Fiftieth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 1 - 5, 2012

The Interference Wiretap Channel with an Arbitrarily Varying Eavesdropper: Aligning Interference with Artificial Noise

Xiang He, Aylin Yener*

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

***Abstract*—In this work, a Gaussian two-user MIMO interference channel is considered in the presence of an external eavesdropper whose channel is completely unknown to the legitimate communication parties and can be varying in an arbitrary fashion from one channel use to the next. We improve our recent result by deriving a larger achievable secrecy degrees of freedom region. In the achievable scheme, the transmitter injects artificial noise to confuse the eavesdropper, and at the same time aligns the injected noise with the interference from the other user at the intended receiver. The achieved secure degrees of freedom are shown to be closely connected to the rank of the effective channel matrix through which the eavesdropper observes the artificial noise. The precoding matrix is then designed to ensure that this rank cannot be reduced under any possible Eve's channel state.**

I. Introduction

Information theoretic secrecy was first introduced by Shannon [1]. This approach measures the information leaked to an eavesdropper by the mutual information between the confidential message and the eavesdropper's observation and aims to find the reliable transmission rates between the message sender and its intended receiver so that the leaked information vanishes when the number of channel uses goes to infinity. Over the past few years, there has been extensive interest in this approach [2]. In these works, the signaling schemes are designed to minimize the leaked information in order to provide secrecy guarantees for the transmitted messages at the physical layer.

One of the main challenges for providing a secrecy guarantee via the physical layer comes from modeling the channel between the sender of the message and the eavesdropper. In cryptography, which provides a secrecy guarantee at the application layer, the eavesdropper is assumed to have perfect knowledge of the signals transmitted by the sender. This is almost never the case in wireless communications, where the signals received by the eavesdropper is always corrupted by interference/noise. In fact, recent works indicate that certain stream ciphers are less vulnerable to known attacks if the cipher text is corrupted by noise [3]. By comparison, the physical layer, i.e., information theoretic security, approach does take into account of the benefit of a noisy channel for secrecy [2]. Yet, when doing so, in most contributions, the eavesdropper's channel is assumed to be (exactly or statistically) known by the sender of the message, see for example [4]–[9] and many others. This is obviously difficult to satisfy in practice for a passive adversary like an eavesdropper.

Recent works have been successful in removing this limiting assumption, by replacing it with one that pertains to limiting the physical resources of the eavesdropper. Specifically, reference [10] has shown the existence of a coding scheme that guarantees strong secrecy irrespective of the eavesdropper channel state for the MIMO wiretap channel, as long as the eavesdropper has fewer antennas than the legitimate parties. It is important to note that with this approach, no exact or statistical knowledge of the eavesdropper channel is assumed, and the eavesdropper channel state can vary arbitrarily from one channel use to the next. Consequently, this model also provides secrecy against infinitely many non-colluding eavesdroppers. It has also been shown recently that for several network information theoretic models, positive strongly secure degrees of freedom can be obtained irrespective of the eavesdropper channel, see [11]–[13], for the two-way wiretap, multiple access and broadcast channels respectively.

In this work, we continue in this direction and study the two-user MIMO Gaussian interference channel in the presence of an adversary eavesdropping on the messages from the two transmitters. Consistent with the above discussion, we assume the eavesdropper has fewer antennas than the sender of the message or its intended receiver, i.e., it is limited in its reception capability. The eavesdropper channel gains are unknown to the legitimate parties and can vary arbitrarily. We provide an achievable secure degrees of freedom region in this set up.

The focus of this work is on a single-sided interference wiretap channel model where the rank of channel matrices between any legitimate transmitter and receiver equals 2 while the adversary has 1 antenna. This model was first studied in [14], which showed the strategy of letting only one user transmit at each channel use is not optimal. In the scheme proposed in [14], the transmitter that does not cause interference in the single-sided interference channel model injects artificial noise to confuse the adversary. The receiver

978-1-4673-4539-2/12/$31.00 ©2012 IEEE

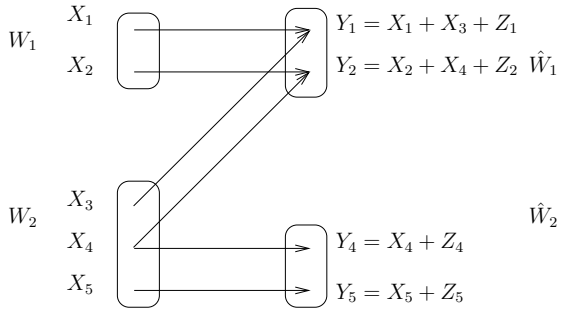

Fig. 1. The single-sided Gaussian MIMO Interference Wiretap Channel. $r(\mathbf{H}_{1,1}) = 2$, $r(\mathbf{H}_{2,1}) = 2$, $r(\mathbf{H}_{2,2}) = 2$, $r([\mathbf{H}_{2,1}^T \mathbf{H}_{2,2}^T]) = 3$. For clarify the eavesdropper channel is not shown.

paired with this transmitter observes two unwanted signals: the interference from the other transmitter and the injected artificial noise. Hence to save the spatial degrees of freedom at this receiver, the artificial noise is linear precoded to align with the user interference so that both can be nullified by the receiver simultaneously. The achieved secrecy rate exceeds the rate achievable through simple time sharing when the transmission power increases.

The main contribution of this work is that we show a new secrecy rate region larger than that in [14] is achievable. The scheme uses aligning artificial noise and interference, but the improvement comes from choosing larger precoding matrices, which project the artificial noise to a higher dimensional linear subspace so that the adversary is unable to cancel out the noise completely. The challenges tackled include how to calculate the secrecy rate in this case, and how to choose the precoding matrix to maximize the secrecy rate. The matrices we use are selected through a rank criterion we establish. Next a series of channel enhancement arguments are used to transform the channel prefixed by the chosen precoding matrix until its secrecy rate can be computed. The transformed channel finally becomes an interference aided Gaussian MIMO wiretap channel where the eavesdropper channel is arbitrarily varying which extends the single user MIMO wiretap channel studied previously in [10]. Consequently, the resulting strongly secure degrees of freedom region can be quantified.

II. System Model and Main Result

The channel model is shown in Figure 1. The transmitters have 2 and 3 antennas respectively. The receivers have 2 antennas each and the eavesdropper has 1 antenna. The eavesdropper is assumed to have a noiseless channel. Thus, during the ith channel use, we have:

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

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

where

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

$$\mathbf{H}_{2,1} = [\mathbf{I}_{2\times 2}, 0_{2\times 1}]_{2\times 3}, \mathbf{H}_{1,2} = 0_{2\times 2}. \tag{4}$$

For clarity, we use subscripts to denote the size of the matrix and $\mathbf{I}$ to denote an identity matrix. $\mathbf{Y}_t(i), t = 1, 2$ 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. $\mathbf{H}_{k,t}, t = 1, 2$ are known by both the legitimate parties and the eavesdropper(s). $\tilde{\mathbf{H}}_k(i), k = 1, 2$ is unknown to the legitimate parties.

Transmitter t sends a message W_t to receiver t over n channel uses. W_1, W_2 must both be kept confidential from the eavesdropper. Message W_i, $i = 1, 2$ needs to be decoded reliably at its intended receiver and is not kept secret from the other legitimate receiver.

The average power constraint for the transmitter t is

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \text{trace}(\mathbf{X}_t(i)(\mathbf{X}_t(i))^H) \leq \bar{P}. \tag{5}$$

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 [10], the *strong* secrecy constraint can be defined as:

$$\lim_{n\to\infty} I\left(W_1, W_2; \tilde{\mathbf{Y}}_\gamma^n\right) = 0, \quad \forall\gamma, \tag{6}$$

We require the limit in (6) to be uniform over all possible sequences of eavesdropper channel states [10].

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 (6) 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:

$$\{(d_1, d_2) : d_t = \limsup_{\bar{P}\to\infty} \frac{R_{s,t}}{\log_2 \bar{P}}, t = 1, 2\}. \tag{7}$$

The main result of this paper is the following theorem, which we shall prove in the next section.

Theorem 1: Consider the single sided interference channel shown in Figure 1. For this channel model, the s.d.o.f. pair $d_1 = 2/3, d_2 = 1$ is achievable.

Remark 1: The achieved s.d.o.f. region and its relationship with previous results is shown Figure 2. It is interesting to note that simple time sharing is optimal in terms of s.d.o.f. region for the MIMO multiple access wiretap channel [12] where the eavesdropper channel is arbitrarily varying, whereas it is strictly sub-optimal for the interference channel. The insight is that in the interference channel, even though the two transmitters can not protect each other through

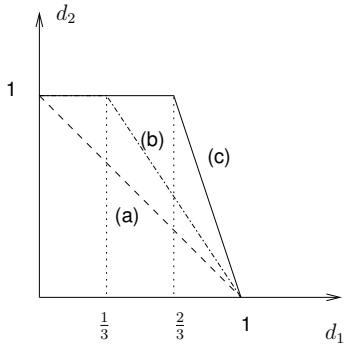

Fig. 2. Achieved Secrecy Degrees of Freedom Region and Its Comparison With Previous Results. (a) Region achieved with simple time sharing. (b) Region achieved in [14]. (c) Region achieved by Theorem 1.

cooperative jamming [5], since the eavesdropper may only receive from one transmitter, these two transmitters still need to coordinate with each other to efficiently utilize the available spatial degrees of freedom.

III. Proof of Theorem 1

A. The Linear Precoding Scheme

Let $\mathbf{v}(x)$ denote the value of the random variable x over M channel uses:

$$\mathbf{v}(x) \triangleq \left[\begin{array}{l} x(i) \\ x(i+1) \\ ... \\ x(i+M-1) \end{array}\right]. \tag{8}$$

Let $diag(\mathbf{A},\mathbf{B})$ denote the block diagonal matrix with matrices $\mathbf{A},\mathbf{B}$ as the diagonal blocks.

$$diag(\mathbf{A},\mathbf{B}) = \left[\begin{array}{ll} \mathbf{A} & \\ & \mathbf{B} \end{array}\right]. \tag{9}$$

Let $diag(\mathbf{v}(\mathbf{H}))$ denote the equivalent channel matrix of $\mathbf{H}$ over M channel uses:

$$diag(\mathbf{v}(\mathbf{H})) = \left[\begin{array}{llll} \mathbf{H}(i) & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \mathbf{H}(i+M-1) \end{array}\right]. \tag{10}$$

Both transmitters perform linear precoding over M channel uses. The inputs to the linear precoder at Transmitter k is denoted by $\mathbf{V}_k$. Transmitter 1 computes $\mathbf{v}(\mathbf{X}_1)$ from $\mathbf{V}_1$ and artificial noise $\mathbf{J}$ using precoding matrix $\mathbf{B}$ and $\mathbf{A}_1$ as

$$\mathbf{v}(\mathbf{X}_1) = \mathbf{B}_{(2M)\times M}\mathbf{V}_{1,M\times 1} + \mathbf{A}_{1,(2M)\times M}\mathbf{J}_{M\times 1}. \tag{11}$$

Transmitter 2 computes $\mathbf{v}(\mathbf{X}_2)$ from $\mathbf{V}_2$ using precoding matrix $\mathbf{A}_2$ as

$$\mathbf{v}(\mathbf{X}_2) = \mathbf{A}_{2,(3M)\times 2M}\mathbf{V}_{2,2M\times 1}. \tag{12}$$

The signals observed by Receiver 1 over M channel uses is given by

$$\mathbf{v}(\mathbf{Y}_1) = \mathbf{v}(\mathbf{H}_{1,1}\mathbf{X}_1) + \mathbf{v}(\mathbf{H}_{2,1}\mathbf{X}_2) + \mathbf{v}(\mathbf{Z}_1) \tag{13}$$

$$= \mathbf{B}\mathbf{V}_1 + \mathbf{A}_1\mathbf{J} + diag(\mathbf{v}(\mathbf{H}_{2,1}))\mathbf{A}_2\mathbf{V}_2 + \mathbf{v}(\mathbf{Z}_1). \tag{14}$$

Receiver 1 uses a matrix $\mathbf{N}_{M\times(2M)}$ to nullify $\mathbf{J}$ and $\mathbf{V}_2$ which must satisfy

$$\mathbf{N}\times\mathbf{A}_1 = \mathbf{0}_{M\times M}, \tag{15}$$

$$\mathbf{N}\times diag(\mathbf{v}(\mathbf{H}_{2,1}))\mathbf{A}_2 = \mathbf{0}_{M\times 2M},, \tag{16}$$

after which it receives

$$\mathbf{N}\mathbf{v}(\mathbf{Y}_1) = \mathbf{N}\mathbf{B}\mathbf{V}_1 + \mathbf{N}\mathbf{v}(\mathbf{Z}_1). \tag{17}$$

The signals observed by Receiver 2 over M channel uses are given by

$$\mathbf{v}(\mathbf{Y}_2) = diag(\mathbf{v}(\mathbf{H}_{2,2}))\mathbf{v}(\mathbf{X}_2) + \mathbf{v}(\mathbf{Z}_2) \tag{18}$$

$$= diag(\mathbf{v}(\mathbf{H}_{2,2}))\mathbf{A}_2\mathbf{V}_2 + \mathbf{v}(\mathbf{Z}_2). \tag{19}$$

Without loss of generality, when proving the messages are secure, we only need to consider two (types of) eavesdroppers [14]: The kth eavesdropper is only receiving from Transmitter k and is only interested in message W_k, $k=1,2$. This is because the condition

$$\lim_{n\to\infty} I\left(W_k; \tilde{\mathbf{Y}}_k^n\right) = 0, k = 1,2 \tag{20}$$

where $\tilde{\mathbf{Y}}_k(i)$ is the signals received by the kth eavesdropper during the ith channel use:

$$\tilde{\mathbf{Y}}_k(i) = \tilde{\mathbf{H}}_k(i)\mathbf{X}_k(i), k = 1,2, \tag{21}$$

implies the secrecy constraint in (6).

Note that $\tilde{\mathbf{H}}_k(i)$ is a 1×2 vector. Without loss of generality, we can assume

$$\tilde{\mathbf{H}}_k(i)^H\tilde{\mathbf{H}}_k(i) = 1, k = 1,2. \tag{22}$$

Over M channel uses, the signals observed by the kth eavesdropper can be written as

$$\mathbf{v}(\tilde{\mathbf{Y}}_k) = diag(\mathbf{v}(\tilde{\mathbf{H}}_k))\mathbf{v}(\mathbf{X}_k), k = 1,2. \tag{23}$$

The corresponding secrecy constraint is given by

$$\lim_{n\to\infty} I\left(W_k; \mathbf{v}(\tilde{\mathbf{Y}}_k)_\gamma^n\right) = 0, \quad \forall\gamma. \tag{24}$$

B. Secrecy of user 2 and achievability of $d_2 = 1$ [14]

The secrecy guarantee for the second user and the achievability of $d_2 = 1$ follows directly from the single-user MIMO wiretap channel. Specifically, from (12) and (23), the signals received by the 2nd eavesdropper over M channel uses can be written as

$$\mathbf{v}(\tilde{\mathbf{Y}}_2) = diag(\mathbf{v}(\tilde{\mathbf{H}}_2))\mathbf{A}_2\mathbf{V}_2. \tag{25}$$

From (25) and (19), we observe the channel connecting Transmitter 2, Receiver 2 and the 2nd eavesdropper is a MIMO wiretap channel with inputs $\mathbf{V}_2$, where the transmitter has $2M$ antennas, the receiver has $2M$ antennas, and the eavesdropper has M antennas. As long as $diag(\mathbf{v}(\mathbf{H}_{2,2}))\mathbf{A}_2$ has full row rank $2M$, which we shall guarantee when choosing $\mathbf{A}_2$, the achieved degrees of freedom for this equivalent channel is $\min\{2M, 2M\} - M = M$ [10], which translates to $d_2 = 1$.

C. Designing $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}, \mathbf{N}$ to achieve $d_1 = 2/3$

Theorem 1 states that the interfered user can have $d_1 = 2/3$. We now demonstrate the achievability of this by designing the precoding matrices that facilitate aligning interference and artificial noise. We observe from (11) and (23) that the signals received by the 1st eavesdropper over M channel uses is given by:

$$\mathbf{v}(\tilde{\mathbf{Y}}_1) = diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B}\mathbf{V}_1 + diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1\mathbf{J}_1. \quad (26)$$

Then we have the following lemma:

Lemma 1: A necessary condition for achieving $d_1 = k/M, d_2 = 1$ using the linear precoding scheme in Section III-A for $0 < k < M$ is that the matrix $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$ has rank k for all possible $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))$ such that $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B}$ has full rank M.

The lemma is proved by first rewriting the eavesdropper channel to a more tractable form by applying singular value decomposition to $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$ and upper bounding the secrecy rate with $I(X;Y|Z)$ for a wiretap channel $\Pr(Y,Z|X)$ where the eavesdropper observes Z. The proof is omitted due to space limitations.

D. An Example

Let us set $M = 3$. Based on Lemma 1, a good $\mathbf{A}_1$ should achieve a high rank for matrix $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$. For $M = 3$, we use the following $\mathbf{A}_1$:

$$\mathbf{A}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}. \quad (27)$$

The reason behind this choice will become apparent by inspecting the rank of $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$. Let $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))$ be denoted by

$$\begin{bmatrix} a & b & & & & \\ & & c & d & & \\ & & & & e & f \end{bmatrix}, \quad (28)$$

where $a, b, ..., f$ are channel gains of the eavesdropper channel subject to the constrain $diag(\mathbf{v}(\tilde{\mathbf{H}}_1)) \times diag(\mathbf{v}(\tilde{\mathbf{H}}_1))^H = \mathbf{I}_{M\times M}$ due to (22). Then $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$ is given by

$$\begin{bmatrix} a & b & \\ & c & d \\ f & & e \end{bmatrix}. \quad (29)$$

Since $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))$ cannot have a row composed entirely of zeros, it is easy to verify (and will be proved later in Lemma 2) that the rank of $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$ is at least 2.

On the other hand, based on the discussion in Section III-A, the matrices $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}, \mathbf{N}$ must satisfy the following requirements to ensure receiver k can recover $\mathbf{V}_k$, $k = 1, 2$:

1) We observe from (17) that $\mathbf{NB}$ needs to have full rank M.
2) The interference from Transmitter 2 and the artificial noise from Transmitter 1 must be aligned at Receiver 1 so that there exists $\mathbf{N}$ to satisfy (15) and (16). This can be achieved by requiring
$$diag(\mathbf{v}(H_{1,1}))\mathbf{A}_1 = diag(\mathbf{v}(H_{2,1}))\mathbf{A}_2. \quad (30)$$
3) From (19), we observe $diag(\mathbf{v}(\mathbf{H}_{2,2}))) \times \mathbf{A}_2$ needs to have rank $2M$.

Requirement 1) can be satisfied by choosing

$$\mathbf{N} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \end{bmatrix} \quad (31)$$

and

$$\mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad (32)$$

for which $\mathbf{NB}$ is an identity matrix.

Define $\mathbf{A}(i:j)$ be the matrix formed by row $i+1, ..., j$ from matrix $\mathbf{A}$. Let $\mathbf{I}_{M\times M}(k)$ be the kth row of an $M \times M$ identity matrix. Then in order to satisfy (30) in the requirement 2), we choose

$$\mathbf{A}_2 = \begin{bmatrix} \mathbf{A}_1(1:2) & 0 \\ 0 & \mathbf{I}_{3\times 3}(1) \\ \mathbf{A}_1(3:4) & 0 \\ 0 & \mathbf{I}_{3\times 3}(2) \\ \mathbf{A}_1(5:6) & 0 \\ 0 & \mathbf{I}_{3\times 3}(3) \end{bmatrix}_{9\times 6}. \quad (33)$$

Then $diag(\mathbf{v}(\mathbf{H}_{1,1}))\mathbf{A}_1 = diag(\mathbf{v}(\mathbf{H}_{2,1}))\mathbf{A}_2$ and

$$diag(\mathbf{v}(\mathbf{H}_{2,2}))\mathbf{A}_2 = \begin{bmatrix} \mathbf{A}_1(2) & 0 \\ 0 & \mathbf{I}_{3\times 3}(1) \\ \mathbf{A}_1(4) & 0 \\ 0 & \mathbf{I}_{3\times 3}(2) \\ \mathbf{A}_1(6) & 0 \\ 0 & \mathbf{I}_{3\times 3}(3) \end{bmatrix} \quad (34)$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (35)$$

Hence $diag(\mathbf{v}(\mathbf{H}_{2,2}))\mathbf{A}_2$ has full rank $2M$ which satisfies the requirement in 3).

To summarize, the eavesdropper channel, when prefixed by the precoding matrix, is given by (26), where $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B}$ is given by

$$\begin{bmatrix} a & & \\ & c & \\ & & e \end{bmatrix}, \quad (36)$$

and $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$ is given by (29). The main channel is obtained by applying the precoding matrices $\mathbf{N}$ and $\mathbf{B}$ to (17) and is given by

$$\mathbf{V}_1 + \mathbf{Z}. \tag{37}$$

with $\mathbf{Z}$ composed of independent rotationally invariant zero mean complex Gaussian random variables whose variance is 2.

Computing the secrecy rate for this channel and proving the existence of a good codebook to achieve this rate directly is difficult. Hence, we next derive a lower bound on the secrecy rate by enhancing the eavesdropper's channel. We consider two cases: (1) $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B}$ is non-singular, i.e., $a \neq 0, c \neq 0, e \neq 0$. (2) $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B}$ is singular. We show that for both cases, the eavesdropper channel after enhancement takes the following form:

$$\sqrt{2}\mathbf{U}_c^H\mathbf{V}_1 + diag(\mathbf{I}_{2\times 2}, 0)\mathbf{J}. \tag{38}$$

where $\mathbf{J}$ is a $M \times 1$ composed of zero mean independent complex rotational invariant Gaussian variable with unit variance.

We first consider the non-singular case. Define $\mathbf{H}_c$ as

$$\mathbf{H}_c = (diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B})^{-1} diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1 \tag{39}$$

$$= \begin{bmatrix} 1 & b/a & \\ & 1 & d/c \\ f/e & 0 & 1 \end{bmatrix}, \tag{40}$$

and (26) can be written as:

$$\mathbf{V}_1 + \mathbf{H}_c\mathbf{J}_1. \tag{41}$$

For $\mathbf{H}_c$ we have the following lemma:

Lemma 2: The second smallest singular value of $\mathbf{H}_c$ is lower bounded by $1/\sqrt{2}$.

Proof: The proof is given in Appendix A. ■

Let $\mathbf{U}_c, \mathbf{D}_c, \mathbf{W}_c$ be the singular value decomposition of $\mathbf{H}_c$, such that $\mathbf{H}_c = \mathbf{U}_c\mathbf{D}_c\mathbf{W}_c$, $\mathbf{D}_c$ is the diagonal matrix, and $\mathbf{U}_c, \mathbf{W}_c$ are unitary matrices. Then (41) can be re-written as:

$$\mathbf{U}_c^H\mathbf{V}_1 + \mathbf{D}_c\mathbf{W}_c\mathbf{J}_1 \tag{42}$$

Again, since $\mathbf{W}_c\mathbf{J}_1$ has the same distribution as $\mathbf{J}_1$, we can rewrite (42) as

$$\mathbf{U}_c^H\mathbf{V}_1 + \mathbf{D}_c\mathbf{J}_1. \tag{43}$$

Then using Lemma 2, the diagonal element of $\mathbf{D}_c$ is either 0 or is at least $1/\sqrt{2}$. Since the diagonal elements on $\mathbf{D}_c$ are sorted, only the diagonal element on the third row of $\mathbf{D}_c$ can be 0. Hence we can enhance the eavesdropper channel to (38).

We next consider $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B}$ being singular.

1) Consider the case that a, c, e contain at least two zeros. Assume $c = 0, e = 0$. Then the signals observed by the eavesdropper is a noisy copy of the first component of $\mathbf{V}_1$ (or 0 if a is also zero), which is degraded with respect to (38) when $\mathbf{U}_c^H$ equals

$$\begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix}. \tag{44}$$

The case where $a = 0, c \neq 0, e = 0$ and $a = 0, c = 0, e \neq 0$ can proved similarly dual to the symmetric structure of $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{B}$ and $diag(\mathbf{v}(\tilde{\mathbf{H}}_1))\mathbf{A}_1$

2) Consider the case that a, c, e contain exactly one zero. We describe the proof for $e = 0, a \neq 0, c \neq 0$. The other two cases $c = 0, a \neq 0, e \neq 0$ and $a = 0, c \neq 0, e \neq 0$ can be proved in a similar fashion. Then the eavesdropper receives:

$$\begin{bmatrix} a & & \\ & c & \\ & & 0 \end{bmatrix}\mathbf{V}_1 + \begin{bmatrix} a & b & \\ & c & d \\ f & & 0 \end{bmatrix}\mathbf{J}_1 \tag{45}$$

Since the three components of $\mathbf{J}_1$ are independent from each other, (45) can be enhanced to

$$\begin{bmatrix} a & \\ & c \end{bmatrix}\begin{bmatrix} V_{1,1} \\ V_{1,2} \end{bmatrix} + \begin{bmatrix} b & 0 \\ c & d \end{bmatrix}\begin{bmatrix} J_{1,2} \\ J_{1,3} \end{bmatrix}, \tag{46}$$

where $V_{1,j}$ and $J_{1,j}$ are the jth components of $\mathbf{V}_1$ and $\mathbf{J}_1$ respectively. It can be enhanced to

$$\begin{bmatrix} a & \\ & c \end{bmatrix}\begin{bmatrix} V_{1,1} \\ V_{1,2} \end{bmatrix} + \begin{bmatrix} b \\ c \end{bmatrix} J_{1,2}, \tag{47}$$

which can be written as

$$\begin{bmatrix} V_{1,1} \\ V_{1,2} \end{bmatrix} + \begin{bmatrix} b/a \\ 1 \end{bmatrix} J_{1,2}. \tag{48}$$

We then perform singular value decomposition on $[b/a, 1]^T$:

$$\begin{bmatrix} b/a \\ 1 \end{bmatrix} = \mathbf{U}_{2\times 2}\begin{bmatrix} \sqrt{|b/a|^2+1} \\ 0 \end{bmatrix}\mathbf{V}_{1\times 1}, \tag{49}$$

and rewrite (48) as:

$$\begin{bmatrix} V_{1,1} \\ V_{1,2} \end{bmatrix} + \mathbf{U}\begin{bmatrix} \sqrt{|b/a|^2+1} \\ 0 \end{bmatrix} J, \tag{50}$$

which can be enhanced to

$$\begin{bmatrix} V_{1,1} \\ V_{1,2} \end{bmatrix} + \mathbf{U}\begin{bmatrix} 1 \\ 0 \end{bmatrix} J. \tag{51}$$

(51) can be rewritten as:

$$\mathbf{U}^H\begin{bmatrix} V_{1,1} \\ V_{1,2} \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} J, \tag{52}$$

which can be enhanced to

$$\begin{bmatrix} \mathbf{U}^H & \\ & 1 \end{bmatrix}\begin{bmatrix} V_{1,1} \\ V_{1,2} \\ V_{1,3} \end{bmatrix} + \begin{bmatrix} J_1 \\ 0 \\ J_2 \end{bmatrix}. \tag{53}$$

(53) can be written as:

$$\begin{bmatrix} \mathbf{U}^H & \\ & 1 \end{bmatrix}\begin{bmatrix} V_{1,1} \\ V_{1,2} \\ V_{1,3} \end{bmatrix} + \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix}\begin{bmatrix} J_1 \\ J_2 \\ 0 \end{bmatrix}, \tag{54}$$

which can be rewritten as

$$\begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix}^H\begin{bmatrix} \mathbf{U}^H & \\ & 1 \end{bmatrix}\mathbf{V} + diag(\mathbf{I}_{2\times 2}, 0)\mathbf{J} \tag{55}$$

which is a degraded version of (38).

Hence we have shown that the secrecy rate of the first user is always lower bounded by the wiretap channel where the eavesdropper channel is given by (38) and the main channel is given by (37). This is a special case of the MIMO wiretap channel described in the next section, in which we shall derive an achievable secrecy rate for this channel and complete the proof of the achievability of $d_2 = 2/3$ and hence Theorem 1.

IV. MIMO WIRETAP CHANNEL WHERE THE EAVESDROPPER CHANNEL STATE IS ARBITRARILY VARYING REVISITED

In this section, we extend the MIMO wiretap channel studied in [10] in that eavesdropper could have the same number of antennas as the legitimate node, but could observe high level of noise at some of its receiving antennas. It turns out the wiretap channel considered in the previous section is a special case of this model. The main channel and the eavesdropper channel for this model are given below

$$\mathbf{Y}_{M\times 1}(i) = \mathbf{X}_{M\times 1}(i) + \mathbf{Z}_{M\times 1}(i) \tag{56}$$

$$\tilde{\mathbf{Y}}(i) = \mathbf{U}(i)_{M\times M}\mathbf{X}(i) + \mathbf{J}(i) \tag{57}$$

where $\mathbf{J}(i)$ denote the noise observed by the eavesdropper. $\mathbf{J}(i)$ is composed of M independent zero mean rotationally invariant Gaussian random variable. The variance of the jth component of $\mathbf{J}(i)$ is $\sigma_j^2 > 0$. $\mathbf{U}(i)$ is always a unitary matrix. It is arbitrarily varying over different channel uses and is independent from channel inputs $\mathbf{X}(i)$. $\mathbf{Z}(i)$ denotes the additive channel noise composed of zero mean rotationally invariant Gaussian random variable whose variance is σ^2. The average power of the transmitter can not exceed P.

For this channel, we have the following theorem.

Theorem 2: Define $P' = P/M$ and $C(x) = \log_2(1+x)$. The following secrecy rate is achievable the wiretap channel given in (56) and (57):

$$\max\{0, MC(\frac{P'}{\sigma^2}) - \sum_{j=1}^{M} C(\frac{P'}{\sigma_j^2})\} \tag{58}$$

Proof: The proof is similar to the derivation in [10]. In Appendix B, we provide an outline of the proof and highlight the proof steps that differ from those in [10]. ∎

To apply Theorem 2 to the wiretap channel model (37) and (37), we allocate $\bar{P}/3$ power to each transmit antenna. At each antenna, P' power is used to transmit Gaussian artificial noise through $\mathbf{J}$, P' power is used to transmit $\mathbf{V}$, and one unit of power is used to transmit Gaussian noise in order to satisfy the condition $\sigma_j^2 > 0$. This means P' must satisfy $6P' + 3 \leq \bar{P}$. Applying Theorem 2, an achievable secrecy rate for the wiretap channel model (37) and (37) is:

$$R_1 = \max\{0, 3C(\frac{P'}{3}) - C(P') - 2C(\frac{P'}{P'+1})\} \tag{59}$$

which implies $d_1 = \lim_{\bar{P}\to\infty} R_1/\log_2(\bar{P}) = 2/3$.

V. CONCLUSION

In this work, we studied a class of single-sided two user Gaussian interference channels where the transmitters have 2 or 3 antennas, the receivers have 2 antennas, and the eavesdropper has 1 antenna. The eavesdropper channel is arbitrarily varying and its state sequence is known to the eavesdropper only. We improved our earlier results and showed that a strongly secure degrees of freedom pair $(d_1 = 2/3, d_2 = 1)$ is achievable. This is accomplished by aligning artificial noise with user interference through linear precoding, and designing the linear precoding matrix through a rank criterion.

APPENDIX A
PROOF FOR LEMMA 2

Let s_i be the ith largest singular value of $\mathbf{H}_c$, $i = 1, 2, 3$. Since $diag(\mathbf{v}(\tilde{\mathbf{H}}_1)) * diag(\mathbf{v}(\tilde{\mathbf{H}}_1))^H = \mathbf{I}_{M\times M}$, we have:

$$\sum_{i=0}^{2} |s_i|^2 = \text{trace}(\mathbf{H}_c^H \mathbf{H}_c) = \frac{1}{|a|^2} + \frac{1}{|c|^2} + \frac{1}{|e|^2}. \tag{60}$$

On the other hand, for s_1, we have:

$$|s_1|^2 = \max_{\mathbf{u}} \|\mathbf{H}_c\mathbf{u}\|^2, \tag{61}$$

subject to the constraint:

$$\|\mathbf{u}\|^2 = 1. \tag{62}$$

Let $\mathbf{u} = [u_1, u_2, u_3]^T$ be the optimal solution to this optimization problem. Then

$$\mathbf{H}_c\mathbf{u} = \begin{bmatrix} \frac{au_1+bu_2}{a} \\ \frac{cu_2+du_3}{c} \\ \frac{fu_1+eu_3}{e} \end{bmatrix} \tag{63}$$

And

$$|s_1|^2 = \|H_c u\|^2 \tag{64}$$

$$\leq \frac{(|a|^2+|b|^2)(|u_1|^2+|u_2|^2)}{|a|^2} + \frac{(|c|^2+|d|^2)(|u_2|^2+|u_3|^2)}{|c|^2} + \frac{(|e|^2+|f|^2)(|u_1|^2+|u_3|^2)}{|e|^2} \tag{65}$$

$$= \frac{|u_1|^2+|u_2|^2}{|a|^2} + \frac{|u_2|^2+|u_3|^2}{|c|^2} + \frac{|u_1|^2+|u_3|^2}{|e|^2} \tag{66}$$

From $|u_1|^2 + |u_2|^2 + |u_3|^2 = 1$, (60) and the upper bound on $|s_1|^2$ given by (66), we have

$$|s_2|^2 + |s_3|^2 \geq \frac{|u_3|^2}{|a|^2} + \frac{|u_1|^2}{|c|^2} + \frac{|u_2|^2}{|e|^2} \tag{67}$$

Note that $\max\{|a|, |c|, |e|\} \leq 1$. Hence (67) is greater than or equal to

$$|u_3|^2 + |u_1|^2 + |u_2|^2 = 1 \tag{68}$$

Since $|s_2| \geq |s_3|$, we have

$$2|s_2|^2 \geq |s_2|^2 + |s_3|^2 \geq 1 \tag{69}$$

Hence $|s_2|^2 \geq 1/2$ and we have proved the lemma.

APPENDIX B
PROOF OUTLINE FOR THEOREM 2

A. Codebook Generation, Encoders and Decoders

The codebook generation, encoding and decoding steps are identical to [10], which we shall summarize below for completeness: The input distribution $Q_{\mathbf{X}^n}(x^n)$ is a truncated Gaussian distribution, which is given by:

$$Q_{\mathbf{X}^n}(x^n) = \mu_{n,\varepsilon_P}^{-1} \varphi(x^n) \prod_{i=1}^{n} Q_{\mathbf{X}}(x_i) \tag{70}$$

where $Q_{\mathbf{X}}(x)$ is an M-dimensional rotationally invariant zero mean complex Gaussian distribution with covariance matrix $(\frac{P(1-\varepsilon_P)}{M})\mathbf{I}_{M\times M}$ for $\varepsilon_P > 0$, and

$$\varphi(x^n) = \begin{cases} 1, & \text{if } \frac{1}{n}\|x^n\|^2 \le P \\ 0, & \text{otherwise} \end{cases} \tag{71}$$

$$\mu_{n,\varepsilon_P} = \int \varphi(x^n) \prod_{i=1}^{n} Q_{\mathbf{X}}(x_i) dx^n \tag{72}$$

Any codebook in the ensemble is constructed by sampling 2^{nR} sequences from the distribution $Q_{\mathbf{X}^n}$ in an independent and identically distributed (i.i.d.) fashion. R is chosen as

$$R = I(\mathbf{X};\mathbf{Y}) - \delta' \tag{73}$$

The mutual information in (73) is evaluated when $\mathbf{X}$ has distribution $Q_{\mathbf{X}}$. δ' is a positive constant that can be arbitrarily small and is included to ensure decodability of the message at the intended receiver.

Each time we sample a codeword, we label it with (i,j). Define N_i and N_j as the range of i and j. They are:

$$N_i = 2^{n(R-I(\mathbf{X};\tilde{\mathbf{Y}})-\delta_n)} \tag{74}$$

$$N_j = 2^{n(I(\mathbf{X};\tilde{\mathbf{Y}})+\delta_n)} \tag{75}$$

$\{\delta_n\}$ is a positive sequence included to ensure the rate of the sub-codebook, composed of codewords with same index i, exceeds the mutual information of the eavesdropper $I(\mathbf{X};\tilde{\mathbf{Y}})$, which will lead to strong secrecy. $I(\mathbf{X};\tilde{\mathbf{Y}})$ is evaluated when $\mathbf{X}$ has distribution $Q_{\mathbf{X}}$, and we drop the subscript γ in this expression since the value of the mutual information does not depend on γ when $\mathbf{X}$ has the distribution $Q_{\mathbf{X}}$.

Let $\mathcal{C}$ denote a codebook in the codebook ensemble $\{\mathcal{C}\}$. Let $x_{i,j}^n$ denote the codeword in the codebook $\mathcal{C}$ that is labeled with (i,j).

The coding scheme uses $K = e^{2\varepsilon' n}$ such codebooks, where ε' is a positive constant that can be made arbitrarily small. As we shall see, more than one codebooks are used to ensure the probability that a bad codebook is used for the given eavesdropper channel state sequence is negligible. Let the confidential message W be uniformly distributed over the set of $\{1,...,N_i\}$. The encoder f_n used by the transmitter is described as follows:

1) In the first stage, the transmitter chooses the value for an integer K' from $\{1,...,K\}$ according to a uniform distribution. Given $W = i$, f_n outputs the label (i,j) computed by $f_{n,\mathcal{C}_{K'}}$ defined as: Given $W = i$, $f_{n,\mathcal{C}}$ selects a codeword from all the codewords with label i in codebook $\mathcal{C}$ according to a uniform distribution.
2) In the second stage, K' is transmitted to the intended receiver using a good codebook for the main channel.

The decoder of the intended receiver first decode K', then decode the confidential message using a maximum likelihood decoder $\psi_{\mathcal{C}_{K'}}$: Upon receiving $\mathbf{Y}^n = y^n$, the decoder $\psi_{\mathcal{C}}(y^n)$ is given by

$$\psi_{\mathcal{C}}(y^n) = \arg \max_{i,j:x_{i,j}^n \in \mathcal{C}} \|y^n - \mathbf{H}^n x^n\|. \tag{76}$$

B. Notations and Definitions

Let $\mathbf{X}_G^n$ denote $\mathbf{X}^n$ when it is sampled in an i.i.d. fashion from the input distribution $Q_{\mathbf{X}}(x)$ instead of the codebook. Let $\mathbf{X}_T^n$ denote $\mathbf{X}^n$ when it is sampled in an i.i.d. fashion from the n-letter truncated Gaussian input distribution $Q_{\mathbf{X}^n}$ instead of the codebook.

Let $\tilde{\mathbf{Y}}_G^n, \tilde{\mathbf{Y}}_T^n, \tilde{\mathbf{Y}}_{\mathcal{C}}^n$ denote $\tilde{\mathbf{Y}}^n$ when $\mathbf{X}^n$ is $\mathbf{X}_G^n$, $\mathbf{X}_T^n$ or uniformly distributed over the codebook $\mathcal{C}$ respectively.

Define normalized variational distance $d'_{\gamma,\mathcal{C}}$ as:

$$d'_{\gamma,\mathcal{C}} = \frac{1}{2}\sum_w p_W(w) \int_{z^n} |f_{\gamma,\tilde{\mathbf{Y}}_G^n}(z^n) - f_{\gamma,\tilde{\mathbf{Y}}_{\mathcal{C}}^n|W}(z^n|w)| dz^n \tag{77}$$

Define information density [15], $i_{\gamma,\mathbf{X}_G^n\tilde{\mathbf{Y}}_G^n}\left(\mathbf{X}^n,\tilde{\mathbf{Y}}^n\right)$, as :

$$i_{\gamma,\mathbf{X}_G^n\tilde{\mathbf{Y}}_G^n}\left(\mathbf{X}^n,\tilde{\mathbf{Y}}^n\right) = \log_2 \frac{\prod_{i=1}^{n} f_{\gamma,\tilde{\mathbf{Y}}|\mathbf{X}}\left(\tilde{\mathbf{Y}}_i|\mathbf{X}_i\right)}{f_{\gamma,\tilde{\mathbf{Y}}_G^n}\left(\tilde{\mathbf{Y}}^n\right)} \tag{78}$$

C. Secrecy Analysis

We shall prove secrecy by proving the variational distance is small. This takes four steps:

1) In the first step, we prove for any given sequence of the eavesdropper channel states, the variational distance averaged over an ensemble of codebooks decreases uniformly and exponentially fast with respect to the code length n.
2) In the second step, we quantize the eavesdropper channel state matrix to a finite set. We show that when the eavesdropper channel state sequence is outside the finite set, the variational distance can be approximated by the variational distance computed using the quantized value of the eavesdropper channel state sequence.
3) Using the results from the first two steps, we show that there exists a small number of codebooks in the codebook ensemble such that the variational distance averaged over these codebooks decreases exponentially fast with respect to n, regardless of whether the eavesdropper channel state sequence falls inside or outside the set of quantized channel state sequences.
4) Finally, a small variational distance (averaged over the small number of codebooks) implies that the secrecy constraint measured by mutual information is satisfied when it decreases exponentially fast with respect to n [16, Lemma 1] [10], which leads to the Theorem 2.

Only step one and two depends on the eavesdropper channel and their proofs need to be modified from [10]. The change in the first step can be summarized by the following lemma. We omit the proof due to space limits.

Lemma 3: For a given $\varepsilon > 0$, if for all n, $\delta_n \geq \varepsilon$, then there exists a constant $\alpha'(\varepsilon) > 0$, such that

$$\Pr\left[\frac{1}{n} i_{\gamma, \mathbf{X}_G^n \tilde{\mathbf{Y}}_G^n}\left(\mathbf{X}_G^n, \tilde{\mathbf{Y}}_G^n\right) > I\left(\mathbf{X}_G; \tilde{\mathbf{Y}}_G\right) + \delta_n\right] \leq e^{-n\alpha'(\varepsilon)} \tag{79}$$

In [10], this lemma was proved for the eavesdropper channel has the following form:

$$\tilde{\mathbf{Y}}(i) = \left[\begin{array}{cc} \mathbf{I}_{k\times k} & 0 \end{array}\right]_{k\times M} \mathbf{U}(i)\mathbf{X}(i) + \mathbf{J}(i) \tag{80}$$

where each component of $\mathbf{J}(i)$ has variance $\sigma_j^2 = 1$. Here it needs to be proved for the eavesdropper channel in (57).

Then using Lemma 3 and following identical proof steps in [10], we can prove that for a positive constant c', the normalized variational distance averaged over the codebook ensemble $\{\mathcal{C}\}$ is bounded as:

$$E_{\mathcal{C}}\left[d'_{\gamma,\mathcal{C}}\right] \leq \exp\left(-c'n\right), \tag{81}$$

which concludes the first step.

In the second step, we construct the finite set $S_{\mathcal{M}}$ of quantized eavesdropper channel state values as follows, where $\mathcal{M}$ is a positive integer that controls the quantization steps.

Recall that the eavesdropper channel state matrix $\tilde{\mathbf{H}}$ is a unitary matrix here and hence the absolute value of the real and imaginary parts of its element cannot exceed 1. Define $\bar{\mathbf{H}}$ as any matrix such that $\mathcal{M}\bar{\mathbf{H}}$ is composed of elements with integral real and imaginary parts taking values in the set $\{-\mathcal{M}, -\mathcal{M}+1, ..., \mathcal{M}-1\}$. For such a $\bar{\mathbf{H}}$, define a hyper-cube over $M \times M$ matrices, denoted by $\mathrm{cube}_{\bar{\mathbf{H}}}$, as

$$\mathrm{cube}_{\bar{\mathbf{H}}} = \left\{ \begin{array}{ll} \mathbf{H}: & 0 \leq \mathrm{Re}(\mathcal{M}\mathbf{H}_{i,j} - \mathcal{M}\bar{\mathbf{H}}_{i,j}) \leq 1 \\ & 0 \leq \mathrm{Im}(\mathcal{M}\mathbf{H}_{i,j} - \mathcal{M}\bar{\mathbf{H}}_{i,j}) \leq 1 \end{array} \right\} \tag{82}$$

$\cup_{\bar{\mathbf{H}}}\mathrm{cube}_{\bar{\mathbf{H}}}$ contains all matrices whose elements' real and imaginary parts are within interval $[-1, 1]$. Within each $\mathrm{cube}_{\bar{\mathbf{H}}}$, we choose *any single* unitary matrix $\tilde{\mathbf{H}}$ *if it exists* and include it in $S_{\mathcal{M}}$. Then $S_{\mathcal{M}}$ is a finite set with at most $(2\mathcal{M}+1)^{2M^2}$ unitary matrices. [1] Then we have the following lemma:

Lemma 4: Define r', r such that $r'^2 = 2M^2P/\mathcal{M}^2$ and

$$r = r' + \sqrt{\sum_{j=1}^{M} \sigma_j^2(1+\varepsilon)} \tag{83}$$

Define $g(r, r')$ as

$$g(r, r') = r'(2r + r') \tag{84}$$

if we can choose $\mathcal{M}$ with respect to n such that

$$ng(r, r') < 1 \tag{85}$$

then there must exist $\gamma' \in S_{\mathcal{M}}$ such that

$$d'_{\gamma,\mathcal{C}} \leq d'_{\gamma',\mathcal{C}} + e^{-n\alpha(\varepsilon)} + ng(r, r'). \tag{86}$$

[1] $S_{\mathcal{M}}$ is not empty since it at least contains the matrix $\mathbf{I}_{M\times M}$.

This is the same lemma as [10, Lemma 7] except that the definition of r is changed to (83) to reflect a different variance in the noise term. The proof is identical to [10, Lemma 7] and hence will not be repeated here. This concludes the second step.

Using (81) and Lemma 4, following identical proofs in [10], it can be shown that there exists K codebooks $\{\mathcal{C}_k\}$ such that for a positive constant ε',

$$\frac{1}{K}\sum_{k=1}^{K} d'_{\gamma,\mathcal{C}_k} < 3e^{-n\varepsilon'} \tag{87}$$

and each codebook leads to vanishing probability of decoding error. These K codebooks are then used by the coding scheme described in Section B-A. The secrecy constraint (24) is implied by (87) through [16, Lemma 1], which completes the proof of Theorem 2.

REFERENCES

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

[2] R. Liu and W. Trappe. *Securing Wireless Communications at the Physical Layer*. Springer, 2009.

[3] Y. S. Khiabani and S. Wei. Creation of degraded wiretap channel through deliberate noise in block ciphered systems. In *IEEE Global Telecommunication Conference, Workshop on Physical Layer Security*, December 2011.

[4] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions. *IEEE Transactions on Information Theory*, 54(6):2493–2507, June 2008.

[5] 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*, 54(6):2735–2751, June 2008.

[6] 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.

[7] X. He and A. Yener. The Gaussian Many-to-One Interference Channel with Confidential Messages. *IEEE Transactions on Information Theory*, 57(5):2730–2745, 2011.

[8] E. Ekrem and S. Ulukus. Degraded Compound Multi-receiver Wiretap Channels. *IEEE Transactions on Information Theory*, 58(9):5699–5710, 2012.

[9] 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.

[10] 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.

[11] 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.

[12] X. He, A. Khisti, and A. Yener. MIMO Multiple Access Channel with an Arbitrarily Varying Eavesdropper. Submitted to the IEEE Transactions on Information Theory, February, 2012, available online at http://arxiv.org/abs/1203.1376.

[13] 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.

[14] X. He and A. Yener. The Gaussian Interference Wiretap Channel When the Eavesdropper Channel is Arbitrarily Varying. In *IEEE International Symposium on Information Theory*, July 2012.

[15] T. S. Han and S. Verdú. Approximation theory of output statistics. *IEEE Transactions on Information Theory*, 39(3):752–772, 1993.

[16] I. Csiszár. Almost Independence and Secrecy Capacity. *Problems of Information Transmission*, 32(1):48–57, 1996.