Secure Degrees of Freedom of Two-User Two-Hop X-Channel

Bardiya Barari, Pedram Kheirkhah Sangdeh, and Bahareh Akhbari

Faculty of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran.
Email:{B.barari, Kheirkhah}@email.kntu.ac.ir; Akhabri@kntu.ac.ir

***Abstract*—In this paper, Secure Degrees of Freedom (SDoF) of two-user two-hop X-channel is investigated. We consider a situation in this channel in which the transmitters and one of the relays benefit from alternating Channel State Information (CSI) including perfect, delayed and no CSI. In another regime from CSI viewpoint, we consider blind transmitters alongside a relay having access to alternating CSI, and there exists feedback from one of the receivers to the relay. For this situation, we also study the case in which the receivers are permitted to cooperatively play a part in ensuring secrecy. Corresponding to each case, we drive an upper bound on SDoF and devise a scheme which successfully obtains the upper bound. So, we present the optimal SDoF and achievable schemes for all considered cases.**

***Index Terms*—Secure Degrees of Freedom; Alternating Channel State Information; Two-User Two-Hop X-channel.**

I. Introduction

Secrecy should be put in the focal point of view for any practical wireless communication system due to vulnerability of wireless medium to malicious attacks, eavesdropping, etc. Variety of fields, like cryptography, signal processing, and information theory, have made remarkable advances to afford reliable and secure data transmission. Consequently, several methods for transmission of confidential messages have been contrived in recent literature such as cooperative jamming, artificial noise transmission, Interference Alignment (IA), to name but a few [1].

In line with growing size of wireless networks in wide spectrum of application, exploring the fundamental limits in multi-user multi-hop networks has become one of the greatest concern in information theory. In this regard, numerous researches deal with secure capacity of these network [2]. However, obtaining the exact secrecy capacity of these networks confronts several challenges. Hence, Secure Degree of Freedom (SDOF) that is the behavior of the secrecy capacity in the high Signal-to-Noise Ratio (SNR) regime offers a valuable tool to study the asymptotic performance of networks in high SNR. In [3], Xie *et al.* have calculated SDoF of several one-hop multi-user wireless networks in which Channel State Information at Transmitter (CSIT) is perfectly available. As an outstanding result, they have proved that SDoF of Gaussian wiretap channel with M helpers is $\frac{M}{M+1}$ for almost all channels. In addition, they have shown that SDoF of Gaussian broadcast channel with confidential messages and M helper is one. In [3], a k-user Gaussian multiple access channel has also been studied, and it has been proved that the optimal SDoF of this channel is $\frac{k(k-1)}{k(k-1)+1}$. In [4], authors have investigated $M \times K$ user X-channel with perfect CSIT. They have proved that the achievable sum-SDOF of this channel is upper-bounded by $\frac{K(M-1)}{K+M-2}$. Furthermore, they have shown that this bound is achievable with integrating interference alignment and artificial noise transmission for $K = M = 2$.

For investigating the information-theoretic limits of multi-hop networks including Degrees of Freedom (DoF) and SDoF, the two-user two-hop wireless network, which is named $2\times2\times2$ for brevity, attracted many attention in the recent decade [5]–[9]. In [5], the authors have considered $2\times2\times2$ when transmitters have not access to perfect CSIT. They have shown that if the relays know certain kinds of side-information while the transmitters are blind, $\frac{4}{3}$ DoF is optimal which equals to optimal DoF of the case in which delayed CSIT is provided. Sangdeh *et al.* have investigated similar conditions for $2\times2\times2$ X-Channel in [6], and they have presented upper bounds on achievable DoF and schemes capable to reach these bounds. Secrecy of several two-user multi-hop networks including $2\times2\times2$ have been studied in [7], in which it has been proved that if perfect CSIT is available in $2\times2\times2$ interference channel SDoF equals to two is achievable almost surely.

Unfortunately, the assumption of perfect and instantaneous CSIT may be too optimistic as CSIT may be delayed, imprecise or unavailable at all in practice. To meet this challenging issue, in [8], authors have considered the same network under two scenarios where transmitters know delayed CSIT, and in another case, they are blind whereas one relay knows CSI and the received signal of one destination with a finite delay. They have shown that optimal SDoF pair for these cases are $(\frac{1}{2}, \frac{1}{2})$. Despite these traditional works which hold a constant view about the state of CSI over time, assumption of alternating CSI opens door for devising and studying networks under more pragmatic conditions since the state of wireless links experiences drastic changes over time due to some random phenomenon in surrounding area. In [10], two-user Multiple-Input Single-Output (MISO) Broadcast Channel with Confidential Messages (BCCM) with alternating CSIT has been considered. Regarding to CSI related to each receiver, overall CSIT's state alternates between nine possible states, and these states occur for arbitrary fractions of time, except for a mild condition of symmetry. Then, the optimal SDoF region of this general model has been characterized. To achieve this region, authors have provided some new optimal achievable

978-1-5090-5963-8/17/$31.00

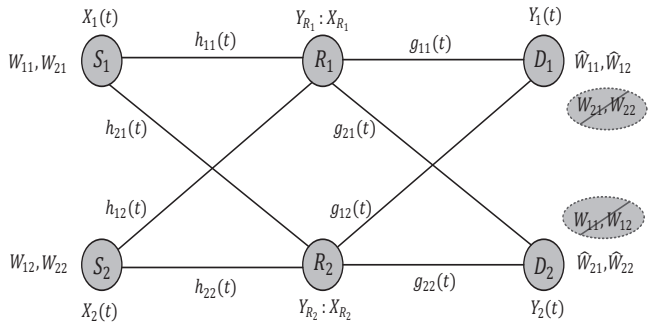

Fig. 1. Two-user two-hop SISO X-channel with confidential messages.

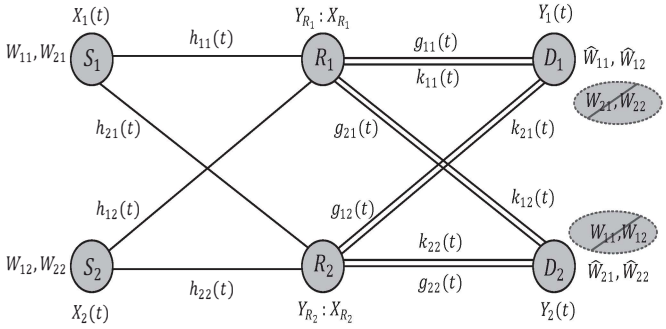

Fig. 2. Two-user two-hop SISO X-channel with cooperative receivers and confidential messages.

schemes for different alternating CSIT patterns and illustrated synergistic benefits of coding across the different alternating states under security constraints.

In pursuing aforementioned trend, a 2×2×2 X-channel with alternating CSI is considered in this paper. First, we assume that the transmitters and one of the relays know alternating CSI without any feedback from the receivers to relays. In the second scenario, the transmitters are completely ignorant about CSIT while one of the relays has alternating CSI and it also benefits from a delayed feedback from one of the receivers. In addition, we consider situation in which receivers play role of helpers to assure secrecy. We drive optimal SDoF and related achievable schemes for all cases. The proposed schemes combine IA technique with artificial noise transmission to reach the optimal SDoF. In these schemes, IA assists the destinations in recovering their desired messages while artificial noises ensure secrecy at both destinations.

The rest of paper is organized as follows. In Section II, we describe the system model in details including network's structure and CSI regime. In Section III, we state our main results, and we present our methods for different cases which achieve optimal sum-SDoF in Section IV. Finally, we conclude the paper in Section V.

II. System Model

In this section, we describe the network model and investigate CSI regimes in details. In the rest of paper, two-user two-hop X-channel is named 2×2×2-X for brevity. As depicted in Fig. 1, 2×2×2-X consists of two sources, two destinations, and two trusted relays. D_i, R_i, and S_i $(i = 1, 2)$ stand for the i^{th} destination, i^{th} relay, and i^{th} source, respectively. In the first hop, the channel coefficient between R_i and S_j in the t_1^{th} time slot is denoted by $h_{ij}(t_1)$. Similarly, $g_{ij}(t_2)$ indicates the channel coefficient between D_i and R_j in the t_2^{th} time slot. There are no direct links between destinations and sources, and each source wishes to send a message to each destination via intermediate nodes, i.e. relays. In fact, S_i intends to send W_{ji} to D_j. In the t_1^{th} time slot, S_i generates $X_i(t_1)$ based on its messages and transmits it over the network. Then, the i^{th} relay receives following signal.

$$Y_{R_i}(t_1) = h_{i1}X_1(t_1) + h_{i2}X_2(t_1); \quad i = 1, 2. \tag{1}$$

It is worth noting, we omit noise in our analysis since we intend to investigate the asymptotic behavior of network in pretty high SNRs. In the t_2^{th} time slot of the second hop, R_i which is a full-duplex relay produces $X_{R_i}(t_2)$, based on its received signals in the past time slots, and sends it. Hence, $Y_i(t_2)$ is received by the i^{th} destination.

$$Y_i(t_2) = g_{i1}X_{R_1}(t_2) + g_{i2}X_{R_2}(t_2); \quad i = 1, 2. \tag{2}$$

Also, there is an average power constraint P on $X_{R_i}(t)$ and $X_i(t)$.

$$\mathbb{E}\left[X_i^2(t_1)\right] \leq P; \forall i, t_1. \tag{3}$$

$$\mathbb{E}\left[X_{R_i}^2(t_2)\right] \leq P; \forall i, t_2. \tag{4}$$

We also consider the cooperation of destinations in assuring secrecy. In such a situation, we encounter to the network model depicted in Fig. 2. In this network, $k_{ij}(t_2)$ stands for the link from D_j to R_i in the t_2^{th} time slot of the second hop. In this model, a destination sends a signal toward relays in appropriate time slots, and $X_{Y_i}(t_2)$ demonstrates the signal sent by D_i in the t_2^{th} time slot. In both networks, all channel coefficients, i.e. $\mathbf{H}_{t_1} = \{h_{ij}(t_1)\}_{i,j}$, $\mathbf{G}_{t_2} = \{g_{ij}(t_2)\}_{i,j}$, and $\mathbf{K}_{t_2} = \{k_{ij}(t_2)\}_{i,j}$ are scalars with complex normal distributions with zero mean and unit variance $\mathcal{CN}(0, 1)$ and they are i.i.d over i, j, t_1 and t_2.

In the networks some nodes have access to alternating CSI which varies between nine possible states regarding to three possible CSI's state of each hop. In these states, P, D, and N mean perfect, delayed and no CSI, respectively. So, the overall side information of each node can be explained by a pair of them, and a sequence of these pairs clarifies the CSI of each nodes over different time slots. Based on the introduced network models and available CSI in different nodes, we represent three following cases which are studied in the rest of paper.

A. Case 1

As the first case, we consider the first model when alternating CSI with (DD, NN, NN, NN) pattern is available at both sources. Therefore, sources know CSI of the first and second hop within a finite delay. For this case and consequent cases, it is assumed that this finite delay equals one time slot. So,

sources know $h_{ij}(1)$ and $g_{ij}(1)$ at the beginning of the second time slot whereas CSI of subsequent time slots are unavailable at sources through next time slots. We also assume that one of the relays is stronger and knows alternating CSI while the other one is totally blind. Without loss of generality, we assume that R_1 is the strong relay and has access to alternating CSI with (NN, ND, DN, PP) pattern.

B. Case 2

Once again, we assume the first model while the sources and R_2 are blind. R_1 knows alternating CSI with (DD, DD, NN, NN) pattern. In addition, there is a feedback from D_1 to R_1, and R_1 knows the received signal by the first destination within a unit delay.

C. Case 3

As the last case, we investigate the network represented in Fig. 2. In this case, alternating CSI with (DD, NN, NN) pattern is available at R_1 while R_2 and sources know nothing about CSI of both hops during different time slots. Also, the strong relay knows $Y_1(t_2)$ at the beginning of the $(t_2+1)^{th}$ time slot.

In all cases, we intend to devise approaches such that each destination recovers its confidential messages successfully while it is unable to extract the messages related to the other destination. We use two following definitions in the rest of paper.

Definition 1: A secrecy rate tuple $(R_{11}, R_{12}, R_{21}, R_{22})$ is achievable if there exists a sequence of codes for $W_{ij} \in \{1, 2, \dots 2^{R_{ij}}\}$ $i, j \in \{1, 2\}$, which satisfies the following constraints at the destinations.

$$Pr\left(\hat{W}_{ij} \neq W_{ij}\right) \leq \epsilon_n, \forall i, j \in \{1, 2\} \tag{5}$$

$$\frac{I(W_{11}, W_{12}; Y_2^n, \mathbf{H}^n, \mathbf{G}^n)}{n} \leq \epsilon_n \tag{6}$$

$$\frac{I(W_{21}, W_{22}; Y_1^n, \mathbf{H}^n, \mathbf{G}^n)}{n} \leq \epsilon_n \tag{7}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Also, $\mathbf{H}^n$ and $\mathbf{G}^n$ indicate global CSI of the first and second hop during n channel uses, respectively and $I(\ ;\ )$ is mutual information between its arguments. Informally, (5) is the reliability constraint at destinations, and the constraints in (6) and (7) ensure that the information leakage per channel use of each destination's messages at another one should be arbitrarily small.

Definition 2: If a rate tuple $(R_{11}, R_{12}, R_{21}, R_{22})$ is achievable for a certain power P, the sum-SDoF d is said to be achieved with definition

$$d = \lim_{P \to \infty} \frac{\sum_{(i,j) \in \{1,2\}^2} R_{ij}}{\log(P)}. \tag{8}$$

III. Main Results

Through following theorems, we state the main results corresponding to presented cases.

Theorem 1: For the channel introduced as Case 1, the maximum achievable sum-SDoF is one.

proof: We express the proof with notations which have been used in [10]. First, it is assumed that relays fully cooperate with each other, and sources send their messages to relays non-casually. Obviously, this assumption does not degrade the secrecy capacity of the original channel. Moreover, the secrecy capacity of the new network is upper bounded by the second hop which acts as a two-user MISO BCCM with alternating CSI given by (NN, ND, DN, PP). It has been shown in [10] that sum-SDoF of two-user MISO BCCM with alternating CSIT is upper bounded by the following equation.

$$\textit{Sum-SDoF} = 2\lambda_P + \lambda_D + \min(\lambda_D, \lambda_N) \tag{9}$$

where λ_P, λ_D, and λ_N are defined as follows.

$$\lambda_P = \lambda_{PP} + \lambda_{PD} + \lambda_{PN} \tag{10}$$

$$\lambda_D = \lambda_{PD} + \lambda_{DD} + \lambda_{DN} \tag{11}$$

$$\lambda_N = \lambda_{PN} + \lambda_{DN} + \lambda_{NN} \tag{12}$$

In (10)-(12), $\lambda_{I_1 I_2}$ indicates the fraction of the time in which $I_1 I_2$ occurs. Hence, according to given alternating pattern above (i.e, (NN, ND, DN, PP)), $\lambda_P = \lambda_D = \frac{1}{4}$ and $\lambda_N = \frac{1}{2}$. If we substitute these values in (9), it clearly could be seen that the sum-SDoF equals one. So, the maximum achievable sum-SDoF in Case 1 is upper bounded by one. Through the next section, we propose a scheme which attains this bound successfully, and this completes the proof.■

Theorem 2: The optimal sum-SDoF of the network introduced as Case 2 is one.

proof:Similar to proof of converse of Theorem 1, we consider enhanced network with assuming full cooperation between two relays while they non-casually know messages of sources. The feedback does not increase the SDoF more than considering fully cooperation. Again the secrecy capacity of the original network is upper bounded by new network which is limited to the second hop. By these assumptions the second hop turns into a two-user MISO BCCM with alternating CSI given by (DD, DD, NN, NN) pattern. Based on (10)-(12), we can compute $\lambda_D = \lambda_N = \frac{1}{2}$ and $\lambda_P = 0$. Then, the optimal sum-SDoF of the second hop is one which is the upper-bound of maximum achievable sum-SDoF in Case 2. This upper-bound is obtained via a scheme presented in Section IV-B, and it proves the optimal sum-SDoF of Case 2 is one.■

Theorem 3: The optimal sum-SDoF of 2×2×2-X under circumstances of Case 3 is $\frac{4}{3}$.

Proof: An immediate upper-bound for the sum-SDoF of the network considered as Case 3 is $\frac{4}{3}$. This comes from the fact that our original network is upper bounded by sum-DoF of 2×2×2-X network with limited Shannon feedback which has been introduced in [5]. The results of [5] and [6] show that optimal sum-DoFs of 2×2×2 and 2×2×2-X with limited Shannon feedback are the same and equals $\frac{4}{3}$, and this constitutes an upper bound for the sum-SDoF of our intended case. It should be mentioned that in the 2×2×2-X with limited Shannon feedback, sources are blind; however, the relays know global CSI and signals received by corresponding destinations with a finite delay. Based on this definition, Case 3 experiences

a weaker regime than that of limited Shannon feedback since the strong relay does not access to CSI of the first hop in Case 3; besides, it knows the CSI of the second hop in alternating pattern given by (DD, NN, NN) which clearly contains less information than (DD, DD, DD). In the following section, we propose a scheme enabling us to reach $\frac{4}{3}$ sum-SDoF ■.

IV. Proposed Methods

In this section, we explain proposed schemes to attain optimal sum-SDoF posed in Theorems 1, 2, and 3. In the schemes, artificial noise transmission and interference alignment are combined in order to enable receivers to decode their intended messages reliably and securely. Through the schemes, u_i denotes the confidential message of S_i for D_1, and v_i indicates confidential message for D_2 sent from S_i. The artificial noises, but not confidential messages, are shared among transmitters.

A. Optimal scheme for Case 1

Based on available CSI at different nodes in Case 1, we propose a scheme consisting of four time slots through which each node acts as follows. Also, we denote the i^{th} time slot in the j^{th} hop by $TiHj$.

T1H1: S_i sends n_i which is an artificial noise. Based on noises and channel coefficients R_i receives $Y_{R_i}(1)$ as:

$$Y_{R_i}(1) = h_{i1}(1)n_1 + h_{i2}(1)n_2 \tag{13}$$

T1H2: Relays forward their received signals in $T1H1$ toward destinations. Hence, D_i receives $Y_i(1)$ as:

$$\begin{aligned} Y_i(1) = &\left(g_{i1}(1)h_{11}(1) + g_{i2}(1)h_{21}(1)\right) n_1 + \\ &\left(g_{i1}(1)h_{12}(1) + g_{i2}(1)h_{22}(1)\right) n_2 \triangleq l_i \end{aligned} \tag{14}$$

where l_i is a linear combination of artificial noises which is received by D_i.

T2H1: At the beginning of this time slot, sources know CSI of the first time slot in both hops. So, they calculate l_1 and l_2. Then, S_i transmits $l_1 + u_i$ and the relays receive the following signal.

$$Y_{R_i}(2) = h_{i1}(2)(u_1 + l_1) + h_{i2}(2)(u_2 + l_1) \tag{15}$$

T2H2: Once again, relays forward the signals received in the same time slot of the first hop.

$$\begin{aligned} Y_i(2) = &\left(g_{i1}(2)h_{11}(2) + g_{i2}(2)h_{21}(2)\right)(u_1 + l_1) + \\ &\left(g_{i1}(2)h_{12}(2) + g_{i2}(2)h_{22}(2)\right)(u_2 + l_1) \end{aligned} \tag{16}$$

T3H1:S_i transmits $v_i + l_2$ in this phase, and R_i receives the following signal.

$$Y_{R_i}(3) = h_{i1}(3)(v_1 + l_2) + h_{i2}(3)(v_2 + l_2) \tag{17}$$

T3H2: Relays forward the received signals in *T3H1*. So, D_i receives $Y_i(3)$ as:

$$\begin{aligned} Y_i(3) = &\left(g_{i1}(3)h_{11}(3) + g_{i2}(3)h_{21}(3)\right)(v_1 + l_2) + \\ &\left(g_{i1}(3)h_{12}(3) + g_{i2}(3)h_{22}(3)\right)(v_2 + l_2) \end{aligned} \tag{18}$$

T4H1: In this time slot of the first hop, sources remain silent and send nothing.

T4H2: In the last time slot, signals should be designed such that each destination attains one additional equation of its intended messages without introducing new interference. Therefore, R_1 transmits $X_{R_1}(4) = \alpha Y_{R_1}(2) + \beta Y_{R_1}(3)$, and R_2 sends $X_{R_2}(4) = Y_{R_2}(2) + Y_{R_2}(3)$. In other words, the strong relay assists destinations in recovering their intended confidential messages via choosing proper values for α and β. At the end of this time slot, destinations receive the following signals.

$$\begin{aligned} Y_1(4) = &\left(\alpha g_{11}(4)h_{11}(2) + g_{12}(4)h_{21}(2)\right)(u_1 + l_1) + \\ &\left(\alpha g_{11}(4)h_{12}(2) + g_{12}(4)h_{22}(2)\right)(u_2 + l_1) + \\ &\left(\beta g_{11}(4)h_{11}(3) + g_{12}(4)h_{21}(3)\right)(v_1 + l_2) + \\ &\left(\beta g_{11}(4)h_{12}(3) + g_{12}(4)h_{22}(3)\right)(v_2 + l_2) \end{aligned} \tag{19}$$

$$\begin{aligned} Y_2(4) = &\left(\alpha g_{21}(4)h_{11}(2) + g_{22}(4)h_{21}(2)\right)(u_1 + l_1) + \\ &\left(\alpha g_{21}(4)h_{12}(2) + g_{22}(4)h_{22}(2)\right)(u_2 + l_1) + \\ &\left(\beta g_{21}(4)h_{11}(3) + g_{22}(4)h_{21}(3)\right)(v_1 + l_2) + \\ &\left(\beta g_{21}(4)h_{12}(3) + g_{22}(4)h_{22}(3)\right)(v_2 + l_2) \end{aligned} \tag{20}$$

To align interference at destinations, α and β should satisfy two next equations.

$$\frac{\beta g_{11}(4)h_{11}(3) + g_{12}(4)h_{21}(3)}{\beta g_{11}(4)h_{12}(3) + g_{12}(4)h_{22}(3)} = \frac{g_{11}(3)h_{11}(3) + g_{12}(3)h_{21}(3)}{g_{11}(3)h_{12}(3) + g_{12}(3)h_{22}(3)} \tag{21}$$

$$\frac{\alpha g_{21}(4)h_{11}(2) + g_{22}(4)h_{21}(2)}{\alpha g_{21}(4)h_{12}(2) + g_{22}(4)h_{22}(2)} = \frac{g_{21}(2)h_{11}(2) + g_{22}(2)h_{21}(2)}{g_{21}(2)h_{12}(2) + g_{22}(2)h_{22}(2)} \tag{22}$$

So, (21) and (22) lead to following values for α and β:

$$\alpha = \frac{g_{21}(2)g_{22}(4)}{g_{21}(4)g_{22}(2)}, \;\; \beta = \frac{g_{11}(3)g_{12}(4)}{g_{11}(4)g_{12}(3)} \tag{23}$$

Due to alternation CSI pattern available at the strong relay, it has enough information to create α and β. For ease of showing equations, let us define A_1, A_2, B_1, and B_2 as:

$$\begin{aligned} A_1 &= \beta g_{11}(4)h_{12}(3) + g_{12}(4)h_{22}(3) \\ B_1 &= g_{11}(3)h_{12}(3) + g_{12}(3)h_{22}(3) \\ A_2 &= \alpha g_{21}(4)h_{12}(2) + g_{22}(4)h_{22}(2) \\ B_2 &= g_{21}(2)h_{12}(2) + g_{22}(2)h_{22}(2) \end{aligned} \tag{24}$$

Now, D_1 subtracts $\frac{Y_1(3)A_1}{B_1}$ from $Y_1(4)$ to reach $Y_1'(4)$.

$$\begin{aligned} Y_1'(4) = &\left(\alpha g_{11}(4)h_{11}(2) + g_{12}(4)h_{21}(2)\right)(u_1 + l_1) + \\ &\left(\alpha g_{11}(4)h_{12}(2) + g_{12}(4)h_{22}(2)\right)(u_2 + l_1) \end{aligned} \tag{25}$$

Clearly, $Y_1'(4)$ and $Y_1(2)$ are linearly independent. Knowing l_1, D_1 eliminates the effect of artificial noises on $Y_1'(4)$ and $Y_1(2)$ to reach a set of two equations consisting of two variables which are its intended messages. Hence, at the end of the last time slot, D_1 easily recovers its desired messages. D_2 pursues similar procedure by subtracting $\frac{Y_2(2)A_2}{B_2}$ from $Y_2(4)$ to form $Y_2'(4)$. Now, D_2 is able to extract v_1 and v_2 from

$Y_2'(4)$ and $Y_2(3)$. From secrecy perspective, despite the fact that D_1 knows $Y_1(3)$, it cannot extract v_1 and v_2 since it does not know l_2. Similarly, D_2 is unable to find u_1 and u_2 due to lack of information about artificial noise l_1. To show that our scheme is fully successful in ensuring secrecy, we evaluate information leakage at receivers and prove that the amount of leakages at unintended receivers are small and are of order $o(\log P)$ for large P. The analysis is somehow similar to those in [4] and [10]. We consider every four time slots as a single block and assume that equivalent channel from (u_1, u_2) to $(\mathbf{Y}_1; \mathbf{H}, \mathbf{G})$ and $(\mathbf{Y}_2; \mathbf{H}, \mathbf{G})$ is memoryless (i.e. we ignore CSI of the previous block). By denoting $Y_2(2) \triangleq I_2(u_1, u_2, l_1)$, the information leakage at D_2 is:

$$\begin{aligned} I(u_1, u_2; \mathbf{Y}_2|\mathbf{H}, \mathbf{G}) &\overset{(a)}{\leq} I(u_1, u_2; I_2(u_1, u_2, l_1)|\mathbf{H}, \mathbf{G}) \\ &= h(I_2(u_1, u_2, l_1)|\mathbf{H}, \mathbf{G}) - h(I_2(u_1, u_2, l_1)|\mathbf{H}, \mathbf{G}, u_1, u_2) \\ &= h(I_2(u_1, u_2, l_1)|\mathbf{H}, \mathbf{G}) - h(l_1|\mathbf{H}, \mathbf{G}, u_1, u_2) \\ &= \ logP - \log P + o(\log P) = o(\log P) \end{aligned} \tag{26}$$

where (a) follows from the Markov chain $(u_1, u_2) \rightarrow I_2 \rightarrow \mathbf{Y}_2$. Note that u_i, v_i, n_i for $i = 1, 2$ are independent Gaussian random variables with zero mean and variance P. Due to symmetry of the considered model, the same result is inferred for information leakage at D_1. Therefore, by using the proposed scheme, each destination securely receives its two confidential messages within four time slots, and the scheme yields one sum-SDoF which is the upper-bound on achievable sum-SDoF. Hence, achieved sum-SDoF and proposed scheme are optimal from secrecy viewpoint.

B. Optimal scheme for Case 2

As described in Section II, transmitters and the weak relay are completely blind in this case; so, the strong relay play the most important role in the proposed scheme. The scheme consists of four time slots, and the transmitted and received signals by different nodes of network through these time slots are described in the following.

T1H1: At the beginning, S_i sends its artificial noise denoted by n_i. R_i receives Y_{R_i} as:

$$Y_{R_i}(1) = h_{i1}(1)n_1 + h_{i2}(1)n_2. \tag{27}$$

T1H2: Relays send their received signal in this time slot. The received signals at the receivers are

$$\begin{aligned} Y_i(1) =& \left(g_{i1}(1)h_{11}(1) + g_{i2}(1)h_{21}(1)\right) n_1 + \\ & \left(g_{i1}(1)h_{12}(1) + g_{i2}(1)h_{22}(1)\right) n_2 \triangleq l_i \end{aligned} \tag{28}$$

T2H1: At this point, S_i sends u_i, and the relays receive signals as:

$$Y_{R_i}(2) = h_{i1}(2)u_1 + h_{i2}(2)u_2 \tag{29}$$

T2H2: Since there is a feedback from D_1 to R_1 with a unit delay, at the beginning of the second time slot, R_1 knows $Y_1(1) = l_1$ that has been received by D_1 at the first time slot. So, R_1 adds l_1 to its received signal in $T2H1$ and sends the result while R_2 forwards its received signal in the previous phase. D_i receives a signal as follows.

$$\begin{aligned} Y_i(2) =& \left(g_{i1}(2)h_{11}(2) + g_{i2}(2)h_{21}(2)\right) u_1 + \\ & \left(g_{i1}(2)h_{12}(2) + g_{i2}(2)h_{22}(2)\right) u_2 + g_{i1}(2)l_1 \end{aligned} \tag{30}$$

T3H1: S_i transmits v_i toward relays, and R_i receives $Y_{R_i}(3)$ as:

$$Y_{R_i}(3) = h_{i1}(3)v_1 + h_{i2}(3)v_2 \tag{31}$$

T3H2: As mentioned above, R_1 knows $Y_1(1) = l_1$ at the beginning of the second time slot. Since $Y_i(1) = g_{i1}(1)Y_{R_1}(1) + g_{i2}(1)Y_{R_2}(1)$ for $i = 1, 2$ and because R_1 knows CSI of the first time slot with DD state (i.e, knows it at the second time slot), it can compute $Y_{R_2}(1)$ from l_1 and therefore compute $l_2 = Y_2(1)$. So, R_1 sends the sum of l_2 and received signal in $T3H1$ while R_2 forwards its received signal in the previous phase. D_i receives a signal as follows.

$$\begin{aligned} Y_i(3) =& \left(g_{i1}(3)h_{11}(3) + g_{i2}(3)h_{21}(3)\right)v_1 + \\ & \left(g_{i1}(3)h_{12}(3) + g_{i2}(3)h_{22}(3)\right)v_2 + g_{i1}(2)l_2 \end{aligned} \tag{32}$$

T4H1: Same as previous scheme, sources send nothing in this time slot.

T4H2: At the beginning of this time slot, R_1 is aware of $Y_1(3)$ and $Y_1(2)$ owing to delayed feedback from D_1. Moreover, similar to what mentioned above, the strong relay is informed of channel coefficients of the second time slot in the current time slot and can easily find $Y_{R_2}(2)$ and $Y_2(2)$ using $Y_{R_1}(2)$ and $Y_1(2)$. Therefore, in this time slot, R_2 remains idle, and R_1 sends sum of $Y_1(3)$ and $Y_2(2)$. Based on transmitted signal by strong relays, D_i receives $Y_i(4)$.

$$Y_i(4) = g_{i1}(4)(Y_1(3) + Y_2(2)) \tag{33}$$

Now, D_1 knows $g_{11}(4)$ and $Y_1(3)$; then; it calculates $Y_2(2)$ which conveys its favorite messages. Similarly, D_2 obtains $Y_1(3)$ because it knows $g_{21}(4)$ and $Y_2(2)$. Therefore, at the end of the last time slot, each receiver has two equations of its two desired messages. By solving the set of equations, they recover their intended confidential messages. In spite of the fact that D_1 has $Y_1(3)$, it cannot extract v_1 and v_2 since it does not know l_2. Similarly, D_2 cannot access to confidential messages of D_1 because it is unable to find l_1. Therefore, u_1 and u_2 are concealed at D_2 due to l_1, and v_1 and v_2 are concealed at D_1 due to l_2. This shows that the information leakage at D_1 and D_2 are bounded by $o(\log P)$. It should be remarked that R_1 does not require any CSI within the third and fourth time slots. Finally, by finishing this scheme, sources succeed to transmit four confidential messages to destinations within four time slots which yields one sum-SDoF. Since the scheme reaches the maximum achievable sum-SDoF, it is optimal from secrecy point of view.

C. Optimal scheme for Case 3

In this case, sources and R_2 are blind whereas R_1 knows CSI of the second hop with alternating pattern given by (DD, NN, NN) and knows output of D_1 within a unit time

delay. The destinations cooperate with sources in ensuring secrecy. To obtain $\frac{4}{3}$ SDoF, the proposed scheme for this case intends to transfer four confidential messages to destinations during three time slots.

T1H1: In this time slot, the i^{th} source sends u_i. At the same time, D_1 transmits an artificial noise denoted by z_1 toward relays. The relays receive a combination of transmitted signal by sources and artificial noise simultaneously.

$$Y_{R_i}(1) = h_{i1}(1)u_1 + h_{i2}(1)u_2 + k_{i1}(1)z_1. \quad (34)$$

T1H2: At this point, relays forward signals received in the previous stage, and destinations receive signals according to:

$$\begin{aligned} Y_i(1) =&(g_{i1}(1)h_{11}(1) + g_{i2}(1)h_{21}(1))u_1+ \\ &(g_{i1}(1)h_{12}(1) + g_{i2}(1)h_{22}(1))u_2+ \\ &(g_{i1}(1)k_{11}(1) + g_{i2}(1)k_{21}(1))z_1 \end{aligned} \quad (35)$$

At the end of this time slot, R_1 knows $Y_1(1)$ because of delayed feedback. It also obtains CSI of the second hop in the first time slot due to DD state of alternating CSI. Then, it easily calculates $Y_{R_2}(1)$ and $Y_2(1)$ similar to what mentioned for Case 2.

T2H1: In this stage, S_i transmits v_i while the second destination sends z_2, which is artificial noise, toward relays. Each relay receives a signal according to (36).

$$Y_{R_i}(2) = h_{i1}(2)v_1 + h_{i2}(2)v_2 + k_{i2}(2)z_2 \quad (36)$$

T2H2: Relays forward received signals in $T2H1$, and D_i receives a signal as follows.

$$\begin{aligned} Y_i(2) =&(g_{i1}(2)h_{11}(2) + g_{i2}(2)h_{21}(2))v_1+ \\ &(g_{i1}(2)h_{12}(2) + g_{i2}(2)h_{22}(2))v_2+ \\ &(g_{i1}(2)k_{12}(2) + g_{i2}(2)k_{22}(2))z_2 \end{aligned} \quad (37)$$

At the end of this time slot, R_1 has access to $Y_1(2)$ owing to delayed feedback.

T3H1: All sources and destinations keep silent in this time slot.

T3H2: While R_2 remains silent in this time slot, R_1 forms $X_{R_1}(3)$ according to the following equation and sends it over the second hop.

$$X_{R_1}(3) = Y_1(2) + Y_2(1) \quad (38)$$

Then, D_i receives the following signal.

$$Y_i(3) = g_{i1}(3)(Y_1(2) + Y_2(1)) \quad (39)$$

At the end of scheme, D_1 knows $g_{11}(3)$ and $Y_1(2)$; then, it finds $Y_2(1)$ which contains its desired confidential messages. In the same manner, D_2 has $g_{21}(3)$ and $Y_2(1)$ and obtains $Y_1(2)$. Therefore, each receiver has two independent equations of two intended unknown messages. It is true that D_1 knows $Y_1(2)$; however, it cannot recover v_1 and v_2 which are confidential messages of D_2 since it does not know z_2. Similarly, without knowing z_1, D_2 is unable to find u_1 and u_2. Therefore, similar to the above cases information leakage at both destinations are bounded by $o(\log P)$. Hence, the proposed scheme successfully transmits four confidential messages over three time slots, and this proves the optimality of the proposed scheme that achieves the upper-bound presented in Section III.

Remark 1: For Case 1, if R_1 knows channel coefficients of the second hop with alternating pattern given by (NN, DN, ND, PP) with similar assumptions at sources, the result is the same as converse part presented for Case 1. In achievable part, we should make a little change in our proposed scheme to achieve optimal SDoF. In this situation, first, sources send their messages to D_2 in the second time slot and afterward, they send their messages to D_1 in the third slot. Similar procedure holds when R_1 knows CSI of the second hop with alternating pattern given by (DD, NN, DD, NN) in Case 2 or alternating pattern given by (NN, DD, NN) in Case 3.

V. Conclusion

In this paper, we have investigated two-user two-hop X-channel with and without a feedback from one of the receivers to one of the relays. Through three different scenarios, we have studied impacts of feedback, strong relay's side information, and receivers' cooperation in assuring secrecy on the maximum achievable sum-SDoF. We have specified an upper bound on sum-SDoF of presented cases. We have devised achievable schemes for each case which all of them are able to obtain the corresponding upper bound on sum-SDoF successfully. Therefore, we have shown that our proposed schemes and achieved sum-SDoF are optimal from secrecy viewpoint.

References

[1] R. Bassily et al., "Cooperative security at the physical layer: a summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16-28, Sept. 2013.

[2] M. Bloch and J. Barros, "Physical-layer security: from information theory to security engineering", Cambridge University Press, 2011.

[3] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3359-3378, June 2014.

[4] Z. Wang, M. Xiao, M. Skoglund and H. V. Poor, "Secure degrees of freedom of wireless X-networks using artificial noise alignment," *IEEE Transactions on Communications*, vol. 63, no. 7, pp. 2632-2646, July 2015.

[5] C. S. Vaze and M. K. Varanasi, "The degrees of freedom of the 2x2x2 interference network with delayed CSIT and with limited shannon feedback," *Proceedings of Allerton Conference on Communication, Control, and Computing*, pp. 824-831, Sept. 2011.

[6] P. K. Sangdeh, M. Mirmohseni and M. A. Akhaee "Interference alignment for two-user two-hop interference X-channel with delayed and no CSIT," *International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT)*, St. Petersburg, Russia, Oct. 2014.

[7] J. Xie and S. Ulukus, "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, Sept. 2013.

[8] Z. Wang, M. Xiao and M. Skoglund, "Secrecy degrees of freedom of the 2x2x2 interference channel with delayed CSIT," *IEEE Wireless Communications Letters*, vol. 3, no. 4, pp. 341-344, Aug. 2014.

[9] T. Gou, S. A. Jafar, S. W. Jeon, and S. Y. Chung, "Aligned interference neutralization and the degrees of freedom of the 2x2x2 interference channel," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4381-4395, July 2012.

[10] P. Mukherjee, R. Tandon, and S. Ulukus, "Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT" Available:https://arxiv.org/abs/1502.02647