The Two-Hop Interference Untrusted-Relay Channel with Confidential Messages

Ahmed A. Zewail and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
aiz103@psu.edu *yener@engr.psu.edu*

***Abstract*—This paper considers the two-user interference relay channel where each source wishes to communicate to its destination a message that is confidential from the other destination. Furthermore, the relay, that is the enabler of communication, due to the absence of direct links, is untrusted. Thus, the messages from both sources need to be kept secret from the relay as well. We provide an achievable secure rate region for this network. The achievability scheme utilizes structured codes for message transmission, cooperative jamming and scaled compute-and-forward. In particular, the sources use nested lattice codes and stochastic encoding, while the destinations jam using lattice points. The relay decodes two integer combinations of the received lattice points and forwards, using Gaussian codewords, to both destinations. The achievability technique provides the insight that we can utilize the untrusted relay node as an encryption block in a two-hop interference relay channel with confidential messages.**

I. Introduction

Cooperation with untrusted, i.e., honest but curious, relays has been studied in [1] and [2]. In contrast to reference [1], where the untrusted relay node is found to be ineffective as a cooperative entity if the relay channel is degraded/reversely degraded, reference [2] has shown that cooperation with an untrusted relay can be useful in other channel set ups. Reference [3] has considered the case where there is no direct link from the source to the destination, i.e., the untrusted relay is the only means of communication, and has shown that a positive secure rate is achievable with the aid of cooperative jamming from the destination. More specifically, in this set up, Gaussian codewords are employed with stochastic encoding, while the destination serves as a cooperative jammer transmitting Gaussian noise, and the relay employs Gaussian signaling and compress-and-forward. This model has been extended to the multiple access channel with an untrusted relay in [4]. The two-hop network with an untrusted relay has been also investigated in [5] where the source and destination use a nested lattice codebook to transmit their signals and the relay employs compute-and-forward. Furthermore, this scheme has also been extended to a multi-hop line network, where it is established that the achievable secure rate is independent of the number of hops [6]. Cooperation with untrusted relays has been further investigated under different scenarios, see, for example, [7]–[11]. In particular, in recent reference [10], the untrusted relay is employed to serve users with different levels of security clearance. Specifically, an X-channel with an untrusted relay has been considered where one of the destinations has higher security clearance. In this set up, each source transmits a common and private message, the common message should be decoded by both destinations, while the private message, should only be decoded by the destination with higher security clearance. Using Gaussian codebooks with stochastic encoding at the sources with the help of cooperative jamming from the destinations and compress-and-forward as the relaying strategy, we have defined an achievable secure rate region for this network [10]. It is worthwhile to note that in this previous work, the destination of higher security clearance has been assumed to have higher jamming power constraint.

In this paper, we consider a more egalitarian model, where each source aims to transmit one confidential message to its intended destination which should be kept secret from the other destination. We assume a two-hop model where a relay is the sole enabler of communication. The relay is untrusted and both messages are to be kept secret from it. The model is termed descriptively as the two-user *two-hop interference untrusted-relay channel with confidential messages*. This model resembles an ad-hoc network where the relay node is shared between different source-destination pairs that do not trust each other. We define an achievable secure rate region for this new model motivated by the recent results in scaled compute-and-forward and successive cancellation in [12] and [13]. In particular, each source uses random binning [14] on a nested lattice codebook, while its destination jams the relay with another independent codeword chosen uniformly from a nested lattice codebook. Therefore, the relay receives a noisy version of four independent lattice points. We require the untrusted relay to decode two integer combinations of these four points, such that it obtains two distinct linear integer combinations each of which represents the transmitted lattice points from a source-destination pair. The relay encodes each combination into a Gaussian codeword and transmits the sum of these two signals to both destinations. With the help of its jamming signal, each destination is able to recover its intended message, while the other message is secure at the unintended destination. In other words, our work shows that the untrusted relay can serve as an *encryption block* to secure the confidential messages over interference relay channels. The remainder of the paper is organized as follows. In Section II, we describe the model. The achievability scheme is detailed in Section III. The equivocation analysis is provided in Section IV. Finally, Section V summarizes our conclusions and learned insights.

II. System model

Consider a two-user interference channel with an untrusted relay as shown in Fig. 1. No direct links exist between the

978-1-4673-7852-9/15/$31.00 ©2015 IEEE

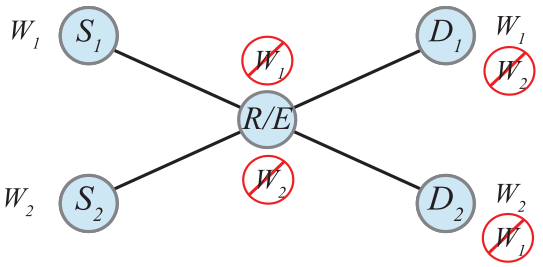

Fig. 1. The two-hop interference untrusted-relay channel with confidential messages.

sources and destinations, therefore, the untrusted relay is the only enabler of communication in this network. Node 1 aims to send a confidential message W_1, from the set $\{1, 2, .., 2^{NR_1}\}$, that should be decoded only by node 3 and be kept secret from node 4 as well as the untrusted relay. Similarly, node 2 aims to send a confidential message W_2, from the set $\{1, 2, .., 2^{NR_2}\}$, that should be decoded only by node 4 and be kept secret from node 3 as well as the untrusted relay. We consider a half-duplex scenario: nodes cannot transmit and receive simultaneously, therefore, the communications alternates between two phases. During the first phase, which occurs over l channel uses, nodes 1 and 2 transmit their signals to the untrusted relay while nodes 3 and 4 serve as cooperative jammers. The relay remains silent during this phase, and its received signal at channel use i is given by

$$Y_r(i) = \sum_{k=1}^{4} \sqrt{h_k} X_k(i) + Z_r(i), \qquad i = 1, ..l, \tag{1}$$

where $\sqrt{h_k}$ is the channel gain from node k to the relay, X_k is the transmitted signal by node k, and Z_r is the additive zero-mean Gaussian noise with unit variance. We assume each source-destination pair implements power control, and considers a received power constraint, or equivalently, we assume, without loss of generality, that $h_1 = h_3$ and $h_2 = h_4$.

During the second phase, which occurs over m channel uses, the relay forwards its signal to nodes 3 and 4. Nodes $1, 2, 3$ and 4 remain silent over this phase, and the received signal by node j at channel use i is expressed as

$$Y_j(i) = \sqrt{g_j} X_r(i) + Z_j(i), \quad i = l+1, .., l+m, \tag{2}$$

where $\sqrt{g_j}$ is the channel gain from the relay node to node j, X_r is the transmitted signal by the relay node and Z_j is the additive zero-mean Gaussian noise with unit variance.

The transmitted signal from each node has to satisfy an average power constraint that is given by

$$\frac{1}{n}\sum_{i=1}^{n} E[X_k^2(i)] \le \bar{P}, \quad k \in \{1, 2, 3, 4\}, \tag{3}$$

$$\frac{1}{n}\sum_{i=1}^{n} E[X_r^2(i)] \le \bar{P}_r, \tag{4}$$

where $n = l + m$ is the total number of the channel uses. Due to the fact that each node is transmitting only over one of the two phases, the transmitted signal from each node is subject to an *effective* average power constraint given by

$$P = \frac{\bar{P}}{\eta}, \qquad P_R = \frac{\bar{P}_r}{1-\eta}, \tag{5}$$

where $\eta = \frac{l}{n}$ is the time sharing parameter of the first phase.

The secrecy of the confidential message W_l needs to be ensured at both the unintended destination and untrusted relay node. Therefore, we define the secrecy constraints at the unintended destinations and relay as follows.

$$\frac{1}{n}H(W_2|Y_3^n, W_1, X_3^n) \ge \frac{1}{n}H(W_2) - \epsilon, \tag{6}$$

$$\frac{1}{n}H(W_1|Y_4^n, W_2, X_4^n) \ge \frac{1}{n}H(W_1) - \epsilon, \tag{7}$$

$$\frac{1}{n}H(W_l|Y_r^n, W_k) \ge \frac{1}{n}H(W_l) - \epsilon \quad l, k = 1, 2; l \ne k. \tag{8}$$

III. Achievable Secure Rate Region

In this section, we provide the details of the achievability scheme.

A. The first phase

At each source, we use nested lattices and random binning, similar to [6]. We start with the illustration of the inner code that is motivated by scaled compute-and-forward proposed in [12] and [13].

Let us first set up the notation related to lattice codes. A lattice Λ is a discrete group of $\mathbb{R}^N$ that satisfies the condition 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

$$Q_\Lambda(x^N) = \arg\min_{t^N \in \Lambda} ||t^N - x^N||, \tag{9}$$

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

$$x^N \mod \Lambda = x^N - \arg\min_{t^N \in \Lambda} ||t^N - x^N||. \tag{10}$$

The fundamental Voronoi region of Λ is defined to be

$$\mathcal{V}(\Lambda) = \{x^N : Q_\Lambda(x^N) = \mathbf{0}\}, \tag{11}$$

where $\mathbf{0}$ is all-zero vector with length N. Λ and Λ_k are nested lattices if $\Lambda_k \subseteq \Lambda$. 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

$$\frac{1}{N\text{Vol}(\mathcal{V}(\Lambda_k))}\int_{\mathcal{V}(\Lambda_k)} ||x^N||^2 dx = \beta_k^2 P. \tag{12}$$

Node k generates its codebook $\mathcal{C}_k = \Lambda \cap \mathcal{V}(\Lambda_k)$ with rate given by

$$R_k^c = \frac{1}{N}\log|\mathcal{C}_k| = \frac{1}{N}\log\frac{\text{Vol}(\mathcal{V}(\Lambda_k))}{\text{Vol}(\mathcal{V}(\Lambda))}. \tag{13}$$

In our achievable scheme, we assume that $\mathcal{C}_1 = \mathcal{C}_3$, $\mathcal{C}_2 = \mathcal{C}_4$, $\beta_1 = \beta_3$ and $\beta_2 = \beta_4$, i.e., each source-destination pair uses

the same nested lattice codebook. To transmit a lattice point t_k^N, node k forms the following signal

$$X_k^N = (t_k^N/\beta_k + d_k^N) \mod \Lambda_k/\beta_k, \tag{14}$$

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 to all network nodes.

Each source applies stochastic encoding as an outer code. More specifically, node k, $k = 1, 2$, divides the codewords of its codebook $\mathcal{C}_k$ 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 from the eavesdropper associated with the relay node as we will see in the following section. To send message W_k, node k randomly picks a point t_k^N from the bin indexed by W_k and then transmits the corresponding signal X_k^N. Meanwhile, nodes 3 and 4 randomly choose $t_3^N \in \mathcal{C}_3$, and $t_4^N \in \mathcal{C}_4$, respectively, and transmit the corresponding signals X_3^N and X_4^N.

Decoding at the relay: We require the relay to decode two different integer combinations of the received lattice points. Let $\boldsymbol{a} = [a_1, .., a_4]^T$ and $\boldsymbol{b} = [b_1, .., b_4]^T$ represent the coefficients of the decoded combinations. The relay follows the same procedure as in [13] for decoding. From its received signal, the relay forms the following signal to decode the first integer combination

$$\bar{y}_1^N = \alpha_1 Y_r^N - \sum_{k=1}^4 a_k\beta_k d_k^N \tag{15}$$

$$= \sum_{k=1}^4 (\alpha_1 h_k - a_k\beta_k)X_k^N + \alpha_1 Z_r^N + \sum_{k=1}^4 a_k\beta_k X_k^N - \sum_{k=1}^4 a_k\beta_k d_k^N, \tag{16}$$

where α_1 is some real number. To simplify the notation, we define $\bar{z}_1^N = \sum_{k=1}^4 (\alpha_1 h_k - a_k\beta_k)X_k^N + \alpha_1 Z_r^N$. Note that thanks to the dither vector d_k^N, the signals t_k^N and X_k^N are independent. Now, we can express (16) as follows.

$$\bar{y}_1^N = \bar{z}_1^N + \sum_{k=1}^4 a_k\beta_k X_k^N - \sum_{k=1}^4 a_k\beta_k d_k^N \tag{17}$$

$$= \sum_{k=1}^4 a_k(\beta_k(t_k^N/\beta_k + d_k^N) - \beta_k Q_{\Lambda_k/\beta_k}(t_k^N/\beta_k + d_k^N)) + \bar{z}_1^N - \sum_{k=1}^4 a_k\beta_k d_k^N \tag{18}$$

$$= \bar{z}_1^N + \sum_{k=1}^4 a_k(t_k^N - Q_{\Lambda_k}(t_k^N + \beta_k d_k^N)) \tag{19}$$

$$= \bar{z}_1^N + \sum_{k=1}^4 a_k \bar{t}_k^N, \tag{20}$$

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 because $\bar{z}_1^N$ $\sum_{k=1}^4 a_k \bar{t}_k^N$ are independent. Hence, the achievable rate for this combination is given by

$$R_{k1} \leq \max\left(\max_{\alpha_1} 0.5 \log \frac{\beta_k P}{N_1(\alpha_1)}, 0\right), \tag{21}$$

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

$$N_1(\alpha_1) = \sum_{k=1}^4 (\alpha_1 h_k - a_k\beta_k)^2 P + \alpha_1^2. \tag{22}$$

The maximization of the rate in (21) is equivalent to minimizing N_1 over α_1, which results in the following value of N_1

$$N_1(\alpha_1^*) = ||\hat{\boldsymbol{a}}||^2 P - \frac{P^2 \boldsymbol{h}^T \hat{\boldsymbol{a}}}{1 + P||\boldsymbol{h}||^2}, \tag{23}$$

where $\boldsymbol{h} = [h_1, .., h_4]^T$ 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

$$\bar{y}_2^N = \alpha_2 Y_r^N - \sum_{k=1}^4 b_k\beta_k d_k^N - \lambda(\sum_{k=1}^4 a_k \bar{t}_k^N + \sum_{k=1}^4 a_k\beta_k d_k^N) \tag{24}$$

$$= \sum_{k=1}^4 [\alpha_2 h_k - (\lambda a_k + b_k)\beta_k]X_k^N + \alpha_2 Z_r^N + \sum_{k=1}^4 b_k \bar{t}_k^N \tag{25}$$

$$= \bar{z}_2^N + \sum_{k=1}^4 b_k \bar{t}_k^N, \tag{26}$$

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

$$R_{k2|\boldsymbol{a}} \leq \max\left(\max_{\alpha_2, \lambda} 0.5 \log \frac{\beta_k P}{N_2(\alpha_2, \lambda)}, 0\right), \tag{27}$$

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

$$N_2(\alpha_2, \lambda) = \sum_{k=1}^4 (\alpha_2 h_k - (\lambda a_k + b_k)\beta_k)^2 P + \alpha_2^2. \tag{28}$$

The maximum rate in (27) is attained when N_2 is given by

$$N_2(\alpha_2^*, \lambda^*) = \hat{\boldsymbol{b}}^{\boldsymbol{T}} \hat{\boldsymbol{b}} P - 0.25 \boldsymbol{q}^{\boldsymbol{T}} \boldsymbol{A} \boldsymbol{q}, \tag{29}$$

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 the optimization over α_1, α_2 and λ are straight forward and thus here omitted.

In our achievability scheme, we choose $\boldsymbol{a}, \boldsymbol{b}$ from the set $\{[1, 0, 1, 0]^T, [0, 1, 0, 1]^T, [1, 1, 1, 1]^T\}$ and $\boldsymbol{a} \neq \boldsymbol{b}$. This choice ensures that after successful decoding of the two integer combinations $\sum_{k=1}^4 a_k \bar{t}_k^N$ and $\sum_{k=1}^4 b_k \bar{t}_k^N$, the relay can get $\bar{t}_1^N + \bar{t}_3^N$ and $\bar{t}_2^N + \bar{t}_4^N$ that will be transmitted to nodes 3 and 4 over the second phase.

Note that 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]. This results in the following achievable transmission

rate region for $\bar{t}_1^N$ and $\bar{t}_2^N$.

$$R_1^1 \leq \begin{cases} R_{11} & \text{if } a_1 = 1 \text{ and } b_1 = 0, \\ R_{12|\boldsymbol{a}} & \text{if } a_1 = 0 \text{ and } b_1 = 1, \\ \min(R_{11}, R_{12|\boldsymbol{a}}) & \text{if } a_1 = 1 \text{ and } b_1 = 1, \end{cases} \quad (30)$$

$$R_2^1 \leq \begin{cases} R_{21} & \text{if } a_2 = 1 \text{ and } b_2 = 0, \\ R_{22|\boldsymbol{a}} & \text{if } a_2 = 0 \text{ and } b_2 = 1, \\ \min(R_{21}, R_{22|\boldsymbol{a}}) & \text{if } a_2 = 1 \text{ and } b_2 = 1. \end{cases} \quad (31)$$

B. The second phase

After obtaining the desired two integer combinations, the relay encodes each of them into a Gaussian codeword and forwards them to nodes 3 and 4. More specifically, the linear combination $\bar{t}_1^N + \bar{t}_3^N$ is encoded into a codeword X_{r3}^m from a Gaussian codebook randomly generated according to $\mathcal{N}(0, \zeta_3 P_r)$, and the linear combination $\bar{t}_2^N + \bar{t}_4^N$ is encoded into a codeword X_{r4}^m from a Gaussian codebook randomly generated according to $\mathcal{N}(0, \zeta_4 P_r)$, where $\zeta_3 + \zeta_4 \in [0, 1]$ and $\zeta_3, \zeta_4 \geq 0$. The relay transmits the signal $X_r^m = X_{r3}^m + X_{r4}^m$.

Decoding at destinations: The channel from the relay to nodes 3 and 4 is a two-user broadcast channel. The weaker receiver (i), i.e., $g_i \leq g_j, i, j \in \{3, 4\}$, decodes its desired signal X_{ri}^m and treats X_{rj}^m as noise. The stronger receiver (j), decodes X_{ri}^m first and then applies successive cancellation and decodes X_{rj}^m. The achievable rate region during the second phase is thus given by

$$R_i^2 \leq C\left(\frac{\zeta_i g_i P_r}{1 + \zeta_j g_i P_r}\right), \qquad R_j^2 \leq C(\zeta_j g_j P_r), \quad (32)$$

where $C(x) = 0.5 \log_2(1 + x)$.

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 jamming signal and the received combination, each of nodes 3 and 4 is able to decode its desired message.

Consequently, we can state the following theorem that represents the main result of this paper.

Theorem 1 *The following secure rate region is achievable for two-user interference untrusted-relay channel with confidential messages*

$$\max_{\boldsymbol{\beta}, \eta, \boldsymbol{a}, \boldsymbol{b}, \zeta_3, \zeta_4} \Big\{ R_1 \leq \min(\eta[R_1^1 - 1]^+, (1 - \eta) R_3^2) \\ R_2 \leq \min(\eta[R_2^1 - 1]^+, (1 - \eta) R_4^2) \Big\}. \quad (33)$$

The proof of this theorem is completed in Section IV.

Observe that the achievability uses both structured and Gaussian signaling. In particular, the sources, nodes 1 and 2, and destinations, nodes 3 and 4, use nested lattice codebooks for sending the confidential messages and jamming, respectively, while the relay node uses a Gaussian codebooks to forward its signals to both destinations.

Remark 1 *Note that imposing secrecy constraints at the relay node results 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 that is needed to ensure the secrecy of the confidential messages at the untrusted relay as will be shown in Section IV. This means that 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.*

Remark 2 *In our previous work in [10], we provided an outer bound for the X-channel with private and common messages and untrusted relay. In developing this outer bound, we only considered the eavesdropper associated with the relay node. It is worth mentioning that this outer bound is applicable -albeit loose- for the model considered in this paper, as removing the eavesdroppers associated with the destinations cannot reduce the secure rate. Also, note that any outer bound that is obtained on $\frac{1}{n} H(W_1|Y_r^n)$ is also an outer bound on $\frac{1}{n} H(W_1|Y_r^n, W_2)$ as conditioning cannot increase the entropy.*

IV. Equivocation Analysis

In this section, we complete the proof of Theorem 1 by calculating the equivocation rates obtained by our achievable scheme. To do this, first we recall some results that are used throughout the equivocation calculations.

Lemma 1 *Crypto lemma [15]: 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 2 *The representation theorem [16]: 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 *[17] For random variables A and B, and discrete random variable T, we have $H(A|B,T) \geq H(A|B) - H(T)$.*

In the following, 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

Here, we focus on the equivocation at the untrusted relay.

$$\begin{aligned} & H(t_1^N|Y_r^n, W_2) \\ & \geq H(t_1^N|Y_r^n, Z_r^n, X_2^n, X_4^n, W_2) && (34) \\ & = H(t_1^N|X_1^N + X_3^N) && (35) \\ & = H(t_1^N|X_1^N + X_3^N \mod \Lambda_1/\beta_1, T_1) && (36) \\ & = H(t_1^N|t_1^N/\beta_1 + t_3^N/\beta_1 \mod \Lambda_1/\beta_1, T_1) && (37) \\ & \geq H(t_1^N|t_1^N/\beta_1 + t_3^N/\beta_1 \mod \Lambda_1/\beta_1) - H(T_1) && (38) \\ & \geq H(t_1^N) - H(T_1) && (39) \\ & \geq H(t_1^N) - N. && (40) \end{aligned}$$

The steps (36) and (40) follow from applying the representation theorem for $K = 2$, where T_1 is an integer such that $1 \leq T_1 \leq 2^N$, while the step (38) results by applying Lemma

2. The step (39) is due to the crypto lemma. Finally, from (40), we obtain

$$\frac{1}{N} I(t_1^N; Y_r^n, W_2) \leq 1. \tag{41}$$

Similarly, we can obtain the following for t_2^N

$$\frac{1}{N} I(t_2^N; Y_r^n, W_1) \leq 1. \tag{42}$$

The above results indicate that the leaked information about the value of t_1^N (t_2^N) to the eavesdropper associated with the relay node cannot exceed 1 bit per channel use, therefore by using stochastic encoding we can ensure the secrecy of the confidential message at the untrusted relay and achieve the rate expression in Theorem 1.

Remark 3 *Note that the secrecy constraints in (8) implies that* $\frac{1}{n} I(W_1, W_2; Y_r^n) \to 0$ *as* $n \to \infty$*, since*

$$\begin{aligned} I(W_1, W_2; Y_r^n) &= I(W_1; Y_r^n) + I(W_2; Y_r^n | W_1) && (43)\\ &= H(W_1) - H(W_1|Y_r^n) + I(W_2; Y_r^n|W_1) && (44)\\ &\leq H(W_1|W_2) - H(W_1|W_2, Y_r^n) + I(W_2; Y_r^n|W_1) && (45)\\ &= I(W_1; Y_r^n|W_2) + I(W_2; Y_r^n|W_1). && (46) \end{aligned}$$

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

B. At the destinations

In this subsection, we focus on the equivocation analysis of the confidential messages at the destinations.

$$\begin{aligned} &H(W_1|Y_2^n, X_4^n, W_2) \geq H(W_1|Y_2^n, X_4^n, W_2, X_{r2}^m, Z_2^m)\\ &= H(W_1|X_{r1}^m) = H(W_1). \end{aligned} \tag{47}$$

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

$$H(W_2|Y_1^n, X_3^n, W_1) \geq H(W_2). \tag{48}$$

Remark 4 *The achievable scheme ensures the secrecy of the confidential messages from any external eavesdropper that can overhear the relay signal during the second phase. This observation illustrates how our scheme utilizes the untrusted relay as an encryption block.*

V. Conclusions

In this work, we have demonstrated the possibility of securing confidential messages using an untrusted relay. In particular, we have studied two-user two-hop interference relay channel, where each source aims to communicate securely with its intended receiver while protecting its message from the untrusted relay and the other destination. We have defined an achievable rate region using a combination of nested lattice code and stochastic encoding at the sources with the help of structured jamming from the destinations. The relay is required to decode two different integer combinations of the four received lattice points and forwards them to both destinations. By using structured signals during the first phase and requiring the untrusted relay to decode specific integer combinations of these signals then forwarding them as Gaussian signals during the second phase, our proposed achievability technique utilizes the untrusted relay as an encryption block in the network.

It is worth noting that this achievability scheme can be extended to the K-user interference relay channel with confidential messages and untrusted relay, where $K > 2$. The transmitted signals from the sources and destinations follow the same procedure. The relay would have to be required to decode K different integer combinations of the received lattice points. The relay would perform *noise prediction* as in [13] to decode the K different integer combinations.

It is also worth noting that we assumed a model where the relay, despite of being untrusted, conforms to the network protocols, i.e., is honest but curious, rather than rogue, e.g., Byzantine, and the nodes on which secrecy constraints are imposed do not collude. Future directions include removing either or both of these assumptions.

References

[1] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. Inf. Theory Workshop (ITW)*. IEEE, 2001.

[2] 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.

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

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

[5] 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.

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

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

[8] 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.

[9] 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.

[10] 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*. IEEE, 2014.

[11] 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.

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

[13] J. Zhu and M. Gastpar, "Multiple access via compute-and-forward," *arXiv:1407.8463*, 2014.

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

[15] 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.

[16] 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.

[17] 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.