MIMO Broadcast Channel with Arbitrarily Varying Eavesdropper Channel: Secrecy Degrees of Freedom

Xiang He*, Ashish Khisti†, Aylin Yener*

* Electrical Engineering Department, The Pennsylvania State University, University Park, PA 16802
†Dept. of Electrical and Computer Engineering, University of Toronto, Toronto, ON, M5S 3G4, Canada
xxh119@psu.edu, akhisti@comm.utoronto.ca, yener@psu.edu

***Abstract*—A two-receiver MIMO broadcast-wiretap channel is considered where the channel state of the eavesdropper is arbitrarily varying. It is assumed that the eavesdropper knows this channel state perfectly whereas the legitimate nodes have no knowledge of it. It is further assumed that the eavesdropper experiences no additive noise. The channel between the transmitter and the two legitimate receivers is a constant MIMO Gaussian broadcast channel. This paper establishes the secrecy degrees of freedom region for transmitting a common-confidential message as well as a private-confidential message to each receiver. It is observed that a straightforward extension of single user random binning does not achieve the optimal secrecy degrees of freedom (s.d.o.f.) region. The proposed coding scheme that achieves the s.d.o.f. region involves simultaneous diagonalization of the channel matrices of the two legitimate receivers using the generalized singular value decomposition (GSVD) as well as a particular *structured binning* across codebooks that minimizes the rate of the fictitious message. While the focus is on achieving weak secrecy for ease of exposition, an outline is provided on how the results can be extended for achieving strong secrecy.**

I. Introduction

All secrecy schemes are based on a small set of reasonable assumptions. The approach of studying secrecy problems using information theory was first studied by Shannon in [1] and was later extended to different network models, see for example, [2]–[6]. The distinctive feature of this approach is that instead of assuming the adversary is computationally limited as in the case of computational security, secrecy is achieved relying solely on assumptions on the communication network, usually described in terms of network topology, channel states or the signal to noise ratio, allowing the adversary to be computationally unlimited. Such an approach therefore establishes the fundamental limits for secure communication rates, and identifies properties inherent to the communication network that can be leveraged to achieve positive secrecy rates for legitimate communication parties.

The possibility of achieving secure communication using multiple antennas has been studied extensively in literature. Most works assume (partial) knowledge of the eavesdropper channel state information and characterize the rates at which secure communication can take place, see [7]–[10] for example.

Since the eavesdropper does not transmit and hence its channel states are hard to obtain for legitimate communication parties, recent works [11], [12] have started to consider the case where the eavesdropper channel is arbitrarily varying and its channel states are known to the eavesdropper *only*. Reference [12] has studied the single-user Gaussian MIMO wiretap channel and found its secrecy degrees of freedom, which is a high SNR characterization of the capacity of this model. Reference [12] has also provided the secrecy degrees of freedom region for a two-receiver Gaussian MIMO broadcast channel where each legitimate node has the same number of antennas, which is obtained as a straightforward extension of the single user case. In both cases, only the number of antennas employed by the eavesdropper is known to the transmitter. This assumption can be justified for the scenarios where the eavesdropping device is small and hence is unlikely to employ more than a certain number of antennas.

In this work, we consider the general setting where the nodes have any number of antennas and characterize the secrecy degrees of freedom region for the two-receiver Gaussian MIMO broadcast channel. The achievability proof is not a straightforward extension of [12] which involves constructing a vector codebook sampled in an i.i.d. fashion and random binning. A direct construction of two codebooks in this manner introduces an independent randomization for each codebook and creates higher than necessary interference between the legitimate users. Instead, our approach involves carefully transmitting a fictitious message, of just enough rate, in a common subspace between the two users so that it can be simultaneously useful for providing secrecy for *both* users. This scheme can be viewed as inducing a structured binning of the codebooks to minimize the size of each bin.

II. System Model

We consider a MIMO Broadcast (BC) wiretap channel with two receivers, as shown in Figure 1. We assume that the transmitter has N_T antennas. For $t = 1, 2$, receiver t has N_{R_t} antennas, The eavesdropper has N_E antennas. During the ith channel use, the channel is:

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

$$\tilde{\mathbf{Y}}(i) = \tilde{\mathbf{H}}(i)\mathbf{X}(i) \tag{2}$$

where $\mathbf{Y}_t(i), t = 1, 2$ denote the signals received at the legitimate receivers, and $\tilde{\mathbf{Y}}(i)$ denotes the received signal at the eavesdropper. $\mathbf{H}_t, t = 1, 2$ and $\tilde{\mathbf{H}}(i)$ 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. $\tilde{\mathbf{H}}(i)$ is unknown to the legitimate parties. $\mathbf{H}_t, t = 1, 2$ are known by both the legitimate parties and the eavesdropper(s).[1]

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

Each receiver t receives a confidential message W_t, and a common confidential message W_0 from the transmitter over $\bar{n}$ channel uses. W_0, W_1, W_2 must be kept confidential from the eavesdropper. Let $\mathcal{W}_i, i = 0, 1, 2$ denote the alphabet for W_i. $|\mathcal{W}_i|$ denotes the cardinality of $\mathcal{W}_i$.

The average power constraint for the transmitter is

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

We assume the eavesdropper channel state information sequence $\{\tilde{\mathbf{H}}(i)\}$ is independent from $\mathbf{X}$. In this case, as shown in [12], the secrecy constraint can be defined as:

$$\lim_{\bar{n}\to\infty} I\left(W_0, W_1, W_2; \tilde{\mathbf{Y}}_\gamma^{\bar{n}}\right) = 0, \quad \forall\gamma \tag{4}$$

where γ is used to index the eavesdropper channel state sequence. We require the limit in (4) to be uniform over all possible sequences of eavesdropper channel states [12].

The secrecy rate for the message W_i, $R_{s,i}$, is defined as $R_{s,i} = \lim_{\bar{n}\to\infty} \frac{1}{\bar{n}} H(W_i), i = 0, 1, 2$ such that $\{W_0, W_t\}$ can be reliably decoded by receiver t, $t = 1, 2$.

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:

$$\{(d_0, d_1, d_2) : d_i = \limsup_{\bar{P}\to\infty} \frac{R_{s,i}}{\log_2 \bar{P}}, i = 0, 1, 2\} \tag{5}$$

III. Main Result

Theorem 1: Let r_1, r_2 be the rank of $\mathbf{H}_1$ and $\mathbf{H}_2$ respectively. Let r_0 be the rank of $[\mathbf{H}_1^T, \mathbf{H}_2^T]^T$. The secrecy degrees of freedom region for the MIMO broadcast wiretap channel in Figure 1 is given by

$$0 \leq d_j, \quad j = 0, 1, 2 \tag{6}$$

$$0 \leq d_0 + d_i \leq \max\{0, r_i - N_E\}, i = 1, 2 \tag{7}$$

$$0 \leq d_0 + d_1 + d_2 \leq \max\{0, r_0 - N_E\} \tag{8}$$

Remark 1: The result here can be viewed as a Gaussian model counterpart of [13] that establishes the secrecy degrees of freedom for a class of deterministic memoryless broadcast channels. However, the result in [13] is based on the use of rank metric codes and does not generalize to Gaussian channels. We also observe that when $N_E = 0$, i.e., there is no eavesdropper, the result here can be shown to be equivalent to the rate region derived in [14] by applying Fourier-Motzkin elimination on [14, (50)-(53)], the constraints on η, δ below [14, (50)-(53)], and $d_i \geq 0, i = 0, 1, 2$. □

[1]Since the eavesdropper channel is arbitrarily varying, the model includes the case of having any number of non-colluding eavesdroppers.

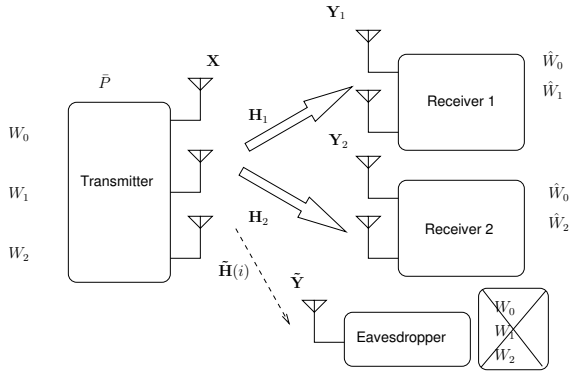

Fig. 1. The MIMO Broadcast Wiretap Channel where $N_T = 3, N_{R_1} = N_{R_2} = 2, N_E = 1$.

IV. Motivating Example: $3 \times 2 \times 2 \times 1$ Channel

Consider the example in Figure 1 where $N_t = 2$, $N_E = 1$ and $N_{R_1} = N_{R_2} = 2$. Assume that $r_1 = r_2 = 2$ and $r_0 = 3$. As we discuss in the sequel, after an appropriate transformation, the channel matrices of the two legitimate receivers reduce to:

$$\mathbf{H}_1 = [\mathbf{I}_{(2\times2)}, \mathbf{0}_{(2\times1)}], \quad \mathbf{H}_2 = [\mathbf{0}_{(2\times1)}, \mathbf{I}_{(2\times2)}] \tag{9}$$

while the effective channel matrix of the eavesdropper is an arbitrary rank one matrix. Reference [12] shows that there exists a codebook $\mathcal{C}_1$ that can be transmitted over the first and the second antenna to achieve $d_1 = 1$, and there exists a codebook $\mathcal{C}_2$ that can be transmitted over the second and the third antenna to achieve $d_2 = 1$. However, since W_1 and W_2 are independent, the signals that $\mathcal{C}_1$ uses to represent W_1 over the second antenna in general do not agree with the signals that $\mathcal{C}_2$ uses to represent W_2 over this antenna, causing a conflict. Thus, we need to construct a new scheme.

Our proposed scheme resolves this conflict by constructing three codebooks, one for each link. A codebook on the second link $\mathcal{C}_E$ is used to transmit a fictitious message W_E via a codeword $X_E^n(W_E)$. An independent codebook on the first link $\mathcal{C}_1$, of twice the rate, is used to transmit a codeword $X_1^n(W_E, W_1)$ while another codebook $\mathcal{C}_2$ on the third link is used to transmit a codeword $X_2^n(W_E, W_2)$. It can be verified that both users 1 and 2 can decode (W_1, W_E) and (W_2, W_E) respectively whereas the secrecy analysis reveals that both (W_1, W_2) are protected from the eavesdropper. In the next section we generalize this scheme to arbitrary number of antennas and a common message W_0.

Note that the proposed construction has three independent messages. In contrast, the naive extension of single-user random binning consists of four independent mes-

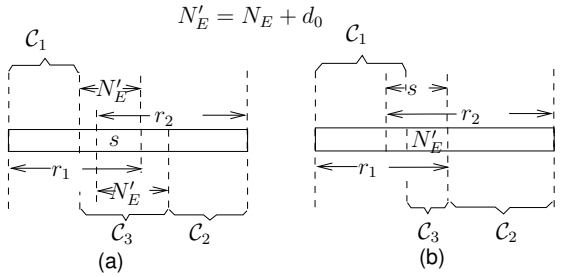

Fig. 2. Codebook generation: (a) $s \leq N_E < \min\{r_1, r_2\}$ (b) $0 < N_E < s$

sages: one message for each user and one message from random codeword selection in each bin and forces the users to decode more information than is necessary. Our construction induces structured binning across the codebooks: given a choice of messages w_0, w_1, w_2 the bin index B_{w_0,w_1,w_2} consists of all sequences of the form $\left\{\bigcup_{w_E}(x_1^n(w_1,w_0,w_E), x_E^n(w_0,w_E), x_2^n(w_2,w_0,w_E))\right\}$. The following lemma, whose proof will be omitted due to space constraints is used in the secrecy analysis.

Lemma 1: Let $|\mathcal{W}_E|$ denote the cardinality of the set of possible values for the fictitious message W_E. Then

1) The size of each B_{w_0,w_1,w_2} equals $|\mathcal{W}_E|$.
2) The codewords within B_{w_0,w_1,w_2} are i.i.d..

V. Proof Outline

The converse follows from standard pairwise upper bound considerations, see [13]. We focus on the achievability proof here.

Define $d(x)$ as $d(x) = \limsup_{\bar{P}\to\infty} \frac{x}{\log_2 \bar{P}}$. For ease of explanation, we shall first prove Theorem 1 in terms of the following secrecy requirement:

$$\lim_{\bar{n}\to\infty} \frac{1}{\bar{n}} d(I\left(W_0, W_1, W_2; \tilde{\mathbf{Y}}_\gamma^{\bar{n}}\right)) = 0, \quad \forall\gamma, \tag{10}$$

and restrict ourselves to the case where the eavesdropper channel state is arbitrary but does not change over time. Later, in Section V-F, we shall outline the techniques required to strengthen the result for the strong secrecy case (4) when the eavesdropper channel is arbitrarily varying.

In the proof, we focus on a special form of channel model. It can be shown through generalized singular value decomposition [8], [14] that the general channel model can be converted to the form we are considering while preserving the degrees of freedom region. In this special form, $N_T = r_0$ and $\bar{\mathbf{\Sigma}}_t$ is a $N_{R_t} \times r_0$ matrix:

$$\mathbf{Y}_t(i) = \bar{\mathbf{\Sigma}}_t \mathbf{X}_{(r_0\times 1)}(i) + \mathbf{Z}_t(i), t = 1, 2 \tag{11}$$

$$\tilde{\mathbf{Y}}(i) = \tilde{\mathbf{H}}_{(N_E\times r_0)}(i)\mathbf{X}_{(r_0\times 1)}(i) \tag{12}$$

The only nonzero elements in $\bar{\mathbf{\Sigma}}_t$ are the first r_1 leading elements on the main diagonal line of $\bar{\mathbf{\Sigma}}_1$ and the last r_2 elements on the main diagonal line of $\bar{\mathbf{\Sigma}}_2$. These nonzero elements are all positive and share the same value, which we denote with $s^2_{\min}$.

As in [12], without loss of generality, we assume $r_0 > N_E$ and consider $\tilde{\mathbf{H}}$ that has the following form:

$$\tilde{\mathbf{H}} = [\mathbf{I}_{N_E\times N_E}, \mathbf{0}_{N_E\times(r_0-N_E)}]\mathbf{U}_E(i) \tag{13}$$

where $\mathbf{U}_E(i)$ is a unitary matrix only known to the eavesdropper. As in [12], [15], we then introduce artificial noise into $\mathbf{X}$ in (11) and (12) by computing $\mathbf{X}$ as:

$$\mathbf{X}(i) = \tilde{\mathbf{X}}_{(r_0\times 1)}(i) + \mathbf{N}(i) \tag{14}$$

where $\mathbf{N}$ is the $r_0 \times 1$ artificial noise vector consisting of independent rotationally invariant complex Gaussian random variables with zero mean and unit variance. The codebook is designed to transmit $\tilde{\mathbf{X}}$.

Define N'_E as $N'_E = N_E + d_0$. As in [13], in the proof we consider two cases:

1) $s \leq N'_E < \min\{r_1, r_2\}$. In this case (8) is not active and to prove the region is achievable we only need to show for a given value of d_0, the pair $(d_1 = r_1 - N'_E, d_2 = r_2 - N'_E)$ is achievable.
2) $0 < N'_E < s$. In this case (8) is active. To prove the region is achievable we only need to show for a given value of d_0 the two corner points $(d_1 = r_1 - N'_E, d_2 = \tilde{r}_2)$ and $(d_1 = \tilde{r}_1, d_2 = r_2 - N'_E)$ are achievable. We shall prove the pair $(d_1 = r_1 - N'_E, d_2 = \tilde{r}_2)$ is achievable since the proof for the other pair is similar.

A. Input Distribution

Let $C(x) = \log_2(1+x)$. Define P such that $P + r_0$ is proportional to $\bar{P}$. Define R as $R = C(s^2_{\min}(P/r_0)/(s^2_{\min}+1))$. We shall allocate a total power of r_0 units on artificial noise $\mathbf{N}$ in (14) and P/r_0 units on each antenna for $\tilde{\mathbf{X}}$.

As mentioned in Section IV, we shall divide the antennas into different groups, which will be described in Section V-B, and generate codebooks for each group. The input distribution we use to generate codebooks is a truncated Gaussian distribution: For a group that contains k antennas, let $\tilde{\mathbf{X}}_{[k]}$ denote a random vector formed by any k components of $\tilde{\mathbf{X}}$ in (14). For a positive constant ε_P, define $Q_{\tilde{\mathbf{X}}_{[k]}}(x)$ be a k-dimensional rotationally invariant complex Gaussian distribution with covariance matrix $(P(1-\varepsilon_P)/r_0)\mathbf{I}_{(k\times k)}$. We define the following truncated n-letter input distribution $Q_{\tilde{\mathbf{X}}^n_{[k]}}(x^n)$ used to generate the codebooks: Let x_i denote the ith component of x^n. $Q_{\tilde{\mathbf{X}}^n_{[k]}}(x^n)$ is given by:

$$Q_{\tilde{\mathbf{X}}^n_{[k]}}(x^n) = \mu^{-1}_{n,k,\varepsilon_P}\varphi(x^n)\prod_{i=1}^n Q_{\tilde{\mathbf{X}}_{[k]}}(x_i) \tag{15}$$

where $\mu_{n,k,\varepsilon_P} = \int \varphi(x^n)\prod_{i=1}^n Q_{\tilde{\mathbf{X}}_{[k]}}(x_i)dx^n$ and $\varphi(x^n)$ equals 1 if $\frac{1}{n}\|x^n\|^2 \leq kP/r_0$ and equals 0 otherwise.

B. Codebook Generation

Let $\{\delta_n\}$ be a positive sequence of n that can be made arbitrarily small. Define $s = r_1 + r_2 - r_0$. $\tilde{r}_t = r_t - s, t = 1, 2$. The codebook generation depends on how the antennas are grouped based on the values of N'_E. This is illustrated in Figure 2 and described in detail below.

1) $s \le N'_E < \min\{r_1, r_2\}$*:*

a) For $t = 1, 2$, $\mathcal{C}_t$ is composed of $2^{n(r_t R - 2\delta_n)}$ i.i.d. sequences sampled from $Q_{\tilde{\mathbf{X}}^n_{[r_t - N'_E]}}(x^n)$.

b) $\mathcal{C}_3$ is composed of $2^{n(N'_E R - \delta_n)}$ i.i.d. sequences sampled from $Q_{\tilde{\mathbf{X}}^n_{[2N'_E - s]}}(x^n)$.

Each codeword in $\mathcal{C}_3$ is labeled with i_3 and j_3. $0 \le i_3 \le 2^{n(N_E R - \delta_n)} - 1$. $0 \le j_3 \le 2^{n(d_0 R)} - 1$. i_3 shall play the role of W_E in Section IV.

For $t = 1, 2$, each codeword in $\mathcal{C}_t$ is labeled with i_t and j_t, $0 \le i_t \le 2^{n(N'_E R - \delta_n)} - 1$, $0 \le j_t \le 2^{n((r_t - N'_E)R - \delta_n)} - 1$.

2) $0 < N'_E < s$*:* To prove the achievability of the corner point $(d_1 = r_1 - N'_E, d_2 = \tilde{r}_2)$, $\mathcal{C}_t$, $1 \le t \le 3$ are generated as follows:

a) $\mathcal{C}_1$ is composed of $2^{n(r_1 R - 2\delta_n)}$ i.i.d. sequences sampled from $Q_{\tilde{\mathbf{X}}^n_{[r_1 - N'_E]}}(x^n)$.

b) $\mathcal{C}_2$ is composed of $2^{n((\tilde{r}_2 + N'_E)R - 2\delta_n)}$ i.i.d. sequences sampled from $Q_{\tilde{\mathbf{X}}^n_{[\tilde{r}_2]}}(x^n)$.

c) $\mathcal{C}_3$ is composed of $2^{n(N'_E R - \delta_n)}$ i.i.d. sequences sampled from $Q_{\tilde{\mathbf{X}}^n_{[N'_E]}}(x^n)$.

We then label $\mathcal{C}_3$ with (i_3, j_3) as described in the previous sub-section, Section V-B1. $\mathcal{C}_1$ is labeled with (i_1, j_1) as described in Section V-B1. Each codeword in $\mathcal{C}_2$ is labeled with i_2 and j_2: $0 \le i_2 \le 2^{n(N'_E R - \delta_n)} - 1$, $0 \le j_2 \le 2^{n(\tilde{r}_2 R - \delta_n)} - 1$.

C. Encoder

Since $\{i_3, j_3\}$ has the same cardinality as $\{i_t\}$, we can define one-to-one mapping between these two. Denote the mapping with h_t.

a) The encoder chooses i_3 based on uniform distribution.

b) The encoder chooses $j_3 = W_0$.

c) For $t = 1, 2$, we compute $\{i_t, j_t\}$ as follows:

$$i_t = h_t(i_3, j_3), \quad j_t = W_t \tag{16}$$

1) $s \le N_E < \min\{r_1, r_2\}$*:* The codeword with label i_1, j_1 is chosen from $\mathcal{C}_1$ and transmitted over the first $r_1 - N_E$ components of $\tilde{\mathbf{X}}$ in (14).

The codeword with label i_2, j_2 is chosen from $\mathcal{C}_2$ and transmitted over the last $r_2 - N_E$ component of $\tilde{\mathbf{X}}$ in (14).

The codeword with label i_3 is chosen from $\mathcal{C}_3$ and transmitted over the remaining $2N_E - s$ components of $\tilde{\mathbf{X}}$ in (14).

2) $0 < N_E < s$*:* As in Section V-C1, the codeword with label i_1, j_1 is chosen from $\mathcal{C}_1$ and transmitted over the first $r_1 - N_E$ component of $\tilde{\mathbf{X}}$ in (14).

The codeword with label i_2, j_2 is chosen from $\mathcal{C}_2$ and transmitted over the last $\tilde{r}_2$ component of $\tilde{\mathbf{X}}$ in (14).

The codeword with label i_3 is chosen from $\mathcal{C}_3$ and transmitted over the remaining N_E components of $\tilde{\mathbf{X}}$ in (14).

D. Decoder

1) $s \le N_E < \min\{r_1, r_2\}$*:* For $t = 1, 2$,

a) Receiver t first decodes the codeword from $\mathcal{C}_3$.
In this step, for receiver 1, the decoder takes the last N'_E components of $\mathbf{Y}_t$ in (11) as inputs. For receiver 2, the decoder takes the first N'_E components of $\mathbf{Y}_t$ in (11) as inputs.
Receiver t then uses the label of the decoded codeword as its estimate for i_3, j_3, which is denoted by $\hat{i}_{3,t}, \hat{j}_{3,t}$. The estimate for the common confidential message W_0, denoted by $\hat{W}_{0,t}$, is then given by $\hat{j}_{3,t}$. The estimate for the label i_t, denoted by $\hat{i}_t$, is then given by $h_t(\hat{i}_{3,t}, \hat{j}_{3,t})$.

b) Receiver t then estimates the transmitted codeword from $\mathcal{C}_t$ based on the remaining $r_t - N'_E$ components of $\mathbf{Y}_t$ in (14). Note that only those codewords in $\mathcal{C}_t$ whose label $i_t = \hat{i}_t$ need to be considered. From the labels of the most likely codeword in $\mathcal{C}_t$, receiver t computes its estimate for label j_t, denoted by $\hat{j}_t$. Its estimate for message W_t, denoted by $\hat{W}_t$, is then given by $\hat{j}_t$.

2) $0 < N_E < s$*:* Each receiver first computes $\hat{i}_{3,t}, \hat{j}_{3,t}$ as described in the previous subsection, Section V-D1. Receiver 1 computes $\hat{W}_1$ as in Section V-D1. Receiver 2 computes $\hat{W}_2$ as in Section V-D1 except that in step b), $r_2 - N'_E$ should be replaced by $\tilde{r}_2$.

E. Secrecy Analysis

In this section, we prove (10). Let $\|\|$ denote the Euclidean distance. As in [12], define the following fictitious decoder:

$$\phi_{\gamma, w_0, w_1, w_2}(\tilde{y}^n) = \arg \max_{x^n \in B_{w_0, w_1, w_2}} \|\tilde{y}^n - \tilde{\mathbf{H}} x^n\| \tag{17}$$

which is the maximum likelihood decoder the eavesdropper can use to decode the transmitted signals when it assumes the secret message values are $W_i = w_i, i = 0, 1, 2$.

Define $\eta_{\mathcal{C},\gamma,w_0,w_1,w_2}$ as the probability of decoding error for this fictitious decoder, which is given by:

$$\Pr\left(\phi_{\gamma, w_0, w_1, w_2}\left(\tilde{\mathbf{Y}}^n_\gamma\right) \ne \tilde{\mathbf{X}}^n | W_i = w_i, i = 0, 1, 2\right) \tag{18}$$

Define $\eta_{\mathcal{C},\gamma}$ as the value of $\eta_{\mathcal{C},\gamma,w_0,w_1,w_2}$ averaged over w_0, w_1, w_2, which is given by:

$$\frac{1}{|\mathcal{W}_0| \times |\mathcal{W}_1| \times |\mathcal{W}_2|} \sum_{w_i \in \mathcal{W}_i, i=0,1,2} \eta_{\mathcal{C},\gamma,w_0,w_1,w_2} \tag{19}$$

Following [12], using Lemma 1, we have the following lemma. Its proof will be provided in the journal version of this work.

Lemma 2: There exists a codebook $\mathcal{C}$, such that $\lim_{n\to\infty} \eta_{\mathcal{C},\gamma} = 0$ uniformly over all γ.

For this codebook and for any γ, we have:

$$H\left(W_0, W_1, W_2 | \tilde{\mathbf{Y}}^n_\gamma\right) = I\left(W_0, W_1, W_2; \tilde{\mathbf{X}}^n | \tilde{\mathbf{Y}}^n_\gamma\right) \tag{20}$$

$$= H\left(\tilde{\mathbf{X}}^n | \tilde{\mathbf{Y}}^n_\gamma\right) - H\left(\tilde{\mathbf{X}}^n | \tilde{\mathbf{Y}}^n, W_0, W_1, W_2\right) \tag{21}$$

(21) is lower bounded through Fano's inequality by

$$H\left(\tilde{\mathbf{X}}^n\right) - I\left(\tilde{\mathbf{X}}^n; \tilde{\mathbf{Y}}^n_\gamma\right) - 1 - \eta_{\mathcal{C},\gamma} \log_2 \left|\{\tilde{\mathbf{X}}^n\}\right| \tag{22}$$

Due to Lemma 2 and the fact that $\log_2 \left|\{\tilde{\mathbf{X}}^n\}\right|$ grows linearly with respect to n, we have

$$\lim_{n\to\infty} \frac{1}{n} d(1 + \eta_{\mathcal{C},\gamma} \log_2 \left|\{\tilde{\mathbf{X}}^n\}\right|) = 0 \tag{23}$$

On the other hand, as shown in [12], we have:

$$\lim_{n\to\infty}\frac{1}{n}d(I\left(\tilde{\mathbf{X}}^n;\tilde{\mathbf{Y}}_\gamma^n\right))\leq N_E \tag{24}$$

For the first term in (22), we have:

$$H\left(\tilde{\mathbf{X}}^n\right)=\log_2|\{i_3\}|+\sum_{i=0}^{2}\log_2|\mathcal{W}_i| \tag{25}$$

a) $s\leq N_E'<\min\{r_1,r_2\}$: In this case, for $t=1,2$,

$$\log_2|\mathcal{W}_0|+\log_2|\{i_3\}|=n(N_E'R-\delta_n) \tag{26}$$

$$\log_2|\mathcal{W}_t|=\log_2|\{j_t\}|=n((r_t-N_E')R-\delta_n) \tag{27}$$

$$\lim_{n\to\infty}\frac{1}{n}d(H\left(\tilde{\mathbf{X}}^n\right))=\sum_{t=1}^{2}(r_t-N_E')+N_E' \tag{28}$$

Applying (28), (23) and (24) to (22), we find $\lim_{n\to\infty}\frac{1}{n}d(H(W_0,W_1,W_2|\tilde{\mathbf{Y}}_\gamma^n))$ is lower bounded by $\sum_{t=1}^{2}(r_t-N_E')+d_0$, which equals $\lim_{n\to\infty}\frac{1}{n}d(H\left(W_0,W_1,W_2\right))$.

b) If $0<N_E'<s$, it can be verified that $\lim_{n\to\infty}\frac{1}{n}d(H\left(\tilde{\mathbf{X}}^n\right))=r_0$. Therefore

$$\lim_{n\to\infty}\frac{1}{n}d(H\left(W_0,W_1,W_2|\tilde{\mathbf{Y}}_\gamma^n\right))\geq r_0-N_E \tag{29}$$

which equals $\lim_{n\to\infty}\frac{1}{n}d(H\left(W_0,W_1,W_2\right))$.

Hence we have proved (10) for both cases.

F. Strong Secrecy for Arbitrarily Varying Channel

In this section, we briefly outline the necessary changes in order to prove the strong secrecy requirement (4) when the eavesdropper channel is arbitrarily varying:

a) As shown in [12], to ensure secrecy when the eavesdropper channel is arbitrarily varying, *"correlation elimination"* [16] should be used. A coding scheme implied by this technique uses a collection of codebooks instead of one codebook. Each time the transmitter randomly chooses one codebook to use and reveals its choice as a *public* message.

b) As we have seen in Lemma 1, the rate of each bin is N_ER, which is smaller than the rate that the eavesdropper can decode, which is $R_e=N_EC(P/r_0)$. To ensure secrecy, we must amplify the bin size. This is done by using $2^{n(R_e-N_ER+\delta_n)}$ codebooks. Each time the transmitter chooses one codebook to use and transmits its choice to the two intended receivers as a *common confidential* message.

The coding scheme combines the two solutions above: The transmitter uses a collection of codebooks $\mathcal{C}^1$,..., $\mathcal{C}^K$. Each $\mathcal{C}^k$ is composed of a collection of sub-codebooks denoted by $\mathcal{C}_{t,k}$ where $1\leq t\leq 3$ and $0\leq k\leq 2^{n(R_e-N_ER+2\delta_n)}-1$. Each $\mathcal{C}_{t,k}$ is generated and labeled as shown in Section V-A-Section V-B.

a) The transmitter chooses the sub-codebook $\mathcal{C}_{t,K''},t=1,2,3$ in $\mathcal{C}^{K'}$ where K',K'' are generated randomly. The confidential messages is encoded as in Section V-C.

b) The transmitter transmits K' as a public message, and K'' as a common confidential message to both receivers.

The receivers first decode K' and K'' and use the sub-codebook $\mathcal{C}_{t,K''},t=1,2,3$ in $\mathcal{C}^{K'}$ to decode the confidential messages as shown in Section V-D. It can be shown that the communication overhead for transmitting K' and K'' does not reduce the achieved secrecy degrees of freedom and Theorem 1 still holds.

VI. Conclusion

In this work, we have introduced a new type of binning scheme. Through this binning scheme, we characterized the secrecy degrees of freedom region for a two-receiver MIMO broadcast wiretap channel where the eavesdropper channel is memoryless and arbitrarily varying for any given number of antennas.

References

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

[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] 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.

[4] 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*, vol. 2009, Article ID 142374, 12 pages, 2009, doi:10.1155/2009/142374.

[5] 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.

[6] E. Ekrem and S. Ulukus, "The Secrecy Capacity Region of the Gaussian MIMO Multi-receiver Wiretap Channel," to appear in IEEE Transactions on Information Theory, submitted in March 2009.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] A. Khisti, D. Silva, and F. Kschischang, "Secure Broadcast Codes over linear determintic channels," in *IEEE International Symposium on Information Theory*, May 2010.

[14] E. Ekrem and S. Ulukus, "Degrees of Freedom Region of the Gaussian MIMO Broadcast Channel with Common and Private Messages," in *IEEE Global Telecommunication Conference*, December 2010.

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

[16] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Probability Theory and Related Fields*, vol. 44, no. 2, pp. 159–175, 1978.