This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

Multi-Terminal Two-Hop Untrusted-Relay Networks with Hierarchical Security Guarantees

Ahmed A. Zewail, *Student Member, IEEE,* and Aylin Yener, *Fellow, IEEE*

***Abstract*—We consider a two-source two-destination two-hop relay network, where all data communication must be kept secret from the relay node. The model considered is the simplest primitive that embodies a multi-transmitter multi-receiver network that needs to communicate sharing an untrusted relay node. We focus on two scenarios. In the first scenario, each source aims to send two messages to be kept secret from the relay: a common message that should be decoded by both destinations, and a private message that should be decoded by the first destination while kept secret from the second one. We define an achievable rate region by utilizing stochastic encoding at the sources, Gaussian noise cooperative jamming from the destinations, and compress-and-forward at the relay. In the second scenario, each source aims to send a confidential message to its intended destination which should be kept secret from the other one as well as the relay. We define an achievable rate region using a combination of nested lattice codes and random binning at the sources, structured cooperative jamming from destinations and scaled compute-and-forward at the relay. We also derive genie-aided outer bounds on the secrecy rate regions. We present numerical results that demonstrate the performance of the proposed achievable schemes. Overall, the work provides insights into how to utilize an untrusted relay to communicate to destinations with different levels of security clearance, and how intentional interference is an enabler of communication.**

***Index Terms*—Untrusted relays, two-hop communications, cooperative jamming, levels of security clearance.**

I. Introduction

Wireless ad-hoc networks offer an efficient solution to provide or enhance wireless coverage and are instrumental in realizing the soon to arrive Internet of Things era. In such networks, nodes act as relays for assisting others in their communication. As such, they are expected to obey the network protocols. At the same time, nodes can join and leave frequently and may not be fully vetted for confidentiality of data. This calls for a system design where information transmitted by the node is kept secret from relay nodes despite the cooperative nature of communications. In particular, the transmitted information should not be obtained by any node except the legitimate end users. The intermediate relay node in such a scenario is called an *untrusted-relay* [1]. From an information theoretic security point of view, this lack of trust is captured by considering an eavesdropper associated with the relay node that has a channel output that is identical to the one received by the relay [1], [2].

Cooperation with an untrusted-relay has been proven to be beneficial [1]. In reference [1], a single-source single-destination untrusted relay network has been investigated, and scenarios have been identified in which using compress-and-forward as a relaying strategy, an untrusted relay can improve the achievable secrecy rate. Untrusted relay models have also been studied when a relay node is the enabler of communication, i.e., the two-hop scenario without a direct link [3]. Reference [3] has shown that a positive secrecy rate is possible with the aid of cooperative jamming from the destination. In the case of a single-source single-destination multi-hop network, e.g., a line network, performing compress-and-forward at the relays results in accumulation of the quantization noise over the hops, which decreases the achievable end-to-end secrecy rate as the number of hops increases. Reference [4] provides an alternative achievable scheme using compute-and-forward relaying and structured signaling by nested lattice codes that yields a constant secrecy end-to-end communication rate irrespective of the number of hops, i.e., the number of intermediate untrusted relays. Additional work utilizing untrusted relays in single-source single-destination and multiple-source single-destination networks include references [5]–[9], and [10] respectively.

In this paper, we propose to utilize untrusted relays to assist in multi-terminal, i.e., multi-source, multi-destination communications; specifically, in designing wireless ad-hoc networks with various hierarchical security clearances. We consider the simplest model that embodies this notion: a two-source two-destination two-hop network utilizing an untrusted relay, under two different scenarios. In the first scenario, each source transmits two independent messages that should be kept secret from the untrusted relay. Furthermore, one of them, the common message, should be decoded by both destinations, while the other message should be decoded by the first destination and be kept secret from the other one. Thus, under this scenario, the first destination has higher level of security clearance compared to the second one. We define an achievable secrecy rate region, using stochastic encoding at the sources, compress-and-forward at the relay, and cooperative jamming by the destinations. All nodes, under this scenario, transmit Gaussian signals. Moreover, we derive genie-aided outer bounds on the secrecy rate region using the relay/eavesdropper separation technique [3]. It is worth mentioning that receivers with different levels of security clearance was considered in reference [11], which studied a three-user broadcast channel with three degraded message sets.

This work was supported in part by the National Science Foundation Grants CCF 13-19338 and CNS 13-14719. This work was presented in part at the 52nd Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Oct. 2014, and the IEEE Information Theory Workshop, Jeju Island, South Korea, Oct. 2015.

A. A. Zewail and A. Yener are with the School of Electrical Engineering and Computer Science, Pennsylvania State University, University Park, PA 16802 USA (e-mail: zewail@psu.edu; yener@ee.psu.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

In particular, the transmitter sends a common message that should be decoded by the three receivers, a secure message that should only be decoded by the first and the second receivers, and a private message that should only be decoded by the first receiver. This reference, however, studied a one-hop setup, and no untrusted relays, whereas our focus is on two-hop networks and the crucial role of the untrusted relay as an enabler of communication.

In the second scenario, we consider the case where each source aims to communicate a message to its intended destination. This message should be kept secret from the untrusted relay as well as the unintended destination. This scenario represents two-hop multi-terminal communication with confidential messages. We define a secrecy achievable rate region using a combination of stochastic encoding and lattice coding at the sources, scaled compute-and-forward at the relay [12] [13], and cooperative jamming from the destinations. In particular, the sources and destinations signal from nested lattice codebooks. The relay decodes two different integer combinations from the received four lattice points such that it can obtain two combinations, each of which represents the lattice points transmitted by a source-destination pair. Using Gaussian codebooks, the relay forwards these two combinations to both destinations.

Some of the material in this paper was presented in part in conference papers [14] and [15]. Section III of this paper generalizes the model and the analysis of [14]. In [14], the secrecy analysis is limited to the case where the user with higher level of security clearance contributes higher jamming power; this assumption is no longer needed in the generalized treatment we provide. Furthermore, here, we derive the outer bounds for the sum of common and private rates utilizing the decodability constraint at the user with higher security clearance. Section IV extends and improves upon the setting considered in [15], specifically by optimization of the MMSE and successive cancellation coefficients of the scaled compute-and-forward. This manuscript also provides detailed proofs as well as comprehensive numerical results that were not presented in the conference papers.

The remainder of the paper is organized as follows. Section II describes the system model. In Section III, we study the first scenario, where the destinations have different levels of security clearance. In Section IV, we investigate the second scenario, i.e., the two-hop interference network with confidential messages. Numerical results that show the performance of the achievability techniques are provided in Section V. Finally, Section VI summarizes our conclusions.

II. System model

Consider a two-source two-destination two-hop relay network depicted in Fig. 1. The sources, S_1 and S_2, have messages for destinations, D_1 and D_2. Assuming a sufficiently distance between the sources and destinations, we assume no direct link between them. Therefore, the relay node, which is untrusted, i.e., honest-but-curious, is the only enabler of communications between the sources and the destinations. Each node is equipped with a single antenna and cannot receive and transmit simultaneously, i.e., operates in a half-duplex mode.

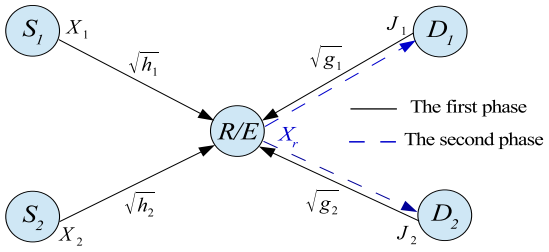

Fig. 1: The two-hop, two-source, two-destination network with an untrusted-relay.

The communication alternates between two phases. In the first phase, which occurs over l channel uses, the sources transmit their signals, X_1 and X_2, to the relay, while the destinations provide cooperative jamming with signals, J_1 and J_2. Therefore, at channel use i, the received signal by the untrusted relay is given by

$$Y_r(i) = \sum_{k=1}^{2} [\sqrt{h_k} X_k(i) + \sqrt{g_k} J_k(i)] + Z_r(i), \tag{1}$$

where Z_r is zero-mean Gaussian noise with unit variance and $\sqrt{h_k}$ ($\sqrt{g_k}$) is the channel gain between S_k (D_k) and the relay. During the second phase, which occurs over m channel uses, the relay transmits its signal, X_r, to both destinations, D_1 and D_2. The received signal by D_k, at channel use j, is given by

$$Y_k(j) = \sqrt{g_k} X_r(j) + Z_k(j), \tag{2}$$

where Z_k is the zero-mean Gaussian noise with unit variance.

The transmitted signals from S_k, the relay and D_k must satisfy the following average power constraints

$$\frac{1}{n} \sum_{i=1}^{n} E[X_k^2(i)] \le \bar{P}_k \quad k \in \{1, 2, r\}, \tag{3}$$

$$\frac{1}{n} \sum_{i=1}^{n} E[J_k^2(i)] \le \bar{P}_{Jk} \quad k \in \{1, 2\}, \tag{4}$$

where $n = l + m$ is the total number of channel uses.

Since, each node transmits over only one of the two phases, the transmitted signals are subject to *effective* average power constraints given by

$$P_r^{\max} = \frac{\bar{P}_r}{1-\eta}, \quad P_k^{\max} = \frac{\bar{P}_k}{\eta}, \quad P_{Jk}^{\max} = \frac{\bar{P}_{Jk}}{\eta}, \tag{5}$$

where $\eta = \frac{l}{n}$ is the time sharing factor of the first phase. In the remainder of this paper, we use the notation $Y^n = \{Y(1), Y(2), \cdots, Y(n)\}$, $C(x) \triangleq 0.5 \log_2(1+x)$ and $[x]^+ \triangleq \max(0, x)$.

Remark 1. *It worth noting that the model under investigation is equivalent to the one where two external jammers jam the relay during the first phase, and the cooperative jamming signal of each of them is conveyed to one of the destinations, which remains silent, over a noiseless link. Therefore, we can consider the received signal at D_k over the n channel uses to be $Y_k^n = \{J_k^l, Y_k^m\}$.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

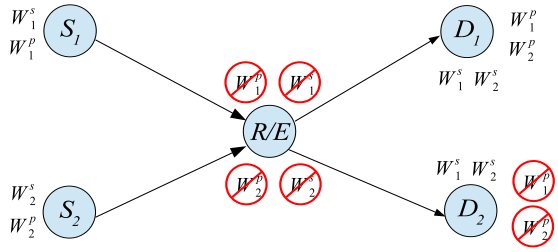

Fig. 2: Senario I: Users with different levels of security clearance.

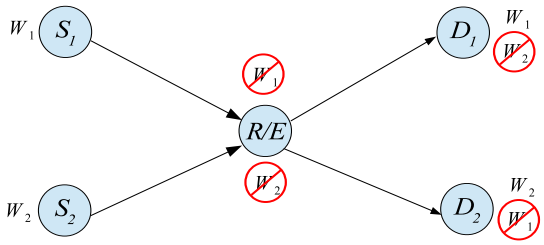

Fig. 3: Scenario II: Interference channel with confidential messages.

We consider two scenarios of this model where the sources wish to communicate securely to the destinations, keeping these messages secret from the relay.

A. Scenario I: Users with different levels of security clearance

In the first scenario, we utilize the untrusted relay to serve end users (legitimate receivers) with different levels of security clearance. In particular, we consider a scenario where S_k transmits two independent messages:

- A common message, W_k^s, with rate R_k^s, which should be decoded by both destinations, D_1 and D_2, and be kept secret *from the untrusted relay*.
- A private message, W_k^p, with rate R_k^p, that should be decoded by D_1 only and be kept secret *from both the untrusted relay and* D_2.

This setup, illustrated in Fig. 2, models a legitimate receiver, D_1, which has higher security clearance compared to the other legitimate receiver, D_2. Applications of such a setup include variety of ad-hoc network scenarios, e.g., healthcare monitoring networks, as well as tactical networks with command hierarchy. The above secrecy requirements are captured by the following constraints:

$$\frac{1}{n}H(\mathcal{S}|Y_r^n) \geq \frac{1}{n}H(\mathcal{S}) - \epsilon \qquad \forall \mathcal{S} \subseteq \mathcal{W}^{ps}, \tag{6}$$

$$\frac{1}{n}H(\mathcal{S}|Y_2^n) \geq \frac{1}{n}H(\mathcal{S}) - \epsilon \qquad \forall \mathcal{S} \subseteq \mathcal{W}^{p}, \tag{7}$$

where $\mathcal{W}^{ps} = \{W_1^s, W_2^s, W_1^p, W_2^p\}$ and $\mathcal{W}^{p} = \{W_1^p, W_2^p\}$.

B. Scenario II: Confidential messages to both users

In the second scenario, we consider the case where S_1 aims to send a confidential message W_1, with rate R_1, that should be decoded only by D_1 and be kept secret from D_2 as well as the untrusted relay. Similarly, S_2 aims to send a confidential message W_2, with rate R_2, that should be decoded only by D_2 and be kept secret from D_1 as well as the untrusted relay, as illustrated in Fig. 3. Therefore, we define the secrecy constraints at the unintended destinations and the untrusted relay as follows.

$$\frac{1}{n}H(W_2|Y_1^n, W_1, J_1^n) \geq \frac{1}{n}H(W_2) - \epsilon, . \tag{8}$$

$$\frac{1}{n}H(W_1|Y_2^n, W_2, J_2^n) \geq \frac{1}{n}H(W_1) - \epsilon, \tag{9}$$

$$\frac{1}{n}H(W_j|Y_r^n, W_k) \geq \frac{1}{n}H(W_j) - \epsilon \quad j,k = 1,2; j \neq k. \tag{10}$$

Remark 2. *The secrecy constraints in (10) ensure that* $\lim_{n\to\infty} \frac{1}{n} I(W_1, W_2; Y_r^n) = 0$, *since*

$$I(W_1, W_2; Y_r^n) = I(W_1; Y_r^n) + I(W_2; Y_r^n|W_1) \tag{11}$$

$$= H(W_1) - H(W_1|Y_r^n) + I(W_2; Y_r^n|W_1) \tag{12}$$

$$\leq H(W_1|W_2) - H(W_1|W_2, Y_r^n) + I(W_2; Y_r^n|W_1) \tag{13}$$

$$= I(W_1; Y_r^n|W_2) + I(W_2; Y_r^n|W_1). \tag{14}$$

(13) follows from the independence between W_1 *and* W_2, *and the fact that conditioning cannot increase the entropy.*

In the following, we study these scenarios, provide achievable secure rate regions and outer bounds.

III. Scenario I: Serving users with different levels of security clearance

Here, we define an achievable secrecy rate region for the considered scenario in Fig. 2. The achievability technique combines stochastic encoding at the sources [16], and compress-and-forward [17], at the relay with the help of cooperative jamming [18] from both destinations.

A. At the sources

Define $0 \leq \alpha_k \leq 1$ and $\bar{\alpha}_k = 1 - \alpha_k, k = 1, 2$. S_k generates $2^{l(R_k^s + R_k^{x1})}$ codewords, U_k^l, drawn from $\mathcal{N}(0, \bar{\alpha}_k P_k)$, where $0 \leq P_k \leq P_k^{\max}$, and distributes them over $2^{lR_k^s}$ bins, each of them is indexed by one of W_k^s's and contains $2^{lR_k^{x1}}$ codewords. Next, S_k generates $2^{l(R_k^p + R_k^{x2})}$ codewords, V_k^l, drawn from $\mathcal{N}(0, \alpha_k P_k)$ and distributes them over $2^{lR_k^p}$ bins, each of them is indexed by one of the W_k^p's and contains $2^{lR_k^{x2}}$ codewords. The randomization rate R_k^{x1} determines the bin size of the codebook of the common secure message which is designed to confuse the untrusted relay, while R_k^{x2} determines the bin size of the codebook of the private message which is chosen to confuse both the untrusted relay and D_2. The values of R_k^{x1} and R_k^{x2} will be specified later.

Finally, to send a pair (W_k^s, W_k^p), S_k chooses uniformly random codewords from the bins indexed by W_k^s and W_k^p, then transmits the sum of these two signals $X_k^l = U_k^l + V_k^l$.

Simultaneously, D_k transmits cooperative jamming signals in the form of zero-mean Gaussian noise with variance P_{Jk}, where $0 \leq P_{Jk} \leq P_{Jk}^{\max}$.

B. At the relay

The relay compresses its received signal Y_r^l into a quantized version $\hat{Y}_r^l$ and transmits the corresponding signal X_r^m. The elements of X_r^m are drawn from $\mathcal{N}(0, P_r)$, where $0 \leq P_r \leq$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

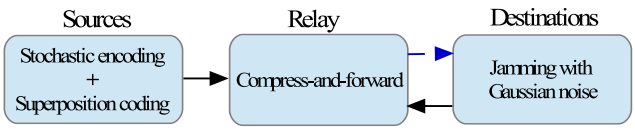

Fig. 4: Building blocks of the achievability scheme for scenario I.

$P_r^{\max}$. The scheme idea is summarized in Fig. 4. Now, we state the achievable secrecy rate region of this setup.

Theorem 1. *The secrecy rates that satisfy the following inequalities are achievable*

$$R_k^s \le \eta\left[\min_{q\in\{1,2\}}\left\{C\left(\frac{\bar{\alpha}_k h_k P_k}{1+g_q P_{Jq}+\alpha_1 h_1 P_1+\alpha_2 h_2 P_2+\sigma_Q^2}\right)\right\} - C\left(\frac{\bar{\alpha}_k h_k P_k}{1+g_1 P_{J1}+g_2 P_{J2}+h_j P_j+\alpha_k h_k P_k}\right)\right]^+, \quad (15)$$

$$R_1^s+R_2^s \le \eta\left[\min_{q\in\{1,2\}}\left\{C\left(\frac{\bar{\alpha}_1 h_1 P_1+\bar{\alpha}_2 h_2 P_2}{1+g_q P_{Jq}+\alpha_1 h_1 P_1+\alpha_2 h_2 P_2+\sigma_Q^2}\right)\right\}, - C\left(\frac{\bar{\alpha}_1 h_1 P_1+\bar{\alpha}_2 h_2 P_2}{1+g_1 P_{J1}+g_2 P_{J2}+\alpha_1 h_1 P_1+\alpha_2 h_2 P_2}\right)\right]^+, \quad (16)$$

$$R_k^p+R_k^s \le \eta\left[C\left(\frac{h_k P_k}{1+g_2 P_{J2}+\sigma_Q^2}\right)-C\left(\frac{h_k P_k}{1+g_1 P_{J1}+g_2 P_{J2}+h_j P_j}\right)\right]^+, \quad (17)$$

$$R_k^p \le \eta\left[C\left(\frac{\alpha_k h_k P_k}{1+g_2 P_{J2}+\sigma_Q^2}\right)-C\left(\frac{\alpha_k h_k P_k}{1+g_1 P_{J1}+\alpha_j h_j P_j+\sigma_Q^2}\right)\right]^+, \quad (18)$$

$$R_1^p+R_2^p \le \eta\left[C\left(\frac{\alpha_1 h_1 P_1+\alpha_2 h_2 P_2}{1+g_2 P_{J2}+\sigma_Q^2}\right)-C\left(\frac{\alpha_1 h_1 P_1+\alpha_2 h_2 P_2}{1+g_1 P_{J1}+\sigma_Q^2}\right)\right]^+, \quad (19)$$

$$\sum_{i=1}^{2} R_i^p+R_i^s \le \eta\left[C\left(\frac{h_2 P_2+h_1 P_1}{1+g_2 P_{J2}+\sigma_Q^2}\right)-C\left(\frac{h_2 P_2+h_1 P_1}{1+g_1 P_{J1}+g_2 P_{J2}}\right)\right]^+, \quad (20)$$

where $k, j \in \{1,2\}$, $k \neq j$, and $\forall \eta$, σ_Q^2 is the quantization noise variance which is determined such that

$$\eta C\left(\frac{h_1 P_1+h_2 P_2+g_q P_{Jq}+1}{\sigma_Q^2}\right) \le (1-\eta) C(g_k P_r), \quad k,q=1,2; k\neq q. \quad (21)$$

Proof. The reliability part is based on the achievability proof of the multiple-access relay channel [19, Section 3.2] [20, Section III-B3] and the detailed analysis is provided in Appendix A. □

C. Discussion

In this achievability technique, all network nodes use Gaussian signaling. In particular, the sources and relay signals are drawn from Gaussian codebooks, while the destinations cooperatively jam with Gaussian noise. It is worth noting that if we deactivate the second destination, i.e., $P_{J2} = 0$, and set the rates of the common messages to zero, the network reduces to a two-user multiple access untrusted-relay channel and the private rate region is equivalent to the one in [10] for $K = 2$.

1) Power control policies: The achievable rates increase with the increase in the time sharing factor η. In order to increase η, the relay should always transmit with its maximum power, $P_r^{\max}$. Also, observe that as the relay power becomes large, quatization noise variance becomes negligible, i.e., when $P_r \to \infty$, the optimal $\eta \to 1$ and the quantization noise variance $\sigma_Q^2 \to 0$. Also, it is easy to see that the power used for cooperative jamming, i.e., the intentional interference to impose security, plays a key role in obtaining non-zero secrecy rates. In particular, to have non-zero secure common rates, we need $\min(g_1 P_{J1}, g_2 P_{J2}) > \sigma_Q^2$. On the other hand, to have non-zero confidential rates, we need $g_1 P_{J1} > \sigma_Q^2$ and $g_1 P_{J1} > g_2 P_{J2}$. Generally, the achievable rates are not increasing functions in the transmitting powers, as for any fixed cooperative jamming power allocations, the secrecy rates go to zero as the transmit powers, P_1 and P_2 go to ∞. Therefore, the optimal power at source k may be less than $P_k^{\max}$, $k = 1, 2$.

2) Cooperative jamming strategies: Suppose that the objective of the two destinations is to maximize the rates of the common messages. Then, D_1 and D_2 should adjust their cooperative jamming powers such that $g_1 P_{J1} = g_2 P_{J2}$. It is evident from (16) that the common rate is governed by the term $\min(g_1 P_{J1}, g_2 P_{J2})$. On the other hand, we can observe that the right hand side of (19) increases with increase in P_{J1} and decrease in P_{J2}. Thus, to maximize the private sum rate, D_1 would jam with its maximum power and D_2 would reduce its cooperative jamming power. We illustrate these two observations via numerical results in Section V.

The previous observation gives the insight that if D_2 is replaced by an adversary jammer that has an objective to reduce the secure rate of the legitimate receiver, i.e., D_1, it can achieve its goal without a necessity of having a direct link to D_1, i.e., even it is not able to jam D_1 during the second phase. It is sufficient for this adversary jammer to jam the relay with its maximum power during the first phase.

D. Outer bounds

In this subsection, we derive genie aided outer bounds on the secrecy rates. We modify the relay/eavesdropper separation technique proposed in [3] as follows. First, we insert an external eavesdropper, E, whose channel statistics are the same as the one associated with the relay node. In particular, the received signal at this external eavesdropper, at channel use i, is given by

$$Y_e(i) = \sqrt{h_1} X_1(i)+\sqrt{h_2} X_2(i)+\sqrt{g_1} J_1(i)+\sqrt{g_2} J_2(i)+Z_e(i), \quad (22)$$

where Z_e is a zero-mean Gaussian noise with unit variance correlated with Z_r with correlation coefficient ρ. Since the external eavesdropper's observation is statistically equivalent to the one at the relay, ensuring the secrecy of the messages at this external eavesdropper, guarantees that these messages are also kept secret from the untrusted relay. Second, we remove

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

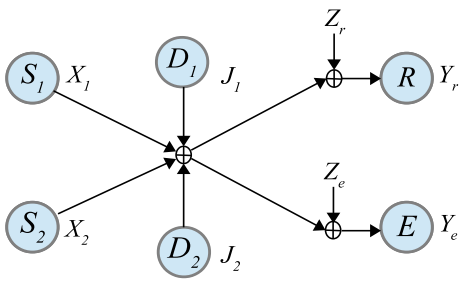

Fig. 5: An equivalent network used to calculate the outer bound.

the eavesdropper associated with the relay node, i.e., consider the relay to be trusted as illustrated in Fig. 5. Moreover, we assume that X_r is conveyed to both destinations as genie information. Lastly, we consider that one of the cooperative jamming signals, J_1, J_2, is given to the relay by a genie. The cooperative jamming signal given to the relay depends on the type of rates that we calculate the outer bound on.To derive the upper bounds on the common rates, we consider a genie transfers the cooperative jamming signal J_2^l to the relay, where the relay is now trusted after the aforementioned transformation, and then we utilize the secrecy constraint at E and the reliability constraint at D_2. On the other hand, to derive the upper bounds for the common and private rates, we consider a genie that provides cooperative jamming signal J_1^l to the relay, and we use the secrecy constraint at E and the reliability constraint at D_1. Note that, in deriving these upper bounds, we ignore the secrecy constraints on the private messages at D_2, and this action cannot decrease the secrecy rates for the private messages.

Theorem 2. *The secure rate region for the model under Scenario I is upper bounded by*

$$R_k^s \leq \max_{\eta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{\frac{\eta}{2}\log_2(A_k), (1-\eta)\min_k C(g_k P_r)\right\}, \quad (23)$$

$$R_1^s + R_2^s \leq \max_{\eta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{\frac{\eta}{2}\log_2 A, (1-\eta)\min_k C(g_k P_r)\right\}, \quad (24)$$

$$R_k^p + R_k^s \leq \max_{\eta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{\frac{\eta}{2}\log_2(B_k), (1-\eta)C(g_1 P_r)\right\}, \quad (25)$$

$$R_1^p + R_2^p + R_1^s + R_2^s \leq \max_{\eta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{0.5\eta\log_2(B), (1-\eta)C(g_1 P_r)\right\}, \quad (26)$$

where

$$A_k = \frac{[(1+O_t)(1+O_{ts}^k) - (O_{ts}^k+\rho)^2](O_{ts}^j+1)}{[(1+O_{ts}^j)(g_1P_{J1}+1) - (g_2P_{J1}+\rho)^2](1+O_t)}, \quad (27)$$

$$A = \frac{[(1+O_t)(1+O_t-g_2P_{J2}) - (O_t-g_2P_{J2}+\rho)^2](g_1P_{J1}+1)}{[(1+g_1P_{J1})^2 - (g_1P_{J1}+\rho)^2](1+O_t)}, \quad (28)$$

$$B_k = \frac{[(1+O_t)(1+O_{tp}^k) - (O_{tp}^k+\rho)^2](O_{tp}^j+1)}{[(1+O_{tp}^j)(g_2P_{J2}+1) - (g_2P_{J2}+\rho)^2](1+O_t)}, \quad (29)$$

$$B = \frac{[(1+O_t)(1+O_t-g_1P_{J1}) - (O_t-g_1P_{J1}+\rho)^2](g_2P_{J2}+1)}{[(1+g_2P_{J2})^2 - (g_2P_{J2}+\rho)^2](1+O_t)}, \quad (30)$$

$O_t = h_1P_1 + h_2P_2 + g_1P_{J1} + g_2P_{J2}$, $O_{tp}^k = h_kP_k + g_2P_{J2}$, $O_{ts}^k = h_kP_k + g_1P_{J1}$ *and* $k, j = 1, 2$, $k \neq j$.

Proof. The derivation is detailed in Appendix B. □

Remark 3. *Suppose that we focus only maximizing the private rates, i.e., we choose* $\alpha_1 = \alpha_2 = 1$ *and* $P_{J2} = 0$. *Also, consider the case where* $\bar{P}_r \to \infty$, *i.e.,* $\sigma_Q^2 = 0$ *and* $\eta = 1$. *When the source transmit power goes to* ∞, *the gap between the upper bound on the private sum rate and the achievable private sum rate converges to*

$$C\left(\frac{g_1P_{J1} + (\rho^*-1)^2}{1-\rho^{*2}}\right) - C(g_1P_{J1}), \quad (31)$$

where ρ^* *is given by*

$$\rho^* = 1 + g_1P_{J1} - \sqrt{g_1P_{J1} + \frac{(g_1P_{J1})^2}{4}}. \quad (32)$$

This gap is a function of the jamming power P_{J1} *only. As* P_{J1} *goes to* ∞, *the upper bounds are asymptotically tight.*

IV. Scenario II: Sending confidential messages via an untrusted relay

In this section, we focus on the second scenario illustrated in Fig. 3. From the results we obtained in the previous section for Scenario I, we readily observe that the destination which contributes more in cooperative jamming, is the one who ensures confidentiality of its messages from the other destination. This is evident from the condition of non-zero private rates in subsection III-C1. Therefore, under Scenario II, utilizing the previous scheme, with Gaussian signaling, will only allow one destination, D_1, to keep its message secret from the other destination and it is not possible to achieve secure positive rate for both destinations simultaneously. The same conclusion can be obtained if the relay employs amplify-and-forward under the same signaling scheme. These observations motivate us to consider structured signaling, under Scenario II, in order to achieve positive secure rates for both users, simultaneously. In particular, the sources and destinations transmit from nested lattice codebooks while the relay performs scaled compute-and-forward [12], [13]. In the following, we detail the achievability scheme.

A. The first phase

At each source, we use a nested lattice codebook as an inner code, and random binning as an outer code, similar to [4]. We start with the illustration of the inner code that is motivated by *scaled compute-and-forward* [12], [13].

Let us first set up the notation related to lattice codes. A lattice Λ is a discrete group of $\mathbb{R}^N$ such that: if $t_1^N, t_2^N \in \Lambda$, then $t_1^N + t_2^N \in \Lambda$. The lattice quantizer, $Q_\Lambda : \mathbb{R}^N \to \Lambda$, is defined as

$$Q_\Lambda(x^N) = \arg\min_{t^N\in\Lambda} ||t^N - x^N||, \quad (33)$$

where $||t^N - x^N||$ is the Euclidean distance between t^N and x^N. The quantization error is given by the modulo operation defined as

$$x^N \mod \Lambda = x^N - \arg\min_{t^N\in\Lambda} ||t^N - x^N||. \quad (34)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

The fundamental Voronoi region of Λ is defined to be

$$\mathcal{V}(\Lambda) = \{x^N : Q_\Lambda(x^N) = \mathbf{0}\}, \tag{35}$$

where $\mathbf{0}$ is all-zero vector with length N. Λ and Λ_k are nested lattices if $\Lambda_k \subseteq \Lambda$, where Λ is the coarse lattice, and Λ_k is the fine lattice. Let β_k be a non-zero real number and $\boldsymbol{\beta} = [\beta_1, .., \beta_4]^T$. Lattices $\Lambda_k \subseteq \Lambda$ for $k = 1, .., 4$, are constructed such that for Λ_k, we have

$$\frac{1}{N\text{Vol}(\mathcal{V}(\Lambda_k))} \int_{\mathcal{V}(\Lambda_k)} ||x^N||^2 dx = \beta_k^2 P. \tag{36}$$

1) Encoding at the sources and destinations: S_k generates its codebook $C_k = \Lambda \cap \mathcal{V}(\Lambda_k)$ with rate given by

$$R_k^c = \frac{1}{N} \log_2 |C_k| = \frac{1}{N} \log_2 \frac{\text{Vol}(\mathcal{V}(\Lambda_k))}{\text{Vol}(\mathcal{V}(\Lambda))}. \tag{37}$$

For simplicity of analysis, we assume without loss of generality that $\bar{P}_k = \bar{P}_{Jk} = P$, $k = 1, 2$. Each source-destination pair uses the same nested lattice codebook, i.e., D_1 uses the codebook C_1, D_2 uses the codebook C_2, and the scaling factors are $\beta_1 = \beta_3$ and $\beta_2 = \beta_4$. Each source-destination pair implements power control, so that we can assume $h_1 = g_1$ and $h_2 = g_2$, during the first phase of communication.

S_k applies stochastic encoding. More specifically, S_k divides the codewords of C_k into 2^{NR_k} bins, each of which is indexed by the corresponding W_k. The size of these bins are chosen to ensure the secrecy of the message W_k at the untrusted relay as we will see in appendix C. To send a message W_k, S_k randomly picks a point t_k^N from the bin indexed by W_k and transmits the corresponding signal X_k^N which is given by

$$X_k^N = (t_k^N/\beta_k + d_k^N) \mod \Lambda_k/\beta_k, \tag{38}$$

where d_k^N is a dither vector that is uniformly distributed over the scaled Voronoi region $\mathcal{V}(\Lambda_k)/\beta_k$, and it is assumed to be known at all network nodes.

Meanwhile, D_k randomly chooses $t_{k+2}^N \in C_k$, and transmits the corresponding signal J_k^N as

$$J_k^N = (t_{k+2}^N/\beta_k + d_{k+2}^N) \mod \Lambda_k/\beta_k. \tag{39}$$

2) Decoding at the relay: We require the relay to decode two different integer combinations of the received lattice points, whose coefficients are given by $\boldsymbol{a} = [a_1, .., a_4]^T$ and $\boldsymbol{b} = [b_1, .., b_4]^T$. We select $\boldsymbol{a}, \boldsymbol{b}$ from the set $\{[1, 0, 1, 0]^T$, $![0, 1, 0, 1]^T$, $[1, 1, 1, 1]^T\}$ and $\boldsymbol{a} \neq \boldsymbol{b}$. Observe that these combinations always satisfy $a_1 = a_3$, $a_2 = a_4$, $b_1 = b_3$ and $b_2 = b_4$.

To decode the first integer combination, the relay forms the following signal

$$\bar{y}_1^N = \alpha_1 Y_r^N - \sum_{k=1}^4 a_k\beta_k d_k^N = \sum_{k=1}^2 [(\alpha_1 h_k - a_k\beta_k)(X_k^N + J_k^N)] + \alpha_1 Z_r^N + \sum_{k=1}^2 a_k\beta_k(X_k^N + J_k^N) - \sum_{k=1}^4 a_k\beta_k d_k^N, \tag{40}$$

where α_1 is some real number. To simplify the notation, we define $\bar{z}_1^N = \sum_{k=1}^2 [(\alpha_1 h_k - a_k\beta_k)(X_k^N + J_k^N)] + \alpha_1 Z_r^N$. Now, we can express (40) as follows.

$$\bar{y}_1^N = \bar{z}_1^N + \sum_{k=1}^2 a_k\beta_k(X_k^N + J_k^N) - \sum_{k=1}^4 a_k\beta_k d_k^N \tag{41}$$

$$= \sum_{k=1}^4 a_k(\beta_k(t_k^N/\beta_k + d_k^N) - \beta_k Q_{\Lambda_k/\beta_k}(t_k^N/\beta_k + d_k^N)) + \bar{z}_1^N - \sum_{k=1}^4 a_k\beta_k d_k^N \tag{42}$$

$$= \bar{z}_1^N + \sum_{k=1}^4 a_k(t_k^N - Q_{\Lambda_k}(t_k^N + \beta_k d_k^N)) = \bar{z}_1^N + \sum_{k=1}^4 a_k \bar{t}_k^N, \tag{43}$$

where $\bar{t}_k^N = t_k^N - Q_{\Lambda_k}(t_k^N + \beta_k d_k^N)$. The relay is able to decode the integer combination $\sum_{k=1}^4 a_k \bar{t}_k^N$ that lies in the coarse lattice Λ by considering $\bar{z}_1^N$ as noise. Note that $\bar{z}_1^N$ and $\sum_{k=1}^4 a_k \bar{t}_k^N$ are independent, as the signals t_k^N and X_k^N are independent due to the nature of the dither vectors. Hence, the achievable rate for the first combination is given by

$$R_{k1} \leq \max\left(\max_{\alpha_1} 0.5 \log_2 \frac{\beta_k^2 P}{N_1(\alpha_1)}, 0\right), \tag{44}$$

where $N_1(\alpha_1)$ is the variance of $\bar{z}_1^N$ which is given by

$$N_1(\alpha_1) = 2\sum_{k=1}^2 (\alpha_1 h_k - a_k\beta_k)^2 P + \alpha_1^2. \tag{45}$$

The maximization of the rate in (44) is equivalent to minimizing N_1 over α_1, which results in the following value of N_1

$$N_1(\alpha_1^*) = ||\hat{\boldsymbol{a}}||^2 P - \frac{P^2(\boldsymbol{h}^T\hat{\boldsymbol{a}})^2}{1 + P||\boldsymbol{h}||^2}, \tag{46}$$

where $\boldsymbol{h} = [h_1, h_2, h_1, h_2]^T$ and $\hat{\boldsymbol{a}} = [\beta_1 a_1, .., \beta_4 a_4]^T$. Using the decoded combination $\sum_{k=1}^4 a_k \bar{t}_k^N$, the relay performs successive cancellation and forms the following signal to decode the second integer combination

$$\bar{y}_2^N = \alpha_2 Y_r^N - \sum_{k=1}^4 b_k\beta_k d_k^N - \lambda(\sum_{k=1}^4 a_k \bar{t}_k^N + \sum_{k=1}^4 a_k\beta_k d_k^N) \tag{47}$$

$$= \sum_{k=1}^2 [\alpha_2 h_k - (\lambda a_k + b_k)\beta_k](X_k^N + J_k^N) + \alpha_2 Z_r^N + \sum_{k=1}^4 b_k \bar{t}_k^N = \bar{z}_2^N + \sum_{k=1}^4 b_k \bar{t}_k^N, \tag{48}$$

where α_2 and λ are some real numbers, and $\bar{z}_2^N = \sum_{k=1}^2 [\alpha_2 h_k - (\lambda a_k + b_k)\beta_k](X_k^N + J_k^N) + \alpha_2 Z_r^N$ is the equivalent noise while decoding the integer combination $\sum_{k=1}^4 b_k \bar{t}_k^N$. Thus, we obtain the following rate for decoding the second integer combination

$$R_{k2|\boldsymbol{a}} \leq \max\left(\max_{\alpha_2, \lambda} 0.5 \log_2 \frac{\beta_k^2 P}{N_2(\alpha_2, \lambda)}, 0\right), \tag{49}$$

where $N_2(\alpha_2, \lambda)$ is the variance of $\bar{z}_2^N$ which is given by

$$N_2(\alpha_2, \lambda) = \sum_{k=1}^4 (\alpha_2 h_k - (\lambda a_k + b_k)\beta_k)^2 P + \alpha_2^2. \tag{50}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

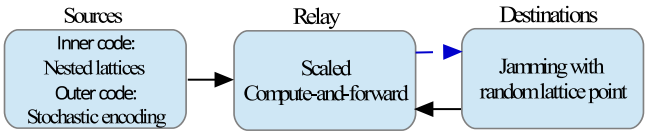

Fig. 6: Building blocks of the achievability scheme for scenario II.

The maximum rate in (49) is attained when N_2 is given by

$$N_2(\alpha_2^*, \lambda^*) = \hat{\boldsymbol{b}}^{\boldsymbol{T}}\hat{\boldsymbol{b}}P - 0.25\boldsymbol{q}^{\boldsymbol{T}}\boldsymbol{A}\boldsymbol{q}, \tag{51}$$

where $\hat{\boldsymbol{b}} = [\beta_1 b_1, .., \beta_4 b_4]^T$, $\boldsymbol{q}^T = \begin{bmatrix} -2\boldsymbol{h}^{\boldsymbol{T}}\hat{\boldsymbol{b}}P & 2\hat{\boldsymbol{b}}^{\boldsymbol{T}}\hat{\boldsymbol{b}}P \end{bmatrix}$, and $\boldsymbol{A} = \begin{bmatrix} 1+\boldsymbol{h}^T\boldsymbol{h}P & -\boldsymbol{h}^{\boldsymbol{T}}\hat{\boldsymbol{a}}P \\ -\boldsymbol{h}^{\boldsymbol{T}}\hat{\boldsymbol{a}}P & \hat{\boldsymbol{a}}^{\boldsymbol{T}}\hat{\boldsymbol{a}}P \end{bmatrix}$. The details of optimizing over α_1, α_2 and λ are provided in appendix D.

The achievable transmission rate of $\bar{t}_k^N$ is restricted by the rates of combinations that have a non-zero coefficient of $\bar{t}_k^N$ [13]. Therefore, we have the following conditions on the achievable transmission rates of $\bar{t}_1^N$ and $\bar{t}_2^N$.

$$R_1^1 \leq \begin{cases} R_{11} & \text{if } a_1 = 1 \text{ and } b_1 = 0, \\ R_{12|\boldsymbol{a}} & \text{if } a_1 = 0 \text{ and } b_1 = 1, \\ \min(R_{11}, R_{12|\boldsymbol{a}}) & \text{if } a_1 = 1 \text{ and } b_1 = 1, \end{cases} \tag{52}$$

$$R_2^1 \leq \begin{cases} R_{21} & \text{if } a_2 = 1 \text{ and } b_2 = 0, \\ R_{22|\boldsymbol{a}} & \text{if } a_2 = 0 \text{ and } b_2 = 1, \\ \min(R_{21}, R_{22|\boldsymbol{a}}) & \text{if } a_2 = 1 \text{ and } b_2 = 1. \end{cases} \tag{53}$$

B. The second phase

1) Encoding at the relay: After decoding of the two integer combinations $\sum_{k=1}^4 a_k\bar{t}_k^N$ and $\sum_{k=1}^4 b_k\bar{t}_k^N$ successfully, the relay has $\bar{t}_1^N + \bar{t}_3^N$ and $\bar{t}_2^N + \bar{t}_4^N$ that will be transmitted to both destinations during the second phase. The relay encodes each of them into a Gaussian codeword and forwards them to the destinations. More specifically, the linear integer combination $\bar{t}_1^N + \bar{t}_3^N$ is encoded into a codeword X_{r1}^m from a Gaussian codebook randomly generated according to $\mathcal{N}(0, \zeta_1 P_r)$, and the linear integer combination $\bar{t}_2^N + \bar{t}_4^N$ is encoded into a codeword X_{r2}^m from a Gaussian codebook randomly generated according to $\mathcal{N}(0, \zeta_2 P_r)$, where $\zeta_1 + \zeta_2 \in [0, 1]$ and $\zeta_1, \zeta_2 \geq 0$. Finally, the relay transmits the signal $X_r^m = X_{r1}^m + X_{r2}^m$.

2) Decoding at destinations: The channel from the relay to the destinations is a two-user broadcast channel. The weaker destination (i), i.e., $g_i \leq g_j, i, j \in \{1, 2\}$, decodes its desired signal X_{ri}^m by treating X_{rj}^m as noise. The stronger destination (j), decodes X_{ri}^m first and then does successive cancellation and decodes X_{rj}^m. The achievable rate region during the second phase is thus given by

$$R_i^2 \leq C\left(\frac{\zeta_i g_i P_r}{1 + \zeta_j g_i P_r}\right), \qquad R_j^2 \leq C(\zeta_j g_j P_r). \tag{54}$$

Note that there is one-to-one mapping between $\bar{t}_k^N$ and t_k^N given the knowledge of the dither vectors d_k^N [13]. Therefore, with the knowledge of its cooperative jamming signal and the received combination, D_k is able to decode it desired message. The scheme idea is summarized in Fig. 6.

Consequently, we can state the following theorem that represents the achievable rate region under the second scenario.

Theorem 3. *The following secrecy rate region is achievable for two-user two-hop interference untrusted-relay channel with confidential messages*

$$\max_{\boldsymbol{\beta},\eta,\boldsymbol{a},\boldsymbol{b},\zeta_1,\zeta_2} \Big\{ R_1 \leq \min(\eta[R_1^1 - 1]^+, (1-\eta)R_1^2), \\ R_2 \leq \min(\eta[R_2^1 - 1]^+, (1-\eta)R_2^2) \Big\}. \tag{55}$$

The proof of this theorem is completed in Appendix C.

C. Discussion

First, observe that the above achievability technique utilizes both structured and Gaussian signaling. In particular, the sources and destinations use nested lattice codebooks for sending the confidential messages and cooperative jamming, respectively, while the relay transmits using Gaussian codebooks. We prefer to forward using Gaussian codebooks during the second phase as they are known to achieve the capacity of the two-user Gaussian broadcast channel.

The secrecy constraints at the relay node result in the loss of 1 bit/channel use from the achievable transmission rate R_k^1. This 1 represents the bin size of the outer code required to guarantee the secrecy of the confidential messages at the untrusted relay as proven in appendix C-A. Therefore, our achievable scheme incurs a η bits channel loss as compared to when the relay is trusted, and this secrecy cost becomes negligible in high SNR.

It is worth noting that this achievable scheme ensures the secrecy of the confidential messages from any external eavesdropper that overhears the relay's signal during the second phase, as evident from the analysis in Appendix C. This observation illustrates how our scheme utilizes the untrusted relay as an encryption block.

We conclude this discussion section with two remarks.

Remark 4. *The achievability scheme can be extended to K-source K-destination two-hop interference untrusted-relay channel with confidential messages, where $K > 2$. The transmitted signals from the sources and destinations follow the same procedure. However, the relay is required to decode K different integer combinations of the received lattice points by performing noise prediction as in [13]. The coefficients of these combinations are chosen such that lattice points from a transmitter-receiver pair always the same. After that the second phase is equivalent to a K-user broadcast channel.*

Remark 5. *In developing the outer bounds in subsection III-D, we only considered the eavesdropper associated with the relay node. It is worth mentioning that this outer bound is applicable for the scenario considered in Section IV, as removing the eavesdroppers associated with the destinations cannot reduce the secrecy rate. Also, note that any outer bound that is obtained on $\frac{1}{n}H(W_k|Y_r^n)$ is also an outer bound on $\frac{1}{n}H(W_k|Y_r^n, W_j)$ as conditioning cannot increase the entropy.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

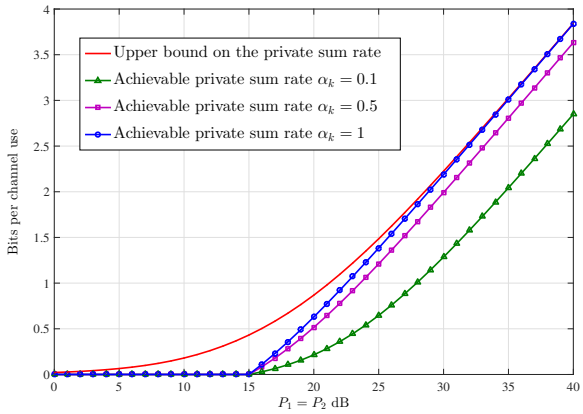

Fig. 7: Scenario I: Private sum rate vs transmit power when $P_r \to \infty$, $P_{J1} = P_1$, $P_{J2} = 15$ dB, $h_1 = h_2 = g_1 = g_2 = 1$ and optimal η.

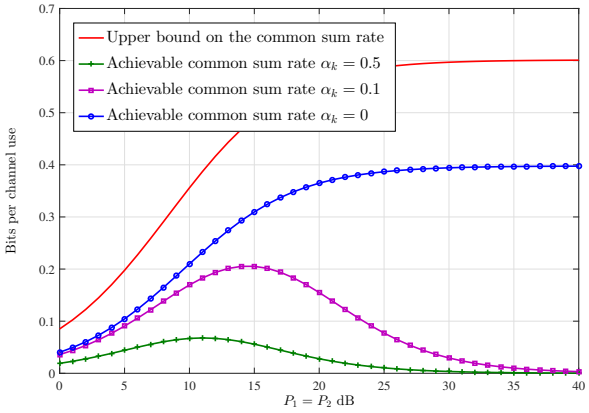

Fig. 8: Scenario I: Common sum rate vs transmit power when $P_r \to \infty$, $P_{J1} = 11$ dB, $P_{J2} = 10$ dB, $h_1 = h_2 = g_1 = g_2 = 1$ and optimal η.

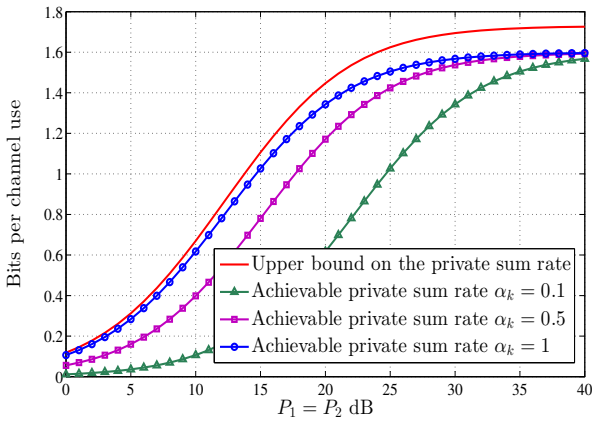

Fig. 9: Scenario I: Private sum rate vs transmit power when $P_r \to \infty$, $P_{J1} = 20$ dB, $P_{J2} = 10$ dB, $h_1 = h_2 = g_1 = g_2 = 1$ and optimal η.

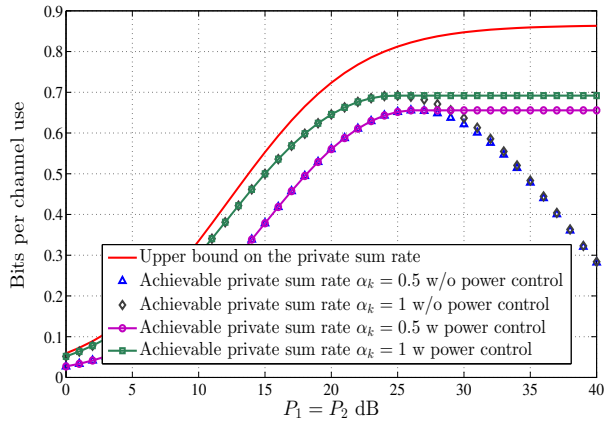

Fig. 10: Scenario I: Private sum rate vs transmit power when $P_r = 25$ dB, $P_{J1} = 20$ dB, $P_{J2} = 10$ dB, $h_1 = h_2 = g_1 = g_2 = 1$ and $\eta = 0.5$.

V. Numerical Results

In this section, we present numerical results that demonstrate the performance of the proposed schemes presented in Sections III and IV.

A. Scenario I

From Fig. 7, we observe that when $P_r \to \infty$, and the cooperative jamming power of D_1 is proportional to the transmitting power, i.e., $P_{J1} \propto P_1 + P_2$ while the cooperative jamming power of D_2 is fixed, the private sum rate is an increasing function in the transmitting powers. The gap between the outer bound and the achievable rate decreases with the increase of the fraction of transmitting power assigned for the private messages. In Fig. 8, we plot the achievable common sum rate for different fraction of power allocations at the sources and the outer bound for the case where cooperative jamming powers of D_1 and D_2 are fixed. We note that for the cases where $\alpha_k = 0.5, 0.1$, the achievable common rate is not monotonically increasing in the source powers. The reason behind this is that after a certain power level the interference due to the private messages signals, at D_2, significantly, decreases the achievable rates. From Fig. 9, we note that when the cooperative jamming powers are fixed, the private sum rate increases in the transmit power until it saturates. In this high power region, both the destinations and eavesdropper associated with the relay node have high signal-to-noise ratios.

For the case where the relay and cooperative jamming powers are limited, as in Fig. 10, we observe that the achievable private sum rates are not monotonically increasing with the sources' transmit powers, see subsection III-C1. The merit of applying a power control policy is evident from Fig. 10. Fig. 11 demonstrates that the proposed achievability scheme achieves strictly positive private and common rates, simultaneously, with fixed and limited relay and cooperative jamming powers. Again, Fig. 11 shows the need of applying power control polices at the sources.

Fig. 12 shows the achievable common sum rate under different values of cooperative jamming powers. It is evident that, for any power allocation at the sources, the achievable common secure rate is higher whenever the difference between the cooperative jamming powers is smaller. On the other hand, Fig. 13 demonstrates the decrease in the achievable private sum rate as the cooperative jamming power of D_2 increases. Figs. 12 and 13 demonstrate our observations in subsection III-C2. The non-zero rate condition for the private messages, indicated in subsection III-C1, can be readily seen from Figs.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

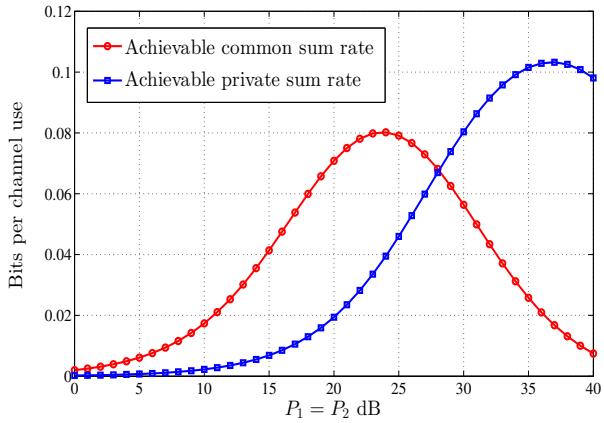

Fig. 11: Scenario I: Private and common sum rates vs transmit power when $P_r = 20$ dB, $P_{J1} = 20$ dB, $P_{J2} = 18$ dB, $h_1 = h_2 = g_1 = g_2 = 1$, $\alpha_k = 0.07$ and $\eta = 0.4$.

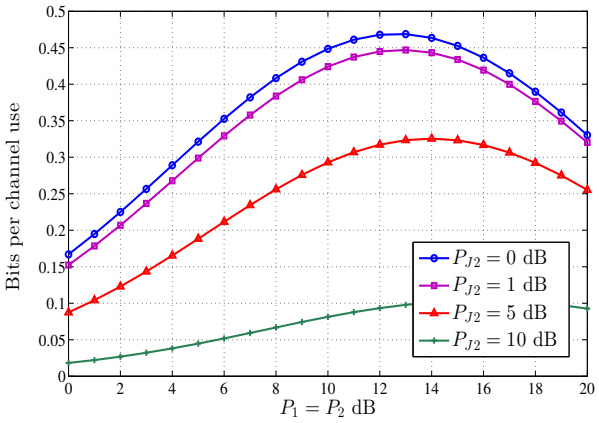

Fig. 13: Scenario I: Private sum rate for different values of P_{J2} when $P_r = 20$ dB, $P_{J1} = 12$ dB, $h_1 = h_2 = g_1 = g_2 = 1$, $\alpha_k = 1$ and $\eta = 0.5$.

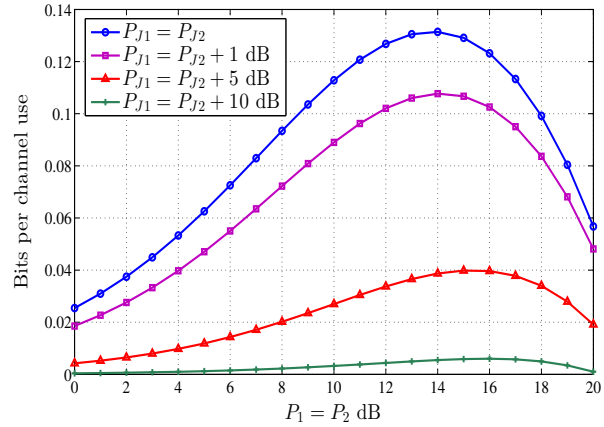

Fig. 12: Scenario I: Common sum rate for different values of P_{J1} when $P_r = 17$ dB, $P_{J2} = 10$ dB, $h_1 = h_2 = g_1 = g_2 = 1$, $\alpha_k = 0$ and $\eta = 0.5$.

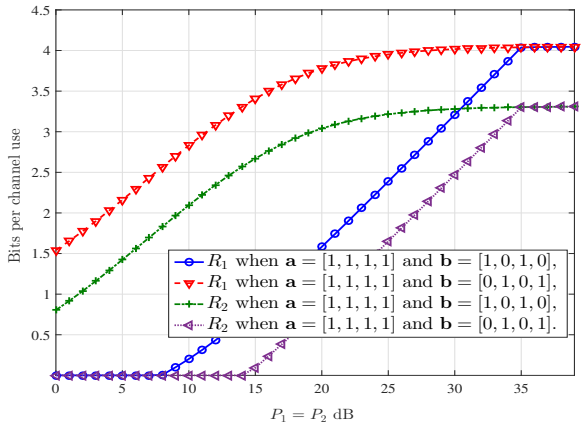

Fig. 14: Scenario II: Achievable secure rates vs transmit power when $\beta_1 = 0.2$, $\beta_2 = 0.12$, $P_r \to \infty$, $h_1 = g_1 = 1$, $h_2 = g_2 = 0.25$ and optimal η.

7 and 13.

B. Scenario II

In Fig. 14, we demonstrate that it is possible to have positive secure rates for both users simultaneously, with finite power budget at the sources. We plot the achievable secure rates for two different choices of decoding coefficients $\boldsymbol{a}$ and $\boldsymbol{b}$. We observe that there is no general optimal choice for the integer linear combinations that maximize the achievable secure rates for all cases. In addition, we observe that two different choices of the decoded combinations at the relay may lead to the same achievable secure rates under certain power region.

In Fig. 15, we plot the achievable secure sum rate for finite relay's power for two different choices of the decoded combinations at the relay. Again, we can observe the ability of structured signaling to achieve positive secure rates for both users simultaneously.

Fig. 16 shows the achievable secure sum rate when $\boldsymbol{a} = [1,1,1,1]^T$ and $\boldsymbol{b} = [1,0,1,0]^T$. We optimize over the time sharing factor, η, and the parameters of the second hop, ζ_1 and ζ_2. Clearly, increasing the relay's power cannot decrease the achievable secure rates of our scheme, however, it can be seen that multiple values of the relay's power can achieve the same secure rate, whenever the achievable secure rate region is governed by the rates of the first hop. Generally, we can conclude that to maximize the achievable secure rates there is a need of optimizing over all the achievable scheme parameters and implementing power control policies at all network terminals.

VI. Conclusions

We have investigated a two-source two-destination two-hop untrusted-relay network under two different scenarios various security clearance levels for the nodes. In the first scenario, the two destinations have different levels of security clearance: Each source transmits two messages that should be kept secret from the relay, and one message should be decoded by both destinations while the other one should be decoded by the first destination and be kept secret from the second one. We have defined an achievable rate region for this scenario, in which we combine stochastic encoding at the sources, cooperative jamming from destinations, and compress-and-forward at the relay, using Gaussian signaling.

In the second scenario, each source wishes to send a confidential message to its intended destination and should be kept secret from the other one. We have obtained an achievable region, by having each source use a combination of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

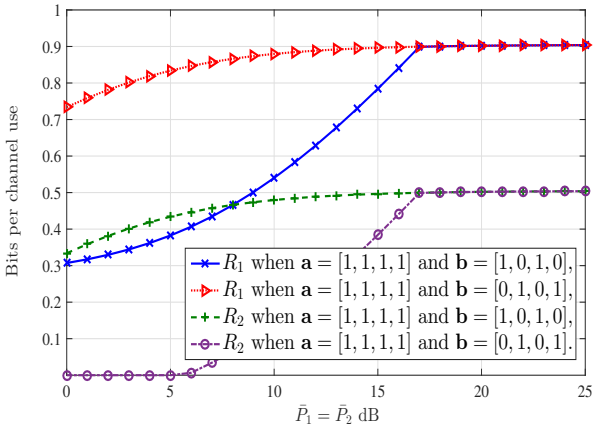

Fig. 15: Scenario II: Achievable secure rates vs transmit power when $\beta_1 = 0.4$, $\beta_2 = 0.2$, $\bar{P}_r = 15$ dB, $h_1 = g_1 = 1$, $h_2 = g_2 = 0.7$, $\zeta_1 = 0.2$, $\zeta_2 = 0.8$ and $\eta = 0.4$.

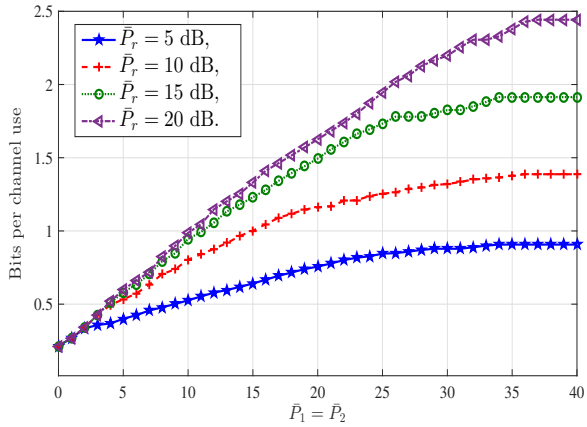

Fig. 16: Scenario II: Achievable sum secure rates vs transmit power when $\beta_1 = 0.3$, $\beta_2 = 0.15$, $h_1 = g_1 = 1$, $h_2 = g_2 = 0.3$ and optimal η.

nested lattice codebooks and random binning, and having the destinations cooperatively jam with nested lattice codewords. The relay performs scaled compute-and-forward to decode two distinct integer combinations of the received lattice points, then forwards using Gaussian codewords. Additionally, we have derived outer bounds to assess the performance of the proposed achievable schemes. Numerical results point out the insights that the outer bounds are tight under specific cases and there is a need for applying power control policies at the sources and destinations.

Overall, this work demonstrates the impact of cooperation with an untrusted relay in multi-source multi-destination networks with heterogeneous nodes. In particular, the untrusted, i.e., honest-but-curious, relay is an invaluable resource to serve users with different levels of security clearance and to convey messages confidential from the unintended destination.

Appendix A
Proof of Theorem 1

Recall that from Remark 1, $Y_k^n = \{J_k^l, Y_k^m\}$. Also, we observe that we have the following Markov chain: $(W_1^p, W_1^s, W_2^p, W_2^s) - (V_1^l, U_1^l, V_2^l, U_2^l) - (X_1^l, X_2^l) - Y_r^l - \hat{Y}_r^l - X_r^m - Y_k^m$. To simplify the notation, define $\boldsymbol{U} = \{U_1^l, U_2^l\}$ and $\boldsymbol{V} = \{V_1^l, V_2^l\}$.

A. Reliability

We choose the channel input distribution as follows

$$p(U_1^l, U_2^l, V_1^l, V_2^l, J_1^l, J_2^l, X_r^m) = p(U_1^l)p(U_2^l)p(V_1^l)p(V_2^l)p(J_1^l)p(J_2^l)p(X_r^m). \quad (56)$$

D_2 considers the signals V_k's as noise while decoding the common secure messages, thus it observes the signals U_k's as the output of a multiple-access relay channel (MARC) [19, Section 3.2] [20, Section III-B3]. To define the achievable region, we need to calculate:

$$\begin{aligned}
&I(U_1^l; Y_2^m, J_2^l, \hat{Y}_r^{\,l} | U_2^l, X_r^m) \\
&= I(U_1^l; Y_2^m, \hat{Y}_r^{\,l} | J_2^l, U_2^l, X_r^m) + I(U_1^l; J_2^l | U_2^l, X_r^m) && (57)\\
&= I(U_1^l; Y_2^m, \hat{Y}_r^{\,l} | J_2^l, U_2^l, X_r^m) && (58)\\
&= I(U_1^l; \hat{Y}_r^{\,l} | Y_2^m, J_2^l, U_2^l, X_r^m) + I(U_1^l; Y_2^m | J_2^l, U_2^l, X_r^m) && (59)\\
&= I(U_1^l; \hat{Y}_r^{\,l} | Y_2^m, J_2^l, U_2^l, X_r^m) + I(U_1^l; Z_2^m | J_2^l, U_2^l, X_r^m) && (60)\\
&= I(U_1^l; \hat{Y}_r^{\,l} | Y_2^m, J_2^l, U_2^l, X_r^m) && (61)\\
&= I(U_1^l; Y_r^l + Z_Q^l | Y_2^m, J_2^l, U_2^l, X_r^m) && (62)\\
&= I(U_1^l; \sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + \sqrt{g_2}J_2^l + \sqrt{h_2}X_2^l + Z_r^l + Z_Q^l \\
&\qquad | \sqrt{g_2}X_r^m + Z_2^m, J_2^l, U_2^l, X_r^m) && (63)\\
&= I(U_1^l; \sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + \sqrt{h_2}V_2^l + Z_r^l + Z_Q^l) && (64)\\
&= lC\left(\frac{\bar{\alpha}_1 h_1 P_1}{1 + g_1 P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right). && (65)
\end{aligned}$$

Similarly, we get

$$I(U_2^l; Y_2^m, J_2^l, \hat{Y}_r^{\,l} | U_1^l, X_r^m) = lC\left(\frac{\bar{\alpha}_2 h_2 P_2}{1 + g_1 P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right), \quad (66)$$

Next, we calculate

$$\begin{aligned}
&I(U_1^l, U_2^l; Y_2^m, J_2^l, \hat{Y}_r^{\,l} | X_r^m) \\
&= I(U_1^l, U_2^l; Y_2^m, \hat{Y}_r^{\,l} | J_2^l, X_r^m) + I(U_1^l, U_2^l; J_2^l | X_r^m) && (67)\\
&= I(U_1^l, U_2^l; Y_2^m, \hat{Y}_r^{\,l} | J_2^l, X_r^m) && (68)\\
&= I(U_1^l, U_2^l; \hat{Y}_r^{\,l} | Y_2^m, J_2^l, X_r^m) + I(U_1^l, U_2^l; Y_2^m | J_2^l, X_r^m) && (69)\\
&= I(U_1^l, U_2^l; \hat{Y}_r^{\,l} | Y_2^m, J_2^l, X_r^m) + I(U_1^l, U_2^l; Z_2^m | J_2^l, X_r^m) && (70)\\
&= I(U_1^l, U_2^l; \hat{Y}_r^{\,l} | Y_2^m, J_2^l, X_r^m) && (71)\\
&= I(U_1^l, U_2^l; Y_r^l + Z_Q^l | Y_2^m, J_2^l, X_r^m) && (72)\\
&= I(U_1^l, U_2^l; \sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + \sqrt{g_2}J_2^l + \sqrt{h_2}X_2^l + Z_r^l + Z_Q^l \\
&\qquad | \sqrt{g_2}X_r^m + Z_2^m, J_2^l, X_r^m) && (73)\\
&= I(U_1^l, U_2^l; \sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + \sqrt{h_2}X_2^l + Z_r^l + Z_Q^l) && (74)\\
&= nC\left(\frac{\bar{\alpha}_1 h_1 P_1 + \bar{\alpha}_2 h_2 P_2}{1 + g_1 P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right). && (75)
\end{aligned}$$

Since, the decodability of the common secure messages needs to be ensured at both destinations, we obtain the following terms for D_1

$$I(U_1^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | U_2^l\, X_r^m) = lC\left(\frac{\bar{\alpha}_1 h_1 P_1}{1 + g_2 P_{J2} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right), \quad (76)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

$$I(U_2^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | U_1^l, X_r^m) = lC\left(\frac{\bar{\alpha}_2 h_2 P_2}{1+g_2 P_{J2}+\alpha_1 h_1 P_1+\alpha_2 h_2 P_2+\sigma_Q^2}\right), \tag{77}$$

$$I(U_1^l, U_2^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | X_r^m) = lC\left(\frac{\bar{\alpha}_1 h_1 P_1+\bar{\alpha}_2 h_2 P_2}{1+g_2 P_{J2}+\alpha_1 h_1 P_1+\alpha_2 h_2 P_2+\sigma_Q^2}\right). \tag{78}$$

After decoding the common secure messages, D_1 starts decoding the private messages. For this, we calculate

$$\begin{aligned}
&I(V_1^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | \boldsymbol{U}, V_2^l, X_r^m) \\
&= I(V_1^l; Y_1^m, \hat{Y}_r^{\,l} | J_1^l, \boldsymbol{U}, V_2^l, X_r^m) + I(V_1^l; J_1^l | \boldsymbol{U}, V_2^l, X_r^m) && (79)\\
&= I(V_1^l; Y_1^m, \hat{Y}_r^{\,l} | J_1^l, \boldsymbol{U}, V_2^l, X_r^m) && (80)\\
&= I(V_1^l; \hat{Y}_r^{\,l} | Y_1^m, J_1^l, \boldsymbol{U}, V_2^l, X_r^m) + I(V_1^l; Y_1^m | J_1^l, \boldsymbol{U}, V_2^l, X_r^m) && (81)\\
&= I(V_1^l; \hat{Y}_r^{\,l} | Y_1^m, J_1^l, \boldsymbol{U}, V_2^l, X_r^m) + I(V_1^l; Z_1^m | J_1^l, \boldsymbol{U}, V_2^l, X_r^m) && (82)\\
&= I(V_1^l; \hat{Y}_r^{\,l} | Y_1^m, J_1^l, \boldsymbol{U}, V_2^l, X_r^m) && (83)\\
&= I(V_1^l; Y_r^l + Z_Q^l | Y_1^m, J_1^l, \boldsymbol{U}, V_2^l, X_r^m) && (84)\\
&= I(V_1^l; \sqrt{h_1} X_1^l + \sqrt{g_1} J_1^l + \sqrt{g_2} J_2^l + \sqrt{h_2} X_2^l + Z_r^l + Z_Q^l \\
&\qquad | \sqrt{g_1} X_r^m + Z_1^m, J_1^l, \boldsymbol{U}, V_2^l, X_r^m) && (85)\\
&= I(V_1^l; \sqrt{h_1} V_1^l + \sqrt{g_2} J_2^l + Z_r^l + Z_Q^l) = lC\left(\frac{\alpha_1 h_1 P_1}{1+g_2 P_{J2}+\sigma_Q^2}\right). && (86)
\end{aligned}$$

Similarly, we get

$$I(V_2^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | \boldsymbol{U}, V_1^l, X_r^m) = lC\left(\frac{\alpha_2 h_2 P_2}{1+g_2 P_{J2}+\sigma_Q^2}\right), \tag{87}$$

$$I(V_1^l, V_2^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | \boldsymbol{U}, X_r) = lC\left(\frac{\alpha_1 h_1 P_1 + \alpha_2 h_2 P_2}{1+g_2 P_{J2}+\sigma_Q^2}\right). \tag{88}$$

Next, we calculate

$$\begin{aligned}
&I(X_1^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | X_2^l, X_r^m) \\
&= I(X_1^l; Y_1^m, \hat{Y}_r^{\,l} | J_1^l, X_2^l, X_r^m) + I(X_1^l; J_1^l | X_2^l, X_r^m) && (89)\\
&= I(X_1^l; Y_1^m, \hat{Y}_r^{\,l} | J_1^l, X_2^l, X_r^m) && (90)\\
&= I(X_1^l; \hat{Y}_r^{\,l} | Y_1^m, J_1^l, X_2^l, X_r^m) + I(X_1^l; Y_1^m | J_1^l, X_2^l, X_r^m) && (91)\\
&= I(X_1^l; \hat{Y}_r^{\,l} | Y_1^m, J_1^l, X_2^l, X_r^m) + I(X_1^l; Z_1^m | J_1^l, X_2^l, X_r^m) && (92)\\
&= I(X_1^l; \hat{Y}_r^{\,l} | Y_1^m, J_1^l, X_2^l, X_r^m) && (93)\\
&= I(X_1^l; Y_r^l + Z_Q^l | Y_1^m, J_1^l, X_2^l, X_r^m) && (94)\\
&= I(X_1^l; \sqrt{h_1} X_1^l + \sqrt{g_1} J_1^l + \sqrt{g_2} J_2^l + \sqrt{h_2} X_2^l + Z_r^l + Z_Q^l \\
&\qquad | \sqrt{g_1} X_r^m + Z_1^m, J_1^l, X_2^l, X_r^m) && (95)\\
&= I(X_1^l; \sqrt{h_1} X_1^l + Z_r^l + \sqrt{g_2} J_2^l + Z_Q^l) = lC\left(\frac{h_1 P_1}{1+g_2 P_{J2}+\sigma_Q^2}\right). && (96)
\end{aligned}$$

Similarly, we can get

$$I(X_2^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | X_1^l, X_r^m) = lC\left(\frac{h_2 P_2}{1+g_2 P_{J2}+\sigma_Q^2}\right), \tag{97}$$

$$I(X_1^l, X_2^l; Y_1^m, J_1^l, \hat{Y}_r^{\,l} | X_r^m) = lC\left(\frac{h_1 P_1 + h_2 P_2}{1+g_2 P_{J2}+\sigma_Q^2}\right). \tag{98}$$

Finally, we must determine the quantization noise variance σ_Q^2 such that both destinations are able to decode their messages. To capture this, we have to calculate the following terms

$$I(X_r^m; Y_2^m, J_2^l) = mC(g_2 P_r), \tag{99}$$

$$I(X_r^m; Y_1^m, J_1^l) = mC(g_1 P_r). \tag{100}$$

Then, we calculate

$$\begin{aligned}
&I(\hat{Y}_r^{\,l}; Y_r^l | X_r^m, Y_2^m, J_2^l) = I(Y_r^l + Z_Q^l; Y_r^l | X_r^m, Z_2^l, J_2^l) && (101)\\
&= I(\sqrt{h_1} X_1^l + \sqrt{g_1} J_1^l + \sqrt{h_2} X_2^l + Z_r^l + Z_Q^l; \\
&\qquad \sqrt{h_1} X_1^l + \sqrt{g_1} J_1^l + \sqrt{h_2} X_2^l + Z_r^l) && (102)\\
&= lC\left(\frac{h_1 P_1 + h_2 P_2 + g_1 P_{J1} + 1}{\sigma_Q^2}\right). && (103)
\end{aligned}$$

Similarly, we get

$$I(\hat{Y}_r^{\,l}; Y_r^l | X_r^m, Y_1^m, J_1^l) = lC\left(\frac{h_1 P_1 + h_2 P_2 + g_2 P_{J2} + 1}{\sigma_Q^2}\right). \tag{104}$$

B. Equivocation Calculations

$$\begin{aligned}
&H(W_1^p W_2^p | Y_2^m J_2^l) \geq H(W_1^p W_2^p | Y_2^m J_2^l \boldsymbol{U} X_r^m \hat{Y}_r^l) && (105)\\
&= H(W_1^p W_2^p | J_2^l \boldsymbol{U} X_r^m \hat{Y}_r^l) && (106)\\
&= H(W_1^p W_2^p | J_2^l \boldsymbol{U}) - I(W_1^p W_2^p; X_r^m \hat{Y}_r^l | J_2^l \boldsymbol{U}) && (107)\\
&= H(W_1^p W_2^p) - I(W_1^p W_2^p; X_r^m | J_2^l \boldsymbol{U}) - I(W_1^p W_2^p; \hat{Y}_r^l | X_r^m J_2^l \boldsymbol{U}). && (108)
\end{aligned}$$

From (56) the channel inputs are independent, thus we have

$$\begin{aligned}
I(W_1^p W_2^p; X_r^m | J_2^l \boldsymbol{U}) &\leq I(W_1^p W_2^p, X_1^l X_2^l; X_r^m | J_2^l \boldsymbol{U}) \\
&= I(X_1^l X_2^l; X_r^m | J_2^l \boldsymbol{U}) = 0. && (109)
\end{aligned}$$

Then, we have

$$\begin{aligned}
&H(W_1^p, W_2^p | Y_2^m J_2^l) \geq H(W_1^p, W_2^p) - I(W_1^p W_2^p; \hat{Y}_r^l | X_r^m J_2^l \boldsymbol{U}) && (110)\\
&= H(W_1^p, W_2^p) - I(W_1^p W_2^p; \hat{Y}_r^l | J_2^l \boldsymbol{U}) && (111)\\
&= H(W_1^p, W_2^p) - h(\hat{Y}_r^l | J_2^l \boldsymbol{U}) + h(\hat{Y}_r^l | W_1^p W_2^p J_2^l \boldsymbol{U}) \\
&\qquad + I(W_1^p W_2^p; \hat{Y}_r^l | J_2^l \boldsymbol{U} \boldsymbol{V}) && (112)\\
&= H(W_1^p, W_2^p) - h(\hat{Y}_r^l | J_2^l \boldsymbol{U}) + h(\hat{Y}_r^l | W_1^p W_2^p J_2^l \boldsymbol{U}) \\
&\qquad + h(\hat{Y}_r^l | J_2^l \boldsymbol{U} \boldsymbol{V}) - h(\hat{Y}_r^l | W_1^p W_2^p J_2^l \boldsymbol{U} \boldsymbol{V}) && (113)\\
&= H(W_1^p, W_2^p) - I(\hat{Y}_r^l; \boldsymbol{V} | J_2^l \boldsymbol{U}) + I(\hat{Y}_r^l; \boldsymbol{V} | W_1^p W_2^p J_2^l \boldsymbol{U}) && (114)\\
&= H(W_1^p, W_2^p) - I(\hat{Y}_r^l; \boldsymbol{V} | J_2^l \boldsymbol{U}) + h(\boldsymbol{V} | W_1^p W_2^p J_2^l \boldsymbol{U}) \\
&\qquad - h(\boldsymbol{V} | W_1^p W_2^p J_2^l \boldsymbol{U} \hat{Y}_r^l) && (115)\\
&\geq H(W_1^p, W_2^p) - I(\hat{Y}_r^l; \boldsymbol{V} | J_2^l \boldsymbol{U}) + h(\boldsymbol{V} | W_1^p W_2^p J_2^l \boldsymbol{U}) \\
&\qquad - h(\boldsymbol{V} | W_1^p W_2^p J_2^l \boldsymbol{U} \hat{Y}_r^l) && (116)\\
&\geq H(W_1^p, W_2^p) - lC\left(\frac{\alpha_1 h_1 P_1 + \alpha_2 h_2 P_2}{1+g_1 P_{J1}+\sigma_Q^2}\right) + lR_1^{x2} + lR_2^{x2} - l\epsilon_1. && (117)
\end{aligned}$$

Note that with the knowledge of Y_r^l, and the bin index the eavesdropper at the relay is assumed to be able to decode the transmitted codeword. Here, whenever $g_2 P_{J2} \geq \sigma_Q^2$, the last term is bounded by Fano's inequality as with the knowledge of $\hat{Y}_r^l$, the cooperative jamming signal from the second destination and the bin index, the eavesdropper at the relay is assumed to be able to decode the transmitted codeword since it has

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

higher SNR than the aforementioned case. Also, observe that if $g_2P_{J2} \leq \sigma_Q^2$, the rates of common secure messages are zero, and in this case we need only to protect the private message from the eavesdropper associated with the relay as the SNR at D_2 will be less than the one at the relay. Similarly, we get

$$H(W_1^p|Y_2^m J_2^l) \geq H(W_1^p) - lC\left(\frac{\alpha_1 h_1 P_1}{1+g_1P_{J1}+\alpha_2 h_2 P_2+\sigma_Q^2}\right) + lR_1^{x2} - l\epsilon_2, \quad (118)$$

$$H(W_2^p|Y_2^m J_2^l) \geq H(W_2^p) - lC\left(\frac{\alpha_2 h_2 P_2}{1+g_1P_{J1}+\alpha_1 h_1 P_1+\sigma_Q^2}\right) + lR_2^{x2} - l\epsilon_3. \quad (119)$$

We need to guarantee that the relay is not able to decode the common secure messages, i.e.,

$$\begin{aligned}
H(W_1^s, W_2^s|Y_r^l) &= H(W_1^s, W_2^s) - I(W_1^s W_2^s; Y_r^l) && (120)\\
&= H(W_1^s, W_2^s) - I(W_1^s W_2^s; Y_r^l) + I(W_1^s W_2^s; Y_r^l|\boldsymbol{U}) && (121)\\
&= H(W_1^s, W_2^s) - h(Y_r^l) + h(Y_r^l|W_1^s W_2^s) \\
&\quad + h(Y_r^l|\boldsymbol{U}) + h(Y_r^l|W_1^s W_2^s \boldsymbol{U}) && (122)\\
&= H(W_1^s, W_2^s) - I(\boldsymbol{U}; Y_r^l) + I(\boldsymbol{U}; Y_r^l|W_1^s W_2^s) && (123)\\
&= H(W_1^s, W_2^s) - I(\boldsymbol{U}; Y_r^l) + h(\boldsymbol{U}|W_1^s W_2^s) - h(\boldsymbol{U}|Y_r^l W_1^s W_2^s) && (124)\\
&= H(W_1^s, W_2^s) + lR_1^{x1} + lR_2^{x1} \\
&\quad - lC\left(\frac{\bar{\alpha}_1 h_1 P_1 + \bar{\alpha}_2 h_2 P_2}{1+g_1P_{J1}+g_2P_{J2}+\alpha_1 h_1 P_1+\alpha_2 h_2 P_2}\right) - l\epsilon_4. && (125)
\end{aligned}$$

Similarly, we can get

$$H(W_1^s|Y_r^l) \geq H(W_1^s) + lR_1^{x1} - lC\left(\frac{\bar{\alpha}_1 h_1 P_1}{1+g_1P_{J1}+g_2P_{J2}+\alpha_1 h_1 P_1+h_2P_2}\right) - l\epsilon_5, \quad (126)$$

$$H(W_2^s|Y_r^l) \geq H(W_2^s) + lR_2^{x1} - lC\left(\frac{\bar{\alpha}_2 P_2}{1+g_1P_{J1}+g_2P_{J2}+\alpha_2 h_2 P_2+h_1P_1}\right) - l\epsilon_6. \quad (127)$$

Finally, since all messages should be kept secret from the relay, we have

$$\begin{aligned}
&H(W_1^s, W_2^s, W_1^p, W_2^p|Y_r^l) \\
&\quad = H(W_1^s, W_2^s, W_1^p, W_2^p) - I(W_1^s W_2^s W_1^p, W_2^p; Y_r^l) && (128)\\
&\quad = H(W_1^s, W_2^s, W_1^p, W_2^p) - I(W_1^s W_2^s W_1^p, W_2^p; Y_r^l) \\
&\qquad + I(W_1^s W_2^s W_1^p W_2^p; Y_r^l|\boldsymbol{U}\boldsymbol{V}) && (129)\\
&\quad = H(W_1^s, W_2^s, W_1^p, W_2^p) + h(Y_r^l|W_1^s W_2^s W_1^p W_2^p) - h(Y_r^l) \\
&\qquad + h(Y_r^l|\boldsymbol{U}\boldsymbol{V}) + h(Y_r^l|W_1^s W_2^s W_1^p W_2^p \boldsymbol{U}\boldsymbol{V}) && (130)\\
&\quad = H(W_1^s, W_2^s, W_1^p, W_2^p) - I(\boldsymbol{V}\boldsymbol{U}; Y_r^l) \\
&\qquad + I(\boldsymbol{V}\boldsymbol{U}; Y_r^l|W_1^s W_2^s W_1^p W_2^p) && (131)\\
&\quad = H(W_1^s, W_2^s, W_1^p, W_2^p) + h(\boldsymbol{V}\boldsymbol{U}|W_1^s W_2^s W_1^p W_2^p) \\
&\qquad - I(\boldsymbol{V}\boldsymbol{U}; Y_r^l) - h(\boldsymbol{V}\boldsymbol{U}|Y_r^l W_1^s W_2^s W_1^p W_2^p) && (132)\\
&\quad = H(W_1^s, W_2^s, W_1^p, W_2^p) - lC\left(\frac{h_1P_1+h_2P_2}{1+g_1P_{J1}+g_2P_{J2}}\right) \\
&\qquad + lR_1^{x1} + lR_2^{x1} + lR_1^{x2} + lR_2^{x2} - l\epsilon_7. && (133)
\end{aligned}$$

Similarly, we can get

$$H(W_1^s, W_1^p|Y_r^l) = H(W_1^s, W_1^p) - lC\left(\frac{h_1P_1}{1+g_1P_{J1}+g_2P_{J2}}\right) + lR_1^{x1} + lR_1^{x2} - l\epsilon_8, \quad (134)$$

$$H(W_2^s, W_2^p|Y_r^l) = H(W_2^s, W_2^p) - lC\left(\frac{h_2P_2}{1+g_1P_{J1}+g_2P_{J2}}\right) + lR_2^{x1} + lR_2^{x2} - l\epsilon_9. \quad (135)$$

Therefore, by proper choice of the bin sizes, represented by the randomization rates, R_k^{x1} and R_k^{x2}, we get the achievable region stated in Theorem 1.

Appendix B
Proof of Theorem 2

Here, we detail the derivation of the outer bounds presented in subsection III-D. For the rate of the message W_1^s, we have

$$\begin{aligned}
H(W_1^s) &\leq H(W_1^s|Y_e^n) + n\epsilon_{10} && (136)\\
&\leq H(W_1^s|Y_e^l) - H(W_1^s|X_2^l X_r^m Y_2^m J_2^l) + n\epsilon_{11} && (137)\\
&= H(W_1^s|Y_e^l) - H(W_1^s|X_2^l X_r^m J_2^l) + n\epsilon_{11} && (138)\\
&\leq H(W_1^s|Y_e^l) - H(W_1^s|X_2^l X_r^m Y_r^l J_2^l) + n\epsilon_{11} && (139)\\
&= H(W_1^s|Y_e^l) - H(W_1^s|X_2^l Y_r^l J_2^l) + n\epsilon_{11} && (140)\\
&= H(W_1^s|Y_e^l) - H(W_1^s|X_2^l, J_2^l, \\
&\qquad \sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + \sqrt{h_2}X_2^l + \sqrt{g_2}J_2^l + Z_r^l) + n\epsilon_{11} && (141)\\
&= H(W_1^s|Y_e^l) - H(W_1^s|\sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + Z_r^l) + n\epsilon_{11} && (142)\\
&\leq H(W_1^s|Y_e^l) - H(W_1^s|\sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + Z_r^l, Y_e^l) + n\epsilon_{11}. && (143)
\end{aligned}$$

(136) is due to the secrecy constraint, $\frac{1}{n}H(W_1^s|Y_e^n) \geq \frac{1}{n}H(W_1^s) - \epsilon$. (137) is due to the fact that the relay receives in the first l channel uses only and thus Y_e^n can be replaced by Y_e^l, and due to Fano's inequality $H(W_1^s|X_2^l X_r^m Y_2^m J_2^l) \leq \epsilon$, i.e., given its received and jamming signals, D_2 must be able to decode W_1^s. In (138), we eliminate Y_2^m as X_r^m is given to the destinations by a genie and $Y_2^m = \sqrt{g_2}X_r^m + Z_2^m$. (139) follows from the fact that conditioning cannot increase the entropy. We have (140) since X_r^m is a deterministic function of Y_r^l. (143) is due to the fact that conditioning cannot increase the entropy. To simplify the notation, define $G_1^l = \sqrt{h_1}X_1^l + \sqrt{g_1}J_1^l + Z_r^l$. Excluding the $n\epsilon_{11}$ term for convenience, (143) becomes

$$\begin{aligned}
&H(W_1^s|Y_e^l) - H(W_1^s|G_1^l, Y_e^l) = I(W_1^s; G_1^l|Y_e^l) && (144)\\
&\leq I(W_1^s, X_1^l; G_1^l|Y_e^l) && (145)\\
&= I(X_1^l; G_1^l|Y_e^l) && (146)\\
&= h(G_1^l|Y_e^l) - h(\sqrt{g_1}J_1^l + Z_r^l|\sqrt{h_2}X_2^l + Z_e^l + \sqrt{g_1}J_1^l + \sqrt{g_2}J_2^l) && (147)\\
&\leq h(G_1^l|Y_e^l) - h(J_1^l + Z_r^l|\sqrt{h_2}X_2^l + Z_e^l + \sqrt{g_1}J_1^l + \sqrt{g_2}J_2^l, J_2^l) && (148)\\
&= h(G_1^l|Y_e^l) - h(\sqrt{g_1}J_1^l + Z_r^l|Z_e^l + \sqrt{g_1}J_1^l + \sqrt{h_2}X_2^l), && (149)
\end{aligned}$$

which can be maximized with Gaussian signals, thus we get the upper bound in (23). Similarly, we proceed to calculate the outer bound on common secure sum rate

$$\begin{aligned}
&H(W_1^s, W_2^s) \leq H(W_1^s, W_2^s|Y_e^n) + n\epsilon_{12} \\
&\leq H(W_1^s, W_2^s|Y_e^l) - H(W_1^s, W_2^s|X_r^m Y_2^m J_2^l) + n\epsilon_{13} && (150)
\end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

$$= H(W_1^s, W_2^s|Y_e^l) - H(W_1^s, W_2^s|X_r^m J_2^l) + n\epsilon_{13} \quad (151)$$
$$\leq H(W_1^s, W_2^s|Y_e^l) - H(W_1^s, W_2^s|X_r^m Y_r^l J_2^l) + n\epsilon_{13} \quad (152)$$
$$= H(W_1^s, W_2^s|Y_e^l) - H(W_1^s, W_2^s|Y_r^l J_2^l) + n\epsilon_{13} \quad (153)$$
$$= H(W_1^s, W_2^s|Y_e^l) - H(W_1^s, W_2^s|\sqrt{h_1}X_1^l + \sqrt{h_2}X_2^l + \sqrt{g_1}J_1^l + Z_r^l) + n\epsilon_{13} \quad (154)$$
$$\leq H(W_1^s, W_2^s|Y_e^l) - H(W_1^s, W_2^s|\sqrt{h_1}X_1^l + \sqrt{h_2}X_2^l + \sqrt{g_1}J_1^l + Z_r^l, Y_e^l) + n\epsilon_{13}. \quad (155)$$

To simplify the notation, let $G_2^l = \sum_{k=1}^{2}\sqrt{h_k}X_k^l + \sqrt{g_1}J_1^l + Z_r^l$. Thus, we have

$$\begin{aligned}
&H(W_1^s, W_2^s|Y_e^l) - H(W_1^s, W_2^s|G_2^l, Y_e^l) \\
&\quad = I(W_1^s, W_2^s; G_2^l|Y_e^l) && (156)\\
&\quad \leq I(W_1^s, W_2^s, X_1^l, X_2^l; G_2^l|Y_e^l) && (157)\\
&\quad = I(X_1^l, X_2^l; G_2^l|Y_e^l) && (158)\\
&\quad = h(G_2^l|Y_e^l) - h(\sqrt{g_1}J_1^l + Z_r^l|Z_e^l + \sqrt{g_1}J_1^l + \sqrt{g_2}J_2^l) && (159)\\
&\quad \leq h(G_2^l|Y_e^l) - h(\sqrt{g_1}J_1^l + Z_r^l|Z_e^l + \sqrt{g_1}J_1^l + \sqrt{g_2}J_2^l, J_2^l) && (160)\\
&\quad = h(G_2^l|Y_e^l) - h(\sqrt{g_1}J_1^l + Z_r^l|Z_e^l + \sqrt{g_1}J_1^l). && (161)
\end{aligned}$$

Thus, we can get the upper bound in (24).

Similar to going from (137) to (149), we have, for the rates of W_1^p and W_1^s,

$$\begin{aligned}
&H(W_1^p, W_1^s|Y_e^n) \\
&\quad \leq h(G_3^l|Y_e^l) - h(\sqrt{g_2}J_2^l + Z_r^l|Z_e^l + \sqrt{h_2}X_2^l + \sqrt{g_2}J_2^l), && (162)
\end{aligned}$$

where $G_3^l = \sqrt{h_1}X_1^l + \sqrt{g_2}J_2^l + Z_r^l$. Let $O_{tp}^k = h_k P_k + g_2 P_{J2}$. Thus, we have the upper bound in (25). The upper bound on the sum rate, $R_1^p + R_2^p + R_1^s + R_2^s$, can be calculated similar to (150)-(161) as

$$\begin{aligned}
&H(W_1^p, W_2^p, W_1^s, W_2^s|Y_e^n) \\
&\quad \leq h(G_4^l|Y_e^l) - h(\sqrt{g_2}J_2^l + Z_r^l|Z_e^l + \sqrt{g_2}J_2^l), && (163)
\end{aligned}$$

where $G_4^l = \sum_{k=1}^{2}\sqrt{h_k}X_k^l + \sqrt{g_2}J_2^l + Z_r^l$. Thus, we get the upper bound in (26).

Appendix C
Proof of Theorem 3

Here, we complete the proof of Theorem 3 by calculating the equivocation rates obtained by the proposed achievability scheme. First, we recall some results that will be used throughout the equivocation analysis.

Lemma 1. *[21] Let t_A, t_B be two independent random variables distributed over compact abelian group and t_B has a uniform distribution, then $t_A \oplus t_B$ is independent from t_A.*

Theorem 4. *The representation theorem [22]: Assume $t_1^N, t_2^N, .., t_K^N$ are K vectors taken from $\mathcal{V}(\Lambda)$. There exist an integer T, such that $1 \leq T \leq K^N$, $\sum_{k=1}^{K} t_k^N$ is uniquely determined by $\{T, \sum_{k=1}^{K} t_k^N \mod \Lambda\}$.*

Lemma 2. *[23] For random variables A and B, and discrete random variable T, we have $H(A|B,T) \geq H(A|B) - H(T)$.*

To simplify the notation, we omit the conditioning on the dither vectors, scaling factors β_k's and the channel gains as they are assumed to be known at all network nodes.

A. At the untrusted relay

$$\begin{aligned}
&H(t_1^N|Y_r^n, W_2) \geq H(t_1^N|Y_r^n, Z_r^n, X_2^n, X_4^n, W_2) && (164)\\
&\quad = H(t_1^N|X_1^N + J_1^N) && (165)\\
&\quad = H(t_1^N|X_1^N + J_1^N \mod \Lambda_1/\beta_1, T_1) && (166)\\
&\quad = H(t_1^N|t_1^N/\beta_1 + t_3^N/\beta_1 \mod \Lambda_1/\beta_1, T_1) && (167)\\
&\quad \geq H(t_1^N|t_1^N/\beta_1 + t_3^N/\beta_1 \mod \Lambda_1/\beta_1) - H(T_1) && (168)\\
&\quad \geq H(t_1^N) - H(T_1) && (169)\\
&\quad \geq H(t_1^N) - N. && (170)
\end{aligned}$$

The steps (166) and (170) follow from the representation theorem for $K = 2$, where T_1 is an integer such that $1 \leq T_1 \leq 2^N$, while step (168) results by applying Lemma 2. (169) is due to Lemma 1. Finally, from (170), we obtain

$$\frac{1}{N} I(t_1^N; Y_r^n, W_2) \leq 1. \quad (171)$$

Similarly, we can obtain the following for t_2^N

$$\frac{1}{N} I(t_2^N; Y_r^n, W_1) \leq 1. \quad (172)$$

The above results imply that the leaked information about the value of t_1^N (t_2^N) to the relay node cannot exceed 1 bit per channel use, therefore by using random binning we can guarantee the secrecy of the messages at the untrusted relay and achieve the rates given in Theorem 3.

B. At the destinations

Here, we focus on the equivocation analysis of the confidential messages at the destinations.

$$\begin{aligned}
H(W_1|Y_2^n, J_2^n, W_2) &\geq H(W_1|Y_2^n, J_2^n, W_2, X_{r2}^m, Z_2^m) \\
&= H(W_1|X_{r1}^m) = H(W_1). && (173)
\end{aligned}$$

The last step follows from Lemma 1, i.e., X_{r1}^m and $\bar{t}_1^N$ are independent. Similarly, we can get

$$H(W_2|Y_1^n, J_1^n, W_1) \geq H(W_2). \quad (174)$$

Appendix D
Optimal α_1, α_2 and λ

A. Optimizing N_1 over α_1

Note that $N_1(\alpha_1)$ expressed in (45) can be written in the following vector form

$$N_1(\alpha_1) = P\alpha_1^2||\boldsymbol{h}||^2 + ||\hat{\boldsymbol{a}}||^2 P - 2\alpha_1 \boldsymbol{h}^T \hat{\boldsymbol{a}} P + \alpha_1^2. \quad (175)$$

By differentiating the right hand side with respect to α_1 and setting the first derivative to be zero, we can obtain the following optimum value of α_1 that minimizes $N_1(\alpha)$

$$\alpha_1^* = \frac{P\boldsymbol{h}^T \hat{\boldsymbol{a}}}{1 + P||\boldsymbol{h}||^2}, \quad (176)$$

which results in the following value for $N_1(\alpha)$

$$N_1(\alpha_1^*) = ||\hat{\boldsymbol{a}}||^2 P - \frac{P^2(\boldsymbol{h}^T \hat{\boldsymbol{a}})^2}{1 + P||\boldsymbol{h}||^2}. \quad (177)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2695163, IEEE Transactions on Information Forensics and Security

B. Optimizing N_2 over α_2 and λ

$N_2(\alpha_2, \lambda)$, defined in (50), can be expressed in the following vector form

$$N_2(\alpha_2, \lambda) = (\alpha_2 \boldsymbol{h} - \hat{\boldsymbol{b}} - \lambda \hat{\boldsymbol{a}})^T (\alpha_2 \boldsymbol{h} - \hat{\boldsymbol{b}} - \lambda \hat{\boldsymbol{a}}) P + \alpha_2^2. \quad (178)$$

Furthermore, we can write the above equation in the following matrix form

$$N_2(\alpha_2, \lambda) = \begin{bmatrix} \alpha_2 & \lambda \end{bmatrix} \begin{bmatrix} 1 + \boldsymbol{h}^T \boldsymbol{h} P & -\boldsymbol{h}^T \hat{\boldsymbol{a}} P \\ -\boldsymbol{h}^T \hat{\boldsymbol{a}} P & \hat{\boldsymbol{a}}^T \hat{\boldsymbol{a}} P \end{bmatrix} \begin{bmatrix} \alpha_2 \\ \lambda \end{bmatrix} + \begin{bmatrix} -2\boldsymbol{h}^T \hat{\boldsymbol{b}} P & 2\hat{\boldsymbol{b}}^T \hat{\boldsymbol{b}} P \end{bmatrix} \begin{bmatrix} \alpha_2 \\ \lambda \end{bmatrix} + \hat{\boldsymbol{b}}^T \hat{\boldsymbol{b}} P. \quad (179)$$

Let $\boldsymbol{x} = \begin{bmatrix} \alpha_2 & \lambda \end{bmatrix}^T$, $\boldsymbol{q}^T = \begin{bmatrix} -2\boldsymbol{h}^T \hat{\boldsymbol{b}} P & 2\hat{\boldsymbol{b}}^T \hat{\boldsymbol{b}} P \end{bmatrix}$, $\boldsymbol{c} = \hat{\boldsymbol{b}}^T \hat{\boldsymbol{b}} P$, and $\boldsymbol{A} = \begin{bmatrix} 1 + \boldsymbol{h}^T \boldsymbol{h} P & -\boldsymbol{h}^T \hat{\boldsymbol{a}} P \\ -\boldsymbol{h}^T \hat{\boldsymbol{a}} P & \hat{\boldsymbol{a}}^T \hat{\boldsymbol{a}} P \end{bmatrix}$. Now, (179) can be rewritten as

$$N_2(\boldsymbol{x}) = \boldsymbol{x}^T \boldsymbol{A} \boldsymbol{x} + \boldsymbol{q}^T \boldsymbol{x} + \boldsymbol{c}. \quad (180)$$

Again, by differentiating and setting the first derivative to be zero, we obtain

$$\boldsymbol{x}^* = -0.5 \boldsymbol{A}^{-1} \boldsymbol{q}. \quad (181)$$

Now, if we plug $\boldsymbol{x}^*$ in (180), we get

$$N_2(\boldsymbol{x}^*) = 0.25 \boldsymbol{q}^T (\boldsymbol{A}^{-1})^T \boldsymbol{A} \boldsymbol{A}^{-1} \boldsymbol{q} - 0.5 \boldsymbol{q}^T \boldsymbol{A}^{-1} \boldsymbol{q} + \boldsymbol{c} \quad (182)$$

$$= \boldsymbol{c} - 0.25 \boldsymbol{q}^T \boldsymbol{A} \boldsymbol{q}. \quad (183)$$

(183) follows from the symmetry of the 2×2 matrix $\boldsymbol{A}$.

REFERENCES

[1] 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.

[2] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. International Symposium on Inf. Theory (ISIT)*. IEEE, 2007.

[3] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Comm. and Networking*, vol. 2009, 2009.

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

[5] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Info. Theory*, vol. 57, no. 1, pp. 137–155, 2011.

[6] 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.

[7] 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.

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

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

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

[11] S. Salehkalaibar, M. Mirmohseni, and M. R. Aref, "One-receiver two-eavesdropper broadcast channel with degraded message sets," *IEEE Tran. on Info. Forensics and Security*, vol. 8, no. 7, pp. 1162–1172, 2013.

[12] J. Zhu and M. C. Gastpar, "Asymmetric compute-and-forward with CSIT," in *International Zurich Seminar on Comm.*, 2014.

[13] J. Zhu and M. Gastpar, "Gaussian multiple access via compute-and-forward," *IEEE Trans. Info. Theory*, 2016.

[14] A. A. Zewail and A. Yener, "Multi-terminal networks with an untrusted relay," in *52nd Annual Allerton Conf. On Comm., Control and Computing*. IEEE, 2014.

[15] ——, "The two-hop interference untrusted-relay channel with confidential messages," in *Proc. Inf. Theory Workshop (ITW)*. IEEE, 2015.

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

[17] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Info. Theory*, vol. 25, no. 5, pp. 572–584, 1979.

[18] 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.

[19] L. Sankaranarayanan, G. Kramer, and N. B. Mandayam, "Capacity theorems for the multiple-access relay channel," in *42nd Annual Allerton Conf. On Comm., Control, and Computing*, 2004, pp. 1782–1791.

[20] ——, "Hierarchical sensor networks: capacity bounds and cooperative strategies using the multiple-access relay channel model," in *First Annual IEEE Comm. Society Conf. on Sensor and Ad Hoc Comm. and Networks, SECON*. IEEE, 2004, pp. 191–199.

[21] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Info. Theory*, vol. 54, no. 11, pp. 5059–5067, 2008.

[22] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Info. Theory*, vol. 60, no. 4, pp. 2121–2138, 2014.

[23] S. A. Jafar, "Capacity with causal and noncausal side information: A unified view," *IEEE Trans. Info. Theory*, vol. 52, no. 12, pp. 5468–5474, 2006.

Ahmed A. Zewail (S'07) received the B.Sc. degree in electrical engineering from Alexandria University, Alexandria, Egypt, in 2011, and the M.Sc. degree in wireless communications from Nile University, Giza, Egypt, in 2013. Since 2013, he has been pursuing the Ph.D. degree and has been a graduate research assistant with the School of Electrical Engineering and Computer Science, Pennsylvania State University, University Park, PA, USA. His research interests include wireless communication, network information theory, information theoretic security, and coded caching.

Aylin Yener (S'91 - M'01 - SM'14 - F'15) received the B.Sc. degree in electrical and electronics engineering and the B.Sc. degree in physics from Bogazici University, Istanbul, Turkey, and the M.S. and Ph.D. degrees in electrical and computer engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ, USA. She is a Professor of Electrical Engineering at The Pennsylvania State University, University Park, PA, USA, since 2010, where she joined the faculty as an Assistant Professor in 2002. Since 2017, she is a Dean's Fellow in the College of Engineering at The Pennsylvania State University. She is currently also a Visiting Professor at the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. From 2008 to 2009, she was a Visiting Associate Professor with the same department. Her research interests include information theory, communication theory, and network science, with recent emphasis on green communications and information security. She received the NSF CAREER award in 2003, the Best Paper Award in Communication Theory in the IEEE International Conference on Communications in 2010, the Penn State Engineering Alumni Society (PSEAS) Outstanding Research Award in 2010, the IEEE Marconi Prize Paper Award in 2014, the PSEAS Premier Research Award in 2014, and the Leonard A. Doggett Award for Outstanding Writing in Electrical Engineering at Penn State in 2014.

Dr. Yener is currently a member of the Board of Governors of the IEEE Information Theory Society, where she was previously the treasurer (2012-2014). She served as the student committee chair for the IEEE Information Theory Society 2007 - 2011, and was the co-founder of the Annual School of Information Theory in North America co-organizing the school in 2008, 2009, and 2010. She was a technical (co)-chair for various symposia/tracks at the IEEE ICC, PIMRC, VTC, WCNC, and Asilomar (2005-2014). She served as an editor for the IEEE TRANSACTIONS ON COMMUNICATIONS (2009 - 2012), an editor and an editorial advisory board member for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS (2001-2012), and a guest editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (2011) and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (2015). Currently, she serves on the editorial board of the IEEE TRANSACTIONS ON MOBILE COMPUTING and as a senior editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.