SECURE MIMO INTERFERENCE CHANNEL WITH CONFIDENTIAL MESSAGES AND DELAYED CSIT

Tong Zhang, and P. C. Ching,

Department of Electronic Engineering, The Chinese University of Hong Kong, Hong Kong S.A.R. of China

ABSTRACT

Secure degrees-of-freedom (SDoF) for multiple-input multiple-output (MIMO) interference channel with confidential messages and delayed channel state information at transmitter (CSIT) remains unclear, even for single-input single-output (SISO) case. In this paper, we propose an achievable SDoF for MIMO interference channel with confidential messages and delayed CSIT by designing a multi-phase achievable scheme. For the proposed scheme, we first establish a multi-phase transmission procedure with undetermined phase durations. In the next, the security and decoding conditions on feasible phase durations are derived. Finally, an achievable SDoF maximization problem with respect to phase durations is solved under security and decoding conditions. Due to effective coordination of interference, the proposed achievable SDoF can be 20% greater than the SDoF of MIMO wiretap channel with delayed CSIT, which removes one transmitter from the MIMO interference channel.

***Index Terms*—** Artificial noise, confidential messages, delayed CSIT, secure degrees-of-freedom, MIMO interference channel

1. INTRODUCTION

The multiple-input multiple-output (MIMO) interference channel has two multiple antenna transmitters and two multiple antenna receivers, and each transmitter attempts to communicate with a corresponding receiver as a communication pair. Physical layer security is an important aim of wireless communications [1–4]. With confidential messages, each communication pair can protect its information from leakage to the other receiver, thus facilitating secure communication [5–7].

The secure channel capacity of the MIMO interference channel with confidential messages characterizes the maximal secure achievable rate for error-free communication. Due to the difficulty in characterizing the secure channel capacity, secure degrees-of-freedom (SDoF) as a first-order approximation of secure channel capacity and a measurement of the maximal number of independent channels was investigated in [8–10]. However, for the above results, channel state information at transmitter (CSIT) is assumed to be perfect and no delay for channel state information (CSI) feedback.

Delayed CSIT can be completely different from the current one, which was first studied from DoF perspective in K-user multiple-input single-output (MISO) broadcast channel without security [11], then two-user MIMO broadcast channel [12] and three-user MIMO broadcast channel without security [13, 14].

With the goal of ensuring security, SDoF with confidential messages and delayed CSIT for two-user MIMO broadcast channel was first obtained in [15]. Thereafter, for the MIMO X channel, the S-DoF with confidential messages, delayed CSIT and output feedback was derived in [16]. For $2 \times 2 \times 2$ single-input single-output (SISO) interference channel with confidential messages and delayed CSIT, SDoF is given in [17]. For a large number of users SISO interference channel with confidential messages and delayed CSIT, an achievable SDoF is given in [18]. The MIMO interference channel is a basic wireless network. Nevertheless, knowledge of SDoF for MIMO interference channel with confidential messages and delayed CSIT remains limited.

In this paper, we investigate the achievable SDoF for MIMO interference channel with confidential messages and delayed CSIT by designing an optimized achievable scheme. We first propose a multi-phase transmission achievable scheme, where artificial noise is utilized with delayed CSIT to provide secure communication. Then, we analyze the decoding condition and security condition, under which we optimize the phase duration of the proposed scheme. In the end, we show that the resulted achievable SDoF can yield a 20% gain over SDoF of MIMO wiretap channel with confidential messages and delayed CSIT. The obtained achievable SDoF that is a lower bound of SDoF is summarized as follows:

$$\text{SDoF} \geq \begin{cases} 0, & M/N \leq 1 \\ \dfrac{2MN(M-N)}{M^2+N^2}, & 1 < M/N \leq 2 \\ 4N/5, & 2 < M/N \end{cases} \tag{1}$$

where each transmitter and each receiver has M antennas and N antennas, respectively.

2. SYSTEM MODEL

2.1. MIMO Interference Channel and Delayed CSIT

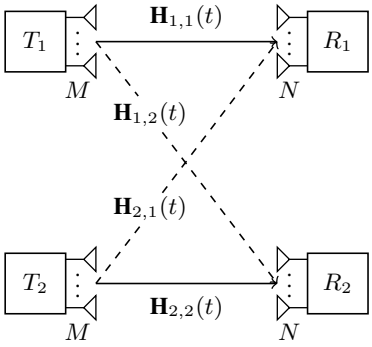

Fig. 1. (M, M, N, N) MIMO interference channel.

A (M, M, N, N) MIMO interference channel has two transmitters and two receivers, which is depicted in Fig. 1. The antenna configurations are symmetrical, that is, each transmitter is equipped with M antennas and each receiver is equipped with N antennas. At time

slot t, the channel state matrix from the transmitter $i, i = 1, 2$ to the receiver j, $j = 1, 2$ is denoted by $\mathbf{H}_{i,j}[t] \in \mathbb{C}^{N\times M}$, whose elements are i.i.d. across space and time, and drawn from a continuous distribution. The CSIT is delayed, i.e., $\mathbf{H}_{i,j}[t-\tau], \tau = 1, 2, \cdots; j = 1, 2$ is available at transmitter $i = 1, 2$. The transmit signal at transmitter $i, i = 1, 2$ and received signal at the receiver $j, j = 1, 2$ are denoted by $\mathbf{x}_i[t]$ and $\mathbf{y}_j[t]$, respectively. All the CSI at receiver is perfect and known at both receivers.

2.2. Confidential Messages and Secure Degrees-of-Freedom

Transmitter 1 communicates with receiver 1 using confidential messages, which incurs zero information leakage to receiver 2. Meanwhile, transmitter 2 communicates with receiver 2 using confidential messages, which incurs zero information leakage to receiver 1. A secure code $(2^{nR_1(\text{SNR})}, 2^{nR_2(\text{SNR})}, n)$ with secure achievable rates $R_1(\text{SNR})$ and $R_2(\text{SNR})$ is defined as follows: The communication process adopts n channel uses. A set of confidential messages at transmitter 1, denoted by $\mathbf{W}_1 = [1 : 2^{nR_1(\text{SNR})}]$. A set of confidential messages at transmitter 2, denoted by $\mathbf{W}_2 = [1 : 2^{nR_2(\text{SNR})}]$. An encoder at transmitter j maps confidential message $w_j \in \mathbf{W}_j$ to a codeword $x^n \in \mathbf{X}^n$. A decoder at receiver j maps the output signal $\mathbf{y}_j^n$ to an estimated message $\widehat{w}_j$. The secure code should both satisfy the following reliability constraint:

$$\lim_{n\to\infty} \Pr[w_j \neq \widehat{w}_j] = 0, \quad j = 1, 2 \tag{2}$$

and the following security constraint:

$$\lim_{n\to\infty} \frac{1}{n} I(w_1; \mathbf{y}_2^n) = 0 \tag{3a}$$

$$\lim_{n\to\infty} \frac{1}{n} I(w_2; \mathbf{y}_1^n) = 0 \tag{3b}$$

Secure channel capacity is defined as the maximal sum of secure achievable rates, given by

$$C = \max \; R_1(\text{SNR}) + R_2(\text{SNR}) \tag{4}$$

Secure degrees-of-freedom, denoted by SDoF for short, is a first-order approximation of secure channel capacity and defined as

$$\text{SDoF} = \lim_{\text{SNR}\to\infty} \frac{C}{\log \text{SNR}} \tag{5}$$

3. PROPOSED ACHIEVABLE SCHEME FOR $M \leq N$ CASE

If the receiver has more antenna than the transmitter's, i.e., $M \leq N$, any transmitted signals from one transmitter can be immediately decoded by an eavesdropper even artificial noise. Therefore, in this case, we claim that the achievable SDoF is 0 and the achievable scheme is that two transmitters keep silent.

4. PROPOSED ACHIEVABLE SCHEME FOR $N < M$ CASE

4.1. Transmission Procedure

The transmission procedure contains five phases. As depicted in Fig. 2, the artificial noise for subsequent secure data transmission is sent in first two phases. In Phases 3 and 4, the data symbols with the received artificial noise signals are transmitted so that the desired receiver can cancel its received artificial noise signals for retrieving data symbol signals while the eavesdropper cannot do. In Phase 5, for providing the lacking equations for decoding, the interference signals in Phases 3 and 4 are combined together and re-transmitted.

Phase-I (Artificial Noise Transmission from Transmitter 1): This phase spans τ_1 time slots. In this phase, transmitter 1 transmits artificial noise. At the same time, transmitter 2 keeps silent. The artificial noise is denoted by $\mathbf{u}_1 \in \mathbb{C}^{\min\{M,2N\}\tau_1}$. After sending artificial noise, the received signals are given by

$$\mathbf{y}_1^{\text{I}} = \underline{\mathbf{H}}_{1,1}^{\text{I}} \mathbf{u}_1 \tag{6a}$$

$$\mathbf{y}_2^{\text{I}} = \underline{\mathbf{H}}_{1,2}^{\text{I}} \mathbf{u}_1 \tag{6b}$$

where $\underline{\mathbf{H}}_{1,1}^{\text{I}}$ and $\underline{\mathbf{H}}_{1,2}^{\text{I}}$ are defined as follows:

$$\underline{\mathbf{H}}_{1,1}^{\text{I}} \triangleq \text{blkdiag}\{\mathbf{H}_{1,1}(1), \cdots, \mathbf{H}_{1,1}(\tau_1)\}$$

$$\underline{\mathbf{H}}_{1,2}^{\text{I}} \triangleq \text{blkdiag}\{\mathbf{H}_{1,2}(1), \cdots, \mathbf{H}_{1,2}(\tau_1)\}$$

Phase-II (Artificial Noise Transmission from Transmitter 2): Transmitter 2 transmits artificial noise. At the same time, transmitter 1 keeps silent. Due to the symmetry of antenna configurations, this phase spans τ_1 time slots as well. The artificial noise is denoted by $\mathbf{u}_2 \in \mathbb{C}^{\min\{M,2N\}\tau_1}$. After sending artificial noise, the received signals are given by

$$\mathbf{y}_1^{\text{II}} = \underline{\mathbf{H}}_{2,1}^{\text{II}} \mathbf{u}_2 \tag{7a}$$

$$\mathbf{y}_2^{\text{II}} = \underline{\mathbf{H}}_{2,2}^{\text{II}} \mathbf{u}_2 \tag{7b}$$

where $\underline{\mathbf{H}}_{2,1}^{\text{II}}$ and $\underline{\mathbf{H}}_{2,2}^{\text{II}}$ are defined as follows:

$$\underline{\mathbf{H}}_{2,1}^{\text{II}} \triangleq \text{blkdiag}\{\mathbf{H}_{2,1}(\tau_1 + 1), \cdots, \mathbf{H}_{2,1}(2\tau_1)\}$$

$$\underline{\mathbf{H}}_{2,2}^{\text{II}} \triangleq \text{blkdiag}\{\mathbf{H}_{2,2}(\tau_1 + 1), \cdots, \mathbf{H}_{2,2}(2\tau_1)\}$$

Phase-III (Secure Data Transmission for Receiver 1): This phase spans τ_2 time slots. The information symbols desired by receiver 1, $\mathbf{s}_1 \in \mathbb{C}^{\min\{M,2N\}\tau_2}$, is transmitted in this phase. The CSIT feedback occurs at the beginning of this phase. Based on the CSIT of Phase-I, transmitter 1 can re-construct the $\mathbf{y}_1^{\text{I}}$. To ensure security, the secure transmit signal at transmitter 1 is designed as follows:

$$\mathbf{x}_1^{\text{III}} = \mathbf{s}_1 + \mathbf{\Phi}_1 \mathbf{y}_1^{\text{I}} \in \mathbb{C}^{\min\{M,2N\}\tau_2} \tag{8}$$

where $\mathbf{\Phi}_1 \in \mathbb{C}^{\min\{M,2N\}\tau_2 \times N\tau_1}$ is the offline full rank matrix and known at all receivers. At the same time, transmitter 2 keeps silent. The received signals are given by

$$\mathbf{y}_1^{\text{III}} = \underline{\mathbf{H}}_{1,1}^{\text{III}} \left(\mathbf{s}_1 + \mathbf{\Phi}_1 \mathbf{y}_1^{\text{I}}\right) \tag{9a}$$

$$\mathbf{y}_2^{\text{III}} = \underline{\mathbf{H}}_{1,2}^{\text{III}} \left(\mathbf{s}_1 + \mathbf{\Phi}_1 \mathbf{y}_1^{\text{I}}\right) \tag{9b}$$

where $\underline{\mathbf{H}}_{1,1}^{\text{III}}$ and $\underline{\mathbf{H}}_{1,2}^{\text{III}}$ are defined as follows:

$$\underline{\mathbf{H}}_{1,1}^{\text{III}} \triangleq \text{blkdiag}\{\mathbf{H}_{1,1}^{\text{III}}(2\tau_1 + 1), \cdots, \mathbf{H}_{1,1}^{\text{III}}(2\tau_1 + \tau_2)\}$$

$$\underline{\mathbf{H}}_{1,2}^{\text{III}} \triangleq \text{blkdiag}\{\mathbf{H}_{1,2}^{\text{III}}(2\tau_1 + 1), \cdots, \mathbf{H}_{1,2}^{\text{III}}(2\tau_1 + \tau_2)\}$$

Receiver 1 cannot decode any desired data symbols, due to lacking equations. In order to decode, receiver 1 needs $(\min\{M, 2N\} - N)\tau_2$ equations, which will be provided in the final phase.

Phase-IV (Secure Data Transmission for Receiver 2): The information symbols desired by receiver 2, $\mathbf{s}_2 \in \mathbb{C}^{\min\{M,2N\}\tau_2}$, is transmitted in this phase. Due to the symmetry of antenna configurations,

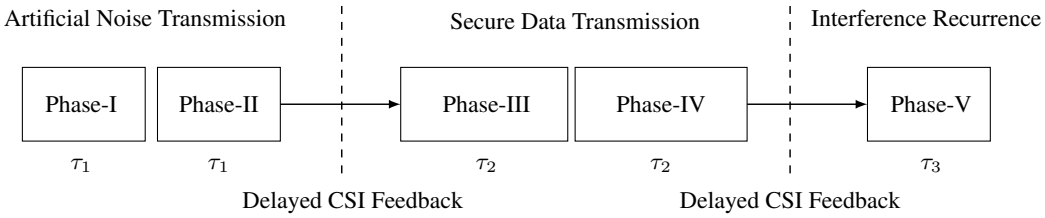

Fig. 2. A flow-diagram of the proposed transmission procedure for $N < M$ case.

this phase spans τ_2 time slots as well. Based on the CSIT of Phase-II, transmitter 2 can re-construct the $\mathbf{y}_2^{\text{II}}$. To ensure the security, the secure transmit signal at transmitter 2 is designed as follows:

$$\mathbf{x}_2^{\text{IV}} = \mathbf{s}_2 + \mathbf{\Phi}_2 \mathbf{y}_2^{\text{II}} \in \mathbb{C}^{\min\{M,2N\}\tau_2} \tag{10}$$

where $\mathbf{\Phi}_2 \in \mathbb{C}^{\min\{M,2N\}\tau_2 \times N\tau_1}$ is the offline full rank matrix and known at all receivers. At the same time, transmitter 1 keeps silent. The received signals are given by

$$\mathbf{y}_1^{\text{IV}} = \underline{\mathbf{H}}_{2,1}^{\text{IV}} \left(\mathbf{s}_2 + \mathbf{\Phi}_2 \mathbf{y}_2^{\text{II}} \right) \tag{11a}$$

$$\mathbf{y}_2^{\text{IV}} = \underline{\mathbf{H}}_{2,2}^{\text{IV}} \left(\mathbf{s}_2 + \mathbf{\Phi}_2 \mathbf{y}_2^{\text{II}} \right) \tag{11b}$$

where $\underline{\mathbf{H}}_{2,1}^{\text{IV}}$ and $\underline{\mathbf{H}}_{2,2}^{\text{IV}}$ are defined as follows:

$$\underline{\mathbf{H}}_{2,1}^{\text{IV}} \triangleq \text{blkdiag}\{\mathbf{H}_{2,1}^{\text{IV}}(2\tau_1 + \tau_2 + 1), \cdots, \mathbf{H}_{2,1}^{\text{IV}}(2\tau_1 + 2\tau_2)\}$$
$$\underline{\mathbf{H}}_{2,2}^{\text{IV}} \triangleq \text{blkdiag}\{\mathbf{H}_{2,2}^{\text{IV}}(2\tau_1 + \tau_2 + 1), \cdots, \mathbf{H}_{2,2}^{\text{IV}}(2\tau_1 + 2\tau_2)\}$$

Receiver 2 cannot decode any desired symbols, due to lacking equations. For decoding, receiver 2 needs $(\min\{M, 2N\} - N)\tau_2$ equations, which will be provided in the last phase.

Phase-V (Interference Recurrence for Equation Switching): This phase spans τ_3 time slots. All lacking equations are provided in this phase. In fact, the designed transmit signals are used to facilitate the switch of unwanted equations in Phases 3 and 4. The transmit signals are given by

$$\mathbf{x}_1^{\text{V}} = \mathbf{B}_1 \mathbf{y}_2^{\text{III}}$$
$$\mathbf{x}_2^{\text{V}} = \mathbf{B}_2 \mathbf{y}_1^{\text{IV}}$$

where $\mathbf{B}_1 \in \mathbb{C}^{N\tau_3 \times N\tau_2}$ and $\mathbf{B}_2 \in \mathbb{C}^{N\tau_3 \times N\tau_2}$ are offline full rank matrix and known at all receivers. Then, the received signals are written as follows:

$$\mathbf{y}_1^{\text{V}} = \underline{\mathbf{H}}_{1,1}^{\text{V}} \mathbf{B}_1 \mathbf{y}_2^{\text{III}} + \underline{\mathbf{H}}_{2,1}^{\text{V}} \mathbf{B}_2 \mathbf{y}_1^{\text{IV}} \tag{12a}$$

$$\mathbf{y}_2^{\text{V}} = \underline{\mathbf{H}}_{1,2}^{\text{V}} \mathbf{B}_1 \mathbf{y}_2^{\text{III}} + \underline{\mathbf{H}}_{2,2}^{\text{V}} \mathbf{B}_2 \mathbf{y}_1^{\text{IV}} \tag{12b}$$

where $\underline{\mathbf{H}}_{1,1}^{\text{V}}, \underline{\mathbf{H}}_{1,2}^{\text{V}}, \underline{\mathbf{H}}_{2,1}^{\text{V}}$, and $\underline{\mathbf{H}}_{2,2}^{\text{V}}$ are defined as follows:

$$\underline{\mathbf{H}}_{1,1}^{\text{V}} \triangleq \text{blkdiag}\{\mathbf{H}_{1,1}^{\text{V}}(2\tau_1 + 2\tau_2 + 1), \cdots, \mathbf{H}_{1,1}^{\text{V}}(2\tau_1 + 2\tau_2 + \tau_3)\}$$
$$\underline{\mathbf{H}}_{1,2}^{\text{V}} \triangleq \text{blkdiag}\{\mathbf{H}_{1,2}^{\text{V}}(2\tau_1 + 2\tau_2 + 1), \cdots, \mathbf{H}_{1,2}^{\text{V}}(2\tau_1 + 2\tau_2 + \tau_3)\}$$
$$\underline{\mathbf{H}}_{2,1}^{\text{V}} \triangleq \text{blkdiag}\{\mathbf{H}_{2,1}^{\text{V}}(2\tau_1 + 2\tau_2 + 1), \cdots, \mathbf{H}_{2,1}^{\text{V}}(2\tau_1 + 2\tau_2 + \tau_3)\}$$
$$\underline{\mathbf{H}}_{2,2}^{\text{V}} \triangleq \text{blkdiag}\{\mathbf{H}_{2,2}^{\text{V}}(2\tau_1 + 2\tau_2 + 1), \cdots, \mathbf{H}_{2,2}^{\text{V}}(2\tau_1 + 2\tau_2 + \tau_3)\}$$

The receiver 1 can obtain lacking equations by the cancellation $\mathbf{y}_1^{\text{V}} - \underline{\mathbf{H}}_{2,1}^{\text{V}} \mathbf{B}_2 \mathbf{y}_1^{\text{IV}}$. The receiver 2 can obtain lacking equations by the cancellation $\mathbf{y}_2^{\text{V}} - \underline{\mathbf{H}}_{1,2}^{\text{V}} \mathbf{B}_1 \mathbf{y}_2^{\text{III}}$.

The duration of each phase has not been determined. That is, τ_1, τ_2 and τ_3 are unknown. Next, we analyze the desired data symbols decoding condition and security condition. Based on these two conditions, we establish an achievable SDoF maximization problem so that optimal τ_1, τ_2 and τ_3 can be obtained.

4.2. Decoding Condition

We investigate the condition that can guarantee the decoding of all transmitted symbols. First, the effective decoding equation of receiver 1 is given by

$$\begin{bmatrix} \mathbf{y}_1^{\text{III}} - \underline{\mathbf{H}}_{1,1}^{\text{III}} \mathbf{\Phi}_1 \mathbf{y}_1^{\text{I}} \\ \mathbf{y}_1^{\text{V}} - \underline{\mathbf{H}}_{1,1}^{\text{V}} \mathbf{B}_1 \underline{\mathbf{H}}_{1,2}^{\text{III}} \mathbf{\Phi}_1 \mathbf{y}_1^{\text{I}} - \underline{\mathbf{H}}_{2,1}^{\text{V}} \mathbf{B}_2 \mathbf{y}_1^{\text{IV}} \end{bmatrix} = \underbrace{\begin{bmatrix} \underline{\mathbf{H}}_{1,1}^{\text{III}} \\ \underline{\mathbf{H}}_{1,1}^{\text{V}} \mathbf{B}_1 \underline{\mathbf{H}}_{1,2}^{\text{III}} \end{bmatrix}}_{\mathbf{H}_1} \mathbf{s}_1 \tag{13}$$

Similarly, the effective decoding equation of receiver 2 is given by

$$\begin{bmatrix} \mathbf{y}_2^{\text{IV}} - \underline{\mathbf{H}}_{2,2}^{\text{IV}} \mathbf{\Phi}_2 \mathbf{y}_2^{\text{II}} \\ \mathbf{y}_2^{\text{V}} - \underline{\mathbf{H}}_{2,2}^{\text{V}} \mathbf{B}_2 \underline{\mathbf{H}}_{2,1}^{\text{IV}} \mathbf{\Phi}_2 \mathbf{y}_2^{\text{II}} - \underline{\mathbf{H}}_{1,2}^{\text{V}} \mathbf{B}_1 \mathbf{y}_2^{\text{III}} \end{bmatrix} = \underbrace{\begin{bmatrix} \underline{\mathbf{H}}_{2,2}^{\text{IV}} \\ \underline{\mathbf{H}}_{2,2}^{\text{V}} \mathbf{B}_2 \underline{\mathbf{H}}_{2,1}^{\text{IV}} \end{bmatrix}}_{\mathbf{H}_2} \mathbf{s}_2 \tag{14}$$

Then, we must ensure that the transmitted symbols desired by receiver 1 and receiver 2 can be decoded by receiver 1 and 2, respectively. This requirement is equivalent to the rank of $\mathbf{H}_1$ and $\mathbf{H}_2$ is equal to dimension of $\mathbf{s}_1$ and $\mathbf{s}_2$, respectively. Due to the symmetry of antenna configurations, we must have $\text{rank}\{\mathbf{H}_1\} = \text{rank}\{\mathbf{H}_2\}$ and $\dim\{\mathbf{s}_1\} = \dim\{\mathbf{s}_2\}$. Thus, it is sufficient to prove that $\text{rank}\{\mathbf{H}_1\} = \dim\{\mathbf{s}_1\}$.

The number of columns of $\mathbf{H}_1$ is $\min\{M, 2N\}\tau_2$ and number of rows of $\mathbf{H}_1$ is $\min\{N\tau_3 + N\tau_2, \min\{M, 2N\}\tau_2\}$, thus the rank of $\mathbf{H}_1$ is $\min\{N\tau_3 + N\tau_2, \min\{M, 2N\}\tau_2\}$. Therefore, the decoding condition, i.e., the rank of $\mathbf{H}_1$ is equal to the number of transmitted symbols desired for receiver 1, is given by

$$\min\{N\tau_3 + N\tau_2, \min\{M, 2N\}\tau_2\} = \min\{M, 2N\}\tau_2, \tag{15}$$

which is equivalent to

$$N\tau_3 = \min\{M - N, N\}\tau_2 \tag{C1}$$

The intuition behind the condition (C1) is that the received equations in the last phase must be equal to the required amount of lacking equations in previous phases.

4.3. Security Condition

The communication pair should maintain security from each other. That is, the symbols transmitted by transmitter 1 and intended for

receiver 1 should be zero mutual information between itself and receiver 2, and vice versa. The zero leakage of information from $\mathbf{s}_1$ to $\mathbf{y}_2 \triangleq [\mathbf{y}_2^I; \cdots; \mathbf{y}_2^V]$ (the collection of all received signals at receiver 2) is shown as follows:

$$
\begin{aligned}
& I(\mathbf{s}_1; \mathbf{y}_2 | \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2) \\
& \overset{(a)}{=} I(\underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1; \mathbf{y}_2 | \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2,) \\
& \overset{(b)}{=} I(\underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1, \mathbf{u}_1; \mathbf{y}_2 | \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2) - I(\mathbf{u}_1; \mathbf{y}_2 | \underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1, \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2) \\
& \overset{(c)}{=} I(\underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1, \mathbf{u}_1; \mathbf{y}_2 | \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2) - I(\mathbf{u}_1; \mathbf{y}_2 | \mathbf{s}_1, \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2) \\
& \overset{(d)}{\leq} I(\underline{\mathbf{H}}^{\mathrm{I}}_{1,2}\mathbf{u}_1, \underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1 + \underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{\Phi}_1\underline{\mathbf{H}}^{\mathrm{I}}_{1,1}\mathbf{u}_1; \mathbf{y}_2 | \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2) \\
& - I(\mathbf{u}_1; \mathbf{y}_2 | \mathbf{s}_1, \mathbf{s}_2, \underline{\mathbf{H}}^{\mathrm{II}}_{2,2}\mathbf{u}_2) \\
& = \mathrm{rank}\left\{ \begin{bmatrix} \mathbf{I}_{N\tau_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{N\tau_2} \\ \mathbf{0} & \underline{\mathbf{H}}^{\mathrm{V}}_{1,2}\mathbf{B}_1 \end{bmatrix} \right\} \log \mathrm{SNR} \\
& - \mathrm{rank}\left\{ \begin{bmatrix} \underline{\mathbf{H}}^{\mathrm{I}}_{1,2} \\ \underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{\Phi}_1\underline{\mathbf{H}}^{\mathrm{I}}_{1,1} \\ \underline{\mathbf{H}}^{\mathrm{V}}_{1,2}\mathbf{B}_1\underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{\Phi}_1\underline{\mathbf{H}}^{\mathrm{I}}_{1,1} \end{bmatrix} \right\} \log \mathrm{SNR} \\
& \overset{(e)}{=} N(\tau_1 + \tau_2) \log \mathrm{SNR} \\
& - \min\{N(\tau_1 + \tau_2), \min\{M, 2N\}\tau_1\} \log \mathrm{SNR} \\
& = \min\{0, N(\tau_1 + \tau_2) - \min\{M, 2N\}\tau_1\} \log \mathrm{SNR} \\
& = 0
\end{aligned}
$$

where

(a) Due to the Markov chains $\mathbf{s}_1 \leftrightarrow \underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1 \leftrightarrow \mathbf{y}_1$ and $\underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1 \leftrightarrow \mathbf{s}_1 \leftrightarrow \mathbf{y}_1$.

(b) Chain rule of mutual information.

(c) The same reason as (a).

(d) Due to the Markov chain $(\underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1, \mathbf{u}_1) \leftrightarrow (\underline{\mathbf{H}}^{\mathrm{I}}_{1,2}\mathbf{u}_1, \underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{s}_1 + \underline{\mathbf{H}}^{\mathrm{III}}_{2}\mathbf{\Phi}_1\underline{\mathbf{H}}^{\mathrm{I}}_{1,1}\mathbf{u}_1) \leftrightarrow \mathbf{y}_2$ and data processing inequality.

(e) The rank of the first matrix is same as blkdiag$\{\mathbf{I}_{N\tau_1}, \mathbf{I}_{N\tau_2}\}$, whose rank is $N(\tau_1 + \tau_2)$. The rank of the second matrix is determined by $[\underline{\mathbf{H}}^{\mathrm{I}}_{1,2}; \underline{\mathbf{H}}^{\mathrm{III}}_{1,2}\mathbf{\Phi}_1\underline{\mathbf{H}}^{\mathrm{I}}_{1,1}]$, whose rank is $\min\{N(\tau_1 + \tau_2), \min\{M, 2N\}\tau_1\}$.

It can be clearly seen that perfect security is equivalent to the following condition:

$$N(\tau_1 + \tau_2) - \min\{M, 2N\}\tau_1 = 0 \qquad \text{(C2)}$$

The intuition behind condition (C2) is that we must ensure that the artificial noise cannot be decoded at receiver 2 (eavesdropper).

For the analysis of zero leakage of information from $\mathbf{s}_2$ to $\mathbf{y}_1 \triangleq [\mathbf{y}_1^I; \cdots; \mathbf{y}_1^V]$, it is similar to the analysis for receiver 1 and omitted for simplicity. Due to the symmetry of antenna configurations, the security condition for receiver 2 is the same as that of receiver 1, which is condition (C2).

4.4. Maximization of Proposed Achievable SDoF

We aim at maximizing the achievable SDoF that the multi-phase transmission can attain. The problem is formulated as follows:

$$
\begin{aligned}
\max_{\tau_1, \tau_2, \tau_3 \in \mathbb{Z}_+} \quad & \frac{2\min\{M, 2N\}\tau_2}{2\tau_1 + 2\tau_2 + \tau_3} \\
\text{s.t.} \quad & \text{C1, C2}
\end{aligned}
$$

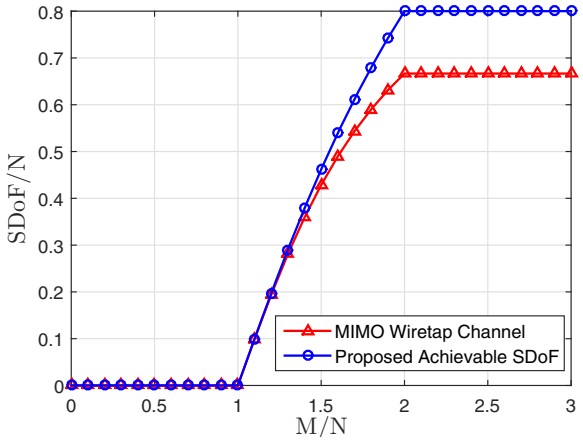

Fig. 3. Comparison with that of MIMO wiretap channel.

The objective function can be re-written as $\frac{2\min\{M,2N\}}{2\tau_1/\tau_2 + 2 + \tau_3/\tau_2}$. One can see that the values of τ_1/τ_2 and τ_3/τ_2 is uniquely determined by conditions (C1) and (C2), respectively. Therefore, the maximal achievable SDoF of proposed scheme is given by

$$\frac{2\min\{M, 2N\}\min\{M-N, N\}N}{2N^2 + 2\min\{M-N, N\}N + (\min\{M-N, N\})^2}$$

Concurrently, we can achieve the above maximal value by setting

$$
\begin{cases}
\tau_1 = N^2 \\
\tau_2 = \min\{M-N, N\}N \\
\tau_3 = (\min\{M-N, N\})^2
\end{cases} \qquad (16)
$$

5. PERFORMANCE COMPARISON

We compare the performance of the proposed achievable SDoF with SDoF of the MIMO wiretap channel with confidential messages and delayed CSIT. The MIMO wiretap channel has one transmitter with M antennas and one receiver with N antennas and single eavesdropper with N antennas, which is a special simplified scenario by removing one transmitter from MIMO interference channel. The SDoF of MIMO wiretap channel with confidential messages and delayed CSIT is given in [15]. The proposed achievable SDoF for MIMO interference channel is given in equation (1). Fig. 3 shows that the proposed achievable SDoF has an advantage over that of MIMO wiretap channel. Specially, when $2N \leq M$, the proposed result exhibits a 20% increase over that of the MIMO wiretap channel with confidential messages and delayed CSIT. The gain is due to the effective coordination of two transmitters, in contrast to the one transmitter in the MIMO wiretap channel.

6. CONCLUSION

In this paper, we proposed an achievable SDoF for MIMO interference channel with confidential messages and delayed CSIT for the first time. The result showed that the proposed achievable SDoF is clearly greater than the SDoF for the MIMO wiretap channel with confidential messages and delayed CSIT. Finally, we conjecture that the proposed achievable SDoF is maximal. Consequently, a tight upper bound is needed, which motivates our future work.

7. REFERENCES

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept 2016.

[4] Y. Ge and P. C. Ching, "Robust secrecy design for MIMO SWIPT with artificial noise and full-duplex receiver jamming," in *Proc. IEEE GlobalSIP, Dec. 2018*.

[5] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[6] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[7] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4529–4542, Oct 2009.

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

[9] K. Banawan and S. Ulukus, "Secure degrees of freedom of the Gaussian MIMO interference channel," in *2015 IEEE Asilomar*, Nov 2015, pp. 40–44.

[10] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[11] 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, July 2012.

[12] C. S. Vaze and M. K. Varanasi, "The degrees of freedom region of the two-user MIMO broadcast channel with delayed CSIT," in *Proc. ISIT*, 2011, pp. 199–203.

[13] M. J. Abdoli, A. Ghasemi, and A. K. Khandani, "On the degrees of freedom of three-user MIMO broadcast channel with delayed CSIT," in *Proc. ISIT*, 2011, pp. 209–213.

[14] T. Zhang, X. W. Wu, Y. F. Xu, Y. Ge, and P. C. Ching, "Three-user MIMO broadcast channel with delayed CSIT: A higher achievable DoF," in *Proc. ICASSP*, 2018, pp. 3709–3713.

[15] S. Yang, M. Kobayashi, P. Piantanida, and S. S. (Shitz), "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5244–5256, Sept 2013.

[16] A. Zaidi, Z. H. Awan, S. Shamai, and L. Vandendorpe, "Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1760–1774, Nov 2013.

[17] Z. Wang, M. Xiao, and M. Skoglund, "Secrecy degrees of freedom of the $2\times2\times2$ interference channel with delayed CSIT," *IEEE Wireless Communications Letters*, vol. 3, no. 4, pp. 341–344, Aug 2014.

[18] M. Seif, R. Tandon, and M. Li, "On the secure degrees of freedom of the K-user interference channel with delayed CSIT," in *Proc. ISIT*, June 2018, pp. 201–205.