Secrecy Degrees of Freedom of Wireless X Networks Using Artificial Noise Alignment

Zhao Wang, Ming Xiao, Mikael Skoglund, and H. Vincent Poor

Abstract—The problem of transmitting confidential messages in $M \times K$ wireless X networks is considered, in which each transmitter intends to send one confidential message to every receiver. In particular, the secrecy degrees of freedom (SDOF) of the considered network achieved by an artificial noise alignment (ANA) approach, which integrates interference alignment and artificial noise transmission, are studied. At first, an SDOF upper bound is derived for the $M \times K$ X network with confidential messages (XNCM) to be $\frac{K(M-1)}{K+M-2}$. By proposing an ANA approach, it is shown that the SDOF upper bound is tight when either $K = 2$ or $M = 2$ for the considered XNCM with time/frequency varying channels. For $K, M \geq 3$, it is shown that an SDOF $\frac{K(M-1)}{K+M-1}$ can be achieved, even when an external eavesdropper appears. The key idea of the proposed scheme is to inject artificial noise to the network, which can be aligned in the interference space at receivers for confidentiality. Moreover, for the network with no channel state information at transmitters, a blind ANA scheme is proposed to achieve the SDOF $\frac{K(M-1)}{K+M-1}$ for $K, M \geq 2$, with reconfigurable antennas at receivers. The proposed method provides a linear approach to handle secrecy coding and interference alignment.

Index Terms—Secrecy degrees of freedom, artificial noise, interference alignment, wireless X network

I. INTRODUCTION

A. Background and Motivation

The notion of secrecy capacity was introduced by Wyner [1] in the context of wire-tap channel, in which a legitimate transmitter intends to send a confidential message to a legitimate receiver by hiding it from a degraded eavesdropper. Later the non-degraded wire-tap channel [2] and Gaussian wire-tap channel [3] were studied to generalize Wyner's work. In recent years, multi-user secret communications has attracted rising research attentions. For example, the interference channel and broadcast channel with secrecy constraints were studied in [4] and [5], the multiple access channels with secrecy constraints were investigated in [6] and [7], the relay-eavesdropper channel was studied in [8]. Usually the exact secrecy capacity region is difficult to find for most of multiuser networks. As a consequence, the secrecy degrees of freedom (SDOF) which serves as an approximation of the secrecy capacity in the high signal-to-noise ratio (SNR) regime has been widely investigated recently [9]–[13].

The secrecy capacity of the original wire-tap channel [1] is essentially the mutual information difference between the

legitimate user pair and transmitter-eavesdropper pair, which renders a vanishing SDOF in the high SNR regime. However, positive SDOF can be achieved for some other multiuser networks, e.g., the multiantenna compound wiretap channel [14], the interference channel [13], [15], the broadcast and multiple access channel with confidential messages [12] *et al.* These results reveal the fact that interference could have positive impact on the secrecy capacity of networks, because it naturally serves as jamming to conceal the messages from eavesdroppers. The assistance of interference in secure communication is well addressed in [16].

As a novel approach to handle interference in multiuser networks, interference alignment (IA) [17] provides advantages to limit the information leakage of confidential messages. Intuitively speaking, IA can pack the unintended messages to a reduced dimensional interference subspace at receivers, where the signals containing confidential messages are superimposed. Therefore, it naturally brings difficulty for the receiver when it tries to decode the information from the interference subspace. It is first noted in [15] that by combining IA and random binning [1], the SDOF $\frac{K(K-1)}{2(K-2)}$ can be achieved in the time/frequency varying K -user Gaussian interference channel. By adopting the Wyner random binning method to provide a secret codebook, IA has been generalized to different networks to obtain positive SDOF, e.g., the multiantenna compound wiretap channel [14], and the multiantenna wiretap channel with block fading channels [18]. The key idea of random binning is to provide randomness to the codebook, such that the eavesdropper is not able to tell the exact codeword from the randomized codebook. From a different transmission approach, artificial noise (AN) works in essentially the same way of providing randomness to the codebook. The AN can be chosen to be a Gaussian process. When the power of the AN is high enough to be comparable with the message power, it can provide enough randomness to confuse decoding. As studied in [12], [13], [19] and [20], the transmission of AN and IA can be integrated to achieve the optimal SDOF of different multiuser networks. The proposed artificial noise alignment (ANA) schemes provide a different perspective and a rather clear approach for investigating the SDOF of networks: instead of random binning, we can inject AN into the confidential message subspace at eavesdroppers. As the design of IA usually comes along with the subspace analysis of signals, the approach of aligning AN to a certain subspace sometimes can offer a more intuitive way for transmission design than random binning. Following this method, the SDOF of the K -user Gaussian interference channel with confidential

Z. Wang, M. Xiao and M. Skoglund are with the Communication Theory Lab., School of Electrical Engineering, Royal Institute of Technology (KTH), Stockholm, Sweden (E-mail: {zhaowang, mingx, skoglund}@kth.se). H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ (E-mail: poor@princeton.edu).

messages (ICCM) is settled to be $\frac{K(K-1)}{2K-1}$ [13] for constant channel state. Likewise, the ANA scheme also achieves the optimal SDOF for MIMO broadcast channels [19] and two hop interference channels [20] with delayed channel state information at transmitters (CSIT), which can be seen as a non-trivial generalization of Maddah-Ali Tse scheme [21] for secret communications. Moreover, compared with random binning the ANA approach offers less system complexity via its linear operations. Therefore, the ANA approach is interesting from both theoretical and practical viewpoint.

B. Our Contributions

We study the SDOF of the wireless X network with confidential messages (XNCM). Specifically, the SDOF of the Gaussian $M \times K$ XNCM is investigated, in which each transmitter intends to send one confidential message to each receiver. The main results can be summarized as follows.

1) *A general SDOF upper bound for XNCM*: We bound the SDOF of the $M \times K$ XNCM to be less or equal to $\frac{K(M-1)}{K+M-2}$ regardless of channel fading variations. Therefore, the proposed bound holds for time/frequency varying channels, and/or constant channels. To compare with the interference channel counterpart, we set $K = M$ to induce the upper bound $\frac{K}{2}$. Henceforth, every user can obtain *at most* half of the resources.

2) *The optimal sum SDOF of the time/frequency varying XNCM*: The optimal sum SDOF of the $M \times K$ XNCM with time/frequency varying channels is shown to be

$$d = \frac{K(M-1)}{K+M-2}, \text{ if } K=2, \text{ or } M=2,$$

and

$$\frac{K(M-1)}{K+M-1} \leq d \leq \frac{K(M-1)}{K+M-2}, \text{ if } K, M \geq 3.$$

Therefore, the upper bound is tight for the network with two transmitters or receivers. The SDOF lower bound is achieved by an ANA approach, which combines standard interference alignment [17], [22] and artificial noise transmission. We note that the achieved SDOF $\frac{K(M-1)}{K+M-1}$ overlaps with the results in [23]. However, we prove it using a new approach: by proposing an ANA scheme we show that $\frac{K(M-1)}{K+M-1}$ can be achieved for the $M \times K$ XNCM with an external eavesdropper (EE), which implies the same SDOF for the considered network without the EE.

3) *The achieved sum SDOF of the XNCM with reconfigurable antennas*: Following a similar principle, we generalize the ANA scheme into a blind approach, where CSIT is not required with the help of reconfigurable antennas at the receivers. By a predefined private antenna switching pattern, we integrate the AN into a blind IA scheme to achieve the SDOF $\frac{K(M-1)}{K+M-1}$ for the $M \times K$ XNCM. It is worth noting that the predefined antenna switch pattern not only provides the channel coherence structure for aligning interference [24], it also serves as the secret key for different receivers to decode.

The rest of the paper is organized as follows. Section II introduces the system model for the $M \times K$ XNCM. We provide the proposed SDOF upper bound in Section III. In

Section IV, we study the SDOF of the considered network with time/frequency varying channels, where the ANA scheme is proposed to achieve the SDOF lower bound. We generalize the ANA into a blind approach in Section V. Conclusions are given in Section VI.

Notation: Throughout the paper, we use bold-faced uppercase letters, plain uppercase letters, and lowercase letters ($\mathbf{X}, X, x$) to represent matrices, vectors, and scalars, respectively, unless otherwise stated. X^n represents the sequence $\{x_1, x_2, \dots, x_n\}$. We define $\mathcal{K} = \{1, 2, \dots, K\}$, and $\mathcal{M} = \{1, 2, \dots, M\}$. $\mathcal{K} - i$ represents the set $\mathcal{K}$ after removing the element $i \in \mathcal{K}$. $\otimes$ represents the *Kronecker Product*. $\mathbf{A} \prec \mathbf{B}$ represents $\text{span}(\mathbf{A}) \subset \text{span}(\mathbf{B})$.

II. SYSTEM MODEL

We mainly consider transmitting confidential messages in the wireless X network. Specifically, we provide the following definitions on the network.

Definition 1: $M \times K$ wireless X network with confidential messages (XNCM).

Consider the $M \times K$ wireless X network, where each of the M transmitters intends to deliver confidential messages to all K users. Therefore, there are MK confidential messages in the considered network, shown in Fig. 1. The received signal for user k , at time t is

$$y_k(t) = \sum_{m \in \mathcal{M}} h_{km}(t)x_m(t) + n_k(t), \quad k \in \mathcal{K},$$

where the scalar $x_m(t)$ represents the transmission signal of transmitter m , the scalar $h_{km}(t)$ represents the channel coefficient from the transmitter m to the receiver k , and $n_k(t) \sim \mathcal{CN}(0, 1)$ is the additive white Gaussian noise (AWGN). We assume the power constraint $\mathbb{E}(x_m(t)^H x_m(t)) \leq P$. We define $W_{k,m} \in \mathcal{W}_{k,m} = [1 : 2^{n_{R_{k,m}}}]$, $k \in \mathcal{K}$ and $m \in \mathcal{M}$, denoting the confidential message from transmitter m to receiver k with the secrecy rate $R_{k,m}$. Let $\mathcal{W} = \{\mathcal{W}_{k,m}\}_{k \in \mathcal{K}, m \in \mathcal{M}}$. A secrecy rate tuple $\mathbf{R} = \{R_{k,m}\}_{k \in \mathcal{K}, m \in \mathcal{M}}$ is achievable if there exists a secret codebook $(n, \mathbf{R}, \mathcal{W})$ to satisfy the reliability and confidentiality constraints simultaneously:

- the reliability: at user k ,

$$\lim_{n \rightarrow \infty} \Pr(\hat{W}_{k,m} \neq W_{k,m}) = 0, \quad \forall m \in \mathcal{M} \quad (1)$$

where $\hat{W}_{k,m}$ is the estimation of the codeword $W_{k,m}$.

- the confidentiality: the equivocation for each subset of messages $\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}}$ at user k

$$\lim_{n \rightarrow \infty} \Delta_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}}^{[k]} \triangleq \lim_{n \rightarrow \infty} \frac{H(\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}} | Y_k^n)}{H(\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}})} = 1, \quad (2)$$

for $\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}} = \{W_{ij} : i \in \mathcal{S}_{\mathcal{I}}, j \in \mathcal{S}_{\mathcal{J}}\}$ and $H(\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}}) > 0$, where $\mathcal{S}_{\mathcal{I}} \subseteq \mathcal{K} - k$, $\mathcal{S}_{\mathcal{J}} \subseteq \mathcal{M}$.

If for a certain power P , $\{R_{k,m}\}$ are achievable, the SDOF d is said to be achieved with definition

$$d = \lim_{P \rightarrow \infty} \frac{\sum_{k \in \mathcal{K}, m \in \mathcal{M}} R_{k,m}}{\log(P)}. \quad (3)$$

We say d is the optimal SDOF if it is the supremum value in the set of all achievable SDOF.

In Section IV, we also considered the network when an external eavesdropper appears. Inherited from the above definition on XNCM, we present the network as follows.

Definition 2: The XNCM with an external eavesdropper (XNCM-EE).

Consider the $M \times K$ XNCM, when an external eavesdropper e appears in the network. The received signal at the eavesdropper e , at time t is

$$y_e(t) = \sum_{m \in \mathcal{M}} h_{em}(t)x_m(t) + n_e(t), \quad k \in \mathcal{K}.$$

Following *Definition 1*, we say a secrecy rate tuple $\mathbf{R}$ is achievable if there exists a secret codebook $(n, \mathbf{R}, \mathcal{W})$ to satisfy the reliability (1), confidentiality (2) and also an extra secrecy constraint at the eavesdropper:

$$\lim_{n \rightarrow \infty} \Delta_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}}^{[e]} \triangleq \lim_{n \rightarrow \infty} \frac{H(\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}} | Y_e^n)}{H(\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}})} = 1, \quad (4)$$

for $\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}} = \{W_{ij} : i \in \mathcal{S}_{\mathcal{I}}, j \in \mathcal{S}_{\mathcal{J}}\}$ and $H(\mathbf{W}_{\mathcal{S}_{\mathcal{I}}, \mathcal{S}_{\mathcal{J}}}) > 0$, where $\mathcal{S}_{\mathcal{I}} \subseteq \mathcal{K}$, $\mathcal{S}_{\mathcal{J}} \subseteq \mathcal{M}$.

III. A SECRECY DEGREES OF FREEDOM UPPER BOUND

In this section, we derive an SDOF upper bound for the $M \times K$ XNCM regardless of channel fading variations. We first present the following lemma, which will be used as an important intermediate step for the proof of the SDOF upper bound.

Lemma 1: For any $\hat{k} \in \mathcal{K}$ and $p \in \mathcal{M}$, we have the following bound for the secrecy rate:

$$n \sum_{j \in \mathcal{M}-p} R_{kj} + n \sum_{i \in \mathcal{K}} R_{ip} \leq h(Y_{\hat{k}}^n) + no(\log(P)), \quad (5)$$

where the lowercase letter h represent the differential entropy.

Proof: The detailed proof is provided in Appendix A. ■

Lemma 1 states that the sum secrecy rate of all messages either coming from transmitter p or intended for receiver $\hat{k}$ can be bounded by the differential entropy of the received signal at receiver $\hat{k}$ within the gap $o(\log(P))$. Now we are ready to present the SDOF upper bound for the $M \times K$ XNCM.

Theorem 1: The optimal sum SDOF of the $M \times K$ XNCM is upper bounded as $d \leq \frac{K(M-1)}{K+M-2}$.

Proof: For brevity, we define the following notation. Let $\mathbf{W}_{\mathcal{I}, \mathcal{J}} = \{W_{i,j} | i \in \mathcal{I}, j \in \mathcal{J}\}$, with two finite sets $\mathcal{I} = \{1, 2, \dots, I\}$ and $\mathcal{J} = \{1, 2, \dots, J\}$. Let $\mathbf{X}_{\mathcal{J}} = \{X_j^n | j \in \mathcal{J}\}$, $\mathbf{Y}_{\mathcal{I}} = \{Y_i^n | i \in \mathcal{I}\}$, and $\mathbf{N}_{\mathcal{I}} = \{N_i^n | i \in \mathcal{I}\}$ denote the transmitted, received signal and the noise sequences in the set $\mathcal{J}$ and $\mathcal{I}$, respectively. Consider all messages in the network that are confidential for receiver $\hat{k}$. Starting from

Fano's inequality, we have

$$\begin{aligned} n \sum_{i \in \mathcal{K}-\hat{k}, j \in \mathcal{M}} R_{ij} &= H(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}) \\ &= I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\mathcal{K}-\hat{k}}) + H(\mathbf{W}_{\mathcal{K}-\hat{k}} | \mathbf{Y}_{\mathcal{K}-\hat{k}}) \\ &\leq I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\mathcal{K}-\hat{k}}) + n\epsilon_1 \\ &\leq I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\mathcal{K}-\hat{k}}) - I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\hat{k}}) \\ &\quad + n(\epsilon_1 + \epsilon_2) \end{aligned} \quad (6)$$

$$\begin{aligned} &\leq I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\mathcal{K}}) - I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\hat{k}}) + n\epsilon_3 \\ &= I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\mathcal{K}-\hat{k}} | \mathbf{Y}_{\hat{k}}) + n\epsilon_3 \\ &= h(\mathbf{Y}_{\mathcal{K}-\hat{k}} | \mathbf{Y}_{\hat{k}}) - h(\mathbf{Y}_{\mathcal{K}-\hat{k}} | \mathbf{Y}_{\hat{k}}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}) + n\epsilon_3 \\ &\leq h(\mathbf{Y}_{\mathcal{K}-\hat{k}} | \mathbf{Y}_{\hat{k}}) + n\epsilon_3 = h(\mathbf{Y}_{\mathcal{K}}) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_3 \end{aligned} \quad (7)$$

$$\begin{aligned} &= I(\mathbf{Y}_{\mathcal{K}}; \mathbf{W}_{\mathcal{K}, \mathcal{M}}) + h(\mathbf{Y}_{\mathcal{K}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_3 \\ &= H(\mathbf{W}_{\mathcal{K}, \mathcal{M}}) - H(\mathbf{W}_{\mathcal{K}, \mathcal{M}} | \mathbf{Y}_{\mathcal{K}}) + h(\mathbf{Y}_{\mathcal{K}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}) \\ &\quad - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_3 \end{aligned}$$

$$\begin{aligned} &\leq H(\mathbf{W}_{\mathcal{K}, \mathcal{M}}) + h(\mathbf{Y}_{\mathcal{K}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_3 \\ &= H(\mathbf{W}_{\mathcal{K}, \mathcal{M}}) + h(\mathbf{Y}_{\mathcal{K}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}, \mathbf{X}_{\mathcal{M}}) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_3 \end{aligned} \quad (8)$$

$$\begin{aligned} &= H(\mathbf{W}_{\mathcal{K}, \mathcal{M}}) + h(\mathbf{N}_{\mathcal{K}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}, \mathbf{X}_{\mathcal{M}}) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_3 \\ &= H(\mathbf{W}_{\mathcal{K}, \mathcal{M}}) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_4 \end{aligned} \quad (9)$$

for some $\epsilon_l > 0$ and $\epsilon_l = O(1)$ ($l = 1, 2, 3, 4$), where $\epsilon_3 = \epsilon_1 + \epsilon_2$ and $\epsilon_4 = \epsilon_3 + K \log(2\pi e)$.

- (6) follows from the secrecy constraint

$$I(\mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}; \mathbf{Y}_{\hat{k}}) \leq n\epsilon_2, \text{ for some } \epsilon_2 > 0 \text{ and } \epsilon_2 = O(1).$$

- (7) follows from

$$\begin{aligned} &h(\mathbf{Y}_{\mathcal{K}-\hat{k}} | \mathbf{Y}_{\hat{k}}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}) \\ &\geq h(\mathbf{Y}_{\mathcal{K}-\hat{k}} | \mathbf{Y}_{\hat{k}}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}}, \mathbf{W}_{\hat{k}, \mathcal{M}}, \mathbf{X}_{\mathcal{M}}) \\ &= h(\mathbf{N}_{\mathcal{K}-\hat{k}}) \geq 0, \end{aligned}$$

where the last inequality follows that the Gaussian noise has positive differential entropy.

- (8) follows the fact that $\mathbf{X}_{\mathcal{M}}$ is a function of the message $\mathbf{W}_{\mathcal{K}, \mathcal{M}}$.

So far, we have bounded the rate of all confidential messages that are not intended for receiver $\hat{k}$ as (9). In order to bound the rate for the whole message set $\mathbf{W}_{\mathcal{K}, \mathcal{M}}$, we would like to apply *Lemma 1* in the proof. We begin with (9) as follows:

$$\begin{aligned} n \sum_{i \in \mathcal{K}-\hat{k}, j \in \mathcal{M}} R_{ij} &\leq H(\mathbf{W}_{\mathcal{K}, \mathcal{M}}) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_4 \\ &= \sum_{p \in \mathcal{M}} \left(n \sum_{i \in \mathcal{K}} R_{ip} \right) - h(\mathbf{Y}_{\hat{k}}) + n\epsilon_4 \\ &\leq \sum_{p \in \mathcal{M}} \left(h(\mathbf{Y}_{\hat{k}}) - n \sum_{j \in \mathcal{M}-p} R_{kj} \right) - h(\mathbf{Y}_{\hat{k}}) + no(\log(P)), \end{aligned} \quad (10)$$

Fig. 1. $M \times K$ XNCM (when an external eavesdropper appears).

where (10) follows by substituting (5) of *Lemma 1*. Equivalently, we have

$$\begin{aligned} n \sum_{i \in \mathcal{K} - \hat{k}, j \in \mathcal{M}} R_{ij} + n \sum_{p \in \mathcal{M}} \sum_{j \in \mathcal{M} - p} R_{\hat{k}j} \\ \leq (M-1)h(\mathbf{Y}_{\hat{k}}) + no(\log(P)). \end{aligned}$$

Manipulating the indices on the left hand side of the above inequality, we have

$$\begin{aligned} n \sum_{i \in \mathcal{K}, j \in \mathcal{M}} R_{ij} + n(M-2) \sum_{j \in \mathcal{M}} R_{\hat{k}j} \\ \leq (M-1)h(\mathbf{Y}_{\hat{k}}) + no(\log(P)). \end{aligned}$$

Considering that $h(\mathbf{Y}_{\hat{k}}) \leq n\log(P) + nO(1)$, we sum up the above inequality for all $\hat{k} \in \mathcal{K}$ to obtain:

$$(K+M-2) \sum_{i \in \mathcal{K}, j \in \mathcal{M}} R_{ij} \leq K(M-1)\log(P) + no(\log(P)).$$

Therefore, we have the SDOF upper bound as follows to conclude the proof

$$\sum_{i \in \mathcal{K}, j \in \mathcal{M}} d_{ij} \leq \frac{K(M-1)}{M+K-2}.$$

Remark 1: We note that the derived SDOF upper bound does not make any assumptions regarding channel fading variations. Therefore, *Theorem 1* provides a general SDOF upper bound for the $M \times K$ XNCM with constant channels, or with time/frequency varying channels. We also note that in the proof of *Theorem 1* the channel state information is assumed to be known at both receivers and transmitters. Consequently, it naturally serves as an upper bound for the SDOF of the considered network with no CSIT.

Remark 2 (At most half of the cake): We observe that the derived SDOF upper bound for the $M \times K$ XNCM equals to the sum degrees of freedom (DOF) of the $(M-1) \times K$ X network without secrecy constraints. Therefore, the impact of confidentiality is equivalent to removing at least one sender from the wireless X network, in terms of DOF. It is also

interesting to note that when $K = M$, the above upper bound yields $\sum_{i,j \in \mathcal{K}} d_{ij} \leq \frac{K(K-1)}{2(K-1)} = \frac{K}{2}$, which coincides with the sum DOF for K -user interference channel without secrecy constraints. Therefore, for the $K \times K$ fully connected wireless network, if all the messages existing in the network are confidential, then every sender can at most obtain half of the resources.

IV. THE SECRECY DEGREES OF FREEDOM OF $M \times K$ XNCM WITH TIME/FREQUENCY-VARYING CHANNELS

In this section, we study the SDOF of the wireless X networks with time or frequency varying channels. We show that the proposed SDOF upper bound is tight when $K = 2$ or $M = 2$ by presenting an artificial noise alignment scheme. The achieved SDOF of XNCM with an external eavesdropper will also be studied in this section. We start with the following theorem.

Theorem 2: The optimal sum SDOF of the $M \times K$ XNCM with time/frequency-varying channels is

$$d = \frac{K(M-1)}{K+M-2}, \text{ if } K=2, \text{ or } M=2,$$

and

$$\frac{K(M-1)}{K+M-1} \leq d \leq \frac{K(M-1)}{K+M-2}, \text{ if } K, M \geq 3.$$

Proof: The converse directly follows from *Theorem 1*. For achievability, we start from the case $K = 2$. We shall show the SDOF $\frac{2(M-1)}{M}$ can be achieved. In the following, we propose an ANA approach, which essentially aligns the artificial noise to the interference space at the receivers. The details are presented as follows.

Considering M symbols extension over the original channel, we will show that a total of $2(M-1)$ SDOF can be achieved. The main idea is to treat one transmitter, say transmitter 1, as a special sender, which only transmits artificial noise. For the rest of the $(M-1)$ transmitters, each sends 2 confidential messages intended for 2 users. By aligning the artificial noise and interference in the same subspace, the information leakage

Fig. 2. The artificial noise alignment (ANA) for $M \times 2$ XNCM.

can be bounded. We illustrate the alignment design in Fig. 2. Therefore, for message $W_{k,1}$, $k \in 1, 2$, the rate $R_{k1} = 0$. For transmitter 2 to M , we shall show that each confidential message $W_{k,j}$ ($j \in \mathcal{M} - 1$), has one SDOF over the channel extensions.

The transmitted signal of transmitter 1 is

$$X_1 = \Phi^{[1]} \nu,$$

where ν is the artificial noise symbol chosen from $\mathcal{CN}(0, P)$, and $\Phi^{[1]}$ is the $M \times 1$ beamforming matrix. At the other transmitters, the transmitted signals can be written as

$$X_j = \sum_{i=1,2} \Phi^{[ij]} \mu_{ij}, \quad j \in \mathcal{M}, j \neq 1,$$

where μ_{ij} is the confidential message symbol originating from transmitter j to receiver i , and the beamforming matrix $\Phi^{[ij]}$ has dimension $M \times 1$. Then, the received signal at the receiver k is ($i \neq k$)

$$\begin{aligned} Y_k &= \mathbf{H}_{k1} \Phi^{[1]} \nu + \sum_{j=2}^M \mathbf{H}_{kj} \left(\sum_{i=1,2} \Phi^{[ij]} \mu_{ij} \right) + N_k \\ &= \sum_{j=2}^M \mathbf{H}_{kj} \Phi^{[kj]} \mu_{kj} + \sum_{j=2}^M \mathbf{H}_{ij} \Phi^{[ij]} \mu_{ij} + \mathbf{H}_{k1} \Phi^{[1]} \nu + N_k, \end{aligned}$$

where $\mathbf{H}_{ki}$ is an $M \times M$ diagonal matrix with each diagonal element picked independently from a continuous distribution. In the achievable scheme, we aim to perfectly align the interference with artificial noise. Therefore, at receiver 1, we have

$$\mathbf{H}_{1j} \Phi^{[2j]} = \mathbf{H}_{11} \Phi^{[1]}, \quad j \in \mathcal{M} - 1, \quad (11)$$

and similarly, at receiver 2, we have

$$\mathbf{H}_{2j} \Phi^{[1j]} = \mathbf{H}_{21} \Phi^{[1]}, \quad j \in \mathcal{M} - 1. \quad (12)$$

Thus, we have

$$\Phi^{[kj]} = \mathbf{H}_{ij}^{-1} \mathbf{H}_{i1} \Phi^{[1]}, \quad j \in \mathcal{M} - 1, k, i \in \{1, 2\}, k \neq i.$$

As the next step, we have to show the effective channel matrices at receivers are full rank. Let $\Lambda^{[k]}$ represent the effective channel matrix at receiver k , where

$$\Lambda^{[k]} = \begin{bmatrix} \mathbf{H}_{k2} \Phi^{[k2]} & \mathbf{H}_{k3} \Phi^{[k3]} & \dots & \mathbf{H}_{kM} \Phi^{[kM]} & \mathbf{H}_{k1} \Phi^{[1]} \end{bmatrix}.$$

Let $\Phi^{[1]} = [\phi_1 \ \phi_2 \ \dots \ \phi_M]^T$, where each element ϕ_m ($m \in \mathcal{M}$) is picked independently from a continuous distribution. With the relations (11) and (12), the effective channel matrices at receivers are presented in the bottom of the next page. In order to show $\Lambda^{[k]}$ has full rank almost surely, we will equivalently show that $|\Lambda^{[k]}| \neq 0$ with probability one. Let $\lambda_{ij}^{[k]}$ represent the element in the i th row and j th column of $\Lambda^{[k]}$. We observe that every $\lambda_{ij}^{[k]}$ can be written in the following form:

$$\lambda_{ij}^{[k]} = \prod_{q=1}^Q \left(\beta_i^{[q]} \right)^{\alpha_{ij}^{[q]}},$$

where $\beta_i^{[q]}$ is a random variable and all exponents are integers, $\alpha_{ij}^{[q]} \in \mathbb{Z}$. Meanwhile,

- $\beta_i^{[q]} | \{\beta_{i'}^{[q']}, \forall (i, q) \neq (i', q')\}$ has a continuous cumulative probability distribution,
 - $\forall i, j, j' \in \mathcal{M}$ and $j \neq j'$
- $$\left(\alpha_{ij}^{[1]}, \alpha_{ij}^{[2]}, \dots, \alpha_{ij}^{[Q]} \right) \neq \left(\alpha_{ij'}^{[1]}, \alpha_{ij'}^{[2]}, \dots, \alpha_{ij'}^{[Q]} \right).$$

Let $C_{ij}^{[k]}$ represent the cofactor corresponding to $\lambda_{ij}^{[k]}$. Then

$$|\Lambda^{[k]}| = \lambda_{11}^{[k]} C_{11}^{[k]} + \lambda_{12}^{[k]} C_{12}^{[k]} + \dots + \lambda_{1M}^{[k]} C_{1M}^{[k]}.$$

$|\Lambda^{[k]}| = 0$ with nonzero probability only if at least one of the following two conditions is satisfied.

- $\beta_i^{[q]}, q = 1, 2, \dots, Q$ are roots of the polynomial formed by setting $|\Lambda^{[k]}| = 0$.
- The polynomial is the zero polynomial.

Note that $\beta_i^{[q]}$ have a continuous cumulative joint distribution conditioned on $C_{1l}, l \in \mathcal{M}$. Therefore, the probability of $\beta_i^{[q]}$ taking values from a finite root set goes to zero. Thus, the first condition collapses almost surely. For the second condition, since each $\beta_i^{[q]}$ has a unique set of exponents, the argument

of the zero polynomial holds with positive probability only if $\Pr(C_{1l}^{[k]} = 0) > 0$, for $l \in \mathcal{M}$. Because $C_{1l}^{[k]}$ is also the determinant of a submatrix of $\mathbf{\Lambda}^{[k]}$, the same argument can be iteratively performed, until reaching to a single element matrix containing λ_{Ml} . Therefore,

$$\Pr(|\mathbf{\Lambda}^{[k]}| = 0) > 0 \Rightarrow \Pr(|\lambda_{Ml}^{[k]}| = 0) > 0.$$

Since $\lambda_{Ml}^{[k]}$ has the form of products of continuous random variable, we can conclude that $\Pr(|\lambda_{Ml}^{[k]}| = 0) = 0$. Therefore $|\mathbf{\Lambda}^{[k]}| \neq 0$ almost surely, and $\mathbf{\Lambda}^{[k]}$ is full rank almost surely.

Because the desired signal occupies $M - 1$ dimensions in $\mathbf{\Lambda}^{[k]}$, we can write the sum rate of confidential messages W_{kj} as follows:

$$\sum_{j=2}^M R_{kj} = \frac{M-1}{M} \log(P) + o(\log(P)), k = 1, 2.$$

In the following, we compute the rate equation after collecting the whole codeword. By choosing $\mathcal{S}_I = 2$, $\mathcal{S}_J = \mathcal{M}$, the equivocation at receiver 1 is

$$\begin{aligned} \Delta_{\mathcal{S}_I, \mathcal{S}_J}^{[1]} &= \Delta_{2, \mathcal{M}} = 1 - \frac{I(\mathbf{W}_{2, \mathcal{M}}; Y_1^n)}{n \sum_{j \in \mathcal{M}} R_{2j}} \\ &\geq 1 - \frac{\frac{n}{M} I(\boldsymbol{\mu}_{2, \mathcal{M}}; Y_1)}{n \sum_{j \in \mathcal{M}} R_{2j}} \\ &= 1 - \frac{\frac{n}{M} (I(\boldsymbol{\mu}_{2, \mathcal{M}}, \nu; Y_1) - I(\nu; Y_1 | \boldsymbol{\mu}_{2, \mathcal{M}}))}{n \sum_{j \in \mathcal{M}} R_{2j}}, \end{aligned}$$

by data processing inequality and the memoryless of channels, where $\boldsymbol{\mu}_{k, \mathcal{M}} = \{\mu_{k,j}, j \in \mathcal{M}\}$, with $\mu_{k,1} \in \emptyset$. We next bound the mutual information terms

$$\begin{aligned} I(\boldsymbol{\mu}_{2, \mathcal{M}}, \nu; Y_1) &\leq I(\boldsymbol{\mu}_{2, \mathcal{M}}, \nu; Y_1, \boldsymbol{\mu}_{1, \mathcal{M}}) \\ &= I(\boldsymbol{\mu}_{2, \mathcal{M}}, \nu; Y_1 | \boldsymbol{\mu}_{1, \mathcal{M}}) \\ &= h(Y_1 | \boldsymbol{\mu}_{1, \mathcal{M}}) - h(Y_1 | \boldsymbol{\mu}_{1, \mathcal{M}}, \boldsymbol{\mu}_{2, \mathcal{M}}, \nu) = \log(P) - O(1). \end{aligned}$$

Similarly,

$$I(\nu; Y_1 | \boldsymbol{\mu}_{2, \mathcal{M}}) = \log(P) + o(\log(P)).$$

Therefore, we can show the equivocation

$$\lim_{n, P \rightarrow \infty} \Delta_{2, \mathcal{M}}^{[1]} = 1.$$

The similar argument can also be applied to receiver 2. Overall, the sum SDOF $\frac{2(M-1)}{M}$ can be achieved for the $M \times 2$ XNCM.

The achievable scheme for the case $M = 2$ follows a similar approach. We omit the details here. For $M, K \geq 3$, the SDOF lower bound overlaps with the results in [23], where random binning is used to provide secrecy. As we will show in the sequel (the proof of Lemma 2), this lower bound can also be achieved by the ANA scheme. We finish the proof here. ■

Remark 3 (Connection to broadcast channels): For $M = 2$, the optimal sum SDOF of the $2 \times K$ XNCM is shown to be 1, which coincides with the optimal SDOF of the single-input single-output (SISO) broadcast channels with confidential messages if there exists an additional helper in the network, as shown in [12].

In the following, we investigate the SDOF of the $M \times K$ XNCM with an external eavesdropper (XNCM-EE). The achieved SDOF of the considered network also implies the lower bound in Theorem 2 when $K, M \geq 3$, because removing the eavesdropper will not decrease the secrecy rate. We present the results in the following lemma.

Lemma 2: For the $M \times K$ XNCM-EE with time/frequency varying channels, the optimal sum SDOF can be bounded as $\frac{K(M-1)}{K+M-1} \leq d \leq \frac{K(M-1)}{K+M-2}$.

Proof: The upper bound directly follows from Theorem 1. The detailed proof for the lower bound is presented as follows. Let $\Gamma = K(M-1)$. We will show that the SDOF $d = \frac{K(M-1)n^\Gamma}{K(n+1)^\Gamma + (M-1)n^\Gamma}$ can be achieved for any $n \in \mathbb{N}$, which yields $d = \frac{K(M-1)}{K+M-1}$ to take the supremum for all n . Let $\mu_n = K(n+1)^\Gamma + (M-1)n^\Gamma$. We consider μ_n -symbol extension over time-varying channel. Then, the channel input-output relationship is

$$Y_k = \sum_{i \in \mathcal{M}} \mathbf{H}_{ki} X_i + N_k, \quad \forall k \in \{\mathcal{K}, e\},$$

where $\mathbf{H}_{ki}$ is the $\mu_n \times \mu_n$ diagonal matrix, and X_i is the $\mu_n \times 1$ vector from transmitter i .

Our essential idea is to let one specific transmitter, say, 1 to send artificial noise only, while the other transmitter sends confidential messages to the intended receiver. Meanwhile we propose an interference alignment scheme to align the confidential messages with artificial noise at every unintended receiver and also the external eavesdropper, to avoid information leakage. For transmitter 2 to M , we can design the transmitted signal as follows:

$$X_i = \sum_{j=1}^K \boldsymbol{\Phi}^{[ji]} \boldsymbol{\mu}_{ji}, \quad \forall i \in \mathcal{M} - 1$$

where $\boldsymbol{\mu}_{ji}$ is the $n^\Gamma \times 1$ symbol vector coded from the confidential message W_{ji} , and $\boldsymbol{\Phi}^{[ji]}$ is the corresponding $\mu_n \times n^\Gamma$ beamforming matrix. At transmitter M , the signal can be specifically designed as

$$X_1 = \sum_{j=1}^K \boldsymbol{\Phi}^{[j1]} \boldsymbol{\nu}_{j1},$$

where $\boldsymbol{\nu}_{j1}$ is the $(n+1)^\Gamma \times 1$ artificial noise symbol vector chosen from Gaussian distribution $\mathcal{CN}(0, \frac{P}{(n+1)^\Gamma} \mathbf{I}_{(n+1)^\Gamma})$, and $\boldsymbol{\Phi}^{[ji]}$ is the corresponding $\mu_n \times (n+1)^\Gamma$ beamforming matrix.

$$\begin{aligned} \mathbf{\Lambda}^{[1]} &= \begin{bmatrix} \mathbf{H}_{12} \mathbf{H}_{22}^{-1} \mathbf{H}_{21} \boldsymbol{\Phi}^{[1]} & \mathbf{H}_{13} \mathbf{H}_{23}^{-1} \mathbf{H}_{21} \boldsymbol{\Phi}^{[1]} & \dots & \mathbf{H}_{1M} \mathbf{H}_{2M}^{-1} \mathbf{H}_{21} \boldsymbol{\Phi}^{[1]} & \mathbf{H}_{11} \boldsymbol{\Phi}^{[1]} \end{bmatrix} \\ \mathbf{\Lambda}^{[2]} &= \begin{bmatrix} \mathbf{H}_{22} \mathbf{H}_{12}^{-1} \mathbf{H}_{11} \boldsymbol{\Phi}^{[1]} & \mathbf{H}_{23} \mathbf{H}_{13}^{-1} \mathbf{H}_{11} \boldsymbol{\Phi}^{[1]} & \dots & \mathbf{H}_{2M} \mathbf{H}_{1M}^{-1} \mathbf{H}_{11} \boldsymbol{\Phi}^{[1]} & \mathbf{H}_{21} \boldsymbol{\Phi}^{[1]} \end{bmatrix} \end{aligned}$$

Thus, the received signal at the k th receiver can be written as

$$Y_k = \sum_{i=2}^M \mathbf{H}_{ki} \left(\sum_{j=1}^K \Phi^{[j]} \mu_{ji} \right) + \mathbf{H}_{k1} \sum_{j=1}^K \Phi^{[j]} \nu_{j1} + N_k.$$

In the following, we will introduce the details of the alignment. At receiver k , $k \in \mathcal{K}$, we would like to have the following alignment conditions, $\forall j \in \mathcal{K} - k$:

$$\text{IA Block } j : \begin{cases} \mathbf{H}_{k2} \Phi^{[j2]} \prec \mathbf{H}_{k1} \Phi^{[j1]} \\ \mathbf{H}_{k3} \Phi^{[j3]} \prec \mathbf{H}_{k1} \Phi^{[j1]} \\ \vdots \\ \mathbf{H}_{kM} \Phi^{[jM]} \prec \mathbf{H}_{k1} \Phi^{[j1]} \end{cases}$$

Generally speaking, there are $K - 1$ alignment blocks at receiver k , and within each block we wish to align all the confidential messages intended for receiver j to the subspace spanned by artificial noise ν_{j1} . Similarly, at the eavesdropper, we would like to have K alignment blocks as follows, $\forall j \in \mathcal{K}$:

$$\text{IA Block } j : \begin{cases} \mathbf{H}_{e2} \Phi^{[j2]} \prec \mathbf{H}_{e1} \Phi^{[j1]} \\ \mathbf{H}_{e3} \Phi^{[j3]} \prec \mathbf{H}_{e1} \Phi^{[j1]} \\ \vdots \\ \mathbf{H}_{eM} \Phi^{[jM]} \prec \mathbf{H}_{e1} \Phi^{[j1]} \end{cases}$$

Therefore, every confidential message intended for receiver $j \in \mathcal{K}$ is aimed to be aligned to the subspace of artificial noise $\Phi^{[j1]}$ within the alignment block j . Let us collect the alignment block j at every receiver, including the eavesdropper. All the relations can be written as

$$\left\{ \begin{array}{l} \text{Receiver } k \neq j : \begin{cases} \mathbf{H}_{k2} \Phi^{[j2]} \prec \mathbf{H}_{k1} \Phi^{[j1]} \\ \mathbf{H}_{k3} \Phi^{[j3]} \prec \mathbf{H}_{k1} \Phi^{[j1]} \\ \vdots \\ \mathbf{H}_{kM} \Phi^{[jM]} \prec \mathbf{H}_{k1} \Phi^{[j1]} \end{cases} \\ \text{Eavesdropper : } \begin{cases} \mathbf{H}_{e2} \Phi^{[j2]} \prec \mathbf{H}_{e1} \Phi^{[j1]} \\ \mathbf{H}_{e3} \Phi^{[j3]} \prec \mathbf{H}_{e1} \Phi^{[j1]} \\ \vdots \\ \mathbf{H}_{eM} \Phi^{[jM]} \prec \mathbf{H}_{e1} \Phi^{[j1]} \end{cases} \end{array} \right.$$

Thus, there are $\Gamma = K(M-1)$ relations for alignment block j . To find the proper solution for all the beamforming matrices, we first let

$$\Phi^{[j2]} = \Phi^{[j3]} = \dots = \Phi^{[jM]}.$$

Then all the Γ relations can be written as

$$\mathbf{T}^{[km]} \Phi^{[j2]} \prec \Phi^{[j1]}, \quad \forall k \in \{\mathcal{K} - j, e\}, \quad m \in \mathcal{M} - 1$$

where

$$\mathbf{T}^{[km]} = (\mathbf{H}_{k1})^{-1} \mathbf{H}_{km}.$$

Reordering all the $\mathbf{T}^{[k,m]}$ by the index from 1 to Γ , and following the method given in [22], $\Phi^{[j1]}$ and $\Phi^{[jM]}$ can be

designed as

$$\Phi^{[j2]} = \left\{ \left(\prod_{i=1,2,\dots,\Gamma} (\mathbf{T}^{[i]})^{\alpha_i} \right) \mathbf{w}^{[j]} : \alpha_i \in \{1, 2, \dots, n\} \right\}$$

$$\Phi^{[j1]} = \left\{ \left(\prod_{i=1,2,\dots,\Gamma} (\mathbf{T}^{[i]})^{\alpha_i} \right) \mathbf{w}^{[j]} : \alpha_i \in \{1, 2, \dots, n+1\} \right\}$$

where $\mathbf{w}^{[j]}$ is the $\mu_n \times 1$ vector, with each element picked independently from a continuous distribution with bounded abstract value. The same method can be applied for all $j \in \mathcal{K}$ alignment blocks. Therefore, the effective channel matrix at receiver k can be written as

$$\mathbf{C}_k = \begin{bmatrix} \mathbf{H}_{k1} \Phi^{[k1]} & \mathbf{H}_{k2} \Phi^{[k2]} & \dots & \mathbf{H}_{kM} \Phi^{[kM]} & \mathbf{I}_k \end{bmatrix}$$

$$= \begin{bmatrix} \mathbf{H}_{k1} \Phi^{[k1]} & \mathbf{H}_{k1} \Phi^{[k2]} & \dots & \mathbf{H}_{kM} \Phi^{[k2]} & \mathbf{I}_k \end{bmatrix}$$

with $\mathbf{I}_k$ defined on the top of next page.

Following the *Lemma 1* and *Lemma 2* in [22], we can prove $\mathbf{C}_k$ is full rank almost surely, in which the signal occupies $(M-1)n^\Gamma$ independent dimensions. Therefore, we have

$$\sum_{m \in \mathcal{M}} R_{km} = \frac{K(M-1)n^\Gamma}{\mu_n} \log(P) + o(\log(P)).$$

In the following, we would like to show that the information leakage can be bounded such that the secrecy constraints at receivers and eavesdropper are satisfied. At the eavesdropper, we can write the received signal as follows:

$$Y_e = [\mathbf{H}_{e1} \Phi^{[11]} \quad \mathbf{H}_{e1} \Phi^{[21]} \quad \dots \quad \mathbf{H}_{e1} \Phi^{[K1]}] \begin{bmatrix} \nu_{11} \\ \nu_{21} \\ \vdots \\ \nu_{K1} \end{bmatrix}$$

$$+ \sum_{i=2}^M [\mathbf{H}_{ei} \Phi^{[1i]} \mu_{1i} \quad \mathbf{H}_{ei} \Phi^{[2i]} \mu_{2i} \quad \dots \quad \mathbf{H}_{ei} \Phi^{[Ki]} \mu_{Ki}] + N_e.$$

Let $\mathcal{S}_I = \mathcal{K}$ and $\mathcal{S}_J = \mathcal{M} - 1$, the information leakage at the eavesdropper is

$$I(\mathbf{W}_{\mathcal{S}_I, \mathcal{S}_J}; Y_e^n) \leq \frac{n}{\mu_n} I(\mu_{\mathcal{S}_I, \mathcal{S}_J}; Y_e)$$

$$= \frac{n}{\mu_n} (I(\mu_{\mathcal{S}_I, \mathcal{S}_J}, \nu_{\mathcal{S}_I, 1}; Y_e) - I(\nu_{\mathcal{S}_I, 1}; Y_e | \mu_{\mathcal{S}_I, \mathcal{S}_J})).$$

Let $\mathbf{A} = [\mathbf{H}_{e1} \Phi^{[11]} \quad \mathbf{H}_{e1} \Phi^{[21]} \quad \dots \quad \mathbf{H}_{e1} \Phi^{[K1]}]$ and $\mathbf{B}_i = [\mathbf{H}_{ei} \Phi^{[1i]} \mu_{1i} \quad \mathbf{H}_{ei} \Phi^{[2i]} \mu_{2i} \quad \dots \quad \mathbf{H}_{ei} \Phi^{[Ki]} \mu_{Ki}]$. Because of the alignment blocks, it is readily shown that $\text{span}(\mathbf{B}_i) \subseteq \text{span}(\mathbf{A})$. By *Lemma 4*, we can observe that the artificial noise dominates every dimension of the received-signal's subspace. It can be shown that $I(\mu_{\mathcal{S}_I, \mathcal{S}_J}, \nu_{\mathcal{S}_I, 1}; Y_e) = K(n+1)^\Gamma \log(P) + o(\log(P))$. Likewise, $I(\nu_{\mathcal{S}_I, 1}; Y_e | \mu_{\mathcal{S}_I, \mathcal{S}_J}) = K(n+1)^\Gamma \log(P) + o(\log(P))$. Therefore, the information leakage is shown to be bounded by $o(\log(P))$. It is readily shown that

$$\lim_{n, P \rightarrow \infty} \Delta_{\mathcal{S}_I, \mathcal{S}_J}^{[e]} = 1 - \frac{I(\mathbf{W}_{\mathcal{K}, \mathcal{M}}; Y_e^n)}{nR_{\mathcal{K}, \mathcal{M}}} = 1.$$

The equivocation at the other receivers can be shown to have limit 1 following the same method. Overall the sum SDOF

$$\mathbf{I}_k = \begin{bmatrix} \mathbf{H}_{k1} \Phi^{[11]} & \mathbf{H}_{k1} \Phi^{[21]} & \dots & \mathbf{H}_{k1} \Phi^{[(k-1),1]} & \mathbf{H}_{k1} \Phi^{[(k+1),1]} & \dots & \mathbf{H}_{k1} \Phi^{[K1]} \end{bmatrix}.$$

is $d = \frac{K(M-1)n^\Gamma}{\mu_n} = \frac{K(M-1)n^\Gamma}{K(n+1)^\Gamma + (M-1)n^\Gamma}$, which approaches to $\frac{K(M-1)}{K+M-1}$ for large n . ■

V. THE SECRECY DEGREES OF FREEDOM OF THE XNCM WITH RECONFIGURABLE ANTENNAS: A BLIND ARTIFICIAL NOISE ALIGNMENT APPROACH

In this section, we study the achieved SDOF of the XNCM with reconfigurable antennas, where the each receiver is equipped with one antenna that can switch among M predefined modes. When an antenna switches its mode according to a predefined pattern, it offers a chance to artificially manipulate the channel coherence structure [24]. The received signal for receiver k , at time t with antenna mode $\hat{m}_k(t)$, is

$$y_k(t) = \sum_{m \in \mathcal{M}} h_{km}(\hat{m}_k(t)) x_m(t) + n_k(t), \quad k \in \mathcal{K}, \quad (13)$$

where $h_{km}(\hat{m}_k(t))$ represents the channel coefficient from the transmitter m to the receiver k .

In the following, we propose a blind ANA that combines the blind interference alignment and artificial noise transmission. The transmission follows a similar principle as presented in Section IV, where we aim to inject artificial noise to the interference space. However, CSIT is not required in this case. IA is based on the channel coherence structure by switching antenna modes. It is worth noting that we assume that the predefined antenna switching mode $\hat{m}_k(t)$ can be known at the transmitter side; however, it is hidden from each other receivers. Intuitively, the predefined antenna switching functions can be utilized as the *key* to provide confidentiality. In order to present the achievable scheme in the XNCM, we first introduce the broadcast channel with confidential messages (BCCM). We propose a blind ANA scheme in the BCCM such that no antenna cooperation is involved, which implies the same achievable SDOF of the coresponding XNCM.

Definition 3: K -user $M \times 1$ BCCM with reconfigurable antennas.

Consider the K -user broadcast channel, where the transmitter has M antennas and each receiver is equipped with one reconfigurable antennas which can switch among M predefined modes. The received signal at receiver k is

$$y_k(t) = H_k(\hat{m}_k(t)) X(t) + n_k(t), \quad k \in \mathcal{K}$$

where $H_k(\hat{m}_k(t)) = [h_{k1}(\hat{m}_k(t)) \ h_{k2}(\hat{m}_k(t)) \ \dots \ h_{kM}(\hat{m}_k(t))]^T$ represents the $1 \times M$ channel vector with the mode $\hat{m}_k(t) \in \mathcal{M}$. $X(t) \in \mathbb{C}^{M \times 1}$ is the transmitted signal and $n_k(t) \sim \mathcal{CN}(0, 1)$. We assume each channel coefficient is drawn independently from a continuous distribution with bounded absolute value. The channel coherence time is assumed to be long enough such that the channels stay constant across a supersymbol, which will be defined in the sequel. We assume the power constraint $\mathbb{E}(X^H X) \leq P$. We assume the transmitter sends an independent confidential message $W_k \in \mathcal{W}_k = [1 : 2^{nR_k}]$

with secrecy rate R_k , which has to be hidden from the other users. With $\mathcal{W} = \{\mathcal{W}_i\}_{i=1}^K$, a secrecy rate tuple $\mathbf{R} = \{R_i\}_{i=1}^K$ is achieved if it exists a secret codebook $(n, \mathbf{R}, \mathcal{W})$ to satisfy the following constraints simultaneously: 1) the reliability: $\limsup_{n \rightarrow \infty} \Pr(\hat{W}_k \neq W_k) = 0$ for user k , 2) the confidentiality: $\lim_{n \rightarrow \infty} \Delta_S^{[k]} \triangleq \lim_{n \rightarrow \infty} \frac{H(\mathbf{W}_S | Y_k^n)}{H(\mathbf{W}_S)} = 1$ for $\mathbf{W}_S = \{W_i : i \in \mathcal{S}\}$ and $H(\mathbf{W}_S) > 0$, with $\mathcal{S} \subseteq \mathcal{K} - k$.

Lemma 3: For the K -user $M \times 1$ BCCM by Definition 3, the SDOF $\frac{K(M-1)}{M+K-1}$ can be achieved.

Proof: The detailed proof can be found in Appendix C. We briefly provide the main idea of the achievability as follows: We intend to transmit M independent streams to each user, which contains $M-1$ streams of independent confidential messages and 1 streams of artificial noise. By an interference alignment based on the channel coherence structure due to antenna switching, these M streams cast exactly M dimensions (M -D) at the intended receiver, while they overlap into 1-D subspace at all the other $K-1$ users, which is filled with the artificial noise. Because the artificial noise has the same scaled power compared with the messages in the interference space, the equivocation can be bounded to zero asymptotically. Compared with the achievable DOF result of the same network without secrecy constraint, $\frac{M}{M+K-1}$, the price to pay for the confidential message is $\frac{1}{M+K-1}$ for every user. As we shall highlight, in the proposed transmission scheme, the DOF loss $\frac{1}{M+K-1}$ is exactly the dimension occupied by the artificial noise in the transmitted signal. The key idea is illustrated in Fig. 3. ■

In order to interpret our main idea, we provide the details of the achievable scheme in the 2-user $M \times 1$ BC-CM for $M = 2$ and $M = 3$. Throughout the transmission scheme, we adopt the antenna switch pattern proposed in [24], such that the channel coherence structure can be manipulated in a systematic way.

A. $K = 2, M = 2$

In this case, each user has 2 modes to switch between. Our goal is to achieve the SDOF $\frac{2}{3}$ in total, which can be obtained by sending 1 data stream of confidential messages to each user in 3 time slots. To guarantee secrecy, 1 stream of artificial noise is also sent to protect the confidential messages at the unintended user. By antenna switching, we have the following channel coherence structure in 3 time slots, $\mathbf{H}_1 = \text{diag}\{1, 2, 1\}$ and $\mathbf{H}_2 = \text{diag}\{1, 1, 2\}$ ¹. $\mathbf{H}_1$ and $\mathbf{H}_2$ are both 3×6 matrices. These 3 time slots can be seen as a supersymbol for transmission. We design the 6×2 beamforming matrix for each user constructed by only 2×2

¹The abbreviation $\mathbf{H}_k = \text{diag}\{m_1, m_2, \dots, m_t, \dots, m_T\}$ denotes a block diagonal matrix with the diagonal element m_t replaced by $1 \times M$ vectors $H_k(m_t)$, $m_t \in \mathcal{M}$. Specifically, $\mathbf{H}_1 = \text{diag}\{1, 2, 1\} \triangleq \text{diag}\{H_1(1), H_1(2), H_1(1)\}$ and $\mathbf{H}_2 = \text{diag}\{1, 1, 2\} \triangleq \text{diag}\{H_2(1), H_2(1), H_2(2)\}$ where $H_k(m)$ is a 1×2 vector for $k, m \in \{1, 2\}$.

Fig. 3. The blind artificial noise alignment scheme for the K -user $M \times 1$ BCCM.

identity matrix and zero matrix. Apparently, the beamforming matrices do not rely on the value of channel states. Let $\Phi^{[k]}$ denote the beamforming matrix for user k , $k \in \{1, 2\}$. The transmitted signal can be represented as

$$\begin{aligned} X &= \text{vec}([X(1) \ X(2) \ X(3)]) \\ &= \underbrace{\begin{bmatrix} \mathbf{I} \\ \mathbf{I} \\ \mathbf{0} \end{bmatrix}}_{\Phi^{[1]}} \begin{bmatrix} \mu_1 \\ \nu_1 \end{bmatrix} + \underbrace{\begin{bmatrix} \mathbf{I} \\ \mathbf{0} \\ \mathbf{I} \end{bmatrix}}_{\Phi^{[2]}} \begin{bmatrix} \mu_2 \\ \nu_2 \end{bmatrix}, \end{aligned}$$

where μ_1 and μ_2 are two independent coded confidential data streams intended for user 1 and 2, respectively, and ν_1, ν_2 are two independent artificial noise streams chosen from Gaussian distribution. We assume the powers of the streams scale equally with P . The received signal at receiver 1 is

$$\begin{aligned} Y_1 &= \begin{bmatrix} y_1(1) \\ y_1(2) \\ y_1(3) \end{bmatrix} = \mathbf{H}_1 X + N_1 = \underbrace{\begin{bmatrix} H_1(1) \\ H_1(2) \\ \mathbf{0} \end{bmatrix}}_{\text{rank}=2} \begin{bmatrix} \mu_1 \\ \nu_1 \end{bmatrix} \\ &\quad + \underbrace{\begin{bmatrix} H_1(1) \\ \mathbf{0} \\ H_1(1) \end{bmatrix}}_{\text{rank}=1} \begin{bmatrix} \mu_2 \\ \nu_2 \end{bmatrix} + \begin{bmatrix} n_1(1) \\ n_1(2) \\ n_1(3) \end{bmatrix}. \end{aligned}$$

We can see μ_1 and ν_1 appear through a rank 2 matrix, while interference μ_2 and ν_2 are aligned into the subspace with rank 1. It is clear to observe that the signal space and the interference space are orthogonal to each other. Therefore, the confidential data stream μ_1 can be resolved from the received signal to obtain 1 DOF. Moreover, because in the 1-D interference subspace, μ_2 and ν_2 are coupled together with the same power level, the artificial noise ν_2 can protect the confidential data at receiver 1. Similarly, at receiver 2, μ_2 can achieve 1 DOF. Therefore, by normalizing the transmission time slots, each user achieve a DOF $\frac{1}{3}$. After collecting the whole codeword, we have the equivocation at receiver 1 as

follows, for $\mathcal{S} = \{2\}$,

$$\begin{aligned} \Delta_S^{[1]} &= 1 - \frac{I(W_2; Y_1^n)}{nR_2} \geq 1 - \frac{I(\mu_2; Y_1^n)}{nR_2} \\ &= 1 - \frac{I(\mu_2, \nu_2; Y_1^n) - I(\nu_2; Y_1^n | \mu_2)}{nR_2} \\ &= 1 - \frac{\frac{n}{3} (I(\mu_2, \nu_2; Y_1) - I(\nu_2; Y_1 | \mu_2))}{nR_2} \\ &= 1 - \frac{o(\log(P))}{\log(P) + o(\log(P))} \end{aligned}$$

where μ_2 and ν_2 represent the sequences of μ_2 and ν_2 , respectively, over the codeword length n . It is clearly that we can show

$$\lim_{n, P \rightarrow \infty} \Delta_S^{[1]} = 1,$$

to guarantee the confidentiality in the limit of large n , P . A similar analysis can be adopted at receiver 2. Finally, we show that the SDOF $\frac{2}{3}$ is achieved, almost surely.

Remark 4: The main idea of keeping the confidentiality at eavesdroppers is to let the artificial noise fill the interference subspace with the same level of power as confidential messages. When $M > 2$, we will carry out dimension-extension in transmission schemes, which leads to the dimension-expansion on the interference space. In other words, the interference space will occupy multiple dimensions in this case. As shown in the following, the key step is to maintain the presence of artificial noise in every dimension of the aligned interference space with high probability.

B. $K = 2$, $M = 3$

In this case, we aim to show the SDOF $\frac{2 \times (3-1)}{3+2-1} = 1$ can be achieved. We consider an 8-slot transmission as a supersymbol, during which 4 streams of confidential messages can be delivered to each user and 2 streams of artificial noise are used for each user. We would like to introduce additional unitary beamforming matrices $\mathbf{V}^{[k]}$ in the transmitted signals, with the purpose of maintaining the existence of artificial noise in the interference space. We can show in the sequel

that the elements in $\mathbf{V}^{[k]}$ are either 1 or 0. Thus they are independent of the value of the channel coefficients. The transmitted signal in a supersymbol for each user is designed as follows, respectively:

$$X_1 = \underbrace{\begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{I} & \mathbf{0} \\ \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \\ \mathbf{0} & \mathbf{I} \\ \mathbf{0} & \mathbf{I} \\ \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}}_{\Phi^{[1]}} \underbrace{\begin{bmatrix} \mathbf{V}_\mu^{[1]} & \mathbf{V}_\nu^{[1]} \end{bmatrix}}_{\mathbf{V}^{[1]}} \begin{bmatrix} \boldsymbol{\mu}_1 \\ \boldsymbol{\nu}_1 \end{bmatrix},$$

$$X_2 = \underbrace{\begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \\ \mathbf{0} & \mathbf{0} \\ \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \\ \mathbf{0} & \mathbf{0} \\ \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{bmatrix}}_{\Phi^{[2]}} \underbrace{\begin{bmatrix} \mathbf{V}_\mu^{[2]} & \mathbf{V}_\nu^{[2]} \end{bmatrix}}_{\mathbf{V}^{[2]}} \begin{bmatrix} \boldsymbol{\mu}_2 \\ \boldsymbol{\nu}_2 \end{bmatrix},$$

where $\boldsymbol{\mu}_k$ and $\boldsymbol{\nu}_k$ are 4×1 and 2×1 vectors, respectively, denoting the confidential data streams and artificial noise. The block matrices $\mathbf{V}_\mu^{[k]}$ and $\mathbf{V}_\nu^{[k]}$ have dimensions 6×4 and 6×2 , respectively. $\mathbf{I}$ and $\mathbf{0}$ are 3×3 identity and zero matrices, respectively. By antenna switching, we are able to have the corresponding channel matrices as $\mathbf{H}_1 = \text{diag}\{1, 2, 3, 1, 2, 3, 1, 2\}$ and $\mathbf{H}_2 = \text{diag}\{1, 1, 1, 2, 2, 2, 3, 3\}$, each representing an 8×24 matrix. Let the transmitted signal $X = X_1 + X_2$. The received signals over all 8 slots at user 1 are

$$Y_1 = \mathbf{H}_1 X + N_1 = \mathbf{H}_1 (X_1 + X_2) + N_1$$

$$= \underbrace{\begin{bmatrix} H_1(1) & 0 \\ H_1(2) & 0 \\ H_1(3) & 0 \\ 0 & H_1(1) \\ 0 & H_1(2) \\ 0 & H_1(3) \\ 0 & 0 \\ 0 & 0 \end{bmatrix}}_{\text{rank}=6} \begin{bmatrix} \mathbf{V}_\mu^{[1]} & \mathbf{V}_\nu^{[1]} \end{bmatrix} \begin{bmatrix} \boldsymbol{\mu}_1 \\ \boldsymbol{\nu}_1 \end{bmatrix}$$

$$+ \underbrace{\begin{bmatrix} H_1(1) & 0 \\ 0 & H_1(2) \\ 0 & 0 \\ H_1(1) & 0 \\ 0 & H_1(2) \\ 0 & 0 \\ H_1(1) & 0 \\ 0 & H_1(2) \end{bmatrix}}_{\text{rank}=2} \begin{bmatrix} \mathbf{V}_\mu^{[2]} & \mathbf{V}_\nu^{[2]} \end{bmatrix} \begin{bmatrix} \boldsymbol{\mu}_2 \\ \boldsymbol{\nu}_2 \end{bmatrix} + N_1$$

where $H_k(m)$ and 0 are 1×3 vectors. We observe from the signal space that 6 streams including 4 data in $\boldsymbol{\mu}_1$ and 2 artificial noise in $\boldsymbol{\nu}_1$ can be resolved almost surely in the 6-D

space. After the alignment, the dimension of the interference space has been reduced to 2 almost surely. As mentioned, for protecting the confidential messages, we aim to fill the artificial noise in the whole interference space, which means the following statement should hold almost surely (a.s.):

$$\text{rank} \left\{ \begin{bmatrix} H_1(1) & 0 \\ 0 & H_1(2) \end{bmatrix} \mathbf{V}_\nu^{[2]} \right\} = 2.$$

One solution for $\mathbf{V}_\nu^{[2]}$ can be $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}^T$, which yields

$$\text{rank} \left\{ \begin{bmatrix} h_1(1,1) & 0 \\ 0 & h_1(2,1) \end{bmatrix} \right\} = 2, \quad (14)$$

where $h_1(1,1)$ and $h_1(2,1)$ represent the first element in channel vectors $H_1(1)$ and $H_1(2)$, respectively. It is clear that (14) holds almost surely. Therefore, $\mathbf{V}^{[2]}$ can be chosen as the an elementary matrix,

$$\mathbf{V}^{[2]} = \begin{bmatrix} \mathbf{V}_\mu^{[2]} & \mathbf{V}_\nu^{[2]} \end{bmatrix} = \left[\begin{array}{cccc|cc} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{array} \right]. \quad (15)$$

By this means, we guarantee the artificial noise can be filled in the whole interference space. The equivocation $\Delta_{S,1}$ can be shown to have the limit 1 when $n, P \rightarrow \infty$. A similar argument can be made at user 2, with $\mathbf{V}^{[1]}$ chosen as the same elementary matrix (15) to keep the presence of artificial noise. Therefore, after the alignment, 4 confidential messages streams are delivered for each user over 8 slots to achieve the SDOF 1.

Remark 5: We note that the channel coherence structure provides the secret key for receivers to decode. In other words, if the private antenna switch function can be known by an eavesdropper, then the eavesdropper can switch its antenna accordingly to mimic the channel coherence structure of the receiver. In this way, the messages can be totally tapped by the eavesdropper. The network with adversary settings can be an interesting work to generalize our work.

Theorem 3: For the $M \times K$ XNCM with reconfigurable antennas, the optimal sum SDOF can be bounded as $\frac{K(M-1)}{K+M-1} \leq d \leq \frac{K(M-1)}{K+M-2}$.

Proof: The converse follows directly from *Theorem 1*. The achievability follows from the proof of *Lemma 3*, where no antenna cooperation is carried out at transmitters. Therefore, by rearranging the message set, we can obtain the same SDOF. ■

VI. CONCLUSIONS

In this paper, we have studied the achievable and optimal SDOF of wireless X networks with confidential messages. In particular, we have proposed a SDOF upper bound for the $M \times K$ XNCM. This upper bound has been shown to be tight for $M = 2$ or $K = 2$, with time/frequency varying channels. The achievability of this bound was shown by an

ANA scheme, where artificial noise has been injected into the interference space at the receivers. The proposed scheme can be generalized to the $M \times K$ XNCM with time/frequency channels for $M, K \geq 3$, even when an external eavesdropper appears. The achieved SDOF lower bound approaches the upper bound asymptotically with large M and/or K . Finally, we have generalized the ANA scheme to the blind case, in which CSIT is not necessarily needed but channel coherence structure may be known to the transmitters. It is interesting to note that by switching antenna modes artificially, we can not only obtain the intended channel coherence structure for IA but also the secret key for decoding. The achieved SDOF is also asymptotically optimal as the number of users in the network approaches infinity. By only restricting to linear operations, we have offered a different approach for handling secrecy coding and interference alignment instead of random binning.

APPENDIX A THE PROOF OF LEMMA 1

We start from the network without secrecy constraints, which certainly will not decrease the capacity region of the original one. Consider arbitrary transmitter p and receiver $\hat{k}$ in the network, $p \in \mathcal{M}$ and $\hat{k} \in \mathcal{K}$. We start from Fano's inequality (we adopt the same notation from the proof of *Theorem 1*)

$$\begin{aligned}
n \sum_{j \in \mathcal{M}} R_{\hat{k}j} &= H(\mathbf{W}_{\hat{k}, \mathcal{M}}) \\
&\leq I(\mathbf{W}_{\hat{k}, \mathcal{M}}; \mathbf{Y}_{\hat{k}}) + n\epsilon_1 \\
&\leq I(\mathbf{W}_{\hat{k}, \mathcal{M}}; \mathbf{Y}_{\hat{k}}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) + n\epsilon_1 \\
&= I(\mathbf{W}_{\hat{k}, \mathcal{M}}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) + n\epsilon_1 \\
&= h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) - h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\hat{k}, \mathcal{M}}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) + n\epsilon_1 \\
&= h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) \\
&\quad - h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\hat{k}, \mathcal{M}}, \mathbf{W}_{\mathcal{K}-\hat{k}, p}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) \\
&\quad - I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\hat{k}, \mathcal{M}}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) + n\epsilon_1 \\
&= h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) - h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}) \\
&\quad - I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\hat{k}, \mathcal{M}}, \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) + n\epsilon_1 \\
&= h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) - h(\mathbf{N}_{\hat{k}}) \\
&\quad - I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, W_{\hat{k}, p}) + n\epsilon_1 \\
&\leq h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) \\
&\quad - I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, W_{\hat{k}, p}) + n\epsilon_1,
\end{aligned} \tag{16}$$

for some $\epsilon_1 > 0$ and $\epsilon_1 = O(1)$.

- (16) follows from the fact that $h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}) = h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}}, \mathbf{X}_{\mathcal{M}}) = h(\mathbf{N}_{\hat{k}})$, because $\mathbf{X}_{\mathcal{M}}$ is a function of $\mathbf{W}_{\mathcal{K}, \mathcal{M}}$.
- (17) follows since Gaussian noise has positive differential entropy.

We now try to bound the term $I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, W_{\hat{k}, p})$. The key idea is to introduce a less noisy version of $\mathbf{Y}_{\hat{k}}$ such that the mutual information difference introduced by the less noisy receiver will not affect

DOF. Define an AWGN process $\tilde{n}_{\hat{k}} \sim \mathcal{N}(0, \tilde{\delta}_{\hat{k}}^2)$, where

$$\tilde{\delta}_{\hat{k}}^2 = \min_{i \in \mathcal{K}} \left(\frac{1}{|h_{i,p}|^2} \right) |h_{\hat{k},p}|^2. \tag{18}$$

If we replace the original noise n_k with $\tilde{n}_k$, the power of the noise has been reduced. Moreover, it introduces an enhanced effective SNR, which is the best among all the channels coming from the sender p . Then, we have

$$\begin{aligned}
&I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, W_{\hat{k}, p}) \\
&= I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, W_{\hat{k}, p}) \\
&= I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; \sum_{j \in \mathcal{M}} h_{\hat{k}, j}^n \mathbf{X}_j + N_{\hat{k}}^n | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, W_{\hat{k}, p}) \\
&= I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; h_{\hat{k}, p}^n \mathbf{X}_p + N_{\hat{k}}^n | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, W_{\hat{k}, p}) \\
&= I(\mathbf{W}_{\mathcal{K}-\hat{k}, p}; h_{\hat{k}, p}^n \mathbf{X}_p + \tilde{N}_{\hat{k}}^n | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, W_{\hat{k}, p}) - n\epsilon_2 \\
&= \sum_{i \in \mathcal{K}-\hat{k}} I \left(W_{i,p}; h_{\hat{k}, p}^n \mathbf{X}_p + \tilde{N}_{\hat{k}}^n | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, \right. \\
&\quad \left. \underbrace{W_{\hat{k}, p}, W_{1,p}, \dots, W_{i-1,p}}_{\doteq \mathbf{S}^{i-1}} \right) - n\epsilon_2 \\
&\geq \sum_{i \in \mathcal{K}-\hat{k}} I(W_{i,p}; h_{i,p}^n \mathbf{X}_p + N_i^n | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, \mathbf{S}^{i-1}) - n\epsilon_2 \\
&= \sum_{i \in \mathcal{K}-\hat{k}} H(W_{i,p} | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, \mathbf{S}^{i-1}) \\
&\quad - H(W_{i,p} | h_{i,p}^n \mathbf{X}_p + N_i^n, \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, \mathbf{S}^{i-1}) - n\epsilon_2 \\
&\geq \sum_{i \in \mathcal{K}-\hat{k}} H(W_{i,p}) - H(W_{i,p} | \mathbf{Y}_i) - n\epsilon_2 \\
&\geq \sum_{i \in \mathcal{K}-\hat{k}} H(W_{i,p}) - n\epsilon_3 - n\epsilon_2 \\
&= n \sum_{i \in \mathcal{K}, i \neq \hat{k}} R_{ip} - n\epsilon_4,
\end{aligned} \tag{19}$$

$$\begin{aligned}
&\geq \sum_{i \in \mathcal{K}-\hat{k}} I(W_{i,p}; h_{i,p}^n \mathbf{X}_p + N_i^n | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, \mathbf{S}^{i-1}) - n\epsilon_2 \\
&= \sum_{i \in \mathcal{K}-\hat{k}} H(W_{i,p} | \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, \mathbf{S}^{i-1}) \\
&\quad - H(W_{i,p} | h_{i,p}^n \mathbf{X}_p + N_i^n, \mathbf{W}_{\mathcal{K}, \mathcal{M}-p}, \mathbf{X}_{\mathcal{M}-p}, \mathbf{S}^{i-1}) - n\epsilon_2 \\
&\geq \sum_{i \in \mathcal{K}-\hat{k}} H(W_{i,p}) - H(W_{i,p} | \mathbf{Y}_i) - n\epsilon_2 \\
&\geq \sum_{i \in \mathcal{K}-\hat{k}} H(W_{i,p}) - n\epsilon_3 - n\epsilon_2 \\
&= n \sum_{i \in \mathcal{K}, i \neq \hat{k}} R_{ip} - n\epsilon_4,
\end{aligned} \tag{20}$$

for some $\epsilon_2, \epsilon_3 > 0$ and $\epsilon_2 = o(\log(P))$, $\epsilon_3 = O(1)$, $\epsilon_4 = \epsilon_2 + \epsilon_3$.

- (19) follows from the fact that $\mathbf{X}_{\mathcal{M}-p}$ is a function of $\mathbf{W}_{\mathcal{K}, \mathcal{M}-p}$.
- (20) is the consequence of (18), and the fact that introducing the less noisy channel will increase the mutual information term by some $o(\log(P))$.
- (21) follows from Chain rules for mutual information.
- (22) follows from the fact that by increasing noise, $h_{i,p}^n \mathbf{X}_p + N_i^n$ is a noisy version of $h_{\hat{k}, p}^n \mathbf{X}_p + \tilde{N}_{\hat{k}}^n$, due to (18).
- (23) follows from the following facts. The first term follows from the fact that $W_{i,p}$ is independent to other messages $W_{\hat{k}, p}$ and the transmitted signals from the other senders $\mathbf{X}_{\mathcal{M}-p}$. The second term comes from the facts that based on $\mathbf{X}_{\mathcal{M}-p}$ and $h_{i,p}^n \mathbf{X}_p$ we can reconstruct the received signal $\mathbf{Y}_i$, and removing conditions will not reduce the entropy.
- (24) follows from the Fano's inequality.

Now we substitute (25) into (17) to conclude the proof

$$\begin{aligned} n \sum_{j \in \mathcal{M}-p} R_{\hat{k}j} + n \sum_{i \in \mathcal{K}} R_{ip} &\leq h(\mathbf{Y}_{\hat{k}} | \mathbf{W}_{\mathcal{K}-\hat{k}, \mathcal{M}-p}) + n\epsilon_4 \\ &\leq h(\mathbf{Y}_{\hat{k}}) + n o(\log(P)). \end{aligned} \quad (26)$$

APPENDIX B

A PRELIMINARY LEMMA FROM LINEAR ALGEBRA

Lemma 4: For matrices $\mathbf{A} \in \mathbb{C}^{M \times N}$, $\mathbf{B}_i \in \mathbb{C}^{M \times T_i}$, with $M \geq N \geq T_i$ and $i \in \{1, 2, \dots, I\}$, if $\text{span}(\mathbf{B}_i) \subseteq \text{span}(\mathbf{A})$, then we have

$$\text{rank}(\mathbf{A}\mathbf{A}^H + \sum_{i=1}^I \lambda_i \mathbf{B}_i \mathbf{B}_i^H) = \text{rank}(\mathbf{A}\mathbf{A}^H), \quad \text{for } \lambda_i \geq 0$$

Proof: Let us assume that $\mathbf{A}$ has rank d , where $d \leq N$. Apply the compact singular value decomposition (SVD) on $\mathbf{A}$ and $\mathbf{B}_i$. Let $\mathbf{U} = [U_1, U_2, \dots, U_d] \in \mathbb{C}^{M \times d}$ and $\mathbf{\Gamma}_i = [\Gamma_1, \Gamma_2, \dots, \Gamma_{d_i}] \in \mathbb{C}^{M \times d_i}$ are the left singular vector matrices of $\mathbf{A}$ and $\mathbf{B}_i$, respectively, corresponding to the nonzeros singular values. We have $d_i \leq d$ because of $\text{span}(\mathbf{B}_i) \subseteq \text{span}(\mathbf{A})$. Our goal is to show that the matrix $\mathbf{A}\mathbf{A}^H + \sum_{i=1}^I \lambda_i \mathbf{B}_i \mathbf{B}_i^H$ has at most d linearly independent column vectors. Because U_j are the eigenvectors of matrix $\mathbf{A}\mathbf{A}^H$, any column vector of $\mathbf{A}\mathbf{A}^H$ can be written as the linear combination of U_j , for $j \in [1 : d]$. We also note that U_j are the basis for the column space of $\mathbf{A}$. We then show that any column vector of $\mathbf{B}_i \mathbf{B}_i^H$ can be also written as the linear combination of U_j . Choose an arbitrary column vector in $\mathbf{B}_i \mathbf{B}_i^H$, denoted as Q . We have $Q = \sum_{k=1}^{d_i} \alpha_k \Gamma_k$. Because $\text{span}(\mathbf{B}_i) \subseteq \text{span}(\mathbf{A})$, $\Gamma_k = \sum_{j=1}^d \beta_j U_j$ which shows that any left singular vector of $\mathbf{B}_i$ can be written as a linear combination of U_j (the basis of $\text{span}(\mathbf{A})$). Thus, $Q = \sum_{k=1}^{d_i} \alpha_k (\sum_{j=1}^d \beta_j U_j)$. Therefore, it shows that any column vector of $\mathbf{A}\mathbf{A}^H + \sum_{i=1}^I \lambda_i \mathbf{B}_i \mathbf{B}_i^H$ can be written as the linear combination of d independent vectors. The rank of $\mathbf{A}\mathbf{A}^H + \sum_{i=1}^I \lambda_i \mathbf{B}_i \mathbf{B}_i^H$ is at most d .

On the other hand, because $\mathbf{A}\mathbf{A}^H$ and $\lambda_i \mathbf{B}_i \mathbf{B}_i^H$ are *Hermitian* matrices, it is clearly

$$\text{rank}(\mathbf{A}\mathbf{A}^H + \sum_{i=1}^I \lambda_i \mathbf{B}_i \mathbf{B}_i^H) \geq \text{rank}(\mathbf{A}\mathbf{A}^H) = d.$$

Therefore, we conclude the rank of matrix $\mathbf{A}\mathbf{A}^H + \sum_{i=1}^I \lambda_i \mathbf{B}_i \mathbf{B}_i^H$ is d to complete the proof. ■

Lemma 4 provides the fundamentals to analyze the dimension of the aligned subspace in our achievable schemes. For instance, if the interference space $\text{span}(\mathbf{B}_i)$ is aligned into the subspace $\text{span}(\mathbf{A})$, then by Lemma 4, we know the aligned subspace is dominated by $\mathbf{A}$.

APPENDIX C

THE PROOF OF LEMMA 3

For the K -user BCC with M reconfigurable modes for the antenna at each receiver, we aim to show that the SDOF $\frac{K(M-1)}{M+K-1}$ can be achieved almost surely. Let $\alpha = (M-1)^{K-1}$ and $\beta = (K+M-1)\alpha$. Consider the α symbols extension over the original channel, and we construct the supersymbol in β

time slots. Then, it is equivalent to show $(M-1)\alpha$ confidential streams can be delivered to each user in β time slots, which yields $d = \frac{(M-1)\alpha}{\beta} = \frac{(M-1)^K}{(K+M-1)(M-1)^{K-1}} = \frac{M-1}{M+K-1}$ achieved for each user. The transmitted signal for the receiver $k \in \mathcal{K}$ can be designed as

$$\begin{aligned} X_k &= \text{vec}[X_k(1) \ X_k(2) \ \dots \ X_k(\beta)] \\ &= \Phi^{[k]} \underbrace{\begin{bmatrix} \mathbf{V}_\mu^{[k]} & \mathbf{V}_\nu^{[k]} \end{bmatrix}}_{\mathbf{V}^{[k]}} \begin{bmatrix} \boldsymbol{\mu}_k \\ \boldsymbol{\nu}_k \end{bmatrix}, \end{aligned}$$

where $\boldsymbol{\mu}_k$ is the $(M-1)\alpha \times 1$ confidential symbols vector intended for user k , $\boldsymbol{\nu}_k$ is the $\alpha \times 1$ artificial noise stream. Thus the whole dimension of the signal vector is $M\alpha$. $\Phi^{[k]}$ is the $M\beta \times M\alpha$ beamforming matrix, $\mathbf{V}^{[k]}$ is a unitary matrix with dimensions $M\alpha \times M\alpha$, in which the block matrix $\mathbf{V}_\nu^{[k]} \in \mathbb{C}^{M\alpha \times \alpha}$ is designed to make sure that the artificial noise can fill the whole interference space almost surely. We adopt the same antenna switching mode as proposed in [24], which gives the specific pattern for each $\mathbf{H}_k$ with dimensions $\beta \times M\beta$. For simplicity, we omit the details of $\mathbf{H}_k$ and $\Phi^{[k]}$ (please refer to [24]), and instead the emphasis is placed on the submatrix $\mathbf{V}_\nu^{[k]}$ for transmitting artificial noise.

Consider the received signal at receiver k , which is

$$\begin{aligned} Y_k &= \mathbf{H}_k \sum_{j \in \mathcal{K}} X_j + N_k = \mathbf{H}_k \Phi^{[k]} \mathbf{V}^{[k]} \begin{bmatrix} \boldsymbol{\mu}_k \\ \boldsymbol{\nu}_k \end{bmatrix} \\ &\quad + \sum_{j \in \mathcal{K}-k} \mathbf{H}_k \Phi^{[j]} \mathbf{V}^{[j]} \begin{bmatrix} \boldsymbol{\mu}_j \\ \boldsymbol{\nu}_j \end{bmatrix} + N_k. \end{aligned}$$

We first set all $\mathbf{V}^{[k]}$ to be the same choice, such that $\mathbf{V}^{[k]} = \mathbf{V}$ for all $k \in \mathcal{K}$. Let $\mathbf{G}_k = \mathbf{H}_k \Phi^{[k]} \mathbf{V}$, and $\mathbf{Q}_j = \mathbf{H}_k \Phi^{[j]} \mathbf{V}$ for $j \in \mathcal{K} - k$. We have

$$Y_k = \mathbf{G}_k \begin{bmatrix} \boldsymbol{\mu}_k \\ \boldsymbol{\nu}_k \end{bmatrix} + \sum_{j \in \mathcal{K}-k} \mathbf{Q}_j \begin{bmatrix} \boldsymbol{\mu}_j \\ \boldsymbol{\nu}_j \end{bmatrix} + N_k. \quad (27)$$

By choosing $\mathbf{H}_k$ and $\Phi^{[k]}$ ($k \in \mathcal{K}$) as in [24], it is shown that $\mathbf{H}_k \Phi^{[k]}$ and $\mathbf{H}_k \Phi^{[j]}$ ($j \in \mathcal{K} - k$) are all orthogonal. Because the isometry of the unitary matrix $\mathbf{V}$, which preserves the orthogonality and matrix rank, it is clearly that $\mathbf{G}_k$ and $\mathbf{Q}_j$ ($j \in \mathcal{K} - k$) are all orthogonal. Moreover, $\mathbf{G}_k$ is shown to have rank $M\alpha$, which implies that $\boldsymbol{\mu}_k$ and $\boldsymbol{\nu}_k$ can be resolved almost surely. Therefore, $\boldsymbol{\mu}_k$ has the rate $R_k = \frac{(M-1)\alpha}{\beta} \log(P) + o(\log(P))$. For the interference subspace, $\mathbf{Q}_j$ is shown to have rank α . To guarantee that the artificial noise can fill the interference space, it suffices to show that

$$\text{rank}\{\mathbf{H}_k \Phi^{[j]} \mathbf{V}_\nu\} = \alpha, \quad \text{a.s.}$$

which yields

$$\text{rank} \left\{ \begin{bmatrix} H'_j(1) & & & \\ & H'_j(2) & & \\ & & \ddots & \\ & & & H'_j(\alpha) \end{bmatrix} \mathbf{V}_\nu \right\} = \alpha, \quad \text{a.s.} \quad (28)$$

where for $t = [1 : \alpha]$

$$H'_j(t) = \begin{cases} H_j(M) & \text{if } t \bmod M = 0 \\ H_j(t \bmod M) & \text{otherwise} \end{cases} \quad (29)$$

We choose $\mathbf{V}_\nu = \mathbf{I} \otimes \Theta$, with $\Theta = [1 \ 0 \ \dots \ 0]^T$ denoting the $M \times 1$ elementary vector, $\mathbf{I}$ denoting the identity matrix with dimension $\alpha \times \alpha$. It yields,

$$\text{rank} \{ \text{diag} \{ h'_j(1, 1), h'_j(2, 1), \dots, h'_j(\alpha, 1) \} \} = \alpha, \text{ a.s. } (30)$$

where $h'_j(i, 1)$ represents the first element of the channel vector $H'_j(i)$. It is clearly that the above statement holds. Thus, $\mathbf{V}$ can be chosen as an elementary matrix with the block $\mathbf{V}_\nu^{[k]} = \mathbf{I} \otimes \Theta$. Let $\bar{\mathbf{Q}}_j = \mathbf{H}_k \Phi^{[j]} \mathbf{V}_\nu$ and $\mathcal{S} = \mathcal{K} - k$. We consider the information leakage at receiver k after the whole codeword length n ,

$$\begin{aligned} \frac{1}{n} I(\mathbf{W}_S; Y_k^n) &\leq \frac{1}{\beta} I(\boldsymbol{\mu}_S; Y_k) \\ &= \frac{1}{\beta} (I(\boldsymbol{\nu}_S; \boldsymbol{\mu}_S; Y_k) - I(\boldsymbol{\nu}_S; Y_k | \boldsymbol{\mu}_S)) \\ &\leq \frac{1}{\beta} \log \det \left(P \sum_{j \in \mathcal{S}} \mathbf{Q}_j \mathbf{Q}_j^H + \mathbf{I} \right) \\ &\quad - \frac{1}{\beta} \log \det \left(P \sum_{j \in \mathcal{S}} \bar{\mathbf{Q}}_j \bar{\mathbf{Q}}_j^H + \mathbf{I} \right) + o(\log(P)) \\ &= o(\log(P)), \end{aligned}$$

where the last equality follows that $\mathbf{Q}_j \mathbf{Q}_j^H$ and $\bar{\mathbf{Q}}_j \bar{\mathbf{Q}}_j^H$ have the same rank almost surely. Then,

$$\Delta_S^{[k]} = 1 - \frac{I(\mathbf{W}_S; Y_k^n)}{n R_S} \geq 1 - \frac{o(\log(P))}{d_S \log(P) + o(\log(P))} \quad (31)$$

with $d_S = \frac{(K-1)(M-1)\alpha}{\beta}$, which yields $\lim_{n, P \rightarrow \infty} \Delta_S^{[k]} = 1$. We conclude the proof here.

REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [4] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channel with confidential messages: secrecy rate regions," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.
- [5] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.
- [6] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wire-tap channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
- [7] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
- [8] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
- [9] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees of freedom of the multiple access channel," *IEEE Trans. Inform. Theory*, 2010, submitted. [Online]. Available: arXiv:1003.0729
- [10] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," *IEEE Trans. Inform. Theory*, 2010. [Online]. Available: arXiv:1007.4801
- [11] A. Khisti and D. Zhang, "Artificial noise alignment for secure multicast using multiple antennas," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1568–1571, Aug. 2013.
- [12] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inform. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.
- [13] —, "Secure degrees of freedom of K-user Gaussian interference channels: a unified view," *IEEE Trans. Inform. Theory*, submitted, 2013.
- [14] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.
- [15] O. O. Koyluoglu, H. El Gamal, L. Lai and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inform. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
- [16] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
- [17] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.
- [18] M. Kobayashi, P. Piantanida, S. Yang, and S. Shamai, "On the secrecy degrees of freedom of the multiantenna block fading wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 703–711, Sep 2011.
- [19] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Trans. Inform. Theory*, vol. 59, pp. 5244–5256, Sep. 2013.
- [20] Z. Wang, M. Xiao, and M. Skoglund, "Secrecy degrees of freedom of the 2x2x2 interference channel with delayed CSIT," *IEEE Wireless Commu. Lett.*, vol. 3, no. 4, pp. 341–344, Aug. 2014.
- [21] M. A. Maddah-Ali and D. N. C. Tse, "Completely stale transmitter channel state information is still very useful," *IEEE Trans. Inform. Theory*, vol. 58, no. 7, pp. 4418–4431, Jul. 2012.
- [22] V. R. Cadambe and S. A. Jafar, "Interference alignment and the degrees of freedom of wireless X networks," *IEEE Trans. Inform. Theory*, vol. 55, no. 9, pp. 3893 – 3908, Sep. 2009.
- [23] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," in *Proceedings of 46th Allerton Annual Conference on Communication, Control and Computing*, Sep. 2008.
- [24] T. Gou, C. Wang, and S. A. Jafar, "Aiming perfectly in the dark-blind interference alignment through staggered antenna switching," *IEEE Trans. Signal Processing*, vol. 59, no. 6, pp. 228–240, Jun. 2011.