-dimensional subspace and $\mathbf{Q} \in \mathbb{C}^{N_r \times (N_r - N_t)}$ be its generator matrix such that $\mathbf{Q}^\dagger \mathbf{Q} = \mathbf{I}_{N_r - N_t}$. Then, the squared chordal distance between $\mathsf{H}_k \in \mathcal{G}_{N_r,N_j}(\mathbb{C})$ and $\mathsf{Q} \in \mathcal{G}_{N_r,N_r-N_t}(\mathbb{C})$ denoted by $d_c^2(\mathsf{H}_k, \mathsf{Q})$ is calculated from the generator matrices of them such that

$$\begin{aligned} d_c^2(\mathsf{H}_k, \mathsf{Q}) &\triangleq \min(N_j, N_r - N_t) - tr(\tilde{\mathbf{H}}_k \tilde{\mathbf{H}}_k^\dagger \mathbf{Q}\mathbf{Q}^\dagger) \\ &\overset{(a)}{=} N_j - tr(\tilde{\mathbf{H}}_k^\dagger \mathbf{Q}\mathbf{Q}^\dagger \tilde{\mathbf{H}}_k), \end{aligned} \tag{7}$$

where the equality (a) holds because $N_r \geq N_t + N_j$ and $tr(\mathbf{AB}) = tr(\mathbf{BA})$. Note that $\tilde{\mathbf{H}}_k \tilde{\mathbf{H}}_k^\dagger$ and $\mathbf{Q}\mathbf{Q}^\dagger$ are the projection matrices onto the subspaces H_k and Q, respectively. See [29] for more details on the chordal distance.

Lemma 1. *The squared chordal distance between* H_k *and* Q *is equivalent to*

$$d_c^2(\mathsf{H}_k, \mathsf{Q}) = tr((\mathbf{Q}^\perp)^\dagger \tilde{\mathbf{H}}_k \tilde{\mathbf{H}}_k^\dagger (\mathbf{Q}^\perp)), \tag{8}$$

where $\mathbf{Q}^{\perp} \in \mathbb{C}^{N_r \times N_t}$ *is the generator matrix of the orthogonal complement subspace of* Q *denoted by* $\mathsf{Q}^{\perp} \in \mathcal{G}_{N_r,N_t}(\mathbb{C})$.

Proof. To prove the equivalence between (7) and (8), it is enough to show $tr(\mathbf{Q}^{\dagger}\tilde{\mathbf{H}}_k\tilde{\mathbf{H}}_k^{\dagger}\mathbf{Q})+tr((\mathbf{Q}^{\perp})^{\dagger}\tilde{\mathbf{H}}_k\tilde{\mathbf{H}}_k^{\dagger}(\mathbf{Q}^{\perp})) = N_j$. Since the concatenated matrix $[\mathbf{Q}, \mathbf{Q}^{\perp}]$ is an unitary matrix such that

$$[\mathbf{Q}, \mathbf{Q}^{\perp}][\mathbf{Q}, \mathbf{Q}^{\perp}]^{\dagger} = [\mathbf{Q}, \mathbf{Q}^{\perp}]^{\dagger}[\mathbf{Q}, \mathbf{Q}^{\perp}] = \mathbf{I}_{N_r},$$

it is satisfied that

$$\begin{aligned} &tr(\mathbf{Q}^{\dagger}\tilde{\mathbf{H}}_k\tilde{\mathbf{H}}_k^{\dagger}\mathbf{Q}) + tr((\mathbf{Q}^{\perp})^{\dagger}\tilde{\mathbf{H}}_k\tilde{\mathbf{H}}_k^{\dagger}(\mathbf{Q}^{\perp})) \\ &\quad = tr([\mathbf{Q}, \mathbf{Q}^{\perp}]^{\dagger}\tilde{\mathbf{H}}_k\tilde{\mathbf{H}}_k^{\dagger}[\mathbf{Q}, \mathbf{Q}^{\perp}]) \overset{(a)}{=} tr(\tilde{\mathbf{H}}_k^{\dagger}[\mathbf{Q}, \mathbf{Q}^{\perp}][\mathbf{Q}, \mathbf{Q}^{\perp}]^{\dagger}\tilde{\mathbf{H}}_k) = N_j, \end{aligned}$$

where the equality (a) holds from $tr(\mathbf{AB}) = tr(\mathbf{BA})$. □

Lemma 2. *Any full rank precoding matrix at each jammer cannot change the jamming subspace at Bob's receiver. For example, when the* k*th jammer uses an arbitrary precoding matrix* $\mathbf{U} \in \mathbb{C}^{N_j \times N_j}$ *of rank* N_j*, it is satisfied that* $\mathrm{span}(\mathbf{H}_k) = \mathrm{span}(\mathbf{H}_k\mathbf{U}) = \mathsf{H}_k$.

Proof. Since both $\mathbf{H}_k$ and $\mathbf{U}$ are the matrices of rank N_j, so is $\mathbf{H}_k\mathbf{U}$. Intuitively, the columns of $\mathbf{H}_k\mathbf{U}$ are linear combinations of the columns of $\mathbf{H}_k$ so that they will span the same subspace. Formally, we can show $d_c^2(\mathbf{H}_k, \mathbf{H}_k\mathbf{U}) = 0$, but it is trivial. □

As stated in Lemma 2, each jamming channel forms an unique subspace invariant to any full rank precoding matrix. Since there are total S jammers, we have S jamming subspaces $\mathsf{H}_1, \ldots, \mathsf{H}_S$ such that $\{\mathsf{H}_1, \ldots, \mathsf{H}_S\} \subset \mathcal{G}_{N_r,N_j}(\mathbb{C})$. Note that each jamming subspace is isotropic in $\mathbb{C}^{N_r}$ and independent of each other because all jamming channels have the elements of i.i.d. complex Gaussian random variables. A graphical interpretation is given in Fig. 3. In Fig. 3, each point on the sphere surface is an N_j-dimensional subspace represented by its generator matrix, while the surface of the sphere is an N_r-dimensional space, i.e., $\mathbb{C}^{N_r}$, which is set of all N_j-dimensional subspaces. Since we should select K jammers among S jammers, we select K points out of S points (jamming subspaces) on the sphere.

B. Alignment Measure among K Jamming Subspaces

Now, our aim is to select K jammers whose jamming subspaces are most aligned in an $(N_r - N_t)$-dimensional subspace. For jammer selection, we define an *alignment measure* to quantify how well K jamming subspaces are aligned and find the relationship between the alignment measure and jammer group size (i.e., S). The alignment measure is based on the mini-max distance of the selected jamming subspaces from an $(N_r - N_t)$-dimensional subspace. For example, the alignment measure of the K subspaces formed by K jammers indexed from 1 to K, i.e., $\mathsf{H}_1, \ldots, \mathsf{H}_K$, is defined by

$$\mathfrak{q}(\mathsf{H}_1, \ldots, \mathsf{H}_K) \triangleq \min_{\mathsf{Q} \in \mathcal{G}_{N_r, N_r - N_t}(\mathbb{C})} \max_{k \in [K]} d_c(\mathsf{H}_k, \mathsf{Q}), \tag{9}$$

where $[K] = \{1, \ldots, K\}$. If $\mathfrak{q}(\mathsf{H}_1, \ldots, \mathsf{H}_K) = 0$, there exists $\mathsf{Q} \in \mathcal{G}_{N_r, N_r - N_t}(\mathbb{C})$ such that

$$d_c(\mathsf{H}_1, \mathsf{Q}) = d_c(\mathsf{H}_2, \mathsf{Q}) = \cdots = d_c(\mathsf{H}_K, \mathsf{Q}) = 0,$$

which means that the K jamming subspaces are perfectly aligned in an $(N_r - N_t)$-dimensional subspace. Otherwise, if $\mathfrak{q}(\mathsf{H}_1, \ldots, \mathsf{H}_K) = \delta$, there exist $\mathsf{Q} \in \mathcal{G}_{N_r, N_r - N_t}(\mathbb{C})$ such that

$$d_c(\mathsf{H}_k, \mathsf{Q}) \leq \delta \qquad \forall k \in [K],$$

which means the K subspaces are aligned in an $(N_r - N_t)$-dimensional subspace within distance δ. Since there are S jammers in our problem, we can select K jammers (i.e., jamming subspaces) with the smallest alignment measure among S jammers. Thus, the alignment measure for the selected jammers becomes

$$\min_{\{s'_1, \ldots, s'_K\} \subset [S]} \mathfrak{q}(\mathsf{H}_{s'_1}, \ldots, \mathsf{H}_{s'_K}).$$

As the number of jammers increases, we can select more-aligned jamming subspaces. Therefore, the question of interest is how small we can make the alignment measure of the K jamming subspaces by opportunistic jammer selection for a given number of total jammers S. To answer this question, we adopt subspace quantization theory [33]–[37].

Suppose that we quantize an arbitrary N_j-dimensional subspace into one of M $(N_r - N_t)$-dimensional subspaces. We define a subspace codebook $\mathcal{Q} \triangleq \{\mathsf{Q}_1, \ldots, \mathsf{Q}_M\}$ comprised of M $(N_r - N_t)$-dimensional

subspaces such that $|\mathcal{Q}| = M$ and $\mathcal{Q} \subset \mathcal{G}_{N_r,N_r-N_t}(\mathbb{C})$. For the mth subspace (or codeword), i.e., Q_m, we define a metric ball with radius δ:

$$B(\mathsf{Q}_m, \delta) \triangleq \{\mathsf{P} \in \mathcal{G}_{N_r,N_j}(\mathbb{C}) : d_c(\mathsf{Q}_m, \mathsf{P}) \leq \delta\},$$

as a set of N_j-dimensional subspaces within a distance δ from the $(N_r - N_j)$-dimensional subspace Q_m.

Generally, the performance of a codebook is measured by two important parameters – the *packing radius* and the *covering radius*. The packing radius of $\mathcal{Q}$ denoted by $\delta_p(\mathcal{Q})$ is the maximum radius of each metric ball which is non-overlapped such that [33]–[35]

$$\delta_p(\mathcal{Q}) \triangleq \max\{\delta : B(\mathsf{Q}_i, \delta) \cap B(\mathsf{Q}_j, \delta) = \emptyset \quad \forall i \neq j\}.$$

The covering radius of $\mathcal{Q}$ denoted by $\delta_c(\mathcal{Q})$ is the minimum radius of the metric ball covering whole space such that [36], [37]

$$\delta_c(\mathcal{Q}) \triangleq \min\{\delta : B(\mathsf{Q}_1, \delta) \cup \cdots \cup B(\mathsf{Q}_M, \delta) = \mathbb{C}^{N_r}\}. \tag{10}$$

A graphical representation of the packing and the covering radii of a codebook are given in Fig. 4(a) and Fig. 4(b), respectively. Obviously, the covering radius is always larger than or equal to the packing radius, i.e., $\delta_p(\mathcal{Q}) \leq \delta_c(\mathcal{Q})$. Since the union of M metric balls with the covering radius $\delta_c(\mathcal{Q})$ is $\mathbb{C}^{N_r}$, any jamming subspace will be contained at least one of the M metric balls with the covering radius. This fact leads to Remark 1.

Remark 1 (Pigeon hole principle)**.** *When there are $S = (K-1)M + 1$ jamming subspaces, at least K subspaces are contained in the same metric ball among $B(\mathsf{Q}_1, \delta_c(\mathcal{Q})), \ldots, B(\mathsf{Q}_M, \delta_c(\mathcal{Q}))$. The illustration is given in Fig. 5.*

Now, we consider two optimal codebooks of size M; one maximizes the packing radius, and the other minimizes the covering radius. Although the optimal codebooks are not unique, the maximum packing radius and the minimum covering radius will be uniquely determined for given codebook size. With a slight abuse of notation, we denote the maximum packing radius and the minimum covering radius

obtained from the codebooks of size M by $\delta_p^\star(M)$ and $\delta_c^\star(M)$, respectively, such that

$$\delta_p^\star(M) = \max_{\substack{\mathcal{Q}\subset\mathcal{G}_{N_r,N_r-N_t}(\mathbb{C}) \\ |\mathcal{Q}|=M}} \delta_p(\mathcal{Q})$$

$$\delta_c^\star(M) = \min_{\substack{\mathcal{Q}\subset\mathcal{G}_{N_r,N_r-N_t}(\mathbb{C}) \\ |\mathcal{Q}|=M}} \delta_c(\mathcal{Q}).$$

Unfortunately, however, the exact values of the optimal packing and covering radii are unknown because finding them are NP-hard problems. Instead, the optimal packing radius $\delta_p^\star(M)$ is shown to be [33]

$$\kappa_1 M^{-\frac{1}{N_t N_j}}(1+o(1)) \le \delta_p^\star(M) \le \kappa_2 M^{-\frac{1}{N_t N_j}}(1+o(1)), \tag{11}$$

where κ_1 and κ_2 are constants invariant to M (see [33] for details).[2] It is also shown that the main terms of both upper and lower bounds are quite accurate estimates of the optimal packing radius when M is sufficiently large.

Obviously, the optimal covering radius is larger than the optimal packing radius. It can be easily proved by contradiction that the optimal covering radius is smaller than the twice of the optimal packing radius. So we can establish the following relationship:

$$\delta_p^\star(M) \le \delta_c^\star(M) \le 2\delta_p^\star(M). \tag{12}$$

From (11) and (12), we obtain the range of the optimal covering radius in Remark 2.

Remark 2. *Using codebook of size M, the optimal covering radius satisfies that*

$$\kappa_1 M^{-\frac{1}{N_t N_j}}(1+o(1)) \le \delta_c^\star(M) \le 2\kappa_2 M^{-\frac{1}{N_t N_j}}(1+o(1)).$$

When the codebook size is sufficiently large (i.e., when M is sufficiently large), the optimal covering radius is scaled by the codebook size M such that

$$\delta_c^\star(M) \propto M^{-\frac{1}{N_t N_j}}.$$

The optimal covering radius is closely related to our problem. As stated in Remark 1, if there are $S=(K-1)M+1$ jammers, we can ensure that there exist K jamming channels aligned in an (N_r-N_t)-dimensional subspace within distance $\delta_c^\star(M)$. Therefore, we establish the following key lemma.

[2] $f(n)=o(g(n))$ means that $f(n)\le cg(n)$ for any $c>0$ when n is sufficiently large.

Lemma 3. *When there are $S = (K-1)M+1$ jammers, we can always pick K jammers whose alignment measure is smaller than $2\kappa_2 M^{-\frac{1}{N_t N_j}}(1+o(1))$, i.e.,*

$$\min_{\{s'_1,\ldots,s'_K\}\subset[S]} \mathfrak{q}(\mathsf{H}_{s'_1},\ldots,\mathsf{H}_{s'_K}) \leq 2\kappa_2 M^{-\frac{1}{N_t N_j}}(1+o(1)),$$

where κ_2 are constants invariant to M, and the term $(1+o(1))$ can be ignored for large M.

Proof. Let $\mathcal{Q}_c^\star = \{\mathsf{Q}_1^\star,\ldots,\mathsf{Q}_M^\star\}$ be the codebook that minimizes the covering radius, and consider M metric balls $B(\mathsf{Q}_1^\star,\delta_c^\star(M)),\ldots,B(\mathsf{Q}_M^\star,\delta_c^\star(M))$. By the definition, the union of the metric balls becomes $\mathbb{C}^{N_r}$. As stated in Remark 1, when there are $S=(K-1)M+1$ jammers, we can always pick K jamming subspaces in the same metric ball. Let $\mathsf{H}_{(1)},\ldots,\mathsf{H}_{(K)}$ be the K jamming subspaces in the same metric ball, and $\mathsf{Q}_m^\star$ be the center of the metric ball. Then, we obtain

$$\begin{aligned}
\min_{\{s'_1,\ldots,s'_K\}\subset[S]} \mathfrak{q}(\mathsf{H}_{s'_1},\ldots,\mathsf{H}_{s'_K}) &\leq \mathfrak{q}(\mathsf{H}_{(1)},\ldots,\mathsf{H}_{(K)}) \\
&\overset{(a)}{\leq} \max_{k\in[K]} d_c(\mathsf{H}_{(k)},\mathsf{Q}_m^\star) \\
&\overset{(b)}{\leq} \delta_c^\star(M) \\
&\overset{(c)}{\leq} 2\kappa_2 M^{-\frac{1}{N_t N_j}}(1+o(1)),
\end{aligned}$$

where the inequality (a) is from the definition of the alignment measure given in (9), and the inequality (b) holds because $\mathsf{H}_{(k)} \in B(\mathsf{Q}_m^\star,\delta_c^\star(M))$ for all $k\in[K]$. Also, the inequality (c) holds from Remark 2.

□

V. Opportunistic Jammer Selection for Secure DoF

We recall the secure DoF of Bob given in (6):

$$\text{Secure DoF} = N_t - \lim_{P\to\infty} \frac{\mathcal{R}_{\text{Bob}}^-}{\log_2 P}. \tag{13}$$

We need an appropriate jammer selection scheme to reduce the DoF loss from the jamming signals. In this section, we propose two opportunistic jammer selection schemes. Firstly, we find the minimum DoF loss jammer selection scheme to achieve the maximum secure DoF. Then, we propose the subspace-based jammer selection scheme.

A. Minimum DoF Loss Jammer Selection Scheme (OJS1)

In the minimum DoF loss jammer selection scheme, Bob directly minimizes the rate loss from the jamming signals, i.e., $\mathcal{R}_{\text{Bob}}^{-}$ in (13). Correspondingly, the DoF loss is minimized. The rate loss from the minimum DoF loss jammer selection at Bob denoted by $\mathcal{R}_{\text{Bob}}^{-(1)}$ is given by

$$\begin{aligned}\mathcal{R}_{\text{Bob}}^{-(1)} &= \mathbb{E}\left[\min_{s_1',\ldots,s_K',\mathbf{V}} \log_2 \left|\mathbf{I}_{N_t} + \frac{P}{N_j}\mathbf{V}^\dagger\left(\sum_{k=1}^{K}\mathbf{H}_{s_k'}\mathbf{H}_{s_k'}^\dagger\right)\mathbf{V}\right|\right] \\ &\overset{(a)}{=} \mathbb{E}\left[\min_{s_1',\ldots,s_K'} \log_2 \prod_{n=N_r-N_t+1}^{N_r}\left[1+\frac{P}{N_j}\lambda_n\left(\sum_{k=1}^{K}\mathbf{H}_{s_k'}\mathbf{H}_{s_k'}^\dagger\right)\right]\right], \end{aligned} \tag{14}$$

where the equality (a) is obtained using the postprocessing matrix

$$\mathbf{V} = \left[\mathbf{v}_{N_r-N_t+1}(\mathbf{A}), \ldots, \mathbf{v}_{N_r}(\mathbf{A})\right],$$

where $\mathbf{A} = \sum_{k=1}^{K}\mathbf{H}_{s_k'}\mathbf{H}_{s_k'}^\dagger$, and $\lambda_n(\cdot)$ and $\mathbf{v}_n(\cdot)$ are the nth largest eigenvalue and corresponding eigenvector of the matrix, respectively. Thus, the selected jammers at Bob become

$$(s_1,\ldots,s_K) = \arg\min_{s_1',\ldots,s_K'} \prod_{n=N_r-N_t+1}^{N_r}\left[1+\frac{P}{N_j}\lambda_n\left(\sum_{k=1}^{K}\mathbf{H}_{s_k'}\mathbf{H}_{s_k'}^\dagger\right)\right].$$

B. Subspace-based Jammer Selection Scheme (OJS2)

In this subsection, we propose the suboptimal jammer selection scheme using the jamming subspaces. First of all, we find an upper bound of the minimum rate loss of Bob, i.e., (14), given by

$$\begin{aligned}\mathcal{R}_{\text{Bob}}^{-(1)} &= \mathbb{E}_{\tilde{\mathbf{H}},\mathbf{\Lambda}}\left[\min_{s_1',\ldots,s_K',\mathbf{V}} \log_2 \left|\mathbf{I}_{N_t} + \frac{P}{N_j}\sum_{k=1}^{K}\mathbf{V}^\dagger\tilde{\mathbf{H}}_{s_k'}\mathbf{\Lambda}_{s_k'}\tilde{\mathbf{H}}_{s_k'}^\dagger\mathbf{V}\right|\right] \\ &\overset{(a)}{\leq} \mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s_1',\ldots,s_K',\mathbf{V}} \mathbb{E}_{\mathbf{\Lambda}}\log_2 \left|\mathbf{I}_{N_t} + \frac{P}{N_j}\sum_{k=1}^{K}\mathbf{V}^\dagger\tilde{\mathbf{H}}_{s_k'}\mathbf{\Lambda}_{s_k'}\tilde{\mathbf{H}}_{s_k'}^\dagger\mathbf{V}\right|\right] \\ &\overset{(b)}{\leq} \mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s_1',\ldots,s_K',\mathbf{V}} \log_2 \left|\mathbf{I}_{N_t} + \frac{P}{N_j}\sum_{k=1}^{K}\mathbf{V}^\dagger\tilde{\mathbf{H}}_{s_k'}\mathbb{E}_{\mathbf{\Lambda}}[\mathbf{\Lambda}_{s_k'}]\tilde{\mathbf{H}}_{s_k'}^\dagger\mathbf{V}\right|\right] \\ &= \mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s_1',\ldots,s_K',\mathbf{V}} \log_2 \left|\mathbf{I}_{N_t} + P\sum_{k=1}^{K}\mathbf{V}^\dagger\tilde{\mathbf{H}}_{s_k'}\tilde{\mathbf{H}}_{s_k'}^\dagger\mathbf{V}\right|\right], \end{aligned} \tag{15}$$

where $\tilde{\mathbf{H}} \in \mathbb{C}^{N_r\times N_j}$ and $\mathbf{\Lambda} \in \mathbb{R}^{N_j\times N_j}$ are obtained from $\mathbf{H} \in \mathbb{C}^{N_r\times N_j}$ by compact singular value decomposition of $\mathbf{H}\mathbf{H}^\dagger$ (i.e., $\mathbf{H}\mathbf{H}^\dagger = \tilde{\mathbf{H}}\mathbf{\Lambda}\tilde{\mathbf{H}}^\dagger$) where $\mathbf{\Lambda}$ is a diagonal matrix whose diagonal elements are the *unordered* non-zero eigenvalues of $\mathbf{H}\mathbf{H}^\dagger$. Then, $\tilde{\mathbf{H}}$ becomes the generator matrix of $\mathbf{H}$. Note that

the generator matrix $\tilde{\mathbf{H}}$ for the matrix $\mathbf{H}$ is not unique, but any generator matrix yields the same $\tilde{\mathbf{H}}\tilde{\mathbf{H}}^{\dagger}$. The inequality (a) is from the fact that the minimum of the averages is larger than the average of the minimums. The inequality (b) holds from Jensen's inequality and the independence between $\tilde{\mathbf{H}}$ and $\mathbf{\Lambda}$. Finally, we obtain (15) from the fact that $\mathbb{E}[\mathbf{\Lambda}_{s'_k}] = N_j \mathbf{I}_{N_j}$ [30].

In the subspace-based jammer selection scheme, we minimize the upper bound given in (15) denoted by $\mathcal{R}_{\text{Bob}}^{-(2)}$ instead of (14). We can rewrite $\mathcal{R}_{\text{Bob}}^{-(2)}$ as

$$\begin{aligned}\mathcal{R}_{\text{Bob}}^{-(2)} &\triangleq \mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s'_1,\ldots,s'_K,\mathbf{V}} \log_2 \left|\mathbf{I}_{N_t} + P\sum_{k=1}^{K} \mathbf{V}^{\dagger}\tilde{\mathbf{H}}_{s'_k}\tilde{\mathbf{H}}_{s'_k}^{\dagger}\mathbf{V}\right|\right] \\ &= \mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s'_1,\ldots,s'_K} \log_2 \prod_{n=N_r-N_t+1}^{N_r}\left[1 + P\lambda_n\left(\sum_{k=1}^{K}\tilde{\mathbf{H}}_{s'_k}\tilde{\mathbf{H}}_{s'_k}^{\dagger}\right)\right]\right] \end{aligned} \tag{16}$$

by applying $\mathbf{V} = [\mathbf{v}_{N_r-N_t+1}(\mathbf{B}), \ldots, \mathbf{v}_{N_r}(\mathbf{B})]$ in (15) where $\mathbf{B} = \sum_{k=1}^{K}\tilde{\mathbf{H}}_{s'_k}\tilde{\mathbf{H}}_{s'_k}^{\dagger}$. Thus, the selected jammers are given by

$$(s_1, \ldots, s_K) = \arg\min_{s'_1,\ldots,s'_K} \prod_{n=N_r-N_t+1}^{N_r}\left[1 + P\lambda_n\left(\sum_{k=1}^{K}\tilde{\mathbf{H}}_{s'_k}\tilde{\mathbf{H}}_{s'_k}^{\dagger}\right)\right].$$

OJS1 considers the channel matrix itself so that the jammer selection criterion involves the channel magnitude. As a result, OJS1 becomes the secure DoF optimal jammer selection scheme minimizing the Bob's DoF loss. On the other hand, OJS2 considers the subspace spanned by the channel matrix so that all channel matrices spanning the same subspace are considered identical regardless of the channel magnitude.

VI. Sufficient Jammer Scaling for Target Secure DoF

In this section, we find a sufficient jammer scaling law for a target secure DoF. In previous section, we proposed two jammer selection schemes which obtain the minimum rate loss $\mathcal{R}_{\text{Bob}}^{-(1)}$ and its upper bound $\mathcal{R}_{\text{Bob}}^{-(2)}$, respectively. From (6), the target secure DoF $d \in (0, N_t]$ is obtained in both schemes when

$$\lim_{P\to\infty}\frac{\mathcal{R}_{\text{Bob}}^{-(1)}}{\log_2 P} = \lim_{P\to\infty}\frac{\mathcal{R}_{\text{Bob}}^{-(2)}}{\log_2 P} = N_t - d.$$

Since it is hard to directly find the required jammer scaling for the target secure DoF, we will find $\mathcal{R}_{\text{Bob}}^{-(3)}$ as a further upper bound of $\mathcal{R}_{\text{Bob}}^{-(1)}$ and find the sufficient jammer scaling law for the target secure DoF

d. This scaling ensures that

$$\lim_{P\to\infty}\frac{\mathcal{R}_{\text{Bob}}^{-(1)}}{\log_2 P}\leq\lim_{P\to\infty}\frac{\mathcal{R}_{\text{Bob}}^{-(2)}}{\log_2 P}\leq\lim_{P\to\infty}\frac{\mathcal{R}_{\text{Bob}}^{-(3)}}{\log_2 P}=N_t-d. \tag{17}$$

The term $\mathcal{R}_{\text{Bob}}^{-(2)}$ given in (16) is upper bounded as follows

$$\begin{aligned}
\mathcal{R}_{\text{Bob}}^{-(2)} &= \mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s'_1,\ldots,s'_K,\mathbf{V}}\log_2\left|\mathbf{I}_{N_t}+P\sum_{k=1}^{K}\mathbf{V}^\dagger\tilde{\mathbf{H}}_{s'_k}\tilde{\mathbf{H}}_{s'_k}^\dagger\mathbf{V}\right|\right]\\
&\overset{(a)}{\leq}\mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s'_1,\ldots,s'_K,\mathbf{V}}N_t\log_2\left(1+\frac{P}{N_t}\sum_{k=1}^{K}tr\big(\mathbf{V}^\dagger\tilde{\mathbf{H}}_{s'_k}\tilde{\mathbf{H}}_{s'_k}^\dagger\mathbf{V}\big)\right)\right]\\
&\overset{(b)}{=}\mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{\substack{s'_1,\ldots,s'_K,\\ \mathsf{V}\in\mathcal{G}_{N_r,N_t}(\mathbb{C})}}N_t\log_2\left(1+\frac{P}{N_t}\sum_{k=1}^{K}d_c^2(\mathsf{H}_{s'_k},\mathsf{V}^\perp)\right)\right]\\
&\overset{(c)}{\leq}\mathbb{E}_{\tilde{\mathbf{H}}}\left[\min_{s'_1,\ldots,s'_K}N_t\log_2\left(1+\frac{P}{N_t}K\left[\mathfrak{q}(\mathsf{H}_{s'_1},\ldots,\mathsf{H}_{s'_K})\right]^2\right)\right]\\
&\overset{(d)}{\leq}N_t\log_2\left(1+\frac{4\kappa_2^2KP}{N_t}\left\lfloor\frac{S-1}{K-1}\right\rfloor^{-\frac{2}{N_tN_j}}\right)+o(1),
\end{aligned} \tag{18}$$

where $\mathsf{V}\in\mathcal{G}_{N_r,N_t}(\mathbb{C})$ is the subspace formed by the postprocessing matrix $\mathbf{V}$, and $\mathsf{V}^\perp\in\mathcal{G}_{N_r,N_r-N_t}(\mathbb{C})$ is the orthogonal complement subspace of V. In the above equations, the inequality (a) is from Jensen's inequality such that $\log(\alpha\beta)\leq 2\log[(\alpha+\beta)/2]$, and the equality (b) holds from Lemma 1. The inequality (c) holds because selecting the subspace V is equivalent to selecting the subspace $\mathsf{V}^\perp$, and it is satisfied that

$$\min_{\mathsf{V}^\perp\in\mathcal{G}_{N_r,N_r-N_t}(\mathbb{C})}\sum_{k=1}^{K}d_c^2(\mathsf{H}_{s'_k},\mathsf{V}^\perp)\leq K\left[\mathfrak{q}(\mathsf{H}_{s'_1},\ldots,\mathsf{H}_{s'_K})\right]^2$$

from the definition of the alignment measure given in (9). Also, the inequality (d) is from Lemma 3 by substituting $M=\lfloor(S-1)/(K-1)\rfloor$. We define (18) as $\mathcal{R}_{\text{Bob}}^{-(3)}$, i.e.,

$$\mathcal{R}_{\text{Bob}}^{-(3)}\triangleq N_t\log_2\left(1+\frac{4\kappa_2^2PK}{N_t}\left\lfloor\frac{S-1}{K-1}\right\rfloor^{-\frac{2}{N_tN_j}}\right).$$

Theorem 1. *The sufficient number of jammers to ensure Bob's rate loss smaller than Δ is given by*

$$S=(K-1)\left[\frac{4\kappa_2^2KP}{N_t\left(2^{\Delta/N_t}-1\right)}\right]^{\frac{N_tN_j}{2}}+1. \tag{19}$$

Proof. If $\mathcal{R}_{\text{Bob}}^{-(3)}=\Delta$, Bob can have rate loss smaller than Δ. By solving $\mathcal{R}_{\text{Bob}}^{-(3)}=\Delta$, we obtain (19). □

Theorem 2. *The target secure DoF of $d \in (0, N_t]$ is achieved when the number of jammers is scaled as $S \propto P^{dN_j/2}$.*

Proof. As stated in (17), the target DoF of d is achieved when $\lim_{P\to\infty} \left(\mathcal{R}_{\text{Bob}}^{-(3)} / \log_2 P\right) = N_t - d$, equivalently,

$$\lim_{P\to\infty} N_t \log_2 \left(1 + \frac{4\kappa_2^2 KP}{N_t} \left\lfloor \frac{S-1}{K-1} \right\rfloor^{-\frac{2}{N_t N_j}}\right) = \log_2 P^{N_t - d}.$$

This condition holds when $S \propto P^{dN_j/2}$. □

Interestingly, the scaling law of the required jammers in Theorem 2 is affected by neither the number of selected jammers K nor the number of receive antennas N_r (but, necessarily, $N_t + N_j \leq N_r < N_t + KN_j$).

Remark 3. *Theorem 2 implies that using single-antenna jammers is more efficient in terms of the minimum required jammer scaling than using multi-antenna jammers for target secure DoF. That is, $S \propto P^{dN_j/2}$ is minimized when $N_j = 1$.*

As shown in Theorem 1, the required number of jammers increases with the number of the selected jammers to achieve a given rate loss; if the number of selected jammers increases from K to $K+1$, the number of required jammers to maintain Bob's rate loss smaller than Δ increases from S to

$$\frac{K}{K-1}\left(\frac{K+1}{K}\right)^{\frac{N_t N_j}{2}} S$$

which becomes S when K is sufficiently large. However, it does not change the scaling law for the given target secure DoF as shown in Theorem 2 because the secure DoF is defined for the asymptotic case that $P \to \infty$.

More receive antennas are likely to be beneficial for jamming signal alignment because a larger number of receive antennas increase the subspace dimensions where the jamming signals (or jamming subspaces) should be aligned, i.e., $N_r - N_t$. However, a larger number of receive antennas also increase signal space of each jamming signal, i.e., N_r, and thus make it harder to align all jamming signals together. This counter-effect cancels the benefit of increased subspace dimensions for jamming signal alignment and makes the scaling law independent of the number of receive antennas. For example, suppose that

we can increase Bob's receive antennas N_r to $N_r + 1$ while maintaining the antenna configuration of $N_t + N_j \leq N_r + 1 < N_t + KN_j$. Although we have increased dimensions $(N_r + 1 - N_t)$ for jamming subspace alignment, each jamming subspace becomes N_j-dimensional subspaces in $\mathbb{C}^{N_r+1}$. The alignment of N_j-dimensional subspaces in $\mathbb{C}^{N_r+1}$ is much more difficult than the alignment of N_j-dimensional subspaces in $\mathbb{C}^{N_r}$. The scaling law of the required number of jammers is unchanged due to this difficulty in spite of the increased dimensions for jamming subspace alignment. These results and insights are generalized by the following theorem.

Theorem 3. *Any wireless communication system can achieve the secure DoF of $d \in (0, N_t]$ via opportunistic jammer selection with a jammer scaling law $S \propto P^{d/2}$. In this case, each jammer should have a single antenna, and $(N_t + 1)$ antennas are enough for Bob's receiver. We can increase the defensible dimensions of the system as many as we want by increasing K to make the achievable DoF of Bob directly become the secure DoF.*

A. OJS with the Partial CSI

In this subsection, we show that Theorem 2 and Theorem 3 are still valid with secrecy outage probability ϵ for practical partial CSI scenarios that CSI for Eve's channel is not known to Alice. Since Eve's CSI is hard to know even when Eve's presence is known, many schemes that work in the absence of Eve's CSI have been proposed [8], [31], [32]. The authors in [8] proposed relay chatting for half-duplexing two-hop amplify-and-forward (AF) relay communication systems. In the relay chatting scheme, the best relay forwards the received signal and the other relays send jamming signals over the null space of the desired channel via distributed beamforming at each stage. Compared to the relay chatting scheme, each jammer in our proposed scheme simply transmits an i.i.d. Gaussian signal; the selected jammers do not require any CSI or joint transmission. Moreover, we consider the defensible dimension to prevent Eve's eavesdropping in multiple antenna configurations.

In Section III-B, we showed that the jamming signals make Eve's DoF zero for each channel realization.

In this case, Eve's channel capacity given in (2) is saturated to

$$\lim_{P\to\infty} \mathcal{C}_{\text{Eve}} = \log_2 \left| \mathbf{I}_{N_e} + \frac{N_j}{N_t} \mathbf{G}_0 \mathbf{G}_0^\dagger \left(\sum_{k=1}^{K} \mathbf{G}_{s_k} \mathbf{G}_{s_k}^\dagger \right)^{-1} \right|. \tag{20}$$

Since the selected jammers are random to Eve, the distribution of $\lim_{P\to\infty} \mathcal{C}_{\text{Eve}}$ will be identical with that of a random variable R defined by

$$R \triangleq \log_2 \left| \mathbf{I}_{N_e} + \frac{N_j}{N_t} \mathbf{G}_0 \mathbf{G}_0^\dagger \left(\sum_{k=1}^{K} \mathbf{G}_k \mathbf{G}_k^\dagger \right)^{-1} \right|, \tag{21}$$

which can be numerically found. We can choose a constant rate r to yield

$$\Pr[R \geq r] = \epsilon, \tag{22}$$

where $\epsilon \in [0, 1]$. Then, using Wyner's encoding scheme with two rates $(\mathcal{R}_{\text{Bob}}, r)$ instead of $(\mathcal{R}_{\text{Bob}}, \mathcal{C}_{\text{Eve}})$, Bob can achieve the secure DoF

$$\mathbb{E}\left\{ \lim_{P\to\infty} \frac{[\mathcal{R}_{\text{Bob}} - r]^+}{\log_2 P} \right\} = \mathbb{E}\left\{ \lim_{P\to\infty} \frac{\mathcal{R}_{\text{Bob}}}{\log_2 P} \right\}$$

with secrecy outage probability ϵ, which is the same as the achievable secure DoF with the knowledge of $\mathcal{C}_{\text{Eve}}$.

Obviously, in (22), the smaller ϵ requires the larger r, but it is independent of P. Therefore, we can almost surely obtain the same target secure DoF by choosing sufficiently large r which makes $\epsilon \approx 0$. Note that this result comes from the independency between the jamming signals and Eve's CSI.

VII. Numerical Results

In this section, we evaluate our proposed opportunistic jammer selection schemes. Fig. 6 shows that Bob can increase the achievable rate via jammer selection while maintaining the same average capacity of Eve's channel. The numbers of antennas at Alice, Bob, jammers, and Eve are assumed by $(N_t, N_j, N_r, N_e) = (2, 2, 4, 4)$, respectively, and Bob selects two jammers (i.e., $K = 2$) in the jammer group. In this case, the number of Eve's receive antennas does not exceed the defensible dimensions, i.e., $N_e \leq KN_j$, so that Eve obtains zero DoF. We also consider the capacity maximizing jammer selection scheme at Bob for

comparison. As shown in Fig. 6, the channel capacities of both Bob and Eve are saturated in the high SNR region because the number of jammers is finite. However, at a fixed SNR, the achievable rate of Bob increases with the number of candidate jammers, while Eve's channel capacity remains unchanged. The gap between the capacities of Bob and Eve increases with the number of candidate jammers, and results in the secure DoF of N_t when $S \to \infty$. As the number of jammers increases, Bob can reduce the negative effects of the jamming signals, and the channel capacity with jammers by the capacity maximizing jammer selection will go to that without jamming signals. Since Eve's capacity with jammers is saturated in the high SNR region, Bob can obtain the secure DoF without Eve's CSI as described in Section VI-A. In the case that $(N_t, N_j, N_r, N_e) = (2, 2, 4, 4)$ and $K = 2$, Fig. 7 shows the secrecy outage probability (i.e., ϵ) when the Eve's achievable rate is treated as a constant (i.e., r). This figure shows that the secrecy outage probability decreases if the constant rate of Eve increases.

The achievable secrecy rates are plotted in Fig. 8 when Bob selects two jammers in the jammer group with a scaled number of jammers. The number of antennas at each node is $(N_t, N_j, N_r, N_e) = (1, 2, 3, 3)$. In this case, the number of defensible dimensions of the security system is $KN_j = 4$ and hence the Eve's DoF becomes zero. In Fig. 8, we consider the optimal jammer selection scheme at Alice with global CSI to maximize the secrecy rate, while in our proposed jammer selection scheme Bob selects jammers with only its own CSI. As a referential upper bound, we also consider the scheme of [27, p.189]. In the referential scheme, Alice with $(N_t + KN_j)$ antennas steers beams with perfect CSIT and sends artificial noise along with information-bearing messages without any help of jammers. On the other hand, Bob and Eve have N_r and N_e antennas, respectively, as in our system model. As shown in Theorem 2, Bob can obtain DoF of one when the number of jammers is scaled by $S \propto P^{dN_j/2} = P$. We consider two jammer scalings $S = P$ and $S = 0.3P$. In both cases, Bob obtains DoF of one which directly becomes secure DoF. In Fig. 9, we consider two scenarios $S = P$ and $S = P^{0.5}$ in the same configuration. As predicted in Theorem 2, Bob obtains secure DoF of one and a half when $S = P$ and $S = P^{0.5}$, respectively. Note that the referential scheme [27, p.189] obtains much higher secrecy rate because Alice not only has more

transmit antennas (i.e., $N_t + KN_j$ antennas) but also exploits perfect CSIT.

In Fig. 10, we consider the antenna configuration $(N_t, N_j, N_r, N_e) = (2, 1, 3, 2)$ and plot the achievable secrecy rates when Bob selects two jammers in the jammer group with a scaled numbers of jammers $S \propto P$ and $S \propto P^{0.5}$, respectively. As predicted in Theorem 2, Bob obtains secure DoF two and one when $S = P$ and $S = P^{0.5}$, respectively.

VIII. Conclusions

In this paper, we proposed the opportunistic jammer selection schemes to achieve the secure DoF in a secure communication system aided by jammers. For the opportunistic jammer selection, we proposed two selection criteria – the minimum DoF loss jammer selection and the subspace-based jammer selection. We proved that the secure DoF can be obtained by aligning jamming signals in a small dimensional subspace at Bob's receiver through the opportunistic jammer selection. From the geometric interpretation, we found the required jammer scaling laws to obtain target secure DoF at Bob's receiver.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, pp. 339–348, May 1978.

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

[5] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commnun. Lett.*, vol. 14, no. 10, pp. 885–887, Oct. 2010.

[6] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung, "Multi-user diversity for secrecy in wireless networks," *Information Theory and Applications Workshop*, 2009.

[7] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," in *Proc. IEEE International Conference on Communications*, Kyoto, Japan, June, 2011.

[8] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, June 2011.

[9] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," in *Proc. 46th Annual Allerton Conference on Communication, Control and Computing*, Sep. 2008.

[10] O. O. Koyluoglu, H. El Gamal, L. Lifeng, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proc. International Symposium on Information Theory*, pp. 384-388, July 2008.

[11] O. O. Koyluoglu, H. El Gamal, L. Lifeng, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Info. Theory*, vol. 57, no. 6, pp. 3323–3332, June 2011.

[12] S. A. Jafar and S. Shamai, "Degrees of freedom region for the MIMO X channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 151–170, Jan. 2008.

[13] V. R. Cadambe and S. A. Jafar, "Interference alignment and the degrees of freedom for the K user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[14] P. Viswanath, D. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1277–1294, June 2002.

[15] Q. Zhou and H. Dai, "Asymptotic analysis on the interaction between spatial diversity and multiuser diversity in wireless networks," *IEEE Trans. Sig. Proc.*, vol. 55, no. 8, pp. 4271–4283, Aug. 2007.

[16] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 506–522, Feb. 2005.

[17] Y. Huang and B. Rao, "Random beamforming with heterogeneous users and selective feedback: individual sum rate and individual scaling laws," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2080–2090, May 2013.

[18] J.-P. Hong and W. Choi, "Throughput characteristics by multiuser diversity in a cognitive radio system," *IEEE Trans. Sig. Proc.*, vol. 59, no. 8, pp. 3749–3763, Aug. 2011.

[19] W. Choi and J. G. Andrews, "The capacity gainfrom intercell scheduling in multi-antenna systems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 2, pp. 714–725, Feb. 2008.

[20] J. H. Lee and W. Choi, "Opportunistic interference alignment by receiver selection in a K-user 1×3 SIMO interference channel," in *Proc. IEEE Global Telecommunications Conference*, Houston, TX, Dec. 2011.

[21] J. H. Lee and W. Choi, "On the achievable DoF and user scaling law of opportunistic interference alignment in 3-transmitter MIMO interference channels," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2743–2753, June 2013.

[22] J. H. Lee, W. Choi, and B. D. Rao, "Multiuser diversity in interfering broadcast channels: achievable degrees of freedom and user scaling law," to appear, *IEEE Trans. Wireless Commun.*

[23] X. He and A. Yener, "Providing secrecy with lattice codes," in *Proc. 46th Allerton Conf. on Commun., Contr., and Comput.*, Sep. 2008.

[24] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.

[25] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath, "Ergodic interference alignment," in *Proc. IEEE Symp. Inf. Theory*, pp. 1769–1773, June 2009.

[26] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. 50th Allerton Conf. on Commun., Contr., and Comput.*, Oct. 2012.

[27] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[28] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. and Trends in Commun. and Inf. Theory*, vol. 5, no. 4-5, pp. 355–580, 2008.

[29] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, and K. Życzkowski, "MUBs and hadamards of order six," *J. Math. Phys.* 48, 052106 (2007), arXiv:quant-ph/0610161

[30] N. Ravindran and N. Jindal, "Limited feedback-based block diagonalization for the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 8, pp. 1473–1482, Oct. 2008.

[31] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[32] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[33] W. Dai, Y. Liu, and B. Rider, "Quantization bounds on Grassmann manifolds and applications to MIMO communications," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1108–1123, Mar. 2008.

[34] A. Barg and D. Y. Nogin "Bounds on packings of spheres in the Grassmann manifold," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2450–2454, Sep. 2002.

[35] O. Henkel "Sphere-packing bounds in the Grassmann and Stiefel manifolds," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3445–3456, Oct. 2005.

[36] A. Ashikhmin, G. Cohen, M. Krivelevich, and S. Litsyn, "Bounds on distance distribution in codes of known size," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 259–264, Jan. 2005.

[37] B. Mondal and R. W. Heath, Jr., "A diversity guarantee and SNR performance for unitary limited feedback mimo systems," *EURASIP J. Applied Signal Processing*, vol. 8, Jan. 2008.

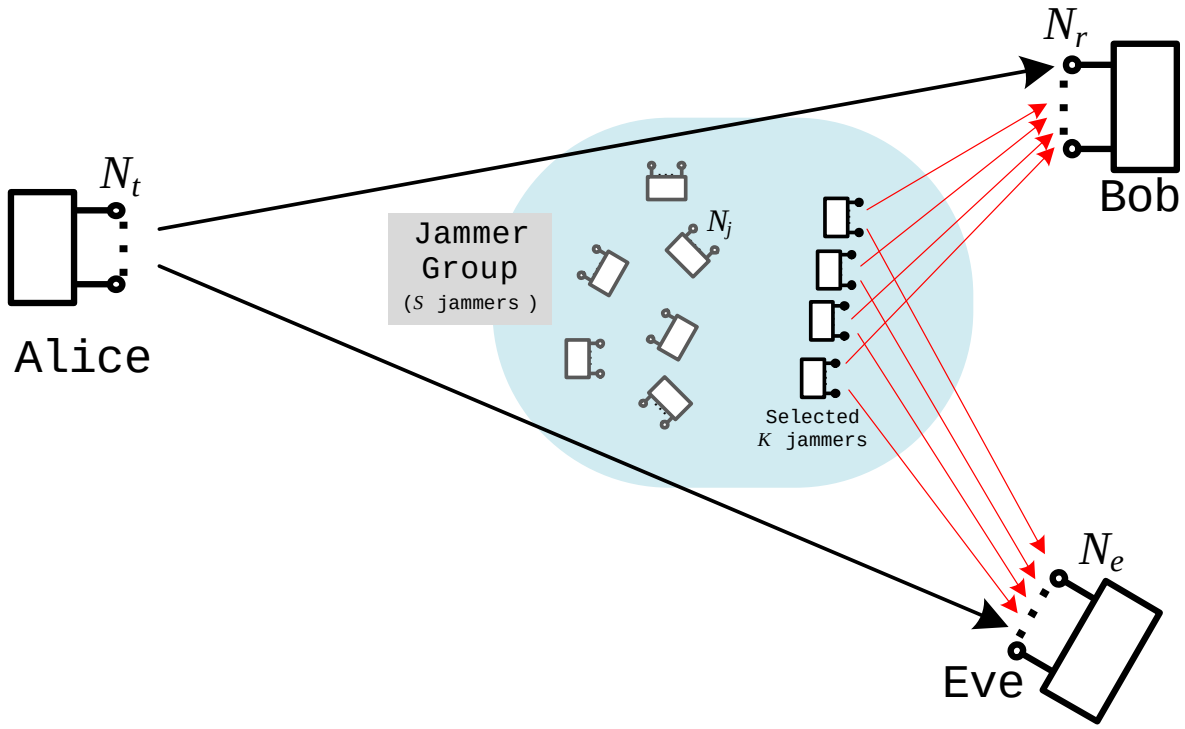


Fig. 1. System model.

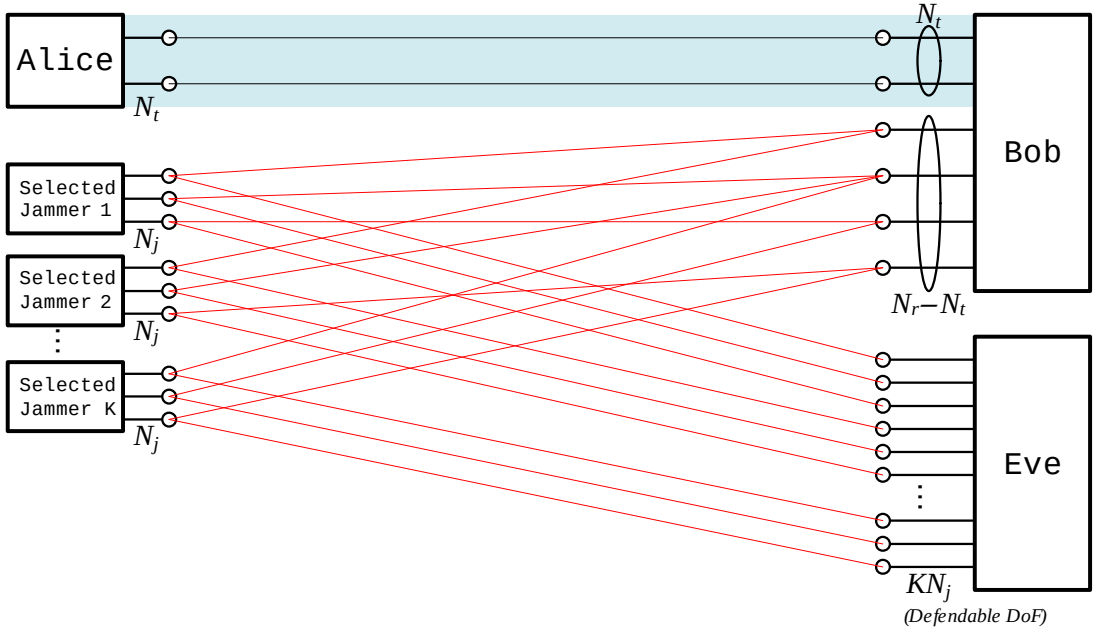


Fig. 2. The basic concept of opportunistic jammer selection. The jamming signals from the selected jammers are aligned at Bob but not at Eve.

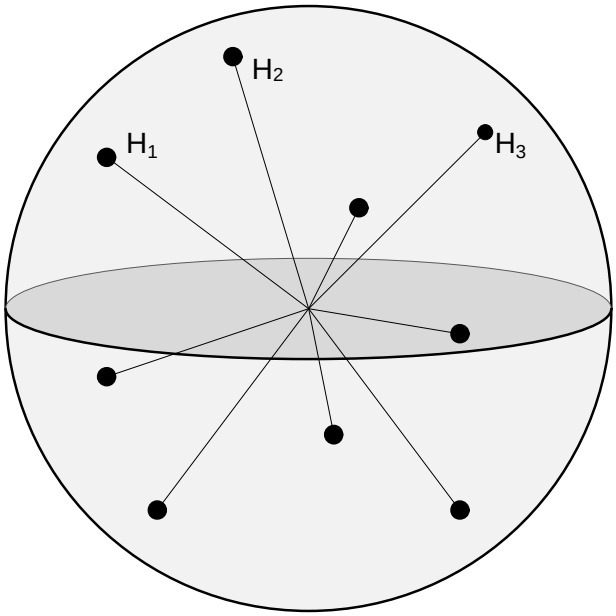
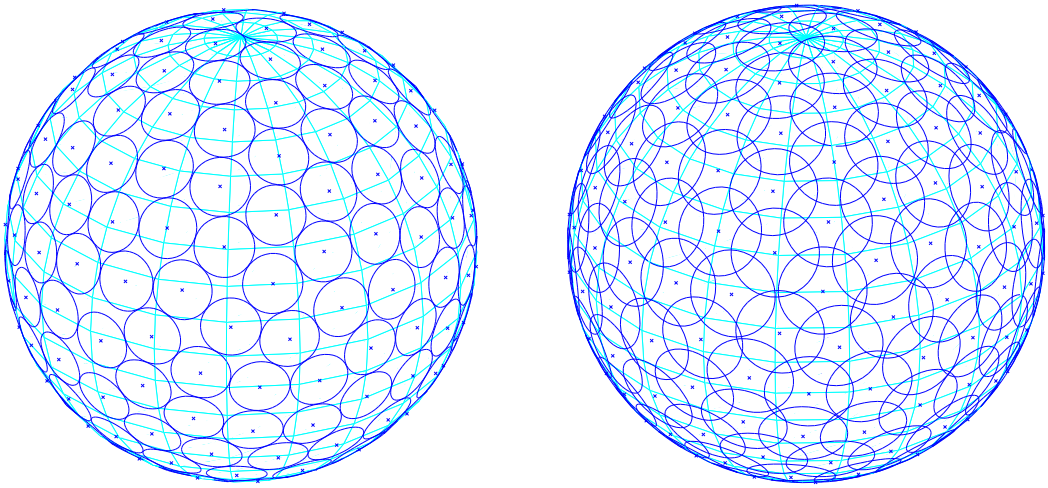


Fig. 3. There are total S points on the sphere. Each point represents the subspace formed by each jammer.



(a) Packing radius (b) Covering radius

Fig. 4. Graphical representation of the packing radius and the covering radius on the sphere. The metric balls at M points pack or cover the sphere.

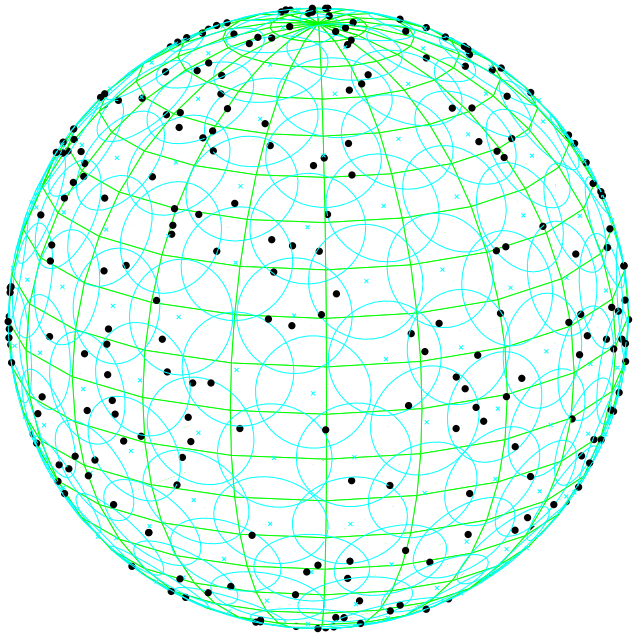


Fig. 5. There are $S = (K-1)M + 1$ jamming subspaces (points) and M metric balls covering the sphere. There exist a metric ball that contains K jamming subspaces.

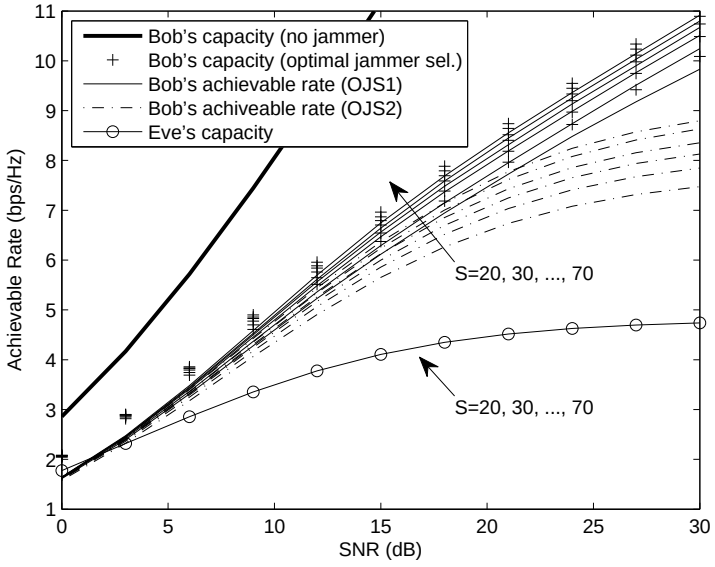


Fig. 6. Achievable rates of Bob when the number of jammers is fixed. $(N_t, N_j, N_r, N_e) = (2, 2, 4, 4)$ and $K = 2$.

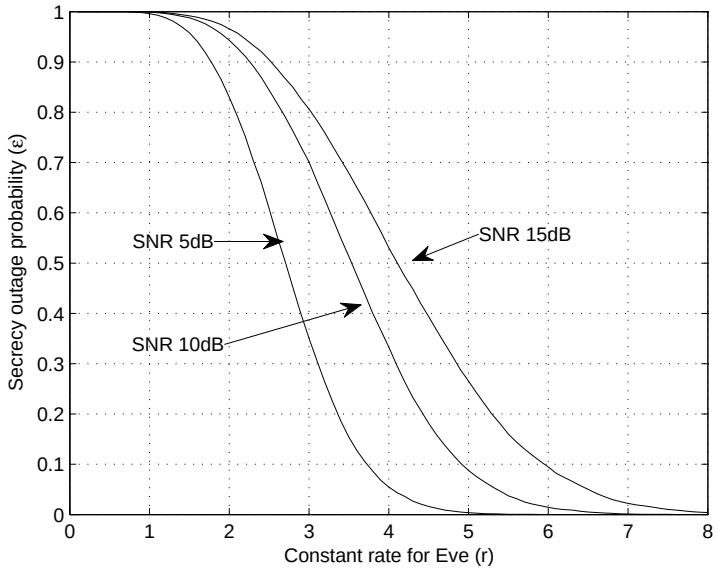


Fig. 7. Secrecy outage probability ϵ when the Eve's achievable rate is treated as a constant r. $(N_t, N_j, N_r, N_e) = (2, 2, 4, 4)$ and $K = 2$.

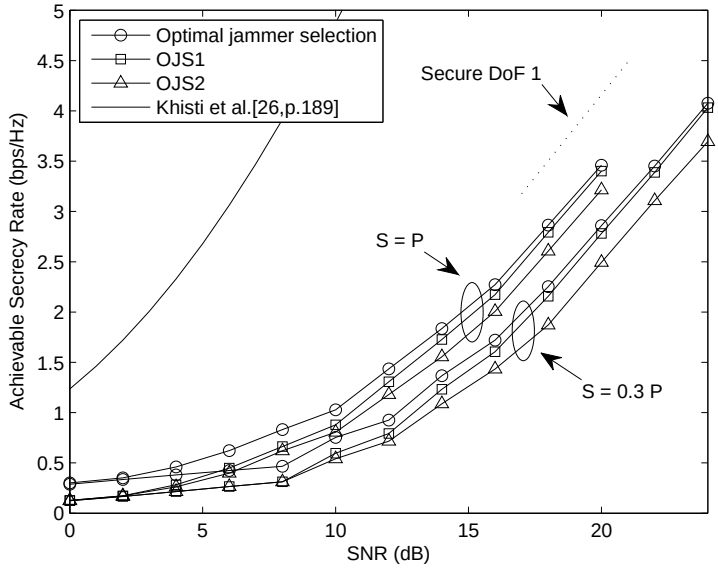


Fig. 8. The achievable secrecy rates for various jammer selection schemes when $(N_t, N_j, N_r, N_e) = (1, 2, 3, 3)$. Bob selects two jammers in the jammer groups of $S = P$ and $S = 0.3P$ jammers, respectively.

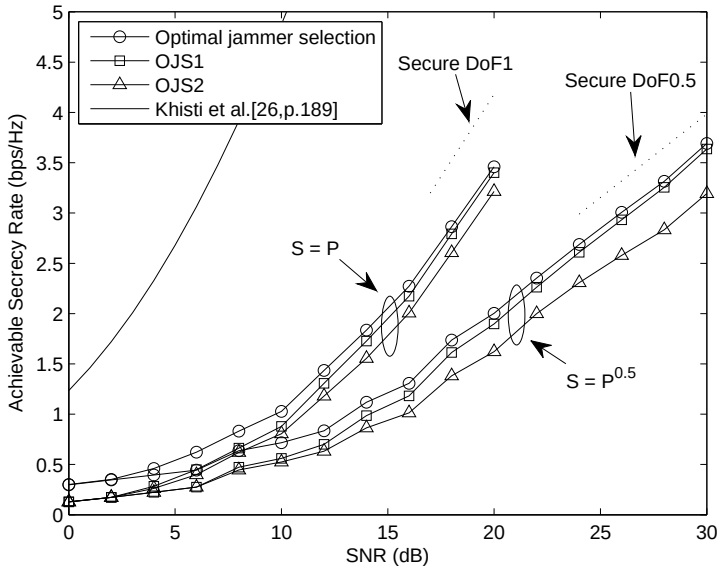


Fig. 9. The achievable secrecy rates for various jammer selection schemes when $(N_t, N_j, N_r, N_e) = (1, 2, 3, 3)$. Bob selects two jammers in the jammer groups of $S = P$ and $S = P^{0.5}$ jammers, respectively.

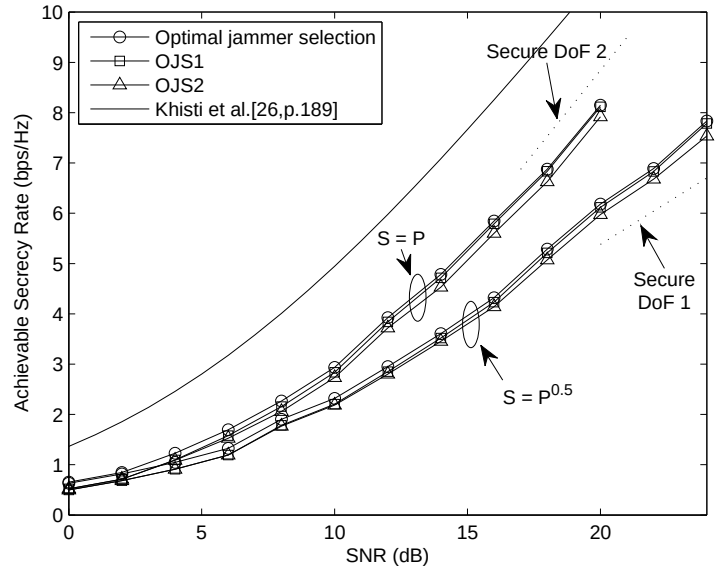


Fig. 10. The achievable secrecy rates for various jammer selection schemes when $(N_t, N_j, N_r, N_e) = (2, 1, 3, 2)$. Bob selects two jammers in the jammer groups of $S = P$ and $S = P^{0.5}$ jammers, respectively.