Gaussian Two-way Wiretap Channel with an Arbitrarily Varying Eavesdropper

Xiang He, Aylin Yener*

* Electrical Engineering Department, The Pennsylvania State University, University Park, PA 16802
hexiang@ieee.org, yener@psu.edu

***Abstract*—In this work, we derive the secrecy degrees of freedom (s.d.o.f.) region of the Gaussian two-way wiretap channel in which the eavesdropper channel state is arbitrarily varying and is unknown to the legitimate nodes. We prove that the s.d.o.f. region is identical to that when the eavesdropper channel is fixed and globally known. A multi-stage coding scheme that combines secret key generation and confidential message transmission is developed to prove achievability. The confidentiality guarantee provided in this work is in the sense of strong secrecy.**

I. Introduction

Providing confidentiality in communication, i.e., secrecy, using information theoretic measure, goes back to Shannon [1]. This approach was later developed in [2] which utilizing different entropy measures. While prevalent architectures for secure communication are still primarily based on cryptographic techniques, providing secrecy using information theory is attractive since it does not rely on unproved assumptions on computational hardness. Furthermore, information theoretic approaches can sometimes lead to cryptographic results as well [3]. Consequently, there appears to be sustained interest in studying secrecy problem using information theory, see [4] for a summary of recent works.

As in all security studies, a significant challenge in information theoretic secrecy is modeling the adversary properly. Most early works assume the eavesdropper channel is fixed and perfectly known to all nodes, while other works assume the distribution of the eavesdropper channel states is known to all nodes [5]. Recently, [6]–[8] study secrecy capacity when the eavesdropper channel is arbitrarily varying and its channel states are known to the eavesdropper only. For this setting, it is shown that the optimal transmission is very different from previous work. Known results focus on the secrecy degrees of freedom (s.o.d.f.) for different channel models, which is a high SNR approximation of the secrecy capacity. Reference [7] finds the s.d.o.f. for the single-user Gaussian multi-input-multi-output (MIMO) wiretap channel. The s.d.o.f. region of the Gaussian MIMO broadcast channel is given in [8]. The s.d.o.f. region of the Gaussian MIMO multiple access channel where all legitimate nodes have the same number of antennas is found in [7].

In this work, we investigate s.o.d.f. region of the Gaussian two-way wiretap channel with this setting. In this channel, two full-duplex transmitters engage in two-way communication in the presence of an eavesdropper. This model was studied extensively assuming the channel state of the eavesdropper is fixed and known to the legitimate communication parties, see [9]–[12] for example. Yet none of the achievability schemes proposed in these works applies to the case of arbitrarily varying eavesdropper channel. Recently, reference [13] studied the same channel model with a even stronger assumption: assuming the channel state is controlled by the eavesdropper but unknown to the legitimate communication parties. It is shown in [13] that it is still possible for the secrecy rate to scale with the transmission power but the s.d.o.f. number achieved in [13] does not match with the converse in [10].

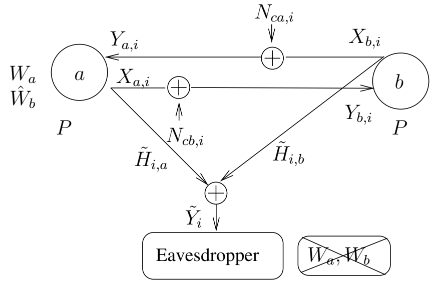

Fig. 1. Gaussian Two-way Wiretap Channel where the Eavesdropper Channel is Arbitrarily Varying

The main contribution of this work is deriving the s.d.o.f. region of the Gaussian two-way wiretap channel when the eavesdropper channel was modeled as arbitrarily varying as in [7] and prove that the converse of [10] is tight for this case. The achievability scheme overlaps secret key generation and confidential message transmission. For secret key generation, a two-step scheme combining [13] and [8] is used to achieve *strong* secrecy.

II. System Model

The channel model is shown in Figure 1. The main channel is a Gaussian two-way channel composed of two full-duplex nodes. The output during the ith channel use for this channel, after canceling the self-interference in a full-duplex transceiver, can be expressed as [9]:

$$Y_{a,i} = X_{b,i} + N_{ca,i}, \quad Y_{b,i} = X_{a,i} + N_{cb,i} \tag{1}$$

where $X_{a,i}$ and $X_{b,i}$ are the signals transmitted by nodes a and b respectively during the ith channel use, and $Y_{a,i}$ and $Y_{b,i}$ denote their received signals. $N_{ca,i}$ and $N_{cb,i}$ are

978-1-4673-0040-7/11/$26.00 ©2011 IEEE

Gaussian random variables with unit variance.[1] We assume the eavesdropper channel to be noiseless as a worst case assumption:

$$\tilde{Y}_i = \tilde{H}_{i,a}X_{a,i} + \tilde{H}_{i,b}X_{b,i} \tag{2}$$

Without loss of generality, we assume $|\tilde{H}_{i,a}|^2 + |\tilde{H}_{i,b}|^2 = 1$. Otherwise, the eavesdropper can normalize its received signals to conform to this constraint.

Node a, b each wants to send a confidential message W_a, W_b to node b, a over $\bar{n}$ channel uses respectively. Node b, a each decodes the message intended for it as $\hat{W}_a, \hat{W}_b$ from the signals it received and any other side information available to it. For reliable reception of $W_l, l \in \{a, b\}$, we require:

$$\lim_{\bar{n}\to\infty} \Pr(W_l \neq \hat{W}_l) = 0, \quad l \in \{a, b\} \tag{3}$$

Let $\tilde{\mathbf{H}}_i$ denote $[\tilde{H}_{i,a}, \tilde{H}_{i,b}]$. We assume the eavesdropper channel state information sequence $\tilde{\mathbf{H}}^{\bar{n}}$ is independent from $\{X_a^{\bar{n}}, X_b^{\bar{n}}\}$. In this case, as shown in [7], the *strong* secrecy constraint can be defined as:

$$\lim_{\bar{n}\to\infty} I\left(W_a, W_b; \tilde{\mathbf{Y}}^{\bar{n}} | \tilde{\mathbf{H}}^{\bar{n}} = \tilde{\mathbf{h}}^{\bar{n}}\right) = 0, \quad \forall \tilde{\mathbf{h}}^{\bar{n}} \tag{4}$$

We require the limit in (4) to be uniform over all possible sequences of eavesdropper channel states [7]. Note that although the definition in (4) is stated for $\tilde{\mathbf{H}}^{\bar{n}}$ being any given sequence $\tilde{\mathbf{h}}^{\bar{n}}$, it also implies the message is secure for $\tilde{\mathbf{H}}^{\bar{n}}$ with any distribution [7].

The secrecy rates for the message W_l, $R_{s,l}, l \in \{a, b\}$, is defined as

$$R_{s,l} = \lim_{\bar{n}\to\infty} \frac{1}{\bar{n}} H(W_l), \quad l \in \{a, b\} \tag{5}$$

such that both (3) and (4) are satisfied. Secrecy capacity region is defined as the union of all achievable secrecy rate pairs.

We assume the transmitter at node a and b are constrained in terms of average transmission power. For simplicity, we use the same power limit for both nodes, i.e.,

$$\lim_{\bar{n}\to\infty} \frac{1}{\bar{n}} \sum_{i=1}^{\bar{n}} \mathrm{E}[|X_{l,i}|^2] \leq \bar{P}, \quad l \in \{a, b\} \tag{6}$$

The secrecy degrees of freedom (s.d.o.f.) region is a characterization of the high SNR behavior of the secrecy capacity region, which is defined as:

$$\{(d_a, d_b) : d_l = \limsup_{\bar{P}\to\infty} \frac{R_{s,l}}{\log_2 \bar{P}}, \quad l \in \{a, b\}\} \tag{7}$$

III. Main Result

Theorem 1: The s.d.o.f. for the Gaussian two way wiretap channel with arbitrarily varying eavesdropper channel described in Section II is given by

$$0 \leq d_l \leq 1, \quad l \in \{a, b\} \tag{8}$$

$$0 \leq d_a + d_b \leq 1 \tag{9}$$

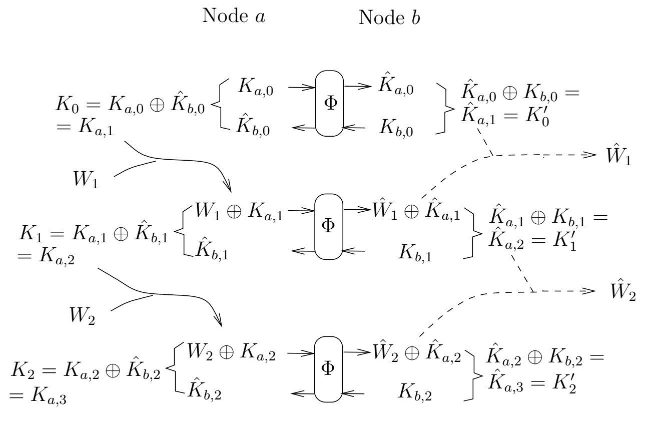

Fig. 2. Key Generation and Message Transmission Scheme. The figure illustrates the first three stages. W_i denotes the confidential message. K_i denotes the key generated at each stage. Φ denotes the secrecy key generation module described in Section VI

The converse proof for Theorem 1 follows from directly from [10]. Hence we only need to prove achievability.

IV. Achievability: Artificial Noise

We only need to prove that $d_a = 1, d_b = 0$ is achievable. The achievability of $d_a = 0, d_b = 1$ follows from the symmetry of the channel model. The whole s.d.o.f. region then follows from time sharing between these two pairs of degrees of freedom.

Since we assume the eavesdropper channel is noiseless, we introduce artificial noise [14] at Node a and b to limit the received signal to noise ratio at the eavesdropper. This means

$$X_{l,i} = \tilde{X}_{l,i} + N_{l,i}, \quad l \in \{a, b\} \tag{10}$$

where $N_{l,i}$ is a Gaussian random variable with zero mean and unit variance. With the inputs given by (10), the channel model can be re-written as:

$$Y_{a,i} = \tilde{X}_{b,i} + N_{b,i} + N_{ca,i} \tag{11}$$

$$Y_{b,i} = \tilde{X}_{a,i} + N_{a,i} + N_{cb,i} \tag{12}$$

$$\tilde{Y}_i = \sum_{l\in\{a,b\}} \tilde{H}_{i,l}\tilde{X}_{l,i} + \sum_{l\in\{a,b\}} \tilde{H}_{i,l}N_{l,i} \tag{13}$$

The coding scheme shall be performed over $\tilde{X}_{l,i}, l \in \{a, b\}$.

V. Achievability: Overview

Since only one node is transmitting the confidential message for the case we are interested, which is $d_a = 1, d_b = 0$, we shall replace W_a with W in the sequel.

As shown in Figure 2, communication is divided into several stages. The ith stage generates a secret key K_i through a key generation protocol Φ, which we shall describe in Section VI. The key generated by the ith stage is then used as a one-time pad in the $i + 1$th stage to transmit a confidential message W_{i+1}. Except for the first stage, each stage serves the dual purpose of generating a new secret key and transmitting a separate confidential message using previously generated keys [15].

[1] The subscript c stands for channel.

VI. Secrecy Key Generation Protocol: Φ

A. Codebook $\mathcal{C}$ with code length n

Define P as the remaining power budget after the power expended on artificial noise. $P = \max\{\bar{P} - 1, 0\}$. Define $C(x) = \log_2(1+x)$. The codebook $\mathcal{C}$ with parameter n is composed of $2^{n(C(P(1-\varepsilon_P)/2)-\delta)}$ i.i.d. n-length sequences sampled from the following distribution:

$$Q_{\tilde{X}^n}(x^n) = \mu_{n,\varepsilon_P}^{-1}\varphi\left(x^n\right)\prod_{i=1}^{n} Q_{\tilde{X}}\left(x_i\right) \tag{14}$$

where $Q_{\tilde{X}}(x)$ is a rotationally invariant complex Gaussian distribution with variance $P(1-\varepsilon_P)$ for a positive constant ε_P which can be arbitrarily small. $\mu_{n,\varepsilon_P} = \int \varphi\left(x^n\right)\prod_{i=1}^{n} Q_{\tilde{X}}\left(x_i\right)dx^n$ and $\varphi\left(x^n\right)$ equals 1 if $\frac{1}{n}\|x^n\|^2 \leq P$ and equals 0 otherwise.

B. Encoders and Decoders for codebook $\mathcal{C}_a, \mathcal{C}_b$

The encoders and decoders used by node a and b each take one codebook as parameters, denoted by $\mathcal{C}_a$ and $\mathcal{C}_b$ respectively. The codebooks are generated as described in Section VI-A.

Define $a \oplus b$ as $a + b \bmod |\mathcal{C}|$, where $|\mathcal{C}|$ is the size of the codebook $\mathcal{C}_a$. $\mathcal{C}_b$ has the same size as $\mathcal{C}_a$.

During the ith stage, node b generates a random number $K_{b,i}$ from $\{0, ..., |\mathcal{C}|-1\}$ and transmits the $K_{b,i}$th codeword from the codebook $\mathcal{C}_b$. For node a, we have the following:

1) In the 0th stage, node a generates a random number $K_{a,0}$ from $\{0, ..., |\mathcal{C}|-1\}$ and transmits the $K_{a,0}$th codeword from the codebook $\mathcal{C}_a$.
2) In the ith stage, $i \geq 1$, it transmits the $(K_{a,i} \oplus W_i)$th codeword from the codebook $\mathcal{C}_a$, where $K_{a,i}$ is computed from the previous stage as we shall describe below in (17). W_i is the confidential message transmitted by this stage.

Node a and b then decode $K_{b,i}$ and $K_{a,i}$ respectively from the signals they received during this stage. Denote the decoding result as $\hat{K}_{l,i}, l \in \{a, b\}$.

The secret key generated at node a is then given by:

$$K_i = K_{a,i} \oplus \hat{K}_{b,i} \tag{15}$$

The secret key generated at node b is given by:

$$K_i' = \hat{K}_{a,i} \oplus K_{b,i} \tag{16}$$

K_i and K_i' should equal to each other with high probability.

Node a then uses K_i as the input to the key generation protocol in the next stage:

$$K_{a,i+1} = K_i \tag{17}$$

C. Two-Step Key Generation

For a given W_i and K_i, the set of codewords that can be transmitted, denoted by B_{W_i,K_i} contains $2^{nC(P(1-\varepsilon_P)/2)}$ i.i.d. sequences. However, in order to confuse the eavesdropper, B_{W_i,K_i} should be greater $2^{nC(P(1-\varepsilon_P))}$, where $C(P(1-\varepsilon_P))$ is the maximal rate at which the eavesdropper can decode. Therefore, the size of B_{W_i,K_i} must be increased. This is achieved by using a two-step scheme [8]: Instead of using just one codebook, we shall use a collection of codebooks. We first generate a secret key at a low rate, then use the generated key to determine which codebook is used. Since the eavesdropper is not aware of the value of the secret key, he must consider the union of B_{W_i,K_i} from all possible codebooks, which effectively makes the set of possible codewords larger. The achievable secrecy rate with this scheme is derived next.

VII. Secrecy Analysis

Let $n_i = a_i n$ be the number of channel uses taken during step $i, i = 1, 2$. $a_i > 0$. $a_1 + a_2 = 1$.

We first need the following result implied by [13].

Lemma 1: There exists a positive number c, such that $(d_1 = c, d_2 = 0)$ is achievable.

For stage k, using Lemma 1, we first generate a secret key $K_{k,1}$ with rate $R_0(P)$ using $a_1 n$ channel uses. Due to Lemma 1, $\lim_{P\to\infty} R_0(P) = \infty$. Let $|K_{k,1}| = 2^{a_1 n R_0(P)}$. $K_{k,1}$ is uniformly distributed over $\{0, ..., |K_{k,1}|-1\}$ and

$$I\left(K_{k,1}; \tilde{Y}_k^{a_1 n}\right) \leq e^{-\alpha a_1 n} \tag{18}$$

Let $\hat{K}_{k,1}$ denote the estimate of $K_{k,1}$ computed by node b.

Each node shall generate beforehand $|K_{k,1}|$ independent codebooks with code length n_2. These codebooks are denoted by $\{\mathcal{C}_{l,t}\}$, $l \in \{a, b\}$, $t \in \{0, ..., |K_{k,1}|-1\}$.

The encoder and decoder at node a, b then uses the scheme described in Section VI-B to generate secret key K_k, where node a uses the codebook $\mathcal{C}_{a,K_{k,1}}$. Node b uses the codebook $\mathcal{C}_{b,\hat{K}_{k,1}}$. We next choose a_1 such that

$$\frac{a_1}{a_2}R_0(P) + C(P(1-\varepsilon_P)/2) - \delta \geq C(P) + \delta \tag{19}$$

for a positive δ that can be made arbitrarily small. Recall that $C(P(1-\varepsilon_P)/2) - \delta$ is the rate of B_{W_i,K_i} without the first step. $\frac{a_1}{a_2}R_0(P)$ is the rate increase due to first step. We amplify B_{W_i,K_i} so that its rate is slightly higher than the rate at which the eavesdropper can decode, which is $C(P)$. Then we have the following lemma:

Lemma 2: There exists a positive α, such that

$$I(K_k; \tilde{Y}_k^n | W_k) \leq \exp(-\alpha n) \tag{20}$$

The proof of Lemma 2 is based on (19) and (18) and will be provided in the journal version of this work. Note that due to Lemma 1, we can satisfy (19) and

$$\lim_{P\to\infty} a_1 = 0 \tag{21}$$

simultaneously. This means introducing step 1 will not decrease the degrees of freedom achieved by step 2.

Clearly the transmission rate we have achieved provide a degree of freedom $d_1 = 1$. We next verify that this rate is a secrecy rate.

Assume the transmission uses $M+1$ stages. We need to show that

$$I\left(W_1, ..., W_M; \tilde{Y}_0^n, \tilde{Y}_1^n, ..., \tilde{Y}_M^n\right) = \tag{22}$$

$$\sum_{k=1}^{M} I\left(W_k; \tilde{Y}_0^n, \tilde{Y}_1^n, ..., \tilde{Y}_M^n | W_1, ..., W_{k-1}\right) \tag{23}$$

vanishes. Each term in (23) can be written as:

$$I\left(W_k; \tilde{Y}_0^n, \tilde{Y}_1^n, ..., \tilde{Y}_M^n | W_1, ..., W_{k-1}\right) \tag{24}$$

$$= I\left(W_k; \tilde{Y}_0^n, ..., \tilde{Y}_k^n | W_1, ..., W_{k-1}\right)$$

$$+ I\left(W_k; \tilde{Y}_{k+1}^n, ..., \tilde{Y}_M^n | W_1, ..., W_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_k^n\right) \tag{25}$$

We next introduce some supporting results.

A. Supporting Results

Lemma 3:

$$I\left(K_{k-1}; \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) < \exp(-n\alpha) \tag{26}$$

Lemma 3 follows from Lemma 2. Its proof is omitted and will be provided in the journal version of this work.

Lemma 4:

$$I\left(K_{k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) \leq (k-1)e^{-n\alpha} \tag{27}$$

Proof: The proof is provided in Appendix A. ■

B. First term in (25) vanishes

The first term in (25) is upper bounded as follows:

$$I\left(W_k; \tilde{Y}_0^n, ..., \tilde{Y}_k^n | W_1, ..., W_{k-1}\right) \tag{28}$$

$$= I\left(W_k; \tilde{Y}_k^n | W_1, ..., W_{k-1}\right)$$

$$+ I\left(W_k; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | \tilde{Y}_k^n, W_1, ..., W_{k-1}\right) \tag{29}$$

The first term in (29) is upper bounded by:

$$I\left(W_k; W_k \oplus K_{a,k}, \tilde{Y}_k^n | W_1, ..., W_{k-1}\right) \tag{30}$$

$$= I\left(W_k; W_k \oplus K_{a,k} | W_1, ..., W_{k-1}\right)$$

$$+ I\left(W_k; \tilde{Y}_k^n | W_k \oplus K_{a,k}, W_1, ..., W_{k-1}\right) \tag{31}$$

$$\leq I\left(W_1, ..., W_k; W_k \oplus K_{a,k}\right)$$

$$+ I\left(W_1, ..., W_k; \tilde{Y}_k^n | W_k \oplus K_{a,k}\right) \tag{32}$$

Note that due to (15) and (17), $K_{a,k}$ is given by

$$K_{a,k} = K_{a,0} \oplus \sum_{t=0}^{k-1} \hat{K}_{b,t} \tag{33}$$

Hence $K_{a,k}$ is uniformly distributed. $K_{a,k}$ is also independent from $W_1, ...W_k$. This implies the first term in (32) is 0. The second term in (32) is 0 because as shown by the transmission scheme in Figure 2, given $W_k \oplus K_{a,k}$, the signal received by the eavesdropper $\tilde{Y}_k^n$ is independent from $W_1, ..., W_k$. Hence (32) is 0. The second term in (29) is upper bounded by:

$$I\left(W_k, \tilde{Y}_k^n; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) \tag{34}$$

$$\leq I\left(W_k, \tilde{Y}_k^n, K_{a,k}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) \tag{35}$$

$$= I\left(K_{a,k}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right)$$

$$+ I\left(W_k; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | K_{a,k}, W_1, ..., W_{k-1}\right)$$

$$+ I\left(\tilde{Y}_k^n; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_k, K_{a,k}, W_1, ..., W_{k-1}\right) \tag{36}$$

The second term in (36) is upper bounded by:

$$I\left(W_k; K_{a,k}, \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n, W_1, ..., W_{k-1}\right) \tag{37}$$

$$= I\left(W_k; K_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n, W_1, ..., W_{k-1}\right) = 0 \tag{38}$$

because W_k is independent from all signals and messages in previous stages. The third term in (36) is 0 because as shown in Figure 2, given $K_{a,k}$ and W_k, the signals $\tilde{Y}_k^n$ are independent from $\tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n, W_1, ..., W_{k-1}$. The first term in (36) is upper bounded by:

$$I\left(K_{a,k}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) \tag{39}$$

$$= I\left(K_{k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) \tag{40}$$

$$\leq (k-1)e^{-n\alpha} \tag{41}$$

due to Lemma 4.

C. Second term in (25) vanishes

$$I\left(W_k; \tilde{Y}_{k+1}^n, ..., \tilde{Y}_M^n | W_1, ..., W_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_k^n\right) \tag{42}$$

$$\leq I(W_k; K_{a,k+1}, \tilde{Y}_{k+1}^n, ..., \tilde{Y}_M^n$$
$$| W_1, ..., W_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_k^n) \tag{43}$$

$$= I\left(W_k; K_{a,k+1} | W_1, ..., W_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_k^n\right) +$$
$$I(W_k; \tilde{Y}_{k+1}^n, ..., \tilde{Y}_M^n$$
$$| K_{a,k+1}, W_1, ..., W_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_k^n) \tag{44}$$

The second term in (44) is upper bounded by:

$$I(W_k; \tilde{Y}_{k+1}^n, ..., \tilde{Y}_M^n$$
$$| K_{a,k+1}, W_1, ..., W_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_k^n) \tag{45}$$

$$\leq I(W_1, ..., W_k, \tilde{Y}_0^n, ..., \tilde{Y}_k^n; \tilde{Y}_{k+1}^n, ..., \tilde{Y}_M^n | K_{a,k+1}) \tag{46}$$

which is 0 because $K_{a,k+1}$ is the only random variable shared between the first k stages and later stages. The first term in (44) can be written as:

$$I\left(W_k; K_k | W_1, ..., W_{k-1}, \tilde{Y}_0^n, ..., \tilde{Y}_k^n\right) \tag{47}$$

$$\leq I\left(W_k, \tilde{Y}_0^n, ..., \tilde{Y}_k^n; K_k | W_1, ..., W_{k-1}\right) \tag{48}$$

$$= I\left(W_k; K_k | W_1, ..., W_{k-1}\right)$$

$$+ I\left(\tilde{Y}_k^n; K_k | W_1, ..., W_k\right)$$

$$+ I\left(\tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n; K_k | W_1, ..., W_k, \tilde{Y}_k^n\right) \tag{49}$$

The first term in (49) is upper bounded by:

$$I\left(W_k; K_k, W_1, ..., W_{k-1}\right) \tag{50}$$

$$\le I\left(W_k; K_{a,k}, \hat{K}_{b,k}, W_1, ..., W_{k-1}\right) \tag{51}$$

which is 0. The second term in (49) vanishes when n goes to ∞ due to Lemma 3. The third term in (49) is upper bounded by:

$$I\left(\tilde{Y}_0^n, .., \tilde{Y}_{k-1}^n; K_{k-1}, K_k, W_k, \tilde{Y}_k^n | W_1, ..., W_{k-1}\right) \tag{52}$$

$$\begin{aligned}&= I\left(\tilde{Y}_0^n, .., \tilde{Y}_{k-1}^n; K_{k-1} | W_1, ..., W_{k-1}\right)\\ &\quad + I\left(\tilde{Y}_0^n, .., \tilde{Y}_{k-1}^n; K_k, W_k, \tilde{Y}_k^n | K_{k-1}, W_1, ..., W_{k-1}\right)\end{aligned} \tag{53}$$

The first term in (53) vanishes when n goes to ∞ due to Lemma 4. The second term in (53) is upper bounded by:

$$I\left(\tilde{Y}_0^n, .., \tilde{Y}_{k-1}^n, W_1, ..., W_{k-1}; K_k, W_k, \tilde{Y}_k^n | K_{k-1}\right) \tag{54}$$

which is 0 because K_{k-1} is the only random variable connecting stage $0, ..., k-1$ to stage k. This implies the second term in (25) vanishes.

VIII. Conclusion

In this work, we have studied the Gaussian two-way wiretap channel in which two full-duplex transmitters engage in two-way communication in the presence of an eavesdropper. The eavesdropper channel is arbitrarily varying and its state only known to the eavesdropper. The s.d.o.f. region for this channel has been identified. It is shown that, surprisingly, the converse previously developed with the eavesdropper channel state fixed and globally known is also tight in this case. The achievability is proved with a multi-stage scheme that combines secret key generation and confidential message transmission.

Appendix A
Proof of Lemma 4

$$I\left(K_{k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) \tag{55}$$

$$\begin{aligned}&= I\left(K_{k-1}; \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right)\\ &\quad + I\left(K_{k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n | \tilde{Y}_{k-1}^n, W_1, ..., W_{k-1}\right)\end{aligned} \tag{56}$$

The first term in (56) vanishes when n goes to infinity due to Lemma 3. The second term in (56) can be written as:

$$\begin{aligned}&I(K_{a,k-1} \oplus K_{b,k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n\\ &\quad |\tilde{Y}_{k-1}^n, W_1, ..., W_{k-1})\end{aligned} \tag{57}$$

$$\begin{aligned}&\le I(K_{a,k-1}, K_{b,k-1}, W_{k-1}, \tilde{Y}_{k-1}^n; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n\\ &\quad |W_1, ..., W_{k-2})\end{aligned} \tag{58}$$

$$\begin{aligned}&\le I(K_{a,k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n | W_1, ..., W_{k-2})\\ &\quad + I(K_{b,k-1}, W_{k-1}, \tilde{Y}_{k-1}^n; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n\\ &\qquad |K_{a,k-1}, W_1, ..., W_{k-2})\end{aligned} \tag{59}$$

The second term in (59) is upper bounded by:

$$\begin{aligned}&I(K_{b,k-1}, W_{k-1}, \tilde{Y}_{k-1}^n; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n, W_1, ..., W_{k-2}\\ &\quad |K_{a,k-1}) = 0\end{aligned} \tag{60}$$

because as shown in Figure 2, given $K_{a,k-1}$, we observe $\{K_{b,k-1}, W_{k-1}, \tilde{Y}_{k-1}^n\}$ are independent from $\{\tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n, W_1, ..., W_{k-2}\}$. Since $K_{a,k-1}$ is just K_{k-2}, the first term in (59) can be written as:

$$I\left(K_{k-2}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n | W_1, .., W_{k-2}\right) \tag{61}$$

Hence from (55) to (61), we find that

$$I\left(K_{k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right) \tag{62}$$

$$\le I\left(K_{k-2}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-2}^n | W_1, .., W_{k-2}\right) + e^{-n\alpha} \tag{63}$$

Applying (55)-(61) repeatedly for $k-1, ..., 1$, we find that

$$\begin{aligned}&I\left(K_{k-1}; \tilde{Y}_0^n, ..., \tilde{Y}_{k-1}^n | W_1, ..., W_{k-1}\right)\\ &\le (k-1)e^{-n\alpha}\end{aligned} \tag{64}$$

References

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

[2] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized Privacy Amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, November 1995.

[3] L. Reyzin. Some Notions of Entropy for Cryptography. *Information Theoretic Security*, pages 138–142, 2011.

[4] 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.

[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] 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.

[7] 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.

[8] 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.

[9] 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.

[10] X. He and A. Yener. The Role of Feedback in Two-Way Secure Communication. Submitted to IEEE Transactions on Information Theory, November, 2009, available online at http://arxiv.org/abs/0911.4432.

[11] A. El-Gamal, O. O. Koyluoglu, M. Youssef, and H. El-Gamal. The Two Way Wiretap Channel: Theory and Practice. Submitted to the IEEE Transactions on Information Theory, June, 2010, available online at http://arxiv.org/abs/1006.0778.

[12] A. J. Pierrot and M. R. Bloch. Strongly Secure Communications Over the Two-Way Wiretap Channel. submitted to IEEE Transactions on Information Forensics and Security, October, 2010, available online at http://arxiv.org/abs/1010.0177.

[13] X. He and A. Yener. Secrecy When the Eavesdropper Controls its Channel States. In *IEEE International Symposium on Information Theory*, July 2011.

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

[15] K. Khalil, M. Youssef, O. Koyluoglu, and H. El Gamal. On the Delay Limited Secrecy Capacity of Fading Channels. In *IEEE International Symposium on Information Theory*, June 2009.