On the Secure Degrees of Freedom of Wireless X Networks

Tiangao Gou, Syed A. Jafar
Electrical Engineering and Computer Science
University of California Irvine, Irvine, California, 92697
Email: {tgou,syed}@uci.edu

***Abstract*— Previous work showed that the X network with M transmitters, N receivers has $\frac{MN}{M+N-1}$ degrees of freedom. In this work we study the degrees of freedom of the X network with secrecy constraints, i.e. the X network where some/all messages are confidential. We consider the $M \times N$ network where all messages are secured and show that $\frac{N(M-1)}{M+N-1}$ degrees of freedom can be achieved. Secondly, we show that if messages from only $M-1$ transmitters are confidential, then $\frac{MN}{M+N-1}$ degrees of freedom can be achieved meaning that there is no loss of degrees of freedom because of secrecy constraints. We also consider the achievable secure degrees of freedom under a more conservative secrecy constraint. We require that messages from any subset of transmitters are secure even if other transmitters are compromised, i.e., messages from the compromised transmitter are revealed to the unintended receivers. We also study the achievable secure degrees of freedom of the K user Gaussian interference channel under two different secrecy constraints where $\frac{1}{2}$ secure degrees of freedom per message can be achieved. The achievable scheme in all cases is based on random binning combined with interference alignment.**

I. Introduction

Security is an important issue if the transmitted information is confidential. Researchers have studied the information theoretic secrecy for different channel models. In [1], Wyner first proposed the wiretap channel model to characterize single user secure communication problem, i.e., a sender transmits a confidential message to its receiver while keeping a wire-tapper totally ignorant of the message. The secrecy level is measured by the equivocation rate, i.e., the entropy rate of the confidential message conditioned on the received signal at the wire-tapper. More recent information-theoretic research on secure communication focuses on multi-user scenarios. In [2], the authors study the compound wire-tap channel where the sender multicasts its messages to multiple receivers while ensuring the confidentiality of the messages at multiple wire-tappers. Multiple access channel with confidential messages has been studied in [3]–[5]. Broadcast channel with confidential messages has been studied in [6], [7]. The two user discrete memoryless interference channel with confidential messages is studied in [7].

It is well known that the secrecy capacity of the Gaussian wiretap channel is the difference between the capacities of the main and the wiretap channels [8]. In other words, there is a rate penalty for ensuring the secrecy. From the degrees of freedom perspective, this is pessimistic since the channel loses all its degrees of freedom. Further, even the two user Gaussian interference channel loses all its degrees of freedom if we have to ensure that messages from both transmitters are confidential, i.e., a message should remain secure from the undesired receiver. The results of the Gaussian wiretap channel and the 2 user Gaussian interference channel prompt one to ask whether it is possible for a network to have positive number of degrees of freedom if the messages in the network are secure. The answer to this question lies in the study of the K user Gaussian interference channel with secure messages [9] which indeed has positive number of degrees of freedom if $K > 2$. It is shown that the network has $\frac{K(K-2)}{2K-2}$ secure degrees of freedom. The key to increase the secure degrees of freedom is interference alignment. Interference signals associated with the messages needed to be secured are aligned to occupy smaller dimension so that the secrecy penalty rate is minimized. At the same time, the degrees of the freedom for the legitimate channel is maximized by interference alignment. Thus, the tool of interference alignment serves the dual purpose of minimizing the secrecy penalty rate and maximizing the rate of the legitimate messages, thus improving the secure degrees of freedom of the network.

In this paper, we generalize the result of [9] to the X network. We study the achievable secure degrees of freedom of the $M \times N$ user wireless X network, i.e., a network with M transmitters and N receivers where independent confidential messages need to be conveyed from each transmitter to each receiver. X networks are interesting since they encompasses different communication scenarios. For example, each transmitter is associated with a broadcast channel, each receiver is associated with a multiple access channel and every pair of transmitters and receivers comprises an interference channel. In other words, broadcast channel, multiple access channel and interference channel are special cases of X networks. In addition, interference alignment is also feasible on X networks. In [11], interference alignment schemes are constructed to achieve $\frac{1}{M+N-1}$ degrees of freedom per frequency/time slot for each message without secrecy constraint. In this paper, we exploit alignment of interference to assist secrecy in the network. We study the achievable secure degrees of freedom under four different secrecy constraints. We show

The work of S. Jafar was supported by ONR Young Investigator Award N00014-08-1-0872.

that if the set of all unintended messages is secured at each receiver, then each message can achieve $\frac{M-1}{M}\frac{1}{M+N-1}$ secure degrees of freedom for a total of $\frac{N(M-1)}{M+N-1}$ secure degrees of freedom. In other words, only a fraction $\frac{1}{M}$ degrees of freedom is lost under this secrecy constraint. Interestingly, if we only secure the set of unintended messages from any $M-1$ transmitters at each receiver, then each message can achieve $\frac{1}{M+N-1}$ secure degrees of freedom which is the same as what one can achieve without secrecy constraint. This corresponds to a scenario where one transmitter's messages need not be secure, perhaps because their confidentiality is ensured cryptographically, by some higher layer. In this case, the other messages increase their degrees of freedom by exploiting this. Next, we consider a more conservative secrecy constraint. Transmitters do not trust each other, so we require that even if any subset of transmitters $\mathcal{S}$ is compromised, i.e., the messages from the compromised transmitter are revealed to the unintended receivers (through a genie), the remaining transmitters' messages are still secure. For this case, we show that if the set of all unintended messages is secured then $\frac{N(M-|\mathcal{S}|-1)}{M+N-1}$ secure degrees of freedom can be achieved for the remaining $(M-|\mathcal{S}|)\times N$ users. If we only need to secure the set of unintended messages from $M-|\mathcal{S}|-1$ transmitters, then $\frac{1}{M+N-1}$ secure degrees of freedom can be achieved for each message. The achievable scheme for all cases is based on random binning combined with interference alignment.

II. System Model and Secrecy Constraints

A. System Model

The $M\times N$ user X network is comprised of M transmitters and N receivers. Each transmitter has an independent message for each receiver. The channel output at the j^{th} receiver over the f^{th} frequency slot and the t^{th} time slot is described as follows:

$$Y_j(f,t)=\sum_{i=1}^{M}H_{ji}(f)X_i(f,t)+Z_j(f,t),\ j=1,2,\ldots,N$$

where $X_i(f,t)$ is the input signal at Transmitter i, $H_{ji}(f)$ is the channel coefficient from Transmitter i to Receiver j and $Z_j(f,t)$ represents the additive white Gaussian noise (AWGN) at Receiver j. We assume the channel coefficients vary across frequency slots but remain constant in time and are drawn from a continuous distribution. We assume all channel coefficients are known to all transmitters and receivers. Using the symbol extension channel in [11], the input-output relationship is characterized as follows:

$$\bar{\mathbf{Y}}_j(t)=\sum_{i=1}^{M}\bar{\mathbf{H}}_{ji}\bar{\mathbf{X}}_i(t)+\bar{\mathbf{Z}}_j(t) \tag{1}$$

where $\bar{\mathbf{X}}_i(t)$ is the $F\times 1$ column vector representing the F symbol extension of the transmitted symbol X_i, i.e., $\bar{\mathbf{X}}_i(t)=[X_i(1,t)\ X_i(2,t)\ \cdots\ X_i(F,t)]^T$. Similarly, $\bar{\mathbf{Y}}_j(t)$ and $\bar{\mathbf{Z}}_j(t)$ represent the symbol extension of Y_j and Z_j, respectively. $\bar{\mathbf{H}}_{ji}$ is the $F\times F$ diagonal matrix representing the extension of the channel, i.e.,

$$\bar{\mathbf{H}}_{ji}=\begin{bmatrix}H_{ji}(1) & 0 & \cdots & 0\\ 0 & H_{ji}(2) & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & H_{ji}(F)\end{bmatrix}$$

Transmitter i has message $W_{ji}\in\{1,2,\ldots,M_{ji}\}$ for Receiver j, for each $i\in\{1,2,\ldots,M\}$, $j\in\{1,2,\ldots,N\}$, resulting in a total of MN independent messages. An $(M_{11},\ldots,M_{NM},n,F,P_e)$ code for the X channel consists of the following:

- MN independent message sets: $\mathcal{W}_{ji}=\{1,2,\ldots,M_{ji}\}$
- M encoding functions, f_i: $\mathcal{W}_{1i}\times\mathcal{W}_{2i}\times\cdots\times\mathcal{W}_{Ni}\to\bar{\mathbf{X}}_i^n$, where $\bar{\mathbf{X}}_i^n=[\bar{\mathbf{X}}_i(1)\ \bar{\mathbf{X}}_i(2)\ \cdots\ \bar{\mathbf{X}}_i(n)]$, which map the message tuple $(w_{1i},w_{2i},\cdots,w_{Ni})\in\mathcal{W}_{1i}\times\mathcal{W}_{2i}\times\cdots\times\mathcal{W}_{Ni}$ to transmitted symbols. Each transmitter has a power constraint, i.e.

$$\frac{1}{nF}\sum_{f=1}^{F}\sum_{t=1}^{n}|X_i(t,f)|^2\le P,\ i\in\{1,2,\ldots,M\}.$$

- N decoding functions, g_j: $\bar{\mathbf{Y}}_j^n\to\mathcal{W}_{j1}\times\mathcal{W}_{j2}\times\cdots\times\mathcal{W}_{jM}$, where $\bar{\mathbf{Y}}_j^n=[\bar{\mathbf{Y}}_j(1)\ \bar{\mathbf{Y}}_j(2)\ \cdots\ \bar{\mathbf{Y}}_j(n)]$, which map the received sequence $\bar{\mathbf{Y}}_j^n$ to the decoded message tuple $(\hat{w}_{j1},\hat{w}_{j2},\cdots,\hat{w}_{jM})\in\mathcal{W}_{j1}\times\mathcal{W}_{j2}\times\cdots\times\mathcal{W}_{jM}$.

The maximal average probability of error P_e for an $(M_{11},\ldots,M_{NM},n,F,P_e)$ code is defined as

$$P_e\triangleq\max\{P_{e,11},P_{e,21},\cdots,P_{e,NM}\}$$

where

$$P_{e,ji}=\frac{1}{M_{ji}}\sum_{w_{ji}\in\mathcal{W}_{ji}}P\{g(\bar{\mathbf{Y}}_j^n)\neq w_{ji}|w_{ji}\text{ sent}\}$$

We use the equivocation rate $\frac{1}{nF}H(W|\bar{\mathbf{Y}}_j^n)$ as the secrecy measure.

A rate tuple $(R_{11},R_{21},\ldots,R_{NM})$ is said to be achievable for the $M\times N$ user X network with confidential messages if for any $\epsilon>0$, there exists an $(M_{11},\ldots,M_{NM},n,F,P_e)$ code such that

$$\frac{1}{nF}\log_2(M_{ji})\ge R_{ji}$$

and the reliability requirement

$$P_e\le\epsilon$$

and the security constraints which will be defined shortly are satisfied. The secure degrees of freedom tuple $(\eta_{11},\ldots,\eta_{NM})$ is achievable if the rate tuple $(R_{11},\ldots,R_{NM})$ is achievable and

$$\eta_{ji}=\lim_{P\to\infty}\frac{R_{ji}(P)}{\log(P)}\ \ \forall(j,i)\in\mathcal{J}\times\mathcal{I},$$
$$\mathcal{I}=\{1,2,\ldots,M\},\ \mathcal{J}=\{1,2,\ldots,N\}$$

B. Secrecy Constraints

We will define four different secrecy constraints as follows:

1) Secrecy Constraint 1: The secrecy constraint is defined as

$$\frac{1}{nF}H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n) \geq \sum_{(r,i)\in(\mathcal{J}-j)\times\mathcal{I}} R_{ri} - \epsilon$$

where

$$\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}} \triangleq \{W_{ri} : \forall(r,i) \in (\mathcal{J}-j)\times\mathcal{I}\}$$

This ensures the perfect secrecy of the set of all unintended messages at each receiver. Moreover, it can be shown that perfect secrecy for a set of messages guarantees perfect secrecy for any subset of that message set, i.e.,

$$\frac{1}{nF}H(\mathbf{W}_S|\bar{\mathbf{Y}}_j^n) \geq \sum_{(r,i)\in S} R_{ri} - \epsilon \quad \forall S \subseteq (\mathcal{J}-j)\times\mathcal{I} \quad (2)$$

To see this, consider

$$\begin{aligned} H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n) &= H(\mathbf{W}_S|\bar{\mathbf{Y}}_j^n) + H(\mathbf{W}_{S^c}|\mathbf{W}_S, \bar{\mathbf{Y}}_j^n) \quad (3)\\ &\leq H(\mathbf{W}_S|\bar{\mathbf{Y}}_j^n) + H(\mathbf{W}_{S^c}) \quad (4)\end{aligned}$$

where S^c denotes the complement of S and (3) follows from the chain rule and (4) follows from the fact that conditioning reduces the entropy. If the message set satisfies the secrecy constraint, i.e.,

$$H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n) \geq H(\mathbf{W}_S) + H(\mathbf{W}_{S^c}) - \epsilon$$

then from (4) we have

$$\begin{aligned} H(\mathbf{W}_S|\bar{\mathbf{Y}}_j^n) + H(\mathbf{W}_{S^c}) &\geq H(\mathbf{W}_S) + H(\mathbf{W}_{S^c}) - \epsilon \\ \Rightarrow H(\mathbf{W}_S|\bar{\mathbf{Y}}_j^n) &\geq H(\mathbf{W}_S) - \epsilon \end{aligned}$$

Thus, the confidentiality of the subset $\mathbf{W}_S$ is preserved.

2) Secrecy Constraint 2: Instead of ensuring the confidentiality of the set of unintended messages of all transmitters, we only secure the set of unintended messages from any $M-1$ transmitters. Secrecy constraint 2 is defined as

$$\frac{1}{nF}H(\mathbf{W}_{(\mathcal{J}-j)\times(\mathcal{I}-l)}|\bar{\mathbf{Y}}_j^n) \geq \sum_{(r,i)\in(\mathcal{J}-j)\times(\mathcal{I}-l)} R_{ri} - \epsilon \; \forall l \in \mathcal{I}$$

where

$$\mathbf{W}_{(\mathcal{J}-j)\times(\mathcal{I}-l)} = \{W_{ri} : \forall(r,i) \in (\mathcal{J}-j)\times(\mathcal{I}-l)\}$$

Again, the perfect secrecy of a message set guarantees perfect secrecy for any subset of that message set, i.e.,

$$\frac{1}{nF}H(\mathbf{W}_{\mathcal{S}_J\times\mathcal{S}_I}|\bar{\mathbf{Y}}_j^n) \geq \sum_{(r,i)\in\mathcal{S}_J\times\mathcal{S}_I} R_{ri} - \epsilon, \quad \forall\mathcal{S}_J \subseteq \mathcal{J}-j, \forall\mathcal{S}_I \subseteq \mathcal{I}-l$$

Note that satisfying secrecy constraint 1 ensures satisfying secrecy constraint 2.

3) Secrecy Constraint 3: Let us define $\mathcal{S}_I \subset \mathcal{I}$ to be the set of transmitters that are compromised, i.e., the messages from the compromised transmitter are revealed to the unintended receivers and $\mathcal{S}_I^c$ to be the set of the remaining transmitters. We define secrecy constraint 3 as

$$\frac{1}{nF}H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}_I^c}|\bar{\mathbf{Y}}_j^n, \mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}_I}) \geq \sum_{(r,i)\in(\mathcal{J}-j)\times\mathcal{S}_I^c} R_{ri} - \epsilon \quad \forall\mathcal{S}_I \subset \mathcal{I}$$

This constraint ensures that secrecy of any subset of transmitters even if all other transmitters are compromised. Also, this secrecy constraint guarantees that

$$\frac{1}{nF}H(\mathbf{W}_{\mathcal{S}_J\times\mathcal{S}_I^c}|\bar{\mathbf{Y}}_j^n, \mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}_I}) \geq \sum_{(r,i)\in\mathcal{S}_J\times\mathcal{S}_I^c} R_{ri} - \epsilon \quad \forall\mathcal{S}_I \subset \mathcal{I}, \forall\mathcal{S}_J \subseteq \mathcal{J}-j$$

4) Secrecy Constraint 4: Even if any subset of transmitters $\mathcal{S}_I \subset \mathcal{I}$ is compromised, we require secrecy of the set of messages from $\mathcal{S}_I^c - l$ transmitters for any $l \in \mathcal{S}_I^c$. We define secrecy constraint 4 as

$$\begin{aligned} &\frac{1}{nF}H(\mathbf{W}_{(\mathcal{J}-j)\times(\mathcal{S}_I^c-l)}|\bar{\mathbf{Y}}_j^n, \mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}_I}) \\ \geq &\sum_{(r,i)\in(\mathcal{J}-j)\times(\mathcal{S}_I^c-l)} R_{ri} - \epsilon \quad \forall\mathcal{S}_I \subset \mathcal{I}, \; \forall l \in \mathcal{S}_I^c \end{aligned}$$

III. The $M \times N$ user X Network with confidential messages

In this section, we consider the achievable secure degrees of freedom of the $M \times N$ user X channel under different secrecy constraints. In order to satisfy the secrecy constraints, we use the random binning coding scheme to generate the codebook. This is a natural extension of the coding scheme used in [7] to achieve the inner bound of the capacity region of the two user discrete memoryless interference channel with confidential messages. To maximize the achievable degrees of freedom, we adopt the interference alignment scheme used in [11]. The main results of this section are presented in the following theorems:

Theorem 1: For the $M \times N$ user X network with single antenna nodes, $\frac{M-1}{M(M+N-1)}$ secure degrees of freedom can be achieved for each message W_{ji}, $\forall j \in \{1,\ldots,N\}, \forall i \in \{1,\ldots,M\}$ and hence a total of $\frac{N(M-1)}{M+N-1}$ secure degrees of freedom can be achieved under secrecy constraint 1.

Proof: We provide a detailed proof in the Appendix. A sketch of the proof is provided here. Consider the F symbol extension channel where $F = N(m+1)^\Gamma + (M-1)m^\Gamma, \forall m \in \mathbb{N}$ and $\Gamma = (N-1)(M-1)$. Over the F symbol extension channel, message W_{j1} is encoded at Transmitter 1 into $m_1 = (m+1)^\Gamma$ independent streams $\mathbf{X}_{j1}(t)$ which is an $(m+1)^\Gamma \times 1$ vector and message $W_{ji}, i \neq 1$ is encoded at Transmitter i into $m_i = m^\Gamma$ independent streams $\mathbf{X}_{ji}(t)$ which is an $m^\Gamma \times 1$ vector based on random binning coding scheme. Note that such coding scheme introduces randomness to ensure the secrecy. Then transmitter i employs the interference alignment

scheme mapping $\mathbf{X}_{ji}(t)$ to $\mathbf{V}_{ji}(t)\mathbf{X}_{ji}(t)$ where $\mathbf{V}_{ji}$ is the $F \times m_i$ matrix. At last, Transmitter i sends signal $\bar{\mathbf{X}}_i(t) = \sum_{j=1}^{N} \mathbf{V}_{ji}(t)\mathbf{X}_{ji}(t)$ into the channel. Note that the precoding matrices $\mathbf{V}_{ji}(t)$ are chosen as given in [11] so that at each receiver, the desired signal vectors span a signal space which is disjoint with the space spanned by the interference vectors. Therefore, each receiver can decode its desired data streams by zero forcing the interference. Note that at Receiver j, the signal vectors associated with M desired messages $W_{ji}, \forall i = 1, \ldots, M$ span a $(m+1)^{\Gamma}+(M-1)m^{\Gamma}$ dimensional subspace in the $F = N(m+1)^{\Gamma} + (M-1)m^{\Gamma}$ dimensional signal space. Thus, to get an interference-free signal subspace, the dimension of the subspace spanned by all interference vectors has to be less than or equal to $(N-1)(m+1)^{\Gamma}$. Notice that the interference vectors from Transmitter 1 span a $(N-1)(m+1)^{\Gamma}$ dimensional subspace. Therefore, we can align the interference vectors from all other transmitters within this subspace so that each receiver can decode its desired data streams by zero forcing the interference in this subspace. Next, it can be shown that the following secrecy rate is achievable:

$$\begin{aligned} R_{ji} &= \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) \\ &- \frac{1}{F} \frac{1}{M(N-1)} \max_{k \in \mathcal{J}} I(\mathbf{X}_{(\mathcal{J}-k)\times\mathcal{I}}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}}) \\ &\qquad \forall (j,i) \in \mathcal{J} \times \mathcal{I} \quad (5) \end{aligned}$$

From [11], we have

$$I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) = (m+1)^{\Gamma} \log(P) + o(\log(P)) \quad i = 1$$

and

$$I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) = m^{\Gamma} \log(P) + o(\log(P)) \quad i = 2, \ldots, M$$

Next, consider the term $I(\mathbf{X}_{(\mathcal{J}-k)\times\mathcal{I}}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}})$ which denotes the secrecy penalty. Notice that all the interference vectors are aligned within the space spanned by $(N-1)(m+1)^{\Gamma}$ interference vectors from Transmitter 1. Therefore, the secrecy penalty is

$$\begin{aligned} & I(\mathbf{X}_{(\mathcal{J}-k)\times\mathcal{I}}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}}) \\ = \; & (N-1)(m+1)^{\Gamma} \log(P) + o(\log(P)) \quad \forall k \in \mathcal{J} \end{aligned}$$

Hence, (5) can be written as

$$R_{ji} = \frac{1}{F}(m+1)^{\Gamma}(1 - \frac{1}{M}) \log(P) + o(\log(P)) \quad i = 1$$

and

$$R_{ji} = \frac{1}{F}(m^{\Gamma} - \frac{(m+1)^{\Gamma}}{M}) \log(P) + o(\log(P)) \quad i = 2, \ldots, M$$

As $m \to \infty$, we have

$$R_{ji} = \frac{M-1}{M(M+N-1)} \log(P) + o(\log(P)) \quad \forall (j,i) \in \mathcal{J} \times \mathcal{I}$$

As a result, each message can achieve $\eta_{ji} = \frac{M-1}{M(M+N-1)}$ secure degrees of freedom for a total of $\frac{(M-1)N}{M+N-1}$ secure degrees of freedom. ■

Note that in [11], it is shown that $\frac{1}{M+N+1}$ degrees of freedom can be achieved for each message W_{ji} without secrecy constraint. Theorem 1 shows that only a fraction $\frac{1}{M}$ degrees of freedom is lost under secrecy constraint 1. However, it is interesting that if we relax the secrecy constraint a little, i.e., only ensure the confidentiality of the set of messages from any $M-1$ out of M transmitters at each receiver, there will be no loss of degrees of freedom. We present the result in the following theorem:

Theorem 2: For the $M \times N$ user X network with single antenna nodes, each message can achieve $\frac{1}{M+N-1}$ secure degrees of freedom for a total of $\frac{MN}{M+N-1}$ secure degrees of freedom under secrecy constraint 2.

Proof: The proof is similar to the proof of Theorem 1. We only provide a sketch of proof here. It can be shown that the following secrecy rate is achievable:

$$\begin{aligned} R_{ji} &= \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) \\ &- \frac{1}{F} \frac{1}{(M-1)(N-1)} \max_{k \in \mathcal{J}, l \in \mathcal{I}} I(\mathbf{X}_{(\mathcal{J}-k)\times(\mathcal{I}-l)}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}}) \\ &\qquad \forall (j,i) \in \mathcal{J} \times \mathcal{I} \; \forall l \in \mathcal{I} \quad (6) \end{aligned}$$

where $F = N(m+1)^{\Gamma}+(M-1)m^{\Gamma}$ and $\Gamma = (M-1)(N-1)$. Through interference alignment, it can be shown that

$$I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) = \eta \log(P) + o(\log(P))$$

where $\eta = (m+1)^{\Gamma}$ when $i = 1$ and $\eta = m^{\Gamma}$ when $i = 2, 3, \ldots, M$. Then consider the secrecy penalty term $I(\mathbf{X}_{(\mathcal{J}-k)\times(\mathcal{I}-l)}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}})$. At each receiver, the interference vectors from Transmitter $2, 3 \ldots, M$ are aligned perfectly with the interference vectors from Transmitter 1, i.e. every interference signal vector from Transmitter $2, 3 \ldots, M$ is aligned along the same dimension with one interference signal vector from Transmitter 1. Note that there are $(m+1)^{\Gamma}$ interference vectors for each message from Transmitter 1, but there are only m^{Γ} interference vectors for each message from Transmitter $2, 3 \ldots, M$. If $l = 1$, $I(\mathbf{X}_{(\mathcal{J}-k)\times(\mathcal{I}-1)}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}})$ denotes the mutual information between the channel output at Receiver k and channel inputs from Transmitter $2, \ldots, M$. Since all vectors from Transmitter $2, 3 \ldots, M$ are aligned perfectly with interference vectors from Transmitter 1, it has zero degrees of freedom, i.e., $I(\mathbf{X}_{(\mathcal{J}-k)\times(\mathcal{I}-1)}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}}) = o(\log(P))$. For $\forall l \neq 1$, the interference vectors from Transmitter l occupy a $(N-1)m^{\Gamma}$ dimensional subspace. Therefore, the remaining transmitters can get a $(N-1)((m+1)^{\Gamma} - m^{\Gamma})$ dimensional space without interference vectors from Transmitter l. Therefore, we have

$$\begin{aligned} & \max_{k \in \mathcal{J}, \; l \in \mathcal{I}} I(\mathbf{X}_{(\mathcal{J}-k)\times(\mathcal{I}-l)}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{I}}) \\ &= (N-1)((m+1)^{\Gamma} - m^{\Gamma}) \log(P) + o(\log(P)) \\ &\qquad \forall (j,i) \in \mathcal{J} \times \mathcal{I} \end{aligned}$$

Thus, (6) can be written as

$$R_{ji} = \frac{(M-1)\eta - ((m+1)^\Gamma - m^\Gamma)}{F(M-1)} \log(P) + o(\log(P)) \quad \forall i = 1, 2, \ldots, M$$

When $m \to \infty$, we have

$$\eta_{ji} = \lim_{m\to\infty} \frac{(M-1)\eta - ((m+1)^\Gamma - m^\Gamma)}{F(M-1)} = \frac{1}{M+N-1}$$

Therefore, each message can achieve $\frac{1}{M+N-1}$ secure degrees of freedom for a total of $\frac{MN}{M+N-1}$ secure degrees of freedom. ■

Next, we consider the achievable secure degrees of freedom under the more conservative secrecy constraints to ensure secrecy of any subset of transmitters even if all other transmitters are compromised. We present the result in the following theorem.

Theorem 3: For the $M \times N$ user X network with single antenna nodes, even if any subset of transmitters, $\mathcal{S} \subset \{1, \ldots, M\}$ is compromised, the remaining $(M - |\mathcal{S}|) \times N$ users can still achieve a total of $\frac{N(M-|\mathcal{S}|-1)}{M+N-1}$ secure degrees of freedom under secrecy constraint 3 and $\frac{N(M-|\mathcal{S}|)}{M+N-1}$ secure degrees of freedom under secrecy constraint 4, as long as $|\mathcal{S}| \leq M-2$.

Proof: To satisfy secrecy constraint 3, we design an achievable scheme to satisfy the following secrecy constraint:

$$\frac{1}{nF} H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}^c} | \bar{\mathbf{Y}}_j^n, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{S}}^n) \geq \sum_{(r,i)\in(\mathcal{J}-j)\times\mathcal{S}^c} R_{ri} - \epsilon \quad \forall \mathcal{S} \subset \mathcal{I}$$

where

$$\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{S}}^n = \{\mathbf{X}_{ji}^n : \forall (j,i) \in (\mathcal{J}-j)\times\mathcal{S}\}$$

$\mathbf{X}_{ji}^n$ denotes the codeword for message W_{ji}. Note that this secrecy constraint is stronger than $\frac{1}{nF} H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}^c} | \bar{\mathbf{Y}}_j^n, \mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}})$. Because

$$\begin{aligned} & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}^c} | \bar{\mathbf{Y}}_j^n, \mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}}) \\ \geq\ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}^c} | \bar{\mathbf{Y}}_j^n, \mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{S}}^n) \\ =\ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{S}^c} | \bar{\mathbf{Y}}_j^n, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{S}}^n) \end{aligned}$$

In other words, we want to ensure secrecy of any subset of transmitters even if all other transmitters' codewords rather than messages are revealed to the unintended receivers. This is possible because the achievability scheme encodes the messages separately and each message has its codewords. The coding scheme is similar to that used in Theorem 1. Then it can be shown that the following secrecy rate is achievable:

$$R_{ji} = \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) - \frac{1}{F} \frac{1}{(M-|\mathcal{S}|)(N-1)} \times \max_{k\in\mathcal{J},\mathcal{S}\subset\mathcal{I}} I(\mathbf{X}_{(\mathcal{J}-k)\times\mathcal{S}^c}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{S}^c}, \mathbf{X}_{\mathcal{J}\times\mathcal{S}}) \quad \forall (j,i) \in \mathcal{J}\times\mathcal{S}^c$$

Consider the term $I(\mathbf{X}_{(\mathcal{J}-k)\times\mathcal{S}^c}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{S}^c}, \mathbf{X}_{\mathcal{J}\times\mathcal{S}})$. Following similar analysis in Theorem 1, if $|\mathcal{S}| \leq M-2$, it can be shown that

$$\max_{k\in\mathcal{J},\mathcal{S}\subset\mathcal{I}} I(\mathbf{X}_{(\mathcal{J}-k)\times\mathcal{S}^c}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{S}^c}, \mathbf{X}_{\mathcal{J}\times\mathcal{S}}) = (N-1)(m+1)^\Gamma \log(P) + o(\log(P))$$

Therefore,

$$R_{ji} = \frac{1}{F}(\eta - \frac{(m+1)^\Gamma}{M-|\mathcal{S}|}) \log(P) + o(\log(P)) \quad \forall (j,i) \in \mathcal{J}\times\mathcal{S}^c$$

where $\eta = (m+1)^\Gamma$ when $i = 1$ and $\eta = m^\Gamma$ when $i = 2, 3, \ldots, M$. As $m \to \infty$,

$$R_{ji} = \frac{1}{M+N-1}(1 - \frac{1}{M-|\mathcal{S}|}) \log(P) + o(\log(P)) \quad \forall (j,i) \in \mathcal{J}\times\mathcal{S}^c$$

Therefore, each message can achieve $\frac{1}{M+N-1}(1 - \frac{1}{M-|\mathcal{S}|})$ secure degrees of freedom for a total of $\frac{N(M-|\mathcal{S}|-1)}{M+N-1}$ secure degrees of freedom under secrecy constraint 3.

Similarly, to satisfy secrecy constraint 4, we design an achievable scheme to satisfy the following constraint:

$$\frac{1}{nF} H(\mathbf{W}_{(\mathcal{J}-j)\times(\mathcal{S}^c-l)} | \bar{\mathbf{Y}}_j^n, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{S}}^n) \geq \sum_{(r,i)\in(\mathcal{J}-j)\times(\mathcal{S}^c-l)} R_{ri} - \epsilon \quad \forall \mathcal{S} \subset \mathcal{I},\ \forall l \in \mathcal{S}_I^c$$

Then it can be shown that the following secure rate is achievable:

$$R_{ji} = \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) - \frac{1}{F} \frac{1}{(M-|\mathcal{S}|-1)(N-1)} \times \max_{k\in\mathcal{J},l\in\mathcal{S}^c,\mathcal{S}\subset\mathcal{I}} I(\mathbf{X}_{(\mathcal{J}-k)\times(\mathcal{S}^c-l)}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{S}^c}, \mathbf{X}_{\mathcal{J}\times\mathcal{S}}) \quad \forall (j,i) \in \mathcal{J}\times\mathcal{S}^c$$

Following similar analysis in Theorem 2, if $|\mathcal{S}| \leq M-2$, it can be shown that

$$\max_{k\in\mathcal{J},l\in\mathcal{S}^c,\mathcal{S}\subset\mathcal{I}} I(\mathbf{X}_{(\mathcal{J}-k)\times(\mathcal{S}^c-l)}; \bar{\mathbf{Y}}_k | \mathbf{X}_{k\times\mathcal{S}^c}, \mathbf{X}_{\mathcal{J}\times\mathcal{S}}) = (N-1)((m+1)^\Gamma - m^\Gamma) \log(P) + o(\log(P))$$

Therefore,

$$R_{ji} = \frac{(M-|\mathcal{S}|-1)\eta - ((m+1)^\Gamma - m^\Gamma)}{F(M-|\mathcal{S}|-1)} \log(P) + o(\log(P)) \quad \forall (j,i) \in \mathcal{J}\times\mathcal{S}^c$$

where $\eta = (m+1)^\Gamma$ when $i = 1$ and $\eta = m^\Gamma$ when $i = 2, 3, \ldots, M$. As $m \to \infty$,

$$R_{ji} = \frac{1}{M+N-1} \log(P) + o(\log(P)) \ \forall (j,i) \in \mathcal{J}\times\mathcal{S}^c$$

Therefore, each message can achieve $\frac{1}{M+N-1}$ secure degrees of freedom for a total of $\frac{N(M-|\mathcal{S}|)}{M+N-1}$ secure degrees of freedom. ■

IV. The K user Gaussian interference channel with confidential messages

In this section, we consider the K user Gaussian interference channel with confidential messages. In [9], this interference channel with confidential messages is considered under secrecy constraint 1, i.e.,

$$\frac{1}{nF}H(\mathbf{W}_{(\mathcal{K}-j)}|\bar{\mathbf{Y}}_j^n) \geq \sum_{i\in(\mathcal{K}-j)} R_i - \epsilon \quad \forall j \in \mathcal{K} = \{1,2,\ldots,K\}$$

It is shown that each user can achieve $\frac{K-2}{2K-2}$ secure degrees of freedom. However, we consider the same channel under secrecy constraint 2, i.e.,

$$\frac{1}{nF}H(\mathbf{W}_{(\mathcal{K}-j-m)}|\bar{\mathbf{Y}}_j^n) \geq \sum_{i\in(\mathcal{K}-j-m)} R_i - \epsilon$$
$$\forall j,m \in \mathcal{K} = \{1,2,\ldots,K\}, j \neq m$$

and secrecy constraint 4, i.e.,

$$\frac{1}{nF}H(\mathbf{W}_{(\mathcal{S}^c-j-m)}|\bar{\mathbf{Y}}_j^n, \mathbf{W}_{\mathcal{S}}) \geq \sum_{i\in(\mathcal{S}^c-j-m)} R_i - \epsilon$$
$$\forall m \in \mathcal{S}^c,\ j \neq m,\ \forall \mathcal{S} \subset \mathcal{K} = \{1,2,\ldots,K\}$$

where $\mathcal{S}$ is the set of users that are compromised. Interestingly, we show that for these two scenarios, each message can achieve $\frac{1}{2}$ secure degrees of freedom which is the same as what one can achieve without secrecy constraint. We present the results in the following theorems:

Theorem 4: For the K user Gaussian interference channel with single antenna nodes, each user can achieve $\frac{1}{2}$ secure degrees of freedom for a total of $\frac{K}{2}$ secure degrees of freedom under secrecy constraint 2.

Proof: The proof is similar to the proof of Theorem 2 and is omitted here. ∎

Theorem 5: For the K user Gaussian interference channel with single antenna nodes, even if any subset of users, $\mathcal{S} \subset \{1,2,\ldots,K\}$ is compromised, then the remaining $K-|\mathcal{S}|$ users can still achieve $\frac{1}{2}$ secure degrees of freedom for each message for a total of $\frac{K-|\mathcal{S}|}{2}$ secure degrees of freedom as long as $|\mathcal{S}| < K-2$.

Proof: The proof is similar to the proof of Theorem 3 and is omitted here. ∎

V. Conclusion

In this work, we obtain the achievable secure degrees of freedom for the $M \times N$ user X network under different secrecy constraints. We also obtain the achievable secure degrees of freedom for the K user Gaussian interference channel under two different secrecy constraints. We can see another advantage of interference alignment, i.e., interference signals are aligned along the same dimensions to assist secrecy in wireless communications.

VI. Appendix

A. Proof of Theorem 1

Proof: Let $\Gamma = (N-1)(M-1)$ and $F = N(m+1)^\Gamma + (M-1)m^\Gamma, \forall m \in \mathbb{N}$. Over the F symbol extension channel, for each message W_{ji}, we generate $2^{nF(R_{ji}+R_{ji}^1+R_{ji}^2+\cdots+R_{ji}^{N-1}+R_{ji}^\dagger)}$ codewords each of length nm_i, where $m_1 = (m+1)^\Gamma$, $m_i = m^\Gamma, \forall i = 2,3,\ldots,M$. Each element of the codewords is i.i.d. $\sim \mathcal{CN}(0, \frac{P-\epsilon}{c})$ such that the power constraint is satisfied. We denote the codeword as

$$\mathbf{X}^n(w_{ji}, b_{ji}^1, b_{ji}^2, \ldots, b_{ji}^{N-1}, b_{ji}^\dagger) = [\mathbf{X}_{ji}(1) \ \cdots \ \mathbf{X}_{ji}(n)].$$

where $w_{ji} \in \{1,\ldots,2^{nFR_{ji}}\}$, $b_{ji}^k \in \{1,\ldots,2^{nFR_{ji}^k}\}, \forall k = 1,\cdots,N-1$, $b_{ji}^\dagger \in \{1,\ldots,2^{nFR_{ji}^\dagger}\}$ and $\mathbf{X}_{ji}(t)$ is an $m_i \times 1$ vector. This can be interpreted as the codebook is first partitioned into $2^{nFR_{ji}}$ message bins and then each bin is divided into $2^{nFR_{ji}^1}$ sub-bins which we refer to the first layer of sub-bins. Each sub-bin in the first layer is further divided into $2^{nFR_{ji}^2}$ sub-bins which comprise the second layer. Such partition is repeated until the $(N-1)^{th}$ layer. Each sub-bin in the last layer contains $2^{nFR_{ji}^\dagger}$ codewords. Hence, $w_{ji}, b_{ji}^1, \ldots, b_{ji}^{N-1}$ represent the message bin and the sub-bin indexes of the $k^{th}, \forall k = 1,\cdots,N-1$ layer respectively.

Now, to send a message w_{ji}, Transmitter i looks into the message bin w_{ji} and randomly selects a sub-bin b_{ji}^1 in the first layer, sub-bin b_{ji}^2 in the second layer and so on according to the uniform distribution. In the sub-bin of the last layer a codeword $b_{ji}^\dagger$ is chosen uniformly over $\{1,\ldots,2^{nFR_{ji}^\dagger}\}$. Here, it obtains a codeword $\mathbf{X}^n(w_{ji}, b_{ji}^1, \cdots, b_{ji}^{N-1}, b_{ji}^\dagger) = [\mathbf{X}_{ji}(1), \cdots, \mathbf{X}_{ji}(n)]$. For each time slot $t \in \{1,\ldots,n\}$, Transmitter i employs the interference alignment scheme mapping $\mathbf{X}_{ji}(t)$ to $\mathbf{V}_{ji}(t)\mathbf{X}_{ji}(t)$ where $\mathbf{V}_{ji}$ is the $F \times m_i$ matrix. At last, Transmitter i sends signal $\bar{\mathbf{X}}_i(t) = \sum_{j=1}^N \mathbf{V}_{ji}(t)\mathbf{X}_{ji}(t)$ into the channel. Note that the pre-coding matrices $\mathbf{V}_{ji}(t)$ are chosen as given in [11].

Without loss of generality, we assume

$$I(\mathbf{X}_{(\mathcal{J}-1)\times\mathcal{I}}; \bar{\mathbf{Y}}_1|\mathbf{X}_{1\times\mathcal{I}}) < I(\mathbf{X}_{(\mathcal{J}-2)\times\mathcal{I}}; \bar{\mathbf{Y}}_2|\mathbf{X}_{2\times\mathcal{I}})$$
$$< \cdots < I(\mathbf{X}_{(\mathcal{J}-N)\times\mathcal{I}}; \bar{\mathbf{Y}}_N|\mathbf{X}_{N\times\mathcal{I}})$$

where $\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}} = \{\mathbf{X}_{ri} : \forall (r,i) \in (\mathcal{J}-j)\times\mathcal{I}\}$ and $\mathbf{X}_{r\times\mathcal{I}} = \{\mathbf{X}_{ri} : \forall i \in \mathcal{I}\}$. We choose rates $R_{ji}, R_{ji}^1, \cdots, R_{ji}^{N-1}, R_{ji}^\dagger$ as follows

$$R_{ji} = \tfrac{1}{F}I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) - \tfrac{1}{F}\tfrac{1}{M(N-1)}I(\mathbf{X}_{(\mathcal{J}-N)\times\mathcal{I}}; \bar{\mathbf{Y}}_N|\mathbf{X}_{N\times\mathcal{I}})$$
$$R_{ji}^1 = \tfrac{1}{F}\tfrac{1}{M(N-1)}[I(\mathbf{X}_{(\mathcal{J}-N)\times\mathcal{I}}; \bar{\mathbf{Y}}_N|\mathbf{X}_{N\times\mathcal{I}})$$
$$-I(\mathbf{X}_{(\mathcal{J}-N+1)\times\mathcal{I}}; \bar{\mathbf{Y}}_{N-1}|\mathbf{X}_{(N-1)\times\mathcal{I}})]$$
$$\vdots$$

$$R_{ji}^{k} = \tfrac{1}{F}\tfrac{1}{M(N-1)} \times$$
$$[I(\mathbf{X}_{(\mathcal{J}-N+k-1)\times\mathcal{I}}; \bar{\mathbf{Y}}_{N-k+1}|\mathbf{X}_{(N-k+1)\times\mathcal{I}})$$
$$-I(\mathbf{X}_{(\mathcal{J}-N+k)\times\mathcal{I}}; \bar{\mathbf{Y}}_{N-k}|\mathbf{X}_{(N-k)\times\mathcal{I}})] \quad (7)$$
$$\vdots$$
$$R_{ji}^{N-1} = \tfrac{1}{F}\tfrac{1}{M(N-1)}[I(\mathbf{X}_{(\mathcal{J}-2)\times\mathcal{I}}; \bar{\mathbf{Y}}_{2}|\mathbf{X}_{2\times\mathcal{I}})$$
$$-I(\mathbf{X}_{(\mathcal{J}-1)\times\mathcal{I}}; \bar{\mathbf{Y}}_{1}|\mathbf{X}_{1\times\mathcal{I}})] \quad (8)$$
$$R_{ji}^{\dagger} = \tfrac{1}{F}\tfrac{1}{M(N-1)} I(\mathbf{X}_{(\mathcal{J}-1)\times\mathcal{I}}; \bar{\mathbf{Y}}_{1}|\mathbf{X}_{1\times\mathcal{I}})) - \epsilon \quad (9)$$

Note that $R_{ji} + R_{ji}^{1} + \cdots + R_{ji}^{\dagger} = \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) - \epsilon$. Next, we will show this scheme satisfies both the reliability requirement and the secrecy constraint.

Since $R_{ji} + R_{ji}^{1} + \cdots + R_{ji}^{\dagger} = \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) - \epsilon < \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j)$, each user can decode its desired streams reliably.

To ensure the secrecy constraint 1, we need to show

$$H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n) \geq \sum_{(r,i)\in(\mathcal{J}-j)\times\mathcal{I}} R_{ri} - \epsilon$$
$$\mathcal{J} = \{1, \ldots, N\},\ \mathcal{I} = \{1, \ldots, M\}$$

We consider the following equivocation lower bound

$$H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n) \geq H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n) \quad (10)$$

where the inequality is due to the fact that conditioning reduces entropy.

$$\begin{aligned} & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n) \\ = \ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n) - H(\bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n) \quad (11) \\ \geq \ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) - H(\bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n) \quad (12) \end{aligned}$$

where $\mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j} = \{\mathbf{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{1}, \mathbf{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{2}, \cdots, \mathbf{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{N-j}\}$ and $\mathbf{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{k} = \{B_{ri}^{k} : \forall (r,i) \in (\mathcal{J}-j)\times\mathcal{I}\}, \forall k = 1, \cdots, N-1$ denotes the set of all the sub-bin indexes of the k^{th} layer for all codewords $\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n$. B_{ri}^{k} denotes the sub-bin index in the k^{th} layer for codeword $\mathbf{X}_{ji}^n$ and is uniformly distributed over $\{1, \ldots, 2^{nFR_{ji}^{k}}\}$. Then, the first term of (12) can be written as

$$\begin{aligned} & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ = \ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ & - H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ = \ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ & + H(\bar{\mathbf{Y}}_j^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ & - H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ = \ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ & + H(\bar{\mathbf{Y}}_j^n|\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \mathbf{X}_{j\times\mathcal{I}}^n) \\ & - H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \end{aligned} \quad (13)$$

where

$$\begin{aligned} & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ = \ & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \end{aligned}$$

since $\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}$, $\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n$ are independent of $\mathbf{X}_{j\times\mathcal{I}}^n$, and

$$\begin{aligned} & H(\bar{\mathbf{Y}}_j^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ = \ & H(\bar{\mathbf{Y}}_j^n|\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \mathbf{X}_{j\times\mathcal{I}}^n) \end{aligned}$$

due to the Markov chain

$$(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \to (\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \mathbf{X}_{j\times\mathcal{I}}^n) \to \bar{\mathbf{Y}}_j^n$$

Hence, from (10), (12), (13), we obtain

$$\begin{aligned} & H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n) \\ & \geq H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ & + H(\bar{\mathbf{Y}}_j^n|\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \mathbf{X}_{j\times\mathcal{I}}^n) - H(\bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n) \\ & - H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ & \geq H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) - I(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n) \\ & - H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n), \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \end{aligned} \quad (14)$$

We now bound each term in (14). Consider the first term. Note that given the first to $(N-j)^{th}$ layers' sub-bin indexes, $\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n$ has $2^{nF\sum_{(r,i)\in\{\mathcal{J}-j\}\times\mathcal{I}}(R_{ri}^{N-j+1}+\cdots+R_{ri}^{N-1}+R_{ri}^{\dagger})}$ possible values with equal probability. Hence

$$\begin{aligned} & H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \\ & = nF \sum_{(r,i)\in(\mathcal{J}-j)\times\mathcal{I}} (R_{ri} + R_{ri}^{N-j+1} + \cdots + R_{ri}^{N-1} + R_{ri}^{\dagger}) \\ & = nF \sum_{(r,i)\in(\mathcal{J}-j)\times\mathcal{I}} R_{ri} + nI(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}; \bar{\mathbf{Y}}_j|\mathbf{X}_{j\times\mathcal{I}}) - \epsilon_1 \end{aligned} \quad (15)$$

where the last step follows from (7) and (9). $\epsilon_1 \to 0$ as $n \to \infty$. Second, we can bound

$$I(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n, \bar{\mathbf{Y}}_j^n|\mathbf{X}_{j\times\mathcal{I}}^n) \leq nI(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j|\mathbf{X}_{j\times\mathcal{I}}) + n\epsilon_2 \quad (16)$$

where $\epsilon_2 \to 0$ as $n \to \infty$. Finally, the third term can be bounded as follows

$$H(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n|\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}, \bar{\mathbf{Y}}_j^n, \mathbf{X}_{j\times\mathcal{I}}^n, \mathcal{B}_{(\mathcal{J}-j)\times\mathcal{I}}^{j}) \leq n\epsilon_3 \quad (17)$$

where $\epsilon_3 \to 0$ as $n \to \infty$. This is because Receiver j can decode the codeword $\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}^n$ given the message, the first to $(N-j)^{th}$ layers' sub-bin indexes and the observation $\bar{\mathbf{Y}}_j^n$. Then, Fano's inequality implies (17).

From (15), (16) and (17) , we can write (14) as

$$\begin{aligned} & \frac{1}{nF} H(\mathbf{W}_{(\mathcal{J}-j)\times\mathcal{I}}|\bar{\mathbf{Y}}_j^n) \\ & \geq \sum_{(r,i)\in(\mathcal{J}-j)\times\mathcal{I}} R_{ri} + \frac{1}{F} I(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}; \bar{\mathbf{Y}}_j|\mathbf{X}_{j\times\mathcal{I}}) \\ & - \frac{1}{F} I(\mathbf{X}_{(\mathcal{J}-j)\times\mathcal{I}}; \bar{\mathbf{Y}}_j|\mathbf{X}_{j\times\mathcal{I}}) - \epsilon_1 - \epsilon_2 - \epsilon_3 \end{aligned}$$

Hence, security condition is satisfied at Receiver j. Therefore, the following secrecy rate is achievable:

$$R_{ji} = \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) - \frac{1}{F} \frac{1}{M(N-1)} I(\mathbf{X}_{(\mathcal{J}-N)\times\mathcal{I}}; \bar{\mathbf{Y}}_N | \mathbf{X}_{N\times\mathcal{I}})$$

From [11], we have

$$I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) = \eta \log(P) + o(\log(P))$$

where $\eta = (m+1)^\Gamma$ when $i = 1$ and $\eta = m^\Gamma$ when $i = 2, 3, \ldots, M$. At each receiver, the interference vectors from Transmitter $2, 3 \ldots, M$ are aligned perfectly with the interference from Transmitter 1. Then, we have

$$I(\mathbf{X}_{(\mathcal{J}-N)\times\mathcal{I}}; \bar{\mathbf{Y}}_N | \mathbf{X}_{N\times\mathcal{I}}) = (N-1)(m+1)^\Gamma \log(P) + o(\log(P))$$

Hence,

$$\begin{aligned} R_{ji} &= \frac{1}{F} I(\mathbf{X}_{ji}; \bar{\mathbf{Y}}_j) - \frac{1}{F} \frac{1}{M(N-1)} I(\mathbf{X}_{(\mathcal{J}-N)\times\mathcal{I}}; \bar{\mathbf{Y}}_N | \mathbf{X}_{N\times\mathcal{I}}) \\ &= \frac{1}{F}(m+1)^\Gamma (1 - \frac{1}{M}) \log(P) + o(\log(P)) \quad i = 1 \end{aligned}$$

and

$$R_{ji} = \frac{1}{F}(m^\Gamma - \frac{(m+1)^\Gamma}{M}) \log(P) + o(\log(P)) \quad i = 2, \ldots, M$$

As $m \to \infty$, we have

$$\begin{aligned} R_{ji} &= \frac{M-1}{M(M+N-1)} \log(P) + o(\log(P)) \\ &\forall (j,i) \in \{1, \ldots, N\} \times \{1, 2, \ldots, M\} \end{aligned}$$

As a result, each message can achieve $\eta_{ji} = \frac{M-1}{M(M+N-1)}$ secure degrees of freedom. Therefore, for a total of MN messages, we can achieve a total of $\frac{N(M-1)}{M+N-1}$ secure degrees of freedom. The proof is complete. ■

REFERENCES

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

[2] Y. Liang, G. Kramer, H. V.Poor and S. Shamai, "Compound Wire-tap channels "in *Proc. Forth-Fifth Annual Allerton Conference*, Allerton House, Illinois, September 2007.

[3] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, July 2006, pp. 952–956.

[4] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, July 2006, pp. 957–961.

[5] E. Tekin, A. Yener, "The Gaussian Multiple Access Wire-Tap Channel" *submitted to IEEE Trans. on Information Theory*.

[6] I. Csiszar and J. Korner, " Broadcast channels with confidential messages," *IEEE Trans. Information Theory*, vol. IT-24, no.3, May 1978.

[7] R. Liu, I. Maric, P. Spasojevic and R.Yates, "Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions " in *IEEE Trans. on Information Theory*, vol. 54, June 2008.

[8] S.K.Leung-Yan-Cheong, M.E. Hellman, " The Gaussian Wire-tap Channel" in *IEEE Trans. Information Theory*, vol. IT-24, no.4, July 1978.

[9] O. O. Koyluoglu, H. El Gamal, L. Lai, H. V. Poor, "On the Secure Degrees of Freedom in the K-User Gaussian Interference Channel," in *Proceedings of the 2008 IEEE International Symposium on Information Theory*, Toronto, ON, Canada, July 6 - 11, 2008

[10] V. Cadambe and S. Jafar, "Interference Alignment and Degrees of Freedom of the K-User Interference Channel," *IEEE Trans. on Inform. Theory*, vol. 54, No.8, August 2008.

[11] V. Cadambe, S. Jafar, "Degrees of Freedom for Wireless X Networks," *Preprint available through http://newport.eecs.uci.edu/syed*,