Two-Hop Untrusted Relay Channel with an External Eavesdropper Under Layered Secrecy Constraints

Ahmed A. Zewail and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
zewail@psu.edu yener@engr.psu.edu

***Abstract*—We consider a Gaussian network consisting of a source that aims to communicate to its legitimate destination via an untrusted relay node in the presence of an external eavesdropper. The source wishes to send two independent messages to the destination: one message must be kept secret from the external eavesdropper only, while the other message must be kept secret from the external eavesdropper and the untrusted relay both. We identify achievable secure rates under these layered secrecy constraints. Considering a two-hop half-duplex setup, we employ the destination as a cooperative jammer in the first phase in order to help provide secrecy from the relay and the external eavesdropper, and the source as a cooperative jammer in the second phase in order to detriment the external eavesdropper. The source encodes its messages using stochastic encoding and security embedding coding. We provide the secrecy analysis and present numerical results to demonstrate the performance of the proposed achievability technique. Our study points to the value of the source serving as a cooperative jammer as well as the need for power control policies at the legitimate nodes in order to ensure secrecy in this system.**

I. Introduction

Cooperative relays can play different roles in enhancing wireless communications. Due to the broadcast nature of the wireless medium, communication can be overheard by non-authorized entities, i.e., external eavesdroppers. In order to keep the communicated data streams confidential from an external eavesdropper, cooperative nodes, i.e., relays, can adjust their strategies to inject the eavesdropper channel with sufficient amount of randomness to ensure that the security constraints are satisfied [1]. The relay node can also act as a cooperative jammer by sending noise signals in order to reduce the capacity of the eavesdropper channel. References [2]–[5] considered different scenarios that include cooperation with trusted relays under physical layer security requirements.

Different than these aforementioned works, cooperation with an *untrusted*, i.e., honest-but-curious, relay has been proposed in [6]. The untrusted relay is a relevant model for cooperation in wireless ad-hoc networks, where intermediate nodes follow the network protocols, however, the communicated data should be kept secret from them. Therefore, security constraints are imposed at the relay nodes to ensure the confidentiality of the transmitted messages. Consequently, while decode-and-forward as a relaying strategy is not an option, compress-and-forward [6]–[9], amplify-and-forward [10], compute-and-forward [11]–[14], have been shown to be effective techniques to improve the end-to-end secure rates. It worth mentioning that even if there is no direct link between the source nodes and the destinations, with the help of cooperative jamming [15], non-zero secure rates are achievable when the untrusted relay is the enabler of communications [7], [12].

In this paper, we investigate the role of cooperation with relays under the both aforementioned confidentiality concerns. We consider a network where a source aims to communicate securely with its destination via an *untrusted* relay node in the presence of an *external eavesdropper*. In particular, we wish to investigate the impact of *layered secrecy constraints* [16] on end-to-end secure communication rates. The source thus aims to send two independent messages to the legitimate destination: the first message must be kept secret from the external eavesdropper, while the second message must be kept secret from the external eavesdropper and the untrusted relay both. Such a model captures the case where the source can trust the untrusted relay for part of the transmitted information but not all of it. Since, we only impose decodability constraints at the legitimate destination, this model differs from the ones in [9] [17], where there are two legitimate destinations with different levels of security clearance.

We consider a two-hop scenario where the untrusted relay is the enabler of communication due to the absence of a direct link between the source and destination. The network nodes are equipped with one antenna each and are not able to receive and transmit simultaneously. Thus, the communication alternates over two phases. In the first phase, the source transmits its signal to the untrusted relay, while the destination jams with a Gaussian noise to confuse the untrusted relay and external eavesdropper. In the second phase, the relay performs amplify-and-forward as a relaying strategy, while the source jams the external eavesdropper with Gaussian noise. The destination uses its knowledge about its jamming signal, during the first phase, to eliminate its impact on the received signal from the relay in order to decode the desired messages. On the other hand, the external eavesdropper overhears signals over the two phases, i.e., the source information signal corrupted with the

This work was supported in part by the National Science Foundation Grants CCF 13-19338 and CNS 13-14719.

978-1-5090-1328-9/16/$31.00 ©2016 IEEE

destination jamming noise and the relay signal corrupted with the source jamming signal. We provide an achievable region for this network, where the source encodes its messages using security embedding coding, and rate splitting [18] [16]. In particular, the layered secrecy constraints allow us to utilize one message as a randomization index to protect the other message from the untrusted relay. An insight revealed by our results is that while the destination's role as a cooperative jammer is crucial for providing secrecy from the untrusted relay, the role of the source as a cooperative jammer is also invaluable to ensure secrecy from the external eavesdropper.

The remainder of this paper is organized as follows. In Section II, we describe the system model. Section III states the main result of this paper. Section IV details the achievability technique. Section V contains the equivocation calculations. In Section VI, we provide numerical results to illustrate the performance of the proposed achievability technique. Finally, Section VII concludes the paper.

II. Channel model

The network consists of a source, S, a destination, D, an untrusted relay, R, and an external eavesdropper, E, as shown in Fig. 1. No direct link exists between the source and destination. S aims to send two independent messages to the destination via the untrusted relay:

- W_1, uniformly distributed over the set $\{1, 2, .., 2^{nR_1}\}$, must be kept secret from E only.
- W_2, uniformly distributed over the set $\{1, 2, .., 2^{nR_2}\}$, must be kept secret from E and R both.

All nodes in the network operate in half-duplex mode. The communications alternate between two phases. For simplicity, each phase occurs over n channel uses, although it is straight forward to extend our analysis to different time sharing factors than $\frac{1}{2}$. In the first phase, S transmits its signal to the untrusted relay, while D performs cooperative jamming with Gaussian noise. At channel use i, the untrusted relay and external eavesdropper receive

$$Y_R(i) = \sqrt{h_1}X_S(i) + \sqrt{h_2}X_D(i) + Z_R(i), \quad i = 1, .., n, \tag{1}$$

$$Y_E(i) = \sqrt{g_1}X_S(i) + \sqrt{g_2}X_D(i) + Z_E(i), \quad i = 1, .., n, \tag{2}$$

where X_S (X_D) is the transmitted signal by S (D), $\sqrt{h_1}$ ($\sqrt{h_2}$) is the channel gain between S (D) and the untrusted relay node, R, $\sqrt{g_1}$ ($\sqrt{g_2}$) is the channel gain between S (D) and the external eavesdropper, E, and Z_R (Z_E) is a zero-mean unit-variance Gaussian noise signal at R (E). The transmitted signals in the first phase have to satisfy power constraints

$$\frac{1}{n}\sum_{i=1}^{n} E[X_S^2(i)] \leq \bar{P}_S, \quad \frac{1}{n}\sum_{i=1}^{n} E[X_D^2(i)] \leq \bar{P}_D. \tag{3}$$

In the second phase, R performs amplify-and-forward (AF). We choose AF for tractability, noting that compress-and-forward or compute-and-forward are also possibilities. The relay transmits

$$X_R = \sqrt{\alpha h_1}X_S + \sqrt{\alpha h_2}X_D + \sqrt{\alpha}Z_R, \tag{4}$$

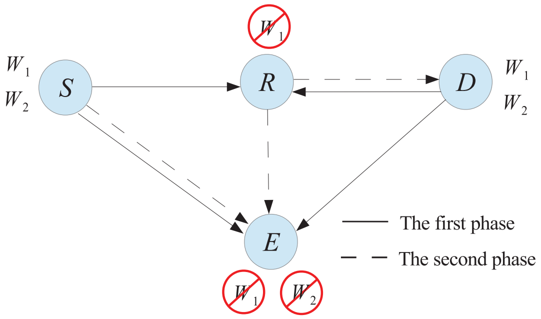

Fig. 1: Two-hop untrusted relay wiretap channel with layered secrecy constraints.

where α is chosen to satisfy the relay's average power constraint $\frac{1}{n}\sum_{i=1}^{n} E[X_R^2(i)] \leq \bar{P}_R$. In the second phase, S performs cooperative jamming with Gaussian noise. At channel use j, $j = n+1, .., 2n$, D and E thus receive

$$Y_D(j) = \sqrt{h_2}X_R(j) + Z_R(j), \tag{5}$$

$$Y_E(j) = \sqrt{g_1}X_J(j) + \sqrt{g_3}X_R(j) + Z_E(j), \tag{6}$$

where X_J is cooperative jamming signal with average power constraint $\frac{1}{n}\sum_{i=1}^{n} E[X_J^2(i)] \leq \bar{P}_J$, $\sqrt{g_3}$ is the channel gain from R to E, and Z_D is a zero-mean unit-variance Gaussian noise signal at D. The secrecy constraints are

$$\frac{1}{2n}I(W_1; Y_R^{2n}) \leq \epsilon, \tag{7}$$

$$\frac{1}{2n}I(W_1, W_2; Y_E^{2n}) \leq \epsilon, \tag{8}$$

where $Y_k^n = \{Y_k(1), Y_k(2) \cdots, Y_k(n)\}$.

Observe that in this model, at the destination, we impose decodability constraints on both messages, i.e., it should decode W_1 and W_2 with vanishing probability of error. On the other hand, at the untrusted relay, we only impose a secrecy constraint on W_1, and we do not impose a decodability nor secrecy constraint on W_2, while, at the external eavesdropper, we impose secrecy constraints on both W_1 and W_2. These requirements can be satisfied by using security embedding encoding instead of superposition encoding [18], [16] as illustrated in Section IV.

III. Main Result

Before stating the main result, we define the following terms

$$C_1 = 0.5\log_2\left(1 + \frac{\alpha h_1 h_2 P_S}{1 + \alpha h_2}\right), \tag{9}$$

$$C_2 = 0.5\log_2\left(1 + \frac{h_1 P_S}{1 + h_2 P_D}\right), \tag{10}$$

$$C_3 = 0.5\log_2\left(1 + \boldsymbol{g^T K_Z^{-1} g} P_S\right), \tag{11}$$

where $\alpha(1+h_1P_S+h_2P_D)\le\bar{P}_R$, $0\le P_k\le\bar{P}_k$, $k\in\{S,D,J\}$, $\boldsymbol{g}=\begin{bmatrix}\sqrt{g_1}\\ \sqrt{\alpha g_3 h_1}\end{bmatrix}$ and

$$\boldsymbol{K_Z}=\begin{bmatrix}g_2P_D+1 & \sqrt{\alpha g_2g_3h_2}P_D\\ \sqrt{\alpha g_2g_3h_2}P_D & \alpha g_3h_2P_D+g_1P_J+\alpha g_3+1\end{bmatrix}.$$

Theorem 1. *Any rate pair (R_1,R_2) that satisfies*

$$R_1\le\frac{1}{2}[C_1-C_2]^+, \tag{12}$$

$$R_1+R_2\le\frac{1}{2}[C_1-C_3]^+, \tag{13}$$

is achievable under the layered secrecy constraints, where $[x]^+=\max(0,x)$. □

In Sections IV and V, we prove Theorem 1.

IV. Achievablility

Depending on the values of C_1, C_2 and C_3, we have several cases, to consider for achievability. Due to space constraints we examine the most interesting case where $C_1>C_2>C_3$ in detail. For the remaining cases, please see Remark 2 in Section V. First, we divide this case into two sub-cases, defined by Regions I and II, in Fig. 2.

A. Region I: $R_2\le C_2-C_3$

The achievability technique for this region utilizes security embedding coding [18], i.e., the message W_2 serves as a randomization index to secure the message W_1 at the untrusted relay. In particular, for any rate pair, (R_1,R_2), in Region I, the source generates 2^{nR_c} codebooks according to $\mathcal{N}(0,P_S)$, such that each codebook contains $2^{n(R_1+R_2+R_2^x)}$ codewords. Then, the codewords of each codebook are randomly distributed over 2^{nR_1} bins such that each bin has $2^{n(R_2+R_2^x)}$ codewords. Each bin is indexed by w_1, where $w_1\in\{1,2,..,2^{nR_1}\}$, i.e., the set of possible values of W_1. Furthermore, the codewords in each bin are indexed by (w_2,w_2^x), where $w_2\in\{1,2,..,2^{nR_2}\}$, i.e., the set of possible values of W_2, and $w_2^x\in\{1,2,..,2^{nR_2^x}\}$ which represents a set of dummy messages. The role of these dummy messages is demonstrated in subsection V-A. To send a pair of messages (W_1,W_2), the source uniformly chooses one of its codebooks and a value for the dummy message W_2^x, then from the bin indexed by W_1, it transmits the codeword indexed by (W_2,W_2^x). Next, the relay amplifies and forwards its received signal to the destination. After canceling the impact of its cooperative jamming signal, X_D, the destination can decode W_1 and W_2, reliably, i.e., with vanishing probability of error whenever [19]

$$R_c+R_2^x+R_2+R_1\le 0.5C_1. \tag{14}$$

The values of R_c and R_2^x will be specified later.

B. Region II: $R_2>C_2-C_3$

In this case, the scheme utilizes rate splitting in addition to security embedding codes. In particular, we divide the message W_2 into two sub-messages, W_{21}, with rate R_{21}, and W_{22}, with rate R_{22}, such that $R_2=R_{21}+R_{22}$, and $R_1+R_{21}\le 0.5[C_1-C_2]$. We generate 2^{nR_c} codebooks each of which contains $2^{n(R_1+R_2)}$ different codewords with elements drawn from $\mathcal{N}(0,P_S)$. The codewords of each codebook are distributed randomly over $2^{n(R_1+R_{21})}$ equal-size bins. Each bin is indexed by a value of (w_1,w_{21}), while the codewords within a bin are indexed by w_{22}. To transmit a pair of messages (W_1,W_2), the source randomly chooses one of the codebooks and from the bin indexed by (W_1,W_{21}), transmits the codeword indexed by W_{22} over the channel. The relay forwards a scaled version of its received signal. After canceling its cooperative jamming signal, the destination is able to decode W_1 and W_2 correctly as long as

$$R_c+R_{21}+R_{22}+R_1\le 0.5C_1. \tag{15}$$

Remark 1. In reference [20], the source node alternates over multiple codebooks to encode its confidential message, and the codebook index is shared with the destination via the feedback using a proper wiretap code. Therefore, the destination does jointly typical decoding over the codewords of the known codebook. In our achievability scheme, the index of the codebook is not known at the destination a priori. Thus, the receiver has to perform jointly typical decoding over the all possible $2^{n(R_1+R_2+R_2^x+R_c)}$ codewords, which requires the sum rate constraints (14) and (15). ■

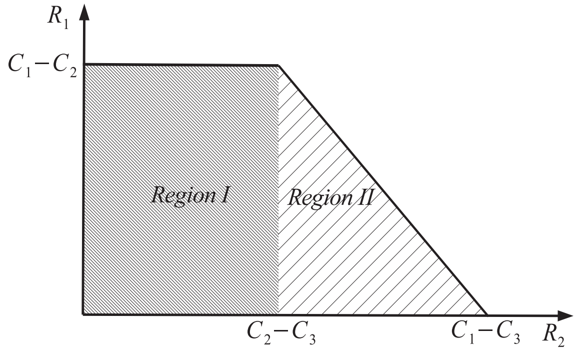

Fig. 2: The achievable rate region when $C_1>C_2>C_3$.

V. Equivocation Analysis

In this section, we calculate the equivocation rates produced by the achievability scheme, described in subsections IV-A and IV-B. Observe that the received signals by the external eavesdropper over the two phases can be equivalently expressed as the received signal of an eavesdropper with two receive antennas, as follows

$$\boldsymbol{Y}_E(i)=\boldsymbol{g}X_S(i)+\boldsymbol{Z}(i), \tag{16}$$

where $i=1,..,n$, $j=i+n$, $\boldsymbol{g}=\begin{bmatrix}\sqrt{g_1}\\ \sqrt{\alpha g_3h_1}\end{bmatrix}$, and

$$\boldsymbol{Z}(i)=\begin{bmatrix}\sqrt{g_2}X_D(i)+Z_E(i)\\ \sqrt{\alpha g_3h_2}X_D(i)+Z_E(j)+\sqrt{\alpha g_3}Z_R(i)+\sqrt{g_1}X_J(j)\end{bmatrix}.$$

A. Region I: $R_2 \le C_2 - C_3$

1) At the external eavesdropper: First, we note that

$$I(W_1, W_2; Y_E^{2n}) \le I(W_1, W_2, W_2^x; Y_E^{2n}). \tag{17}$$

Therefore, if $I(W_1, W_2, W_2^x; Y_E^{2n}) \le 2n\epsilon$, then the secrecy constraint at the external eavesdropper is satisfied.

$$\begin{aligned}
&H(W_1, W_2, W_2^x | Y_E^{2n}) = H(W_1, W_2, W_2^x | \boldsymbol{Y}_E^n) \\
&= H(W_1, W_2, W_2^x | \boldsymbol{Y}_E^n) - H(W_1, W_2, W_2^x | \boldsymbol{Y}_E^n, X_S^n) && (18)\\
&= I(W_1, W_2, W_2^x; X_S^n | \boldsymbol{Y}_E^n) && (19)\\
&= h(X_S^n | \boldsymbol{Y}_E^n) - h(X_S^n | \boldsymbol{Y}_E^n, W_1, W_2, W_2^x) && (20)\\
&\ge h(X_S^n | \boldsymbol{Y}_E^n) - n\epsilon_1 && (21)\\
&= h(X_S^n) - I(X_S^n; \boldsymbol{Y}_E^n) - n\epsilon_1. && (22)
\end{aligned}$$

(21) follows from the fact that with the knowledge of the W_1, W_2, and W_2^x, E can decode the codebook index, if

$$R_c \le \frac{1}{4}\log_2(1 + P_S \boldsymbol{g}^T \boldsymbol{K}_{\boldsymbol{Z}}^{-1} \boldsymbol{g}). \tag{23}$$

Now, we focus on the term $I(X_S^n; \boldsymbol{Y}_E^n)$

$$\begin{aligned}
I(X_S^n; \boldsymbol{Y}_E^n) &= h(\boldsymbol{Y}_E^n) - h(\boldsymbol{Y}_E^n | X_S^n) && (24)\\
&= h(\boldsymbol{Y}_E^n) - h(\boldsymbol{Z}^n) && (25)\\
&\le \sum_{i=1}^{n} h(\boldsymbol{Y}_E(i)) - \sum_{i=1}^{n} h(\boldsymbol{Z}(i)) && (26)\\
&= \sum_{i=1}^{n} [h(\boldsymbol{Y}_E(i)) - h(\boldsymbol{Y}_E(i) | X_S(i))] && (27)\\
&= \sum_{i=1}^{n} I(\boldsymbol{Y}_E(i), X_S(i)) && (28)\\
&= \sum_{i=1}^{n} I(\boldsymbol{V}_{MMSE} \boldsymbol{Y}_E(i), X_S(i)) && (29)\\
&\le \frac{n}{2}\log_2(1 + P_S \boldsymbol{g}^T \boldsymbol{K}_{\boldsymbol{Z}}^{-1} \boldsymbol{g}). && (30)
\end{aligned}$$

(26) follows from the fact that conditioning cannot increase the entropy and $\boldsymbol{Z}(i)$'s are independent due to the nature of its i.i.d. Gaussian components. In (29), we utilize the information theoretic optimality of the MMSE in SIMO setup under Gaussian signaling [21]. Plugging (30) in (22) gives

$$\begin{aligned}
H(W_1, W_2, W_2^x | Y_E^{2n}) \ge & nR_1 + nR_2 + nR_2^x + nR_c - n\epsilon_1 \\
& - \frac{n}{2}\log_2(1 + P_S \boldsymbol{g}^T \boldsymbol{K}_{\boldsymbol{Z}}^{-1} \boldsymbol{g}). && (31)
\end{aligned}$$

2) At the untrusted relay:

$$\begin{aligned}
H(W_1 | Y_R^n) &= H(W_1 | Y_R^n) - H(W_1 | Y_R^n, X_S^n) && (32)\\
&= I(W_1; X_S^n | Y_R^n) && (33)\\
&= h(X_S^n | Y_R^n) - h(X_S^n | Y_R^n, W_1) && (34)\\
&\ge h(X_S^n | Y_R^n) - n\epsilon_2 && (35)\\
&= h(X_S^n) - I(X_S^n; Y_R^n) - n\epsilon_2. && (36)
\end{aligned}$$

(35) follows from the fact that given W_1, the untrusted relay can decode X_S^n, with vanishing probability of error, if

$$R_c + R_2^x + R_2 \le 0.5C_2. \tag{37}$$

From (36), we have

$$H(W_1 | Y_E^{2n}) \ge nR_1 + nR_2 + nR_2^x + nR_c - nC_2 - n\epsilon_2. \tag{38}$$

By choosing R_c to be arbitrary close to C_3, and R_2^x to make $R_2 + R_2^x$ arbitrary close to $C_2 - C_3$, we can satisfy (7) and (8).

B. Region II: $R_2 > C_2 - C_3$

1) At the external eavesdropper:

$$\begin{aligned}
&H(W_1, W_2 | Y_E^{2n}) \\
&\quad = H(W_1, W_2 | \boldsymbol{Y}_E^n) - H(W_1, W_2 | \boldsymbol{Y}_E^n, X_S^n) && (39)\\
&\quad = I(W_1, W_{21}, W_{22}; X_S^n | \boldsymbol{Y}_E^n) && (40)\\
&\quad = h(X_S^n | \boldsymbol{Y}_E^n) - h(X_S^n | \boldsymbol{Y}_E^n, W_1, W_{21}, W_{22}) && (41)\\
&\quad \ge h(X_S^n | \boldsymbol{Y}_E^n) - n\epsilon_3 && (42)\\
&\quad = h(X_S^n) - I(X_S^n; \boldsymbol{Y}_E^n) - n\epsilon_3. && (43)
\end{aligned}$$

(42) follows from the fact that with the knowledge of the W_1, W_{21} and W_{22}, the external eavesdropper can decode the codebook index, whenever (23) is satisfied. From (43), we get

$$H(W_1, W_2 | \boldsymbol{Y}_E^n) \ge nR_1 + nR_2 + nR_c - nC_3 - n\epsilon_3. \tag{44}$$

2) At the untrusted relay: Note that

$$I(W_1; Y_R^n) \le I(W_1, W_{21}; Y_R^n). \tag{45}$$

Consequently, if $I(W_1, W_{21}; Y_R^n) \le n\epsilon$, then the secrecy constraint, $I(W_1; Y_R^n) \le n\epsilon$, is satisfied.

$$\begin{aligned}
&H(W_1, W_{21} | Y_R^n) \\
&\quad = H(W_1, W_{21} | Y_R^n) - H(W_1, W_{21} Y_R^n, X_S^n) && (46)\\
&\quad = I(W_1, W_{21}; X_S^n | Y_R^n) && (47)\\
&\quad = h(X_S^n | Y_R^n) - h(X_S^n | Y_R^n, W_1, W_{21}) && (48)\\
&\quad \ge h(X_S^n | Y_R^n) - n\epsilon_4 && (49)\\
&\quad = h(X_S^n) - I(X_S^n; Y_R^n) - n\epsilon_4. && (50)
\end{aligned}$$

(49) follows from the fact that given W_1 and W_{21}, the untrusted relay can decode X_S^n, as long as

$$R_c + R_{22} \le 0.5C_2. \tag{51}$$

From (50), we obtain

$$H(W_1, W_{21} | Y_R^n) \ge nR_1 + nR_2 + nR_c - nC_2 - n\epsilon_4. \tag{52}$$

Therefore, by choosing R_c and R_{22} to be arbitrary close to C_3 and $C_2 - C_3$, respectively, we guarantee the satisfaction of the secrecy requirements.

Remark 2. For the different values of C_1, C_2 and C_3, we have the following remaining cases:

- $C_1 \le \min(C_2, C_3)$: $R_1 = R_2 = 0$.
- $C_3 < C_1 \le C_2$: In this case $R_1 = 0$, and the network reduces to a trusted relay network with external eavesdropper, where the source aims to communicate W_2 securely to its destination with the help of the relay [4].
- $C_2 \le C_3 < C_1$: In this case, the inequality (12) is loose, and the region is determined by (13) only, as demonstrated in Fig. 3. In this case, ensuring the secrecy

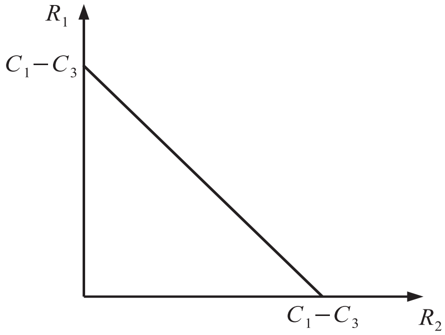

Fig. 3: The achievable rate region when $C_2 \leq C_3 < C_1$.

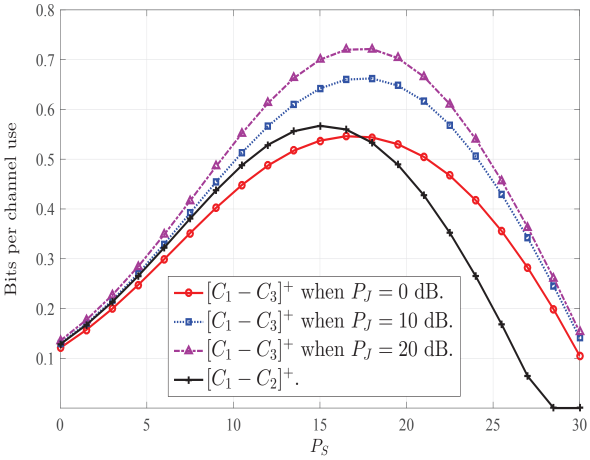

Fig. 4: The system performance when $P_R = P_D = 15$ dB, $h_1 = g_2 = 1$, $h_2 = g_3 = 0.8$, and $g_1 = 0.5$.

of W_1 and W_2 at the external eavesdropper, implies the secrecy of W_1 at the untrusted relay. The achievability of this case follows from the results in [22]. The source performs stochastic encoding [23] to provide sufficient amount of randomness in order to confuse the external eavesdropper and the untrusted relay. ■

VI. Discussion

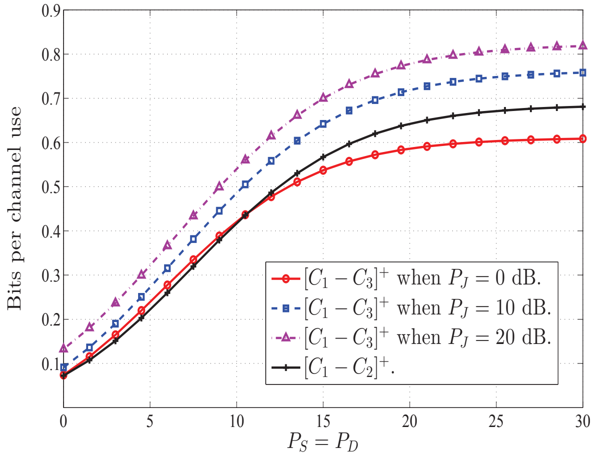

Fig. 5: The system performance when $P_R = 15$ dB, $h_1 = g_2 = 1$, $h_2 = g_3 = 0.8$, and $g_1 = 0.5$.

In this section, we provide numerical results to illustrate the performance of the proposed achievability scheme. We can gain from imposing the layered secrecy constraints at multiple eavesdroppers if we require fewer number of messages to be secured at the stronger eavesdropper. In this case, some transmitted messages serve as additional source of randomization to confuse the stronger eavesdropper. In our model, the external eavesdropper observes the transmitted signals over the two phases, while the untrusted relay receives during the first phase only. Therefore, we require the source to cooperatively jam the external eavesdropper during the second phase, in order to mitigate what she can gain from observing the relay's signal. In Fig. 4, we show the performance for different values of the source's cooperative jamming power. The role of the source jamming is crucial in reshaping the achievable rate region, as demonstrated in Figs. 2 and 3. Also, we can observe from Fig. 4 that for a fixed jamming power the achievable secure rates are not monotonically increasing in the source power. On the other hand, Fig. 5 shows the performance when the destination jamming power scales with the source transmit power. The achievable secure rates increase and saturate in the high power region. It is evident from these two figures that the system under investigation requires power control policies in order to maximize the achievable secure rates.

Outer bound

It worth mentioning that the outer bound derived in [7] can serve as an outer bound on the rate of the message W_1. By removing the external eavesdropper from the network in Fig. 1, our network reduces to the one in [7]. Clearly, any outer bound for the reduced network is also an outer bound on the original network as removing an eavesdropper cannot reduce the secrecy rate.

To obtain an outer bound on the sum rate, $R_1 + R_2$, we consider the network with a weaker eavesdropper. In particular, we remove the eavesdropper associated with relay node, i.e., we treat the relay as a trusted node. Moreover, we assume that the external eavesdropper can overhear the signals over the first phase only. Again, this can only increase the secrecy rates. In addition, we assume a genie that exchanges the transmitted signals between the relay and destination, i.e., the genie provides the relay with X_D^n, and the destination with X_R^n. Let $\mathcal{W} = \{W_1, W_2\}$, then we have

$$\begin{aligned}
&H(\mathcal{W}|Y_E^{2n}) \leq H(\mathcal{W}|Y_E^n) \\
&\leq H(\mathcal{W}|Y_E^n) - H(\mathcal{W}|X_R^n, X_D^n, Y_D^n) + n\epsilon && (53)\\
&= H(\mathcal{W}|Y_E^n) - H(\mathcal{W}|X_R^n, X_D^n) + n\epsilon && (54)\\
&\leq H(\mathcal{W}|Y_E^n) - H(\mathcal{W}|Y_R^n, X_R^n, X_D^n) + n\epsilon && (55)\\
&= H(\mathcal{W}|Y_E^n) - H(\mathcal{W}|Y_R^n, X_D^n) + n\epsilon && (56)\\
&= H(\mathcal{W}|Y_E^n) - H(\mathcal{W}|\sqrt{h_1}X_S^n + Z_R^n) + n\epsilon && (57)
\end{aligned}$$

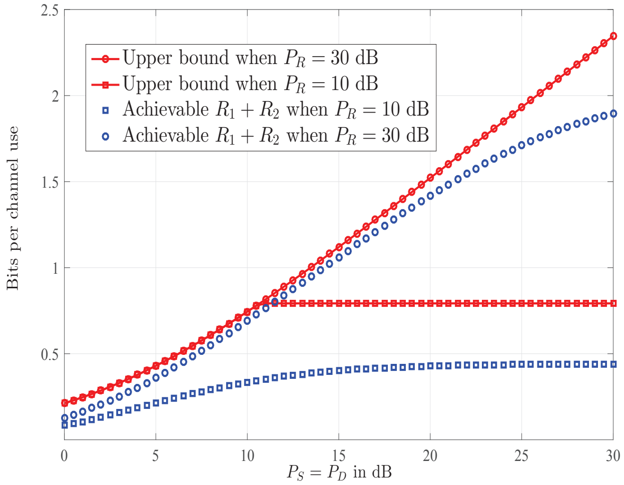

Fig. 6: Achievable sum rate vs the upper bound when $P_J = P_R$, $h_1 = g_2 = 1$, $h_2 = g_3 = 0.8$, and $g_1 = 0.5$.

$$= H(\mathcal{W}|Y_E^n) - H(\mathcal{W}|\sqrt{h_1}X_S^n + Z_R^n, Y_E^n) + n\epsilon \quad (58)$$
$$= I(\mathcal{W}; \sqrt{h_1}X_S^n + Z_R^n|Y_E^n) + n\epsilon \quad (59)$$
$$\leq I(\mathcal{W}, X_S^n; \sqrt{h_1}X_S^n + Z_R^n|Y_E^n) + n\epsilon \quad (60)$$
$$= I(X_S^n; \sqrt{h_1}X_S^n + Z_R^n|Y_E^n) + n\epsilon \quad (61)$$
$$= h(\sqrt{h_1}X_S^n + Z_R^n|Y_E^n) - h(\sqrt{h_1}X_S^n + Z_R^n|X_S^n, Y_E^n) + n\epsilon \quad (62)$$
$$= h(\sqrt{h_1}X_S^n + Z_R^n|Y_E^n) - h(Z_R^n|X_S^n) + n\epsilon. \quad (63)$$

Note that step (53) follows from applying Fano's inequality at the destination and the information exchange by the genie. Step (55) is due to the fact that conditioning cannot increase the entropy, and step (61) follows from the Markov chain $\mathcal{W} - X_S^n - Y_E^n$. Therefore, we can obtain the following bound

$$R_1 + R_2 \leq \frac{1}{4} \min \Big\{ \log_2(1 + h_2 P_R), \log_2 \left(1 + h_1 P_S - \frac{g_1 h_1 P_S^2}{1 + g_1 P_S + g_2 P_D} \right) \Big\}. \quad (64)$$

From the assumptions used to derive this outer bound, one can expect it to be not tight in general. In Fig. 6, we compare between the achievable sum rate and the upper bound for different power allocations. We can observe that when the source jamming and relay power are high the gap decreases between the achievable sum rate and the upper bound.

VII. Conclusions

In this work, we have investigated a Gaussian two-hop half-duplex untrusted relay channel with an external eavesdropper under layered secrecy constraints at the untrusted relay and at the eavesdropper. We have derived an achievable secure rate region for this network. In the achievability scheme, the source encodes the messages using stochastic encoding, security embedding encoding and rate splitting techniques, while the relay employs amplify-and-forward. In addition, the destination and source send cooperative jamming signals over the first and second phases, respectively. The numerical results demonstrate the crucial role of the source cooperative jamming signal in reshaping the achievable rate region, and the need of applying power control policies on all nodes, under the proposed scheme.

References

[1] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Info. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[2] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Proc.*, vol. 59, no. 10, pp. 4985–4997, 2011.

[3] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Proc.*, vol. 61, no. 6, pp. 1544–1554, 2013.

[4] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. on Info. Forensics and Security*, vol. 10, no. 3, pp. 574–583, 2015.

[5] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Proc.*, vol. 59, no. 10, pp. 4871–4884, 2011.

[6] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Info. Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[7] ——, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[8] A. A. Zewail and A. Yener, "The multiple access channel with an untrusted relay," in *IEEE Info. Theory Workshop (ITW)*, 2014.

[9] A. A. Zewail, M. Nafea, and A. Yener, "Multi-terminal networks with an untrusted relay," in *52 Annual Allerton Conf. On Communication, Control and Computing*, 2014.

[10] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Proc.*, vol. 60, no. 1, pp. 310–325, 2012.

[11] X. He and A. Yener, "Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay," *IEEE Trans. Info. Theory*, vol. 59, no. 1, pp. 177–192, 2013.

[12] ——, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Communications*, vol. 12, no. 1, pp. 1–11, 2013.

[13] V. Shashank and N. Kashyap, "Lattice coding for strongly secure compute-and-forward in a bidirectional relay," in *IEEE International Symposium on Info. Theory (ISIT)*, 2013.

[14] Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Secure transmission using an untrusted relay with scaled compute-and-forward," in *IEEE Info. Theory Workshop (ITW)*, 2015.

[15] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[16] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1841–1856, 2015.

[17] A. A. Zewail and A. Yener, "The two-hop interference untrusted-relay channel with confidential messages," in *IEEE Info. Theory Workshop (ITW)*, 2015.

[18] H. D. Ly, T. Liu, and Y. Blankenship, "Security embedding codes," *IEEE Trans. on Info. Forensics and Security*, vol. 7, no. 1, pp. 148–159, 2012.

[19] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2006.

[20] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Info. Theory*, vol. 59, no. 12, pp. 8115–8130, 2013.

[21] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[22] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[23] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.