Secrecy When the Eavesdropper Controls its Channel States

Xiang He Aylin Yener

Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xxh119@psu.edu *yener@ee.psu.edu*

***Abstract*—This work investigates providing information theoretically secure communication in a scenario where the eavesdropper is more powerful as compared to models considered to date. Specifically, we consider the setting where the eavesdropper, based on signals it received in the past, modifies its channel state in order to benefit its reception of the legitimate parties' messages. Natural to this setting is that the legitimate parties do not have any knowledge of the eavesdropper's channel state. In this setting, we study the Gaussian two-way wiretap channel, namely two legitimate nodes connected by a bi-directional link in the presence of an eavesdropper that receives the superposition of signals from both nodes. We show that a positive secrecy rate in the sense of strong secrecy is achievable even under these assumptions. The secrecy rate obtained scales with transmit power. The achievable strategy involves cooperative jamming pointing out to its robustness to the adaptive nature of the eavesdropper channel.**

I. Introduction

All recognized secrecy schemes are based on a small set of reasonable assumptions. The approach of studying secrecy problems using information theory was originated by Shannon in [1] and was later extended to different network models, see for example, [2]–[8]. The distinctive feature of this approach is that instead of assuming the adversary is computationally limited as in the case in 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.

A commonly used assumption in information theoretic secrecy is that the eavesdropper is a passive entity who does not in any way contribute to the setting other than employing a capable receiver with access to information on the channels and codebooks. A consequence of this assumption, which is that the eavesdropper does not interact with and adaptively modify its channel states, allows for a cleaner setting, yet presents a vulnerability against malicious entities. In this paper, we present a new setting that allows the eavesdropper to manipulate its channel states, and prove that information theoretically secure communication *is possible* against this eavesdropper.

This work is particularly motivated by the increasing popularity of using cooperative jamming, first proposed in [7], [8], to achieve secrecy. In references [3], [7], [8], it was proposed that if an eavesdropper had a good reception from a legitimate transmitter, that transmitter could transmit with the specific aim to degrade the quality of the signals observed by the eavesdropper, preventing it from intercepting confidential messages sent by other legitimate transmitters. Yet, it is conceivable that a smart eavesdropper could choose to move away from such a jamming transmitter, for example, by monitoring the locations of legitimate transmitters and measuring if there is a sudden increase in the number of frames in error. The eavesdropper can then use a sophisticated directional antenna and adjust the radiation pattern of the antenna quickly so that it is reinforced in a direction not affected by the cooperative jammer. The effectiveness of using a cooperative jammer would then become limited.

In this paper, to model this behavior, we assume that the eavesdropper has *complete control* over the states of the eavesdropper channel using a possibly stochastic controller based on the channel outputs it observed in the past. The eavesdropper does not transmit any signals and hence is still a passive entity. However, with this new capability of manipulating its channel, it is a more powerful entity.

With this new assumption, we revisit the Gaussian two-way wiretap channel first studied in reference [9] and then in references [3], [10]–[12]. Additionally, in line with recent developments, we consider the setting where the legitimate nodes *do not* have any knowledge of the eavesdropper channel [13]. We show a positive secrecy rate is still achievable by generating cooperative jamming sequences carefully through a three stage communication protocol. The achieved secrecy rate is in the sense of *strong secrecy* and scales with transmission power. The result implies that secure connectivity of a bidirectional link is possible unconditionally.

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 [14]. The inputs and outputs during ith channel use for

978-1-4577-0594-6/11/$26.00 ©2011 IEEE

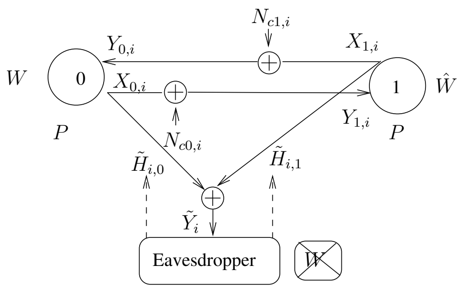

Fig. 1. two-way wiretap channel model where the eavesdropper controls its channel states

this channel, after canceling the self-interference in a full-duplex transceiver, can be expressed as [3]:

$$Y_{0,i} = X_{1,i} + N_{c1,i}, \quad Y_{1,i} = X_{0,i} + N_{c0,i} \tag{1}$$

We assume the eavesdropper channel to be noiseless as a worst case assumption:

$$\tilde{Y}_i = \tilde{H}_{i,0} X_{0,i} + \tilde{H}_{i,1} X_{1,i} \tag{2}$$

Without loss of generality, we assume $|\tilde{H}_{i,0}|^2 + |\tilde{H}_{i,1}|^2 = 1$. Otherwise the eavesdropper can normalize its received signals to conform to this constraint.

Let $\tilde{\mathbf{H}}_i$ denote $[\tilde{H}_{i,0}, \tilde{H}_{i,1}]$. We assume the eavesdropper can choose $\tilde{\mathbf{H}}_i$, based on the signals it received in the past. Let M_e be the local randomness available to the eavesdropper. Then this means:

$$\tilde{\mathbf{H}}_i = g_i(M_e, \tilde{Y}^{i-1}) \tag{3}$$

where g_i is a deterministic function used by the eavesdropper to calculate $\tilde{\mathbf{H}}_i$. Equation (3) implies the eavesdropper has perfect knowledge of the eavesdropper channel state information.

We assume that node 0 and 1 do not have knowledge on *the distribution* or *the realization* of M_e. Neither do they have knowledge on g_i. We also assume that node 0 and 1 do not have knowledge on *the distribution* or *the realization* of $\{\tilde{\mathbf{H}}_i\}$.

We assume the transmitters at node 0 and 1 are constrained in terms of average transmission power. For simplicity, we use the same power limit for both nodes, given by

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \mathrm{E}[|X_{j,i}|^2] \le \bar{P}, \quad j = 0, 1 \tag{4}$$

Node 0 wants to send a confidential message W to node 1. Node 1 decodes the message as $\hat{W}$ from the signals it received and any other side information available to it. For reliable reception of W, we require:

$$\lim_{n\to\infty} \Pr(W \neq \hat{W}) = 0 \tag{5}$$

Additionally, we require W to be kept secret from the eavesdropper. Thus, we require the following secrecy constraint to hold for any M_e:

$$\lim_{n\to\infty} I(W; \tilde{Y}^n, M_e) = 0, \quad \forall M_e, \{g_i\} \tag{6}$$

Observe that (6) is the *strong* secrecy constraint [13]. We require the convergence in (6) to be uniform over all possible choice of M_e and $\{g_i\}$, which also implies there are infinitely many secrecy constraints in the form of (6) to satisfy.

Throughout the paper, we consider the above setting. The obvious extension to providing confidential message transmission from node 1 to node 0 is via time sharing.

III. The Achievable Scheme

Communication is divided to three stages:

1) The first stage takes n channel uses. In this stage, nodes 0 and 1 transmit i.i.d. Gaussian random sequences with zero mean. Let P denote its variance. Let J_i denote the signal transmitted by node $i, i = 0, 1$ during this stage.
2) The second stage also takes n channel uses. In this stage, only node 0 transmits. Node 0 generates a binary i.i.d. sequence T^n, such that $\Pr(T_i = 0) = 1/2, i = 1, ..., n$. Observe that node 0 at this moment has the knowledge of
   a) J_0^n, which is the sequence it transmitted during the first stage.
   b) $J_1^n + N_{c1}^n$, which is the sequence it received during the first stage.

   Node 0 then constructs a jamming sequence J_r^n, such that

$$J_{r,i} = \begin{cases} J_{0,i}, & T_i = 0 \\ J_{1,i} + N_{c1,i}, & T_i = 1 \end{cases} \tag{7}$$

   The transmitter at node 0 takes input V^n and transmits

$$V_i + J_{r,i} + N_{J,i} \tag{8}$$

   during the ith channel use in the second stage, where $\{N_J^n\}$ is an i.i.d. Gaussian sequence with zero mean and unit variance.
   The confidential message W shall be encoded in V^n through a stochastic encoder.
3) During the third stage, only node 0 transmits. In this stage, node 0 broadcasts T^n as a public message to node 1.

IV. Secrecy Analysis

A. Main Result

Theorem 1: Let $C(x) = \log_2(1 + x)$. Let $P = (\bar{P} - 1)/2$. Let $[x]^+$ be $\max\{x, 0\}$. Then for an arbitrarily small constant $\delta' > 0$, the following secrecy rate R_s is achievable:

$$\alpha_2 \left[\begin{array}{l} \frac{1}{2}\left[C\left(\frac{P}{2}\right) + C\left(P(\frac{P+1}{2P+1})\right)\right] \\ -\frac{1}{2}\left[C\left(P\right) + C\left(\frac{2P}{P+2}\right)\right] - \delta' \end{array} \right]^+ \tag{9}$$

where α_2 is the time sharing factor of the second stage. Clearly $\alpha_2 > 1/3$ for sufficiently large $\bar{P}$.

B. Proof of Theorem 1

For $i = 1, ..., n$, define $\tilde{X}^n$ and J^n as

$$\tilde{X}_i = J_{1-T_i,i}, \quad J_i = J_{T_i,i} \tag{10}$$

Since $\{J_0^n\}$ has the same distribution as $\{J_1^n\}$, and $\{T^n\}$ is independent from $\{J_0^n\}$ and $\{J_1^n\}$, we observe from (10) that $\tilde{X}^n$ and J^n are independent from T^n. Then (8) can be written in the following form:

$$V_i + \tilde{X}_i + T_i N_{c1,i} + N_{J,i} \tag{11}$$

Let $\tilde{Y}^n$ denote the signals received by the eavesdropper during the first stage. Then from (10), $\tilde{Y}_i$ is given by:

$$\tilde{Y}_i = \tilde{H}_{i,1-T_i}\tilde{X}_i + \tilde{H}_{i,T_i}J_i \tag{12}$$

Let $\tilde{Y}'_i$ denote the signals received by the eavesdropper during the second stage. Without loss of generality, we assume $\tilde{Y}'_i$ is given by (11). Define Y'_i as:

$$Y'_i = V_i + \tilde{X}_i + N_{J,i} \tag{13}$$

with which, from (11), $\tilde{Y}'_i$ can be written as:

$$\tilde{Y}'_i = Y'_i + T_i N_{c1,i} \tag{14}$$

With these notations, the mutual information in the secrecy constraint (6) can be written as:

$$I\left(W; M_e, \tilde{Y}^n, \tilde{Y}'^n, T^n\right) \tag{15}$$

We next examine the first stage in detail. We begin by defining the binary valued function $\beta()$ such that for a positive constant $\delta \in (0, 1/2)$ and $\alpha = 1/2 - \delta$,

$$\beta(\tilde{\mathbf{H}}_i) = \left\{ \begin{array}{l} 0, |\tilde{H}_{i,0}|^2 > \alpha \\ 1, |\tilde{H}_{i,0}|^2 < \alpha, |\tilde{H}_{i,1}|^2 > \alpha \end{array} \right. \tag{16}$$

Note that since $\alpha < 1/2$, $\beta()$ is well defined due to the fact that $|\tilde{H}_{i,0}|^2 + |\tilde{H}_{i,1}|^2 = 1$.

Define E_i as

$$E_i = \beta_i(\tilde{\mathbf{H}}_i) \oplus T_i \tag{17}$$

where $\oplus$ denotes the binary XOR operation. Then E_i is independent from $\tilde{\mathbf{H}}_i$.

We next express the signals received by the eavesdropper during the first stage so that they are degraded versions of signals which are function of E_i, $\tilde{X}_i$ and Gaussian noise only.

Observe that (12) can be rewritten as:

$$\tilde{Y}_i = \tilde{H}_{i,1-T_i}\tilde{X}_i + |\tilde{H}_{i,T_i}|\tilde{J}_i \tag{18}$$

with $\tilde{J}_i$ having the same distribution as J_i but independent from $\tilde{\mathbf{H}}_i$ and T_i. We can do this modification because it does not change the joint distribution of W and eavesdropper's knowledge implied by the following distribution

$$p_W(w)\, p_{V^n|W}(v^n|w)\{\prod_{i=1}^n f_{\tilde{X}_i}(\tilde{x}_i)\}\{\prod_{i=1}^n p_T(t_i)\} f_{M_e}(m_e)$$

$$\prod_{i=1}^n\{f_{\tilde{\mathbf{H}}_i|\tilde{Y}^{i-1},M_e}\left(\tilde{\mathbf{h}}_i|\tilde{y}^{i-1}, m_e\right) f_{\tilde{Y}_i|T_i,\tilde{X}_i,\tilde{\mathbf{H}}_i}\left(\tilde{y}_i|t_i, \tilde{x}_i, \tilde{\mathbf{h}}_i\right)$$

$$f_{\tilde{Y}'_i|V_i,\tilde{X}_i,T_i}(\tilde{y}'_i|v_i, \tilde{x}_i, t_i)\} \tag{19}$$

because the distribution of $\tilde{J}_i$ is rotationally invariant. This means the value of (15) remains the same.

When $E_i = 0$, we have $1 \geq |H_{i,T_i}|^2 > \alpha = 1/2 - \delta$.

Since $|\tilde{H}_{i,0}|^2 + |\tilde{H}_{i,1}|^2 = 1$, we have $|H_{i,1-T_i}|^2 \leq 1/2 + \delta$.

Define $|\gamma|$ as a positive constant such that:

$$\frac{1/2 - \delta}{1/2 + \delta} = |\gamma|^2 \tag{20}$$

Then $|H_{i,1-T_i}|^2|\gamma|^2 \leq |H_{i,T_i}|^2$.

Hence when $E_i = 0$, we can rewrite (18) as:

$$\tilde{H}_{i,1-T_i}(\tilde{X}_i + |\gamma|J'_i) + \sqrt{|\tilde{H}_{i,T_i}|^2 - |\tilde{H}_{i,1-T_i}|^2|\gamma|^2} J''_i \tag{21}$$

where the sequence $\{J'_i\}$ and $\{J''_i\}$ have the same distribution as $\{J_i\}$ conditioned on all other random variable and are independent from each other. In particular, they are also independent from $\tilde{\mathbf{H}}_i$ and T_i. We can rewrite (18) as (21) since it does not change the joint distribution of W and eavesdropper's knowledge implied by the distribution (19).

If $E_i = 1$, to unify the notation, we rewrite (18) as:

$$\tilde{H}_{i,1-T_i}\tilde{X}_i + |\tilde{H}_{i,T_i}|J''_i \tag{22}$$

We then write (21) and (22) in a unified form:

$$\tilde{H}_{i,1-T_i}(\tilde{X}_i + \psi_\delta[E_i, J'_i]) + \phi_\delta[T_i, \tilde{\mathbf{H}}_i, J''_i] \tag{23}$$

$$\psi_\delta[E_i, J'_i] = \left\{ \begin{array}{ll} |\gamma|J'_i, & E_i = 0 \\ 0, & E_i = 1 \end{array} \right. \tag{24}$$

$$\phi_\delta[T_i, \tilde{\mathbf{H}}_i, J''_i] = \left\{ \begin{array}{ll} \sqrt{|\tilde{H}_{i,T_i}|^2 - |\tilde{H}_{i,1-T_i}|^2|\gamma|^2} J''_i, & E_i = 0 \\ |\tilde{H}_{i,T_i}|\tilde{J}''_i, & E_i = 1 \end{array} \right. \tag{25}$$

where E_i is computed from T_i and $\tilde{\mathbf{H}}_i$ according to (17).

Define $\tilde{Z}_i$ as

$$\tilde{Z}_i = \tilde{X}_i + \psi_\delta[E_i, J'_i] \tag{26}$$

Then $\tilde{Y}_i$ can be expressed as

$$\tilde{Y}_i = \tilde{H}_{i,1-T_i}\tilde{Z}_i + \phi_\delta[T_i, \tilde{\mathbf{H}}_i, J''_i] \tag{27}$$

To proceed to bound (15), we need the following lemma:

Lemma 1: Let the symbol A_i^n denote the set $\{A_i, A_{i+1}, ..., A_n\}$. A_{n+1}^n is empty. Then for $m = 2, ..., n+1$,

$$I\left(W; M_e, Y'^n, \tilde{Y}^{m-1}, \tilde{\mathbf{H}}^{m-1}, T^{m-1}, \tilde{Z}_m^n, E_m^n\right) \leq \tag{28}$$

$$I\left(W; M_e, Y'^n, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-2}, T^{m-2}, \tilde{Z}_{m-1}^n, E_{m-1}^n\right) \tag{29}$$

Proof: The proof is provided in Appendix A. ■

Using Lemma 1 we can replace $\{\tilde{Y}^n, \tilde{\mathbf{H}}^n, T^n\}$ with $\{\tilde{Z}^n, E^n\}$ and use (14) to obtain the following Lemma:

Lemma 2:

$$I\left(W; \tilde{Y}'^n, \tilde{Y}^n, M_e, T^n\right) \leq I\left(W; Y'^n, \tilde{Z}^n, E^n\right) \tag{30}$$

The proof of Lemma 2 is omitted due to space limitations and is provided in the upcoming journal version of this work.

Lemma 2 shows that when designing the stochastic encoder that maps W to V^n, we can design it for a wiretap channel which takes inputs V^n and in the eavesdropper channel produces outputs $\{Y'^n,\tilde{Z}^n,E^n\}$ and in the main channel produces the outputs: $\{\tilde{Y}'^n+N'^n_{c0},J^n_0+N^n_{c0},J^n_1,T^n\}$ where N^n_{c0} and N'^n_{c0} denote the channel noise of the main channel during the first and the second stage respectively.

It can then be shown with standard methods that there exists a codebook and a stochastic encoder that achieves the following secrecy rate for the above wiretap channel:

$$\left[I\left(V;\tilde{Y}'+N'_{c0},J_0+N_{c0},J_1,T\right)-I\left(V;Y',\tilde{Z},E\right)\right]^+ \tag{31}$$

which, by Lemma 2, secures W for the two-way wiretap channel as well. We then evaluate (31) with a Gaussian input distribution with zero mean and variance P for V,J_0,J_1, and use the fact $|\gamma|$ can be made arbitrarily close to 1, which yields (9). It can be readily verified that by choosing $P=(\bar{P}-1)/2$, the average power constraint (4) is satisfied.

V. Conclusion

In this work we presented a new setting in information theoretic security which allows the eavesdropper to control the states of the eavesdropper channel based on the channel outputs it observed in the past in an arbitrary (and potentially stochastic) manner. With this new setting, we studied the Gaussian two-way wiretap channel and proved that it *is* possible to achieve a positive secrecy rate for this model that scales with transmission power.

Appendix A
Proof of Lemma 1

Equation (28) is upper bounded by adding the term $\tilde{Z}_{m-1}$ as shown below:

$$\begin{aligned}
&I\left(W;\tilde{Y}^{m-1},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}^n_{m-1},E^n_m,Y'^n\right) &&(32)\\
=&I\left(W;\tilde{Y}_{m-1}|\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}^n_{m-1},E^n_m,Y'^n\right)\\
+&I\left(W;\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}^n_{m-1},E^n_m,Y'^n\right) &&(33)
\end{aligned}$$

We next show that the first term in (33) is 0:

$$\begin{aligned}
&I\left(W;\tilde{Y}_{m-1}|\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}^n_{m-1},E^n_m,Y'^n\right)\\
&\leq I(W;J''_{m-1}\\
&\qquad|\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}^n_{m-1},E^n_m,Y'^n) &&(34)\\
&\leq I(W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}^n_{m-1},Y'^n;J''_{m-1}\\
&\qquad|E^n_m) &&(35)\\
&= I(W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n;J''_{m-1}\\
&\qquad|E^n_m)+I(\tilde{Z}^n_m;J''_{m-1}|E^n_m,\\
&\qquad\qquad W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n) &&(36)
\end{aligned}$$

where (34) follows from (27) and the fact that $\tilde{Z}_{m-1},T_{m-1},\tilde{\mathbf{H}}_{m-1}$ are present as condition terms.

We then observe

$$I(W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n;J''_{m-1}) \tag{37}$$

equals 0 because J''_{m-1} is independent from all the other terms in (37). In particular, Y'^n is the signals transmitted by node 0 in the second stage and is independent from J''_{m-1}.

Then we use the fact that for random variable A,B,C,D,

$$I\left(A;B|C,D\right)-I\left(A;B|C\right)\leq I\left(B;D|C,A\right) \tag{38}$$

where $I(A;B|C)$ corresponds to (37) with C being empty, $I(A;B|C,D)$ corresponds to the first term in (36). (38) implies the first term in (36) is upper bounded by:

$$\begin{aligned}
&I(J''_{m-1};E^n_m|W,\\
&\quad\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n) &&(39)\\
\leq&I(J''_{m-1},W,\\
&\quad\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n;E^n_m) &&(40)\\
\leq&I(J''_{m-1},W,\\
&\quad\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n,\tilde{\mathbf{H}}^n_m;E^n_m) &&(41)\\
=&I\left(\tilde{\mathbf{H}}^n_m;E^n_m\right)+I(J''_{m-1},W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},\\
&\quad M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n;E^n_m|\tilde{\mathbf{H}}^n_m) &&(42)\\
=&I\left(\tilde{\mathbf{H}}^n_m;E^n_m\right)+I(J''_{m-1},W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},\\
&\quad M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n;T^n_m|\tilde{\mathbf{H}}^n_m) &&(43)\\
=&I(J''_{m-1},W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},\\
&\quad M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n;T^n_m|\tilde{\mathbf{H}}^n_m) &&(44)\\
\leq&I(J''_{m-1},W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},\\
&\quad M_e,T^{m-1},\tilde{Z}_{m-1},\tilde{\mathbf{H}}^n_m,V^n,\tilde{X}^n,N^n_J;T^n_m)=0 &&(45)
\end{aligned}$$

In (44), we drop the term $I\left(\tilde{\mathbf{H}}^n_m;E^n_m\right)$ since it is 0 due to (17) and the fact that T_i is uniformly distributed and independent from $\tilde{\mathbf{H}}_i$ and T^n_m is generated *after* the first stage. From (44) to (45), we replace the term Y'^n using (13). (45) is 0 because T^n_m is independent from all the other random variables in this term. In particular, T^n_m is independent from $\{\tilde{X}^n,T^{m-1}\}$.

Hence we have shown that the first term in (36) is 0. The second term in (36) is upper bounded by:

$$\begin{aligned}
&I(\tilde{Z}^n_m,\tilde{X}^n_m;J''_{m-1}|E^n_m,\\
&\qquad W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n) &&(46)\\
=&I(\tilde{Z}^n_m;J''_{m-1}|E^n_m,\\
&\qquad\tilde{X}^n_m,W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n)\\
&+I(\tilde{X}^n_m;J''_{m-1}|E^n_m,\\
&\qquad W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n) &&(47)
\end{aligned}$$

Using (26), the first term in (47) is upper bounded by:

$$\begin{aligned}
&I(J'^n_m;J''_{m-1}|E^n_m,\\
&\qquad\tilde{X}^n_m,W,\tilde{Y}^{m-2},\tilde{\mathbf{H}}^{m-1},M_e,T^{m-1},\tilde{Z}_{m-1},Y'^n) &&(48)
\end{aligned}$$

since $\tilde{X}^n_m$ and E^n_m are present in the condition term. Since

$$I(J'^n_m;J''_{m-1}|$$

$$W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) = 0, \quad (49)$$

we can subtract (48) by (49) and upper bound it via the inequality in (38) as

$$\begin{aligned} &I(J''_{m-1}; E^n_m, \tilde{X}^n_m | J'^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) \qquad (50) \\ &= I(J''_{m-1}; \tilde{X}^n_m | J'^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) \\ &+ I(J''_{m-1}; E^n_m | \tilde{X}^n_m, J'^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) \qquad (51) \end{aligned}$$

The first term in (51) is upper bounded by:

$$\begin{aligned} &I(J''_{m-1}; \tilde{X}^n_m, J'^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) = 0 \qquad (52) \end{aligned}$$

since J''_{m-1} is independent from all the other terms in (52).

The second term in (51) is upper bounded by:

$$\begin{aligned} &I(J''_{m-1}, \tilde{X}^n_m, J'^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n; E^n_m) \qquad (53) \\ &\leq I(J''_{m-1}, \tilde{X}^n_m, J'^n_m, \tilde{\mathbf{H}}^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n; E^n_m) \qquad (54) \\ &= I(\tilde{\mathbf{H}}^n_m; E^n_m) + I(J''_{m-1}, \tilde{X}^n_m, J'^n_m, W, \\ &\qquad \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n; T^n_m | \tilde{\mathbf{H}}^n_m) \qquad (55) \\ &\leq I(J''_{m-1}, J'^n_m, W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, \\ &\qquad V^n, \tilde{X}^n, N^n_J, \tilde{\mathbf{H}}^n_m; T^n_m) = 0 \qquad (56) \end{aligned}$$

where in (56), we replace Y'^n with $V^n, \tilde{X}^n, N^n_J$, which allows us to merge the term $\tilde{X}^n_m$ into $\tilde{X}^n$.

Hence, we have shown that the first term in (47) is 0. The second term in (47) is upper bounded by moving E^n_m out of the condition terms as shown below:

$$\begin{aligned} &I(\tilde{X}^n_m, E^n_m; J''_{m-1} | \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) \qquad (57) \\ &= I(\tilde{X}^n_m; J''_{m-1} | W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, \\ &\qquad M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) + I(E^n_m; J''_{m-1} | \tilde{X}^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) \qquad (58) \end{aligned}$$

The first term in (58) is upper bounded by:

$$\begin{aligned} &I(\tilde{X}^n_m, W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, \\ &\qquad Y'^n; J''_{m-1}) = 0 \qquad (59) \end{aligned}$$

since J''_{m-1} is independent from all the other terms in (59). The second term in (58) is upper bounded by:

$$\begin{aligned} &I(E^n_m; J''_{m-1}, \tilde{X}^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Y}_{m-1}, Y'^n) \qquad (60) \\ &\leq I(E^n_m; \tilde{\mathbf{H}}^n_m, J''_{m-1}, \tilde{X}^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n) \qquad (61) \\ &= I(E^n_m; \tilde{\mathbf{H}}^n_m) + I(T^n_m; J''_{m-1}, \tilde{X}^n_m, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, Y'^n | \tilde{\mathbf{H}}^n_m) \qquad (62) \\ &\leq I(T^n_m; J''_{m-1}, \tilde{X}^n, V^n, N^n_J, \\ &\qquad W, \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}_{m-1}, \tilde{\mathbf{H}}^n_m) = 0 \qquad (63) \end{aligned}$$

where in (63) we replace Y'^n with $V^n, \tilde{X}^n, N^n_J$, which allows us to merge the term $\tilde{X}^n_m$ into $\tilde{X}^n$.

Hence, we have shown that the second term in (58) is 0. This means the second term in (47) is 0. Thus we have shown that the second term in (36) is 0. This implies that the first term in (33) is 0. The second term in (33) is upper bounded by adding E_{m-1}:

$$I\left(W; \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-1}, \tilde{Z}^n_{m-1}, E^n_{m-1}, Y'^n\right) \quad (64)$$

from which we then drop T_{m-1} due to the presence of both $\tilde{\mathbf{H}}_{m-1}$ and E_{m-1} and rewrite it as:

$$I\left(W; \tilde{Y}^{m-2}, \tilde{\mathbf{H}}^{m-1}, M_e, T^{m-2}, \tilde{Z}^n_{m-1}, E^n_{m-1}, Y'^n\right) \quad (65)$$

from which we then drop $\tilde{\mathbf{H}}_{m-1}$ due to the presence of M_e and $\tilde{Y}^{m-2}$, which leads to (29). Hence, we have proved Lemma 1.

References

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

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

[3] 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.

[4] Y. Liang and H. V. Poor. Multiple Access Channels With Confidential Messages. *IEEE Transactions on Information Theory*, 54(3):976–1002, 2008.

[5] A. Khisti and G. Wornell. Secure Transmission with Multiple Antennas-II: The MIMOME Wiretap Channel. *IEEE Transactions on Information Theory*, 56(11):5515–5532, November 2010.

[6] E. Ekrem and S. Ulukus. The Secrecy Capacity Region of the Gaussian MIMO Multi-receiver Wiretap Channel. *IEEE Transactions on Information Theory*, 57(4):2083–2114, April 2011.

[7] E. Tekin and A. Yener. Achievable Rates for the General Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy. In *Allerton Conference on Communication, Control, and Computing*, September 2006.

[8] E. Tekin and A. Yener. The Multiple Access Wire-Tap Channel: Wireless Secrecy and Cooperative Jamming. In *The Information Theory and Applications Workshop*, January 2007.

[9] E. Tekin and A. Yener. Achievable Rates for Two-Way Wire-Tap Channels. In *International Symposium on Information Theory*, June 2007.

[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. 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.

[14] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti. Achieving Single Channel, Full Duplex Wireless Communication. In *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, September 2010.