The Gaussian Interference Wiretap Channel When the Eavesdropper Channel is Arbitrarily Varying

Xiang He Aylin Yener

Wireless Communications and Networking Laboratory, Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xianghe@microsoft.com yener@ee.psu.edu

***Abstract*—In this work we considered the Gaussian two-user interference channel where the eavesdropper channel is arbitrarily varying, all channel matrices have rank less than or equal to 2, and the eavesdropper has 1 antenna. We identify a class of these channel models for which the secrecy degrees of freedom (s.d.o.f.) region is achieved by letting only one user transmit a time. We also provided a non-trivial example for which such a transmission strategy is sub-optimal in terms of s.d.o.f. region. The achievable scheme for this example introduces a new technique to achieve secrecy for MIMO wiretap channels, in which the transmitter-receiver pair uses linear precoding so that effectively the signals are beam-formed toward a direction that can not be attained by the eavesdropper and is at the same time orthogonal to interference from the other user.**

I. Introduction

Information theoretic security was introduced by Shannon in [1], which studied the problem of transmitting confidential information in a communication system in the presence of an eavesdropper with unbounded computation power. Since then, a huge body of work has been devoted to studying this problem for different network models by deriving fundamental transmission rate limits [2], [3] and designing low-complexity schemes to approach these limits in practice [4].

Recently a lot of efforts in information theoretic security are made to address the problem that an eavesdropper is a passive entity and hence its location or channel states can not be accurately obtained by the legitimate parties. Several different channel models have been proposed with the aim to increase the robustness of a secrecy scheme when the eavesdropper channel states are only known by distribution [5], [6], or only available with delays [7], or only known to take values in a finite set [8], [9].

As a more pessimistic but stronger assumption, references [10], [11] study secrecy capacity when the eavesdropper channel is arbitrarily varying and its channel states are known to the eavesdropper only. Reference [11] studies the single-user Gaussian multi-input-multi-output (MIMO) wiretap channel and characterizes the so-called secrecy degrees of freedom (s.d.o.f.), which is the pre-log of the secrecy capacity at high SNR. The s.d.o.f. region of two user Gaussian MIMO broadcast channel with an arbitrarily varying eavesdropper channel was found in [12]. The s.d.o.f. region for two user Gaussian MIMO multiple access channel and Gaussian two-way channel with the eavesdropper channel being arbitrarily varying were given in [13] and [14] respectively. These works introduced several new techniques to prove converse and achievability which were not present in the study of secure MIMO communication with known eavesdropper channel states.

In this work, we continue this line of work by studying the two-user MIMO interference channel with an external eavesdropper. Previously this channel model was only studied with the eavesdropper channel state perfectly known to all nodes and its s.d.o.f. region is still open [15], [16]. Here we study the channel model where the eavesdropper channel state is arbitrarily varying and known to the eavesdropper only. We focus on the case where the ranks of channel matrices between legitimate nodes do not exceed 2 while the eavesdropper has 1 antenna. For a nontrivial class of these channels models, we find its s.d.o.f. region which is achieved by allowing only one user to transmit at a time. We also provide a non-trivial example for which we show such a transmission strategy is suboptimal. The achievability proof for this example introduces a new technique to achieve secrecy in MIMO wiretap channels. The technique leverages the fact that the eavesdropper can not obtain arbitrary linear combinations of the signals transmitted over multiple channel uses due to it having only one antenna. Hence the transmitter and receiver can use linear precoding such that effectively the information-carrying signals are beam-formed toward a direction which can not be attained by the eavesdropper and at the same time is orthogonal to the interference from the other transmitter. The transmitter injects noise to jam the eavesdropper [17] but precodes its jamming signals so that they align with the interference at the intended receiver. This enables the receiver to nullify both interference and jamming signals and achieve secrecy.

II. System Model

The Gaussian two-user MIMO interference channel with an arbitrarily varying eavesdropper channel is shown in Figure 1. The transmitter t, $t = 1, 2$ has $N_{T,t}$ antennas and receiver t has $N_{R,t}$ antennas and the eavesdropper has $N_E = 1$ antennas. During the ith channel use, the channel is:

$$\mathbf{Y}_t(i) = \sum_{k=1}^{2} \mathbf{H}_{k,t}\mathbf{X}_k(i) + \mathbf{Z}_t(i), t = 1, 2, \qquad (1)$$

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

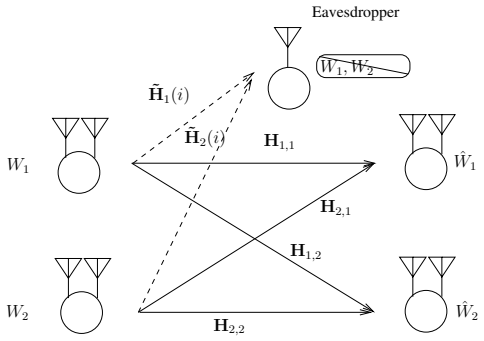

Fig. 1. The two-user Gaussian MIMO interference channel with an arbitrarily varying eavesdropper Channel

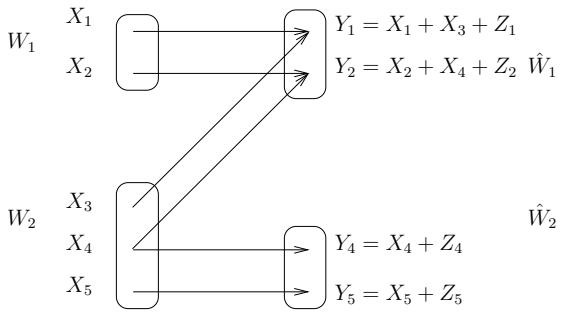

Fig. 2. The single-sided Gaussian MIMO Interference Wiretap Channel. $r(\mathbf{H}_{1,1}) = 2$, $r(\mathbf{H}_{2,1}) = 2$, $r(\mathbf{H}_{2,2}) = 2$, $r(\mathbf{H}_{2,1} \vee \mathbf{H}_{2,2}) = 1$. For clarity the eavesdropper channel is not shown.

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

where $\mathbf{Y}_t(i), t = 1, 2$ denote the signals received at the legitimate receiver t, and $\tilde{\mathbf{Y}}(i)$ denotes the received signal at the eavesdropper. $\mathbf{H}_{k,t}, k = 1, 2, t = 1, 2$ and $\tilde{\mathbf{H}}_k(i), k = 1, 2$ are the channel matrices. $\mathbf{Z}_t, t = 1, 2$ is the additive Gaussian noise observed by the intended receiver t, which is composed of independent rotationally invariant complex Gaussian random variables with unit variance. $\tilde{\mathbf{H}}_k(i), k = 1, 2$ is unknown to the legitimate parties. $\mathbf{H}_{k,t}, t = 1, 2$ are known by both the legitimate parties and the eavesdropper(s).

Transmitter t sends a message W_t to receiver t over n channel uses. W_1, W_2 must be kept confidential from the eavesdropper, but are not necessarily kept secret from the legitimate receivers.

The average power constraint for the transmitter t is

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \text{trace}(\mathbf{X}_t(i)(\mathbf{X}_t(i))^H) \le \bar{P}. \tag{3}$$

For clarity, we shall use γ to represent a sequence of $\{\tilde{\mathbf{H}}_k(i), k = 1, 2\}$ and use $\{\tilde{\mathbf{Y}}_\gamma(i)\}$ to represent the outputs of the eavesdropper channel that corresponds to this sequence of eavesdropper channel states.

We assume the eavesdropper channel state information sequence $\{\tilde{\mathbf{H}}(i)\}$ is independent from $\{\mathbf{X}_t(i), t = 1, 2\}$. In this case, as shown in [11], the secrecy constraint can be defined as:

$$\lim_{n\to\infty} I\left(W_1, W_2; \tilde{\mathbf{Y}}_\gamma^n\right) = 0, \quad \forall\gamma. \tag{4}$$

We require the limit in (4) to be uniform over all possible sequences of eavesdropper channel states [11].

The secrecy rate for the message W_t, $R_{s,t}$, is defined as $R_{s,t} = \lim_{n\to\infty} \frac{1}{n} H(W_t), t = 1, 2$ such that W_t can be reliably decoded by receiver t and (4) is satisfied.

In this paper, we use the secrecy degrees of freedom (s.d.o.f.) region as a characterization of the high SNR behavior of the secrecy capacity for this channel. The s.d.o.f. region is defined as:

$$\{(d_1, d_2) : d_t = \limsup_{\bar{P}\to\infty} \frac{R_{s,t}}{\log_2 \bar{P}}, t = 1, 2\}. \tag{5}$$

We use the notation $\mathbf{A}_{n\times m}$ to denote a matrix $\mathbf{A}$ with m columns and n rows and use $r(\mathbf{A})$ to denote its rank. For two matrices $\mathbf{A}$ and $\mathbf{B}$ with the same number of rows, define $r(\mathbf{A} \wedge \mathbf{B})$ as

$$r(\mathbf{A} \wedge \mathbf{B}) = r(\mathbf{A}) + r(\mathbf{B}) - r([\mathbf{A}, \mathbf{B}]). \tag{6}$$

For two matrices $\mathbf{A}$ and $\mathbf{B}$ with the same number of columns, define $r(\mathbf{A} \vee \mathbf{B})$ as

$$r(\mathbf{A} \vee \mathbf{B}) = r(\mathbf{A}) + r(\mathbf{B}) - r([\mathbf{A}^H, \mathbf{B}^H]). \tag{7}$$

III. Main Results

Define two regions

$$\{d_t \ge 0, t = 1, 2, d_1 + d_2 \le 1\}, \tag{8}$$

$$\{0 \le d_t \le 1, t = 1, 2\}. \tag{9}$$

Theorem 1: Let $N_E = 1$, $r(\mathbf{H}_{1,1}) = r(\mathbf{H}_{2,2}) = 2$, then the s.d.o.f. region is given by (8) if the following conditions hold:

$$1 \le r(\mathbf{H}_{1,1} \wedge \mathbf{H}_{2,1}) \le 2, \tag{10}$$

$$1 \le r(\mathbf{H}_{2,1} \vee \mathbf{H}_{2,2}) = r(\mathbf{H}_{2,1}) \le 2. \tag{11}$$

We next describe a non-trivial example, in the sense that it is not known whether the region (9) is achievable for this model. However the next theorem shows its s.d.o.f. region is strictly greater than (8).

Theorem 2: Consider the single sided interference channel shown in Figure 2, where

$$\mathbf{H}_{1,1} = \mathbf{I}_{2\times 2}, \mathbf{H}_{2,2} = [0_{2\times 1}, \mathbf{I}_{2\times 2}]_{2\times 3}, \tag{12}$$

$$\mathbf{H}_{2,1} = [\mathbf{I}_{2\times 2}, 0_{2\times 1}]_{2\times 3}, \mathbf{H}_{1,2} = 0_{2\times 2}. \tag{13}$$

For this channel model, any s.d.o.f. pair $d_1, d_2 = 1$ is achievable if $0 \le d_1 < 1/3$.

IV. Proof of Theorem 1

We first need to transform the channel model so that it is easier to analyze. In particular, it is desirable to decompose at least three MIMO links of the interference channels, i.e., two intended links, and one interfering link, into parallel subchannels. The following lemma describes a special case for which this is possible.

Lemma 1: When

$$r(\mathbf{H}_{2,1} \vee \mathbf{H}_{2,2}) = r(\mathbf{H}_{2,1}) \leq r(\mathbf{H}_{2,2}), \tag{14}$$

the channel can be transformed into the following form while retaining the s.d.o.f. region: Receiver 1 observes a multiple access channel composed of parallel links:

$$y_{1i} = x_{1i} + z_i, \quad i \in \mathcal{A}, \tag{15}$$

$$y_{1i} = x_{1i} + x_{2i} + z_i, \quad i \in \mathcal{B}, \tag{16}$$

$$y_{1i} = x_{2i} + z_i, \quad i \in \mathcal{C}, \tag{17}$$

where $|\mathcal{A}| + |\mathcal{B}| = r(\mathbf{H}_{1,1}), |\mathcal{B}| + |\mathcal{C}| = r(\mathbf{H}_{2,1}), |\mathcal{B}| = r(\mathbf{H}_{1,1} \wedge \mathbf{H}_{2,1})$. The noise random variables across the sub-channels $\{z_i\}_{i\in\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}}$ are independent and each is distributed according to $\mathcal{CN}(0,1)$. $\{x_{1i}\}_{i\in\mathcal{A}\cup\mathcal{B}}$ denote the transmit symbols of user 1 and $\{x_{2i}\}_{i\in\mathcal{B}\cup\mathcal{C}}$ denote (a subset of) the transmit symbols of user 2.

Receiver 2 observes

$$\mathbf{Y}_2 = \begin{bmatrix} \mathbf{X}_2' \\ 0 \end{bmatrix}_{N_{R,2}\times 1} + \mathbf{H}_{1,2}\mathbf{X}_1 + \mathbf{Z}_2, \tag{18}$$

where $\mathbf{X}_2'$ is the transmitted signals of user 2, which is a $r(\mathbf{H}_{2,2}) \times 1$ vector whose first $r(\mathbf{H}_{2,1})$ components are $\{x_{2i}\}_{i\in\mathcal{B}\cup\mathcal{C}}$.

Proof Outline: We first apply Generalized Singular Value Decomposition (GSVD) to $[\mathbf{H}_{1,1}, \mathbf{H}_{2,1}]$. It can be shown that it is possible to transform the channel observed by receiver 1 into the form (15)-(17) without affecting the s.d.o.f. region of the channel [13]. After this transformation, we can represent $\mathbf{H}_{2,1}$ as follows:

$$\mathbf{H}_{2,1} = \begin{bmatrix} \mathbf{I}_{r(\mathbf{H}_{2,1})\times r(\mathbf{H}_{2,1})} & \\ & 0 \end{bmatrix}_{r(\mathbf{H}_{1,1}\wedge\mathbf{H}_{2,1})\times N_{T_2}}. \tag{19}$$

Note that the transformation will affect all channel matrices of legitimate links due to changes in the representation of transmitted signals. During the transformation we either multiply $\mathbf{H}_{i,j}$ with nonsingular matrices or removing all zero rows from $\mathbf{H}_{2,1}$ (which only affects the receiver). Hence it does not change $r(\mathbf{H}_{2,1})$ or $r(\mathbf{H}_{2,1} \vee \mathbf{H}_{2,2})$.

From (14), we have

$$r([\mathbf{H}_{2,1}^H, \mathbf{H}_{2,2}^H]) = r(\mathbf{H}_{2,2}) \geq r(\mathbf{H}_{2,1}). \tag{20}$$

In order to satisfy (20) for (19), the number of nonzero columns of $\mathbf{H}_{2,2}$ (after applying the GSVD step above) cannot exceed $r(\mathbf{H}_{2,2})$. Without loss of generality, we assume the last $N_{T,2} - r(\mathbf{H}_{2,2})$ columns of $\mathbf{H}_{2,2}$ are zeros. We next apply singular value decomposition to the remaining $r(\mathbf{H}_{2,2})$ columns of $\mathbf{H}_{2,2}$, denoted by $\mathbf{H}_{2,2}'$ which leads to:

$$\mathbf{H}_{2,2}' = \mathbf{U}\begin{bmatrix} \mathbf{D}_{r(\mathbf{H}_{2,2})\times r(\mathbf{H}_{2,2})} \\ 0 \end{bmatrix}_{N_{R,2}\times r(H_{2,2})} \mathbf{V}, \tag{21}$$

where $\mathbf{U}$, $\mathbf{V}$ are unitary matrices and $\mathbf{D}$ is a diagonal matrix whose diagonal elements are the singular values of $\mathbf{H}_{2,2}'$. The channel observed by receiver 2 can then be written as following after canceling $\mathbf{U}$:

$$\mathbf{Y}_2 = [(\mathbf{D}\mathbf{V}\mathbf{X}_2')^T; 0]^T + \mathbf{H}_{1,2}\mathbf{X}_1 + \mathbf{Z}_2. \tag{22}$$

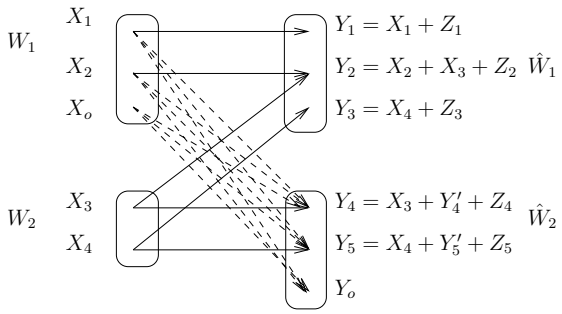

Fig. 3. $r(\mathbf{H}_{1,1} \wedge \mathbf{H}_{2,1}) = 1, r(\mathbf{H}_{2,1} \vee \mathbf{H}_{2,2}) = r(\mathbf{H}_{2,1}) = 2$

DV is an invertible matrix, which can be canceled from (22) without affecting s.d.o.f. region. Hence we obtain (18). ■

We next prove Theorem 1 in two cases. In both cases the achievability followed directly from letting only one user transmit at a time. Hence we only need to prove converse.

A. *Case 1:* $r(\mathbf{H}_{1,1} \wedge \mathbf{H}_{2,1}) = 1$

Due to Lemma 1, the channel after applying transformation can be represented by Figure 3. We use Y_o to represent the $N_{R,2} - r(\mathbf{H}_{2,2})$ components in the signals observed by receiver 2 which does not depend on signals transmitted by user 2. X_o represents the signals transmitted by user 1 which can not be observed by receiver 1. $Y_k', k = 3, 4$ represents the components in Y_k that only depends on the signals transmitted by user 1.

Since $r(\mathbf{H}_{1,1} \wedge \mathbf{H}_{2,1}) = 1$, we have $r(\mathbf{H}_{2,1}) \geq 1$. On the other hand, there is no need to consider the case $r(\mathbf{H}_{2,1}) = 1$ separately, which corresponds to removing y_3 in Figure 3. This is because when proving converse for this case, we can always reveal y_3 to receiver 1 as genie information and apply the converse described in this section.

Let $\{\delta_n\}$ denote the non-negative sequence that goes to 0 when n goes to infinity. First assume the eavesdropper monitors X_1^n, then from Fano's inequality and the confidentiality requirement on W_1, we have

$$n(R_1 - \delta_n) \tag{23}$$

$$\leq I(W_1; Y_1^n, Y_2^n, Y_3^n) - I(W_1; X_1^n) \tag{24}$$

$$\leq I(W_1; Y_1^n, Y_2^n, Y_3^n | X_1^n) \tag{25}$$

$$= I(W_1; X_2^n + X_3^n + Z_2^n | X_1^n, Y_3^n) \tag{26}$$

$$\leq I(X_1^n, X_2^n, X_o^n; X_2^n + X_3^n + Z_2^n | X_1^n, Y_3^n) \tag{27}$$

$$= h(X_2^n + X_3^n + Z_2^n | X_1^n, Y_3^n) - h(X_3^n + Z_2^n | X_4^n + Z_3^n, X_1^n, X_2^n, X_o^n) \tag{28}$$

$$= h(X_2^n + X_3^n + Z_2^n | X_1^n, Y_3^n) - h(X_3^n + Z_2^n | X_4^n + Z_3^n) \tag{29}$$

Next we assume the eavesdropper monitors Y_5^n. Then we have:

$$n(R_2 - \delta_n) \tag{30}$$

$$\leq I(W_2; Y_4^n, Y_5^n, Y_o^n) - I(W_2; Y_5^n) \tag{31}$$

$$\leq I(W_2; Y_4^n, Y_o^n | Y_5^n) \tag{32}$$

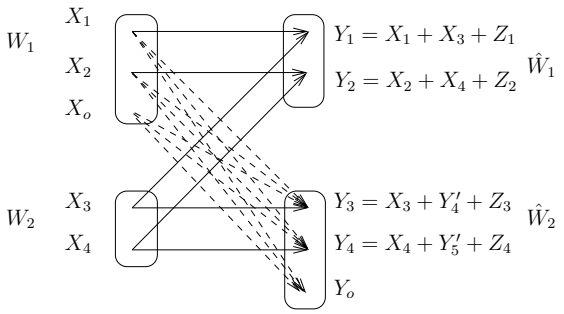

Fig. 4. $r\left(\mathbf{H}_{1,1} \wedge \mathbf{H}_{2,1}\right) = 2$

$$\begin{aligned}
&\leq I\left(W_2; Y_4^n, Y_o^n, X_1^n, X_2^n | Y_5^n\right) && (33)\\
&= I\left(W_2; Y_4^n | Y_5^n\right) \\
&\quad + I\left(W_2; Y_o^n, X_1^n, X_2^n | Y_4^n, Y_5^n\right) && (34)\\
&= I\left(W_2; Y_4^n | Y_5^n\right) && (35)\\
&\leq I\left(X_3^n, X_4^n; Y_4^n | Y_5^n\right) && (36)\\
&= h\left(X_3^n + Z_4^n | X_4^n + Z_5^n\right) - h\left(Z_4^n\right). && (37)
\end{aligned}$$

Note that

$$h\left(X_3^n + Z_2^n | X_4^n + Z_3^n\right) = h\left(X_3^n + Z_4^n | X_4^n + Z_5^n\right). \quad (38)$$

Hence, adding (29) to (37), we get

$$\begin{aligned}
&n\left(R_1 + R_2 - \delta_n\right) && (39)\\
&\leq h\left(X_2^n + X_3^n + Z_2^n | X_1^n, Y_3^n\right) - h\left(Z_4^n\right). && (40)
\end{aligned}$$

Since the pre-log of $h\left(X_2^n + X_3^n + Z_2^n | X_1^n, Y_3^n\right)$ can not exceed one, we find that $d_1 + d_2 \leq 1$.

B. Case 2: $r\left(\mathbf{H}_{1,1} \wedge \mathbf{H}_{2,1}\right) = 2$

The channel after applying transformation can be represented by Figure 4. Assume the eavesdropper monitors X_2^n, we have

$$\begin{aligned}
&n(R_1 - \delta_n) && (41)\\
&\leq I\left(W_1; Y_1^n, Y_2^n | X_2^n\right) && (42)\\
&= I\left(W_1; X_1^n + X_3^n + Z_1^n | X_4^n + Z_2^n, X_2^n\right) && (43)\\
&\leq I\left(X_1^n, X_o^n; X_1^n + X_3^n + Z_1^n | X_4^n + Z_2^n, X_2^n\right) && (44)\\
&= h\left(X_1^n + X_3^n + Z_1^n | X_4^n + Z_2^n, X_2^n\right) \\
&\quad - h\left(X_3^n + Z_1^n | X_4^n + Z_2^n\right). && (45)
\end{aligned}$$

The upper bound on R_2 is the same as (37). Hence, adding (45) to (37) and applying (38), we get

$$\begin{aligned}
&n\left(R_1 + R_2 - 2\delta_n\right) && (46)\\
&\leq h\left(X_1^n + X_3^n + Z_1^n | X_4^n + Z_2^n, X_2^n\right) - h\left(Z_4^n\right). && (47)
\end{aligned}$$

Since the pre-log of $h\left(X_2^n + X_3^n + Z_2^n | X_1^n, Y_3^n\right)$ can not exceed one, we find that $d_1 + d_2 \leq 1$.

V. Proof Outline of Theorem 2

In the channel model in Figure 2, the signals received by the eavesdropper Y_e can be represented by two parts:

$$Y_e = Y_{e1,i} + Y_{e2,i}, \quad (48)$$

$$\begin{aligned}
Y_{e1,i} &= a_i X_{1,i} + b_i X_{2,i}, && (49)\\
Y_{e2,i} &= c_i X_{3,i} + d_i X_{4,i} + e_i X_{5,i}, && (50)
\end{aligned}$$

where a_i, b_i, c_i, d_i, e_i is the channel gain observed by the eavesdropper at the ith channel use. Then for any given sequence of $\{a_i, b_i, c_i, d_i, e_i, i = 1, ..., n\}$, we have the following lemma [13]:

Lemma 2:

$$\begin{aligned}
\lim_{n\to\infty} I(W_1; Y_{e1}^n) &= 0, && (51)\\
\lim_{n\to\infty} I(W_2; Y_{e2}^n) &= 0, && (52)
\end{aligned}$$

imply $\lim_{n\to\infty} I\left(W_1, W_2; Y_e^n\right) = 0$.

We next describes an achievable scheme such that (51) and (52) are satisfied.

A. Linear Precoding

Let $X_{j,i}$ denote the value of X_j during the ith channel uses. For a large positive integer M, transmitter 1 computes $X_{3,i}$ as

$$\begin{aligned}
X_{3,i} &= 0, \quad i \bmod M = 0 \text{ or } M-1, && (53)\\
X_{3,i} &= -X_{4,i-1}, \quad i \bmod M = 1, ..., M-2. && (54)
\end{aligned}$$

For i such that $i \bmod M = 1, ..., M-2$, Receiver 1 can compute the quantity Y_i defined as

$$\begin{aligned}
Y_i &= Y_{1,i} + Y_{2,i-1} && (55)\\
&= X_{1,i} + X_{2,i-1} + Z_{1,i} + Z_{2,i-1}. && (56)
\end{aligned}$$

For these channel indices $\{i\}$, transmitter 1 performs linear precoding over every three channel uses. This means, for i such that $i \bmod M = 1, ..., M-2$ and $i+1 \bmod 3 = 2$, Transmitter 1 computes the transmitted signals as:

$$\begin{cases} X_{1,i} = U_{1,i} + J_i \\ X_{2,i} = 0 \end{cases} \quad (57)$$

$$\begin{cases} X_{1,i-1} = U_{1,i-1} + J_{i-1} \\ X_{2,i-1} = U_{2,i-1} - J_i \end{cases} \quad (58)$$

$$\begin{cases} X_{1,i-2} = 0 \\ X_{2,i-2} = U_{2,i-2} - J_{i-1} \end{cases} \quad (59)$$

where J_i is Gaussian jamming noise injected by transmitter 1, and $U_{i,j}$ is the effective input from user 1. By substituting (57)-(59) into (56), we observe that receiver 1 gets

$$\begin{aligned}
&U_{1,i} + U_{2,i-1} + Z_{1,i} + Z_{2,i-1}, && (60)\\
&U_{1,i-1} + U_{2,i-2} + Z_{1,i-1} + Z_{2,i-2}. && (61)
\end{aligned}$$

For every three channel uses, the eavesdropper receives

$$\begin{aligned}
&U_{1,i} + J_i, && (62)\\
&a_{i-1}\left(U_{1,i-1} + J_{i-1}\right) + b_{i-1}\left(U_{2,i-1} - J_i\right), && (63)\\
&U_{2,i-2} - J_{i-1}. && (64)
\end{aligned}$$

The channel gains $a_i, b_i, a_{i-2}, b_{i-2}$ do not appear in these signals because $X_{2,i} = 0$ and $X_{1,i-2} = 0$. Equivalently, since the eavesdropper knows its channel states $\{a_i, b_i\}$, we

can represent the signals it received as following without any loss of information:

$$U_{1,i} + J_i, \tag{65}$$

$$a_{i-1}\left(U_{1,i-1} + U_{2,i-2}\right) + b_{i-1}\left(U_{1,i} + U_{2,i-1}\right), \tag{66}$$

$$U_{2,i-2} - J_{i-1}. \tag{67}$$

Finally, let $U_{2,i-1} = U_{1,i}$ and $U_{2,i-2} = U_{1,i-1}$. The signals observed by receiver 1 becomes

$$2U_{1,i} + Z_{1,i} + Z_{2,i-1}, \tag{68}$$

$$2U_{1,i-1} + Z_{1,i-1} + Z_{2,i-2}. \tag{69}$$

The signals received by the eavesdropper becomes

$$U_{1,i} + J_i, \quad U_{1,i-1} - J_{i-1}, \tag{70}$$

$$a_{i-1}U_{1,i-1} + b_{i-1}U_{1,i}. \tag{71}$$

B. Secrecy for User 1

For every three channel uses, the intended receiver obtains two clear signals (68)-(69), while Eve gets one overlapping copy of signals (71) and two heavily jammed signals (70). For this equivalent wiretap channel whose inputs are $[U_{1,i}, U_{1,i-1}]$, it can be shown by following [11] that a secrecy degree of freedom of 1 is achievable using a randomly generated Gaussian codebook and random binning scheme such that (68) is satisfied. By choosing a sufficiently large M, this means d_1 can be made arbitrarily close to $1/3$ in the original channel.

C. Secrecy of User 2

For transmitter 2, we view every M channel uses as a single channel use. The effective channel inputs is a $2M \times 1$ complex vector $\mathbf{X}_{M,k}, k \geq 0$ given by

$$[X_{4,Mk}, X_{5,Mk}, ..., X_{4,M(k+1)-1}, X_{5,M(k+1)-1}]. \tag{72}$$

Due to the restriction placed on (53), the equivalent eavesdropper channel is memoryless whose output is a $M \times 1$ vector. The channel matrix is given by:

$$\begin{bmatrix} d_k & e_k & & & & \\ -c_i & 0 & d_i & e_i & & \\ & & & \ldots & & \\ & & -c_j & 0 & d_j & e_j \end{bmatrix}_{M \times 2M}, \tag{73}$$

where the subscript of the tth row equals $Mk+t$. The channel is therefore a single-user MIMO-wiretap channel, in which the transmitter and the receiver has $2M$ antennas, and the eavesdropper has M antennas. In [11], it was shown that there exists a codebook that achieves an s.d.o.f. of M for this channel which satisfies (52). This translates to an s.d.o.f. of $d_2 = 1$ for the original channel.

VI. Conclusion

In this work, we studied the Gaussian two-user interference channel with an external eavesdropper, where the eavesdropper channel is arbitrarily varying and its state is known to the eavesdropper only. We focused on the case where all channel matrices between legitimate transmitter and receiver had rank less than or equal to 2 and the eavesdropper had 1 antenna. The s.d.o.f. region for a class of this type of channel models was found, which was achieved by allowing only one user to transmit at a time. We also provided a non-trivial example for which we proved such a transmission strategy was sub-optimal. The achievability proof for this example introduced a new method in which the artificial noise injected by the transmitter is aligned with interference at its intended receiver through linear precoding. This enables the transmitter to effectively jams the eavesdropper while the receiver can nullify the interference and jamming signals at the same time and achieves secrecy.

References

[1] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, September 1949.

[2] I. Csiszár and J. Körner. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[3] Y. Liang, H.V. Poor, and S. Shamai Shitz. Information theoretic security. *Foundations and Trends in Communications and Information Theory*, 5(4–5):355–580, 2009.

[4] M. Bellare and S. Tessaro. Polynomial-Time, Semantically-Secure Encryption Achieving the Secrecy Capacity. 2012. available online at http://arxiv.org/abs/1201.3160.

[5] P. K. Gopala, L. Lai, and H. El-Gamal. On the Secrecy Capacity of Fading Channels. *IEEE Transactions on Information Theory*, 54(9):4687–4698, October 2008.

[6] F. Renna, M. Bloch, and N. Laurenti. Semi-Blind Key-Agreement over MIMO Fading Channels. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–6. IEEE, 2011.

[7] S. Yang, P. Piantanida, M. Kobayashi, and S. Shamai. On the Secrecy Degrees of Freedom of Multi-Antenna Wiretap Channels with Delayed CSIT. In *IEEE International Symposium on Information Theory*, July 2011.

[8] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai. Compound Wiretap Channels. *Eurasip Journal on Wireless Communication and Networking, Special issue in Wireless Physical Layer Security*, 2009, Article ID 142374, 12 pages, 2009. doi:10.1155/2009/142374.

[9] A. Khisti. Interference Alignment for the Multi-Antenna Compound Wiretap Channel. *IEEE Transactions on Information Theory*, 57(5):2967–2993, May 2011.

[10] 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.

[11] 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.

[12] 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.

[13] X. He, A. Khisti, and A. Yener. MIMO Multiple Access Channel with an Arbitrarily Varying Eavesdropper. In *49th Allerton Conference on Communication, Control and Computing*, September 2011. The ordering of authors is alphabetical.

[14] X. He and A. Yener. Gaussian Two-way Wiretap Channel with an Arbitrarily Varying Eavesdropper. In *IEEE Global Telecommunication Conference, Workshop on Physical Layer Security*, December 2011.

[15] 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.

[16] O. Koyluoglu, H. El-Gamal, L. Lai, and H. V. Poor. Interference Alignment for Secrecy. to appear in IEEE Transactions on Information Theory, submitted in October, 2008, available online at http://arxiv.org/abs/0810.1187.

[17] S. Goel and R. Negi. Guaranteeing Secrecy using Artificial Noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, June 2008.