Secure Degrees of Freedom of MIMO X-Channels with Output Feedback and Delayed CSI

Abdellatif Zaidi Zohaib Hassan Awan Shlomo Shamai (Shitz) Luc Vandendorpe

***Abstract*— We investigate the problem of secure transmission over a two-user multi-input multi-output (MIMO) X-channel with noiseless local feedback and delayed channel state information (CSI) available at transmitters. The transmitters are equipped with M antennas each, and the receivers are equipped with N antennas each. For this model, we characterize the optimal sum secure degrees of freedom (SDoF) region. We show that, in presence of local feedback and delayed CSI, the sum SDoF region of the MIMO X-channel is *same* as the SDoF region of a two-user MIMO BC with $2M$ antennas at the transmitter and N antennas at each receiver. This result shows that, upon availability of feedback and delayed CSI, there is no performance loss in sum SDoF due to the distributed nature of the transmitters. Next, we show that this result also holds if only *global* feedback is conveyed to the transmitters. We also study the case in which only local feedback is provided to the transmitters, i.e., without CSI, and derive a lower bound on the sum SDoF for this model. Furthermore, we specialize our results to the case in which there are no security constraints. In particular, similar to the setting with security constraints, we show that the optimal sum degrees of freedom (sum DoF) region of the (M, M, N, N)-MIMO X-channel is same of the DoF region of a two-user MIMO BC with $2M$ antennas at the transmitter and N antennas at each receiver. We illustrate our results with some numerical examples.**

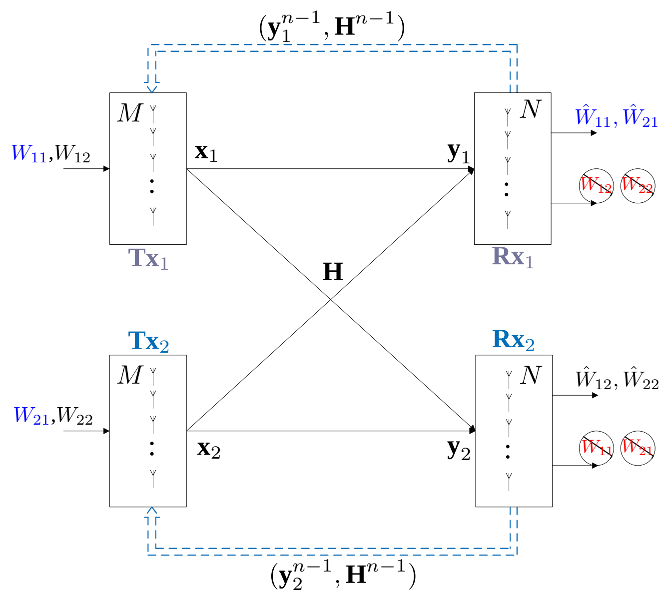

Fig. 1. MIMO X-channel with local feedback and delayed CSI with security constraints.

I. Introduction

We consider a two-user MIMO X-channel in which each transmitter is equipped with M antennas, and each receiver is equipped with N antennas. Each transmitter sends information messages to both receivers. More precisely, Transmitter 1 wants to transmit messages W_{11} and W_{12} to Receiver 1 and Receiver 2, respectively. Similarly, Transmitter 2 wants to transmit messages W_{21} and W_{22} to Receiver 1 and Receiver 2, respectively. The transmission is subject to fast fading effects. Also, we make two assumptions, namely 1) each receiver is assumed to have perfect instantaneous knowledge of its channel coefficients (i.e., CSIR) as well as knowledge of the other receiver's channel coefficients with one unit delay, and 2) there is a noiseless output and CSI feedback from Receiver i, $i = 1, 2$, to Transmitter i. We will refer to such output feedback as being *local*, by opposition to *global* feedback which corresponds to each receiver feeding back its output to both transmitters. The considered model is shown in Figure 1. Furthermore, the messages that are destined to each receiver are meant to be kept secret from the other receiver. That is, Receiver 2 wants to capture the pair (W_{11}, W_{21}) of messages that are intended for Receiver 1; and so, in addition to that it is a legitimate receiver of the pair (W_{12}, W_{22}), it also acts as an eavesdropper on the MIMO multiaccess channel to Receiver 1. Similarly, Receiver 1 wants to capture the pair (W_{12}, W_{22}) of messages that are intended for Receiver 2; and so, in addition to that it is a legitimate receiver of the pair (W_{11}, W_{21}), it also acts as an eavesdropper on the MIMO multiaccess channel to Receiver 2. The model that we study can be seen as being that of [1] but with security constraints imposed on the transmitted messages. We concentrate on the case of perfect secrecy, and focus on asymptotic behaviors, captured by the allowed secure degrees of freedom over this network model. The reader may refer to [2]–[4] for some other related works.

The main contributions of this paper can be summarized as follows. First, we characterize the sum SDoF region of the two-user (M, M, N, N)–MIMO X-channel with local feedback and delayed CSI shown in Figure 1. We show that the sum SDoF region of this model is same as the SDoF region of a two-user MIMO broadcast channel with $2M$ transmit antennas and N antennas at each receiver in which delayed CSI is provided to the transmitter. This result shows that, for symmetric antennas configurations, the distributed nature of the transmitters does not cause any loss in terms of sum secure degrees of freedom. The result also emphasizes the usefulness of local output feedback when used in conjunction with delayed CSI in securing the transmission of messages in MIMO-X channels, by opposition to in MIMO broadcast channels. That is, for the two-user MIMO X-channel, not only local output feedback with delayed CSI does increase the DoF region as shown in [1], it also increases the *secure* DoF region of this network model. The coding scheme that we use for the proof of the direct part is based on an appropriate extension of that developed by Yang *et. al.* [5] in the context of secure transmission over a two-user MIMO BC with delayed CSI at the transmitter; and it demonstrates how each transmitter exploits optimally the available output feedback and delayed CSI.

Next, concentrating on the role of output feedback in the absence of CSI at the transmitters from a secrecy degrees of freedom viewpoint, we study two variations of the model of Figure 1. In the first model, the transmitters are completely ignorant of the CSI, but are provided with *global* output feedback. As we mentioned previously, this output feedback is assumed to be noiselessly and is provided by both receivers to both transmitters. In the second model, the transmitters are provided with only local feedback, i.e., the model of Figure 1 but with no delayed CSI at the transmitters.

For the model with global feedback at the transmitters, we show that the sum SDoF region is same as the sum SDoF region of the model with local feedback and delayed CSI available at the transmitters, i.e., the model of Figure 1. In other terms, the lack of CSI at the transmitters does not cause any loss in terms of sum SDoF as long as the transmitters are provided with global output feedback. In this case, each transmitter readily gets the side information or interference that is available at the unintended receiver by means of the global feedback; and, therefore, it can align it with the information that is destined to the intended receiver directly, with no need of any CSI.

For the model in which only local output feedback is provided to the transmitters, we establish an inner bound on the sum SDoF region. This inner bound is in general strictly smaller than that of the model of Figure 1; and, so, although its optimality is shown only in some specific cases, it gives insights about the loss incurred by the lack of delayed CSI at the transmitters. This loss is caused by the fact that, unlike the coding schemes that we develop for the setting with local output feedback and delayed CSI at the transmitters and that with global feedback at the transmitters, for the model with only local feedback each transmitter can not learn the side information that is available at the unintended receiver and which is pivotal for the alignment of the interferences in such models.

Furthermore, we specialize our results to the case in which there are no security constraints. Similar to the setting with security constraints, we show that the optimal sum degrees of freedom (sum DoF) region of the (M,M,N,N)-MIMO X-channel is same of the DoF region of a two-user MIMO BC with $2M$ antennas at the transmitter and N antennas at each receiver. Finally, we illustrate our results with some numerical examples.

II. System Model and Definitions

We consider a two-user (M,M,N,N) X-channel, as shown in Figure 1. There are two transmitters and two receivers. Both transmitters send messages to both receivers. Transmitter 1 wants to transmit message $W_{11} \in \mathcal{W}_{11} = \{1,\dots,2^{nR_{11}(P)}\}$ to Receiver 1, and message $W_{12} \in \mathcal{W}_{12} = \{1,\dots,2^{nR_{12}(P)}\}$ to Receiver 2. Similarly, Transmitter 2 wants to transmit message $W_{21} \in \mathcal{W}_{21} = \{1,\dots,2^{nR_{21}(P)}\}$ to Receiver 1, and message $W_{22} \in \mathcal{W}_{22} = \{1,\dots,2^{nR_{22}(P)}\}$ to Receiver 2. The messages pair (W_{11},W_{21}) that is intended to Receiver 1 is meant to be concealed from Receiver 2; and the messages pair (W_{21},W_{22}) that is intended to Receiver 2 is meant to be concealed from Receiver 1.

We consider a fast fading model, and assume that each receiver knows the perfect instantaneous CSI along with the past CSI of the other receiver. Also, we assume that Receiver i, $i=1,2$, feeds back its channel output along with the delayed CSI to Transmitter i. The outputs received at Receiver 1 and Receiver 2 at each time instant are given by

$$\begin{aligned} \mathbf{y}_1[t] &= \mathbf{H}_{11}[t]\mathbf{x}_1[t] + \mathbf{H}_{12}[t]\mathbf{x}_2[t] + \mathbf{z}_1[t] \\ \mathbf{y}_2[t] &= \mathbf{H}_{21}[t]\mathbf{x}_1[t] + \mathbf{H}_{22}[t]\mathbf{x}_2[t] + \mathbf{z}_2[t], \quad t=1,\dots,n \end{aligned} \tag{1}$$

where $\mathbf{x}_i \in \mathbb{C}^M$ is the input vector from Transmitter i, $i=1,2$, and $\mathbf{H}_{ji} \in \mathbb{C}^{N\times M}$ is the channel matrix connecting Transmitter i to Receiver j, $j=1,2$. We assume arbitrary stationary fading processes, such that $\mathbf{H}_{11}[t]$, $\mathbf{H}_{12}[t]$, $\mathbf{H}_{21}[t]$ and $\mathbf{H}_{22}[t]$ are mutually independent and change independently across time. The noise vectors $\mathbf{z}_j[t] \in \mathbb{C}^N$ are assumed to be independent and identically distributed (i.i.d.) white Gaussian, with $\mathbf{z}_j \sim \mathcal{CN}(\mathbf{0},\mathbf{I}_N)$ for $j=1,2$. Furthermore, we consider average block power constraints on the transmitters inputs, as

$$\sum_{t=1}^{n} \mathbb{E}[\|\mathbf{x}_i[t]\|^2] \le nP, \qquad \text{for } \ i \in \{1,2\}. \tag{2}$$

For convenience, we let $\mathbf{H}[t] = \begin{bmatrix} \mathbf{H}_{11}[t] & \mathbf{H}_{12}[t] \\ \mathbf{H}_{21}[t] & \mathbf{H}_{22}[t] \end{bmatrix}$ designate the channel state matrix and $\mathbf{H}^{t-1} = \{\mathbf{H}[1],\dots,\mathbf{H}[t-1]\}$ designate the collection of channel state matrices for the past $(t-1)$ symbols. For convenience, we set $\mathbf{H}^0 = \emptyset$. We assume that, at each time instant t, the channel state matrix $\mathbf{H}[t]$ is full rank almost surely. Also, we denote by $\mathbf{y}_j^{t-1} = \{\mathbf{y}_j[1],\dots,\mathbf{y}_j[t-1]\}$ the collection of the outputs at Receiver j, $j=1,2$, over the past $(t-1)$ symbols. At each time instant t, the past states of the channel $\mathbf{H}^{t-1}$ are known to all terminals. However the instantaneous states $(\mathbf{H}_{11}[t],\mathbf{H}_{21}[t])$ are known only to Receiver 1, and the instantaneous states $(\mathbf{H}_{12}[t],\mathbf{H}_{22}[t])$ are known only to Receiver 2. Furthermore, at each time instant, Receiver 1 feeds back the output vector $\mathbf{y}_1^{t-1}$ to Transmitter 1, and Receiver 2 feeds back the output vector $\mathbf{y}_2^{t-1}$ to Transmitter 2.

Definition 1: A code for the Gaussian (M,M,N,N)–MIMO X-channel with local feedback and delayed CSI consists of two sequences of stochastic encoders at the transmitters,

$$\begin{aligned} &\{\phi_{1t} \ : \ \mathcal{W}_{11}\times\mathcal{W}_{12}\times\mathcal{H}^{t-1}\times\mathcal{Y}_1^{N(t-1)} \longrightarrow \mathcal{X}_1^M\}_{t=1}^n \\ &\{\phi_{2t} \ : \ \mathcal{W}_{21}\times\mathcal{W}_{22}\times\mathcal{H}^{t-1}\times\mathcal{Y}_2^{N(t-1)} \longrightarrow \mathcal{X}_2^M\}_{t=1}^n \end{aligned} \tag{3}$$

where the messages W_{11}, W_{12}, W_{21} and W_{22} are drawn uniformly over the sets $\mathcal{W}_{11}$, $\mathcal{W}_{12}$, $\mathcal{W}_{21}$ and $\mathcal{W}_{22}$, respectively; and four decoding functions at the receivers,

$$\begin{aligned} \psi_{11} \ &: \ \mathcal{Y}_1^{Nn}\times\mathcal{H}^{n-1}\times\mathcal{H}_{11}\times\mathcal{H}_{12} \longrightarrow \hat{\mathcal{W}}_{11} \\ \psi_{21} \ &: \ \mathcal{Y}_1^{Nn}\times\mathcal{H}^{n-1}\times\mathcal{H}_{11}\times\mathcal{H}_{12} \longrightarrow \hat{\mathcal{W}}_{21} \\ \psi_{12} \ &: \ \mathcal{Y}_2^{Nn}\times\mathcal{H}^{n-1}\times\mathcal{H}_{21}\times\mathcal{H}_{22} \longrightarrow \hat{\mathcal{W}}_{12} \\ \psi_{22} \ &: \ \mathcal{Y}_2^{Nn}\times\mathcal{H}^{n-1}\times\mathcal{H}_{21}\times\mathcal{H}_{22} \longrightarrow \hat{\mathcal{W}}_{22}. \end{aligned} \tag{4}$$

Definition 2: A rate quadruple $(R_{11}(P),R_{12}(P),R_{21}(P),R_{22}(P))$ is said to be achievable if there exists a sequence of codes such that,

$$\lim_{P\to\infty} \limsup_{n\to\infty} \Pr\{\hat{W}_{ij} \neq W_{ij} | W_{ij}\} = 0, \ \forall\, (i,j) \in \{1,2\}^2. \tag{5}$$

Definition 3: A SDoF quadruple $(d_{11},d_{12},d_{21},d_{22})$ is said to be achievable if there exists a sequence of codes satisfying the following reliability conditions at both receivers,

$$\begin{aligned} &\lim_{P\to\infty} \liminf_{n\to\infty} \frac{\log|\mathcal{W}_{ij}(n,P)|}{n\log P} \ge d_{ij}, \quad \forall \ (i,j) \in \{1,2\}^2 \\ &\lim_{P\to\infty} \limsup_{n\to\infty} \Pr\{\hat{W}_{ij} \neq W_{ij} | W_{ij}\} = 0, \ \forall (i,j) \in \{1,2\}^2 \end{aligned} \tag{6}$$

as well as the perfect secrecy conditions

$$\begin{aligned} &\lim_{P\to\infty} \limsup_{n\to\infty} \frac{I(W_{12},W_{22};\mathbf{y}_1^n,\mathbf{H}^n)}{n\log P} = 0 \\ &\lim_{P\to\infty} \limsup_{n\to\infty} \frac{I(W_{11},W_{21};\mathbf{y}_2^n,\mathbf{H}^n)}{n\log P} = 0. \end{aligned} \tag{7}$$

Definition 4: We define the sum secure degrees of freedom region of the MIMO X-channel with local feedback and delayed CSI, which we denote by $\mathcal{C}^{\text{sum}}_{\text{SDoF}}$, as the set of all of all pairs $(d_{11}+d_{21}, d_{12}+d_{22})$ for all achievable non-negative quadruples $(d_{11}, d_{21}, d_{12}, d_{22})$. We also define the total (sum) secure degrees of freedom as $\text{SDoF}^{\text{d-CSI,F}}_{\text{total}} = \max_{(d_{11},d_{21},d_{12},d_{22})} d_{11} + d_{21} + d_{12} + d_{22}$.

Due to space limitation, the results of this paper are either outlined only or mentioned without proofs. Detailed proofs can be found in [6].

III. Sum SDoF of (M, M, N, N)–MIMO X-channel with local feedback and delayed CSI

For convenience we define the following quantity that we will use extensively in the sequel. Let, for given non-negative (M, N),

$$d_s(N, N, M) = \begin{cases} 0 & \text{if } M \leq N \\ \frac{NM(M-N)}{N^2+M(M-N)} & \text{if } N \leq M \leq 2N \\ \frac{2N}{3} & \text{if } M \geq 2N \end{cases} \quad (8)$$

Theorem 1: The sum SDoF region $\mathcal{C}^{\text{sum}}_{\text{SDoF}}$ of the two-user (M, M, N, N)–MIMO X-channel with local feedback and delayed CSI is given by the set of all non-negative pairs $(d_{11}+d_{21}, d_{12}+d_{22})$ satisfying

$$\begin{aligned} \frac{d_{11}+d_{21}}{d_s(N,N,2M)} + \frac{d_{12}+d_{22}}{\min(2M,2N)} &\leq 1 \\ \frac{d_{11}+d_{21}}{\min(2M,2N)} + \frac{d_{12}+d_{22}}{d_s(N,N,2M)} &\leq 1 \end{aligned} \quad (9)$$

for $2M \geq N$; and $\mathcal{C}^{\text{sum}}_{\text{SDoF}} = \{(0,0)\}$ if $2M \leq N$.

Proof: The converse proof follows by allowing the transmitters to cooperate and then using the outer bound established in [5, Theorem 3] in the context of secure transmission over MIMO broadcast channels with delayed CSI at the transmitter, by taking $2M$ transmit antennas and N antennas at each receiver. Note that Theorem 3 of [5] continues to hold if one provides additional feedback from the receivers to the transmitter. The proof of achievability is given in Section IV.

Remark 1: In the case in which $2M \geq N$, the sum SDoF region of Theorem 1 is characterized fully by the three corner points $(d_s(N, N, 2M), 0)$, $(0, d_s(N, N, 2M))$ and

$$(d_{11} + d_{21}, d_{12} + d_{22}) = \begin{cases} \left(\frac{N(2M-N)}{2M}, \frac{N(2M-N)}{2M}\right) & \text{if } N \leq 2M \leq 2N \\ \left(\frac{N}{2}, \frac{N}{2}\right) & \text{if } 2N \leq 2M \end{cases} \quad (10)$$

Remark 2: The sum SDoF region of Theorem 1 is same as the SDoF region of a two-user MIMO BC in which the transmitter is equipped with $2M$ antennas and each receiver is equipped with N antennas, and delayed CSI is provided to the transmitter [5, Theorem 3]. Therefore, Theorem 1 shows that there is no performance loss in terms of sum SDoF due to the distributed nature of the transmitters in the MIMO X-channel that we consider. Note that, in particular, this implies that, like the setting with no security constraints [1, Theorem 1], the total secure degrees of freedom, defined as in Definition 4 and given by

$$\text{SDoF}^{\text{d-CSI,F}}_{\text{total}} = \begin{cases} 0 & \text{if } 2M \leq N \\ \frac{N(2M-N)}{M} & \text{if } N \leq 2M \leq N \\ N & \text{if } 2M \geq 2N \end{cases} \quad (11)$$

is also preserved upon the availability of output feedback and delayed CSI at the transmitters, although the latters are distributed.

IV. Proof of Direct Part of Theorem 1

In this section, we provide a description of the coding scheme that we use for the proof of Theorem 1. This coding scheme can be seen as an extension, to the case of non-cooperative or distributed transmitters, of that established by Yang *et al.* [5] in the context of secure transmission over a two-user MIMO BC with delayed CSI provided to the transmitter.

In the case in which $2M \geq N$,it is enough to prove that the corner points that are given in Remark 1 are achievable, since the entire region can then be achieved by time-sharing. The achievability of each of the two corner points $(d_s(N, N, 2M), 0)$ follows by the coding scheme of [5, Theorem 1], by having the transmitters sending information messages only to one receiver and the other receiver acting as an eavesdropper. In what follows, we show that the point given by (10) is achievable. We concentrate on the analysis of the case $N \leq 2M \leq 2N$. If $M \geq N$, it is enough to use the coding scheme below with each transmitter utilizing N of its antennas.

A. Case 1: $N \leq 2M \leq 2N$

The achievability in this case follows by a careful combination of Maddah Ali-Tse coding scheme [7] developed for the MIMO broadcast channel with additional noise injection. Also, as we already mentioned, it has connections with, and can be seen as an extension to the case of distributed transmitters of that developed by Yang *et. al.* [5] in the context of secure transmission over a two-user MIMO broadcast channel with delayed CSI at the transmitter. The scheme also extends Tandon *et. al.* [1] coding scheme about X-channels without security constraints to the setting with secrecy. The communication takes place in four phases. For simplicity of the analysis and, in accordance with the degrees of freedom framework, we ignore the additive noise impairment.

Phase 1: Injecting artificial noise

In the first phase, the communication takes place in $T_1 = N^2$ channel uses. Let $\mathbf{u}_1 = [u_1^1, \dots, u_1^{MT_1}]^T$ and $\mathbf{u}_2 = [u_2^1, \dots, u_2^{MT_1}]^T$ denote the artificial noises injected by Transmitter 1 and Transmitter 2 respectively. The channel outputs at Receiver 1 and Receiver 2 during this phase are given by

$$\mathbf{y}_1^{(1)} = \tilde{\mathbf{H}}_{11}^{(1)}\mathbf{u}_1 + \tilde{\mathbf{H}}_{12}^{(1)}\mathbf{u}_2 \quad (12)$$

$$\mathbf{y}_2^{(1)} = \tilde{\mathbf{H}}_{21}^{(1)}\mathbf{u}_1 + \tilde{\mathbf{H}}_{22}^{(1)}\mathbf{u}_2 \quad (13)$$

where $\tilde{\mathbf{H}}_{ji}^{(1)} = \text{diag}(\{\mathbf{H}_{ji}^{(1)}[t]\}_t) \in \mathbb{C}^{NT_1 \times MT_1}$, for $t = 1, \dots, T_1$, $i = 1, 2$, $j = 1, 2$, $\mathbf{y}_1^{(1)} \in \mathbb{C}^{NT_1}$ and $\mathbf{y}_2^{(1)} \in \mathbb{C}^{NT_1}$. During this phase, each receiver gets NT_1 linearly independent equations that relate $2MT_1$ $\mathbf{u}_1$- and $\mathbf{u}_2$-variables. At the end of this phase, the channel output at Receiver i, $i = 1, 2$, is fed back along with the past CSI to Transmitter i.

Phase 2: Fresh information for Receiver 1

In this phase, the communication takes place in $T_2 = N(2M - N)$ channel uses. Both transmitters transmit to Receiver 1 confidential messages that they want to conceal from Receiver 2. To this end, Transmitter 1 sends fresh information $\mathbf{v}_{11} = [v_{11}^1, \dots, v_{11}^{MT_2}]^T$ along with a linear combination of the channel output $\mathbf{y}_1^{(1)}$ of Receiver 1 during the first phase; and Transmitter 2 sends only fresh information $\mathbf{v}_{21} = [v_{21}^1, \dots, v_{21}^{MT_2}]^T$ intended for Receiver 1, i.e.,

$$\mathbf{x}_1 = \mathbf{v}_{11} + \Theta_1\mathbf{y}_1^{(1)}, \qquad \mathbf{x}_2 = \mathbf{v}_{21} \quad (14)$$

where $\Theta_1 \in \mathcal{C}^{MT_2 \times NT_1}$ is a matrix that is known at all nodes and whose choice will be specified below. The channel outputs at the receivers during this phase are given by

$$\mathbf{y}_1^{(2)} = \tilde{\mathbf{H}}_{11}^{(2)}(\mathbf{v}_{11} + \Theta_1 \mathbf{y}_1^{(1)}) + \tilde{\mathbf{H}}_{12}^{(2)} \mathbf{v}_{21} \tag{15a}$$

$$\mathbf{y}_2^{(2)} = \tilde{\mathbf{H}}_{21}^{(2)}(\mathbf{v}_{11} + \Theta_1 \mathbf{y}_1^{(1)}) + \tilde{\mathbf{H}}_{22}^{(2)} \mathbf{v}_{21} \tag{15b}$$

where $\tilde{\mathbf{H}}_{ji}^{(2)} = \text{diag}(\{\mathbf{H}_{ji}^{(2)}[t]\}_t) \in \mathbb{C}^{NT_2 \times MT_2}$, for $t = 1, \ldots, T_2$, $i = 1, 2$, $j = 1, 2$, $\mathbf{y}_1^{(2)} \in \mathbb{C}^{NT_2}$ and $\mathbf{y}_2^{(2)} \in \mathbb{C}^{NT_2}$. At the end of this phase, the channel output at Receiver i, $i = 1, 2$, is fed back along with the delayed CSI to Transmitter i.

Since Receiver 1 knows the CSI $(\tilde{\mathbf{H}}_{11}^{(2)}, \tilde{\mathbf{H}}_{12}^{(2)})$ and the channel output $\mathbf{y}_1^{(1)}$ from Phase 1, it subtracts out the contribution of $\mathbf{y}_1^{(1)}$ from the received signal $\mathbf{y}_1^{(2)}$ and, thus, obtains NT_2 linearly independent equations with $2MT_2$ $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-variables. Thus, Receiver 1 requires $(2M - N)T_2$ extra linearly independent equations to successfully decode the $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-symbols that are intended to it during this phase. Let $\tilde{\mathbf{y}}_2^{(2)} \in \mathbb{C}^{(2M-N)T_2}$ denote a set of $(2M - N)T_2$ such linearly independent equations, selected among the available NT_2 side information equations $\mathbf{y}_2^{(2)} \in \mathbb{C}^{NT_2}$ (recall that $2M - N \leq N$ in this case). If these equations can be conveyed to Receiver 1, they will suffice to help it decode the $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-symbols, since the latter already knows $\mathbf{y}_1^{(1)}$. These equations will be transmitted *jointly* by the two transmitters in Phase 4, and are learned as follows. Transmitter 2 learns $\mathbf{y}_2^{(2)}$, and so $\tilde{\mathbf{y}}_2^{(2)}$, directly by means of the output feedback from Receiver 2 at the end of this phase. Transmitter 1 learns $\mathbf{y}_2^{(2)}$, and so $\tilde{\mathbf{y}}_2^{(2)}$, by means of output as well as delayed CSI feedback from Receiver 1 at the end of Phase 2, as follows. First, Transmitter 1 utilizes the fed back output $\mathbf{y}_1^{(2)}$ to learn the $\mathbf{v}_{21}$-symbols that are transmitted by Transmitter 2 during this phase. This can be accomplished correctly since Transmitter 1, which already knows $\mathbf{v}_{11}$ and $\mathbf{y}_1^{(1)}$, has also gotten the delayed CSI $(\tilde{\mathbf{H}}_{11}^{(2)}, \tilde{\mathbf{H}}_{12}^{(2)})$ and $M \leq N$. Next, Transmitter 1, which also knows the delayed CSI $(\tilde{\mathbf{H}}_{21}^{(2)}, \tilde{\mathbf{H}}_{22}^{(2)})$, reconstructs $\mathbf{y}_2^{(2)}$ as given by (15b).

Phase 3: Fresh information for Receiver 2

This phase is similar to Phase 2, with the roles of Transmitter 1 and Transmitter 2, as well as those of Receiver 1 and Receiver 2, being swapped. More specifically, the communication takes place in $T_2 = N(2M - N)$ channel uses. Fresh information is sent by both transmitters to Receiver 2, and is to be concealed from Receiver 1. Transmitter 1 transmits fresh information $\mathbf{v}_{12} = [v_{12}^1, \ldots, v_{12}^{MT_2}]^T$ to Receiver 2, and Transmitter 2 transmits $\mathbf{v}_{22} = [v_{22}^1, \ldots, v_{22}^{MT_2}]^T$ along with a linear combination of the channel output $\mathbf{y}_2^{(1)}$ at Receiver 2 during Phase 1, i.e.,

$$\mathbf{x}_1 = \mathbf{v}_{12}, \qquad \mathbf{x}_2 = \mathbf{v}_{22} + \Theta_2 \mathbf{y}_2^{(1)} \tag{16}$$

where $\Theta_2 \in \mathcal{C}^{MT_2 \times NT_1}$ is matrix that is known at all nodes and whose choice will be specified below. The channel outputs during this phase are given by

$$\mathbf{y}_1^{(3)} = \tilde{\mathbf{H}}_{11}^{(3)} \mathbf{v}_{12} + \tilde{\mathbf{H}}_{12}^{(3)}(\mathbf{v}_{22} + \Theta_2 \mathbf{y}_2^{(1)}) \tag{17a}$$

$$\mathbf{y}_2^{(3)} = \tilde{\mathbf{H}}_{21}^{(3)} \mathbf{v}_{12} + \tilde{\mathbf{H}}_{22}^{(3)}(\mathbf{v}_{22} + \Theta_2 \mathbf{y}_2^{(1)}) \tag{17b}$$

where $\tilde{\mathbf{H}}_{ji}^{(3)} = \text{diag}(\{\mathbf{H}_{ji}^{(3)}[t]\}_t) \in \mathcal{C}^{NT_2 \times MT_2}$ for $t = 1, \ldots, T_2$, $i = 1, 2$, $j = 1, 2$, $\mathbf{y}_1^{(3)} \in \mathbb{C}^{NT_2}$ and $\mathbf{y}_2^{(3)} \in \mathbb{C}^{NT_2}$. At the end of this phase, the channel output at Receiver i, $i = 1, 2$, is fed back along with the delayed CSI to Transmitter i.

Similar to Phase 2, at the end of Phase 3 Transmitter 1 learns $\mathbf{y}_1^{(3)}$, and so $\tilde{\mathbf{y}}_1^{(3)}$, directly by means of the output feedback from Receiver 1 at the end of this phase. Also, Transmitter 2 learns $\mathbf{y}_1^{(3)}$, and so $\tilde{\mathbf{y}}_1^{(3)}$, by means of output as well as delayed CSI feedback from Receiver 2 at the end of Phase 3.

Phase 4: Interference alignment and decoding

Recall that, at the end of Phase 3, Receiver 1 requires $(2M - N)T_2$ extra equations to successfully decode the sent $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-symbols, and Receiver 2 requires $(2M - N)T_2$ extra equations to successfully decode the sent $\mathbf{v}_{12}$- and $\mathbf{v}_{22}$-symbols. Also, recall that at the end of this third phase, *both* transmitters can re-construct the side information, or interference, equations $\tilde{\mathbf{y}}_1^{(3)} \in \mathbb{C}^{(2M-N)T_2}$ and $\tilde{\mathbf{y}}_2^{(2)} \in \mathbb{C}^{(2M-N)T_2}$ that are required by both receivers. In this phase, both transmitters transmit these equations jointly, as follows.

The communication takes place in $T_3 = (2M - N)^2$ channel uses. Let

$$I = \Phi_1[\ \underbrace{\tilde{\mathbf{y}}_2^{(2)}}_{(2M-N)T_2}\ \ \underbrace{\phi}_{(2N-2M)T_2}\ ]^T + \Phi_2[\ \underbrace{\tilde{\mathbf{y}}_1^{(3)}}_{(2M-N)T_2}\ \ \underbrace{\phi}_{(2N-2M)T_2}\ ]^T$$

where $\Phi_1 \in \mathcal{C}^{2MT_3 \times NT_2}$ and $\Phi_2 \in \mathcal{C}^{2MT_3 \times NT_2}$ are linear combination matrices that are assumed to be known to all the nodes. During this phase, the transmitters send

$$\mathbf{x}_1 = [I^1, \ldots, I^{MT_3}], \qquad \mathbf{x}_2 = [I^{(M+1)T_3}, \ldots, I^{2MT_3}].$$

At the end of Phase 4, Receiver 1 gets NT_3 equations in $2NT_3$ variables. Since Receiver 1 knows $\mathbf{y}_1^{(3)}$ from Phase 3 as well as the CSI, it can subtract out the contribution of $\tilde{\mathbf{y}}_1^{(3)}$ from its received signal to get NT_3 equations in NT_3 variables. Thus, Receiver 1 can recover the $\tilde{\mathbf{y}}_2^{(2)} \in \mathbb{C}^{(2M-N)T_2}$ interference equations. Then, using the pair of output vectors $(\mathbf{y}_1^{(2)}, \tilde{\mathbf{y}}_2^{(2)})$, Receiver 1 first subtracts out the contribution of $\mathbf{y}_1^{(1)}$; and, then, it inverts the resulting $2MT_2$ linearly independent equations relating the sent $2MT_2$ $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-symbols. Thus, Receiver 1 successfully decodes the $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-symbols that are intended to it. Receiver 2 performs similar operations to successfully decode the $\mathbf{v}_{12}$- and $\mathbf{v}_{22}$-symbols that are intended to it.

The complete analysis of the secrecy level that is enabled by this scheme can be found in [6]. Through algebra that we omit here for brevity, it is shown therein that $2MN(2M - N)$ symbols are transmitted securely to each receiver over a total of $4M^2$ time slots, thus yielding the achievability of the sum SDoF point $(d_{11} + d_{21}, d_{12} + d_{22}) = (N(2M - N)/2M, N(2M - N)/2M)$.

V. SDoF of MIMO X-channel with Only Output Feedback

In this section, we focus on the two-user MIMO X-channel with only feedback available at transmitters. We study two special cases of availability of feedback at transmitters, 1) the case in which each receiver feeds back its channel output to both transmitters, to which we will refer as *global feedback*, and 2) the case in which Receiver i, $i = 1, 2$, feeds back its output only to Transmitter i, i.e., local feedback. In both cases, no CSI is provided to the transmitters.

A. MIMO X-channel with global feedback

Theorem 2: The sum SDoF region of the two-user (M, M, N, N)–MIMO X-channel with global output feedback is given by that of Theorem 1.

Remark 3: The sum SDoF region of the MIMO X-channel with global feedback is same as the sum SDoF region of the MIMO X-channel with local feedback and delayed CSI. Investigating the coding scheme of the MIMO X-channel with local feedback and delayed CSI of Theorem 1, it can be seen that the delayed CSI is utilized therein to provide each transmitter with the equations (or, side information) that are heard at the other receiver, which is unintended. With the availability of global feedback, this information is readily available at each transmitter; and, thus, there is no need for any CSI at the transmitters in order to achieve the same sum SDoF as that of Theorem 1.

B. MIMO X-channel with only local feedback

We now consider the case in which only local feedback is provided from the receivers to the receivers, i.e., Receiver i, $i = 1, 2$, feeds back its output to only Transmitter i.
For convenience we define the following quantity. Let, for given non-negative (M, N),

$$d_s^{\text{local}}(N,N,M) = \begin{cases} 0 & \text{if } M \leq N \\ \frac{M^2(M-N)}{2N^2+(M-N)(3M-N)} & \text{if } N \leq M \leq 2N \\ \frac{2N}{3} & \text{if } M \geq 2N \end{cases} \tag{18}$$

Theorem 3: An inner bound on the sum SDoF region of the two-user (M, M, N, N)–MIMO X-channel with local feedback is given by the set of all non-negative pairs $(d_{11} + d_{21}, d_{12} + d_{22})$ satisfying

$$\begin{aligned} \frac{d_{11}+d_{21}}{d_s^{\text{local}}(N,N,2M)} + \frac{d_{12}+d_{22}}{\min(2M,2N)} &\leq 1 \\ \frac{d_{11}+d_{21}}{\min(2M,2N)} + \frac{d_{12}+d_{22}}{d_s^{\text{local}}(N,N,2M)} &\leq 1 \end{aligned} \tag{19}$$

for $2M \geq N$; and $\mathcal{C}^{\text{sum}}_{\text{SDoF}} = \{(0, 0)\}$ if $2M \leq N$.

Remark 4: The main reason for which the SDoF of the MIMO X-channel with local feedback is smaller than that in Theorem 1 for the model with local feedback and delayed CSI can be explained as follows. Consider the Phase 4 in the coding scheme of Theorem 1. Each receiver requires $N(2M - N)(2M - N)$ extra equations to decode the symbols that are intended to it correctly. Given that there are more equations that need to be transmitted to both receivers than the number of available antennas at the transmitters, some of the equations need to be sent by both transmitters, i.e., some of the available antennas send sums of two equations, one intended for each receiver. Then, it can be seen easily that this is only possible if both transmitters know the ensemble of side information equations that they need to transmit, i.e., not only a subset of them corresponding to one receiver. In the coding scheme of Theorem 1, this is made possible by means of availability of both local output feedback and delayed CSI at the transmitters. Similarly, in the coding scheme of Theorem 2, this is made possible by means of availability of global feedback at the transmitters. For the model with only local feedback, however, this is not possible because of the lack of CSI knowledge; and this explains the loss incurred in the sum SDoF region.

VI. MIMO-X Channels Without Security Constraints

In this section, we consider an (M, M, N, N)-X channel *without* security constraints. We show that the main equivalences that we established in the previous sections continue to hold.

Theorem 4: The sum DoF region $\mathcal{C}^{\text{sum}}_{\text{DoF}}$ of the two-user (M, M, N, N)–MIMO X-channel with local feedback and delayed CSI is given by the set of all non-negative pairs $(d_{11}+d_{21}, d_{12}+d_{22})$ satisfying

$$\begin{aligned} \frac{d_{11}+d_{21}}{\min(2M,2N)} + \frac{d_{12}+d_{22}}{\min(2M,N)} &\leq 1 \\ \frac{d_{11}+d_{21}}{\min(2M,N)} + \frac{d_{12}+d_{22}}{\min(2M,2N)} &\leq 1. \end{aligned} \tag{20}$$

Remark 5: The sum DoF region of Theorem 4 is same as the DoF region of a two-user MIMO BC in which the transmitter is equipped with $2M$ antennas and each receiver is equipped with N antennas, and delayed CSIT is provided to the transmitter [8, Theorem 2]. Thus, similar to Theorem 1, Theorem 4 shows that, in the context of no security constraints as well, the distributed nature of the transmitters in the MIMO X-model with a symmetric antenna configuration does not cause any loss in terms of sum degrees of freedom. This can be seen as a generalization of [1, Theorem 1] in which it is shown that the loss is zero from a total degrees of freedom perspective.

Remark 6: Like for the setting with secrecy constraints, it can be easily shown that the sum DoF of the (M, M, N, N)-MIMO X-channel with global output feedback is also given by that of Theorem 4.

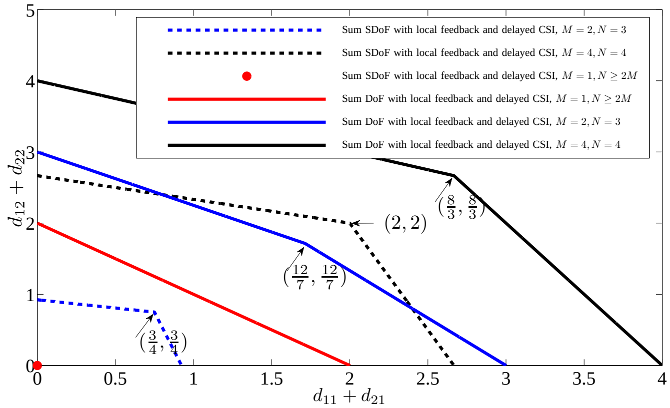

Fig. 2. Sum SDoF and sum DoF regions of the (M, M, N, N)-X channel with local output feedback and delayed CSI, for different antennas configurations.

Figure 2 illustrates the optimal sum SDoF and sum DoF regions of the (M, M, N, N)-MIMO X-channel with local output feedback and delayed CSI as given in Theorem 1 and Theorem 4, respectively, for different values of the transmit- and receive antennas.

References

[1] R. Tandon, S. Mohajer, H. V. Poor, and S. Shamai (Shitz), "On X-channels with feedback and delayed CSI," in *Proc. IEEE Int. Symp. Information Theory*, Boston, USA, Jul. 2012, pp. 1887–1891.

[2] L. Yang and W. Zhang, "On achievable degrees of freedom for MIMO X channels," *IEEE Trans. Inf. Theory, submitted for publication, available at arxiv.org/abs/1208.2900*, Aug. 2012.

[3] H. Maleki, V. R. Cadambe, and S. A. Jafar, "Index coding: an interference alignment perspective," *IEEE Trans. Inf. Theory, submitted for publication, available at arxiv.org/abs/1205.1483v1*, May 2012.

[4] H. Sun, C. Geng, and S. A. Jafar, "Topological interference management with alternating connectivity," *IEEE Trans. Inf. Theory, submitted for publication, available at arxiv.org/abs/1302.4020*, Feb. 2013.

[5] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai (Shitz), "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Trans. Inf. Theory, submitted for publication, available at arxiv.org/abs/1112.2306*, 2011.

[6] A. Zaidi, Z. Awan, S. Shamai (Shitz), and L. Vandendorpe, "Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSi," *Draft, available at http://www-syscom.univ-mlv.fr/∼zaidi/publications/proofs-itw2013.pdf*, 2013.

[7] M. A. Maddah-Ali and D. Tse, "Completely stale transmitter channel state information is still very useful," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4418–4431, Jul. 2012.

[8] C. S. Vaze and M. K. Varanasi, "The degrees of freedom region of the two-user and certain three-user mimo broadcast channel with delayed CSI," 2011. [Online]. Available: http://arxiv.org/abs/1101.0306