Secure Degrees of Freedom of Two-User X-Channel with Synergistic Alternating Channel State Information at Transmitters

Article *in* IET Information Security · August 2018

DOI: 10.1049/iet-ifs.2018.5239

Pedram Kheirkhah
University of Louisville

Secure Degrees of Freedom of Two-User X-Channel with Synergistic Alternating Channel State Information at Transmitters

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; akhbari@kntu.ac.ir

Abstract

In this paper, a two-user single-input single-output X-channel with confidential messages is addressed. In this model, we assume that the transmitters have access to synergistic alternating channel state information. During different time slots, the Channel State Information at Transmitters (CSIT) alternate between three states including perfect CSIT, delayed CSIT, and no CSIT. By using the eminent synergistic benefits of CSIT pattern, some schemes capable of attaining the maximum achievable Secure Degrees of Freedom (SDoF) are presented. Additionally, in devising the schemes, the minimal CSIT patterns required to achieve optimal SDoF are introduced. It is shown that for CSIT patterns which are weaker than minimal ones, using a half-duplex relay can assist the network in obtaining the optimal SDoF. Indeed, the relay alleviates the effects of the lack of knowledge at transmitters on achievable SDoF.

I. Introduction

Secure data transmission at the highest possible rate has a great importance in any communication network; however, due to broadcast nature of wireless medium, interference becomes a huge obstacle toward reaching this ultimate goal. Despite the negative effects of interference on the transmission rate in multi-user networks, it can meticulously be exploited to understand fundamental capacity limits of wireless networks [1]. Unfortunately, in the most of multi-user wireless networks, analysis of exact capacity region is difficult whereas Degrees of Freedom (DoF) affords an invaluable tool in order to study asymptotic performance of networks at high Signal-to-Noise Ratio (SNR) [1]. In the recent decade, characterizing

* Corresponding Author

DoF of different wireless networks has intrigued many researches which led to a promising technique named Interference Alignment (IA) [2], [3]. In the most of IA schemes, Channel State Information at Transmitters (CSIT) plays an important role in obtaining desirable DoF. By utilizing IA techniques, a wide spectrum of wireless networks and their optimal DoF have been investigated [1].

In [4], Cadambe and Jafar have studied $M \times N$ X-channel with perfect CSIT and single-antenna nodes, and they have shown that the optimal sum-DoF of this channel is $\frac{M \times N}{M+N-1}$. Only when the transmitters know perfect instantaneous CSIT, this DoF is achievable; however, this assumption of perfect instantaneous CSIT is too optimistic. Actually, in real applications, CSIT is delayed, imprecise or not available. Apart from this unpragmatic presumption about permanent availability of perfect CSIT, it may vary over time due to random and time variant phenomenon in wireless medium, like shadowing, fading, interference, and pathloss. In [5], Tandon *et al.* have formalized alternating CSIT model whose availability of CSIT is time-variant. Indubitably, this is a more practical assumption. They have shown that alternating CSIT could be beneficial for increasing DoF of two-user Multiple-Input Single-Output Broadcast Channel (MISO-BC). In another study, two-user SISO X-channel with alternating CSIT has been considered, and it is demonstrated that synergistic alternation of CSIT is still very advantageous in networks with distributed transmitters [6]. The aforementioned network without CSIT has been addressed in [7], and it is shown that a half-duplex relay can pave the way for reaching the optimal sum-DoF via IA. This aim can be accomplished by using either a two-antenna relay with delayed CSI or a single-antenna relay with perfect CSI. Then, the results have been extended to the general case of K-user X-channel with half-duplex relays which have access to perfect CSI [8].

In parallel with efforts to explore the capacity of wireless networks, paramount strides have been done to investigate secrecy capacity of these networks. To characterize the secrecy capacity, the Secure Degrees of Freedom (SDoF) has widely been studied for different networks [9], and the most related works are presented here. The works in [10] and [11] have investigated the SDoF of MIMO X-channel in which the transmitters and receivers have M antennas and N antennas, respectively. The authors of [10] and [11] have also considered a feedback from receivers to transmitters which offers the information of received signals at the receivers and delayed CSIT. In such situation, the authors have characterized the optimal sum-SDoF and shown the sum-SDoF region is exactly the same as SDoF region of a two-user MIMO BC channel with two N-antenna receivers and one $2 \times M$-antenna transmitter which has access to delayed CSIT. The valuable implication of this result is that if asymmetric output feedback and delayed CSIT are available, the distributed transmitters do not inflict any performance degradation on the system. In [12], $M \times K$ X-channel with perfect CSIT has been investigated, and it has been shown that the sum-SDoF of this network is upper bounded by $\frac{K \times (M-1)}{K+M-2}$. It is worth noting that for a two-user X-channel

($K = M = 2$), this bound can be achieved by using the artificial noise method. It means that the optimal sum-SDoF of two-user X-channel is one. Some of the results presented in [12], has also been noted by Jafar and Gou in [13] which verifies previous findings.

Since, this paper mainly aims at investigating the SDoF of a X-channel when synergistic alternating CSIT is available, in the following, some relevant studies on the SDoF of broadcast channel with alternating CSIT are reviewed. In [14], the authors have studied two-user MISO-BC with Confidential Messages (BCCM) with alternating CSIT and characterized optimal SDoF region for this general model. Also, they have provided new optimal achievable schemes for different alternating CSIT regimes. Similarly, [15], [16], [17] have investigated the SDoF region of broadcast channels with two or multiple receivers while the alternating CSIT is available at the transmitter. In a special case which has been considered in both [14] and [16], the similar upper-bound has been derived in both papers for a transmitter which has access to three possible states of CSIT including perfect, delayed, and no CSIT.

Motivated by [6], in this paper, sum-SDoF of two-user SISO X-channel with alternating CSIT and confidential messages is investigated, and three different schemes corresponding to three minimal CSIT patterns sufficing to achieve the maximum sum-SDOF, which is equal to one, are proposed. In addition, the requirements on the CSIT alternation pattern, which should be satisfied in order to reach the optimal SDoF, are specified. Moreover, inspired by [7], weaker patterns violating the minimum mandatory knowledge for the proposed schemes are considered, and it is proved that using one half-duplex relay enables the network to attain the optimal sum-SDoF again. In other words, the relay compensates the degradation of sum-SDoF caused by lack of sufficient side information at transmitters and makes it possible to obtain the optimal sum-SDoF again.

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

II. System Model

In this section, we introduce two X-channels, which are investigated in this paper, through the two following sub-sections. First, we consider the two-user SISO X-channel as our main concern. Then, by adding one relay, we study relay-aided two-user SISO X-channel.

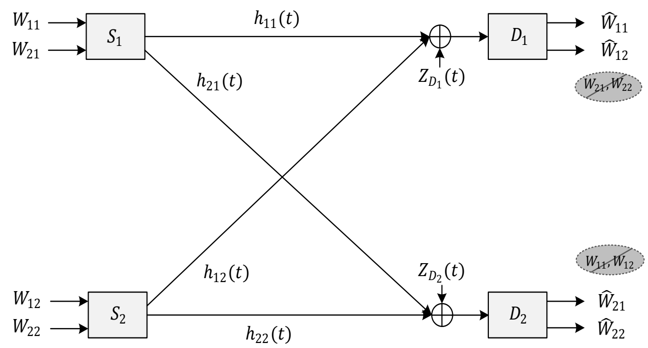

Fig. 1: Two-user SISO X-channel with confidential messages.

A. Two-user SISO X-channel

As depicted in Fig. 1, the two-user SISO X-channel consists of two single-antenna sources and two destinations. S_i and D_j $(i, j = 1, 2)$ denote the i^{th} source and the j^{th} destination, respectively. The channel coefficient between S_i and D_j in the t^{th} channel use is indicated by $h_{ji}(t)$. Each source wishes to send one message to each destination. Accordingly, W_{ji} represents the message of S_i for D_j. In the t^{th} channel use, the source $S_i\,(i = 1, 2)$ using W_{1i}, W_{2i} and its side information, forms $X_i(t) \in \mathbb{C}$, which $\mathbb{C}$ is the set of complex numbers. The $X_i(t)$ satisfies the following power constraint within all channel uses,

$$\mathbb{E}\left[X_i^2(t)\right] \leq P; \quad i = 1, 2. \tag{1}$$

where P and $\mathbb{E}$ are power constraint and expectation operator, respectively. In the t^{th} channel use, D_j receives $Y_j(t) \in \mathbb{C}$ according to the following equations.

$$Y_1(t) = h_{11}(t)X_1(t) + h_{12}(t)X_2(t) + Z_{D_1}(t); \tag{2}$$

$$Y_2(t) = h_{21}(t)X_1(t) + h_{22}(t)X_2(t) + Z_{D_2}(t); \tag{3}$$

where $Z_{D_i}(t) \in \mathbb{C}$ is an additive white Gaussian noise at D_i in the t^{th} channel use. All channel coefficients, i.e $\mathbf{H}_t = \{h_{ij}(t)\}_{i,j}$, and additive white Gaussian noises are scalars with complex normal distribution $\mathcal{CN}(0, 1)$ and they are i.i.d over i, j, and t. We suppose that all sources and destinations know the distribution.

From side information perspective, CSIT related to each destination varies over channel uses among three different states. P, D, N are used for representing perfect CSI, delayed CSI, and no CSI, respectively. So, each pair of these three states clarifies sources' local knowledge about channels related to two sources and belongs to a set with nine possible states. For instance, PD in the t^{th} channel use indicates

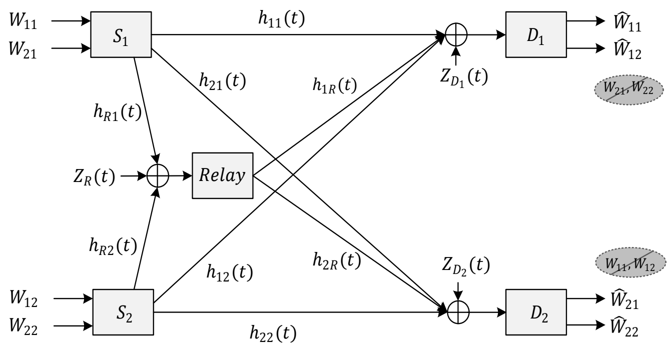

Fig. 2: Relay-aided two-user SISO X-channel with confidential messages.

that that S_1 and S_2 know $h_{11}(t)$ and $h_{12}(t)$ perfectly while receive information about $h_{21}(t)$ and $h_{22}(t)$ with a finite delay. Through the rest of paper, we assume that the delays equal to one channel use for simplicity. Moreover, since there is no time limit on decoding, we can assume that the available CSI at the destinations is perfect and instantaneous.

B. *Relay-aided two-user SISO X-channel*

Fig. 2 illustrates the relay-aided two-user SISO X-channel which is similar to the previous channel except that a half-duplex relay is added to it; so, we ignore repeating the same details here. The relay is a trusted node and assists network with sending $X_R(t) \in \mathbb{C}$ in the t^{th} channel use. The relay receives $Y_R(t) \in \mathbb{C}$:

$$Y_R(t) = h_{R1}(t)X_1(t) + h_{R2}(t)X_2(t) + Z_R(t); \tag{4}$$

where $h_{Ri}(t)$ stands for the channel coefficient between S_i and the relay, and $Z_R(t) \in \mathbb{C}$ is additive white Gaussian noise at the relay in the t^{th} channel use. In the t^{th} channel use, the received signals by destinations are:

$$Y_1(t) = h_{11}(t)X_1(t) + h_{12}(t)X_2(t) + h_{1R}(t)X_R(t) + Z_{D_1}(t); \tag{5}$$

$$Y_2(t) = h_{21}(t)X_1(t) + h_{22}(t)X_2(t) + h_{2R}(t)X_R(t) + Z_{D_2}(t); \tag{6}$$

where $h_{jR}(t)$ indicates the channel coefficient between D_j and the relay in the t^{th} channel use. The relay always knows global CSI instantaneously while sources know alternating CSIT given by (DD, NN, NN, NN) during four channel uses. Furthermore, 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 which satisfies the following constraints at the destinations:

$$W_{ij} \in \{1, 2, \ldots, 2^{R_{ij}}\} \quad \forall i, j \in \{1, 2\} \tag{7}$$

$$Pr\left(\hat{W}_{ij} \neq W_{ij}\right) \leq \epsilon_n, \quad \forall i, j \in \{1, 2\} \tag{8}$$

$$\frac{I(W_{11}, W_{12}; Y_2^n, \mathbf{H}^n)}{n} \leq \epsilon_n \tag{9}$$

$$\frac{I(W_{21}, W_{22}; Y_1^n, \mathbf{H}^n)}{n} \leq \epsilon_n \tag{10}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Also, $\mathbf{H}^n$ indicates global CSI of the network during n channel uses, and $I(;)$ is mutual information between its arguments. Informally, (8) is the reliability constraint at destinations, and the constraints in (9) and (10) 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 achievable with definition

$$d = \lim_{P \to \infty} \frac{\sum_{(i,j) \in \{1,2\}^2} R_{ij}}{\log(P)}. \tag{11}$$

III. MAIN RESULTS

In this section, the main results for aforementioned systems are presented through the following theorems. In the first theorem, we consider the two-user SISO X-channel and present some necessary and sufficient conditions on CSIT alternation pattern which yields attaining the optimal sum-SDoF for this channel.

Theorem 1: For the two-user SISO X-channel in time varying or frequency selective settings, the upper bound on the sum-SDoF is achievable if the following requirements on the CSIT alternation pattern are satisfied during four time slots: (i) In the 1^{st} time slot, each source has at least delayed CSIT; (ii) Each source has a delayed CSIT followed by a perfect CSIT over the $2^{nd}, 3^{rd}$, and 4^{th} time slots; (iii) During the $2^{nd}, 3^{rd}$, and 4^{th} time slots, at least one of sources knows some kind of CSIT (perfect or delayed). Therefore, two sources should not be unaware of CSIT simultaneously; (iv) In the 4^{th} time slot, at least one of sources knows perfect CSIT.

Note that since the proof of this theorem strictly depends on the proposed scheme, we present it after mentioning the third proposed scheme in Section IV.

Now, consider a problematic situation in which the sources' knowledge about CSIT are less than three minimal CSIT alternation patterns mentioned before; for example, look at (DD, NN, NN, DD) pattern which violates the necessary conditions for attaining optimal sum-SDoF. Here, the question is that whether achievable sum-SDoF collapses or not. Is there any solution to recover sum-SDoF again? Admittedly, without any further action the sum-SDoF drastically decreases. Nevertheless, adding one half-duplex relay to two-user SISO X-channel, which turns it into relay-aided two-user SISO X-channel introduced in Section II-B, revives the sum-SDoF. In this case, not only adding the relays is beneficial in terms of sum-SDoF, but it also achieves the optimal sum-SDoF for patterns which are stronger than (DD, NN, NN, NN). In this regard, the relay-aided two-user SISO X-channel with the weakest possible CSIT patterns, i.e. (DD, NN, NN, NN) is studied, and it is assumed that the relay perfectly knows global CSI within different time slots. In the following theorem, we state the main result about this case.

Theorem 2: For the relay-aided two-user X-channel with alternating CSIT given by (DD, NN, NN, NN), the maximum achievable sum-SDoF is one.

Proof: First and foremost, it is proved that the achievable sum-SDoF of the channel is upper bounded by one, regardless of the number of antennas at the relay. The sum-SDoF of the X-channel with alternating CSIT given by (DD, NN, NN, NN) with one relay is upper bounded by the optimal sum-SDoF of the channel with perfect CSIT and the same relay. For arbitrary number of antennas at the relay, the authors in [18] have shown that relaying does not increase achievable sum-DoF of X-channel when all nodes benefit from global CSI and there are direct links between all pair of sources and destinations. Definitely, the relay uses one of relaying strategies and have no cooperation in ensuring secrecy; hence, the result for sum-DoF is valid for sum-SDoF of this channel too. Then it is concluded that the optimal sum-SDoF of the relay-aided two-user X-channel with global CSI is one, which is clearly an upper bound for the channel which we deal with. In the next section, a scheme is proposed which successfully attains this upper bound, and this proves that the optimal sum-SDoF for the channel with mentioned CSI regime is one ■.

IV. Proposed Method

In this section, three schemes corresponding to three minimal CSI alternation patterns are proposed to achieve the upper bound on sum-SDoF of two-user SISO X-channel. Then, the relay-aided two-user SISO X-channel is investigated, and a scheme is presented to compensate the lack of sufficient side information at sources.

A. Two-user SISO X-channel

To obtain optimal sum-SDoF, the following achievability schemes consist of four time slots through which each source sends a confidential message to each destination. In these schemes, artificial noise forwarding method is used for assuring secrecy. The artificial noise symbols are drawn from a complex normal distribution $\mathcal{CN}(0, P)$ and are shared among sources. The sources do not cooperate in transmissions of confidential messages. In this section, let consider S_i wants to send u_i for D_1 and v_i for D_2. In the next three sub-sections, we show that these symbols can be transmitted reliably and securely to their intended destinations over four time slots via schemes based on three minimal patterns of alternating CSIT.

*1) **Scheme 1**:* First, we consider the CSIT alternation pattern is (DD, DD, PN, NP) over four time slots. Based on this pattern, we devise the first scheme as follows.

Time slot 1: In the first time slot, S_i sends n_i which is an artificial noise injected by the i^{th} source. In addition, each source knows both n_1 and n_2. Hence, in this time slot $X_i(1) = n_i$ and:

$$Y_1(1) = h_{11}(1)n_1 + h_{12}(1)n_2 = l_1(n_1, n_2). \tag{12}$$

$$Y_2(1) = h_{21}(1)n_1 + h_{22}(1)n_2 = l_2(n_1, n_2). \tag{13}$$

where $l_i(n_1, n_2)$ indicates a linear combination of n_1 and n_2 received by D_i.

Time slot 2: Since the channel coefficients of the first time slot are available with unit delay at sources, and they know n_1 and n_2, source S_i can form $l_i(n_1, n_2)$ at the beginning of this time slot. Hence, S_i sends $X_i(2) = u_i + v_i + l_i(n_1, n_2)$. For brevity, in the following equations l_i stands for $l_i(n_1, n_2)$.

$$\begin{aligned} Y_1(2) =& h_{11}(2)u_1 + h_{12}(2)u_2 + h_{11}(2)v_1 + \\ & h_{12}(2)v_2 + h_{11}(2)l_1 + h_{12}(2)l_2 \\ =& L_1^1(u_1, u_2, l_1) + I_1(v_1, v_2, l_2) \end{aligned} \tag{14}$$

$$\begin{aligned} Y_2(2) =& h_{21}(2)u_1 + h_{22}(2)u_2 + h_{21}(2)v_1 + \\ & h_{22}(2)v_2 + h_{21}(2)l_1 + h_{22}(2)l_2 \\ =& L_2^1(v_1, v_2, l_2) + I_2(u_1, u_2, l_1) \end{aligned} \tag{15}$$

where L_i^1 denotes a linear combination of desired messages and l_i for D_i, and I_i indicates a linear combination of unintended messages and $l_{j \neq i}$ for D_i.

Time slot 3: Since the CSIT alternation pattern of the second and third time slots are DD and PN respectively, the i^{th} source knows $h_{1i}(3)$ and $h_{1i}(2)$ in this moment. Then, sources form appropriate signals to send. Furthermore, S_2 has enough information to construct l_2 because it knows the CSI of the first time slot based on the mentioned CSIT alternation pattern.

$$X_1(3) = h_{11}^{-1}(3)h_{11}(2)v_1 \tag{16}$$

$$X_2(3) = h_{12}^{-1}(3)h_{12}(2)(v_2 + l_2) \tag{17}$$

$$
\begin{aligned}
Y_1(3) =& h_{11}(3)h_{11}^{-1}(3)h_{11}(2)v_1 + h_{12}(3)h_{12}^{-1}(3)h_{12}(2)(v_2 + l_2) \\
=& I_1(v_1, v_2, l_2) \qquad (18)
\end{aligned}
$$

$$
\begin{aligned}
Y_2(3) =& h_{21}(3)h_{11}^{-1}(3)h_{11}(2)v_1 + h_{22}(3)h_{12}^{-1}(3)h_{12}(2)(v_2 + l_2) \\
=& L_2^2(v_1, v_2, l_2) \qquad (19)
\end{aligned}
$$

Time slot 4: According to CSIT pattern, S_i knows $h_{2i}(4)$ in this time slot. Besides, S_1 has sufficient information to reconstruct l_1. Therefore,

$$X_1(4) = h_{21}^{-1}(4)h_{21}(2)(u_1 + l_1) \qquad (20)$$

$$X_2(4) = h_{22}^{-1}(4)h_{22}(2)u_2 \qquad (21)$$

$$
\begin{aligned}
Y_1(4) =& \; h_{11}(4)h_{21}^{-1}(4)h_{21}(2)(u_1 + l_1) + h_{12}(4)h_{22}^{-1}(4)h_{22}(2)u_2 \\
=& \; L_1^2(u_1, u_2, l_1) \qquad (22)
\end{aligned}
$$

$$
\begin{aligned}
Y_2(4) =& \; h_{21}(4)h_{21}^{-1}(4)h_{21}(2)(u_1 + l_1) + h_{22}(4)h_{22}^{-1}(4)h_{22}(2)u_2 \\
=& \; I_2(u_1, u_2, l_1) \qquad (23)
\end{aligned}
$$

At the end of this time slot, the i^{th} destination knows all channel coefficients of four time slots and l_i. Based on received signals of all time slots, each destination successfully recovers its desired confidential messages. To extract intended messages, D_1 removes $I_1(v_1, v_2, l_2)$ in (18) from (14) and reaches $L_1^1(u_1, u_2, l_1)$. In addition, it has $L_1^2(u_1, u_2, l_1)$ and knows l_1. Therefore, it subtracts effect of l_1 from L_1^1 and L_1^2 in order to catch a set of two equations including two variables. It easily solves this set of equations and recovers u_1 and u_2. In a similar procedure, D_2 draws its intended messages from (15) and (19) since it knows l_2 and $I_2(u_1, u_2, l_1)$. From secrecy perspective, despite the fact that D_1 knows $I_2(v_1, v_2, l_2)$, it is unable to evaluate v_1 and v_2 since it cannot find out l_2 in order to reach enough equations about these messages to decode all of them. Thus, sources transmit four confidential messages over four time slots via the proposed scheme, and it achieves sum-SDoF equals one, which is the upper bound on sum-SDoF in our case. This pinpoints optimality of the scheme and the achieved sum-SDoF.

2) ***Scheme 2:*** Now, we propose a scheme for the second minimal CSIT alternation pattern, i.e. (DD, ND, DN, PP). The scheme involves four time slots within which each source sends well-designed signals as follows.

Time slot 1: In the first time slot, S_i sends its artificial noise denoted by n_i over the channel, and destinations receive:

$$Y_1(1) = h_{11}(1)n_1 + h_{12}(1)n_2 = l_1(n_1, n_2). \qquad (24)$$

$$Y_2(1) = h_{21}(1)n_1 + h_{22}(1)n_2 = l_2(n_1, n_2). \tag{25}$$

where l_1 and l_2 indicate a linear combination of artificial noises.

Time slot 2: In the second time slot, transmitted signals by sources and received signals by destinations are (26)-(28). Each source knows CSI of the previous time slot and shared artificial noises, and it can construct l_1 and l_2 in the second and next time slots where needed.

$$X_i(2) = u_i + l_i \qquad (i = 1, 2) \tag{26}$$

$$\begin{aligned} Y_1(2) &= h_{11}(2)u_1 + h_{12}(2)u_2 + (h_{11}(2) + h_{12}(2))l_1 \\ &= L_1^1(u_1, u_2, l_1) \end{aligned} \tag{27}$$

$$\begin{aligned} Y_2(2) &= h_{21}(2)u_1 + h_{22}(2)u_2 + (h_{21}(2) + h_{22}(2))l_1 \\ &= I_2(u_1, u_2, l_1) \end{aligned} \tag{28}$$

Time slot 3: In the third time slot, the i^{th} source sends $X_i(3) = v_i + l_2$ $(i = 1, 2)$, so the destinations receive:

$$\begin{aligned} Y_1(3) &= h_{11}(3)v_1 + h_{12}(3)v_2 + (h_{11}(3) + h_{12}(3))l_2 \\ &= I_1(v_1, v_2, l_2) \end{aligned} \tag{29}$$

$$\begin{aligned} Y_2(3) &= h_{21}(3)v_1 + h_{22}(3)v_2 + (h_{21}(3) + h_{22}(3))l_2 \\ &= L_2^1(v_1, v_2, l_2) \end{aligned} \tag{30}$$

Time slot 4: In the last time slot, since the CSIT is perfectly available for both sources, they know their channel coefficients locally. They send $X_1(4)$ and $X_2(4)$ according to (31)-(32), and destinations receive signals mentioned in (33)-(34).

$$X_1(4) = h_{21}^{-1}(4)h_{21}(2)(u_1 + l_1) + h_{11}^{-1}(4)h_{11}(3)(v_1 + l_2) \tag{31}$$

$$X_2(4) = h_{22}^{-1}(4)h_{22}(2)(u_2 + l_1) + h_{12}^{-1}(4)h_{12}(3)(v_2 + l_2) \tag{32}$$

$$\begin{aligned} Y_1(4) &= I_1(v_1, v_2, l_2) + L_1^2(u_1, u_2, l_1) \\ L_1^2(u_1, u_2, l_1) &\triangleq A_1u_1 + B_1u_2 + (A_1 + B_1)l_1 \\ A_1 &= h_{11}(4)h_{21}^{-1}(4)h_{21}(2) \\ B_1 &= h_{12}(4)h_{22}^{-1}(4)h_{22}(2) \end{aligned} \tag{33}$$

$$Y_2(4) = I_2(u_1, u_2, l_1) + L_2^2(v_1, v_2, l_2) \tag{34}$$
$$L_2^2(v_1, v_2, l_2) \triangleq A_2 v_1 + B_2 v_2 + (A_2 + B_2) l_2$$
$$A_2 = h_{21}(4) h_{11}^{-1}(4) h_{11}(3)$$
$$B_2 = h_{22}(4) h_{12}^{-1}(4) h_{12}(3)$$

At the end of this time slot, D_1 knows CSI of all time slots, I_1, L_1^1, and l_1 explicitly. By removing I_1 from $Y_1(4)$, D_1 attains L_1^2. Hence, it can easily extract u_1 and u_2 from a set of two equations with two variables which are its desired confidential messages. In the same way, knowing I_2 provides L_2^2 for D_2, and this destination already knows L_2^1. Based on these linear combinations, it recovers its intended messages, i.e. v_1 and v_2. Thus, the scheme enables each destination to receive two confidential messages within four time slots which yields one sum-SDoF. So, the proposed scheme is optimal from sum-SDoF viewpoint.

*3) **Scheme 3**:* For the last minimal CSIT alternation pattern, i.e. (DD, DN, PD, NP), an optimal achievablity scheme is proposed which catches one sum-SDoF through four time slots.

Time slot 1: In the first time slot, each source sends its artificial noise toward destinations, and destinations receive:

$$Y_1(1) = h_{11}(1) n_1 + h_{12}(1) n_2 = l_1(n_1, n_2). \tag{35}$$
$$Y_2(1) = h_{21}(1) n_1 + h_{22}(1) n_2 = l_2(n_1, n_2). \tag{36}$$

Time slot 2: Since the channel coefficients of the first time slot are available with a unit delay at sources and they know n_1 and n_2, each source can form both l_1 and l_2 at the beginning of the second time slot. Then, S_i transmits $X_i(2) = v_i + l_2$, and destinations receive the following signals accordingly.

$$\begin{aligned} Y_1(2) &= h_{11}(2) v_1 + h_{12}(2) v_2 + (h_{11}(2) + h_{12}(2)) l_2 \\ &= I_1(v_1, v_2, l_2) \end{aligned} \tag{37}$$
$$\begin{aligned} Y_2(2) &= h_{21}(2) v_1 + h_{22}(2) v_2 + (h_{21}(2) + h_{22}(2)) l_2 \\ &= L_2^1(v_1, v_2, l_2) \end{aligned} \tag{38}$$

where both L_2^1 and I_1 are linear combination of v_1, v_2, and l_2. L_2^1 contains the desired message of the second destination and a known combination of artificial noises, and I_1 constitutes unintended messages of D_1 while these messages are added by unknown combination of artificial noise.

Time slot 3: According to the CSIT alternation pattern, in this time slot S_1 knows $h_{11}(2)$ and $h_{11}(3)$ while S_2 knows $h_{12}(2)$ and $h_{12}(3)$. Then, sources transmit the following signals.

$$X_1(3) = u_1 + l_1 + h_{11}^{-1}(3)h_{11}(2)(v_1 + l_2) \tag{39}$$

$$X_2(3) = u_2 + l_1 + h_{12}^{-1}(3)h_{12}(2)(v_2 + l_2) \tag{40}$$

Based on $X_1(3)$ and $X_2(3)$, the signals received by destinations are:

$$\begin{aligned} Y_1(3) &= L_1^1(u_1, u_2, l_1) + I_1(v_1, v_2, l_2) \\ L_1^1(u_1, u_2, l_1) &\triangleq h_{11}(3)u_1 + h_{12}(3)u_2 + (h_{11}(3) + h_{12}(3))l_1 \end{aligned} \tag{41}$$

$$\begin{aligned} Y_2(3) =& h_{21}(3)u_1 + h_{22}(3)u_2 + (h_{21}(3) + h_{22}(3))\, l_1 + \\ & A_1 v_1 + B_1 v_2 + (A_1 + B_1) l_2 \\ =& I_2(u_1, u_2, l_1) + L_2^2(v_1, v_2, l_2) \\ A_1 =& h_{21}(3)h_{11}^{-1}(3)h_{11}(2) \\ B_1 =& h_{22}(3)h_{12}^{-1}(3)h_{12}(2) \end{aligned} \tag{42}$$

Time slot 4: In the fourth time slot, S_i knows $h_{2i}(3)$ and $h_{2i}(4)$. Hence, each source transmits a signal as following.

$$X_1(4) = h_{21}^{-1}(4)h_{21}(3)(u_1 + l_1) \tag{43}$$

$$X_2(4) = h_{22}^{-1}(4)h_{22}(3)(u_2 + l_1) \tag{44}$$

Based on the transmitted signals, destinations receive following signals.

$$\begin{aligned} Y_1(4) &= A_2 u_1 + B_2 u_2 + (A_2 + B_2) l_1 \triangleq L_1^2(u_1, u_2, l_1) \\ A_2 &= h_{11}(4)h_{21}^{-1}(4)h_{21}(3), \quad B_2 = h_{12}(4)h_{22}^{-1}(4)h_{22}(3) \end{aligned} \tag{45}$$

$$Y_2(4) = I_2(u_1, u_2, l_1) \tag{46}$$

Similar to previous schemes, each destination easily recovers its desired confidential messages based on the received signals and known CSI at this point. However, they cannot access to confidential messages of each other. Once Again, the proposed scheme succeeded in achieving sum-SDoF equals to one which is the highest possible value in this case.

Remark 1: We can use *Scheme 1* for alternating CSIT given by (DD, DD, NP, PN) with minor modifications that swaps the transmitted signals in the second and third time slots. Similarly, with minor modifications in the second and third schemes, we could use them for alternating CSIT patterns given by (DD, DN, ND, PP) and (DD, ND, DP, PN), respectively.

Remark 2: 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 a large P. We consider every four time slots as a single block and assume that equivalent channel from (u_1, u_2) to $(\mathbf{Y_1}; \mathbf{H})$ and $(\mathbf{Y_2}; \mathbf{H})$ is memoryless, i.e. we ignore CSI of the previous blocks. The information leakage at D_2 is:

$$\begin{aligned} I(u_1, u_2; \mathbf{Y_2}|\mathbf{H}) &\overset{(a)}{\leq} I(u_1, u_2; I_2(u_1, u_2, l_1)|\mathbf{H}) \\ &= h(I_2(u_1, u_2, l_1)|\mathbf{H}) - \\ &\quad h(I_2(u_1, u_2, l_1)|\mathbf{H}, u_1, u_2) \\ &= h(I_2(u_1, u_2, l_1)|\mathbf{H}) - h(l_1|\mathbf{H}, u_1, u_2) \\ &= \log P - \log P + o(\log P) = o(\log P) \end{aligned} \tag{47}$$

where (a) follows from the Markov chain $(u_1, u_2) \to I_2 \to Y_2$. Note that u_i, v_i, and 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 can be inferred for the information leakage at D_1.

Remark 3: Three minimal CSIT alternation patterns are the lowest possible ones from side information point of view. It is axiomatic that any pattern affording more information can be approached by one of these schemes; for instance, (PD, NP, PN, PP) avails the first scheme.

Proof of Theorem 1: At the beginning, we explain the first requirement for the 1^{st} time slot. As we see in our proposed schemes, transmitters use l_1 and l_2 that are created in the 1^{st} time slot at receiver 1 and 2, as security keys in the next time slots for providing secrecy. Therefore, at the end of the 1^{st} time slot, they need at least delayed CSIT to compute these values. Hence, the minimum channel state information should be in DD mode. It is obvious that higher side information in the 1^{st} time slot, i.e. PD, DP and PP, have similar result. If we follow the same procedure as [6], we can easily see that there are nine minimal patterns that satisfy the first and second requirements. Six of these nine patterns satisfy the third and fourth requirements too and are listed in Table I with corresponding schemes which achieve the upper bound of sum-SDoF for each pattern. The three remaining patterns which do not meet the third and fourth requirements are (DD, DD, PP, NN), (DD, DD, NN, PP), and (DD, NN, DD, PP). For the first one, the minimum CSIT patterns that satisfy all four requirements are (DD, DD, PP, PN), which conveys more side information than (DD, DD, NP, PN), and (DD, DD, PP, NP) which has more information than (DD, DD, PN, NP). As seen in Table I, we can achieve sum-SDoF equals one using

TABLE I: Achievable schemes for different CSIT states

CSIT State	Corresponding Scheme	CSIT State	Corresponding Scheme
(DD, DD, PN, NP)	Scheme 1	(DD, ND, DN, PP)	Scheme 2
(DD, DD, NP, PN)	Scheme 1	(DD, ND, DP, PN)	Scheme 3
(DD, DN, ND, PP)	Scheme 2	(DD, DN, PD, NP)	Scheme 3

the first scheme in both cases. Similarly, for (DD, DD, NN, PP) pattern, the minimum CSIT patterns that satisfy the requirements of Theorem 1 are (DD, DD, ND, PP) and (DD, DD, DN, PP) for which the sum-SDoF equals one can be achieved using the second scheme. Finally, for (DD, NN, DD, PP), the minimum CSIT patterns which meet the requirements of Theorem 1 are (DD, ND, DD, PP) and (DD, DN, DD, PP), and the second scheme is useful regarding this pattern in order to reach optimal sum-SDoF ■.

B. Relay-aided Two-user SISO X-channel

Here, we encounter to a challenging situation in which sources know the delayed CSI of the first time slot, and they know nothing about channel coefficients of the following time slots. Indeed, this pattern violates all minimal patterns. Without a shadow of doubt, this severe condition results in collapsing achievable sum-SDoF without any further action. However, adding one relay compensates the effects of poor CSIT on sum-SDoF. Now, we propose a scheme which is able to attain sum-SDoF equals one, and as we have proved in the section III, it is the maximum achievable value for sum-SDoF. The proposed scheme consists of four time slots as described in the following.

Time slot 1: In this time slot, the artificial noises are injected to the network. The i^{th} source sends $X_i(1) = n_i$ while the relay remains silent. Similar to the previous schemes, it is assumed that artificial noises, but not confidential messages, are shared between sources.

$$Y_1(1) = h_{11}(1)n_1 + h_{12}(1)n_2 = l_1(n_1, n_2) \tag{48}$$

$$Y_2(1) = h_{21}(1)n_1 + h_{22}(1)n_2 = l_2(n_1, n_2) \tag{49}$$

Since the sources know the delayed CSIT at the end of this time slot, they can reconstruct both l_1 and l_2 during the next time slots.

Time slot 2: In this time slot, the relay keeps silent while S_i sends $X_i(2) = u_i + l_1$. The relay and destinations receive signals according to the next three equations.

$$Y_1(2) = h_{11}(2)(u_1 + l_1) + h_{12}(2)(u_2 + l_1) \tag{50}$$

$$Y_2(2) = h_{21}(2)(u_1 + l_1) + h_{22}(2)(u_2 + l_1) \tag{51}$$

$$Y_R(2) = h_{R1}(2)(u_1 + l_1) + h_{R2}(2)(u_2 + l_1) \tag{52}$$

Time slot 3: Once again, the relay sends nothing whereas the i^{th} source transmits $X_i(3) = v_i + l_2$. So, the received signals at the relay and destinations are as follows:

$$Y_1(3) = h_{11}(3)(v_1 + l_2) + h_{12}(3)(v_2 + l_2) \tag{53}$$

$$Y_2(3) = h_{21}(3)(v_1 + l_2) + h_{22}(3)(v_2 + l_2) \tag{54}$$

$$Y_R(3) = h_{R1}(3)(v_1 + l_2) + h_{R2}(3)(v_2 + l_2) \tag{55}$$

Time slot 4: In the last time slot, we should establish signals at sources and the relay such that each destination gets one additional equation to recover its intended confidential messages without yielding extra interference. S_1 transmits $X_1(4) = u_1 + v_1 + l_1 + l_2$, and the relay sends $X_R(4) = \alpha Y_R(2) + \beta Y_R(3)$ while S_2 remains silent. The α and β are scrupulously chosen according to (56) and (57).

$$\alpha = \frac{h_{21}(4)h_{22}(2)}{h_{21}(2)h_{2R}(4)h_{R2}(2) - h_{22}(2)h_{2R}(4)h_{R1}(2)} \tag{56}$$

$$\beta = \frac{h_{11}(4)h_{12}(3)}{h_{11}(3)h_{1R}(4)h_{R2}(3) - h_{12}(3)h_{1R}(4)h_{R1}(3)} \tag{57}$$

Based on the transmitted signals, the destinations receive:

$$\begin{aligned} Y_1(4) =& h_{11}(4)(u_1 + l_1) + h_{11}(4)(v_1 + l_2) + \\ & \alpha h_{1R}(4)h_{R1}(2)(u_1 + l_1) + \alpha h_{1R}(4)h_{R2}(2)(u_2 + l_1) \\ & + \beta h_{1R}(4)h_{R1}(3)(v_1 + l_2) + \beta h_{1R}(4)h_{R2}(3)(v_2 + l_2) \\ =& (h_{11}(4) + \alpha h_{1R}(4)h_{R1}(2))(u_1 + l_1) + \\ & \alpha h_{1R}(4)h_{R2}(2)(u_2 + l_1) + \\ & (h_{11}(4) + \beta h_{1R}(4)h_{R1}(3))(v_1 + l_2) + \\ & \beta h_{1R}(4)h_{R2}(3)(v_2 + l_2) \end{aligned} \tag{58}$$

$$\begin{aligned} Y_2(4) =& (h_{21}(4) + \alpha h_{2R}(4)h_{R1}(2))(u_1 + l_1) + \\ & \alpha h_{2R}(4)h_{R2}(2)(u_2 + l_1) + (h_{21}(4) + \\ & \beta h_{2R}(4)h_{R1}(3))(v_1 + l_2) + \end{aligned}$$

$$\beta h_{2R}(4)h_{R2}(3)(v_2 + l_2) \tag{59}$$

At the end of the last time slot, since the destinations have CSI of all time slots, they remove the effects of unintended messages from signals received in the last time slot. Moreover, they have enough information to compute α and β. Then, D_1 and D_2 calculate $Y_1'(4)$ and $Y_2'(4)$, respectively.

$$\begin{aligned} Y_1'(4) =& Y_1(4) - Y_1(3)\frac{\beta h_{1R}(4)h_{R2}(3)}{h_{12}(3)} \\ =& (h_{11}(4) + \alpha h_{1R}(4)h_{R1}(2))(u_1 + l_1) + \\ & \alpha h_{1R}(4)h_{R2}(2)(u_2 + l_1) \end{aligned} \tag{60}$$

$$\begin{aligned} Y_2'(4) =& Y_2(4) - Y_2(2)\frac{\alpha h_{2R}(4)h_{R2}(2)}{h_{22}(2)} = \\ & (h_{21}(4) + \beta h_{2R}(4)h_{R1}(3))(v_1 + l_2) + \\ & \beta h_{2R}(4)h_{R2}(3)(v_2 + l_2) \end{aligned} \tag{61}$$

The delicate point to be alluded to is that $Y_1'(4)$ and $Y_1(2)$, $Y_2'(4)$ and $Y_2(3)$ are pairwise linearly independent. With these two linearly independent equations, each destination finds its intended confidential messages. Without knowing l_2, D_1 is prevented from finding out v_1 and v_2 . Similarly, D_2 cannot compute u_1 and u_2. Finally, the proposed scheme succeeded in transmitting two confidential messages to each destination reliably and securely over four time slots. Then, one sum-SDoF is achievable and the proposed scheme is optimal.

Remark 4: When we confront a relay with delayed CSI and sources with alternating CSIT as at least (DD, NN, NN, NN), adding another antenna to the relay makes up the staleness of available CSI at the relay, and we can achieve the optimal sum-SDoF again. The scheme is similar to the presented scheme in the first three time slots. In the last time slot, since the relay is equipped with two antennas and knows delayed CSI, it easily recovers the transmitted noises and messages sent in the previous time slots. Then, it reconstructs l_1 and l_2 to guarantee secrecy and makes signals needed to assist destinations in providing enough equations sufficing to decode their desired confidential messages.

Remark 5: We can generalize the presented scheme to the k-user X-channel with one relay which accesses to global CSI. The scheme is underpinned by adding one additional time slot and performing noise forwarding scenario. Then, with the help of the relay, it is possible to achieve optimal $\frac{k}{2}$ sum-SDoF. In this model, it is mandatory that the relay possesses at least $k - 1$ antennas.

Remark 6: In [10], the authors have shown that sum-SDoF of two-user X-channel with feedback and delayed CSIT is the same as two-user MISO-BC with delayed CSIT. In other words, the adverse effect of distributed nature of transmitters on SDoF is compensated by output feedback. In a similar manner, if the presented results for the model considered in this paper with delayed CSIT are compared to the corresponding MISO-BC with delayed CSIT in [14], it is easily can be found that performance loss caused by distributed nature of transmitters can be compensated by adding one single-antenna relay or a 2-antenna relay which have access to perfect instantaneous CSIT and delayed CSIT, respectively. With the aid of these relays, our proposed scheme is able to obtain the same sum-SDoF achieved in the corresponding MISO-BC with delayed CSIT.

V. Conclusion

In this study, the two-user X-channel with alternating CSIT has been investigated. For this network, it has been demonstrated that the maximum achievable sum-SDoF is one. Three minimal patterns of CSIT providing the lowest possible information required to reach optimal sum-SDoF have been introduced, and three schemes corresponding to each minimal pattern have been devised. These schemes use artificial noises and synergistic alternating CSIT to obtain the optimal sum-SDoF. Any other pattern containing more information can be utilized in one of the proposed schemes. In addition, it has been shown that for patterns weaker than minimal ones, using a half-duplex relay in the network is highly beneficial to compensate the lack of sufficient side information at transmitters. In fact, by using the relay, optimal sum-SDoF is achievable under alternating CSIT regimes offering information less than minimal patterns.

References

[1] Jafar S.: ’Interference Alignment-A New Look at Signal Dimensions in a Communication Network’(Now Publications, 2011)

[2] Maddah-Ali M., Motahari A., Khandani A.: ’Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis’, IEEE Transactions on Information Theory,, 2008, 54, (8), pp. 3457–3470

[3] Cadambe V. R., Jafar S. A.: ’Interference alignment and degrees of freedom of the K-user interference channel’, IEEE Transactions on Information Theory, 2008, 54, (8), pp. 3425–3441

[4] Cadambe V. R., Jafar S. A.: ’Interference alignment and the degrees of freedom of wireless X networks’, IEEE Transactions on Information Theory, 2009, 55,(9), pp. 3893–3908

[5] Tandon R., Jafar S., Shamai Shitz S., et al.: ’On the synergistic benefits of alternating CSIT for the MISO broadcast channel’, IEEE Transactions on Information Theory, 2013, 59, (7), pp. 4106–4128

[6] Wagdy A., El-Keyi A., Khattab T., et al.: ’On the degrees of freedom of SISO X-networks with synergistic alternating channel state information at transmitters’, 2016, arXiv:1605.07069v1

[7] Tian Y., Yener A.: ’Relay-aided interference alignment for the X channel with limited CSI’, Proc. of 2012 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, 2012, pp. 465–469

[8] Tian Y., Yener A.: ’Guiding blind transmitters: relay-aided interference alignment for the X channel’, Proc. of 2012 IEEE Int. Symp. on Information Theory, Cambridge, MA, 2012, pp. 1513–1517

[9] Xie J., Ulukus S.: ’Secure Degrees of Freedom of One-Hop Wireless Networks’, IEEE Transactions on Information Theory, 2014, 60, (6), pp. 3359–3378

[10] Zaidi A., Awan Z. H., Shitz S. S., et al.: ’Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSI’, Information Theory Workshop (ITW), 2013, IEEE 2013, pp. 1–5

[11] Zaidi A., Awan Z. H., Shamai S., et al.: ’Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT’, IEEE Transactions on Information Forensics and Security, 2013, 8, (11), pp. 1760–74

[12] Wang Z., Xiao M., Skoglund M., et al.: ’Secure degrees of freedom of wireless X networks using artificial noise alignment’, IEEE Transactions on Communications, 2015, 63, (7), pp. 2632–2646

[13] Gou T., Jafar S. A.: ’On the secure degrees of freedom of wireless X networks’ In Communication, Control, and Computing’, 2008, 46th Annual Allerton Conference, pp. 826–833.

[14] Mukherjee P., Tandon R., Ulukus S.: ’Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT’, IEEE Transactions on Information Theory, 2017, 63, (6), pp. 3823–3853

[15] Awan Z. H., Zaidi A., Sezgin A.: ’Achievable secure degrees of freedom of MISO broadcast channel with alternating CSIT’, 2014 IEEE International Symposium on Information Theory, Honolulu, HI, 2014, pp. 31–35

[16] Awan Z. H., Zaidi A., Sezgin A.: ’On SDoF of Multi-Receiver Wiretap Channel With Alternating CSIT’, IEEE Transactions on Information Forensics and Security, 2016, 11, (8), pp. 1780–1795

[17] Awan Z. H., Zaidi A., Sezgin A.: ’On SDoF of multi-receiver wiretap channel with alternating CSIT’, 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, 2016, pp. 2973–2977

[18] Cadambe V. R., Jafar S. A.: ’Degrees of freedom of wireless networks with relays, feedback, cooperation and full duplex operation’, IEEE Transactions on Information Theory, 2009, 55, (5), pp.

2334–2344