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

Abdellatif Zaidi, Zohaib Hassan Awan, Shlomo Shamai (Shitz) *Fellow, IEEE*, Luc Vandendorpe *Fellow, IEEE*

Abstract

We investigate the problem of secure transmission over a two-user multi-input multi-output (MIMO) X-channel in which channel state information is provided with one-unit delay to both transmitters (CSIT), and each receiver feeds back its channel output to a different transmitter. We refer to this model as MIMO X-channel with *asymmetric* output feedback and delayed CSIT. The transmitters are equipped with M antennas each, and the receivers are equipped with N antennas each. For this model, accounting for both messages at each receiver, we characterize the optimal sum secure degrees of freedom (SDoF) region. We show that, in presence of asymmetric output feedback and delayed CSIT, 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

Abdellatif Zaidi is with Université Paris-Est Marne-la-Vallée, 77454 Marne-la-Vallée Cedex 2, France. Email: abdellatif.zaidi@univ-mlv.fr

Zohaib Hassan Awan was with the ICTEAM institute, Université catholique de Louvain, Louvain-la-Neuve. Email: zohaib.awan@uclouvain.be

Shlomo Shamai (Shitz) is with the Department of Electrical Engineering, Technion Institute of Technology, Technion City, Haifa 32000, Israel. Email: sshlomo@ee.technion.ac.il

Luc Vandendorpe is with the ICTEAM institute (École Polytechnique de Louvain), Université catholique de Louvain, Louvain-la-Neuve 1348, Belgium. Email: luc.vandendorpe@uclouvain.be

This work has been supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications (NEWCOM#), and the Concerted Research Action, SCOOP. The authors would also like to thank BELSPO for the support of the IAP BESTCOM network.

The results in this work will be presented in part at the IEEE Information Theory Workshop, Sept. 2013.

transmitter, N antennas at each receiver and delayed CSIT. This result shows that, upon availability of asymmetric output feedback and delayed CSIT, there is no performance loss in terms of sum SDoF due to the distributed nature of the transmitters. Next, we show that this result also holds if only output feedback is conveyed to the transmitters, but in a *symmetric* manner, i.e., each receiver feeds back its output to both transmitters and no CSIT. We also study the case in which only asymmetric output feedback is provided to the transmitters, i.e., without CSIT, 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 DoF region of the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT is same as the DoF region of a two-user MIMO BC with $2M$ antennas at the transmitter, N antennas at each receiver, and delayed CSIT. We illustrate our results with some numerical examples.

I. Introduction

In modern era, there is a growing requirement for high data rates in wireless networks, in which multiple users communicate with each other over a shared medium. The information transmission by multiple users on a common channel raises an important issue of interference in networks. In existing literature on multi-user channels, such as [1], several interference alignment techniques have been proposed. Most of these techniques rely on the availability of perfect channel state information at the transmitting nodes (CSIT). However, because the wireless medium is characterized by its inherent randomness, such an assumption is rather idealistic and is difficult to obtain in practice. In [2], Maddah-Ali and Tse study a multi-input single-output (MISO) broadcast channel with delayed CSI available at the transmitter, from a degrees of freedom (DoF) perspective. They show that delayed (or stale) CSIT is useful, in the sense that it increases the DoF region in comparison with the same MISO setting without any CSIT. The model with delayed CSIT of [2] has been extended to study a variety of models. These include the two-user MIMO BC [3], the three-user MIMO BC [3], [4], the two-user MIMO interference channel [5], [6], and the K-user single-input single-output (SISO) interference and X-channels [7], [8].

In [9], Jafar and Shamai introduced a two-user X-channel model. The two-user X-channel consists of two transmitters and two receivers, with each transmitter sending two independent messages to both receivers. For this model, the authors establish bounds on the DoF region under the assumption of full CSIT. In [10], Maleki *et al.* study a two-user SISO X-channel with output feedback provided asymmetrically to the transmitters. They establish a lower bound on the allowed sum DoF. For MIMO X-channels, the setting with no CSIT is studied in [11]; the setting with delayed CSIT is studied [12]; and the setting with delayed CSIT and asymmetric noiseless output feedback is studied in [13], all from

a DoF viewpoint. In all these works, a symmetric antenna topology is assumed, with each transmitter being equipped with M antennas and each receiver equipped with N antennas. In [12], it is assumed that each receiver knows the CSI of its own channel and also the past CSI of the channel to the other receiver. Also, the past CSI available at each receiver is provided to the corresponding transmitter over a noiseless link. For this model, the authors establish a lower bound on the sum DoF over all messages in the network (in the rest of this paper, we will refer to this as being the *total* DoF). In [13], Tandon *et al.* study a model which is similar to the one that is investigated in [12], but with additional asymmetric noiseless output feedback from the receivers to the transmitters. In particular, they show that the total DoF of this two-user MIMO X-channel with asymmetric output feedback and delayed CSIT is same as the total DoF of a two-user broadcast channel with delayed CSIT, with $2M$ transmit antennas and N antennas at each receiver. For this model, the availability of the output feedback together with the delayed CSIT help each transmitter reconstruct the information transmitted by the other transmitter. The reader may refer to [14]–[16] for some other related works.

In his seminal work [17], Wyner introduced a basic information-theoretic model to study security by exploiting the physical layer attributes of the channel. The model consists of a sender which transmits information to a legitimate receiver; and this information is meant to be kept secret from an external wiretapper that overhears the transmission. Wyner's basic setup has been extended to study the secrecy capacity of various multiuser channels, such as the broadcast channel [18], [19], the multi-antennas wiretap channel [20]–[23], the multiple access wiretap channel [24]–[28], the relay channel [29]–[31], the interference channel [32], [33] and X networks [34] (the reader may also refer to [35] for a review of many other related contributions). In [36], the authors study a K-user interference channel with security constraints, from a SDoF perspective. Similar to the setting with no security constraints, the SDoF captures the way the spatial multiplexing gain, or secrecy capacity prelog or degrees of freedom, scales asymptotically with the logarithm of the signal-to-noise ratio (SNR). In [37], the authors study a K-user Gaussian multiaccess channel with an external eavesdropper, and derive a lower bound on the allowed total SDoF under the assumption of perfect instantaneous CSI available at the transmitter and receivers. In [38], Yang *et al.* study secure transmission over a two-user MIMO BC with delayed CSIT. They provide an exact characterization of the SDoF region. The coding scheme of [38] can be seen as an appropriate extension of Maddah Ali-Tse scheme [2] to accommodate additional noise injection that accounts for security constraints.

In this paper, 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 as shown in Figure 1. Transmitter 1 wants

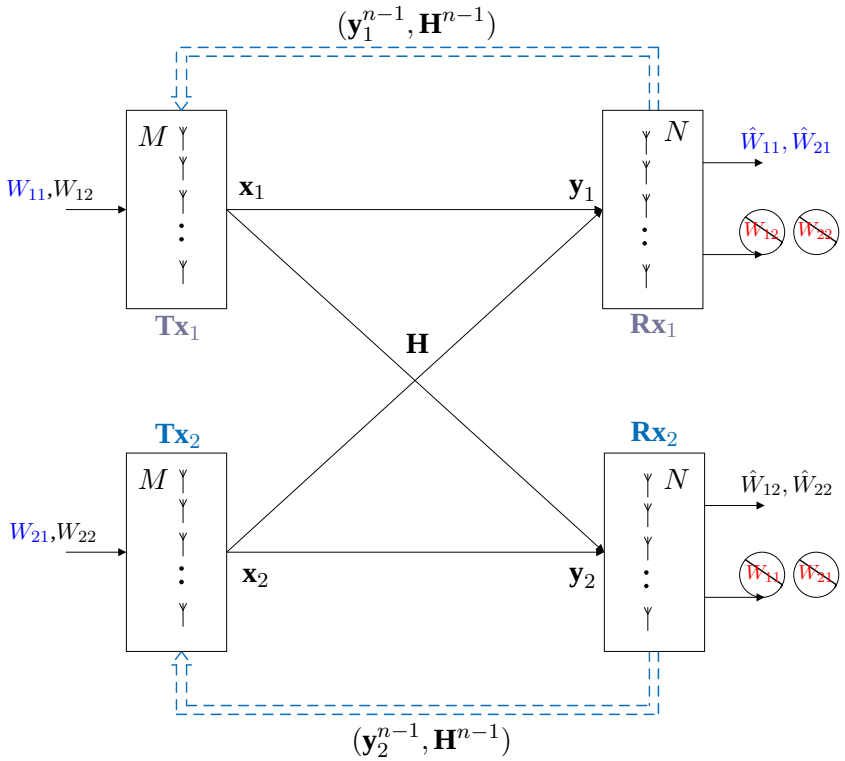

Fig. 1. MIMO X-channel with asymmetric output feedback and delayed CSIT, with security constraints.

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 *asymmetric*, by opposition to *symmetric* 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. Both eavesdroppers are assumed to be passive, i.e., they are not allowed to modify the transmission. The model that we study can be seen as being that of [13] 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.

A. Contributions

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 asymmetric output feedback and delayed CSIT 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 BC with delayed CSIT, $2M$ transmit antennas and N antennas at each receiver. This result shows that, for symmetric antennas configurations, the distributed nature of the transmitters does not cause any loss in terms of sum SDoF. The result also emphasizes the usefulness of asymmetric output feedback when used in conjunction with delayed CSIT 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 asymmetric output feedback with delayed CSIT does increase the DoF region as shown in [13], 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 the one developed by Yang *et al.* [38] in the context of secure transmission over a two-user MIMO BC with delayed CSIT; and it demonstrates how each transmitter exploits optimally the available output feedback and delayed CSIT.

Next, concentrating on the role of output feedback in the absence of CSIT 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 *symmetric* output feedback. As we mentioned previously, this output feedback is assumed to be provided noiselessly by both receivers to both transmitters. In the second model, the transmitters are provided with only asymmetric output feedback, i.e., the model of Figure 1 but with no CSIT at all.

For the model with symmetric output feedback at the transmitters, we show that the sum SDoF region is same as the sum SDoF region of the model with asymmetric output feedback and delayed CSIT, i.e., the model of Figure 1. In other words, the lack of CSIT does not cause any loss in terms of sum SDoF region as long as each transmitter is provided with output feedback from both recievers. In this case, each transmitter readily gets the side information or interference that is available at the unintended receiver by means of the output feedback; and, therefore, it can align it with the information that is destined to

the intended receiver directly, with no need of any CSIT.

For the model in which only asymmetric 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 CSIT. This loss is caused by the fact that, unlike the coding schemes that we develop for the setting with asymmetric output feedback and delayed CSIT and that with symmetric output feedback, for the model with only asymmetric output 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 DoF region of the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT is same of the DoF region of a two-user MIMO BC with $2M$ transmit-antennas, N antennas at each receiver, and delayed CSIT. Finally, we illustrate our results with some numerical examples.

This paper is structured as follows. Section II provides a formal description of the channel model that we consider, together with some useful definitions. Section III states the sum SDoF region of the two-user (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT of Figure 1. In section IV, we provide the formal proof of the coding scheme that we use to establish the achievability result. In section V, we study the role of output feedback in the absence of CSIT. In Section VI, we specialize the results to the setting with no security constraints; and, in Section VII, we illustrate our results through some numerical examples. Finally, section VIII concludes the paper by summarizing its contributions.

B. Notation

We use the following notations throughout the paper. Boldface upper case letters, e.g., $\mathbf{X}$, denote matrices; boldface lower case letters, e.g., $\mathbf{x}$, denote vectors; and calligraphic letters designate alphabets, i.e., $\mathcal{X}$. For integers $i \leq j$, we use the notation $\mathbf{X}_i^j$ as a shorthand for $(\mathbf{X}_i, \ldots, \mathbf{X}_j)$. The notation $\text{diag}(\{\mathbf{H}[t]\}_t)$ denotes the block diagonal matrix with $\mathbf{H}[t]$ as diagonal elements for all t. The Gaussian distribution with mean μ and variance σ^2 is denoted by $\mathcal{CN}(\mu, \sigma^2)$. Finally, throughout the paper, logarithms are taken to base 2, and the complement to unity of a scalar $u \in [0, 1]$ is denoted by $\bar{u}$, i.e., $\bar{u} = 1 - u$.

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 $W_{11} \in \mathcal{W}_{11} = \{1, \ldots, 2^{nR_{11}(P)}\}$ to Receiver 1, and message $W_{12} \in \mathcal{W}_{12} = \{1, \ldots, 2^{nR_{12}(P)}\}$ to Receiver 2. Similarly, Transmitter 2 wants to transmit message $W_{21} \in \mathcal{W}_{21} = \{1, \ldots, 2^{nR_{21}(P)}\}$ to Receiver 1, and message $W_{22} \in \mathcal{W}_{22} = \{1, \ldots, 2^{nR_{22}(P)}\}$ 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_{12}, W_{22}) that is intended to Receiver 2 is meant to be concealed from Receiver 1. Both eavesdroppers are allowed to only overhear the transmission and not modify it, i.e., are assumed to be *passive*.

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

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

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

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

For convenience, we let $\mathbf{H}[t] = \left[\begin{smallmatrix} \mathbf{H}_{11}[t] & \mathbf{H}_{12}[t] \\ \mathbf{H}_{21}[t] & \mathbf{H}_{22}[t] \end{smallmatrix}\right]$ designate the channel state matrix and $\mathbf{H}^{t-1} = \{\mathbf{H}[1], \ldots, \mathbf{H}[t-1]\}$ 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 $\mathbf{y}_j^{t-1} = \{\mathbf{y}_j[1], \ldots, \mathbf{y}_j[t-1]\}$ 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 $(\mathbf{H}_{11}[t], \mathbf{H}_{12}[t])$ are known only to Receiver 1, and the instantaneous states $(\mathbf{H}_{21}[t], \mathbf{H}_{22}[t])$ 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.

From a practical viewpoint, the two-user MIMO X-channel with asymmetric output feedback and delayed CSIT of Figure 1 may model a cellular network in which two base stations communicate with two destinations. Each base station sends information messages to both receivers; and, in doing so, it wants to keep the information that is sent to each receiver secret from the other receiver. Here, by opposition to classic wiretap channels in which the eavesdropper is generally not willing to feed back information about its channel to the transmitter from which it wants to intercept the transmission, each receiver is not merely an eavesdropper for the information sent by the transmitters to the other receiver but is also a legitimate receiver intended to get other information messages from the *same* transmitters. For this reason, in its desire to help the transmitters obtain a better estimate of the channel, the receivers may find it useful to feedback information on their channels to the transmitters. Depending on the strength of the feedback signal, this may be heard at both or only one of the transmitters.

Definition 1: A code for the Gaussian (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT 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,

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

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,

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

as well as the perfect secrecy conditions

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

Definition 4: We define the sum secure degrees of freedom region of the MIMO X-channel with asymmetric output feedback and delayed CSIT, which we denote by $\mathcal{C}_{\text{SDoF}}^{\text{sum}}$, 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 secure degrees of freedom as $\text{SDoF}_{\text{total}}^{\text{d-CSIT,F}} = \max_{(d_{11},d_{21},d_{12},d_{22})} d_{11} + d_{21} + d_{12} + d_{22}$.

III. Sum SDoF of (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT

In this section we state our main result on the optimal sum SDoF region of the two-user MIMO X-channel with asymmetric output feedback and delayed CSIT. We illustrate our result by providing few examples which give insights into the proposed coding scheme.

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

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

The following theorem characterizes the sum SDoF region of the MIMO X-channel with asymmetric output feedback and delayed CSIT.

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

satisfying

$$\frac{d_{11}+d_{21}}{d_s(N,N,2M)}+\frac{d_{12}+d_{22}}{\min(2M,2N)}\leq 1$$
$$\frac{d_{11}+d_{21}}{\min(2M,2N)}+\frac{d_{12}+d_{22}}{d_s(N,N,2M)}\leq 1 \tag{9}$$

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

Proof: The converse proof follows by allowing the transmitters to cooperate and then using the outer bound established in [38, Theorem 3] in the context of secure transmission over MIMO broadcast channels with delayed CSIT, by taking $2M$ transmit antennas and N antennas at each receiver. Note that Theorem 3 of [38] 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

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

Remark 2: The sum SDoF region of Theorem 1 is same as the SDoF region of a two-user MIMO BC with delayed CSIT in which the transmitter is equipped with $2M$ antennas and each receiver is equipped with N antennas [38, Theorem 3]. Therefore, Theorem 1 shows that there is no performance loss in terms of total 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 [13, Theorem 1], the total secure degrees of freedom, defined as in Definition 4 and given by

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

is also preserved upon the availability of asymmetric output feedback and delayed CSI at the transmitters, even though the transmitters are distributed.

Figure 2 illustrates the optimal sum SDoF region of the (M,M,N,N)–MIMO X-channel with asymmetric output feedback and delayed CSIT as given in Theorem 1, for different values of the transmit- and receive-antennas. Obviously, secure messages transmission is not possible if, accounting for the antennas

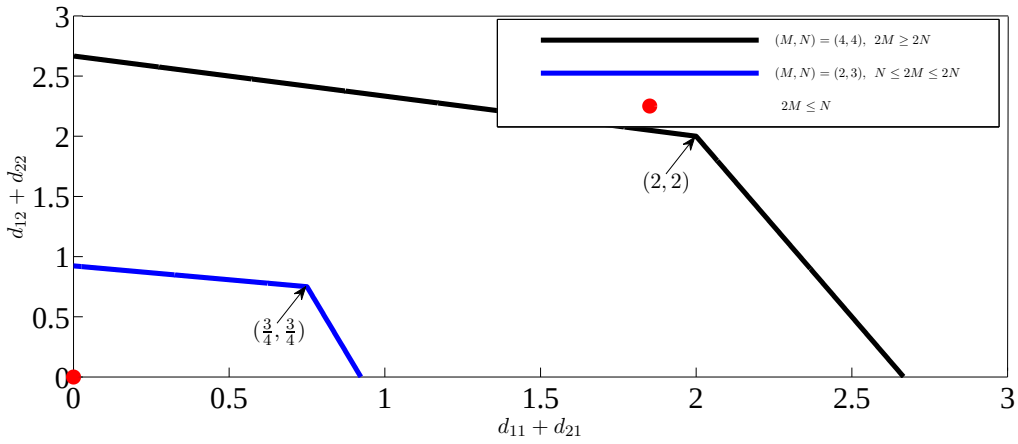

Fig. 2. Sum SDoF region of the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT, for different antennas configurations.

Case	$\text{SDoF}_{\text{total}}^{\text{d-CSIT,F}}$	$\text{DoF}_{\text{total}}^{\text{d-CSIT,F}}$ [13]	$\text{DoF}_{\text{total}}^{\text{n-CSIT,nF}}$ [11]
$2M \leq N$	0	$2M$	$2M$
$N \leq 2M \leq 2N$	$\frac{N(2M-N)}{M}$	$\frac{4MN}{2M+N}$	N
$2N \leq 2M$	N	$\frac{4N}{3}$	N

TABLE I

TOTAL SDOF AND TOTAL DOF OF (M, M, N, N)–MIMO X-CHANNELS WITH DIFFERENT DEGREES OF OUTPUT FEEDBACK AND DELAYED CSIT.

available at both transmitters, there are less transmit antennas than receive antennas at each receiver, i.e., $2M \leq N$. Also, the sum SDoF region increases with the pair (M, N) if $N \leq 2M \leq 2N$. For a given number N of receiver antennas at each receiver, the sum SDoF region no longer increases with the number of transmit-antennas M at each transmitter as long as $M \geq N$. This shows that, from a SDoF perspective, there is no gain from equipping the transmitters with more than N antennas each. A similar behavior is shown in Table I and Figure 3 from a total secure degrees of freedom viewpoint. Table I summarizes the optimal total SDoF of the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT as given by (11), as well as the total DoF of the (M, M, N, N)–MIMO X-channel without security constraints, with asymmetric output feedback and delayed CSIT [13, Theorem 1] and with no output feedback and no CSIT [11, Theorem 11]. Figure 3 depicts the evolution of the total SDoF (11) as a function of the number of transmit antennas at each transmitter, for an example

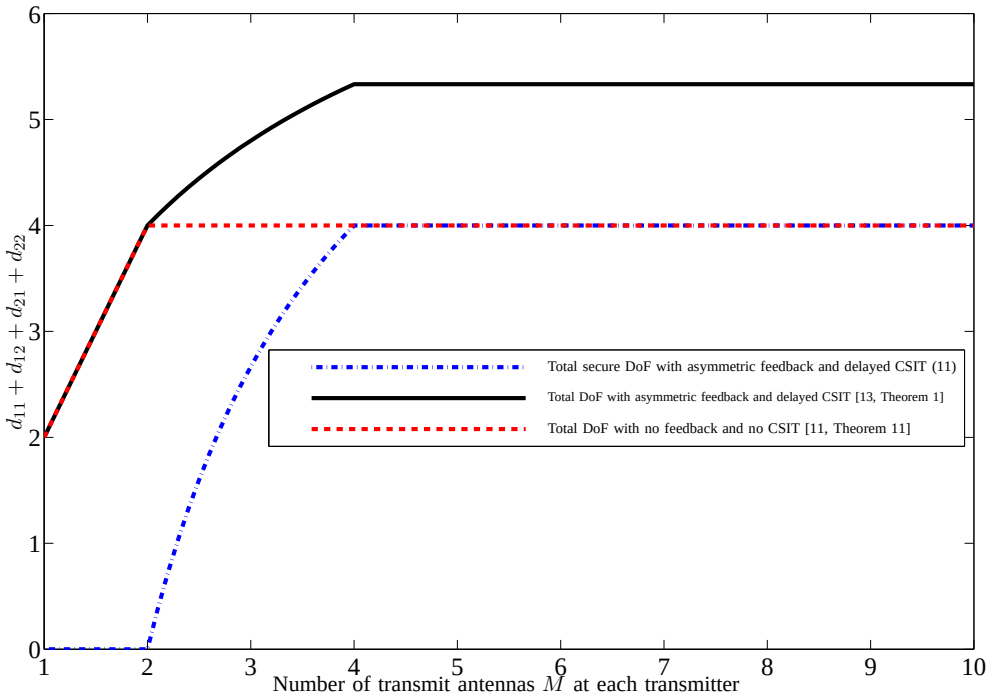

Fig. 3. Total secure degrees of freedom of the (M, M, N, N)–MIMO X-channel as a function of the number of transmit antennas M at each transmitter, for a fixed number $N = 4$ of receive antennas at each receiver.

configuration in which each receiver is equipped with $N = 4$ antennas. It is interesting to note that, for the case $M \geq N$ the total SDoF of the MIMO X-channel with asymmetric output feedback and delayed CSIT is same as the DoF of the MIMO X-channel with no feedback and no CSIT. Thus, providing the transmitters with asymmetric output feedback and delayed CSIT can be interpreted as the price for secrecy in this case.

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.* [38] in the context of secure transmission over a two-user MIMO BC with delayed CSIT.

In the case in which $2M \leq N$, every receiver has enough antennas to decode all of the information that is sent by the transmitters; and, so, secure transmission of messages is not possible. 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 [38, 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 divide the analysis into two cases.

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

The achievability in this case follows by a careful combination of Maddah Ali-Tse coding scheme [2] 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.* [38] in the context of secure transmission over a two-user MIMO BC with delayed CSIT. The scheme also extends Tandon *et al.* [13] 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 DoF 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 $\mathbf{u}_1 = [u_1^1, \ldots, u_1^{MT_1}]^T$ and $\mathbf{u}_2 = [u_2^1, \ldots, u_2^{MT_1}]^T$ 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

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

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

where $\tilde{\mathbf{H}}_{ji}^{(1)} = \text{diag}(\{\mathbf{H}_{ji}^{(1)}[t]\}_t) \in \mathbb{C}^{NT_1 \times MT_1}$, for $t = 1, \ldots, T_1$, $i = 1, 2$, $j = 1, 2$, $\mathbf{y}_1^{(1)} \in \mathbb{C}^{NT_1}$ 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 $\mathbf{v}_{11} = [v_{11}^1, \ldots, v_{11}^{MT_2}]^T$ 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

$\mathbf{v}_{21} = [v_{21}^1, \ldots, v_{21}^{MT_2}]^T$ intended for Receiver 1, i.e.,

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

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.,

$$\begin{aligned} \mathbf{x}_1 &= \mathbf{v}_{12} \\ \mathbf{x}_2 &= \mathbf{v}_{22} + \Theta_2 \mathbf{y}_2^{(1)} \end{aligned} \tag{16}$$

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 since Receiver 2 knows the CSI $(\tilde{\mathbf{H}}_{21}^{(3)}, \tilde{\mathbf{H}}_{22}^{(3)})$ and the channel output $\mathbf{y}_2^{(1)}$ from Phase 1, it subtracts out the contribution of $\mathbf{y}_2^{(1)}$ from the received signal $\mathbf{y}_2^{(3)}$ and, thus, obtain NT_2 linearly independent equations with $2MT_2$ $\mathbf{v}_{12}$- and $\mathbf{v}_{22}$-variables. Thus, similar to Receiver 1 at the end of Phase 2, Receiver 2 requires $(2M-N)T_2$ extra linearly independent equations to successfully decode the $\mathbf{v}_{12}$- and $\mathbf{v}_{22}$-symbols that are intended to it during this phase. Let $\tilde{\mathbf{y}}_1^{(3)} \in \mathbb{C}^{(2M-N)T_2}$ denote a set of $(2M - N)T_2$ such linearly independent equations, selected among the available NT_2 side information equations $\mathbf{y}_1^{(3)} \in \mathbb{C}^{NT_2}$. If these equations can be conveyed to Receiver 2, they will suffice to help it decode the $\mathbf{v}_{12}$- and $\mathbf{v}_{22}$-symbols, since the latter already knows $\mathbf{y}_2^{(1)}$. These equations will be transmitted *jointly* by the two transmitters in Phase 4, and are learned as follows. 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. 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, as follows. First, Transmitter 2 utilizes the fed back output $\mathbf{y}_2^{(3)}$ to learn the $\mathbf{v}_{12}$-symbols that are transmitted by Transmitter 1 during this phase. This can be accomplished correctly since Transmitter 2, which already knows $\mathbf{v}_{22}$ and $\mathbf{y}_2^{(1)}$, has also gotten the delayed CSI $(\tilde{\mathbf{H}}_{21}^{(3)}, \tilde{\mathbf{H}}_{22}^{(3)})$ and $M \leq N$. Next, Transmitter 2, which also knows the delayed CSI $(\tilde{\mathbf{H}}_{11}^{(3)}, \tilde{\mathbf{H}}_{12}^{(3)})$, reconstructs $\mathbf{y}_1^{(3)}$ as given by (17a).

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 reconstruct 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

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

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

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

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.

Security Analysis

The analysis and algebra in this section are similar to in [38] in the context of secure broadcasting of messages on a two-user MIMO broadcast channel with delayed CSIT.

At the end of Phase 4, the channel outputs at the receivers can be written as

$$\mathbf{y}_1 =$$

$$\underbrace{\begin{bmatrix} \tilde{\mathbf{H}}_2 & \tilde{\mathbf{H}}_{11}^{(2)}\Theta_1 & \mathbf{0} \\ \tilde{\mathbf{H}}_4\Phi_1\tilde{\mathbf{G}}_2 & \tilde{\mathbf{H}}_4\Phi_1\tilde{\mathbf{H}}_{21}^{(2)}\Theta_1 & \tilde{\mathbf{H}}_4\Phi_2 \\ \mathbf{0} & \mathbf{I}_{NT_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{NT_2} \end{bmatrix}}_{\hat{\mathbf{H}} \in \mathbb{C}^{4M^2N \times 4M^2N}} \begin{bmatrix} \mathbf{v}_1 \\ \tilde{\mathbf{H}}_1\mathbf{u} \\ \tilde{\mathbf{H}}_3\mathbf{v}_2 + \tilde{\mathbf{H}}_{12}^{(3)}\Theta_2\tilde{\mathbf{G}}_1\mathbf{u} \end{bmatrix} \tag{18}$$

$$\mathbf{y}_2 = \underbrace{\begin{bmatrix} \mathbf{0} & \mathbf{I}_{NT_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{NT_2} \\ \tilde{\mathbf{G}}_3 & \tilde{\mathbf{H}}_{22}^{(3)}\Theta_2 & \mathbf{0} \\ \tilde{\mathbf{G}}_4\Phi_2\tilde{\mathbf{H}}_3 & \tilde{\mathbf{G}}_4\Phi_2\tilde{\mathbf{H}}_{12}^{(3)}\Theta_2 & \tilde{\mathbf{G}}_4\Phi_1 \end{bmatrix}}_{\hat{\mathbf{G}} \in \mathbb{C}^{4M^2N \times 4M^2N}} \begin{bmatrix} \mathbf{v}_2 \\ \tilde{\mathbf{G}}_1\mathbf{u} \\ \tilde{\mathbf{G}}_2\mathbf{v}_1 + \tilde{\mathbf{H}}_{21}^{(2)}\Theta_1\tilde{\mathbf{H}}_1\mathbf{u} \end{bmatrix} \tag{19}$$

where $\tilde{\mathbf{H}}_t = [\tilde{\mathbf{H}}_{11}^{(t)} \;\; \tilde{\mathbf{H}}_{12}^{(t)}]$, $\tilde{\mathbf{G}}_t = [\tilde{\mathbf{H}}_{21}^{(t)} \;\; \tilde{\mathbf{H}}_{22}^{(t)}]$, for $t = 1, \ldots, 4$, $\mathbf{u} = [\mathbf{u}_1^T \;\; \mathbf{u}_2^T]^T$, $\mathbf{v}_1 = [\mathbf{v}_{11}^T \;\; \mathbf{v}_{21}^T]^T$, and $\mathbf{v}_2 = [\mathbf{v}_{12}^T \;\; \mathbf{v}_{22}^T]^T$. The information rate to Receiver 1 is given by the mutual information $I(\mathbf{v}_1; \mathbf{y}_1)$, and can be evaluated as

$$\begin{aligned} I(\mathbf{v}_1; \mathbf{y}_1) &= I(\mathbf{v}_1, \tilde{\mathbf{H}}_1\mathbf{u}, \tilde{\mathbf{H}}_3\mathbf{v}_2 + \tilde{\mathbf{H}}_{12}^{(3)}\Theta_2\tilde{\mathbf{G}}_1\mathbf{u}; \mathbf{y}_1) \\ &\quad - I(\tilde{\mathbf{H}}_1\mathbf{u}, \tilde{\mathbf{H}}_3\mathbf{v}_2 + \tilde{\mathbf{H}}_{12}^{(3)}\Theta_2\tilde{\mathbf{G}}_1\mathbf{u}; \mathbf{y}_1 | \mathbf{v}_1) \\ &\overset{(a)}{=} \text{rank}(\hat{\mathbf{H}}).\log(2P) - \text{rank}\begin{pmatrix} \tilde{\mathbf{H}}_{11}^{(2)}\Theta_1 & \mathbf{0} \\ \tilde{\mathbf{H}}_4\Phi_1\tilde{\mathbf{H}}_{21}^{(2)}\Theta_1 & \tilde{\mathbf{H}}_4\Phi_2 \\ \mathbf{I}_{NT_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{NT_2} \end{pmatrix}.\log(2P) \\ &\overset{(b)}{=} N(T_1+T_2).\log(2P) + \text{rank}\begin{pmatrix} \tilde{\mathbf{H}}_2 \\ \tilde{\mathbf{H}}_4\Phi_1\tilde{\mathbf{G}}_2 \end{pmatrix}.\log(2P) \\ &\quad - N(T_1+T_2).\log(2P) \\ &= \text{rank}\begin{pmatrix} \tilde{\mathbf{H}}_2 \\ \tilde{\mathbf{H}}_4\Phi_1\tilde{\mathbf{G}}_2 \end{pmatrix}.\log(2P) \end{aligned}$$

$$\stackrel{(c)}{=} 2MN(2M-N).\log(2P) \tag{20}$$

where (a) follows from [38, Lemma 2]; (b) follows from the block diagonalization structure of $\hat{\mathbf{H}}$; and (c) follows by reasoning as in [38] for the selection of Φ_1 with appropriate rank such that the equality holds.

Similarly, the information leaked to Receiver 2 can be bounded as

$$\begin{aligned}
&I(\mathbf{v}_1;\mathbf{y}_2) = I(\mathbf{v}_1;\mathbf{y}_2|\mathbf{v}_2) \leq I(\tilde{\mathbf{G}}_2\mathbf{v}_1;\mathbf{y}_2|\mathbf{v}_2)\\
&= I(\tilde{\mathbf{G}}_2\mathbf{v}_1,\mathbf{u};\mathbf{y}_2|\mathbf{v}_2) - I(\mathbf{u};\mathbf{y}_2|\tilde{\mathbf{G}}_2\mathbf{v}_1,\mathbf{v}_2)\\
&\leq I(\tilde{\mathbf{G}}_1\mathbf{u},\tilde{\mathbf{G}}_2\mathbf{v}_1+\tilde{\mathbf{H}}_{21}^{(2)}\Theta_1\tilde{\mathbf{H}}_1\mathbf{u};\mathbf{y}_2|\mathbf{v}_2) - I(\mathbf{u};\mathbf{y}_2|\tilde{\mathbf{G}}_2\mathbf{v}_1,\mathbf{v}_2)\\
&\stackrel{(a)}{=} \text{rank}\begin{pmatrix} \mathbf{I}_{NT_1} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}_{NT_2}\\ \tilde{\mathbf{H}}_{22}^{(3)}\Theta_2 & \mathbf{0}\\ \tilde{\mathbf{G}}_4\Phi_2\tilde{\mathbf{H}}_{12}^{(3)}\Theta_2 & \tilde{\mathbf{G}}_4\Phi_1\end{pmatrix}.\log(2P)\\
&- \text{rank}\begin{pmatrix} \tilde{\mathbf{G}}_1\\ \tilde{\mathbf{H}}_{21}^{(2)}\Theta_1\tilde{\mathbf{H}}_1\\ \tilde{\mathbf{H}}_{22}^{(3)}\Theta_2\tilde{\mathbf{G}}_1\\ \tilde{\mathbf{G}}_4\Phi_2\tilde{\mathbf{H}}_{12}^{(3)}\Theta_2\tilde{\mathbf{G}}_1+\tilde{\mathbf{G}}_4\Phi_1\tilde{\mathbf{H}}_{21}^{(2)}\Theta_1\tilde{\mathbf{H}}_1\end{pmatrix}.\log(2P)\\
&= N(T_1+T_2).\log(2P) - \text{rank}\begin{pmatrix}\tilde{\mathbf{G}}_1\\ \tilde{\mathbf{H}}_{21}^{(2)}\Theta_1\tilde{\mathbf{H}}_1\end{pmatrix}.\log(2P)\\
&\stackrel{(b)}{=} 0
\end{aligned} \tag{21}$$

where (a) follows from [38, Lemma 2]; and (b) follows by choosing Θ_1 by reasoning similar to in [38]. From the above analysis, it can be easily seen that $2MN(2M-N)$ symbols are transmitted securely to Receiver 1 over a total of $4M^2$ time slots, thus yielding $d_{11}+d_{21} = N(2M-N)/2M$ sum SDoF at this receiver. Similar reasoning and algebra shows that $2MN(2M-N)$ symbols are also transmitted securely to Receiver 2 over a total of $4M^2$ time slots, thus yielding $d_{12}+d_{22} = N(2M-N)/2M$ sum SDoF at this receiver.

B. Case 2: $2M \geq 2N$

In this case, one can use the coding scheme of Section IV-A, with each transmitter utilizing only N antennas among the M antennas with which it is equipped. In what follows, we briefly describe an alternate coding scheme in which Receiver i, $i = 1, 2$, feeds back only its output to transmitter i, i.e., delayed CSI is not required. Also, as it will be seen from what follows, this coding scheme requires a shorter time delay comparatively. Some of the details of the analysis of this coding scheme are similar to in Section IV-A, however; and so we only outline them briefly. More specifically, the communication takes place in four phases, each composed of only one time slot.

Phase 1: Injecting artificial noise

In this phase, both transmitters inject artificial noise. Let $\mathbf{u}_1 = [u_1^1, \ldots, u_1^N]^T$ denote the artificial noise injected by Transmitter 1, and $\mathbf{u}_2 = [u_2^1, \ldots, u_2^N]^T$ denote the artificial noise injected by Transmitter 2. The channel outputs at the receivers during this phase are given by

$$\mathbf{y}_1^{(1)} = \mathbf{H}_{11}^{(1)}\mathbf{u}_1 + \mathbf{H}_{12}^{(1)}\mathbf{u}_2 \tag{22}$$

$$\mathbf{y}_2^{(1)} = \mathbf{H}_{21}^{(1)}\mathbf{u}_1 + \mathbf{H}_{22}^{(1)}\mathbf{u}_2 \tag{23}$$

where $\mathbf{H}_{ji}^{(1)} \in \mathbb{C}^{N\times N}$, for $i = 1, 2$, $j = 1, 2$, $\mathbf{y}_1^{(1)} \in \mathbb{C}^N$ and $\mathbf{y}_2^{(1)} \in \mathbb{C}^N$. At the end of this phase, the output at Receiver i, $i = 1, 2$, is fed back to Transmitter i.

Phase 2: Fresh information for Receiver 1

In this phase, both transmitters transmit confidential messages to Receiver 1. These messages are meant to be concealed from Receiver 2. To this end, Transmitter 1 transmits fresh information $\mathbf{v}_{11} = [v_{11}^1, \ldots, v_{11}^N]^T$ along with a linear combination of the channel output at Receiver 1 during Phase 1, and Transmitter 2 transmits fresh information $\mathbf{v}_{21} = [v_{21}^1, \ldots, v_{21}^N]^T$ intended for Receiver 1, i.e.,

$$\begin{aligned}\mathbf{x}_1 &= \mathbf{v}_{11} + \Theta_1\mathbf{y}_1^{(1)}\\ \mathbf{x}_2 &= \mathbf{v}_{21}\end{aligned} \tag{24}$$

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

$$\mathbf{y}_1^{(2)} = \mathbf{H}_{11}^{(2)}(\mathbf{v}_{11} + \Theta_1\mathbf{y}_1^{(1)}) + \mathbf{H}_{12}^{(2)}\mathbf{v}_{21} \tag{25a}$$

$$\mathbf{y}_2^{(2)} = \mathbf{H}_{21}^{(2)}(\mathbf{v}_{11} + \Theta_1\mathbf{y}_1^{(1)}) + \mathbf{H}_{22}^{(2)}\mathbf{v}_{21} \tag{25b}$$

where $\mathbf{H}_{ji}^{(2)} \in \mathbb{C}^{N\times N}$, for $i = 1, 2$, $j = 1, 2$, $\mathbf{y}_1^{(2)} \in \mathbb{C}^N$ and $\mathbf{y}_2^{(2)} \in \mathbb{C}^N$. At the end of this phase, the channel output at Receiver i, $i = 1, 2$, is fed back to Transmitter i. Since Receiver 1 knows the CSI and

the channel output $\mathbf{y}_1^{(1)}$ from Phase 1, it subtracts out the contribution of $\mathbf{y}_1^{(1)}$ from $\mathbf{y}_1^{(2)}$ and, thus, obtains N linearly independent equations that relates the $2N$ $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-symbols. Thus, Receiver 1 requires N extra linearly independent equations to successfully decode the $\mathbf{v}_{11}$- and $\mathbf{v}_{21}$-symbols that are intended to it during this phase. These extra equations will be provided by transmitting $\mathbf{y}_2^{(2)}$ by Transmitter 2 in Phase 4. Transmitter 2 learns $\mathbf{y}_2^{(2)}$ directly by means of the output feedback from Receiver 2 at the end of this phase.

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. The information messages are sent by both transmitters to Receiver 2, and are to be concealed from Receiver 1. More specifically, Transmitter 1 transmits fresh information $\mathbf{v}_{12} = [v_{12}^1, \ldots, v_{12}^N]^T$ to Receiver 2, and Transmitter 2 transmits $\mathbf{v}_{22} = [v_{22}^1, \ldots, v_{22}^N]^T$ along with a linear combination of the channel output received at Receiver 2 during Phase 1, i.e.,

$$\begin{aligned} \mathbf{x}_1 &= \mathbf{v}_{12} \\ \mathbf{x}_2 &= \mathbf{v}_{22} + \Theta_2 \mathbf{y}_2^{(1)} \end{aligned} \tag{26}$$

where $\Theta_2 \in \mathcal{C}^{N\times N}$ is 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

$$\mathbf{y}_1^{(3)} = \mathbf{H}_{11}^{(3)}\mathbf{v}_{21} + \mathbf{H}_{12}^{(3)}(\mathbf{v}_{22} + \Theta_2\mathbf{y}_2^{(1)}) \tag{27a}$$

$$\mathbf{y}_2^{(3)} = \mathbf{H}_{21}^{(3)}\mathbf{v}_{21} + \mathbf{H}_{22}^{(3)}(\mathbf{v}_{22} + \Theta_2\mathbf{y}_2^{(1)}) \tag{27b}$$

where $\mathbf{H}_{ji}^{(3)} \in \mathbb{C}^{N\times N}$, for $i = 1, 2$, $j = 1, 2$, $\mathbf{y}_1^{(3)} \in \mathbb{C}^N$ and $\mathbf{y}_2^{(3)} \in \mathbb{C}^N$. At the end of this phase, the channel output at Receiver i, $i = 1, 2$, is fed back to Transmitter i. Since Receiver 2 knows the CSI and the channel output $\mathbf{y}_2^{(1)}$ from Phase 1, it subtracts out the contribution of $\mathbf{y}_2^{(1)}$ from $\mathbf{y}_2^{(3)}$ and, thus, obtains N linearly independent equations that relates the $2N$ $\mathbf{v}_{21}$- and $\mathbf{v}_{22}$-symbols. Thus, Receiver 2 requires N extra linearly independent equations to successfully decode the $\mathbf{v}_{21}$- and $\mathbf{v}_{22}$-symbols that are intended to it during this phase. These extra equations will be provided by transmitting $\mathbf{y}_1^{(3)}$ by Transmitter 1 in Phase 4. Transmitter 1 learns $\mathbf{y}_1^{(3)}$ directly by means of the output feedback from Receiver 1 at the end of this phase.

Phase 4: Interference alignment and decoding

Recall that, at the end of Phase 3, Receiver 1 knows $\mathbf{y}_1^{(3)}$ and requires $\mathbf{y}_2^{(2)}$; and Receiver 2 knows $\mathbf{y}_2^{(2)}$ and requires $\mathbf{y}_1^{(3)}$. Also, at the end of this phase, Transmitter 1 has learned $\mathbf{y}_1^{(3)}$ by means of output feedback

from Receiver 1; and Transmitter 2 has learned $\mathbf{y}_2^{(2)}$ by means of output feedback from Receiver 2. The inputs by the two transmitters during Phase 4 are given by

$$\begin{aligned}\mathbf{x}_1 &= \Phi_2 \mathbf{y}_1^{(3)} \\ \mathbf{x}_2 &= \Phi_1 \mathbf{y}_2^{(2)}\end{aligned} \tag{28}$$

where $\Phi_1 \in \mathcal{C}^{N\times N}$ and $\Phi_2 \in \mathcal{C}^{N\times N}$ are matrices that are assumed to be known by all the nodes. At the end of Phase 4, Receiver 1 gets N equations in $2N$ variables. Since Receiver 1 knows $\mathbf{y}_1^{(3)}$, as well as the CSI, it can subtract out the side information, or interference, equations $\mathbf{y}_2^{(2)}$ that are seen at Receiver 2 during Phase 2. Then, using the pair of output vectors $(\mathbf{y}_1^{(2)}, \mathbf{y}_2^{(2)})$, Receiver 1 first subtracts out the contribution of $\mathbf{y}_1^{(1)}$; and, then, it inverts the resulting $2N$ linearly independent equations relating the sent $2N$ $\mathbf{v}_{11}$- 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.

Security Analysis

At the end of Phase 4, the channel outputs at the receivers are given by

$$\mathbf{y}_1 = \underbrace{\begin{bmatrix} \mathbf{H}_2 & \mathbf{H}_{11}^{(2)}\Theta_1 & \mathbf{0} \\ \mathbf{H}_{12}^{(4)}\Phi_1\mathbf{G}_2 & \mathbf{H}_{12}^{(4)}\Phi_1\mathbf{H}_{21}^{(2)}\Theta_1 & \mathbf{H}_{11}^{(4)}\Phi_2 \\ \mathbf{0} & \mathbf{I}_N & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_N \end{bmatrix}}_{\hat{\mathbf{H}} \in \mathbb{C}^{4N\times 4N}} \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{H}_1\mathbf{u} \\ \mathbf{H}_3\mathbf{v}_2 + \mathbf{H}_{12}^{(3)}\Theta_2\mathbf{G}_1\mathbf{u} \end{bmatrix} \tag{29}$$

$$\mathbf{y}_2 = \underbrace{\begin{bmatrix} \mathbf{0} & \mathbf{I}_N & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_N \\ \mathbf{G}_3 & \mathbf{H}_{22}^{(3)}\Theta_2 & \mathbf{0} \\ \mathbf{H}_{21}^{(4)}\Phi_2\mathbf{H}_3 & \mathbf{H}_{21}^{(4)}\Phi_2\mathbf{H}_{12}^{(3)}\Theta_2 & \mathbf{H}_{22}^{(4)}\Phi_1 \end{bmatrix}}_{\hat{\mathbf{G}} \in \mathbb{C}^{4N\times 4N}} \begin{bmatrix} \mathbf{v}_2 \\ \mathbf{G}_1\mathbf{u} \\ \mathbf{G}_2\mathbf{v}_1 + \mathbf{H}_{21}^{(2)}\Theta_1\mathbf{H}_1\mathbf{u} \end{bmatrix} \tag{30}$$

where $\mathbf{H}_t = [\mathbf{H}_{11}^{(t)} \;\; \mathbf{H}_{12}^{(t)}]$, $\mathbf{G}_t = [\mathbf{H}_{21}^{(t)} \;\; \mathbf{H}_{22}^{(t)}]$, for $t = 1, \ldots, 3$, $\mathbf{u} = [\mathbf{u}_1^T \;\; \mathbf{u}_2^T]^T$, $\mathbf{v}_1 = [\mathbf{v}_{11}^T \;\; \mathbf{v}_{21}^T]^T$, and $\mathbf{v}_2 = [\mathbf{v}_{12}^T \;\; \mathbf{v}_{22}^T]^T$. Similar to the analysis of the previous case, the information rate to Receiver 1 is given by

the mutual information $I(\mathbf{v}_1;\mathbf{y}_1)$, and can be evaluated as

$$
\begin{aligned}
&I(\mathbf{v}_1;\mathbf{y}_1) = I(\mathbf{v}_1, \mathbf{H}_1\mathbf{u}, \mathbf{H}_3\mathbf{v}_2 + \mathbf{H}_{12}^{(3)}\Theta_2\mathbf{G}_1\mathbf{u};\mathbf{y}_1) \\
&- I(\mathbf{H}_1\mathbf{u}, \mathbf{H}_3\mathbf{v}_2 + \mathbf{H}_{12}^{(3)}\Theta_2\mathbf{G}_1\mathbf{u};\mathbf{y}_1|\mathbf{v}_1) \\
&\overset{(a)}{=} \text{rank}(\hat{\mathbf{H}}).\log(2P) \\
&- \text{rank}\begin{pmatrix} \mathbf{H}_{11}^{(2)}\Theta_1 & \mathbf{0} \\ \mathbf{H}_{12}^{(4)}\Phi_1\mathbf{H}_{21}^{(2)}\Theta_1 & \mathbf{H}_{11}^{(4)}\Phi_2 \\ \mathbf{I}_N & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_N \end{pmatrix}.\log(2P) \\
&\overset{(b)}{=} 2N.\log(2P) + \text{rank}\begin{pmatrix} \mathbf{H}_2 \\ \mathbf{H}_{12}^{(4)}\Phi_1\mathbf{G}_2 \end{pmatrix}.\log(2P) - 2N.\log(2P) \\
&= \text{rank}\begin{pmatrix} \mathbf{H}_2 \\ \mathbf{H}_{12}^{(4)}\Phi_1\mathbf{G}_2 \end{pmatrix}.\log(2P) \\
&\overset{(c)}{=} 2N.\log(2P)
\end{aligned} \tag{31}
$$

where (a) follows from [38, Lemma 2]; (b) follows by using the block diagonalization structure of $\hat{\mathbf{H}}$; and (c) follows by reasoning as in [38] for the selection of Φ_1 with appropriate rank such that the equality holds.

Similarly, the information leaked to Receiver 2 can be bounded as

$$
\begin{aligned}
&I(\mathbf{v}_1;\mathbf{y}_2) \\
&\leq I(\mathbf{G}_1\mathbf{u}, \mathbf{G}_2\mathbf{v}_1 + \mathbf{H}_{21}^{(2)}\Theta_1\mathbf{H}_1\mathbf{u};\mathbf{y}_2|\mathbf{v}_2) - I(\mathbf{u};\mathbf{y}_2|\mathbf{G}_2\mathbf{v}_1, \mathbf{v}_2) \\
&\overset{(a)}{=} \text{rank}\begin{pmatrix} \mathbf{I}_N & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_N \\ \mathbf{H}_{22}^{(3)}\Theta_2 & \mathbf{0} \\ \mathbf{H}_{21}^{(4)}\Phi_2\mathbf{H}_{12}^{(3)}\Theta_2 & \mathbf{H}_{22}^{(4)}\Phi_1 \end{pmatrix}.\log(2P)
\end{aligned}
$$

$$
\begin{aligned}
&- \text{rank}\begin{pmatrix} \mathbf{G}_1 \\ \mathbf{H}_{21}^{(2)}\Theta_1\mathbf{H}_1 \\ \mathbf{H}_{22}^{(3)}\Theta_2\mathbf{G}_1 \\ \mathbf{H}_{21}^{(4)}\Phi_2\mathbf{H}_{12}^{(3)}\Theta_2\mathbf{G}_1 + \mathbf{H}_{22}^{(4)}\Phi_1\mathbf{H}_{21}^{(2)}\Theta_1\mathbf{H}_1 \end{pmatrix}.\log(2P) \\
&= 2N.\log(2P) - \text{rank}\begin{pmatrix} \mathbf{G}_1 \\ \mathbf{H}_{21}^{(2)}\Theta_1\mathbf{H}_1 \end{pmatrix}.\log(2P) \\
&\overset{(b)}{=} 0
\end{aligned} \tag{32}
$$

where (a) follows from [38, Lemma 2]; and (b) follows by choosing Θ_1 with the reasoning similar to [38].

From the above analysis, it can be easily seen that $2N$ symbols are transmitted securely to Receiver 1, over a total of 4 time slots, yielding $d_{11}+d_{21} = N/2$ sum SDoF. Similar analysis shows that the scheme also offers $d_{12} + d_{22} = N/2$ sum SDoF for Receiver 2.

This concludes the proof of the direct part of Theorem 1.

Remark 3: Investigating the coding scheme of Theorem 1, it can be seen that in the case in which $N \leq M$, asymmetric output feedback only suffices to achieve the optimum sum SDoF point. That is, the transmitters exploit only the availability of asymmetric output feedback, and do not make use of the available delayed CSIT.

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, i.e., *symmetric output feedback*, and 2) the case in which Receiver i, $i = 1, 2$, feeds back its output only to Transmitter i, i.e., *asymmetric output feedback*. In both cases, no CSI is provided to the transmitters. The model with symmetric output feedback may model a setting in which both feedback signals are strong and can be heard by both transmitters. The model with asymmetric output feedback may model a setting in which the feedback signals are weak and can be heard by only one transmitter each.

A. MIMO X-channel with symmetric output feedback

The following theorem provides the sum SDoF region of the MIMO X-channel with symmetric output feedback.

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

Remark 4: The sum SDoF region of the MIMO X-channel with symmetric output feedback is same as the sum SDoF region of the MIMO X-channel with asymmetric output feedback and delayed CSIT. Investigating the coding scheme of the MIMO X-channel with asymmetric output feedback and delayed CSIT of Theorem 1, it can be seen that the delayed CSIT 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 the output feedback symmetrically, this information is readily available at each transmitter; and, thus, there is no need for any CSIT at the transmitters in order to achieve the same sum SDoF region as that of Theorem 1.

Proof: The proof of the outer bound can be obtained by reasoning as follows. Let us denote the two-user MIMO X-channel with symmetric output feedback that we study as MIMO-X$^{(0)}$. Consider the MIMO X-channel obtained by assuming that, in addition to symmetric output feedback, i) delayed CSIT is provided to both transmitters and that ii) the transmitters are allowed to cooperate. Denote the obtained MIMO X-channel as MIMO-X$^{(1)}$. Since the transmitters cooperate in MIMO-X$^{(1)}$, this model is in fact a MIMO BC with $2M$ antennas at the transmitter and N antennas at each receiver, with delayed CSIT as well as output feedback given to the transmitter. Then, an outer bound on the SDoF of this MIMO-X$^{(1)}$ is given by [38, Theorem 3]. This holds because the result of [38, Theorem 3] continues to hold if one provides outputs feedback from the receivers to the transmitter in the two-user MIMO BC with delayed CSIT that is considered in [38]. Next, since delayed CSIT at the transmitters and cooperation can only increase the SDoF, it follows that the obtained outer bound is also an outer bound on the SDoF of MIMO-X$^{(0)}$. Thus, the region of Theorem 1 is an outer bound on the sum SDoF region for the MIMO X-channel in which the transmitters are provided only with symmetric output feedback.

We now provide a brief outline of the coding scheme that we use to establish the sum SDoF region of Theorem 2. This coding scheme is very similar to that we use for the proof of Theorem 1, with the following (rather minor) differences. For the case in which $2M \leq N$ and that in which $2N \leq 2M$, the coding strategies are exactly same as those that we used for the proof of Theorem 1. For the case in

which $N \leq 2M \leq 2N$, the first three phases are similar to those in the coding scheme of Theorem 1, but with, at the end of these phases, the receivers feeding back their outputs to both transmitters, instead of Receiver i, $i = 1, 2$, feeding back its output together with the delayed CSI to Transmitter i. Note that, during these phases, each transmitter learns the required side information equations *directly* from the symmetric output feedback that it gets from the receivers (see Remark 4). Phase 4 and the decoding procedures are similar to those in the proof of Theorem 1. This concludes the proof of Theorem 2. □

B. MIMO X-channel with only asymmetric output feedback

We now consider the case in which only asymmetric output feedback is provided from the receivers to the transmitters, 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),

$$d_s^{\text{local}}(N, N, M) = \begin{cases} 0 & \text{if } \ M \leq N \\ \frac{M^2(M-N)}{2N^2+(M-N)(3M-N)} & \text{if } \ N \leq M \leq 2N \\ \frac{2N}{3} & \text{if } \ M \geq 2N \end{cases} \tag{33}$$

The following theorem provides an inner bound on the sum SDoF region of the two-user MIMO X-channel with asymmetric output feedback.

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

$$\begin{aligned} \frac{d_{11}+d_{21}}{d_s^{\text{local}}(N,N,2M)} + \frac{d_{12}+d_{22}}{\min(2M,2N)} &\leq 1 \\ \frac{d_{11}+d_{21}}{\min(2M,2N)} + \frac{d_{12}+d_{22}}{d_s^{\text{local}}(N,N,2M)} &\leq 1 \end{aligned} \tag{34}$$

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

Remark 5: Obviously, the region of Theorem 1 is an outer bound on the sum SDoF region of the MIMO X-channel with asymmetric output feedback. Also, it is easy to see that the inner bound of Theorem 3 is tight in the case in which $M \geq N$.

Remark 6: The main reason for which the inner bound of Theorem 3 is smaller than that of Theorem 1 for the model with asymmetric output feedback and delayed CSIT can be explained as follows. Consider the Phase 4 in the coding scheme of Theorem 1 in Section IV-B. 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 asymmetric output feedback and delayed CSIT. Similarly, in the coding scheme of Theorem 2, this is made possible by means of availability of symmetric output feedback at the transmitters. For the model with only asymmetric output feedback, however, it is not clear how this can be obtained (if possible at all); and this explains the loss incurred in the sum SDoF region. More specifically, consider Phase 2 of the coding scheme of Theorem 1. Recall that, at the beginning of this phase, Transmitter 1 utilizes the fed back CSI $(\tilde{\mathbf{H}}_{11}^{(2)}, \tilde{\mathbf{H}}_{12}^{(2)})$ to learn the $\mathbf{v}_{21}$-symbols that are transmitted by Transmitter 2 during this phase; and then utilizes the fed back CSI $(\tilde{\mathbf{H}}_{21}^{(2)}, \tilde{\mathbf{H}}_{22}^{(2)})$ to reconstruct the side information output vector $\mathbf{y}_2^{(2)}$ that is required by Receiver 1 (given by (15b)). Also, Transmitter 2 performs similar operations to learn the side information output vector $\mathbf{y}_1^{(3)}$ that is required by Receiver 2 (given by (17a)). In the case of only asymmetric output feedback given to the transmitters, as we mentioned previously, it is not clear whether this could be possible because of the lack of availability of CSIT.

Proof: We now provide an outline of the coding scheme for the MIMO X-channel with asymmetric output feedback.

For the case in which $2M \leq N$ and the case in which $N \leq M$, the achievability follows trivially by using the coding scheme of Theorem 1 (see Remark 3).

For the case in which $N \leq 2M \leq 2N$, the proof of achievability follows by a variation of the coding scheme of Theorem 1 that we outline briefly in what follows. The communication takes place in four phases.

Phase 1: The transmission scheme in this phase is similar to that in Phase 1 of the coding scheme of Theorem 1, but with at the end of this phase, Receiver i, $i = 1, 2$, feeding back only its output to Transmitter i, instead of feeding back its output together with the delayed CSI to Transmitter i.

Phase 2: The communication takes place in $T_2 = M(2M - N)$ channel uses. The transmission scheme is same as that of Phase 2 of the coding scheme of Theorem 1, with the following modifications. The inputs $(\mathbf{x}_1, \mathbf{x}_2)$ from the transmitters and outputs $(\mathbf{y}_1^{(2)}, \mathbf{y}_2^{(2)})$ at the receivers are again given by (14) and (15), respectively. At the end of these phases, Receiver i, $i = 1, 2$, feeds back its output to Transmitter i. At the

end of this phase, 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 by (only) Transmitter 2 in Phase 4. 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.

Phase 3: The communication takes place in $T_2 = M(2M-N)$ channel uses. The transmission scheme is same as that of Phase 3 of the coding scheme of Theorem 1, with the following modifications. The inputs $(\mathbf{x}_1, \mathbf{x}_2)$ from the transmitters and outputs $(\mathbf{y}_1^{(2)}, \mathbf{y}_2^{(2)})$ at the receivers are again given by (16) and (17), respectively. At the end of this phase, Receiver 2 requires $(2M-N)T_2$ extra linearly independent equations to successfully decode the $\mathbf{v}_{12}$- and $\mathbf{v}_{22}$-symbols that are intended to it during this phase. Let $\tilde{\mathbf{y}}_1^{(3)} \in \mathbb{C}^{(2M-N)T_2}$ denote a set of $(2M-N)T_2$ such linearly independent equations, selected among the available NT_2 side information equations $\mathbf{y}_1^{(3)} \in \mathbb{C}^{NT_2}$ (recall that $2M-N \leq N$ in this case). These equations will be transmitted by (only) Transmitter 1 in Phase 4. 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.

Phase 4: Recall that at the end of Phase 3, Receiver 1 requires the side information output vector $\tilde{\mathbf{y}}_2^{(2)}$, and Receiver 2 requires the side information output vector $\tilde{\mathbf{y}}_1^{(3)}$. In Phase 4, the communication takes place in $T_3 = (2M-N)(2M-N)$ channel uses. During this phase, Transmitter 1 transmits $\mathbf{x}_1 = \Phi_2 \mathbf{y}_1^{(3)}$ and Transmitter 2 transmits $\mathbf{x}_2 = \Phi_1 \mathbf{y}_2^{(2)}$, where $\Phi_1 \in \mathcal{C}^{MT_3 \times NT_2}$, and $\Phi_2 \in \mathcal{C}^{MT_3 \times NT_2}$, in T_3 channel uses.

Decoding: At the end of Phase 4, Receiver 1 gets NT_3 equations in $2MT_3$ 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 obtain the side information output vector $\tilde{\mathbf{y}}_2^{(2)}$. 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 analysis of the sum SDoF that is allowed by the described coding scheme can be obtained by proceeding as in the proof of Theorem 1, to show that $2M^2(2M-N)$ symbols are transmitted securely

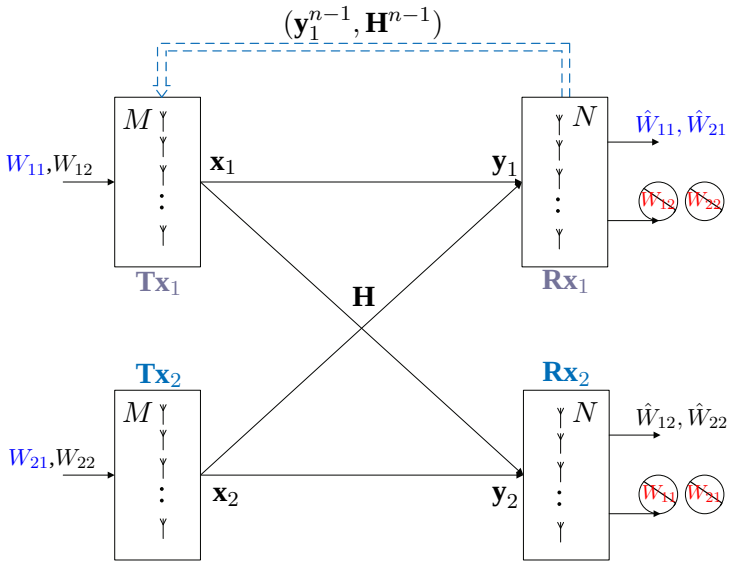

Fig. 4. MIMO X-channel with asymmetric output feedback and delayed CSIT with security constraints.

to Receiver 1 over a total of $T_1 + 2T_2 + T_3 = 2(4M^2 - 3MN + N^2)$ channel uses, thus yielding $d_{11} + d_{21} = M^2(2M - N)/(4M^2 - 3MN + N^2)$ sum SDoF at this receiver. Similar reasoning and algebra shows that $d_{12} + d_{22} = M^2(2M - N)/(4M^2 - 3MN + N^2)$ sum SDoF for Receiver 2. This concludes the proof of Theorem 3. □

The analysis so far reflects the utility of both output feedback and delayed CSIT that are provided to both transmitters in terms of SDoF. However, the models that we have considered so far are *symmetric* in the sense that both transmitters see the same degree of output feedback and delayed CSI from the receivers. The relative importance of output feedback and delayed CSIT depends on the studied configuration. In what follows, it will be shown that, in the symmetric model of Theorem 3 one can replace the asymmetric output feedback that is provided to one transmitter with delayed CSIT given to the other transmitter without diminishing the achievable sum SDoF region.

Remark 7: Investigating closely the coding scheme of Theorem 3, it can be seen that the key ingredient in the achievability proof is that, at the end of the third phase, each of the side information output vector $\tilde{\mathbf{y}}_2^{(2)}$ that is required by Receiver 1 to successfully decode the symbols that are intended to it and the side information output vector $\tilde{\mathbf{y}}_1^{(3)}$ that is required by Receiver 2 to successfully decode the symbols that

are intended to it be learned by *exactly* one of the transmitters[1]. In the coding scheme of Theorem 3, the side information output vectors $\tilde{\mathbf{y}}_1^{(3)}$ and $\tilde{\mathbf{y}}_2^{(2)}$ are learned by distinct transmitters at the end of Phase 3. The above suggests that the inner bound of Theorem 3 will also remain achievable if these side information output vectors are both learned by the *same* transmitter. Figure 4 shows a variation model that is asymmetric in the sense that asymmetric output feedback and delayed CSI are provided only to Transmitter 1. In this model, by means of the output feedback and delayed CSI from Receiver 1, Transmitter 1 can learn *both* side information output vectors $(\tilde{\mathbf{y}}_1^{(3)}, \tilde{\mathbf{y}}_2^{(2)})$ (See the analysis of Phase 2 in the coding scheme of Theorem 1). Taking this into account, it is easy to show that the inner bound of Theorem 3 is also achievable for the model shown in Figure 4.

Proposition 1: For the model with asymmetric output feedback and delayed CSI provided only to Transmitter 1 shown in Figure 4, an inner bound on the sum SDoF region is given by Theorem 3.

VI. MIMO X-Channels Without Security Constraints

In this section, we consider an (M, M, N, N)–MIMO 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 $\mathcal{C}_{\text{DoF}}^{\text{sum}}$ of the two-user (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT is given by the set of all non-negative pairs $(d_{11}+d_{21}, d_{12}+d_{22})$ satisfying

$$\begin{aligned} \frac{d_{11}+d_{21}}{\min(2M,2N)} + \frac{d_{12}+d_{22}}{\min(2M,N)} &\leq 1 \\ \frac{d_{11}+d_{21}}{\min(2M,N)} + \frac{d_{12}+d_{22}}{\min(2M,2N)} &\leq 1. \end{aligned} \tag{35}$$

Proof: The converse proof follows immediately from the DoF region of a two-user MIMO BC with delayed CSIT [3, Theorem 2] in which the transmitter is equipped with $2M$ antennas and the receivers are equipped with N antennas each. The proof of the direct part follows by a coding scheme that can be obtained by specializing that of Theorem 1 to the setting without security constraints, and that we only outline briefly here. First, note that the region of Theorem 4 is fully characterized by the corner points $(\min(2M,N),0)$, $(0,\min(2M,N))$ and the point P given by the intersection of the lines defining the equations in (35). It is not difficult to see that the corner points $(\min(2M,N),0)$ and $(0,\min(2M,N))$

[1]By opposition, in the coding scheme of Theorem 1, both side information output vectors have been learned by both transmitters at the end of Phase 3, as we mentioned previously.

are achievable without feedback and without delayed CSIT, as the system is equivalent to coding for a MIMO multiple access channel for which the achievability follows from straightforward results. We now outline the achievability of the point P. If $2M \leq N$, the point $P = (M, M)$ is clearly achievable. If $N \leq 2M \leq 2N$, the achievability of the point $P = (2NM/(2M+N), 2NM/(2M+N))$ can be obtained by modifying the coding scheme of Theorem 1, essentially by ignoring Phase 1. Note that, at the end of the transmission, $2MN(2M-N)$ symbols are sent to each receiver over $2T_2+T_4 = (2M-N)(2M+N)$, i.e., a sum DoF of $2MN/(2M+N)$ for each. In the case in which $2M \geq 2N$, one can use the coding scheme of the previous case with each transmitter utilizing only N antennas. □

Remark 8: 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 [3, 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 DoF. This can be seen as a generalization of [13, Theorem 1] in which it is shown that the loss is zero from a total DoF perspective.

Remark 9: Like for the setting with secrecy constraints, it can be easily shown that the sum DoF region of the (M, M, N, N)–MIMO X-channel with symmetric output feedback is also given by Theorem 4.

VII. Numerical Examples

In this section, we illustrate the results of the previous sections (i.e., Theorems 1, 2, 3 and 4) through some numerical examples. We also include comparisons with some previously known results for the MIMO X-channel without security constraints and with different degrees of CSIT and output feedback.

Figure 5 illustrates the optimal sum SDoF of the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT given by Theorem 1, for different values of the transmit- and receive antennas. For comparison reasons, Figure 5 also shows the optimal DoF of the same model, i.e., (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT, but without security constraints, as given by Theorem 4. The gap that is visible in the figure illustrates the rate loss that is caused asymptotically, in the signal-to-noise ratio, by imposing security constraints on the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT. Thus, it can be interpreted as the *price for secrecy* for the model that we study.

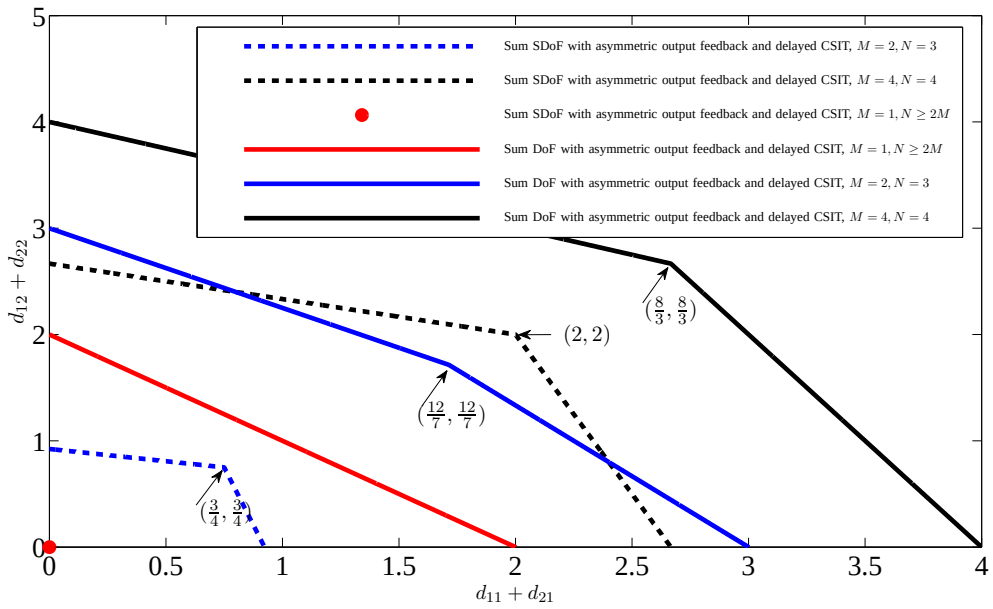

Fig. 5. Sum SDoF and sum DoF regions of the (M, M, N, N)–X channel with asymmetric output feedback and delayed CSIT, for different antennas configurations.

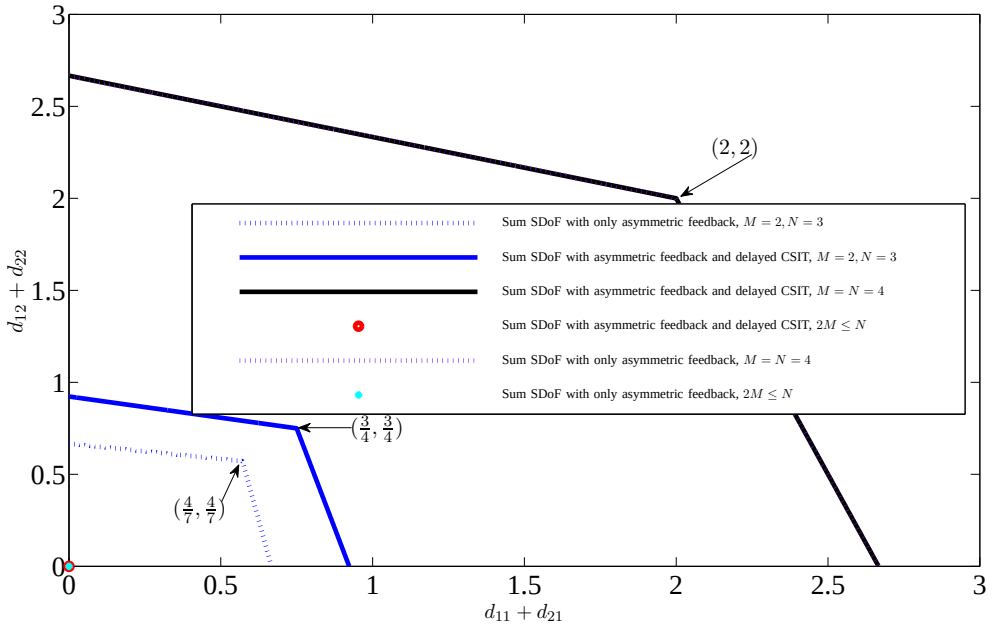

Fig. 6. Sum SDoF region of the (M, M, N, N)–X channel with different degrees of output feedback and delayed CSIT, for some antennas configurations.

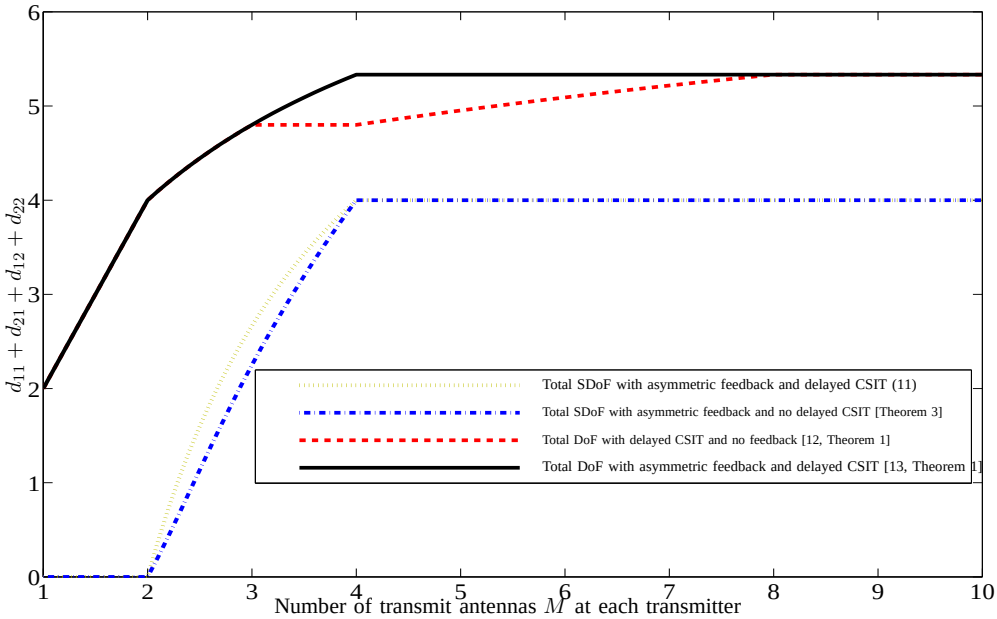

Fig. 7. Total secure degrees of freedom of the MIMO (M, M, N, N)–X channel, as a function of the number of transmit antennas M at each transmitter, for a fixed number $N = 4$ of receive antennas at each receiver.

Figure 6 shows the inner bound of Theorem 3, for different antennas configurations. As we mentioned previously, although the optimality of the inner bound of Theorem 3 is still to be shown, the loss in terms of secure degrees of freedom that is visible in the figure for $N \leq 2M \leq 2N$ sheds light on the role and utility of providing delayed CSI to the transmitters from a secrecy viewpoint. For $M \geq N$, however, the lack of delayed CSIT does not cause any loss in terms of secure degrees of freedom in comparison with the model with output and delayed CSIT of Theorem 1.

Figure 7 depicts the evolution of the total secure degrees of freedom of the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT as function of the number of transmit-antennas M at each transmitter, for a given number of receive-antennas at each receiver $N = 4$. The figure also shows the total secure degrees of freedom with only asymmetric output feedback provided to the transmitters (obtained from Theorem 3), as well as the total DoF without security constraints [13, Theorem 1] (which can also be obtained from Theorem 4). Furthermore, the figure also shows the total DoF of the MIMO X-channel with only delayed CSIT, no feedback and no security constraints [12].

VIII. Conclusion

In this paper, we study the sum SDoF region of a two-user multi-input multi-output X-channel with M antennas at each transmitter and N antennas at each receiver. We assume perfect CSIR, i.e., each receiver has perfect knowledge of its channel. In addition, all the terminals are assumed to know the past CSI; and there is a noiseless asymmetric output feedback at the transmitters, i.e., Receiver i, $i = 1, 2$, feeds back its past channel output to Transmitter i. We characterize the optimal sum SDoF region of this model. We show that the sum SDoF region of this MIMO X-channel with asymmetric output feedback and delayed CSIT is *same* as the SDoF region of a two-user MIMO BC with $2M$ transmit antennas and N antennas at each receiver and delayed CSIT. The coding scheme that we use for the proof of the direct part follows through an appropriate extension of that by Yang *et al.* [38] in the context of secure transmission over MIMO broadcast channels with delayed CSIT. Furthermore, investigating the role of the delayed CSIT, we also study two-user MIMO X-channel models with no CSIT. In the first model, the transmitters have no knowledge of the CSI but are provided with noiseless output feedback from both receivers, i.e., *symmetric output feedback*. In the second model, each transmitters is provided by only output feedback from a different receiver, i.e., *asymmetric output feedback*. For the model with symmetric output feedback, we show that the sum SDoF is same as that of the MIMO X-channel with asymmetric output feedback and delayed CSIT. For the model with only asymmetric output feedback, we establish an inner bound on the allowed sum SDoF region. Next, we specialize our results to the setting without security constraints, and show that the sum DoF region of the (M, M, N, N)–MIMO X-channel with asymmetric output feedback and delayed CSIT is same as the DoF region of a two-user MIMO BC with $2M$ transmit antennas and N antennas at each receiver and delayed CSIT. The established results emphasize the usefulness of output feedback and delayed CSIT for transmission over a two-user MIMO X-channel with and without security constraints.

References

[1] S. A. Jafar, "Interference alignment — A new look at signal dimensions in a communication network," *Foundations and Trends in Communications and Information Theory*, vol. 7, no. 1, pp. 1–134, 2010.

[2] 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.

[3] 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

[4] M. J. Abdoli, A. Ghasemi, and A. K. Khandani, "On the degrees of freedom of three-user MIMO broadcast channel with delayed CSIT," in *IEEE International Symposium on Information Theory*, St. Petersburg, Russia, Aug. 2011, pp. 209–213.

[5] C. S. Vaze and M. K. Varanasi, "The degrees of freedom region and interference alignment for the MIMO interference channel with delayed CSIT," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4396–4417, Jul. 2012.

[6] A. Ghasemi, A. S. Motahari, and A. K. Khandani, "Interference alignment for the MIMO interference channel with delayed local CSIT," 2011. [Online]. Available: http://arxiv.org/abs/1102.5673

[7] M. J. Abdoli, A. Ghasemi, and A. K. Khandani, "On the degrees of freedom of K-user SISO interference and X channels with delayed CSIT," 2011. [Online]. Available: http://arxiv.org/abs/1109.4314

[8] R. Tandon, S. Mohajer, H. Poor, and S. Shamai, "Degrees of freedom region of the MIMO interference channel with output feedback and delayed CSIT," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1444–1457, 2013.

[9] S. A. Jafar and S. Shamai (Shitz), "Degrees of freedom region of the MIMO X channel," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 151–170, Jan. 2008.

[10] H. Maleki, S. A. Jafar, and S. Shamai (Shitz), "Retrospective interference alignment over interference networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 3, pp. 228–240, Jun. 2012.

[11] C. S. Vaze and M. K. Varanasi, "The degrees of freedom regions of MIMO broadcast, interference, and cognitive radio channels with no CSIT," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5354–5374, Aug. 2012.

[12] A. Ghasemi, M. J. Abdoli, and A. K. Khandani, "On the degrees of freedom of MIMO X channel with delayed CSIT," in *IEEE International Symposium on Information Theory*, Boston, USA, Jul. 2012, pp. 1902–1906.

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

[14] L. Yang and W. Zhang, "On achievable degrees of freedom for MIMO X channels," Aug. 2012. [Online]. Available: http://arxiv.org/abs/1208.2900

[15] H. Maleki, V. R. Cadambe, and S. A. Jafar, "Index coding: an interference alignment perspective," May 2012. [Online]. Available: http://arxiv.org/abs/1205.1483v1

[16] H. Sun, C. Geng, and S. A. Jafar, "Topological interference management with alternating connectivity," Feb. 2013. [Online]. Available: http://arxiv.org/abs/1302.4020

[17] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

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

[19] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[20] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[21] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[22] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[23] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journal on Wireless Commnunications and Networking. Special issue on physical layer security*, Nov. 2009.

[24] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[25] Y. Liang and H. V. Poor, “Multiple access channels with confidential messages,” *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[26] E. Tekin and A. Yener, “The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[27] Z. H. Awan, A. Zaidi, and L. Vandendorpe, “On multiaccess channel with unidirectional cooperation and security constraints,” in *50th Annual Allerton Conference Communication, Control and Computing*, Monticello, IL, USA, Oct. 2012, pp. 982–987.

[28] ——, “Multiaccess channel with partially cooperating encoders and security constraints,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1243–1254, Jul. 2013.

[29] L. Lai and H. E. Gamal, “The relay eavesdropper channel: Cooperation for secrecy,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[30] Z. H. Awan, A. Zaidi, and L. Vandendorpe, “On secure transmission over parallel relay eavesdropper channel,” in *48th Annual Allerton Conference Communication, Control and Computing*, Monticello, IL, USA, Sept. 2010, pp. 859–866.

[31] ——, “Secure communication over parallel relay channel,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 359–371, Apr. 2012.

[32] O. O. Koyluoglu and H. E. Gamal, “Cooperative encoding for secrecy in interference channels,” *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5682–5694, Sept. 2011.

[33] Z. Li, R. Yates, and W. Trappe, “Secrecy capacity of a class of one-sided interference channel,” in *IEEE International Symposium on Information Theory*, Toronto, ON, Jul. 2008, pp. 379–383.

[34] T. Gou and S. A. Jafar, “On the secure degrees of freedom of wireless X networks,” in *46th Annual Allerton Conference Communication, Control and Computing*, Monticello IL, USA, Oct. 2008.

[35] Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Information theoretic security,” *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[36] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, “Interference alignment for secrecy,” *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[37] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, “On the secure Degrees-of-Freedom of the Multiple-Access-Channel,” 2010. [Online]. Available: http://arxiv.org/abs/1003.0729

[38] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai (Shitz), “Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT,” *to appear in IEEE Transactions on Information Theory*, 2013.

Abdellatif Zaidi received the B.S. degree in Electrical Engineering from École Nationale Supérieure de Techniques Avancés, ENSTA ParisTech, France in 2002 and the M. Sc. and Ph.D. degrees in Electrical Engineering from École Nationale Supérieure des Télécommunications, TELECOM ParisTech, Paris, France in 2002 and 2005, respectively.

From December 2002 to December 2005, he was with the Communications and Electronics Dept., TELECOM ParisTech, Paris, France and the Signals and Systems Lab., CNRS/Supélec, France pursuing his PhD degree. From May 2006 to September 2010, he was at École Polytechnique de Louvain, Université catholique de Louvain, Belgium, working as a research assistant. Dr. Zaidi was ”Research Visitor” at the University of Notre Dame, Indiana, USA, during fall 2007 and Spring 2008. He is now, an associate professor at Université Paris-Est Marne-la-Vallée, France.

His research interests cover a broad range of topics from signal processing for communication and multi-user information theory. Of particular interest are the problems of relaying and cooperation, network coding, interference mitigation, secure communication, coding and interference mitigation in multi-user channels, source coding and side-informed problems, with application to sensor networking and ad-hoc wireless networks. A. Zaidi is an Associate Editor of the Eurasip Journal on Wireless Communications and Networking (EURASIP JWCN).

Zohaib Hassan Awan received the B.S. degree in Electronics Engineering from Ghulam Ishaq Khan Institute (GIKI), Topi, Pakistan in 2005 and the M.S. degree in Electrical Engineering with a majors in wireless systems from Royal Institute of Technology (KTH), Stockholm, Sweden in 2008. He received the Ph.D. degree in Electrical Engineering from Université catholique de Louvain (UCL), Belgium in 2013. From Sept. 2013, he is with the Department of Electrical Engineering and Information Technology, Ruhr-Universität Bochum, Bochum, Germany.

His current research interests include information-theoretic security, cooperative communications and communication theory.

Shlomo Shamai (Shitz) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion—Israel Institute of Technology, in 1975, 1981 and 1986 respectively.

During 1975-1985 he was with the Communications Research Labs, in the capacity of a Senior Research Engineer. Since 1986 he is with the Department of Electrical Engineering, Technion—Israel Institute of Technology, where he is now a Technion Distinguished Professor, and holds the William Fondiller Chair of Telecommunications. His research interests encompasses a wide spectrum of topics in information theory and statistical communications.

Dr. Shamai (Shitz) is an IEEE Fellow, a member of the Israeli Academy of Sciences and Humanities and a Foreign Associate of the US National Academy of Engineering. He is the recipient of the 2011 Claude E. Shannon Award. He has been awarded the 1999 van der Pol Gold Medal of the Union Radio Scientifique Internationale (URSI), and is a corecipient of the 2000 IEEE Donald G. Fink Prize Paper Award, the 2003, and the 2004 joint IT/COM societies paper award, the 2007 IEEE Information Theory Society Paper Award, the 2009 European Commission FP7, Network of Excellence in Wireless COMmunications (NEWCOM++) Best Paper Award, and the 2010 Thomson Reuters Award for International Excellence in Scientific Research. He is also the recipient of 1985 Alon Grant for distinguished young scientists and the 2000 Technion Henry Taub Prize for Excellence in Research. He has served as Associate Editor for the Shannon Theory of the IEEE Transactions on Information Theory, and has also served twice on the Board of Governors of the Information Theory Society. He is a member of the Executive Editorial Board of the IEEE Transactions on Information Theory.

Luc Vandendorpe (M'93-SM'99-F'06) was born in Mouscron, Belgium, in 1962. He received the Electrical Engineering degree (summa cum laude) and the Ph. D. degree from the Université catholique de Louvain (UCL) Louvain-la- Neuve, Belgium in 1985 and 1991 respectively. Since 1985, L. Vandendorpe is with the Communications and Remote Sensing Laboratory of UCL where he first worked in the field of bit rate reduction techniques for video coding. In 1992, he was a Visiting Scientist and Research Fellow at the Telecommunications and Traffic Control Systems Group of the Delft Technical University, Netherlands, where he worked on Spread Spectrum Techniques for Personal Communications Systems. From October 1992 to August 1997, L. Vandendorpe was Senior Research Associate of the Belgian NSF at UCL. Presently, he is Full Professor and Head of the Institute for Information and Communication Technologies, Electronics and Applied Mathematics of UCL.

His current interest is in digital communication systems and more precisely resource allocation for OFDM(A) based multicell systems, MIMO and distributed MIMO, sensor networks, turbo-based communications systems, physical layer security and UWB based positioning.

In 1990, he was co-recipient of the Biennal Alcatel-Bell Award from the Belgian NSF for a contribution in the field of image coding. In 2000 he was co-recipient (with J. Louveaux and F. Deryck) of the Biennal Siemens Award from the Belgian NSF for a contribution about filter bank based multicarrier transmission. In 2004 he was co-winner (with J. Czyz) of the Face Authentication Competition, FAC 2004. L. Vandendorpe is or has been TPC member for numerous IEEE conferences (VTC Fall, Globecom Communications Theory Symposium, SPAWC, ICC) and for the Turbo Symposium. He was co-technical chair (with P. Duhamel) for IEEE ICASSP 2006.

He was an editor of the IEEE Trans. on Communications for Synchronization and Equalization between 2000 and 2002, associate editor of the IEEE Trans. on Wireless Communications between 2003 and 2005, and associate editor of the IEEE Trans. on Signal Processing between 2004 and 2006. He was chair of the IEEE Benelux joint chapter on Communications and Vehicular Technology between 1999 and 2003. He was an elected member of the Signal Processing for Communications committee between 2000 and 2005, and between 2009 and 2011, and an elected member of the Sensor Array and Multichannel Signal Processing committee of the Signal Processing Society between 2006 and 2008. Currently, he is the Editor in Chief for the Eurasip Journal on Wireless Communications and Networking. L. Vandendorpe is a Fellow of the IEEE.