Forty-Ninth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 28 - 30, 2011

# MIMO Multiple Access Channel with an Arbitrarily Varying Eavesdropper

Xiang He[‡] , Ashish Khisti[*], Aylin Yener[†]

[*]Dept. of Electrical and Computer Engineering, University of Toronto, Toronto, ON, M5S 3G4, Canada
[†] Electrical Engineering Department, The Pennsylvania State University, University Park, PA 16802
*hexiang@ieee.org, akhisti@comm.utoronto.ca, yener@psu.edu*

***Abstract*—We investigate a two-transmitter Gaussian multiple access wiretap channel with multiple antennas at each of the nodes. The channel transfer matrices at the legitimate terminals are fixed and revealed to all the terminals, whereas the channel transfer matrix of the eavesdropper is arbitrarily varying and only revealed to the eavesdropper. We characterize the secrecy degrees of freedom (s.d.o.f.) region under a strong secrecy constraint. A transmission scheme that orthogonalizes the transmit signals of the two users at the intended receiver and uses a single-user wiretap code is sufficient to achieve the s.d.o.f. region. The converse involves establishing an upper bound on a *weighted-sum-rate* expression. This is accomplished by using an induction procedure, where at each step we combine the secrecy and multiple-access constraints associated with an adversary eavesdropping a carefully selected group of sub-channels.**

## I. Introduction

While prevalent architectures for secure communication are primarily based on cryptographic techniques [1], they cannot address all the vulnerabilities in complex networked systems. The area of physical layer security [2]–[4] investigates security solutions using resources at the physical layer and compliments existing cryptographic techniques. Furthermore the associated techniques do not rely on a computationally bounded adversarial model, but instead provide a rigorous theoretical proof of security [5] making such techniques appealing in certain mission-critical application.

Secure communication using multiple antennas has been extensively studied in recent times, see e.g., [6]–[14]. These works investigate efficient signaling mechanisms using the spatial degrees of freedom provided by multiple antennas to limit an eavesdropper's ability to decode information. The underlying information theoretic problem, the multi-antenna wiretap channel, is studied and the associated secrecy capacity is investigated. We note that these works assume that the eavesdropper's channel state information is available either completely or partially, although such an assumption cannot be justified in practice.

More recently, [15]–[17] study secrecy capacity when the eavesdropper channel is arbitrarily varying and its channel states are known to the eavesdropper only. Reference [16] studies the single-user Gaussian multi-input-multi-output (MIMO) wiretap channel and characterizes the secrecy degrees of freedom (s.d.o.f.). The two user Gaussian MIMO multiple access (MIMO-MAC) channel is also investigated in [16] for the special case when all the legitimate terminals have equal number of antennas. A time-sharing based technique is shown to be sufficient in achieving the s.d.o.f. region. As we develop in this paper, the case of unequal number of antennas requires a non-trivial extension of [16].

Our main contribution is to characterize the s.d.o.f. region of the two-transmitter MIMO MAC channel when the eavesdropper channel is arbitrarily varying. The s.d.o.f. region can be achieved by a scheme that orthogonalizes the transmit signals of the two users at the intended receiver. Moreover, it suffices to use a single-user wiretap channel code [16] and no cooperation from the other user is necessary, except in sharing the transmit dimensions. To establish the optimality of this scheme, our converse proof decomposes the MIMO MAC channel into a set of parallel and independent channels using the generalized singular value decomposition (GSVD). A set of eavesdroppers, each monitoring a subset of links, is selected using an induction procedure (Definition 1) and the resulting secrecy constraints are combined to obtain an upper bound on a weighted sum-rate expression. The upper bound matches the achievable rate in terms of the s.d.o.f. region, thus settling the problem raised in [16] for the case of two transmitters.

To the best of our knowledge the s.d.o.f. region remains open when the eavesdropper channel is perfectly known to all terminals. A significant body of literature already exists on this problem. See e.g., [3], [18]–[20]. If the channel model has real inputs and outputs, Gaussian signaling is in general suboptimal and user cooperating strategies as well as signal alignment techniques are necessary [21]. In [22] it is established that s.d.o.f. of $1/2$ is achievable using real interference alignment for almost all configurations of channel gains. If the channel model has complex inputs and outputs, it is shown in [23, Section 5.16] that in general s.d.o.f. of $1/2$ is achievable using asymmetric Gaussian signaling. In contrast, the best known upper bound on the s.d.o.f. of individual rates is $2/3$ for both cases, established in [23, Section 5.5].

The remainder of this paper is organized as follows. In Section II, we describe the system model. The main result is stated as Theorem 1 in Section IV. Due to page limit, we shall only prove the converse of Theorem 1 for the case of parallel channels, which is given in Section V. The general case can be easily reduced to this case through general singular value

‡ The ordering of authors is alphabetical.

978-1-4577-1818-2/11/$26.00 ©2011 IEEE 

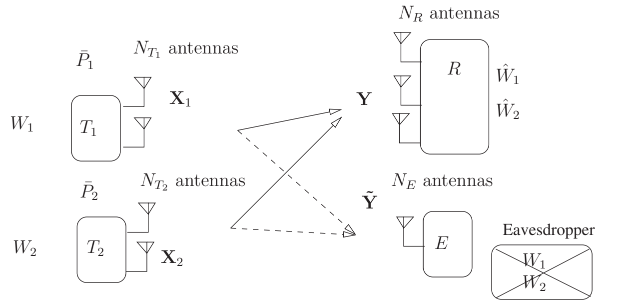


Fig. 1. The MIMO MAC wiretap channel where $N_{T_1} = N_{T_2} = 2$, $N_R = 3$, $N_E = 1$.

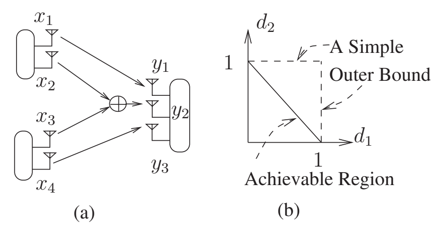


Fig. 2. (a) A special case of MIMO MAC wiretap channel where $N_{T_1} = N_{T_2} = 2$, $N_R = 3$, $N_E = 1$, (b) Comparison between achievable s.d.o.f. region and a simple outer bound derived by considering one eavesdropper at a time.

decomposition [24] and its proof will be given in the journal version of this work.

We use the following notation throughout the paper: For a set $\mathcal{A}$, $V_{i,\mathcal{A}}$ and $V_{\mathcal{A}}$ denote the set of random variables $\{V_{i,j}, j \in \mathcal{A}\}$ and $\{V_j, j \in \mathcal{A}\}$ respectively. $\{\delta_n\}$ denotes a non-negative sequence of $n$ that converges to 0 when $n$ goes to $\infty$. We use bold upper-case font for matrices and vectors and lower-case font for scalars. The distinction between matrices and vectors will be clear from the context. For a set $\mathcal{A}$, $|\mathcal{A}|$ denotes its cardinality and a short hand notation $x^n$ is used for the sequence $\{x_1, x_2, \ldots, x_n\}$. $\phi$ denotes the empty set.

## II. System Model

As shown in Figure 1, we consider a discrete-time channel model where two transmitters communicate with one receiver in the presence of an eavesdropper. We assume transmitter $i$ has $N_{T_i}$ antennas, $i = 1, 2$, the legitimate receiver has $N_R$ antennas whereas the eavesdropper has $N_E$ antennas. The channel model is defined by

$$\mathbf{Y}(i) = \sum_{k=1}^{2} \mathbf{H}_k \mathbf{X}_k(i) + \mathbf{Z}(i) \tag{1}$$

$$\tilde{\mathbf{Y}}(i) = \sum_{k=1}^{2} \tilde{\mathbf{H}}_k(i) \mathbf{X}_k(i) \tag{2}$$

where $i \in \{1, \ldots, n\}$ denotes the time-index, $\mathbf{H}_k, k = 1, 2$, are channel matrices and $\mathbf{Z}$ is the additive Gaussian noise observed by the intended receiver, which is composed of independent rotationally invariant complex Gaussian random variables with zero mean and unit variance. The sequence of eavesdropper channel matrices $\{\tilde{\mathbf{H}}_k(i), k = 1, 2\}$, is an arbitrary sequence of length $n$ and only revealed to the eavesdropper. In contrast, $\mathbf{H}_k, k = 1, 2$ are revealed to both the legitimate parties *and* the eavesdropper(s). We assume $N_E$, the number of eavesdropper antennas, is known to the legitimate parties and the eavesdropper.

User $k$, $k = 1, 2$, wishes to transmit a confidential message $W_k$, $k = 1, 2$, to the receiver over $n$ channel uses, while both messages, $W_1$ and $W_2$, must be kept confidential from the eavesdropper. We use $\gamma$ to index a specific sequence of $\{\tilde{\mathbf{H}}_k(i), k = 1, 2\}$ over $n$ channel uses and use $\tilde{\mathbf{Y}}_\gamma^n$ to represent the corresponding channel outputs for $\tilde{\mathbf{Y}}^n$. The secrecy constraint is [16]:

$$\lim_{n \to \infty} I\left(W_1, W_2; \tilde{\mathbf{Y}}_\gamma^n\right) = 0, \quad \forall \gamma \tag{3}$$

where the convergence must be uniform over $\gamma$. The average power constraints for the two users are given by

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} |\mathbf{X}_k(i)|^2 \leq \bar{P}_k, \quad k = 1, 2. \tag{4}$$

The secrecy rate for user $k$, $R_{s,k}$, is defined as

$$R_{s,k} = \lim_{n \to \infty} \frac{1}{n} H(W_k), \quad k = 1, 2. \tag{5}$$

such that $W_k$ can be reliably decoded by the receiver, and (3) and (4) are satisfied.

We define the secrecy degrees of freedom as:

$$\left\{(d_1, d_2) : d_k = \limsup_{\bar{P}_1 = \bar{P}_2 = \bar{P} \to \infty} \frac{R_{s,k}}{\log_2 \bar{P}}, \quad k = 1, 2\right\} \tag{6}$$

## III. Motivation

Before stating the main result, we illustrate the main difficulty in characterizing the s.d.o.f. region through a simple example. As illustrated in Figure 2(a), each transmitter has 2 antennas and the intended receiver has 3 antennas. We assume the eavesdropper only has 1 antenna. Let $x_1, x_2, x_3, x_4$ denote the transmitted signals from the two users and $y_1, y_2, y_3$ denote the signals observed by the intended the receiver. And the main channel is given by

$$y_1 = x_1 + z_1, \quad y_3 = x_4 + z_3 \tag{7}$$

$$y_2 = x_2 + x_3 + z_2 \tag{8}$$

where $z_i, i = 1, 2, 3$ denote additive channel noise. As shown in [16], a secrecy degree of freedom $\min(N_{T_k}, N_R) - N_E = 1$ is achievable for a user if the other user remains silent. Time sharing between these two users lead to the following achievable s.d.o.f. region:

$$d_1 + d_2 \leq 1, \quad d_k \geq 0, \quad k = 1, 2 \tag{9}$$

For the converse, we begin by considering a simple upper bound, which reduces each channel to a single-user MIMO wiretap channel. First, by revealing the signals transmitted by user 2 to the intended receiver and assuming that the eavesdropper monitors either $x_1$ or $x_2$ we have that $d_1 \leq 1$.

Similarly we argue that $d_2 \leq 1$. To obtain an upper bound on the sum-rate we let the two transmitters to cooperate and reduce the system to a $3 \times 3$ MIMO link. The s.d.o.f. of this channel [16] yields $d_1 + d_2 \leq 2$. This outer bound, illustrated in Figure 2(b), does not match with the achievable region given by (9).

As we shall show in Theorem 1, (9) is indeed the s.d.o.f. capacity region and hence a new converse is necessary to prove this result. Our key observation is that the above upper bound only considers one eavesdropper at a time in deriving each of the three bounds. For example, when deriving $d_1 \leq 1$, we assume there is only one eavesdropper which is monitoring either $x_1$ or $x_2$. When deriving $d_2 \leq 1$, we assume there is only one eavesdropper which is monitoring either $x_3$ or $x_4$. Similarly when deriving $d_1 + d_2 \leq 2$ we again assume that there is one eavesdropper on either of the links. As we shall discuss below, a tighter upper bound is possible if we consider the simultaneous effect of two eavesdroppers.

In our system model, there are infinitely many possible eavesdroppers, each corresponding to a different channel state sequence. The main difficulty is to find out a finite number of eavesdroppers, whose joint effect leads to a tight converse. Our choice of eavesdroppers is based on the following intuition: When an eavesdropper chooses which links to monitor, it should give precedence to those links over which only one user can transmit. This is because these links are the major contributor to the sum s.d.o.f. $d_1 + d_2$ since they are dedicated links to a certain user. Based on this intuition, we consider the following two eavesdroppers: one monitor $y_1$ for $W_1$ and the other monitors $y_3$ for $W_2$. As we shall show later in Lemma 1, the first eavesdropper implies the following upper bound on $R_1$:

$$n(R_1 - \delta_n) \leq I\left(x_2^n; y_2^n | y_1^n, x_{\{3,4\}}^n\right) \tag{10}$$

and the second eavesdropper implies the following upper bound on $R_2$:

$$n(R_2 - \delta_n) \leq I\left(y_1^n, x_{\{3,4\}}^n; y_2^n\right) \tag{11}$$

Their joint effect can be captured by adding (10) and (11) [25], which lead to:

$$n(R_1 + R_2 - 2\delta_n) \leq I\left(x_2^n, y_1^n, x_{\{3,4\}}^n; y_2^n\right) \tag{12}$$

Since there is only one term, which is $y_2^n$, at the right side of the mutual information $I\left(x_2^n, y_1^n, x_{\{3,4\}}^n; y_2^n\right)$, we observe the sum s.d.o.f. can not exceed 1, thereby justifying that (9) is indeed the largest possible s.d.o.f. region for Figure 2(a).

The above example reveals one key idea behind the converse. As captured by (10) and (11), a simultaneous selection of two different eavesdroppers for the two users reduces the effective signal dimension at the receiver from three to one, thus leading to a tighter converse. As we shall show later in Section V-B, in generalizing this example we are required to systematically select a sequence of eavesdroppers using an induction procedure.

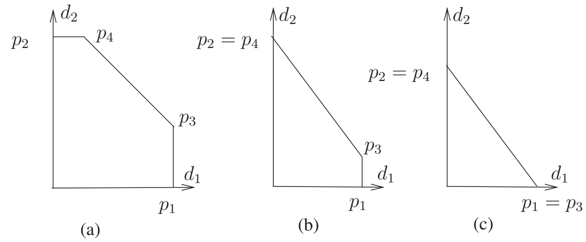


Fig. 3. The secrecy degrees of freedom (s.d.o.f.) region in Theorem 1: (a) $0 \leq N_E \leq \min\{r_0 - r_1, r_0 - r_2\}$, (b) $\min\{r_0 - r_1, r_0 - r_2\} \leq N_E \leq \max\{r_0 - r_1, r_0 - r_2\}$, (c) $\max\{r_0 - r_1, r_0 - r_2\} \leq N_E$

## IV. Main Result

In this section, we state the main result of this work. To express our result, we define $r_t$ as the rank of $\mathbf{H}_t, t = 1, 2$ and $r_0$ as the rank of $[\ \mathbf{H}_1 \mid \mathbf{H}_2\ ]$. We will refer to $r_t$ as the number of transmit dimensions at user $t = 1, 2$ and $r_0$ as the number of dimensions at the receiver.

*Theorem 1:* The secrecy degrees of freedom region of the MIMO multiple access channel with arbitrarily varying eavesdropper channel is given by the convex hull of the following five points of $(d_1, d_2)$:

$$p_0 = (0,0), \quad p_1 = \left([r_1 - N_E]^+, 0\right) \tag{13}$$

$$p_2 = \left(0, [r_2 - N_E]^+\right) \tag{14}$$

$$p_3 = \left([r_1 - N_E]^+, [r_0 - r_1 - N_E]^+\right) \tag{15}$$

$$p_4 = \left([r_0 - r_2 - N_E]^+, [r_2 - N_E]^+\right) \tag{16}$$

where we use $[x]^+ \triangleq \max\{x, 0\}$. □

Fig. 3 illustrates the structure of the s.d.o.f. region as a function of the number of eavesdropping antennas. In Fig. 3 (a) we have $N_E \leq \min(r_0 - r_1, r_0 - r_2)$. In this case the s.d.o.f. region is a polymatroid (see e.g., [26, Definition 3.1]) described by $d_i \leq r_i - N_E$ and $d_1 + d_2 \leq r_0 - 2N_E$. Fig. 3 (b) illustrates the shape of the s.d.o.f. region when $\min\{r_0 - r_1, r_0 - r_2\} \leq N_E \leq \max\{r_0 - r_1, r_0 - r_2\}$. In Fig. 3 (b), without loss of generality, we assume $r_1 < r_2$ and the s.d.o.f. region is bounded by the lines $d_i \geq 0$, $d_1 \leq r_1 - N_E$ and

$$\begin{aligned}(r_1 + r_2 - r_0)d_1 + (r_1 - N_E)d_2 \\ \leq (r_1 - N_E) \times (r_2 - N_E).\end{aligned} \tag{17}$$

When $\min(r_1, r_2) > N_E \geq \max(r_0 - r_1, r_0 - r_2)$, the s.d.o.f. region, as illustrated in Fig. 3 (c) is bounded by $d_i \geq 0$ and the line

$$\frac{d_1}{r_1 - N_E} + \frac{d_2}{r_2 - N_E} \leq 1. \tag{18}$$

The s.d.o.f. region in Theorem 1 allows the following simple interpretation: The region can be expressed as a convex hull of a set of rectangles shown by Figure 4 (illustrated for Figure 3 (a)). Each rectangle is parameterized by the dimensions of the subspace occupied by the transmission signals from the two users, denoted by $(t_1, t_2)$, where $t_i$

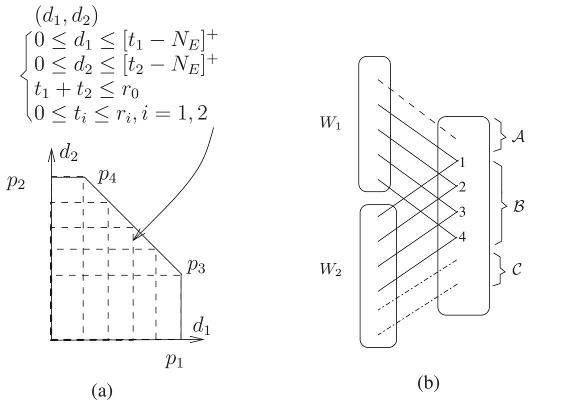


Fig. 4. **(a)** Interpretation of the s.d.o.f. region as a convex hull of rectangles: $(d_1, d_2) : 0 \leq d_i \leq [t_i - N_E]^+, i = 1, 2$, where $t_i$ is the number of degrees of freedom occupied by user $i$. To achieve reliable transmission, we must have (19). **(b)** Definition of the set $\mathcal{A}, \mathcal{B}, \mathcal{C}$, where $|\mathcal{B}| = 4$.

indicates the dimension of user $i$, $i = 1, 2$. Then in order for the signals from both transmitters to be received reliably by the receiver, we must have

$$t_1 + t_2 \leq r_0, \quad 0 \leq t_i \leq r_i, i = 1, 2 \tag{19}$$

Each user then transmits confidential messages with $0 \leq d_i \leq [t_i - N_E]^+$ over the available $t_i$ dimensions, where the $-N_E$ term is an effect of the secrecy constraint (3).

It is clear that $p_3, p_4$ given by (15) and (16) are in one of these rectangles. Hence the convex hull of these rectangles yields the s.d.o.f. region stated in Theorem 1.

*Remark 1:* As evident from the interpretation above, each user sacrifices $N_E$ in degrees of freedom to protect its own message and there is no cooperation between the two users to achieve the optimal s.d.o.f. region. □

## V. Proof for the Parallel Channel Model

In this section we establish Theorem 1 for the case of parallel channels. As illustrated in Fig. 4, the receiver observes

$$y_i = x_{1i} + z_i, \quad i \in \mathcal{A}, \tag{20}$$

$$y_i = x_{1i} + x_{2i} + z_i, \quad i \in \mathcal{B}, \tag{21}$$

$$y_i = x_{2i} + z_i, \quad i \in \mathcal{C}, \tag{22}$$

where the noise random variables across the sub-channels are independent and each is distributed according to $\mathcal{CN}(0, 1)$ and $\{x_{1i}\}_{i \in \mathcal{A} \cup \mathcal{B}}$ and $\{x_{2i}\}_{i \in \mathcal{B} \cup \mathcal{C}}$ denote the transmit symbols of user 1 and user 2 respectively.

The parallel channel model is a special case of (1) with

$$\mathbf{H}_1 = \begin{bmatrix} \mathbf{I}_{|\mathcal{A}|} & & \\ & \mathbf{I}_{|\mathcal{B}|} & \\ & & \mathbf{O}_{|\mathcal{C}|} \end{bmatrix}, \; \mathbf{H}_2 = \begin{bmatrix} \mathbf{O}_{|\mathcal{A}|} & & \\ & \mathbf{I}_{|\mathcal{B}|} & \\ & & \mathbf{I}_{|\mathcal{C}|} \end{bmatrix}, \tag{23}$$

where $\mathbf{I}_{|\mathcal{A}|}$, $\mathbf{I}_{|\mathcal{B}|}$ and $\mathbf{I}_{|\mathcal{C}|}$ denote the identity matrices of size $|\mathcal{A}|$, $|\mathcal{B}|$ and $|\mathcal{C}|$ respectively, and $\mathbf{O}_{|\mathcal{A}|}$ and $\mathbf{O}_{|\mathcal{B}|}$ denote the matrices, all of whose entries are zeros. We note that we do not make any assumption on the eavesdropper's channel model (2).

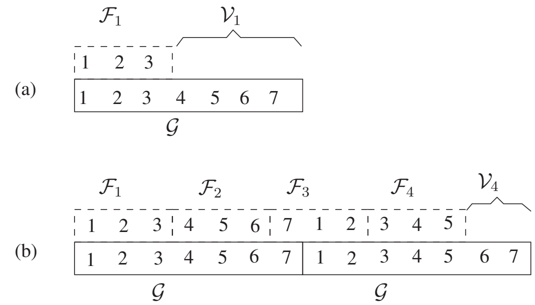


Fig. 5. The set $\mathcal{F}_k$, $\mathcal{G}$, and $\mathcal{V}_k$ when $|\mathcal{F}| = 3$, $|\mathcal{G}| = 7$ and $|\mathcal{B}| = 8$. (a) Case I, $i = 1$, $c_1 = 1$. (b) Case II, $i = 4$, $\mathcal{H}_5 = \{1\}$, $\mathcal{F}_5 = \{6, 7, 1\}$, $\mathcal{V}_5 = \{2, 3, 4, 5, 6, 7\}$, $c_4 = 2$, $c_5 = 3$.

### A. Converse : $N_E \leq \min(|\mathcal{A}|, |\mathcal{C}|)$

We need to show that the s.d.o.f. region is contained within

$$d_1 \leq |\mathcal{A}| + |\mathcal{B}| - N_E \tag{24}$$

$$d_2 \leq |\mathcal{C}| + |\mathcal{B}| - N_E \tag{25}$$

$$d_1 + d_2 \leq |\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}| - 2N_E \tag{26}$$

Since (24) and (25) directly follow from the single user case in [16], we only need to show (26).

Let $\mathcal{E}_k$ be the set of links such that an eavesdropper is monitoring for $W_k$, $k = 1, 2$. $|\mathcal{E}_1| = |\mathcal{E}_2| = N_E$. $\mathcal{A} \supseteq \mathcal{E}_1$, $\mathcal{C} \supseteq \mathcal{E}_2$. We establish the following upper bound on the achievable rate pairs.

*Lemma 1:*

$$n(R_{s,1} - \delta_n) \leq I\left(X^n_{1,\mathcal{A}\setminus\mathcal{E}_1}; Y^n_{\mathcal{A}\setminus\mathcal{E}_1}\right) + I\left(X^n_{1,\mathcal{B}}; Y^n_{\mathcal{B}} | M\right) \tag{27}$$

$$n(R_{s,2} - \delta_n) \leq I(X^n_{2,\mathcal{C}\setminus\mathcal{E}_2}; Y^n_{\mathcal{C}\setminus\mathcal{E}_2}) + I\left(M; Y^n_{\mathcal{B}}\right) \tag{28}$$

where $M = \left(Y^n_{1,\mathcal{A}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right)$.

*Proof:* The proof is provided in Appendix A. ■

The proof is completed upon adding (27) and (28) so that

$$\begin{aligned} &n(R_{s,1} + R_{s,2} - 2\delta_n) \\ &\leq (X^n_{1,\mathcal{A}\setminus\mathcal{E}_1}; Y^n_{1,\mathcal{A}\setminus\mathcal{E}_1}) + I(X^n_{2,\mathcal{C}\setminus\mathcal{E}_2}; Y^n_{2,\mathcal{C}\setminus\mathcal{E}_2}) \\ &\quad + I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{B}}) \end{aligned} \tag{29}$$

and using

$$d\left(\frac{1}{n} I(X^n_{\mathcal{A}\setminus\mathcal{E}_1}; Y^n_{\mathcal{A}\setminus\mathcal{E}_1})\right) \leq |\mathcal{A}| - N_E \tag{30}$$

$$d\left(\frac{1}{n} I(X^n_{\mathcal{C}\setminus\mathcal{E}_2}; Y^n_{\mathcal{C}\setminus\mathcal{E}_2})\right) \leq |\mathcal{C}| - N_E \tag{31}$$

$$d\left(\frac{1}{n} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{B}})\right) \leq |\mathcal{B}| \tag{32}$$

where $d(x) \triangleq \lim_{P\to\infty} \frac{x(P)}{\log_2 P}$ characterizes the pre-log scaling of $x$ with respect to $P$.

### B. Converse : $N_E > \max(|\mathcal{A}|, |\mathcal{C}|)$

Without loss of generality, we assume $|\mathcal{C}| \geq |\mathcal{A}|$. Let $\mathcal{E}_k$ be the set of links such that an eavesdropper is monitoring for $W_k$, $k = 1, 2$. Let $|\mathcal{E}_1| = |\mathcal{E}_2| = N_E$, $\mathcal{A} \subset \mathcal{E}_1$, and $\mathcal{C} \subset \mathcal{E}_2$.

Define the set $\mathcal{F}, \mathcal{G}$ such that $\mathcal{F} = \mathcal{B} \backslash \mathcal{E}_1$, $\mathcal{G} = \mathcal{B} \backslash \mathcal{E}_2$. Since $|\mathcal{C}| \geq |\mathcal{A}|$, we have $|\mathcal{G}| \geq |\mathcal{F}|$.

Then Theorem 1 reduces to $d_k \geq 0, k = 1, 2$ and

$$|\mathcal{G}|d_1 + |\mathcal{F}|d_2 \leq |\mathcal{F}| \times |\mathcal{G}| \tag{33}$$

which we now show. We first introduce the following lemma:

*Lemma 2:* For any choice of $\mathcal{F} \subseteq \mathcal{B}$ and $\mathcal{G} \subseteq \mathcal{B}$ with appropriate cardinalities the rates $R_{s,1}$ and $R_{s,2}$ are upper bounded by

$$n(R_{s,1} - \delta_n) \leq I\left(X^n_{1,\mathcal{F}}; Y^n_{\mathcal{F}} | M, X^n_{1,\mathcal{B}\backslash\mathcal{F}}\right) \tag{34}$$

$$n(R_{s,2} - \delta_n) \leq I\left(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{G}}\right) \tag{35}$$

where $M = \left\{Y^n_{1,\mathcal{A}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right\}$.

*Proof:* The proof is provided in Appendix B. ∎

For the remainder of the proof we assume without loss of generality that $\mathcal{B} = \{1, \ldots, |\mathcal{B}|\}$. We fix $\mathcal{G} = \{1, \ldots, |\mathcal{G}|\}$ while choosing $|\mathcal{G}|$ different sets of $|\mathcal{F}|$ elements: $\mathcal{F}_1, \ldots, \mathcal{F}_{|\mathcal{G}|}$ as we explain below.

*Definition 1:* Let $\mathcal{V}_0 = \mathcal{G}$, $c_0 = 1$. For $i \geq 1$ recursively construct $\mathcal{F}_i$ as follows.

1) **Case I:** $|\mathcal{V}_{i-1}| \geq |\mathcal{F}|$
   Let $\mathcal{F}_i = \{\mathcal{V}_{i-1}(1), \ldots, \mathcal{V}_{i-1}(|F|)\}$, where $\mathcal{V}_{i-1}(k)$ denotes the $k$th smallest element in $\mathcal{V}_{i-1}$. Let $\mathcal{V}_i = \mathcal{V}_{i-1} \backslash \mathcal{F}$, and $c_i = c_{i-1}$. This case is illustrated in Figure 5(a) for $i = 1$.
2) **Case II:** $|\mathcal{V}_{i-1}| < |\mathcal{F}|$
   Let $\mathcal{F}_i = \mathcal{V}_{i-1} \cup \mathcal{H}_i$, and $\mathcal{V}_i = \mathcal{G} \backslash \mathcal{H}_i$, and $c_i = c_{i-1} + 1$, where $\mathcal{H}_i = \{1, 2, \ldots, |\mathcal{F}| - |\mathcal{V}_{i-1}|\}$. This case is illustrated in Figure 5(b) for $i = 4$.

To interpret the above construction, we note that the set $\mathcal{G}$ is a row-vector with $|\mathcal{G}|$ elements and let $\mathcal{G}^{\otimes}$ be obtained by concatenating $|\mathcal{F}|$ identical copies of the $\mathcal{G}$ vector i.e.,

$$\mathcal{G}^{\otimes} = \underbrace{[\mathcal{G} \mid \mathcal{G} \mid \ldots \mathcal{G}]}_{|\mathcal{F}| \text{ copies}} \tag{36}$$

As shown in Figure 5, by our construction, the vector $\mathcal{F}_1$ spans the first $|\mathcal{F}|$ elements of $\mathcal{G}^{\otimes}$, the vector $\mathcal{F}_2$ spans the next $|\mathcal{F}|$ elements of $\mathcal{G}^{\otimes}$ etc. The constant $c_i$ denotes the number of copies of the $\mathcal{G}$ vector necessary to cover $\mathcal{F}_i$ .

When $i = |\mathcal{G}|$ the row-vector $\mathcal{F}_i$ terminates exactly at the end of the last $\mathcal{G}$ vector in $\mathcal{G}^{\otimes}$. Hence,

$$c_{|\mathcal{G}|} = |\mathcal{F}|, \qquad \mathcal{V}_{|\mathcal{G}|} = \phi. \tag{37}$$

By going through the above recursive procedure and invoking Lemma 2 repeatedly, each time by setting $\mathcal{F}$ in (34) and (35) to be $\mathcal{F}_i$, we establish the following upper bound on the rate region.

*Lemma 3:* For each $i = 0, 1, \ldots, |\mathcal{G}|$ and the set of channels $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{|\mathcal{G}|}$ defined in Def. 1, the rate pair $(R_{s,1}, R_{s,2})$ satisfies the following upper bound

$$i \cdot n(R_{s,1} - \delta_n) + c_i \cdot n(R_{s,2} - \delta_n) \leq \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i}). \tag{38}$$

Before providing a proof, we note that (33) follows from (38) as described below. Evaluating (38) with $i = |\mathcal{G}|$, using (37) and letting $\tilde{R}_{s,i} = R_{s,i} - \delta_n$,

$$n|\mathcal{G}|\tilde{R}_{s,1} + n|\mathcal{F}|\tilde{R}_{s,2} \leq \sum_{j=1}^{|\mathcal{G}|} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) \tag{39}$$

$$= \sum_{j=1}^{|\mathcal{G}|} \left\{h(Y^n_{\mathcal{F}_j}) - h(Y^n_{\mathcal{F}_j} | M, X^n_{1,\mathcal{B}})\right\} \tag{40}$$

$$= n\left\{|\mathcal{G}| \cdot |\mathcal{F}| \cdot \log_2 P + \Theta(1)\right\}, \tag{41}$$

where the last step uses the fact that

$$h(Y^n_{\mathcal{F}_j}) \leq \sum_{k \in \mathcal{F}_j} h(Y^n_k) \leq n\{|\mathcal{F}| \log_2 P + O(1)\}, \tag{42}$$

and

$$h(Y^n_{\mathcal{F}_j} | M, X^n_{1,\mathcal{B}}) = h(Y^n_{\mathcal{F}_j} | X^n_{1,\mathcal{F}_j}, X^n_{2,\mathcal{F}_j}) = n \cdot O(1). \tag{43}$$

Dividing each side of (41) by $\log_2 P$ and taking the limit $P \to \infty$ yields (33).

*Proof of Lemma 3:* We use induction over the variable $i$ to establish (38). For $i = 0$, note that $c_0 = 0$ and $\mathcal{V}_1 = \mathcal{G}$ and hence (38) is simply (35). This completes the proof for the base case.

For the induction step, we assume that (38) holds for some $t = i$, we need to show that (38) also holds for $t = i + 1$, i.e.,

$$(i+1) \cdot n(R_{s,1} - \delta_n) + c_{i+1} \cdot n(R_{s,2} - \delta_n) \leq \sum_{j=1}^{i+1} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \tag{44}$$

holds. For our proof we separately consider the cases when $|\mathcal{F}| \leq |\mathcal{V}_i|$ and when $|\mathcal{V}_i| < |\mathcal{F}|$ holds.

When $|\mathcal{F}| \leq |\mathcal{V}_i|$, from Definition 1

$$\mathcal{F}_{i+1} \subseteq \mathcal{V}_i, \qquad \mathcal{V}_{i+1} = \mathcal{V}_i \backslash \mathcal{F}_{i+1}, \qquad c_{i+1} = c_i \tag{45}$$

holds. Then (44) follows by combining (38) with (34) as we show below. Note that

$$I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i}) = I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{F}_{i+1}} | Y^n_{\mathcal{V}_i\backslash\mathcal{F}_{i+1}}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \tag{46}$$

$$\leq I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}, Y^n_{\mathcal{V}_i\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \tag{47}$$

$$\leq I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}, X^n_{1,\mathcal{V}_i\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \tag{48}$$

$$\leq I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}, X^n_{1,\mathcal{G}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \tag{49}$$

$$= I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \tag{50}$$

where (46) follows from the chain rule of the mutual information and the definition of $\mathcal{V}_{i+1}$ in (45), while (48) follows from the Markov condition

$$Y^n_{\mathcal{V}_i\backslash\mathcal{F}_{i+1}} \leftrightarrow (X^n_{1,\mathcal{V}_i\backslash\mathcal{F}_{i+1}}, X^n_{2,\mathcal{V}_i\backslash\mathcal{F}_{i+1}}) \leftrightarrow (M, Y^n_{\mathcal{F}_{i+1}}, X^n_{1,\mathcal{B}\backslash\mathcal{G}}) \tag{51}$$

and the fact that $M = (X^n_{2,\mathcal{B}\cup\mathcal{C}}, Y^n_{1,\mathcal{A}})$ already includes $X^n_{2,\mathcal{V}_i\backslash\mathcal{F}_{i+1}}$, (49) follows from the fact that $\mathcal{V}_i \subseteq \mathcal{G}$, while (50) follows from the fact that $\{\mathcal{B}\backslash\mathcal{G}\}\cup\{\mathcal{G}\backslash\mathcal{F}_{i+1}\} = \{\mathcal{B}\backslash\mathcal{F}_{i+1}\}$.

Substituting (50) into the last term in (38) we get

$$\begin{aligned}
&i\cdot n(R_{s,1}-\delta_n) + c_i\cdot n(R_{s,2}-\delta_n)\\
&\le \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i})\\
&\le \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}})\\
&\quad + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}). \qquad (52)
\end{aligned}$$

Finally combining (52) with (34) and using $c_{i+1} = c_i$ (c.f. (45)) we have

$$\begin{aligned}
&(i+1)\cdot n(R_{s,1}-\delta_n) + c_{i+1}\cdot n(R_{s,2}-\delta_n)\\
&\le \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}})\\
&\quad + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}})\\
&\quad + I(X^n_{1,\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}|M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}) \qquad (53)\\
&= \sum_{j=1}^{i+1} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \qquad (54)
\end{aligned}$$

as required .

When $|\mathcal{F}| > |\mathcal{V}_i|$, as stated in Definition 1 we introduce $\mathcal{H}_{i+1} = \{1, 2, \ldots, |\mathcal{F}| - |\mathcal{V}_i|\}$ and recall that

$$\mathcal{F}_{i+1} = \mathcal{V}_i \cup \mathcal{H}_{i+1}, \qquad \mathcal{V}_{i+1} = \mathcal{G}\backslash\mathcal{H}_{i+1}, \qquad c_{i+1} = c_i + 1 \qquad (55)$$

holds. From (35) and (44) we have that

$$\begin{aligned}
&i\cdot n(R_{s,1}-\delta_n) + (c_i+1)\cdot n(R_{s,2}-\delta_n)\\
&= \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i})\\
&\quad + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{G}}) \qquad (56)\\
&= \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i})\\
&+ I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{G}\backslash\mathcal{H}_{i+1}}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}}) \qquad (57)
\end{aligned}$$

As we will show subsequently,

$$\begin{aligned}
&I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{G}\backslash\mathcal{H}_{i+1}})\\
&\qquad \le I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}). \qquad (58)
\end{aligned}$$

Combining (34), (57) and (58) and using $c_{i+1} = c_i + 1$ we get that

$$\begin{aligned}
&(i+1)\cdot n(R_{s,1}-\delta_n) + c_{i+1}\cdot n(R_{s,2}-\delta_n)\\
&\le \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}})\\
&+ I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}) + I(X^n_{\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}|M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}) \qquad (59)\\
&= \sum_{j=1}^{i} I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_j}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_{i+1}})\\
&\quad + I(M, X^n_{1,\mathcal{B}}; Y^n_{\mathcal{F}_{i+1}}), \qquad (60)
\end{aligned}$$

which establishes (44).

It only remains to establish (58) which we do now. First, since $\mathcal{F}_{i+1} \subseteq \mathcal{G}$ it follows that $\{\mathcal{B}\backslash\mathcal{G}\} \subseteq \{\mathcal{B}\backslash\mathcal{F}_{i+1}\}$ and hence we bound the first term in the left hand side of (58) as

$$I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i}) \le I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{V}_i}). \qquad (61)$$

Next, since the set $\mathcal{H}_{i+1} = \{1, \ldots, |\mathcal{F}|-|\mathcal{V}_i|\}$ constitutes the first $|\mathcal{F}|-|\mathcal{V}_i|$ elements of $\mathcal{G}$ and $\mathcal{V}_i = \{|\mathcal{G}|-|\mathcal{V}_i|+1, \ldots, |\mathcal{G}|\}$ constitutes the last $|\mathcal{V}_i|$ elements of $\mathcal{G}$ and $|\mathcal{F}| \le |\mathcal{G}|$ we have that

$$\begin{aligned}
&\{\mathcal{G}\backslash\mathcal{H}_{i+1}\} = \{|\mathcal{F}| - |\mathcal{V}_i| + 1, \ldots, |\mathcal{G}|\}\\
&= \{|\mathcal{F}| - |\mathcal{V}_i| + 1, \ldots, |\mathcal{G}| - |\mathcal{V}_i|\} \cup \{|\mathcal{G}| - |\mathcal{V}_i| + 1, \ldots, |\mathcal{G}|\}\\
&= \{\mathcal{G}\backslash(\mathcal{H}_{i+1} \cup \mathcal{V}_i)\} \cup \mathcal{V}_i\\
&= \{\mathcal{G}\backslash\mathcal{F}_{i+1}\} \cup \mathcal{V}_i \qquad (62)
\end{aligned}$$

where the last relation follows from the definition of $\mathcal{F}_{i+1}$ (c.f. (55)). Using (62) we can bound the second term in (58) as follows.

$$\begin{aligned}
&I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{G}\backslash\mathcal{H}_{i+1}})\\
&= I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{G}\backslash\mathcal{F}_{i+1}}, Y^n_{\mathcal{V}_i}) \qquad (63)\\
&\le I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}, Y^n_{\mathcal{G}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{V}_i}) \qquad (64)\\
&\le I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}, X^n_{1,\mathcal{G}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{V}_i}) \qquad (65)\\
&= I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{V}_i}), \qquad (66)
\end{aligned}$$

where in (65), we use the Markov relation

$$Y^n_{\mathcal{G}\backslash\mathcal{F}_{i+1}} \leftrightarrow (X^n_{1,\mathcal{G}\backslash\mathcal{F}_{i+1}}, X^n_{2,\mathcal{G}\backslash\mathcal{F}_{i+1}}) \leftrightarrow (M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}, Y^n_{\mathcal{F}_{i+1}}) \qquad (67)$$

and the fact that $M = (X^n_{2,\mathcal{B}\cup\mathcal{C}}, Y^n_{1,\mathcal{A}})$ already contains $X^n_{2,\mathcal{G}\backslash\mathcal{F}_{i+1}}$. Combining (61) and (66) gives

$$\begin{aligned}
&I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{V}_i}) + I(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{H}_{i+1}}|Y^n_{\mathcal{G}\backslash\mathcal{H}_{i+1}})\\
&\qquad \le I(M, X^n_{1,\mathcal{B}\backslash\mathcal{F}_{i+1}}; Y^n_{\mathcal{F}_{i+1}}), \qquad (68)
\end{aligned}$$

thus establishing (58).

This completes the proof. ■

*C. Converse:* $\min(|\mathcal{A}|, |\mathcal{C}|) \le N_E \le \max(|\mathcal{A}|, |\mathcal{C}|)$

The proof of this case is similar to the previous two cases. It is omitted here and will be provided in the journal version of this work.

## VI. Conclusion

In this work we have studied the two-transmitter Gaussian complex MIMO-MAC channel where the eavesdropper channel is arbitrarily varying and its state is known to the eavesdropper only, and the main channel is static and its state is known to all nodes. We have completely characterized the s.d.o.f. region for this channel for all possible antenna configurations. The converse was proved by carefully changing the set of signals available to the eavesdropper through an induction procedure in order to obtain an upper bound on a weighted-sum-rate expression.

As suggested by this work, the optimal strategy for a communication network where the eavesdropper channel is arbitrarily varying can potentially be very different from the case where the eavesdropper channel is fixed and its state is known to all terminals. Characterizing secure transmission limits for a broader class of communication models is hence important and is left as future work.

## Appendix A
## Proof of Lemma 1

For $R_{s,1}$, from Fano's inequality, we have

$$n(R_{s,1}-\delta_n) \le I(W_1;Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}) - I(W_1;Y^n_{\mathcal{E}_1}) \quad (69)$$
$$\le I\left(W_1;Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{E}_1}\right) \quad (70)$$
$$\le I\left(W_1;Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}},X^n_{2,\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{E}_1}\right) \quad (71)$$
$$= I\left(W_1;Y^n_{\mathcal{A}\cup\mathcal{B}},X^n_{2,\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{E}_1}\right) \quad (72)$$

where the last step (72) relies on the fact that the additive noise at each receiver end of each sub-channel in Figure 4 is independent from each other and hence

$$Y^n_{\mathcal{C}} \to X^n_{2,\mathcal{C}} \to (W_1,Y^n_{\mathcal{A}\cup\mathcal{B}},Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}})$$

holds. Since $\left(X^n_{2,\mathcal{C}},X^n_{2,\mathcal{B}}\right)$ is independent from $W_1$, and $\mathcal{E}_1 \subseteq \mathcal{A}$, (72) can be written as:

$$I\left(W_1;Y^n_{\mathcal{A}\cup\mathcal{B}}|Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right)$$
$$=I\left(W_1;Y^n_{(\mathcal{A}\setminus\mathcal{E}_1)\cup\mathcal{B}}|Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \quad (73)$$
$$=I\left(W_1;Y^n_{\mathcal{A}\setminus\mathcal{E}_1}|Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) + I\left(W_1;Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \quad (74)$$

where the last step (74) follows from the fact $\mathcal{E}_1 \subseteq \mathcal{A}$ and hence $\mathcal{A} = (\mathcal{A}\setminus\mathcal{E}_1)\cup\mathcal{E}_1$. We separately bound each of the two terms above.

$$I\left(W_1;Y^n_{\mathcal{A}\setminus\mathcal{E}_1}|Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \le I\left(W_1,Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}\cup\mathcal{C}};Y^n_{\mathcal{A}\setminus\mathcal{E}_1}\right)$$
$$\le I\left(W_1,Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}\cup\mathcal{C}},X^n_{1,\mathcal{A}\setminus\mathcal{E}_1};Y^n_{\mathcal{A}\setminus\mathcal{E}_1}\right) \quad (75)$$
$$= I\left(X^n_{1,\mathcal{A}\setminus\mathcal{E}_1};Y^n_{\mathcal{A}\setminus\mathcal{E}_1}\right) \quad (76)$$

where the last step follows from the Markov chain relation $Y^n_{1,\mathcal{A}\setminus\mathcal{E}_1} \leftrightarrow X^n_{\mathcal{A}\setminus\mathcal{E}_1} \leftrightarrow (W_1,Y^n_{\mathcal{E}_1},X^n_{2,\mathcal{B}\cup\mathcal{C}})$, We upper bound the second term in (74) as follows

$$I\left(W_1;Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right)$$
$$\le I\left(X^n_{1,\mathcal{A}\cup\mathcal{B}};Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \quad (77)$$
$$= I\left(X^n_{1,\mathcal{B}};Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) + I\left(X^n_{1,\mathcal{A}};Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}},X^n_{1,\mathcal{B}}\right) \quad (78)$$
$$= I\left(X^n_{1,\mathcal{B}};Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \quad (79)$$

where we use the Markov relation $W_1 \leftrightarrow X^n_{1,\mathcal{A}\cup\mathcal{B}} \leftrightarrow (Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}})$ in step (77) and (79) follows from the fact Markov relation

$$Y^n_{\mathcal{B}} \leftrightarrow (X^n_{1,\mathcal{B}},X^n_{2,\mathcal{B}}) \leftrightarrow (X^n_{2,\mathcal{C}},Y^n_{\mathcal{A}}) \quad (80)$$

Note that (27) follows upon substituting (76) and (79) into (74).

For $R_{s,2}$, from Fano's inequality and the secrecy constraint, we have:

$$n(R_{s,2}-\delta_n) \le I(W_2;Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}) - I(W_2;X^n_{2,\mathcal{E}_2}) \quad (81)$$
$$\le I\left(W_2;Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}|X^n_{2,\mathcal{E}_2}\right) \quad (82)$$
$$=I\left(W_2;Y^n_{\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2}\right) \quad (83)$$
$$=I\left(W_2;Y^n_{(\mathcal{C}\setminus\mathcal{E}_2)\cup\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2}\right) \quad (84)$$
$$=I\left(W_2;Y^n_{\mathcal{C}\setminus\mathcal{E}_2}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2}\right) + I\left(W_2;Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2},Y^n_{\mathcal{C}\setminus\mathcal{E}_2}\right) \quad (85)$$

where (83) follows from the fact that $Y^n_{\mathcal{A}}$ is independent of $(W_2,X^n_{2,\mathcal{B}\cup\mathcal{C}})$ and (84) follows from the fact that $Y^n_{\mathcal{E}_2} \to X^n_{2,\mathcal{E}_2} \to (Y^n_{\mathcal{B}\cup\mathcal{C}\setminus\mathcal{E}_2},W_2,Y^n_{\mathcal{A}})$ holds. We separately bound each term in (85).

$$I\left(W_2;Y^n_{\mathcal{C}\setminus\mathcal{E}_2}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2}\right) \le I\left(W_2,Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2};Y^n_{\mathcal{C}\setminus\mathcal{E}_2}\right) \quad (86)$$
$$\le I\left(X^n_{2,\mathcal{C}\setminus\mathcal{E}_2},W_2,Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2};Y^n_{\mathcal{C}\setminus\mathcal{E}_2}\right) \quad (87)$$
$$= I\left(X^n_{2,\mathcal{C}\setminus\mathcal{E}_2};Y^n_{\mathcal{C}\setminus\mathcal{E}_2}\right), \quad (88)$$

where the justification for establishing (88) is identical to (76) and hence omitted. We finally bound the second term in (85).

$$I\left(W_2;Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2},Y^n_{\mathcal{C}\setminus\mathcal{E}_2}\right) \quad (89)$$
$$\le I\left(X^n_{2,\mathcal{B}\cup\mathcal{C}};Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{E}_2},Y^n_{\mathcal{C}\setminus\mathcal{E}_2}\right) \quad (90)$$
$$\le I\left(Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}},X^n_{2,\mathcal{E}_2},Y^n_{\mathcal{C}\setminus\mathcal{E}_2};Y^n_{\mathcal{B}}\right) \quad (91)$$
$$=I\left(Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}},X^n_{2,\mathcal{E}_2};Y^n_{\mathcal{B}}\right) + I\left(Y^n_{\mathcal{C}\setminus\mathcal{E}_2};Y^n_{\mathcal{B}}|Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}},X^n_{2,\mathcal{E}_2}\right) \quad (92)$$
$$=I\left(Y^n_{\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}};Y^n_{\mathcal{B}}\right) \quad (93)$$

where the justification for arriving at (93) is similar to (79) and hence omitted.

Substituting (88) and (93) into (85) we establish (28).

## Appendix B
## Proof of Lemma 2

Assume the eavesdropper monitors $Y^n_{\mathcal{A}}$ and $X^n_{1,\mathcal{E}_1\setminus\mathcal{A}}$ for $W_1$. Then for $R_{s,1}$, from Fano's inequality, we have:

$$n(R_{s,1}-\delta_n)$$
$$\le I\left(W_1;Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}\right) - I\left(W_1;Y^n_{\mathcal{A}},X^n_{1,\mathcal{E}_1\setminus\mathcal{A}}\right) \quad (94)$$
$$\le I\left(W_1;Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{A}},X^n_{1,\mathcal{E}_1\setminus\mathcal{A}}\right) \quad (95)$$
$$=I\left(W_1;Y^n_{\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{A}},X^n_{1,\mathcal{E}_1\setminus\mathcal{A}}\right) \quad (96)$$
$$\le I\left(W_1;Y^n_{\mathcal{B}\cup\mathcal{C}},X^n_{2,\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{A}},X^n_{1,\mathcal{E}_1\setminus\mathcal{A}}\right) \quad (97)$$
$$=I\left(W_1;Y^n_{\mathcal{B}\cup\mathcal{C}}|Y^n_{\mathcal{A}},X^n_{1,\mathcal{E}_1\setminus\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \quad (98)$$
$$=I\left(W_1;Y^n_{\mathcal{F}}|Y^n_{\mathcal{A}},X^n_{1,\mathcal{E}_1\setminus\mathcal{A}},X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \quad (99)$$

$$=I\left(W_1; Y^n_{\mathcal{F}} | Y^n_{\mathcal{A}}, X^n_{1,\mathcal{B}\backslash\mathcal{F}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) \quad (100)$$

where (98) follows from the fact that $X^n_{2,\mathcal{B}\cup\mathcal{C}}$ is independent of $(W_1, Y^n_{\mathcal{A}}, X^n_{1,\mathcal{E}_1\backslash\mathcal{A}})$. while (99) follows from the fact that since the noise across the channels is independent the Markov condition

$$(Y^n_{\mathcal{E}_1\backslash\mathcal{A}}, Y^n_{\mathcal{C}}) \leftrightarrow (X^n_{1,\mathcal{E}_1\backslash\mathcal{A}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}) \leftrightarrow (W_1, Y^n_{B\backslash\mathcal{E}_1}, Y^n_{\mathcal{A}})$$

holds and furthermore we have defined $\mathcal{F} = \mathcal{B}\backslash\mathcal{E}_1$.

Since the channel noise is independent of the message, $W_1 \leftrightarrow X^n_{1,\mathcal{A}\cup\mathcal{B}} \leftrightarrow (Y^n_{\mathcal{F}\cup\mathcal{A}}, X^n_{1,\mathcal{B}\backslash\mathcal{F}}, X^n_{2,\mathcal{B}\cup\mathcal{C}})$ holds. Hence

$$\begin{aligned}
&I\left(W_1; Y^n_{\mathcal{F}} | Y^n_{\mathcal{A}}, X^n_{1,\mathcal{B}\backslash\mathcal{F}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) && (101)\\
\leq &I\left(X^n_{1,\mathcal{A}\cup\mathcal{B}}; Y^n_{\mathcal{F}} | Y^n_{\mathcal{A}}, X^n_{1,\mathcal{B}\backslash\mathcal{F}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) && (102)\\
= &I\left(X^n_{1,\mathcal{F}}; Y^n_{\mathcal{F}} | Y^n_{\mathcal{A}}, X^n_{1,\mathcal{B}\backslash\mathcal{F}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right)\\
&\quad + I\left(X^n_{1,\mathcal{A}\cup\mathcal{B}\backslash\mathcal{F}}; Y^n_{\mathcal{F}} | Y^n_{\mathcal{A}}, X^n_{1,\mathcal{B}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) && (103)\\
= &I\left(X^n_{1,\mathcal{F}}; Y^n_{\mathcal{F}} | Y^n_{\mathcal{A}}, X^n_{1,\mathcal{B}\backslash\mathcal{F}}, X^n_{2,\mathcal{B}\cup\mathcal{C}}\right) && (104)
\end{aligned}$$

where the last step uses the fact that the second term in (103) involves conditioning on $(X^n_{1,\mathcal{F}}, X^n_{2,\mathcal{F}})$ and hence is zero. This establishes (34).

For $R_{s,2}$, we assume the eavesdropper is monitoring $X^n_{2,\mathcal{C}}, X^n_{2,\mathcal{E}_2\backslash\mathcal{C}}$ for $W_2$. Using Fano's inequality and the secrecy constraint, we have:

$$\begin{aligned}
&n(R_{s,2} - \delta_n) \leq I\left(W_2; Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}\right) - I\left(W_2; X^n_{2,\mathcal{E}_2}\right) && (105)\\
\leq &I\left(W_2; Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}} | X^n_{2,\mathcal{E}_2}\right) && (106)\\
\leq &I\left(W_2; Y^n_{\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}} | X^n_{2,\mathcal{E}_2}\right) && (107)\\
= &I\left(W_2; Y^n_{\mathcal{B}\cup\mathcal{C}} | X^n_{2,\mathcal{E}_2}, Y^n_{\mathcal{A}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}\right) && (108)\\
\leq &I\left(X^n_{2,\mathcal{B}\cup\mathcal{C}}; Y^n_{\mathcal{B}\cup\mathcal{C}} | X^n_{2,\mathcal{E}_2}, Y^n_{\mathcal{A}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}\right) && (109)\\
= &I\left(X^n_{2,\mathcal{B}\cup\mathcal{C}}; Y^n_{\mathcal{G}\cup\mathcal{E}_2} | X^n_{2,\mathcal{E}_2}, Y^n_{\mathcal{A}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}\right) && (110)\\
= &I\left(X^n_{2,\mathcal{B}\cup\mathcal{C}}; Y^n_{\mathcal{G}} | X^n_{2,\mathcal{E}_2}, Y^n_{\mathcal{A}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}\right)\\
&\quad + I\left(X^n_{2,\mathcal{B}\cup\mathcal{C}}; Y^n_{\mathcal{E}_2} | X^n_{2,\mathcal{E}_2}, Y^n_{\mathcal{A}\cup\mathcal{G}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}\right) && (111)\\
= &I\left(X^n_{2,\mathcal{B}\cup\mathcal{C}}; Y^n_{\mathcal{G}} | X^n_{2,\mathcal{E}_2}, Y^n_{\mathcal{A}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}\right) && (112)\\
\leq &I\left(X^n_{2,\mathcal{B}\cup\mathcal{C}}, Y^n_{\mathcal{A}}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}; Y^n_{\mathcal{G}}\right) && (113)\\
\leq &I\left(M, X^n_{1,\mathcal{B}\backslash\mathcal{G}}; Y^n_{\mathcal{G}}\right) && (114)
\end{aligned}$$

where (108) follows from the fact that $(X^n_{1,\mathcal{E}_2\cap\mathcal{B}}, Y^n_{\mathcal{A}})$ are the transmitted signals from user 1 and independent of $(W_2, X^n_{2,\mathcal{E}_2})$ and (110) follows from the fact that $\mathcal{C} \subseteq \mathcal{E}_2 \subseteq \mathcal{B}\cup\mathcal{C}$ and $\mathcal{G} = \mathcal{B}\backslash\mathcal{E}_2$ and hence $\mathcal{E}_2\cup\mathcal{G} = \mathcal{B}\cup\mathcal{C}$ holds. Eq. (112) follows from the fact that since the noise on each channel is Markov, we have $Y^n_{\mathcal{E}_2} \leftrightarrow (X^n_{2,\mathcal{E}_2}, X^n_{1,\mathcal{E}_2\cap\mathcal{B}}) \leftrightarrow (Y^n_{\mathcal{A}\cup\mathcal{G}}, X^n_{\mathcal{B}\cup\mathcal{C}})$ and hence the second term in (111) is zero.

Hence we have proved Lemma 2.

## References


[1] J. Katz and Y. Lindell, *Introduction to modern cryptography*. Chapman & Hall / CRC, 2008.

[2] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] Y. Liang and H. V. Poor, "Multiple Access Channels With Confidential Messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[4] L. Lai and H. El Gamal, "Cooperation for Secrecy: The Relay-Eavesdropper Channel," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.

[5] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, September 1949.

[6] X. Li, J. Hwu, and E. P. Ratazzi, "Using Antenna Array Redundancy and Channel Diversity for Secure Wireless Transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, 2007.

[7] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[8] A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *IEEE International Symposium on Information Theory*, June 2007.

[9] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas-I: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[10] ——, "Secure Transmission with Multiple Antennas-II: The MIMOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, November 2010.

[11] R. Liu, T. Liu, and H. V. Poor, "Multiple-input Multiple-output Gaussian Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4215–4227, September 2010.

[12] E. Ekrem and S. Ulukus, "The Secrecy Capacity Region of the Gaussian MIMO Multi-receiver Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.

[13] M. Kobayashi, Y. Liang, S. Shamai, and M. Debbah, "On the Compound MIMO Broadcast Channels with Confidential Messages," in *IEEE International Symposium on Information Theory*, June 2009.

[14] A. Mukherjee and A. L. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[15] E. MolavianJazi, "Secure Communication Over Arbitrarily Varying Wiretap Channels," *Master Thesis*, December 2009, available online at http://etd.nd.edu/ETD-db/theses/available/etd-12112009-112419/unrestricted/MolavianJaziE122009.pdf.

[16] X. He and A. Yener, "MIMO Wiretap Channels with Arbitrarily Varying Eavesdropper Channel States," submitted to the IEEE Transactions on Information Theory, July, 2010, available online at http://arxiv.org/abs/1007.4801.

[17] X. He, A. Khisti, and A. Yener, "MIMO Broadcast Channel with Arbitrarily Varying Eavesdropper Channel: Secrecy Degrees of Freedom," in *IEEE Global Telecommunication Conference*, December 2011.

[18] 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, June 2008.

[19] E. Ekrem and S. Ulukus, "On the Secrecy of Multiple Access Wiretap Channel," in *46th Allerton Conference on Communication, Control, and Computing*, September 2008.

[20] D. S. Papailiopoulos and A. G. Dimakis, "Distributed Storage Codes Meet Multiple-Access Wiretap Channels," in *48th Allerton Conference on Communication, Control and Computing*, September 2010.

[21] X. He and A. Yener, "Providing Secrecy With Structured Codes: Tools and Applications to Gaussian Two-user Channels," submitted to IEEE Transactions on Information Theory, July, 2009, in revision, available online at http://arxiv.org/abs/0907.5388.

[22] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the Secure Degrees-of-Freedom of the Multiple-Access-Channel," in *IEEE International Symposium on Information Theory*, June 2010.

[23] X. He, "Cooperation and Information Theoretic Security in Wireless Networks," *PhD Dissertation*, August 2009, available online at http://etda.libraries.psu.edu/theses/approved/WorldWideIndex/ETD-5342/index.html.

[24] C. C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM Journal on Numerical Analysis*, vol. 18, no. 3, pp. 398–405, 1981.

[25] A. Khisti, "Interference Alignment for the Multi-Antenna Compound Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2967–2993, May 2011.

[26] D. N. C. Tse and S. V. Hanly, "Multiaccess Fading Channels. I. Polymatroid Structure, Optimal Resource Allocation and Throughput Capacities," *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 2796–2815, 1998.