Secure MIMO Interference Channel with Confidential Messages and Delayed CSIT

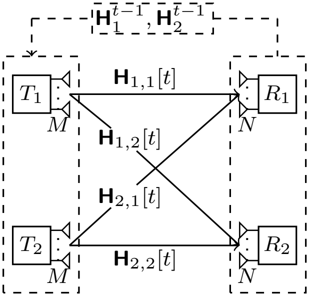
Zhang Tong, Prof. P.C. Ching
Department of Electronic Engineering
The Chinese University of Hong Kong

ICASSP 2019, Brighton UK
May 16, 2019

Outline

Outline

MIMO Interference Channel with Delayed Channel State Information at Transmitter (CSIT)



- Each transmitter has M antennas and each receiver has N antennas.
- The CSI matrices from the transmitter $i, i = 1, 2$ to the receiver $j, j = 1, 2$ at time slot t is denoted by $\mathbf{H}_{i,j}[t]$.
- The collection of delayed CSI matrices, i.e., $\mathbf{H}_{i,j}^{t-1}, i, j = 1, 2$, is fed back to all transmitters at time slot t.

Secure Degrees-of-Freedom (SDoF)

- Transmitter 1 sends confidential message W_1 to receiver 1 without information leakage to receiver 2.
- Transmitter 2 sends confidential message W_2 to receiver 2 without information leakage to receiver 1.
- SDoF is a first-order approximation of secure channel capacity.
- Mathematically, the sum-SDoF is defined as follows:

$$\text{Sum-SDoF} = \sup \lim_{n \to \infty} \frac{\log |W_1| + \log |W_2|}{n \log(\text{SNR})} \tag{1}$$

  where n denotes the number of channel uses.
- Physically, the sum-SDoF represents the maximal number of secure independent channels that a network can support.

Outline

Related Works & The Problem

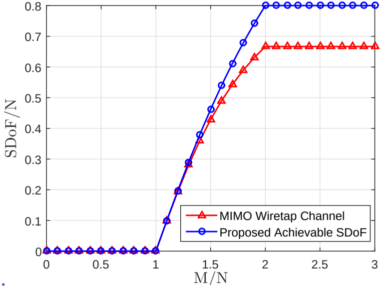
- **With perfect CSIT**, sum-SDoF of MIMO interference channel has been obtained by [Banawan and Ulukus, 2015, Banawan and Ulukus, 2019].
- **With delayed CSIT**
  - SDoF region of two-user MIMO broadcast channel [Yang et al., 2013].
  - SDoF region of K-user MISO broadcast channel [Yang and Kobayashi, 2015].
  - Sum-SDoF of multi-user wiretap channel [Awan et al., 2016, Tandon et al., 2014, Yang and Kobayashi, 2015]
  - Sum-SDoF of $2 \times 2 \times 2$ SISO interference channel [Wang et al., 2014]
- **Problem**: For MIMO interference channel with delayed CSIT, the sum-SDoF has not been thoroughly studied.

Contributions

- For the first time, an achievable sum-SDoF was derived in this paper, which is a lower bound of sum-SDoF and given by

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

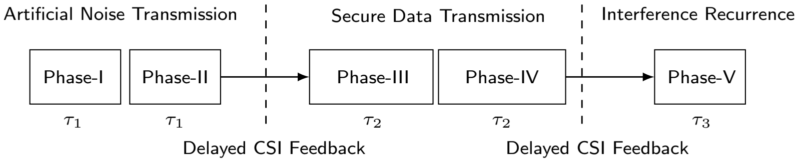
- The proposed achievable sum-SDoF can be 20% greater than that of MIMO wiretap channel with delayed CSIT.



Outline

Sketch of The Proposed Design

- If $M \leq N$, we claim that the achievable sum-SDoF is 0. Because, the artificial noise sent by the single transmitter can be immediately decoded, thus the security cannot be guaranteed.
- If $N < M$, we then design a multi-phase transmission scheme, which will be introduced later on. The sketch is given by



Proposed Scheme for $N < M$ Case

- **Definition 1**: We define the effective CSI matrices from Phase-I to Phase-V as follows:

$$\underline{\mathbf{H}}^{\mathsf{I}}_{i,j} \triangleq \text{blkdiag}\{\mathbf{H}^{\mathsf{I}}_{i,j}(1), \cdots, \mathbf{H}^{\mathsf{I}}_{i,j}(\tau_1)\}$$
$$\underline{\mathbf{H}}^{\mathsf{II}}_{i,j} \triangleq \text{blkdiag}\{\mathbf{H}^{\mathsf{II}}_{i,j}(\tau_1+1), \cdots, \mathbf{H}^{\mathsf{II}}_{i,j}(2\tau_1)\}$$
$$\underline{\mathbf{H}}^{\mathsf{III}}_{i,j} \triangleq \text{blkdiag}\{\mathbf{H}^{\mathsf{III}}_{i,j}(2\tau_1+1), \cdots, \mathbf{H}^{\mathsf{III}}_{i,j}(2\tau_1+\tau_2)\}$$
$$\underline{\mathbf{H}}^{\mathsf{IV}}_{i,j} \triangleq \text{blkdiag}\{\mathbf{H}^{\mathsf{IV}}_{i,j}(2\tau_1+\tau_2+1), \cdots, \mathbf{H}^{\mathsf{IV}}_{i,j}(2\tau_1+2\tau_2)\}$$
$$\underline{\mathbf{H}}^{\mathsf{V}}_{i,j} \triangleq \text{blkdiag}\{\mathbf{H}^{\mathsf{V}}_{i,j}(2\tau_1+2\tau_2+1), \cdots, \mathbf{H}^{\mathsf{V}}_{i,j}(2\tau_1+2\tau_2+\tau_3)\}$$

  where $i, j = 1, 2$.
- **Definition 2**: We also set the full-rank randomized matrices, which are pre-stored at all transmitters and receivers, as follows:

$$\mathbf{\Phi}_1 \in \mathbb{C}^{\min\{M,2N\}\tau_2 \times N\tau_1}, \qquad \mathbf{\Phi}_2 \in \mathbb{C}^{\min\{M,2N\}\tau_2 \times N\tau_1}$$
$$\mathbf{B}_1 \in \mathbb{C}^{N\tau_3 \times N\tau_2}, \qquad \mathbf{B}_2 \in \mathbb{C}^{N\tau_3 \times N\tau_2}$$

Proposed Scheme for $N < M$ Case

- *Phase-I (Artificial Noise Transmission from Transmitter 1)*: Transmitter 1 sends artificial noise $\mathbf{u}_1 \in \mathbb{C}^{\min\{M,2N\}\tau_1}$, while transmitter 2 keeps silent. The received signals are given by

$$\mathbf{y}_1^{\mathsf{I}} = \underline{\mathbf{H}}_{1,1}^{\mathsf{I}} \mathbf{u}_1 \quad (3a)$$

$$\mathbf{y}_2^{\mathsf{I}} = \underline{\mathbf{H}}_{1,2}^{\mathsf{I}} \mathbf{u}_1 \quad (3b)$$

- *Phase-I (Artificial Noise Transmission from Transmitter 2)*: Transmitter 2 sends artificial noise $\mathbf{u}_2 \in \mathbb{C}^{\min\{M,2N\}\tau_2}$, while transmitter 1 keeps silent. The received signals are given by

$$\mathbf{y}_1^{\mathsf{II}} = \underline{\mathbf{H}}_{1,1}^{\mathsf{II}} \mathbf{u}_2 \quad (4a)$$

$$\mathbf{y}_2^{\mathsf{II}} = \underline{\mathbf{H}}_{1,2}^{\mathsf{II}} \mathbf{u}_2 \quad (4b)$$

Proposed Scheme for $N < M$ Case

- *Phase-III (Secure Data Transmission for Receiver 1)*:
  The secure transmit signal at transmitter 1 is designed as follows:

$$\mathbf{x}_1^{\mathsf{III}} = \mathbf{s}_1 + \mathbf{\Phi}_1 \mathbf{y}_1^{\mathsf{I}} \in \mathbb{C}^{\min\{M,2N\}\tau_2} \tag{5}$$

  At the same time, transmitter 2 keeps silent. The received signals:

$$\mathbf{y}_1^{\mathsf{III}} = \underline{\mathbf{H}}_{1,1}^{\mathsf{III}} \left(\mathbf{s}_1 + \mathbf{\Phi}_1 \mathbf{y}_1^{\mathsf{I}}\right) \tag{6a}$$

$$\mathbf{y}_2^{\mathsf{III}} = \underline{\mathbf{H}}_{1,2}^{\mathsf{III}} \left(\mathbf{s}_1 + \mathbf{\Phi}_1 \mathbf{y}_1^{\mathsf{I}}\right) \tag{6b}$$

- *Phase-IV (Secure Data Transmission for Receiver 2)*:
  The secure transmit signal at transmitter 2 is designed as follows:

$$\mathbf{x}_2^{\mathsf{IV}} = \mathbf{s}_2 + \mathbf{\Phi}_2 \mathbf{y}_2^{\mathsf{II}} \in \mathbb{C}^{\min\{M,2N\}\tau_3} \tag{7}$$

  At the same time, transmitter 1 keeps silent. The received signals:

$$\mathbf{y}_1^{\mathsf{IV}} = \underline{\mathbf{H}}_{1,1}^{\mathsf{IV}} \left(\mathbf{s}_2 + \mathbf{\Phi}_2 \mathbf{y}_2^{\mathsf{II}}\right) \tag{8a}$$

$$\mathbf{y}_2^{\mathsf{IV}} = \underline{\mathbf{H}}_{1,2}^{\mathsf{IV}} \left(\mathbf{s}_2 + \mathbf{\Phi}_2 \mathbf{y}_2^{\mathsf{II}}\right) \tag{8b}$$

Proposed Scheme for $N < M$ Case

- *Phase-V (Interference Recurrence for Equation Switching)*: The transmit signals are designed to facilitate the switch of equations in Phases-III and Phase-IV, which are given by

$$\mathbf{x}_1^{\mathsf{V}} = \mathbf{B}_1 \mathbf{y}_2^{\mathsf{III}} \tag{9a}$$

$$\mathbf{x}_2^{\mathsf{V}} = \mathbf{B}_2 \mathbf{y}_1^{\mathsf{IV}} \tag{9b}$$

  Therefore, the received signals are given by

$$\mathbf{y}_1^{\mathsf{V}} = \underline{\mathbf{H}}_{1,1}^{\mathsf{V}} \mathbf{B}_1 \mathbf{y}_2^{\mathsf{III}} + \underline{\mathbf{H}}_{2,1}^{\mathsf{V}} \mathbf{B}_2 \mathbf{y}_1^{\mathsf{IV}} \tag{10a}$$

$$\mathbf{y}_2^{\mathsf{V}} = \underline{\mathbf{H}}_{1,2}^{\mathsf{V}} \mathbf{B}_1 \mathbf{y}_2^{\mathsf{III}} + \underline{\mathbf{H}}_{2,2}^{\mathsf{V}} \mathbf{B}_2 \mathbf{y}_1^{\mathsf{IV}} \tag{10b}$$

- **Decoding Condition**: To ensure all transmitted symbols can be decoded, τ_2 and τ_3 should satisfy

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

- **Security Condition**: To ensure zero information leakage to the other receiver, τ_1 and τ_2 should satisfy

$$N(\tau_1 + \tau_2) = \min\{M, 2N\}\tau_1 \tag{C2}$$

Analysis of Decoding and Security Conditions

- For the decoding condition $(C1)$, it can be re-written w.r.t. τ_3/τ_2 as follows:

Table: Re-writing of Decoding Condition $(C1)$

$N < M < 2N$	$M \geq 2N$
$\tau_3/\tau_2 = (M-N)/N$	$\tau_3/\tau_2 = 1$

- For the security condition $(C2)$, it can be re-written w.r.t. τ_2/τ_1 as follows:

Table: Re-writing of Security Condition $(C2)$

$N < M < 2N$	$M \geq 2N$
$\tau_2/\tau_1 = (M-N)/N$	$\tau_2/\tau_1 = 1$

- We can see that both τ_3/τ_2 and τ_2/τ_1 are not more than 1.

Proposed Scheme for $N < M$ Case

- **Proposed Achievable Sum-SDoF Maximization Problem**:

$$\max_{\tau_1,\tau_2,\tau_3 \in \mathbb{Z}_+} \quad \frac{2\min\{M,2N\}\tau_2}{2\tau_1 + 2\tau_2 + \tau_3} \qquad \text{s.t.} \quad \text{C1, C2} \tag{11}$$

  Problem re-formulation:

$$\max_{\tau_1/\tau_2,\ \tau_3/\tau_2} \quad \frac{2\min\{M,2N\}}{2\tau_1/\tau_2 + 2 + \tau_3/\tau_2} \qquad \text{s.t.} \quad f_1(\tau_1/\tau_2) = 0, f_2(\tau_3/\tau_2) = 0 \tag{12}$$

  where C1 $\Longleftrightarrow f_1(\tau_1/\tau_2) = 0,$ C2 $\Longleftrightarrow f_2(\tau_3/\tau_2) = 0.$

- **Optimal Solution**: Re-writing condition (C1) and condition (C2) yields the optimal solutions. For example, we can select

$$\begin{cases} \tau_1^* = N^2 \\ \tau_2^* = \min\{M-N, N\}N \\ \tau_3^* = (\min\{M-N, N\})^2 \end{cases} \tag{13}$$

Outline

Conclusion & Future Work

- **Conclusion**: An achievable sum-SDoF for secure MIMO interference channel with confidential messages and delayed CSIT was proposed in this paper. This is the first attempt to the best of our knowledge.
- **Future Work**: To figure out the exact sum-SDoF, an upper bound is needed, which motivates future work.

Outline

Preliminary

Related Works & Contributions

The Proposed Scheme

Conclusion & Future Work

References

References I

Z. H. Awan, A. Zaidi, and A. Sezgin, “On SDoF of multi-receiver wiretap channel with alternating CSIT,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1780–1795, Aug 2016.

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

K. Banawan and S. Ulukus, “Secure degrees of freedom region of static and time-varying gaussian MIMO interference channel,” *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 444–461, Jan 2019.

R. Tandon, P. Piantanida, and S. Shamai, “On multi-user MISO wiretap channels with delayed CSIT,” in *2014 IEEE International Symposium on Information Theory*, June 2014, pp. 211–215.

References II

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

S. Yang and M. Kobayashi, "Secure communication in K-user multi-antenna broadcast channel with state feedback," in *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015, pp. 1976–1980.

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.