On the Secure Degrees of Freedom of $2 \times 2 \times 2$ Multi-Hop Network with Untrusted Relays

Mohamed Seif Ravi Tandon Ming Li

Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ, USA.
E-mail: {*mseif, tandonr, lim*}@email.arizona.edu

***Abstract*—We study the impact of untrusted relays on the degrees of freedom of multi-antenna multi-hop networks. In particular, we consider the two user two-hop interference network, where two source nodes want to send independent messages securely to their designated receivers through the help of two untrusted relays. The relays are considered untrusted in terms of eavesdropping the messages sent by the sources. Moreover, we also assume that the messages are confidential, i.e., each receiver must not be able to decode the information meant for the other receiver. We assume that all the terminals (i.e., sources, relays, and the receivers) are equipped with multiple number of antennas. The goal of this work is to understand the secure degrees of freedom (SDoF) region of this multi-hop MIMO network under the two constraints of a) untrusted relays; and b) confidential messages. To cope with the untrusted nature of relays, we present achievable schemes in which both sources mix their information symbols with artificial noises so that the signals at each relay are completely immersed in the artificial noises space. However, this mixing must be done carefully, so as to ensure the feasibility of interference neutralization in the second hop to allow successful decoding at the respective destination. To this end, we devise transmission schemes based on interference alignment and interference neutralization techniques. The main contributions of this work are as follows: a) we present an upper bound on the SDoF region as a function of the number of antennas at the terminals, b) we present two achievable schemes, the first scheme is based on secure interference alignment and neutralization and is shown to be information theoretically optimal when all terminals have the same number of antennas; and a second scheme, based on secure sub-space alignment and neutralization, which is shown to be optimal for another specific antenna configuration. To the best of our knowledge, these are the first results on multi-hop MIMO relay networks with untrusted relays and confidential messages.**

Index Terms: Degrees of freedom (DoF), secrecy, secure degrees of freedom, multi-hop networks.

I. Introduction

Interference is considered as a fundamental barrier in wireless communications. Seminal works [1]–[3] were conducted to advance our understanding of the capacity of single-hop wireless networks and multi-hop networks. One of the seminal works in multi-hop networks is [4] where the authors studied the $2 \times 2 \times 2$ interference network in which there are two source nodes, two relays and two destinations, each equipped with a single antenna. It was shown in [4] that the cut-set bound of 2 DoF can be achieved using aligned interference neutralization. The authors in [5] extended the work of $2\times2\times2$ interference network to the case of MIMO setting, and showed the achievability of the cut-set bound using a combination of beamforming and aligned interference neutralization techniques. In [6], the authors generalized the work of the $2\times2\times2$ interference network in [4] into $K \times K \times K$ interference network, and it was shown that K DoF are achieved via aligned network diagonalization scheme.

Due to the nature of the wireless communications environment, secrecy is a challenging problem, especially due to the presence of eavesdroppers and/or unauthenticated nodes in the network. Information theoretic secrecy for wireless networks has been investigated for various channel models [7]–[9]. Seminal works studied the secrecy degrees of freedom in multi-hop networks (see, [10], [11]). The authors in [10] have studied the sum secure degrees of freedom for the two-unicast layered network with different number of hops and connection configurations. They assumed that each source node sends a message that is intended to its desired destination node and kept secure from the unintended receivers. In [11], a scenario was considered in which a source-destination pair are communicating only through an untrusted intermediate relay node. In their work, they imposed a cooperative jammer by deliberately making the jammer send artificial noises along with the information symbols from the source nodes to confuse the relay and hence protecting the legitimate receiver. In [12], the authors have studied this setup when there is an untrusted relay in the presence of external eavesdropper. Also, each source wants to send to the other a message and one of these messages is enforced to be secured at the untrusted relay. An achievable scheme based on rate splitting and stochastic encoding was devised for this network. To the best of our knowledge, the problem of multi-hop networks with untrusted relay(s) and confidential messages has not been settled yet.

The contributions of this paper are summarized as follows:
- First, we consider the (N_S, N_R, N_D) MIMO multi-hop network with N_S antennas at sources, N_R antennas at relays, N_D antennas at destinations. We present an upper bound on the SDoF region of the MIMO multi-hop network and show a matching scheme for certain antenna configurations.
- We then present an achievable scheme based on asymptotic secure interference alignment and interference neutralization to achieve the upper bound on the SDoF for the MIMO setting with antenna parameters: $(N_S, N_D, N_R) = (N_S, N, N)$ and

The work of M. Seif and R. Tandon was supported by the U.S. NSF through grants CCF-1559758 and CNS-1715947. The work of M. Seif and M. Li was supported in part by the U.S. NSF grant CNS-1564477, and ONR YIP grant N00014-16-1-2650.

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

$N \leq N_S$.

• Finally, we present another achievable scheme based on secure sub-space alignment along with interference neutralization for the MIMO setting $(N_S, N_D, N_R) = (N, N, N_R)$ and $N \leq N_R$. We show the optimality of this scheme when $N_R = \frac{4N}{3}$. The key distinction of the second scheme is that it is not asymptotic in nature (i.e., does not require channel extensions) and is still information-theoretically optimal for the above antenna configurations.

Notations: Boldface uppercase letters denote matrices and boldface lowercase letters are used for vectors. $\mathbb{C}$, $\mathbb{R}$ denote the complex and real domain, respectively. For a matrix $\mathbf{A}$ or a vector $\mathbf{a}$ their transpose are denoted by $\mathbf{A}^T$ and $\mathbf{a}^T$, respectively.

II. System Model

We consider a layered $2 \times 2 \times 2$ multi-hop network as shown in Fig. 1, where each source node S_i has a message W_i to its corresponding destination node D_i, $\forall i \in \{1, 2\}$. Each source node S_i has N_S antennas, each relay node R_i has N_R antennas and each destination has N_D antennas. We assume there are no direct links between the sources and destinations hence the messages from the sources are relayed over the relays $\{R_k\}_{k=1}^2$. In the first hop, the received signals at relays $\{R_k\}_{k=1}^2$ are as follows:

$$\mathbf{y}_{R_k}(t) = \mathbf{F}_{k1}(t)\mathbf{x}_1(t) + \mathbf{F}_{k2}(t)\mathbf{x}_2(t) + \mathbf{n}_{R_k}(t), \quad (1)$$

where $\mathbf{F}_{ij}(t) \in \mathbb{C}^{N_R \times N_S}$ represents the complex Gaussian channel coefficients of the first hop at time t between source node S_j and relay node R_i, $\mathbf{x}_i(t) \in \mathbb{C}^{N_S \times 1}$ is the transmitted signal from S_i and $\mathbf{n}_{R_k}(t) \in \mathbb{C}^{N_R \times 1}$ is the additive noise, which is assumed to be distributed i.i.d. over time, as circularly symmetric Gaussian with zero mean and unit variance. In the second hop, $\{R_k\}_{k=1}^2$ transmit symbols $\{\mathbf{x}_{R_k}\}_{k=1}^2$ to $\{D_k\}_{k=1}^2$. The received signal at D_k is given by:

$$\mathbf{y}_{D_k}(t) = \mathbf{G}_{k1}(t)\mathbf{x}_{R_1}(t) + \mathbf{G}_{k2}(t)\mathbf{x}_{R_2}(t) + \mathbf{n}_{D_k}(t), \quad (2)$$

where $\mathbf{G}_{ki}(t) \in \mathbb{C}^{N_D \times N_R}$ is the complex Gaussian channel coefficient for the second hop between relay node R_i and destination node D_k, and $\mathbf{n}_{D_k}(t) \in \mathbb{C}^{N_D \times 1}$ is the receiver circularly symmetric Gaussian noise with zero mean-unit variance at time slot t. In addition, the transmitted signals from the nodes have an average power constraint P. The relays are assumed to be full-duplex (i.e., the relays can transmit and receive signals at the same time but in different channels). We assume perfect channel state information about the time-varying channel coefficients at the transmitters, i.e. channel coefficients for receiver i are known instantaneously and without error. Specifically, the source nodes know the channels for the first hop only, relays know the channels for both hops, and destination nodes know the channels for the second hop only. We consider secrecy constraints in the network, such that the relays are enforced not to know the transmitted symbols from the source nodes $\{S_i\}_{i=1}^2$, and each destination D_i is considered as an eavesdropper for the symbols of the other destination D_j, $i \neq j$. The relays are untrusted in terms of eavesdropping the messages sent by the sources, but they are trusted in terms of honestly forwarding the information and correctly executing the communication protocol. Also, each destination is considered an eavesdropper for the messages intended for the other destination. A secure rate pair (R_1, R_2) is achievable if there exists a sequence of codes that satisfy the reliability constraints at the destinations such that:

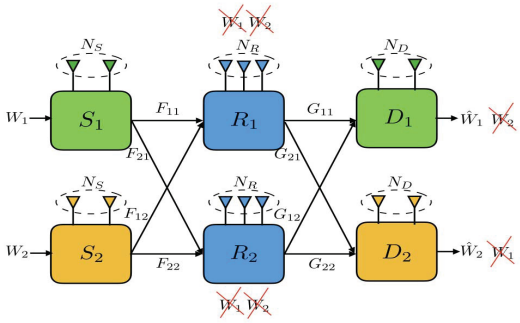


Fig. 1. System model for the $2 \times 2 \times 2$ multi-hop network with N_S antennas at sources (S_1, S_2), N_R antennas at relays (R_1, R_2) and N_D antennas at destinations (D_1, D_2). The relays are assumed to be untrustworthy and the message W_i must be securely delivered to the destination D_i $(i = \{1, 2\})$.

$$\Pr\left[\hat{W}_i \neq W_i\right] \leq \epsilon_n \quad (3)$$

and the secrecy constraints such that:

$$I\left(W_1, W_2; Y_{R_i}^n\right) \leq \epsilon_n, \ i = 1, 2, \quad (4)$$

$$I\left(W_i; Y_{D_j}^n\right) \leq \epsilon_n, \ i, j = 1, 2, i \neq j, \quad (5)$$

where n is the number of channel uses and $\epsilon_n \to 0$ as $n \to \infty$.

Let $R_i(P)$ denote the achievable secure rate of message W_i for a given transmission power P defined as $R_i(P) \triangleq \frac{\log_2(|\mathcal{W}_i|)}{n}$ where $|\mathcal{W}_i|$ is the cardinality of the message set. The secure degrees of freedom (SDoF) region $\mathcal{D}$ for the 2-user multi-hop network is defined as the set of all achievable pairs $(d_1, d_2) \in \mathbb{R}_+^2$ where,

$$d_i \triangleq \lim_{P \to \infty} \frac{R_i(P)}{\log_2(P)}, i = 1, 2 \quad (6)$$

is the degrees of freedom (DoF) for message W_i. The sum secure DoF of the network is defined as:

$$\text{SDoF}_{\text{sum}} \triangleq \max_{(d_1, d_2) \in \mathcal{D}} d_1 + d_2. \quad (7)$$

III. Main Results

In this section, we first present our result on the outer bound on the SDoF region $\mathcal{D}$ for the MIMO multi-hop network. We then present two special cases of antenna configurations and show their optimality of matching the outer bounds on the SDoF region $\mathcal{D}$. The first case is when $(N_S, N_D, N_R) = (N_S, N, N)$ and $N \leq N_S$. For this case, we devise our transmission scheme where we use asymptotic secure interference alignment and neutralization technique to keep the information symbols secured at the untrusted relays and the unintended receiver. The second case is when $(N_S, N_D, N_R) = (N, N, N_R)$ and $N \leq N_R$. For this case, we devise sub-space alignment and neutralization technique, and show the optimality of this scheme when $N_R = \frac{4N}{3}$.

Theorem 1: The SDoF region $\mathcal{D}$ for the $2 \times 2 \times 2$ multi-

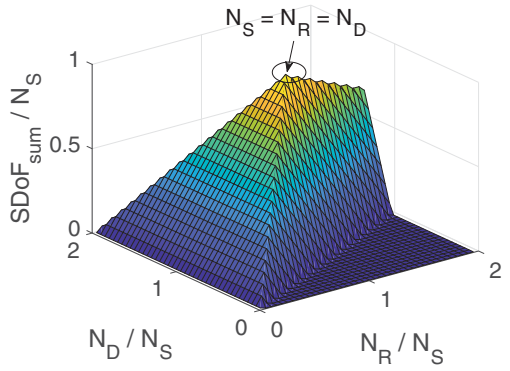


Fig. 2. The upper bound on SDoF_{sum} normalized by N_S vs $\frac{N_R}{N_S}$ and $\frac{N_D}{N_S}$ for the $2 \times 2 \times 2$ MIMO interference network. Maximum value of the SDoF_{sum} is attained when $N_S = N_R = N_D = N$.

hop interference network with N_S antennas at each source node S_i, N_R at each relay node R_i and N_D antennas at each destination node D_i is contained within the following region:

$$\mathcal{D}_{out} \triangleq \Big\{(d_1, d_2) \in \mathbb{R}_+^2 :$$
$$d_1 \leq \min(N_S, N_D, (2N_R - N_D)^+) \quad (8)$$
$$d_2 \leq \min(N_S, N_D, (2N_R - N_D)^+) \quad (9)$$
$$d_1 + d_2 \leq N_R \quad (10)$$
$$d_1 + d_2 \leq N_D + (N_R - N_D)^+ \quad (11)$$
$$d_1 + d_2 \leq (2N_S - N_R)^+ \Big\}, \quad (12)$$

where $(a)^+ \triangleq \max(0, a)$.

From the above outer bound, we can observe that the SDoF region is empty (i.e., positive secure degrees of freedom are infeasible) when either of the following conditions holds: $2N_R < N_D$ or $2N_S < N_R$. Fig. 2 depicts the upper bound on the SDoF_{sum}. The converse proof of this Theorem is provided in Section IV.

Remark 1: We take a special case when $N_D = N_R = N$, i.e., we consider the case when the destinations and the relays have the same number of antennas. For this special case, the outer bound on SDoF region of Theorem 1 simplifies to the following region(s) depending on the relative value of N_S compared to N:

- Case (a): $N \leq N_S$

$$d_1 + d_2 \leq N. \quad (13)$$

- Case (b): $N > N_S$

$$d_1 \leq N_S, \quad (14)$$
$$d_2 \leq N_S, \quad (15)$$
$$d_1 + d_2 \leq 2N_S - N. \quad (16)$$

Next, we show that the outer bound is optimal for Case (a).

Theorem 2: The SDoF region $\mathcal{D}$ for the $2 \times 2 \times 2$ MIMO multi-hop interference network with $(N_S, N_D, N_R) = (N_S, N, N)$ and $N \leq N_S$ is the set of non-negative pairs (d_1, d_2) such that:

$$d_1 + d_2 \leq N. \quad (17)$$

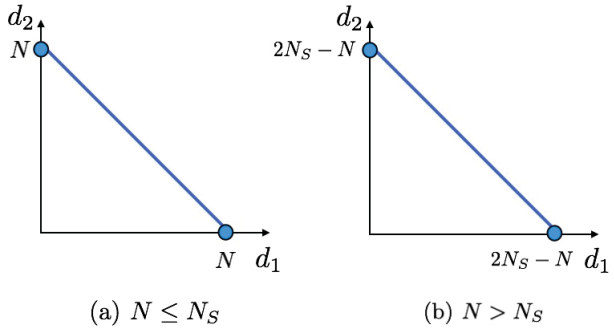


Fig. 3. Upper bounds for SDoF regions from Theorem 1 for the special case $(N_S, N_D, N_R) = (N_S, N, N)$ and two sub-cases: (a) $N \leq N_S$, (b) $N > N_S$. For case (a), Theorem 2 shows the optimality for this bound. Characterizing the optimal SDoF region for case (b) remains open.

To prove the above result, we show the achievability of the SDoF pair $(d_1, d_2) = (0, N)$ through the aligned interference neutralization scheme in Section V. The converse follows from Theorem 1. The resulting outer bounds for both the cases are shown in Fig. 3. We show in Section V that the outer bound for Case (a) is indeed optimal and can be achieved by a matching scheme.

Theorem 3: The achievable SDoF region $\mathcal{D}_{in}$ for the $2 \times 2 \times 2$ multi-hop interference network with $(N_S, N_D, N_R) = (N, N, N_R)$ and $N \leq N_R$ is

$$d_1 + d_2 = 2 \min \left\{ \frac{N}{3}, 3N - 2N_R \right\}. \quad (18)$$

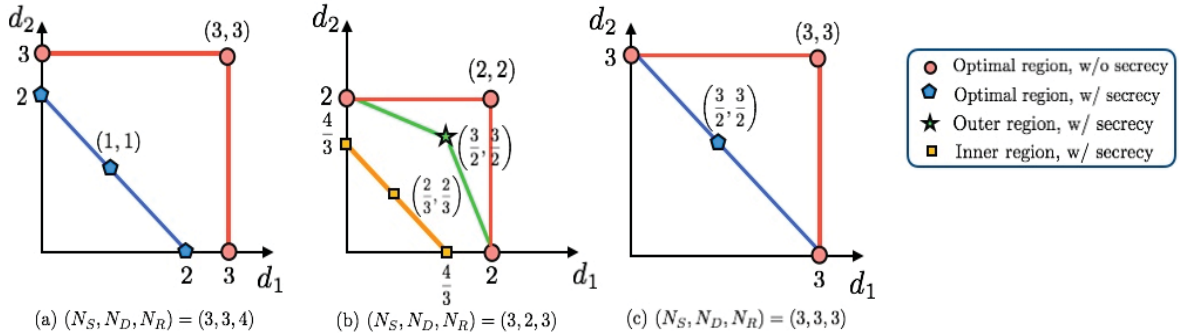
The proof of this Theorem is presented in Section VI.

Remark 2: It is worth noting that the achievable SDoF region $\mathcal{D}$ coincides with the outer bound on SDoF region $\mathcal{D}_{out}$ when either $\frac{2N}{3}$ or $2(3N - 2N_R)$ equal $2N - N_R$ which holds for both cases when $N_R = \frac{4N}{3}$.

Fig. 4 shows a comparison between DoF regions with different antennas configurations with the case of no secrecy [5] and with secrecy constraints. We see that the SDoF region is diminished because of the secrecy constraints in the network. In Fig. 4 (a), the optimal SDoF region is achieved by secure sub-space alignment and neutralization. In Fig. 4 (b), the inner bound on the SDoF region achieved by secure sub-space alignment and neutralization does not match with the outer bound for this setting. In Fig. 4 (c), the optimal SDoF region is achieved by asymptotic interference alignment and neutralization (Theorem 3).

IV. Proof of Theorem 1

The outer bounding mechanism works as follows: we take information cuts (i.e., a partition of nodes that separates source(s) and respective destination(s)) across the multi-hop network, and bound the information theoretic quantities, while accounting for a) the secrecy and confidentiality constraints;



(a) $(N_S, N_D, N_R) = (3,3,4)$ (b) $(N_S, N_D, N_R) = (3,2,3)$ (c) $(N_S, N_D, N_R) = (3,3,3)$

Fig. 4. Comparison between non-secure and secure DoF regions for different antenna configurations (N_S, N_D, N_R).

b) the number of antennas at all terminals; and c) the decoding constraints at the destinations. Now we will prove each constraint in the outer bound SDoF region $\mathcal{D}_{\text{out}}$.

• Constraint (8): We first note that the bound $d_1 \leq \min(N_S, N_D)$ follows trivially from cut-set arguments. Hence, we provide the proof of $d_1 \leq (2N_R - N_D)^+$. We upper bound the rate of user 1 by using Fano's inequality as follows:

$$\begin{aligned} nR_1 &\leq I(W_1; X_{R_1}^n, X_{R_2}^n) + n\epsilon_n, \\ &\leq I(W_1; X_{R_1}^n, X_{R_2}^n, Y_{D_2}^n) + n\epsilon_n, \\ &\overset{(a)}{\leq} I(W_1; X_{R_1}^n, X_{R_2}^n | Y_{D_2}^n) + n\epsilon_n, \\ &\leq h(X_{R_1}^n, X_{R_2}^n | Y_{D_2}^n) + n\epsilon_n, \\ &\overset{(b)}{\leq} n(2N_R - N_D)^+ \log(P) + n\epsilon_n, \end{aligned}$$

where (a) follows from the confidentiality constraint for message W_1, and (b) follows from the fact that the Gaussian distribution maximizes the entropy and the pre-log $n(2N_R - N_D)^+$ comes from the following argument: Given $Y_{D_2}^n$ in the conditioning (or N_D equations in $2N_R$ variables per time slot), the remaining degrees of freedom of the term $(X_{R_1}^n, X_{R_2}^n)$ can be readily upper bounded by $(2N_R - N_D)^+$. Hence, we have the proof of $d_1 \leq \min(N_S, N_D, (2N_R - N_D)^+)$. Similarly, for constraint (9), it can be shown that $d_2 \leq \min(N_S, N_D, (2N_R - N_D)^+)$.

• Constraint (10): To prove this bound, we start by upper bounding the sum rate by using Fano's inequality as follows:

$$\begin{aligned} n(R_1 + R_2) &\leq I(W_1, W_2; Y_{R_1}^n, Y_{R_2}^n) + n\epsilon_n, \\ &= I(W_1, W_2; Y_{R_1}^n) + I(W_1, W_2; Y_{R_2}^n | Y_{R_1}^n) + n\epsilon_n, \\ &\overset{(a)}{\leq} \epsilon_n + h(Y_{R_2}^n | Y_{R_1}^n) - h(Y_{R_2}^n | W_1, W_2, Y_{R_1}^n) + n\epsilon_n, \\ &\leq (n+1)\epsilon_n + h(Y_{R_2}^n), \\ &\leq (n+1)\epsilon_n + nN_R \log(P), \end{aligned} \tag{19}$$

where (a) follows from the secrecy constraint at the untrusted relay 1. Dividing (19) by n and letting $n \to \infty$, we have

$$R_1 + R_2 \leq N_R \log(P). \tag{20}$$

Subsequently, dividing (20) by $\log(P)$ and letting $P \to \infty$, we have $d_1 + d_2 \leq N_R$.

• Constraint (11): To prove this bound, we start by bounding the sum rate as follows:

$$\begin{aligned} n(R_1 + R_2) &\leq I(W_1, W_2; Y_{D_1}^n, Y_{R_2}^n, X_{R_1}^n) + n\epsilon_n, \\ &\overset{(a)}{\leq} I(W_1, W_2; Y_{D_1}^n, Y_{R_2}^n | X_{R_1}^n) + n\epsilon_n, \\ &= h(Y_{D_1}^n, Y_{D_2}^n | X_{R_1}^n) \\ &\quad - h(Y_{D_1}^n, Y_{D_2}^n | X_{R_1}^n, W_1, W_2) + n\epsilon_n, \\ &\leq h(Y_{D_1}^n, Y_{D_2}^n | X_{R_1}^n) + n\epsilon_n, \\ &= h(Y_{D_1}^n | X_{R_1}^n) + h(Y_{D_2}^n | X_{R_1}^n, Y_{D_1}^n) + n\epsilon_n, \\ &\overset{(b)}{\leq} nN_D \log(P) + n(N_R - N_D)^+ \log(P) + n\epsilon_n, \end{aligned}$$

where (a) follows from the secrecy constraint at untrusted relay 1, and (b) follows from the fact that the Gaussian distribution maximizes the entropy and the pre-log N_D comes from the fact that given $X_{R_1}^n$, the number of equations in $X_{R_1}^n$ at D_1 is N_D. For the second term, given $(X_{R_1}^n, Y_{D_1}^n)$, the remaining degrees of freedom in $Y_{D_2}^n$ are upper bounded by $(N_R - N_D)^+$. Taking the limits $n \to \infty$, and $P \to \infty$, we arrive at (11).

• Constraint (12): To prove this bound, we start by bounding the sum rate as follows:

$$\begin{aligned} n(R_1 + R_2) &\leq I(W_1, W_2; X_{S_1}^n, X_{S_2}^n, Y_{R_1}^n) + n\epsilon_n, \\ &\overset{(a)}{\leq} I(W_1, W_2; X_{S_1}^n, X_{S_2}^n | Y_{R_1}^n) + n\epsilon_n, \\ &\leq h(X_{S_1}^n, X_{S_2}^n | Y_{R_1}^n) + n\epsilon_n, \\ &\overset{(b)}{\leq} n(2N_S - N_R)^+ \log(P) + n\epsilon_n, \end{aligned}$$

where (a) follows from secrecy constraint at the untrusted relay 1, and (b) follows from the fact that given $Y_{R_1}^n$, the remaining degrees of freedom in $(X_{S_1}^n, X_{S_2}^n)$ are upper bounded by $(2N_S - N_R)^+$. Hence, taking the limits $n \to \infty$, and $P \to \infty$, we have the proof of (12).

V. Proof of Theorem 2

In this section, we give an achievable scheme to achieve the points $\mathbf{P}_1 = (N, 0)$ and $\mathbf{P}_2 = (0, N)$ in Fig. 3(a). Motivated by the work of [4], we introduce our transmission scheme. In particular, it is sufficient to show the achievability of point $\mathbf{P}_2$, i.e. $(d_1, d_2) = (0, N)$ is achievable. The other point $\mathbf{P}_1$ is achievable by the reversing the roles of the transmitters. Any point between $\mathbf{P}_1$ and $\mathbf{P}_2$ is then achievable via time sharing. We show that for the point $\mathbf{P}_2$, the pair $(d_1, d_2) = (0, \frac{NL-1}{L})$ is achievable where L is the number of symbol extensions of the channel. Hence by taking $L \to \infty$, we achieve $(d_1, d_2) = (0, N)$. Our scheme is divided into

two parts: Over the first hop, we devise a secure interference alignment scheme, in which we align the transmitted signals along with artificial noises at the relays such that the relays can not infer any of these information signals. Over the second hop of the network, we perform secure interference neutralization, in which the relays carefully transmit the signals such that the unintended signals are cancelled out at that unintended destination.

I. Achieving $(d_1, d_2) = (0, N)$: [1]

When considering L symbol extension of the network, the effective channel coefficients for the two hops can be written as:

$$\tilde{\mathbf{F}}_{kj} = \text{blkdiag}(\mathbf{F}_{kj}(1), \mathbf{F}_{kj}(2), \ldots, \mathbf{F}_{kj}(L)), \quad (21)$$

$$\tilde{\mathbf{G}}_{kj} = \text{blkdiag}(\mathbf{G}_{kj}(1), \mathbf{G}_{kj}(2), \ldots, \mathbf{G}_{kj}(L)), \quad (22)$$

where $\tilde{\mathbf{F}}_{kj}$ and $\tilde{\mathbf{G}}_{kj}, k, j \in \{1, 2\}$ are block diagonal matrices of dimensions $NL \times NL$.

Let the transmitted symbols of sources $S_i, i \in \{1, 2\}$ be as follows:

$$\mathbf{s}_1 = [n_1 \quad n_2 \quad \ldots \quad n_{NL-1} \quad n_{NL}]^T_{NL\times 1}, \quad (23)$$

$$\mathbf{s}_2 = [b_1 \quad b_2 \quad \ldots \quad b_{NL-2} \quad b_{NL-1}]^T_{NL-1\times 1}, \quad (24)$$

where $\{b_i\}_{i=1}^{NL-1}$ are the information symbols sent from S_2, and $\{n_i\}_{i=1}^{NL}$ are the artificial noises[2] sent from S_1. Source node S_1 sends $s_1(i)$ along with precoding vector $\mathbf{v}_{1,i} \in \mathbb{C}^{NL\times 1}, i \in \{1, \ldots, NL\}$, also S_1. Source node S_2 sends $s_2(i)$ along with precoding vector $\mathbf{v}_{2,i} \in \mathbb{C}^{NL\times 1}, i \in \{1, \ldots, NL-1\}$. Then, the transmitted signal from source S_1 is as follows:

$$\mathbf{x}_1 = [\mathbf{v}_{1,1} \quad \mathbf{v}_{1,2} \quad \ldots \quad \mathbf{v}_{1,NL}]\, \mathbf{s}_1. \quad (25)$$

Similarly, source node S_2 sends $s_2(i)$ along with precoding vector $\mathbf{v}_{2,i} \in \mathbb{C}^{NL\times 1}, i \in \{1, \ldots, NL-1\}$. Then, the transmitted signal from source S_2 is:

$$\mathbf{x}_2 = [\mathbf{v}_{2,1} \quad \mathbf{v}_{2,2} \quad \ldots \quad \mathbf{v}_{2,NL-1}]\, \mathbf{s}_2. \quad (26)$$

Now we design the precoding vectors at the source nodes $\{S\}_{i=1}^{2}$ in the following subsection.

1) Secure Interference Alignment conditions:

$$\tilde{\mathbf{F}}_{11}\mathbf{v}_{1,i+1} = \tilde{\mathbf{F}}_{12}\mathbf{v}_{2,i}, \quad (27)$$

$$\tilde{\mathbf{F}}_{21}\mathbf{v}_{1,i} = \tilde{\mathbf{F}}_{22}\mathbf{v}_{2,i}. \quad (28)$$

We align the $(i+1)^{\text{th}}$ element of $\mathbf{x}_1$ with the i^{th} element of $\mathbf{x}_2$. As a result, the artificial noises from sources S_1 will be aligned with the information symbols sent from S_2 at relay R_1 except for the first element of $\mathbf{x}_1$ then this element must be an artificial noise. Similarly, for relay R_2, the i^{th} element of $\mathbf{x}_1$ is aligned with the i^{th} element of $\mathbf{x}_2$ except for the last element of $\mathbf{x}_1$. From conditions (27) and (28), we can write the precoding vectors $\mathbf{v}_{1,i}$ and $\mathbf{v}_{2,i}, \forall i \in \{1, \ldots, NL-1\}$ as:

$$\mathbf{v}_{i+1,1} = \left(\tilde{\mathbf{F}}_{11}^{-1}\tilde{\mathbf{F}}_{12}\tilde{\mathbf{F}}_{22}^{-1}\tilde{\mathbf{F}}_{21}\right)^{i} \mathbf{v}_{1,1}, \quad (29)$$

$$\mathbf{v}_{2,i} = \left(\tilde{\mathbf{F}}_{22}^{-1}\tilde{\mathbf{F}}_{21}\tilde{\mathbf{F}}_{11}^{-1}\tilde{\mathbf{F}}_{12}\right)^{i-1} \tilde{\mathbf{F}}_{22}^{-1}\tilde{\mathbf{F}}_{21}\mathbf{v}_{1,1}, \quad (30)$$

where $\mathbf{v}_{1,1} \in \mathbb{R}^n$ is chosen to be all one vector. Note that as proved in [4], it can be easily verified that $\{\mathbf{v}_{1,i}\}_{i=1}^{NL}$ (and$\{\mathbf{v}_{2,i}\}_{i=1}^{NL-1}$as well) are linearly independent (see Section III. A in [4]). Now the received signal at relay R_1 will be:

$$\begin{aligned}\mathbf{y}_{R_1} &= \tilde{\mathbf{F}}_{11}\mathbf{x}_1 + \tilde{\mathbf{F}}_{12}\mathbf{x}_2, \\ &= \tilde{\mathbf{F}}_{11}\mathbf{v}_{1,1}x_{1,1} + \sum_{i=1}^{NL-1} \tilde{\mathbf{F}}_{11}\mathbf{v}_{1,i+1}(x_{1,i+1} + x_{2,i}). \quad (31)\end{aligned}$$

Similarly, for R_2, we have

$$\begin{aligned}\mathbf{y}_{R_2} &= \tilde{\mathbf{F}}_{21}\mathbf{x}_1 + \tilde{\mathbf{F}}_{22}\mathbf{x}_2, \\ &= \sum_{i=1}^{NL-1} \tilde{\mathbf{F}}_{21}\mathbf{v}_{1,i}(x_{1,i} + x_{2,i}) + \tilde{\mathbf{F}}_{21}\mathbf{v}_{1,NL}x_{1,NL}. \quad (32)\end{aligned}$$

Then each relay R_i will multiply the received signal with the inverse of the effective channel F_{R_i} to transmit in the second hop as follows:

$$\mathbf{x}_{R_1} = \tilde{\mathbf{F}}_{R_1}^{-1}\mathbf{y}_{R_1} = [n_1 \quad b_1 + n_2 \quad \ldots \quad b_{NL-1} + n_{NL}]^T,$$

where $\tilde{\mathbf{F}}_{R_1} = \left[\tilde{\mathbf{F}}_{11}\mathbf{v}_{1,1} \quad \tilde{\mathbf{F}}_{11}\mathbf{v}_{1,2} \quad \ldots \quad \tilde{\mathbf{F}}_{11}\mathbf{v}_{1,NL}\right]$ and

$$\begin{aligned}\mathbf{x}_{R_2} &= \tilde{\mathbf{F}}_{R_2}^{-1}\mathbf{y}_{R_2}, \\ &= [b_1 + n_1 \quad b_2 + n_2 \quad \ldots \quad b_{NL-1} + n_{NL-1} \quad n_{NL}]^T,\end{aligned}$$

where $\tilde{\mathbf{F}}_{R_2} = \left[\tilde{\mathbf{F}}_{21}\mathbf{v}_{1,1} \quad \tilde{\mathbf{F}}_{21}\mathbf{v}_{1,2} \quad \ldots \quad \tilde{\mathbf{F}}_{21}\mathbf{v}_{1,NL}\right]$.

Fig. 5 shows an example for $L = 6$ symbol extensions and $N = 1$ antenna. Source node S_1 sends artificial noises $\{n_i\}_{i=1}^{6}$ while source node S_2 sends information symbols $\{b_i\}_{i=1}^{5}$. The resulting alignment of artificial noises at both the relays are illustrated in the figure. Now we design the precoding vectors at the relay nodes $\{R\}_{i=1}^{2}$ in the following subsection.

2) Secure Interference Neutralization Conditions:

$$\tilde{\mathbf{G}}_{11}\mathbf{v}_{R_1,i+1} = -\tilde{\mathbf{G}}_{12}\mathbf{v}_{R_2,i}, \quad (33)$$

$$\tilde{\mathbf{G}}_{21}\mathbf{v}_{R_1,i} = -\tilde{\mathbf{G}}_{22}\mathbf{v}_{R_2,i}, \quad (34)$$

Now we neutralize $\{b_i\}_{i=1}^{NL-1}$ at destination D_1, similarly for D_2, we neutralize the contributions of $\{n_i\}_{i=1}^{NL}$. From conditions (33) and (34), we can write the precoding vectors $\mathbf{v}_{R_1,i}$ and $\mathbf{v}_{R_2,i}, \forall i \in \{1, \ldots, NL-1\}$ as:

$$\mathbf{v}_{R_1,i+1} = -\left(\tilde{\mathbf{G}}_{11}^{-1}\tilde{\mathbf{G}}_{12}\tilde{\mathbf{G}}_{22}^{-1}\tilde{\mathbf{G}}_{21}\right)^{i} \mathbf{v}_{R_1,1}, \quad (35)$$

$$\mathbf{v}_{R_2,i} = -\left(\tilde{\mathbf{G}}_{22}^{-1}\tilde{\mathbf{G}}_{21}\mathbf{G}_{11}^{-1}\tilde{\mathbf{G}}_{12}\right)^{i-1} \tilde{\mathbf{G}}_{22}^{-1}\tilde{\mathbf{G}}_{21}\mathbf{v}_{R_1,1}, \quad (36)$$

where $\mathbf{v}_{R_1,1} \in \mathbb{R}^{NL\times 1}$ is chosen to be all one vector. Note that as proved in [4], it can be shown that $\{\mathbf{v}_{R_1,i}\}_{i=1}^{NL}$ $\left(\{\mathbf{v}_{R_2,i}\}_{i=1}^{NL-1}\text{as well}\right)$ are linearly independent

[1] Each source node uses $\min(N, N_s) = N$ antennas to transmit its data symbols. Hence, $\mathbf{F}_{kj}(n) \in \mathbb{C}^{N\times N}, \forall n = 1, \ldots, N$.

[2] The artificial noises $\{n_i\}_{i=1}^{NL}$ are chosen as i.i.d. Gaussian distribution with power P.

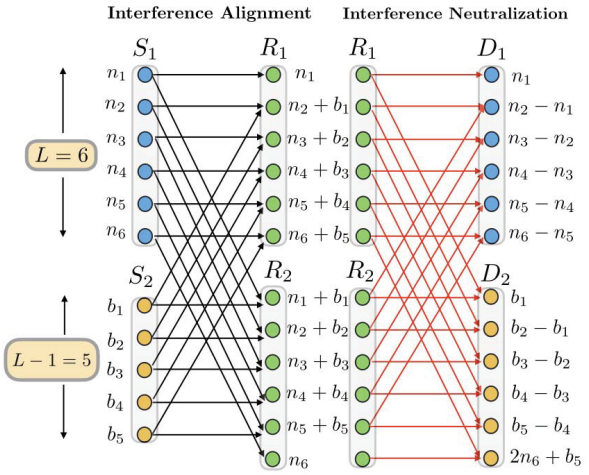


Fig. 5. A proposed scheme achieves $\text{SDoF}_{\text{sum}} = \frac{L-1}{L} = \frac{5}{6}$ with $L = 6$ symbol extensions and $N_S = N = 1$ antenna. D_1 receives only artificial noises and D_2 is able to decode $(b_1, \ldots, b_5)$.

(see Section III. A in [4]). The received signal at D_1 is

$$\begin{aligned}\mathbf{y}_{D_1} &= \tilde{\mathbf{G}}_{11}\mathbf{x}_{R_1} + \tilde{\mathbf{G}}_{12}\mathbf{x}_{R_2},\\ &= \tilde{\mathbf{G}}_{11}\mathbf{v}_{R_1,1}x_{1,1}\\ &\quad + \sum_{i=1}^{NL-1} \tilde{\mathbf{G}}_{11}\mathbf{v}_{R_1,i+1}\left(x_{1,i+1} - x_{1,i}\right). \end{aligned} \tag{37}$$

Thus, due to secure neutralization, destination D_1 only sees the contribution due to artificial noises, and has no contribution from the information symbols intended for destination D_2. Also, the received signal at D_2 is as follows:

$$\begin{aligned}\mathbf{y}_{D_2} &= \tilde{\mathbf{G}}_{21}\mathbf{x}_{R_1} + \tilde{\mathbf{G}}_{22}\mathbf{x}_{R_2},\\ &= \tilde{\mathbf{G}}_{21}\mathbf{v}_{R_1,NL}\left(x_{1,NL} + x_{2,NL-1}\right)\\ &\quad + \sum_{i=1}^{NL-1} \tilde{\mathbf{G}}_{22}\mathbf{v}_{R_2,i}\left(x_{2,i} - x_{2,i-1}\right). \end{aligned} \tag{38}$$

Similarly, D_2 can decode $x_{2,1}$ and subtract it from the second element to decode $x_{2,2}$ and so on to decode all the messages successively. It is worth mentioning that aligned interference neutralization scheme satisfies the decodability and preserves the secrecy for both destinations $\{D_i\}_{i=1}^2$ [4]. Fig. 5 shows the required neutralization conditions in order to make sure that destination D_2 decodes its information symbols while destination D_1 receives only noises. The achievable SDoF_{sum} for this example is $5/6$. To sum up, by applying the previous scheme we can achieve almost surely $d_1 + d_2 = \frac{NL-1}{L} \underset{L\to\infty}{\longrightarrow} N$.

II. Secrecy constraints validation at relays:

In this subsection, we prove that the proposed scheme preserves the secrecy constraints at relays. Let $\vec{B} = (b_1, b_2, \ldots, b_{NL-1})$. Then,

$$\begin{aligned} I(\vec{B}; Y_{R_1}) &= h(Y_{R_1}) - h(Y_{R_1}|\vec{B}), && (39)\\ &\leq \sum_{i=1}^{L} h\left(Y_{R_1(i)}\right) - NL\log(P), && (40)\\ &\leq NL\log(P) + o(\log(P)) - NL\log(P), && (41)\\ &= o(\log(P)). && (42)\end{aligned}$$

In the next section, we present our achievable scheme for MIMO setting $(N_S, N_D, N_R) = (N, N, N_R)$ and $N \leq N_R$.

VI. Proof of Theorem 3

Each transmitter transmits signals of dimension $3N_S - 2N_R$, where $\mathbf{a}$ and $\mathbf{b}$ are the information symbols sent from transmitter 1 and 2, respectively. $\{\mathbf{u}_i\}_{i=1}^2$ and $\{\mathbf{w}_i\}_{i=1}^2$ are the cooeprative jammer signals transmitted from transmitter 1 and 2, respectively. The transmitted signals are:

$$\mathbf{x}_1 = \mathbf{V}_1\mathbf{a} + \mathbf{V}_2\mathbf{u}_1 + \mathbf{V}_3\mathbf{u}_2, \tag{43}$$
$$\mathbf{x}_2 = \mathbf{V}_4\mathbf{b} + \mathbf{V}_5\mathbf{w}_1 + \mathbf{V}_6\mathbf{w}_2. \tag{44}$$

For the first hop, we precode these signals such that the information symbols of one transmitter lies in the same subspace as the cooperative jamming of the other transmitter at both relays. Hence, we can write the received signals at relays as:

$$\begin{aligned}\mathbf{y}_{R_1} &= (\mathbf{F}_{11}\mathbf{V}_1\mathbf{a} + \mathbf{F}_{12}\mathbf{V}_5\mathbf{w}_1) + (\mathbf{F}_{11}\mathbf{V}_2\mathbf{u}_1 + \mathbf{F}_{12}\mathbf{V}_4\mathbf{b})\\ &\quad + \mathbf{F}_{11}\mathbf{V}_3\mathbf{u}_2 + \mathbf{F}_{12}\mathbf{V}_6\mathbf{w}_2, && (45)\\ \mathbf{y}_{R_2} &= (\mathbf{F}_{21}\mathbf{V}_1\mathbf{a} + \mathbf{F}_{22}\mathbf{V}_6\mathbf{w}_2) + (\mathbf{F}_{21}\mathbf{V}_3\mathbf{u}_2 + \mathbf{F}_{22}\mathbf{V}_4\mathbf{b})\\ &\quad + \mathbf{F}_{21}\mathbf{V}_2\mathbf{u}_1 + \mathbf{F}_{22}\mathbf{V}_5\mathbf{w}_1. && (46)\end{aligned}$$

The precoding matrices are chosen such that

$$\text{span}\{\mathbf{F}_{11}\mathbf{V}_1\} \subseteq \text{span}\{\mathbf{F}_{12}\mathbf{V}_5\}, \tag{47}$$
$$\text{span}\{\mathbf{F}_{11}\mathbf{V}_2\} \subseteq \text{span}\{\mathbf{F}_{12}\mathbf{V}_4\}, \tag{48}$$
$$\text{span}\{\mathbf{F}_{21}\mathbf{V}_1\} \subseteq \text{span}\{\mathbf{F}_{22}\mathbf{V}_6\}, \tag{49}$$
$$\text{span}\{\mathbf{F}_{21}\mathbf{V}_3\} \subseteq \text{span}\{\mathbf{F}_{22}\mathbf{V}_4\}. \tag{50}$$

The solution to the previous conditions (47) and (49) can be obtained by solving the following equations,

$$\begin{bmatrix}\mathbf{F}_{11} & -\mathbf{F}_{12} & \mathbf{0}_{N_R\times N_S}\\ \mathbf{F}_{21} & \mathbf{0}_{N_R\times N_S} & -\mathbf{F}_{22}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1\\ \mathbf{V}_5\\ \mathbf{V}_6\end{bmatrix} = \mathbf{0}_{2N_R\times(3N_S-2N_R)}. \tag{51}$$

Similarly for conditions (48) and (50), the solution can be obtained as:

$$\begin{bmatrix}\mathbf{F}_{11} & \mathbf{0}_{N_R\times N_S} & -\mathbf{F}_{12}\\ \mathbf{0}_{N_R\times N_S} & \mathbf{F}_{21} & -\mathbf{F}_{22}\end{bmatrix}\begin{bmatrix}\mathbf{V}_2\\ \mathbf{V}_3\\ \mathbf{V}_4\end{bmatrix} = \mathbf{0}_{2N_R\times(3N_S-2N_R)}. \tag{52}$$

In order to decode the received signals at the relays, the total dimensions at each relay $4\times(3N_S - 2N_R)$ should be at most N_R and hence after decoding these signals, each user's signal is protected at each relay. For the second hop, each relay R_i will multiply the received signal with the inverse of the effective channel $\mathbf{F}_{R_i}$, then each relay will have the following

signals:

$$\mathbf{x}_{R_1} = \mathbf{F}_{R_1}^{-1}\mathbf{y}_{R_1}, \tag{53}$$

$$= [\mathbf{a}+\mathbf{w}_1 \quad \mathbf{u}_1+\mathbf{b} \quad \mathbf{u}_2 \quad \mathbf{w}_2]^T, \tag{54}$$

where $\mathbf{F}_{R_1} = [\mathbf{F}_{11}\mathbf{V}_1 \quad \mathbf{F}_{11}\mathbf{V}_4 \quad \mathbf{F}_{11}\mathbf{V}_3 \quad \mathbf{F}_{12}\mathbf{V}_6]$ and for R_2 as:

$$\mathbf{x}_{R_2} = \mathbf{F}_{R_2}^{-1}\mathbf{y}_{R_2}, \tag{55}$$

$$= [\mathbf{a}+\mathbf{w}_2 \quad \mathbf{u}_2+\mathbf{b} \quad \mathbf{u}_1 \quad \mathbf{w}_1]^T, \tag{56}$$

where $\mathbf{F}_{R_2} = [\mathbf{F}_{21}\mathbf{V}_1 \quad \mathbf{F}_{21}\mathbf{V}_3 \quad \mathbf{F}_{21}\mathbf{V}_2 \quad \mathbf{F}_{22}\mathbf{V}_5]$. For the second hop, each relay will transmit the following:

$$\mathbf{x}_{R_1} = \tilde{\mathbf{V}}_1(\mathbf{a}+\mathbf{w}_1) + \tilde{\mathbf{V}}_4\mathbf{u}_2 + \tilde{\mathbf{V}}_5\mathbf{w}_3, \tag{57}$$

$$\mathbf{x}_{R_2} = \tilde{\mathbf{V}}_2\mathbf{w}_1 + \tilde{\mathbf{V}}_3(\mathbf{u}_2+\mathbf{b}). \tag{58}$$

where $\mathbf{w}_3$ is an artificial noise generated at R_1. For the second hop, we precode these signals such that one receiver gets its information symbols cleanly after neutralizing its associated artificial noise while keeping the unintended signals for that receiver secured by making them lie in the subspace of the artificial noise. Hence, the received signals at destinations are written as:

$$\begin{aligned}\mathbf{y}_{D_1} &= (\mathbf{G}_{11}\tilde{\mathbf{V}}_1(\mathbf{a}+\mathbf{w}_1) + \mathbf{G}_{12}\tilde{\mathbf{V}}_2\mathbf{w}_1) \\ &\quad + (\mathbf{G}_{11}\tilde{\mathbf{V}}_5\mathbf{w}_3 + \mathbf{G}_{12}\tilde{\mathbf{V}}_3(\mathbf{u}_2+\mathbf{b})) + \mathbf{G}_{11}\tilde{\mathbf{V}}_4\mathbf{u}_2, \end{aligned}\tag{59}$$

$$\begin{aligned}\mathbf{y}_{D_2} &= (\mathbf{G}_{22}\tilde{\mathbf{V}}_3(\mathbf{u}_2+\mathbf{b}) + \mathbf{G}_{21}\tilde{\mathbf{V}}_4\mathbf{u}_2) \\ &\quad + (\mathbf{G}_{21}\tilde{\mathbf{V}}_5\mathbf{w}_3 + \mathbf{G}_{22}\tilde{\mathbf{V}}_2\mathbf{w}_1) + \mathbf{G}_{21}\tilde{\mathbf{V}}_1(\mathbf{a}+\mathbf{w}_1). \end{aligned}\tag{60}$$

The precoding matrices are chosen such that

$$\text{span}\{\mathbf{G}_{11}\tilde{\mathbf{V}}_1\} \subseteq \text{span}\{-\mathbf{G}_{12}\tilde{\mathbf{V}}_2\}, \tag{61}$$

$$\text{span}\{\mathbf{G}_{22}\tilde{\mathbf{V}}_3\} \subseteq \text{span}\{-\mathbf{G}_{21}\tilde{\mathbf{V}}_4\}, \tag{62}$$

$$\text{span}\{\mathbf{G}_{21}\tilde{\mathbf{V}}_5\} \subseteq \text{span}\{\mathbf{G}_{22}\tilde{\mathbf{V}}_2\}, \tag{63}$$

$$\text{span}\{\mathbf{G}_{11}\tilde{\mathbf{V}}_5\} \subseteq \text{span}\{\mathbf{G}_{12}\tilde{\mathbf{V}}_3\}. \tag{64}$$

The design of the precoders can be determined as follows:

$$\tilde{\mathbf{V}}_5 \to \tilde{\mathbf{V}}_2 \to \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_5 \to \tilde{\mathbf{V}}_3 \to \tilde{\mathbf{V}}_4, \tag{65}$$

where $\tilde{\mathbf{V}}_5$ is chosen randomly and $\tilde{\mathbf{V}}_2$ ($\tilde{\mathbf{V}}_3$ as well) can be obained afterwards. After obtaining $\tilde{\mathbf{V}}_2$ and $\tilde{\mathbf{V}}_3$, $\tilde{\mathbf{V}}_1$ can be determined as function of $\tilde{\mathbf{V}}_2$, similary $\tilde{\mathbf{V}}_4$ is determined as a function of $\tilde{\mathbf{V}}_3$. It is worth noting that these condtions have a solution when $N_D \leq N_R$. The achievable SDoF_{sum} for this scheme is

$$d_1 + d_2 = 2\min\left\{\frac{N_D}{3}, 3N_S - 2N_R\right\}. \tag{66}$$

Then after presenting the achievable scheme for a general setting, we take the special MIMO case $(N_S, N_D, N_R) = (N, N, N_R)$ and $N \leq N_R$. For this case, we obtain the following achievable SDoF_{sum}

$$d_1 + d_2 = 2\min\left\{\frac{N}{3}, 3N - 2N_R\right\}. \tag{67}$$

This completes the proof of Theorem 3.

VII. Conclusion

In this paper, we studied the $2 \times 2 \times 2$ multi-hop network with untrusted relays and confidential messages. We first presented an outer bound on the SDoF region for the MIMO multi-hop network with arbitrary number of antennas. We devised achievable schemes under certain antenna configurations based on the ideas of a) secure interference alignment and b) secure subspace alignment along with interference neutralization techniques. We are currently investigating the problem in full generality with arbitrary number of antennas. An interesting open problem is to characterize the secure DoF region for all remaining antenna configurations.

References

[1] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow: A deterministic approach," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1872–1905, Mar. 2011.

[2] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3425–3441, Jul. 2008.

[3] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3457–3470, Jul. 2008.

[4] T. Gou, S. A. Jafar, C. Wang, S.-W. Jeon, and S.-Y. Chung, "Aligned interference neutralization and the degrees of freedom of 2×2×2 interference channel," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4381–4395, Mar. 2012.

[5] C. S. Vaze and M. K. Varanasi, "Beamforming and aligned interference neutralization achieve the degrees of freedom region of the 2×2×2 MIMO interference network," in *Information Theory and Applications Workshop (ITA)*, Apr. 2012, pp. 199–203.

[6] I. Shomorony and A. S. Avestimehr, "Degrees of freedom of two-hop wireless networks: Everyone gets the entire cake," *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 2417–2431, Mar. 2014.

[7] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[8] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, Jan. 1978.

[9] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2647–2661, Mar. 2015.

[10] ——, "Sum secure degrees of freedom of two-unicast layered wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1931–1943, Aug. 2013.

[11] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *IEEE Global Communications Conference (GLOBECOM)*, Dec. 2008.

[12] A. A. Zewail and A. Yener, "Two-hop untrusted relay channel with an external eavesdropper under layered secrecy constraints," in *IEEE Global Communications Conference (GLOBECOM)*, Feb. 2016.