On Secure Degrees of Freedom of MIMO X-Channel With Output Feedback and Delayed CSI

Zohaib Hassan AWAN[‡], Abdellatif ZAIDI[†], Luc VANDENDORPE[‡]

[‡]Université catholique de Louvain
Place du Levant.2, B-1348 Louvain-la-Neuve, Belgique

[†]Université Paris-Est Marne La Vallée,
Laboratoire d'Informatique Gaspard Monge UMR CNRS 8049
5 Bd Descartes, 77454 Marne-la-Vallée Cedex 2, France
{zohaib.awan, luc.vandendorpe}@uclouvain.be, abdellatif.zaidi@univ-mlv.fr

Abstract – We investigate the problem of secure transmission over a two-user multi-input multi-output (MIMO) X-channel with noiseless local feedback and delayed channel state information (CSI) available at transmitters. The transmitters are equipped with M antennas at each node and the receivers are equipped with N antennas at each node respectively. We characterize the optimal sum secure degrees of freedom (SDoF) region for the two-user (M, M, N, N)–MIMO X-channel with local feedback and delayed CSI. The coding scheme is based on an extension of the scheme developed earlier by Yang *et. al.* [1] in the context of the two-user MIMO BC. The achievability follows by appropriately exploiting the availability of both resources, i.e., output feedback and delayed CSI at each receiver. We also study some special cases of availability of output feedback at transmitters. For the two-user MIMO X-channel with local feedback and delayed CSI we characterize the optimal sum secure degrees of freedom (SDoF) region. It is shown that, in presence of local feedback and delayed CSI, the sum SDoF region of the MIMO X-channel is *same* as the SDoF region of the two-user MIMO BC with $2M$ antennas at the transmitter and N antennas at each receiver respectively. This result shows that, upon availability of feedback and delayed CSI, 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 *global* feedback is conveyed to the transmitters. Furthermore, we also study the case in which only local feedback is provided to the transmitters, i.e., without CSI, and we derive a lower bound on the sum SDoF for this model. We illustrate our results with the help of some numerical examples.

1 Introduction

The X-channel with delayed CSI and without secrecy constraints is studied recently in [2,3] from DoF perspective. In [2], the authors study a two-user MIMO X-channel with delayed CSI and establish a lower bound on the sum DoF. Tandon *et. al.* in [3] study a model similar to the one in [2] with channel output feedback from each receiver available to the respective transmitter. In [3], optimal sum degrees of freedom of the MIMO X-channel is characterized. This result sheds light on the role of feedback for the MIMO X-channel — due to availability of feedback and delayed CSI, not only Transmitter 1 is able to reconstruct the information transmitted by Transmitter 2, it also helps Transmitter 2 to reconstruct the information sent by Transmitter 1. In [3], among other observations, it is shown that the ability of each transmitter to reconstruct the information sent by the other transmitter is a fundamental step in the optimality. Yang *et. al.* in [1] study the problem of secure transmission over a two-user MIMO BC with delayed CSI available at the transmitter. In [1], 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) and is characterized for the two-user MIMO BC. The achievability follows by a combination of Maddah Ali-Tse scheme [4] with additional noise injection for security.

In this work, we consider the two-user (M, M, N, N)–MIMO X-channel studied by Tandon *et. al.* in [3] by introducing additional security constraints at the transmission as shown in Figure 1, where each transmitter is equipped with M-antennas and each receiver is equipped with N-antennas respectively. In this model, Transmitter 1 transmits confidential messages W_{11} to Receiver 1 and W_{12} to Receiver 2 respectively. Similarly, Transmitter 2 transmits W_{21} to Receiver 1 and W_{22} to Receiver 2 respectively. The channel output at each receiver along with the delayed CSI is fed back to the respective transmitter. For this setup each receiver plays the role of an eavesdropper for the other receiver, i.e., for message W_{11} and W_{21}, Receiver 2 acts as an eavesdropper for the messages intended for Receiver 1 ; and for message W_{12} and W_{22}, Receiver 1 acts as an eavesdropper for the messages intended for Receiver 2. For this model, we study *secure* transmission from degrees of freedom perspective.

2 Channel Model and Definitions

We consider the two-user MIMO X-channel in which each receiver knows the perfect instantaneous CSI along with the past CSI of the other receiver. The outputs received at Receiver 1 and 2 for each symbol time are given by

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

where $\mathbf{x}_i \in \mathbb{C}^M$ is the input vector transmitted by $\mathbf{Tx}_i$, $i \in \{1, 2\}$ and $\mathbf{H}_{ji} \in \mathbb{C}^{N\times M}$ is the channel matrix connecting $\mathbf{Tx}_i$ and $\mathbf{Rx}_j$,

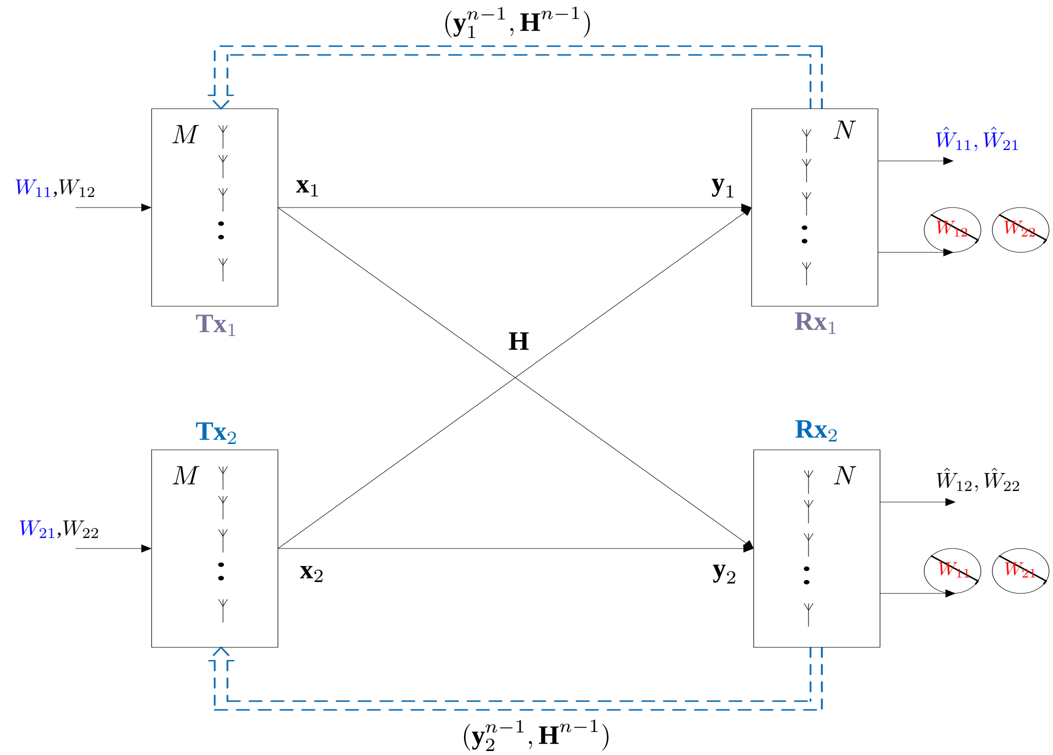

FIGURE 1 – The MIMO X-channel with local feedback and delayed CSI with security constraints.

$j \in \{1,2\}$, $\mathbf{y}_j \in \mathbb{C}^N$ is the output vector received at the jth receiver and $\mathbf{z}_j \in \mathbb{C}^N$ represents the additive noise vector at the jth receiver, where $\mathbf{z}_j \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$. Furthermore, the channel fading coefficients are independent and identically distributed (i.i.d.) complex Gaussian random variables. The transmitter inputs are bounded by average block power constraints $\sum_{t=1}^{n} \mathbb{E}[\|\mathbf{x}_i[t]\|^2] \leq nP$, for, $i \in \{1,2\}$. We define $\mathbf{H}[t] := \begin{bmatrix} \mathbf{H}_{11}[t] & \mathbf{H}_{12}[t] \\ \mathbf{H}_{21}[t] & \mathbf{H}_{22}[t] \end{bmatrix}$ be the channel state matrix and $\mathbf{H}^{t-1} := \{\mathbf{H}[1], \dots, \mathbf{H}[t-1]\}$ be the collection of channel state matrices for the past $t-1$ symbols duration. We assume that the channel state matrix $\mathbf{H}[t]$ is a full rank matrix almost surely at each time instant. We denote $\mathbf{y}_j^{t-1} := \{\mathbf{y}_j[1], \dots, \mathbf{y}_j[t-1]\}$ be the output at $\mathbf{Rx}_j$ for the past $t-1$ symbols. At each time instant t, the past states of the channel $\mathbf{H}^{t-1}$ are known to all terminals. However the instantaneous states $(\mathbf{H}_{11}[t], \mathbf{H}_{21}[t])$ are known only to Receiver 1 ; and the instantaneous states $(\mathbf{H}_{12}[t], \mathbf{H}_{22}[t])$ are known only to Receiver 2. The coding scheme for the Gaussian (M, M, N, N)–MIMO X-channel with local feedback and delayed CSI consists of a sequence of two stochastic encoding functions at the transmitters

$$\{\phi_{1t} \;:\; \mathcal{W}_{11} \times \mathcal{W}_{12} \times \mathcal{H}^{t-1} \times \mathcal{Y}_1^{N(t-1)} \longrightarrow \mathcal{X}_1^M\}_{t=1}^{n}$$
$$\{\phi_{2t} \;:\; \mathcal{W}_{21} \times \mathcal{W}_{22} \times \mathcal{H}^{t-1} \times \mathcal{Y}_2^{N(t-1)} \longrightarrow \mathcal{X}_2^M\}_{t=1}^{n}, \quad (2)$$

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

$$\psi_{11} \;:\; \mathcal{Y}_1^{Nn} \times \mathcal{H}^{n-1} \times \mathcal{H}_{11} \times \mathcal{H}_{12} \longrightarrow \hat{\mathcal{W}}_{11},$$
$$\psi_{21} \;:\; \mathcal{Y}_1^{Nn} \times \mathcal{H}^{n-1} \times \mathcal{H}_{11} \times \mathcal{H}_{12} \longrightarrow \hat{\mathcal{W}}_{21},$$
$$\psi_{12} \;:\; \mathcal{Y}_2^{Nn} \times \mathcal{H}^{n-1} \times \mathcal{H}_{21} \times \mathcal{H}_{22} \longrightarrow \hat{\mathcal{W}}_{12},$$
$$\psi_{22} \;:\; \mathcal{Y}_2^{Nn} \times \mathcal{H}^{n-1} \times \mathcal{H}_{21} \times \mathcal{H}_{22} \longrightarrow \hat{\mathcal{W}}_{22}. \quad (3)$$

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

$$\lim_{P\to\infty} \limsup_{n\to\infty} p\{\hat{W}_{ij} \neq W_{ij} | W_{ij}\} = 0, \;\; \text{for all } (i,j) \in \{1,2\}^2. \quad (4)$$

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

$$\lim_{P\to\infty} \liminf_{n\to\infty} \frac{\log |\mathcal{W}_{ij}(n,P)|}{n \log P} \geq d_{ij}, \quad \text{for all } (i,j) \in \{1,2\}^2$$
$$\lim_{P\to\infty} \limsup_{n\to\infty} p\{\hat{W}_{ij} \neq W_{ij} | W_{ij}\} = 0, \quad \text{for all } (i,j) \in \{1,2\}^2, \quad (5)$$

as well as the perfect secrecy conditions

$$\lim_{P\to\infty} \limsup_{n\to\infty} \frac{I(W_{12}, W_{22}; \mathbf{y}_1^n, \mathbf{H}^n)}{n \log P} = 0$$
$$\lim_{P\to\infty} \limsup_{n\to\infty} \frac{I(W_{11}, W_{21}; \mathbf{y}_2^n, \mathbf{H}^n)}{n \log P} = 0. \quad (6)$$

We define the sum SDoF region of the MIMO X-channel with local feedback and delayed, $\mathcal{C}_{\text{SDoF}}^{\text{sum}}$, as the set of all pairs $(d_{11} + d_{21}, d_{12} + d_{22})$ for all achievable non-negative SDoF quadruple $(d_{11}, d_{12}, d_{21}, d_{22})$. We define the total (sum) SDoF as $\text{SDoF}_{\text{total}}^{\text{d-CSI,F}}$ = $\max_{(d_{11}+d_{21}, d_{12}+d_{22})} d_{11} + d_{12} + d_{21} + d_{22}$.

3 Main Results

Due to the space limitations, the proofs of the results of this paper are omitted. Complete proofs are available in [5]. Before proceeding to the formal statement of the theorem, we first define a quantity that is repeatedly used in this section.

Definition 1 *Let, for given non-negative* (M, N)*,*

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

The following theorem provides the sum SDoF region for the MIMO X-channel with local feedback and delayed CSI.

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

$$\begin{aligned} \frac{d_{11}+d_{21}}{d_s(N,N,2M)} + \frac{d_{12}+d_{22}}{\min(2M,2N)} &\leq 1 \\ \frac{d_{11}+d_{21}}{\min(2M,2N)} + \frac{d_{12}+d_{22}}{d_s(N,N,2M)} &\leq 1 \end{aligned} \qquad (7)$$

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

Remark 1 *The sum SDoF region of the MIMO X-channel in Theorem 1 is same as the SDoF region of the two-user MIMO BC given in [1, Corollary 3.1] with* $2M$*-transmit antennas and* N*-antennas at each receiver respectively. This result shows that there is no performance loss in terms of sum SDoF due to the distributed nature of the transmitter antennas.*

We now consider the two-user MIMO X-channel with global feedback. In this model, the output at each receiver is fed back to both transmitters. For the two-user MIMO X-channel, the output fed back from each receiver to both transmitters is still useful because each receiver not only acts as an eavesdropper for the other receiver but also gets useful information from the corresponding transmitter of the other receiver. For example, Receiver 2 acts as an eavesdropper for the message W_{11} which is transmitted from Transmitter 1 and is intended for Receiver 1, but also gets message W_{12} from Transmitter 1. In this case feed back to Transmitter 1 from Receiver 2 can still provide some useful information which can be used by Transmitter 1's encoder.
The following theorem provides the sum SDoF region of MIMO X-channel with global feedback.

Theorem 2 *The sum SDoF region of two-user* (M, M, N, N)*–MIMO X-channel with global feedback is given by* (7)*.*

We now consider the two-user MIMO X-channel with local feedback. In this model, the output at the ith Receiver, $i = 1, 2$ is fedback to the ith Transmitter only. In this model, each receiver which acts as an eavesdropper to the other receiver only feeds back the information to the corresponding transmitter. Before proceeding to the formal statement of the theorem, we first define a quantity $d_s^{\text{local}}(N, N, M)$.

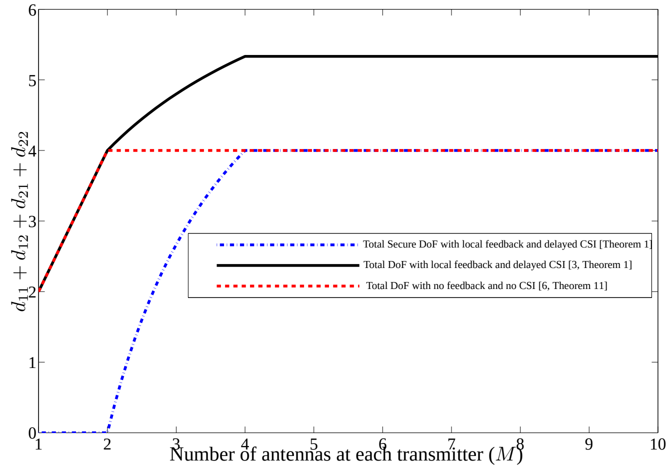

FIGURE 2 – Total Degrees of Freedom as a function of number of antennas at the transmitter, with fixed number of antennas at each receiver, $N = 4$.

Definition 2 *Let, for given non-negative* (M, N)*,*

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

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

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

$$\begin{aligned} \frac{d_{11}+d_{21}}{d_s^{local}(N,N,2M)} + \frac{d_{12}+d_{22}}{\min(2M,2N)} &\leq 1 \\ \frac{d_{11}+d_{21}}{\min(2M,2N)} + \frac{d_{12}+d_{22}}{d_s^{local}(N,N,2M)} &\leq 1 \end{aligned} \qquad (8)$$

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

Now, we compare the total SDoF of the model in Figure 1 with the total DoF of (M, M, N, N)–MIMO X-channel with feedback and delayed CSI ; and no feedback and no CSI available at the transmitters. Figure 2 shows the total DoF as a function of transmit antennas with fixed number of antennas at each receiver, i.e., $N = 4$. The total SDoF increases with the number of antennas at the transmitter and saturates as the number of antennas at transmitter becomes equal to the number of antennas at the receiver. This shows that there is no gain in terms of total SDoF if $M \geq N$. It is interesting to note that for the case $M \geq N$ the total SDoF of the MIMO X-channel with local output feedback and delayed CSI is the same as the total DoF of the MIMO X-channel with no feedback and no CSI at transmitters. This result shows that there is no performance loss due to security constraint if local feedback and delayed CSI is available at the transmitters.

Acknowledgment

This work has been supported in part by the European Commission in the framework of the 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.

Références

[1] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," 2011. [Online]. Available : http://arxiv.org/abs/1112.2306

[2] 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.

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

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

[5] A. Zaidi, Z. H. Awan, S. S. (Shitz), and L. Vandendorpe, "Secure degrees of freedom of MIMO X-channel with output feedback and delayed CSI." [Online]. Available : http://www-syscom.univ-mlv.fr/~zaidi/publications

[6] 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, 2012.