ARC '16

مؤتمر مؤسسة قطر
السنوي للبحوث

QATAR FOUNDATION
ANNUAL RESEARCH
CONFERENCE

Towards World-class
Research and Innovation

Information Communications Technology Pillar

http://dx.doi.org/10.5339/qfarc.2016.ICTSP2944

The Secure Degrees of Freedom of the MIMO BC and MIMO MAC with Multiple Unknown Eavesdroppers

Mohamed Khalil, Tamer Khattab, Tarek Elfouly, Amr Mohamed

Qatar University, QA

Email: mohamed.amir@qu.edu.qa

We investigate the secure degrees of freedom (SDoF) of a two-transmitter Gaussian multiple access channel with multiple antennas at the transmitters, a legitimate receiver and an unknown number of eavesdroppers each with a number of antennas less than or equal to a known value NE. The channel matrices between the legitimate transmitters and the receiver are available everywhere, while the legitimate pair have no information about the fading eavesdroppers' channels. We provide the exact sum SDoF for the considered system. We show that it is equal to min(M_1+M_2–NE, 1/2(max(M_1;N_2+max(M_2;N)–NE,N). A new comprehensive upperbound is deduced and a new achievable scheme based on utilizing jamming is exploited. We prove that Cooperative Jamming is SDoF optimal even without the eavesdropper CSI available at the transmitters.

I. Introduction

The noisy wiretap channel was first studied by Wyner [1], in which a legitimate transmitter (Alice) wishes to send a message to a legitimate receiver (Bob), and hide it from an eavesdropper (Eve). Wyner proved that Alice can send positive secure rate using channel coding. He derived capacityequivocation region for the degraded wiretap channel. A significant amount of work was carried thereafter to study the information theoretic physical layer security for different network models. The secure degrees of freedom (SDoF) region of multiple access channel (MAC) was presented in [2]. The SDoF is the the pre-log of the secrecy capacity region in the high-SNR regime. All the aforementioned work assumes availability of either partial or complete channel state information (CSI) at the transmitter. Given that the eavesdropper is passive, it is of high importance to study the case where the channel state information is completely unknown to the legitimate users. In this paper, we study the MIMO BC and MIMO MAC with unknown eavesdroppers' CSI at the legitimate transmitters and receiver. We provide a new upperbound for the achievable SDoF and determine the exact sum SDoF by providing an achievable scheme. We show that our scheme is

Cite this article as: Khalil M, Khattab T, Elfouly T, Mohamed A. (2016). The Secure Degrees of Freedom of the MIMO BC and MIMO MAC with Multiple Unknown Eavesdroppers. Qatar Foundation Annual Research Conference Proceedings 2016: ICTSP2944 http://dx.doi.org/10.5339/qfarc.2016.ICTSP2944.

optimal and that the achievable bounds and the new upperbounds are tight. For the case of known eavesdropper channels with constant or time varying channels, we show that it has the same sum SDoF as the previous case, closing an open problem since the best known achievable region was presented in [3]. We use the following notation, a for vectors, A for matrices, Ay for the This research was made possible by NPRP 5-559-2-227 grant from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors. hermitian transpose of A, [A]+ for the max A; 0 and Null(A) to define the nullspace of A.

II. System model

We consider two communication systems, the broadcast channel with a single transmitter and two receivers, and the MAC channel with two transmitters and a single receiver in vicinity of an unknown number of passive eavesdroppers. Transmitter *i* is equipped with M_i. The legitimate receiver *j* is equipped with N_j antennas, while the *l* th eavesdropper is equipped with $N_{El} \leq N_E$ antennas. Let $\vec{x}_i$ denote the $M_i \times 1$ vector of symbols to be transmitted by transmitter *i*, where $i \in \{1,2\}$. We can write the received signal at the legitimate receiver *j* at time (sample) *k* as

$$\vec{Y}_j(k) = \sum_{i=1}^{2} \vec{H}_i \vec{V}_i \vec{x}_i(k) + \vec{n}(k)$$

and the received signal at the *l* th eavesdropper as

$$\vec{Z}_l(k) = \sum_{i=1}^{2} \vec{G}_{i,l}(k) \vec{V}_i \vec{x}_i(k) + \vec{n}_{El}(k),$$

where $\vec{H}_i$ and $\vec{G}_{i,l}(k)$ are the matrices containing the i.i.d time varying channel coefficients drawn from a continuous distribution with mean η and variance σ_e^2, $\vec{V}_i$ is the precoding unitary matrix. $\vec{n}(k)$ and $\vec{n}_{Ej}(k)$ are the $N \times 1$ and the $N_{Ej} \times 1$ additive white Gaussian noise vectors with zero mean and variance σ^2 at the legitimate receiver and the *j*th eavesdropper, respectively. We assume that the transmitters know the maximum number of antennas any eavesdropper can possess; namely, N_E, but they do not know any of the eavesdroppers' channels. We assume that $N_E < M,N$, where $M = M_1 + M_2$ and $N = N_1 + N_2$.

Each transmitter *i* intends to send a message W_i over *n* channel uses (samples) to the legitimate receiver simultaneously while preventing the eavesdroppers from decoding its message. The encoding occurs under a constrained power given by

$$E\{\vec{X}_i \vec{X}_i\} \leq P \text{ for all } i = \{1,2\}$$

At each transmitter, the message W_i is uniformly and independently chosen from a set of possible secret messages for transmitter *i*, $W_i = \{1,2,\ldots,2^{nR_i}\}$. The rate for message W_i is $R_i \triangleq \frac{1}{n}\log|W_i|$, where $|\cdot|$ denotes the cardinality of the set. Transmitter *i* uses a stochastic encoding function $f_i : W_i \rightarrow \vec{X}_i^n$ to map the secret message into a transmitted symbol. The receiver has a decoding function $\phi : \vec{Y}^n \rightarrow (\hat{W}_1, \hat{W}_2)$, where $\hat{W}_i$ is an estimate of W_i. A secure rate tuple (R_1,R_2) is said to be achievable if for any $\in$>0 there exist *n*-length codes such that the legitimate receiver can decode the messages reliably, i.e.,

$$Pr\{(W_1,W_2) \neq (\hat{W}_1,\hat{W}_2)\} \leq \epsilon$$

and the messages are kept information-theoretically secure against the eavesdroppers, i.e.,

$$\lim_{n\to\infty} \frac{1}{n} H(W_1,W_2 \mid \vec{Z}_j^n) \geq \lim_{n\to\infty} \frac{1}{n} H(W_1,W_2) - \epsilon$$

where $H(\cdot)$ is the Entropy function.

The sum SDoF is defined as

$$D_s = \lim_{P\to\infty} \sup \sum_i \frac{R_i}{\frac{1}{2}\log P}$$

where the supremum is over all achievable secrecy rate tuples (R_1,R_2), $D_s = d_1 + d_2$ and d_1 and d_2 are the secure DoF of transmitters one and two, respectively.

III. Main results

The SDoF of the two user BC channel is,

$$D_s^{BC} \leq \min(N_1 + N_2, M - N_E)$$

The sum SDoF of the two user MAC channel is

$$D_s^{MAC} \leq \min\&\left(N, M_1 + M_2 - N_E, \frac{1}{2}(\max(M_1, N) + \max(M_2, N) - N_E)\right)$$

IV. Converse

The sum SDoF of the two user BC channel is upperbounded as,

$$D_s^{BC} \& \leq \min(N_1 + N_2, M - N_E)$$

The first bound is the due to the limited number of antennas at the receiver, given that the receiver has only $N_1 + N_2$ antennas.

The second bound represent the DoF loss caused by the number of eavesdroppers' antennas on the transmitter side.

The number of SDoF of the two user MAC channel is upperbound as,

$$D_s^{Mac} \leq \min\&\left(N, M_1 + M_2 - N_E, \frac{1}{2}(\max(M_1, N) + \max(M_2, N) - N_E)\right)$$

The first bound is the due to the limited number of antennas at the receiver, given that the receiver has only N antennas. The second bound represent the DoF loss caused by the number of eavesdroppers' antennas on the transmitter side. The third bound represents the DoF loss of each transmitter due to the number of eavesdroppers antennas available. Full version of the converse can be found at [4], [5].

V. Achievable scheme

For securing the legitimate messages, the transmitters uses a two-step noise injection by simultaneously sending a jamming signal and using a stochastic encoder as follows,

1) The transmitter sends a jamming signal with power $P^J = \alpha P$ that guarantees that all eavesdropper have a constant rate ($o(logP)$) for all legitimate signal power values.
2) A stochastic encoder is built using random binning. The encoder randomness is designed to be larger that any of the eavesdroppers leakage, hence all eavesdroppers would have zero rate when the code length goes to infinity which meet the secrecy constraints.

The jamming signal transmitted is a N_E vector $\vec{r} = [\vec{r}_1 \vec{r}_2]^T$ with random symbols using $\vec{V}_1^J$ and $\vec{V}_2^J$ as jamming precoders[1]. Hence, the transmitted coded signal can be broken into legitimate signal, $\vec{s}_i$, and jamming signal, $\vec{r}_i$, such that

$$\vec{x}_i = \begin{bmatrix} \vec{s}_i \\ \vec{r}_i \end{bmatrix}, i \in \{1,2\}.$$

Accordingly, the precoder, $\vec{V}_i$ can be also broken into legitimate precoder, $\vec{V}_i^L$, and jamming precoder, $\vec{V}_i^J$ such that

$$\vec{V}_i = \begin{bmatrix} \vec{V}_i^L & \vec{V}_i^J \end{bmatrix} i \in \{1,2\}.$$

The transmitter/s align/s the jamming in a minimal space at receiver/s by using the legitimate channels null space and jamming alignment using the precoder $\vec{V}_i^J$. Then use/s the free space for the legitimate signal to achieve the upperbound using the precoder $\vec{V}_i^L$. Full version of the scheme can be found at [4],[5].

[1] For the special case $N_E = 1$, only one user sends a single jamming symbol.

Conclusion

We studied the two user broadcast and multiple access wiretap channel with multiple antennas at the transmitters, legitimate receivers and eavesdroppers. Generalizing new upperbound was established and a new achievable scheme was provided. We used the new optimal scheme to derive the sum secure DoF of the channel. We showed that the our scheme meets the upperbound or all M_1,M_2,N_E combinations. We showed that Cooperative Jamming is SDoF optimal even without the eavesdropper CSI available at the transmitters.

References

[1] A. D. Wyner. The wiretap channel. Bell systems technical journal, vol. 8, Oct. 1975.

[2] Jianwei Xie and Sennur Ulukus Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming The Annual Conference on Information Sciences and Systems (CISS), March 2013.

[3] Ghadamali Bagherikaram, Abolfazl S. Motahari, Amir K. Khandani On the Secure Degrees-of-Freedom of the Multiple-Access-Channel IEEE Transaction Information Theory, submitted March 2010. Also available at [arXiv:1003.0729]

[4] M. Amir, T. Khattab, T. Elfouly, and A. Mohamed Secrecy for MIMO Wiretap and MIMO Broadcast Channels with fading Eavesdroppers: CSI does not increase the Secure DoF, IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Aug. 2015.

[5] M. Amir, T. Khattab, T. Elfouly, and A. Mohamed The secrecy degrees of freedom of MIMO Multiple access channel with unknown eavesdroppers, Arxiv:1404.5007.