Fifty-second Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 1 - 3, 2014

Multi-terminal Networks with an Untrusted Relay

Ahmed A. Zewail, Mohamed Nafea, and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
{*aiz103,msn139*}*@psu.edu* *yener@engr.psu.edu*

***Abstract*—This paper investigates the impact of cooperation with an untrusted relay in multi-source multi-destination networks. The set up considered is one where the relay is the only means of communications due to the absence of direct links between the sources and the destinations. Since the relay is untrusted, all messages from the sources need to be kept secret from the relay. Furthermore, the destinations are assumed to have different levels of security clearance, i.e., some private messages should only be decoded by their intended receiver and should be kept secret from other destinations. An achievable secure rate region is found by using random binning at the sources, cooperative jamming from the destinations, and compress-and-forward at the relay. Additionally, a genie aided outer bound on the secure rate region is derived. Comparison of inner and outer bounds are provided.**

I. Introduction

Cooperative relaying is imperative for wireless multihop networking. More often than not, once can envision a single node serving as a shared relay to many source destination pairs. In such scenarios, a natural concern is one of confidentiality, to ensure that only the intended destinations have access to messages sent by the sources. Previous work has shown that in the three-node model, it is possible to provide reliable communication rates from the source to the destination utilizing the relay node while simultaneously keeping source's messages information theoretically secure from the relay [1]. Such a node, where the relay is a legitimate entity in the network who is willing to cooperate, yet is treated as an eavesdropper by the system is termed an *untrusted relay* [2].

This paper builds upon the extensive literature on providing reliable communications under information theoretic security guarantees for multiterminal systems, see for example [1]–[11]. Cooperation with untrusted relays in single source destination set up goes back to [1], [2], [8], see also [9]. References [2], [8], [12] have considered models with untrusted relays with no direct link between the source(s) and the destination, making the untrusted relay(s) essential for communication. In these instances, cooperative jamming by the destination proves useful in providing secure communication. In addition to untrusted nodes that relay signals, once can also envision different security clearances by different destinations. In particular, some messages may need to be kept secret from unintended receivers [11], [13], [14].

In this paper, we consider a set up that captures cooperative communications by means of an untrusted relay to be shared between multiple source and destinations (receivers) with different levels of security clearance. Specifically, we consider a Gaussian two-source two-destination network with a shared relay, and no direct link between the sources and the destinations. All communication is via the untrusted relay node which is treated as an eavesdropper. We assume that one of the two destinations, the first one, has a higher level of security clearance. More specifically, each source transmits two independent messages that should be kept secret from the relay and one of them should only be decoded by the first destination and be kept secret from the second one. The model generalizes that considered in recent work [12], which considers a multiple access relay channel with an untursted relay to multiple destinations and private and common communication rates. We define an achievable secure rate region, using random binning at the sources and compress-and-forward as a relaying strategy with the help of cooperative jamming from both destinations, under the assumption that the destination cleared to decode all messages is also a node with higher jamming power. Second, we derive a genie aided outer bound on the secure rate region. Similar to the approach in [2], [12], the outer bound is derived by adding an external eavesdropper to the network that receives a signal which is statistically equivalent to the one received by the relay. We compare the the inner and outer bounds.

The remainder of the paper is organized as follows. Section II describes the system model and the main assumptions. The achievability scheme is provided in Section III. In Section IV, the outer bound is developed. Section V presents the numerical results and Section VI concludes the paper.

II. System model

Consider an X-channel, where sources (S_1, S_2) have messages for destinations (D_1, D_2). There is no direct link between the sources and the destinations, see Fig. 1. $S_k, k = 1, 2$ transmits two messages:

- A common secure message (W_k^s) from the set $\{1, .., 2^{nR_k^s}\}$, which should be decoded by both D_1 and D_2, but needs to be kept secret from the untrusted relay.
- A private message (W_k^p) from the set $\{1, .., 2^{nR_k^p}\}$ that should be decoded by D_1 only and kept secret from both the untrusted relay and D_2.

We assume all nodes operate in half-duplex mode. The communication is done over two phases. In the first phase, which

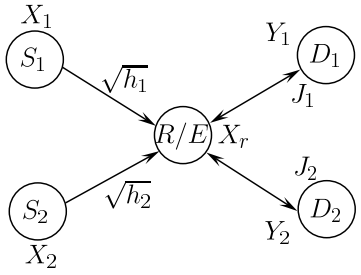

Fig. 1. The X-channel with untrusted relay.

occurs over n channel uses, sources transmit their signals, X_1 and X_2, to the relay while the two destinations jam the relay with Gaussian noise J_k and $k \in \{1,2\}$ respectively. The received signal at the relay, at channel use i, is given by

$$Y_r(i) = \sqrt{h_1}X_1(i) + \sqrt{h_2}X_2(i) + J_1(i) + J_2(i) + Z_r(i), \quad (1)$$

where Z_r is zero-mean Gaussian noise with unit variance and $\sqrt{h_k}$ is the channel gain from S_k to the relay. In the second phase, which occurs over m channel uses, the relay broadcasts the signal X_r to D_1 and D_2, thus the received signal at D_k, at channel use j, is given by

$$Y_k(j) = X_r(j) + Z_k(j), \qquad k \in \{1,2\}, \quad (2)$$

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

Let $N = n + m$ be the total number of channel uses and define $\beta = \frac{n}{N}$ as the time sharing parameter of the first phase. The transmitted signals from S_k, D_k and the relay should satisfy the following average power constraints

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

$$\frac{1}{N}\sum_{i=1}^{N} E[X_r^2(i)] \le \bar{P}_r. \quad (3)$$

Since each node transmits in only one of the two phases, each node has an *effective* average power constraint

$$P_r = \frac{\bar{P}_r}{1-\beta}, \quad P_k = \frac{\bar{P}_k}{\beta}, \quad P_{Jk} = \frac{\bar{P}_{Jk}}{\beta}, \quad k \in \{1,2\}. \quad (4)$$

As a modeling assumption, we require D_1, the terminal that is required to decode all the messages, i.e., the terminal with the highest security clearance, to also be the terminal that can offer to be a more powerful cooperative jammer, i.e., $P_{J1} \ge P_{J2}$. Let $W^{ps} = \{W_1^s, W_2^s, W_1^p, W_2^p\}$, $W^p = \{W_1^p, W_2^p\}$ and $Y^N = \{Y(1), Y(2), \cdots, Y(N)\}$. The secrecy constraints are [4]:

$$\frac{1}{N}H(\mathcal{S}|Y_r^N) \ge \frac{1}{N}H(\mathcal{S}) - \epsilon, \qquad \forall \mathcal{S} \subseteq W^{ps}, \quad (5)$$

$$\frac{1}{N}H(\mathcal{S}|Y_2^N) \ge \frac{1}{N}H(\mathcal{S}) - \epsilon, \qquad \forall \mathcal{S} \subseteq W^{p}. \quad (6)$$

Remark 1 *Note that this model is equivalent to the one where there are two external jammers which jam the relay during the first phase, and the jamming signal of each of them is heard by one of the two 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 $Y_k^N = \{J_k^n, Y_k^m\}$.*

In the remainder of this paper, we use $C(x) \triangleq 0.5\log_2(1+x)$ and $[x]^+ \triangleq \max(0,x)$. Also, we omit the index for channel use whenever it is obvious from the context.

III. An achievable secure rate region

In this section, we define an achievable secure rate region for the X-channel with an untrusted relay. We use stochastic encoding at the sources, and compress-and-forward at the relay as in [2], [12] with the help of cooperative jamming from both destinations.

1) At the sources: We generate $2^{n(R_k^s + R_k^{x1})}$ codewords $\{U_k^n\}$ drawn from $\mathcal{N}(0, \bar{\alpha}_k P_k)$ and distribute them over $2^{nR_k^s}$ bins, each of them is indexed by one of W_k^s's and contains $2^{nR_k^{x1}}$ codewords. Next, we generate $2^{n(R_k^p + R_k^{x2})}$ codewords $\{V_k^n\}$ drawn from $\mathcal{N}(0, \alpha_k P_k)$ and distribute them over $2^{nR_k^p}$ bins, each of them is indexed by one of the W_k^p's and contains $2^{nR_k^{x2}}$ codewords, where $\bar{\alpha}_k + \alpha_k = 1 - \delta_k$ and δ_k is an arbitrary small number to guarantee that the corresponding power constraint is satisfied. R_k^{x1} is chosen to confuse the relay while R_k^{x2} is chosen to confuse both the relay and D_2. The values R_k^{x1} and R_k^{x2} will be specified later. Finally, to transmit a pair (W_k^s, W_k^p), S_k picks uniformly random codewords from the bins indexed by W_k^s and W_k^p, then forms the transmitted signal $X_k^n = U_k^n + V_k^n$.

2) At the relay: The relay compresses the received signal Y_r^n into a quantized version $\hat{Y}_r^n$ and transmits the corresponding signal X_r^m. The elements of X_r^m are drawn from $\mathcal{N}(0, P_r)$. We have the following condition on the channel input distribution

$$p(U_1^n, U_2^n, V_1^n, V_2^n, J_1^n, J_2^n, X_r^m) = p(U_1^n)p(U_2^n)p(V_1^n)p(V_2^n)p(J_1^n)p(J_2^n)p(X_r^m). \quad (7)$$

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

$$R_k^s \le \beta\Bigg[C\left(\frac{\bar{\alpha}_k h_k P_k}{1 + P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right) - C\left(\frac{\bar{\alpha}_k h_k P_k}{1 + P_{J1} + P_{J2} + h_j P_j + \alpha_k h_k P_k}\right)\Bigg]^+, \quad (8)$$

$$R_1^s + R_2^s \le \beta\Bigg[C\left(\frac{\bar{\alpha}_1 h_1 P_1 + \bar{\alpha}_2 h_2 P_2}{1 + P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right) - C\left(\frac{\bar{\alpha}_1 h_1 P_1 + \bar{\alpha}_2 h_2 P_2}{1 + P_{J1} + P_{J2} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2}\right)\Bigg]^+, \quad (9)$$

$$R_k^p + R_k^s \le \beta\Bigg[C\left(\frac{h_k P_k}{1+P_{J2}+\sigma_Q^2}\right) - C\left(\frac{h_k P_k}{1+P_{J1}+P_{J2}+h_j P_j}\right)\Bigg]^+, \quad (10)$$

$$R_k^p \le \beta\left[C\left(\frac{\alpha_k h_k P_k}{1+P_{J2}+\sigma_Q^2}\right) - C\left(\frac{\alpha_k h_k P_k}{1+P_{J1}+\alpha_j h_j P_j+\sigma_Q^2}\right)\right]^+, \quad (11)$$

$$R_1^p + R_2^p \le \beta\Bigg[C\left(\frac{\alpha_1 h_1 P_1+\alpha_2 h_2 P_2}{1+P_{J2}+\sigma_Q^2}\right) - C\left(\frac{\alpha_1 h_1 P_1+\alpha_2 h_2 P_2}{1+P_{J1}+\sigma_Q^2}\right)\Bigg]^+, \quad (12)$$

$$R_1^p + R_1^s + R_2^p + R_2^s \le \beta\Bigg[C\left(\frac{h_2 P_2+h_1 P_1}{1+P_{J2}+\sigma_Q^2}\right) - C\left(\frac{h_2 P_2+h_1 P_1}{1+P_{J1}+P_{J2}}\right)\Bigg]^+, \quad (13)$$

where $k, j \in \{1,2\}$, $k \neq j$, and $\forall \beta$ σ_Q^2 is the quantization noise which is calculated from

$$\beta C\left(\frac{h_1 P_1+h_2 P_2+P_{J1}+1}{\sigma_Q^2}\right) = (1-\beta)C(P_r). \quad (14)$$

Proof: The proof is provided in the appendix.

Remark 2 *Since the achievable rates increase with the increase in the time sharing parameter β, the relay should always transmits with its maximum power.*

Remark 3 *If $\bar{P}_r \to \infty$, then the optimal $\beta \to 1$ and the quantization noise $\sigma_Q^2 \to 0$.*

Remark 4 *In general, the achievable rates are not increasing functions in the transmitting powers. Therefore, there exists an optimal power allocation at the sources which may not be equal to the maximum power.*

Remark 5 *If we deactivate the first destination node, i.e., $P_{J1} = 0$, the network reduces to a multiple access relay channel and the common secure rate region is equivalent to the one in [12] for $K = 2$.*

IV. Outer bound on the secure rate region

In this section, we derive a genie aided outer bound on the secure rate region of the network. We modify the relay/eavesdropper separation technique proposed in [2], and utilized in [12] as follows. First, we insert an external eavesdropper (E) into the network, that has the same channel statistics as the one associated to the relay node. More specifically, the received signal at this external eavesdropper, at channel use i, is given by

$$Y_e(i) = \sqrt{h_1}X_1(i)+\sqrt{h_2}X_2(i)+J_1(i)+J_2(i)+Z_e(i), \quad (15)$$

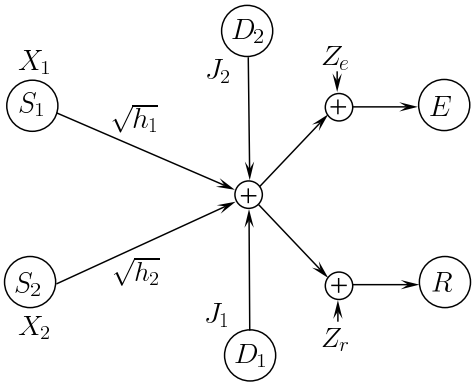

Fig. 2. An equivalent network used to calculate the outer bound.

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

Second, we remove the eavesdropper associated with the relay, i.e., consider the relay to be trusted as illustrated in Fig. 2. In addition, we assume that X_r is delivered to both destinations as genie information. Lastly, we consider that one of the jamming signals, J_1, J_2, is given to the relay by the genie, where the jamming signal given to the relay depends on the type of rates that we calculate the outer bound on, i.e., common or private rates.

To derive the upper bounds for the common rates, we consider that the genie transfers the jamming signal J_2 to the relay, where the relay is now trusted with the above transformation, and then we utilize the secrecy constraint at E and the reliability constraint at D_2. Note that the bound on the common message rate comes from the bound on the secure rates of D_2 as it is assumed to be the weaker jammer. For the rate of the message W_1^s, we have

$$\begin{aligned}
&H(W_1^s|Y_e^n)\\
&\le H(W_1^s|Y_e^n) - H(W_1^s|X_2^n X_r^m Y_2^m J_2^n) + n\epsilon_1 && (16)\\
&= H(W_1^s|Y_e^n) - H(W_1^s|X_2^n X_r^m J_2^n) + n\epsilon_1 && (17)\\
&\le H(W_1^s|Y_e^n) - H(W_1^s|X_2^n X_r^m Y_r^n J_2^n) + n\epsilon_1 && (18)\\
&= H(W_1^s|Y_e^n) - H(W_1^s|X_2^n Y_r^n J_2^n) + n\epsilon_1 && (19)\\
&= H(W_1^s|Y_e^n) - H(W_1^s|\sqrt{h_1}X_1^n + J_1^n + Z_r^n) + n\epsilon_1 && (20)\\
&\le H(W_1^s|Y_e^n) - H(W_1^s|\sqrt{h_1}X_1^n + J_1^n + Z_r^n, Y_e^n) + n\epsilon_1. && (21)
\end{aligned}$$

(16) results from Fano's inequality. In (17), Y_2^m was removed as X_r^m is given to the destinations by a genie. Also, since J_2^n is provided as a genie information to the relay, we get (16)-(19). To simplify the notation, let $G_1^n = \sqrt{h_1}X_1^n + J_1^n + Z_r^n$. Thus, (21) can be rewritten as

$$H(W_1^s|Y_e^n) - H(W_1^s|G_1^n, Y_e^n) + n\epsilon_1$$

$$= I(W_1^s; G_1^n|Y_e^n) + n\epsilon_1 \quad (22)$$
$$\leq I(W_1^s, X_1^n; G_1^n|Y_e^n) + n\epsilon_1 \quad (23)$$
$$= I(X_1^n; G_1^n|Y_e^n) + n\epsilon_1 \quad (24)$$
$$= h(G_1^n|Y_e^n) - h(J_1^n + Z_r^n|\sqrt{h_2}X_2^n + Z_e^n + J_1^n + J_2^n) + n\epsilon_1 \quad (25)$$
$$\leq h(G_1^n|Y_e^n) - h(J_1^n + Z_r^n|\sqrt{h_2}X_2^n + Z_e^n + J_1^n + J_2^n, J_2^n) + n\epsilon_1 \quad (26)$$
$$= h(G_1^n|Y_e^n) - h(J_1^n + Z_r^n|Z_e^n + J_1^n + \sqrt{h_2}X_2^n) + n\epsilon_1, \quad (27)$$

which can be maximized with Gaussian signals. Let $O_t = h_1P_1 + h_2P_2 + P_{J1} + P_{J2}$ and $O_{ts}^k = h_kP_k + P_{J1}$. We have the following upper bound on R_k^s.

$$R_k^s \leq \max_{\beta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{0.5\beta\log_2(A_k), (1-\beta)C(P_r)\right\}, \quad (28)$$

where,

$$A_k = \frac{[(1+O_t)(1+O_{ts}^k) - (O_{ts}^k+\rho)^2](O_{ts}^j+1)}{[(1+O_{ts}^j)(P_{J1}+1) - (P_{J1}+\rho)^2](1+O_t)}, \quad (29)$$

and $k, j = 1, 2$, $k \neq j$. Similarly, we proceed to calculate the following outer bound on common secure sum rate.

$$H(W_1^s, W_2^s|Y_e^n)$$
$$\leq H(W_1^s, W_2^s|Y_e^n) - H(W_1^s, W_2^s|X_r^m Y_2^m J_2^n) + n\epsilon_2 \quad (30)$$
$$= H(W_1^s, W_2^s|Y_e^n) - H(W_1^s, W_2^s|X_r^m J_2^n) + n\epsilon_2 \quad (31)$$
$$\leq H(W_1^s, W_2^s|Y_e^n) - H(W_1^s, W_2^s|X_r^m Y_r^n J_2^n) + n\epsilon_2 \quad (32)$$
$$= H(W_1^s, W_2^s|Y_e^n) - H(W_1^s, W_2^s|Y_r^n J_2^n) + n\epsilon_2 \quad (33)$$
$$= H(W_1^s, W_2^s|Y_e^n) + n\epsilon_2 - H(W_1^s, W_2^s|\sqrt{h_1}X_1^n + \sqrt{h_2}X_2^n + J_1^n + Z_r^n) \quad (34)$$
$$\leq H(W_1^s, W_2^s|Y_e^n) + n\epsilon_2 - H(W_1^s, W_2^s|\sqrt{h_1}X_1^n + \sqrt{h_2}X_2^n + J_1^n + Z_r^n, Y_e^n). \quad (35)$$

To simplify the notation, let $G_2^n = \sum_{k=1}^2 \sqrt{h_k}X_k^n + J_1^n + Z_r^n$. Thus, (35) is rewritten as

$$H(W_1^s, W_2^s|Y_e^n) - H(W_1^s, W_2^s|G_2^n, Y_e^n) + n\epsilon_2$$
$$= I(W_1^s, W_2^s; G_2^n|Y_e^n) + n\epsilon_2 \quad (36)$$
$$\leq I(W_1^s, W_2^s, X_1^n, X_2^n; G_2^n|Y_e^n) + n\epsilon_2 \quad (37)$$
$$= I(X_1^n, X_2^n; G_2^n|Y_e^n) + n\epsilon_2 \quad (38)$$
$$= h(G_2^n|Y_e^n) - h(J_1^n + Z_r^n|Z_e^n + J_1^n + J_2^n) + n\epsilon_2 \quad (39)$$
$$\leq h(G_2^n|Y_e^n) - h(J_1^n + Z_r^n|Z_e^n + J_1^n + J_2^n, J_2^n) + n\epsilon_2 \quad (40)$$
$$= h(G_2^n|Y_e^n) - h(J_1^n + Z_r^n|Z_e^n + J_1^n) + n\epsilon_2. \quad (41)$$

Thus, we can get the following upper bound on the sum rate.

$$R_1^s + R_2^s \leq \max_{\beta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{0.5\beta\log_2(A), (1-\beta)C(P_r)\right\}, \quad (42)$$

where,

$$A = \frac{[(1+O_t)(1+O_t-P_{J2}) - (O_t-P_{J2}+\rho)^2](P_{J1}+1)}{[(1+P_{J1})^2 - (P_{J1}+\rho)^2](1+O_t)}. \quad (43)$$

Next, to derive the upper bounds for the private rates, we consider a genie that provides the jamming signal J_1 to the relay, and we use the secrecy constraint at E and the reliability constraint at D_1. Note that, in deriving the upper bounds for the private rates, we ignore the secrecy constraints on the private messages at D_2, and this action can not decrease the secrecy rates for the private messages. Similar to going from (16) to (27), we have, for the rate of the message W_1^p,

$$H(W_1^p|Y_e^n) \leq h(G_3^n|Y_e^n) - h(J_2^n + Z_r^n|Z_e^n + \sqrt{h_2}X_2^n + J_2^n), \quad (44)$$

where $G_3^n = \sqrt{h_1}X_1^n + J_2^n + Z_r^n$. Let $O_{tp}^k = h_kP_k + P_{J2}$. Thus, we have the following upper bound on R_i^p.

$$R_k^p \leq \max_{\beta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{0.5\beta\log_2(B_k), (1-\beta)C(P_r)\right\}, \quad (45)$$

where,

$$B_k = \frac{[(1+O_t)(1+O_{tp}^k) - (O_{tp}^k+\rho)^2](O_{tp}^j+1)}{[(1+O_{tp}^j)(P_{J2}+1) - (P_{J2}+\rho)^2](1+O_t)}, \quad (46)$$

and $k, j = 1, 2$, $k \neq j$. The upper bound on the private sum rate can be calculated similar to (30)-(41) as

$$H(W_1^p, W_2^p|Y_e^n) \leq h(G_4^n|Y_e^n) - h(J_2^n + Z_r^n|Z_e^n + J_2^n), \quad (47)$$

Thus we have the following upper bound on $R_1^p + R_2^p$

$$R_1^p + R_2^p \leq \max_{\beta\in(0,1]} \min_{-1\leq\rho\leq 1} \min\left\{0.5\beta\log_2(B), (1-\beta)C(P_r)\right\}, \quad (48)$$

where,

$$B = \frac{[(1+O_t)(1+O_t-P_{J1}) - (O_t-P_{J1}+\rho)^2](P_{J2}+1)}{[(1+P_{J2})^2 - (P_{J2}+\rho)^2](1+O_t)}. \quad (49)$$

V. Numerical Results

In this section, we present numerical results and the ensuing insights. First, we observe that when $P_r \to \infty$, $P_{J1} \propto P_1 + P_2$, and P_{J2} is fixed, the private sum rate is an increasing function in the transmitting powers, and there is a gap between the upper bound and the achievable private sum rate as shown in Fig. 3. On the other hand, the upper bound on common sum rate and the achievable common sum rate are decreasing functions in P_{J1}, and the achievable rate goes to zero with the increase in P_{J1}, as shown in Fig. 4.

Next, we observe that for the case where $P_r \to \infty$, and both P_{J1} and P_{J2} are proportional to $P_1 + P_2$ under the condition of $P_{J1} \geq P_{J2}$, the achievable common sum rate and the private sum rate are not monotonically increasing functions in the transmitting powers as shown in Fig. 5 and 6. Also, the gap between the upper bound and the achievable private rates increases with the increase in the transmitting powers.

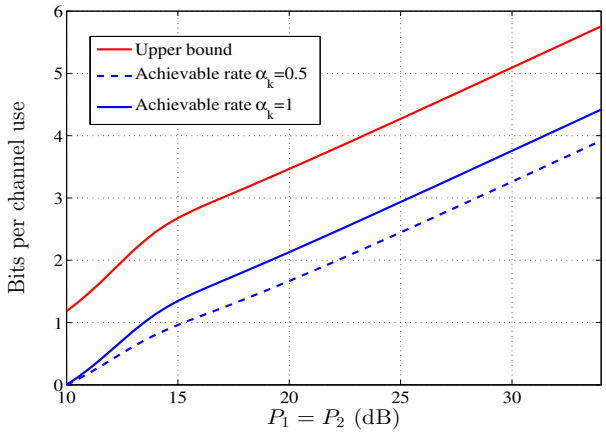

Fig. 3. Private sum rate vs transmit power when $P_r \to \infty$, $P_{J1} = P_1$, $P_{J2} = 10$ dB, $h_1 = h_2 = 1$ and optimal β.

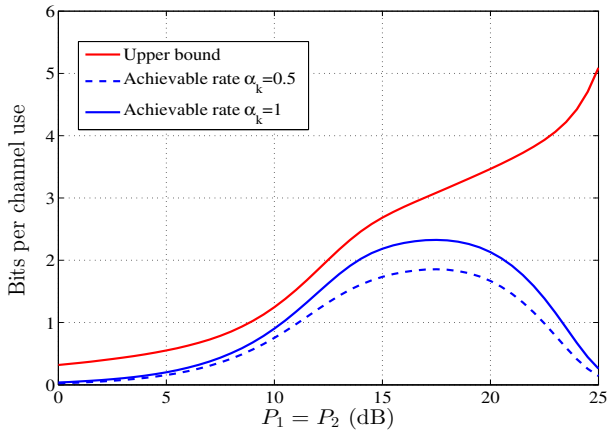

Fig. 5. Private sum rate vs transmit power when $P_r \to \infty$, $P_{J1} = P_1$, $P_{J2} = 0.1P_1$, $h_1 = h_2 = 1$ and optimal β.

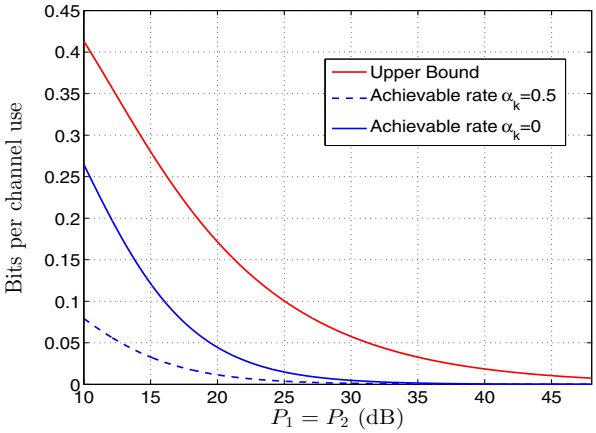

Fig. 4. Common sum rate vs transmit power when $P_r \to \infty$, $P_{J1} = P_1$, $P_{J2} = 10$ dB, $h_1 = h_2 = 1$ and optimal β.

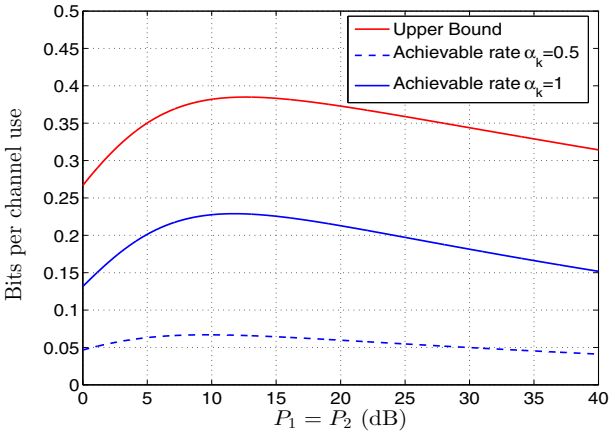

Fig. 6. Common sum rate vs transmit power when $P_r \to \infty$, $P_{J1} = P_1$, $P_{J2} = 0.9P_1$, $h_1 = h_2 = 1$ and optimal β.

For the case where $\bar{P}_r$ is limited, $P_{J1} \propto P_1 + P_2$ and P_{J2} is fixed, the private sum rate is not an increasing function in the transmitting powers as shown in 7. Finally, Fig. 8 demonstrates that we can obtain a positive private sum rate and a positive common sum rate simultaneously if the jamming powers are fixed and limited.

VI. Conclusions

In this paper, we have considered an X-channel, where each source sends two messages, common and private, that should kept secret from the eavesdropper associated with the relay, which is the only means of communication due to the absence of any direct links. Furthermore, the second destination is considered as an eavesdropper for the private messages that should only be decoded by the first destination. We have shown that positive secure communication rates are achievable using random binning at the sources and compress-and-forward at the relay with the help of a cooperative jamming signals from the destinations. Moreover, we have derived an outer bound on the secure rate region.

In this paper, we have considered the model where the destination with higher security clearance is also the node that can expend more power on cooperative jamming as compared to the destination with lower security clearance. We also considered Gaussian noise as the jamming strategy. Removing these assumptions as well as examination of more general models with multiple untrusted relays are interesting future directions.

Acknowledgment

This work was supported by NSF Grants: CCF 09-64362, CCF 13-19338 and CNS 13-14719.

Appendix

Recall that from Remark 1, $Y_k^N = \{J_k^n, Y_k^m\}$. Also, we observe that we have the following Markov chain: $(W_1^p, W_1^s, W_2^p, W_2^s) \to (V_1^n, U_1^n, V_2^n, U_2^n) \to (X_1^n, X_2^n) \to$

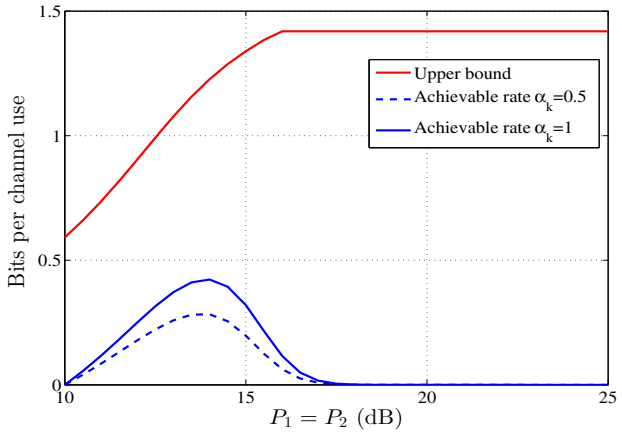

Fig. 7. Private sum rate vs transmit power when $P_r = 17$ dB, $P_{J1} = P_1$, $P_{J2} = 10$ dB, $h_1 = h_2 = 1$ and $\beta = 0.5$.

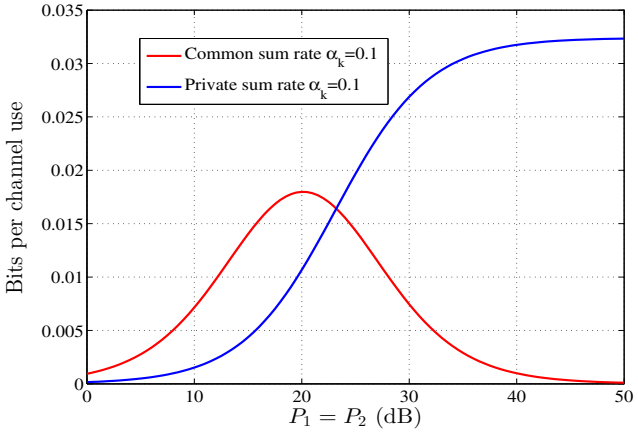

Fig. 8. Private and common sum rates vs transmit power when $P_r = 17$ dB, $P_{J1} = 17$ dB, $P_{J2} = 15$ dB, $h_1 = h_2 = 1$ and $\beta = 0.1$.

$Y_r^n \to \hat{Y}_r^n \to X_r^m \to Y_k^m$. Let $\boldsymbol{U} = \{U_1^n, U_2^n\}$ and $\boldsymbol{V} = \{V_1^n, V_2^n\}$.

A. Achievability

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) [15], and we have to calculate the following terms

$$I(U_1^n; Y_2^m, J_2^n, \hat{Y}_r^{\,n} | U_2^n, X_r^m)$$
$$= I(U_1^n; Y_2^m, \hat{Y}_r^{\,n} | J_2^n, U_2^n, X_r^m) + I(U_1^n; J_2^n | U_2^n, X_r^m) \quad (50)$$
$$= I(U_1^n; Y_2^m, \hat{Y}_r^{\,n} | J_2^n, U_2^n, X_r^m) \quad (51)$$
$$= I(U_1^n; \hat{Y}_r^{\,n} | Y_2^m, J_2^n, U_2^n, X_r^m) + I(U_1^n; Y_2^m | J_2^n, U_2^n, X_r^m) \quad (52)$$
$$= I(U_1^n; \hat{Y}_r^{\,n} | Y_2^m, J_2^n, U_2^n, X_r^m) + I(U_1^n; Z_2^m | J_2^n, U_2^n, X_r^m) \quad (53)$$
$$= I(U_1^n; \hat{Y}_r^{\,n} | Y_2^m, J_2^n, U_2^n, X_r^m) \quad (54)$$
$$= I(U_1^n; Y_r^n + Z_Q^n | Y_2^m, J_2^n, U_2^n, X_r^m) \quad (55)$$
$$= I(U_1^n; \sqrt{h_1} X_1^n + J_1^n + J_2^n + \sqrt{h_2} X_2^n + Z_r^n + Z_Q^n \quad | X_r^m + Z_2^m, J_2^n, U_2^n, X_r^m) \quad (56)$$
$$= I(U_1^n; \sqrt{h_1} X_1^n + J_1^n + \sqrt{h_2} V_2^n + Z_r^n + Z_Q^n) \quad (57)$$
$$= nC\left(\frac{\bar{\alpha}_1 h_1 P_1}{1 + P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right). \quad (58)$$

Similarly, we get

$$I(U_2^n; Y_2^m, J_2^n, \hat{Y}_r^{\,n} | U_1^n, X_r^m)$$
$$= nC\left(\frac{\bar{\alpha}_2 h_2 P_2}{1 + P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right). \quad (59)$$

Next, we calculate

$$I(U_1^n, U_2^n; Y_2^m, J_2^n, \hat{Y}_r^{\,n} | X_r^m)$$
$$= I(U_1^n, U_2^n; Y_2^m, \hat{Y}_r^{\,n} | J_2^n, X_r^m) + I(U_1^n, U_2^n; J_2^n | X_r^m) \quad (60)$$
$$= I(U_1^n, U_2^n; Y_2^m, \hat{Y}_r^{\,n} | J_2^n, X_r^m) \quad (61)$$
$$= I(U_1^n, U_2^n; \hat{Y}_r^{\,n} | Y_2^m, J_2^n, X_r^m) + I(U_1^n, U_2^n; Y_2^m | J_2^n, X_r^m) \quad (62)$$
$$= I(U_1^n, U_2^n; \hat{Y}_r^{\,n} | Y_2^m, J_2^n, X_r^m) + I(U_1^n, U_2^n; Z_2^m | J_2^n, X_r^m) \quad (63)$$
$$= I(U_1^n, U_2^n; \hat{Y}_r^{\,n} | Y_2^m, J_2^n, X_r^m) \quad (64)$$
$$= I(U_1^n, U_2^n; Y_r^n + Z_Q^n | Y_2^m, J_2^n, X_r^m) \quad (65)$$
$$= I(U_1^n, U_2^n; \sqrt{h_1} X_1^n + J_1^n + J_2^n + \sqrt{h_2} X_2^n + Z_r^n + Z_Q^n \quad | X_r^m + Z_2^m, J_2^n, X_r^m) \quad (66)$$
$$= I(U_1^n, U_2^n; \sqrt{h_1} X_1^n + J_1^n + \sqrt{h_2} X_2^n + Z_r^n + Z_Q^n) \quad (67)$$
$$= nC\left(\frac{\bar{\alpha}_1 h_1 P_1 + \bar{\alpha}_2 h_2 P_2}{1 + P_{J1} + \alpha_1 h_1 P_1 + \alpha_2 h_2 P_2 + \sigma_Q^2}\right). \quad (68)$$

Note that since $P_{J1} \geq P_{J2}$, if D_2 is able to decode the common messages, then D_1 is able too. After decoding the common messages, D_1 decodes the private messages, therefore we have to calculate the following terms

$$I(V_1^n; Y_1^m, J_1^n, \hat{Y}_r^{\,n} | \boldsymbol{U}, V_2^n, X_r^m)$$
$$= I(V_1^n; Y_1^m, \hat{Y}_r^{\,n} | J_1^n, \boldsymbol{U}, V_2^n, X_r^m) + I(V_1^n; J_1^n | \boldsymbol{U}, V_2^n, X_r^m) \quad (69)$$
$$= I(V_1^n; Y_1^m, \hat{Y}_r^{\,n} | J_1^n, \boldsymbol{U}, V_2^n, X_r^m) \quad (70)$$
$$= I(V_1^n; \hat{Y}_r^{\,n} | Y_1^m, J_1^n, \boldsymbol{U}, V_2^n, X_r^m) + I(V_1^n; Y_1^m | J_1^n, \boldsymbol{U}, V_2^n, X_r^m) \quad (71)$$
$$= I(V_1^n; \hat{Y}_r^{\,n} | Y_1^m, J_1^n, \boldsymbol{U}, V_2^n, X_r^m) + I(V_1^n; Z_1^m | J_1^n, \boldsymbol{U}, V_2^n, X_r^m) \quad (72)$$
$$= I(V_1^n; \hat{Y}_r^{\,n} | Y_1^m, J_1^n, \boldsymbol{U}, V_2^n, X_r^m) \quad (73)$$
$$= I(V_1^n; Y_r^n + Z_Q^n | Y_1^m, J_1^n, \boldsymbol{U}, V_2^n, X_r^m) \quad (74)$$
$$= I(V_1^n; \sqrt{h_1} X_1^n + J_1^n + J_2^n + \sqrt{h_2} X_2^n + Z_r^n + Z_Q^n$$

$$|X_r^m + Z_2^m, J_1^n, \boldsymbol{U}, V_2^n, X_r^m) \tag{75}$$
$$= I(V_1^n; \sqrt{h_1}V_1^n + J_2^n + Z_r^n + Z_Q^n) \tag{76}$$
$$= nC\left(\frac{\alpha_1 h_1 P_1}{1 + P_{J2} + \sigma_Q^2}\right). \tag{77}$$

Similarly, we get

$$I(V_2^n; Y_1^m, J_1^n, \hat{Y_r}^n|\boldsymbol{U}, V_1^n, X_r^m) = nC\left(\frac{\alpha_2 h_2 P_2}{1 + P_{J2} + \sigma_Q^2}\right). \tag{78}$$

$$I(V_1^n, V_2^n; Y_1^m, J_1^n, \hat{Y_r}^n|\boldsymbol{U}, X_r) = nC\left(\frac{\alpha_1 h_1 P_1 + \alpha_2 h_2 P_2}{1 + P_{J2} + \sigma_Q^2}\right). \tag{79}$$

Next, we calculate

$$I(X_1^n; Y_1^m, J_1^n, \hat{Y_r}^n|X_2^n, X_r^m)$$
$$= I(X_1^n; Y_1^m, \hat{Y_r}^n|J_1^n, X_2^n, X_r^m) + I(X_1^n; J_1^n|X_2^n, X_r^m) \tag{80}$$
$$= I(X_1^n; Y_1^m, \hat{Y_r}^n|J_1^n, X_2^n, X_r^m) \tag{81}$$
$$= I(X_1^n; \hat{Y_r}^n|Y_1^m, J_1^n, X_2^n, X_r^m) + I(X_1^n; Y_1^m|J_1^n, X_2^n, X_r^m) \tag{82}$$
$$= I(X_1^n; \hat{Y_r}^n|Y_1^m, J_1^n, X_2^n, X_r^m) + I(X_1^n; Z_1^m|J_1^n, X_2^n, X_r^m) \tag{83}$$
$$= I(X_1^n; \hat{Y_r}^n|Y_1^m, J_1^n, X_2^n, X_r^m) \tag{84}$$
$$= I(X_1^n; Y_r^n + Z_Q^n|Y_1^m, J_1^n, X_2^n, X_r^m) \tag{85}$$
$$= I(X_1^n; \sqrt{h_1}X_1^n + J_1^n + J_2^n + \sqrt{h_2}X_2^n + Z_r^n + Z_Q^n$$
$$|X_r^m + Z_1^m, J_1^n, X_2^n, X_r^m) \tag{86}$$
$$= I(X_1^n; \sqrt{h_1}X_1^n + Z_r^n + J_2^n + Z_Q^n) \tag{87}$$
$$= nC\left(\frac{h_1 P_1}{1 + P_{J2} + \sigma_Q^2}\right). \tag{88}$$

Similarly, we can get

$$I(X_2^n; Y_1^m, J_1^n, \hat{Y_r}^n|X_1^n, X_r^m) = nC\left(\frac{h_2 P_2}{1 + P_{J1} + \sigma_Q^2}\right), \tag{89}$$

$$I(X_1^n, X_2^n; Y_1^m, J_1^n, \hat{Y_r}^n|X_r^m) = nC\left(\frac{h_1 P_1 + h_2 P_2}{1 + P_{J1} + \sigma_Q^2}\right). \tag{90}$$

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

$$I(X_r^m, Y_2^m, J_2^n) = I(X_r^m, Y_1^m, J_1^n) = mC(P_r). \tag{91}$$

$$I(\hat{Y_r}^n; Y_r^n|X_r^m, Y_2^m, J_2^n)$$
$$= I(Y_r^n + Z_Q^n; Y_r^n|X_r^m, Z_2^n, J_2^n) \tag{92}$$
$$= I(\sqrt{h_1}X_1^n + J_1^n + \sqrt{h_2}X_2^n + Z_r^n + Z_Q^n;$$
$$\sqrt{h_1}X_1^n + J_1^n + \sqrt{h_2}X_2^n + Z_r^n) \tag{93}$$
$$= nC\left(\frac{h_1 P_1 + h_2 P_2 + P_{J1} + 1}{\sigma_Q^2}\right). \tag{94}$$

Similarly, we get

$$I(\hat{Y_r}^n; Y_r^n|X_r^m, Y_1^m, J_1^n) = nC\left(\frac{h_1 P_1 + h_2 P_2 + P_{J2} + 1}{\sigma_Q^2}\right). \tag{95}$$

However, we assume $P_{J1} \geq P_{J2}$, thus we obtain (14).

B. Equivocation Calculations

$$H(W_1^p W_2^p|Y_2^m J_2^n)$$
$$\geq H(W_1^p W_2^p|Y_2^m J_2^n \boldsymbol{U} X_r^m \hat{Y}_r^n) \tag{96}$$
$$= H(W_1^p W_2^p|J_2^n \boldsymbol{U} X_r^m \hat{Y}_r^n) \tag{97}$$
$$= H(W_1^p W_2^p|J_2^n \boldsymbol{U}) - I(W_1^p W_2^p; X_r^m \hat{Y}_r^n|J_2^n \boldsymbol{U}) \tag{98}$$
$$= H(W_1^p W_2^p) - I(W_1^p W_2^p; X_r^m|J_2^n \boldsymbol{U})$$
$$- I(W_1^p W_2^p; \hat{Y}_r^n|X_r^m J_2^n \boldsymbol{U}). \tag{99}$$

However, from (7) the channel inputs are independent

$$I(W_1^p W_2^p; X_r^m|J_2^n \boldsymbol{U}) \leq I(W_1^p W_2^p, X_1^n X_2^n; X_r^m|J_2^n \boldsymbol{U})$$
$$= I(X_1^n X_2^n; X_r^m|J_2^n \boldsymbol{U}) = 0. \tag{100}$$

Then, we have

$$H(W_1^p, W_2^p|Y_2^m J_2^n)$$
$$\geq H(W_1^p, W_2^p) - I(W_1^p W_2^p; \hat{Y}_r^n|X_r^m J_2^n \boldsymbol{U}) \tag{101}$$
$$= H(W_1^p, W_2^p) - I(W_1^p W_2^p; \hat{Y}_r^n|J_2^n \boldsymbol{U}) \tag{102}$$
$$= H(W_1^p, W_2^p) - h(\hat{Y}_r^n|J_2^n \boldsymbol{U})$$
$$+ h(\hat{Y}_r^n|W_1^p W_2^p J_2^n \boldsymbol{U}) + I(W_1^p W_2^p; \hat{Y}_r^n|J_2^n \boldsymbol{U}\boldsymbol{V}) \tag{103}$$
$$= H(W_1^p, W_2^p) - h(\hat{Y}_r^n|J_2^n \boldsymbol{U}) + h(\hat{Y}_r^n|W_1^p W_2^p J_2^n \boldsymbol{U})$$
$$+ h(\hat{Y}_r^n|J_2^n \boldsymbol{U}\boldsymbol{V}) - h(\hat{Y}_r^n|W_1^p W_2^p J_2^n \boldsymbol{U}\boldsymbol{V}) \tag{104}$$
$$= H(W_1^p, W_2^p) - I(\hat{Y}_r^n; \boldsymbol{V}|J_2^n \boldsymbol{U})$$
$$+ I(\hat{Y}_r^n; \boldsymbol{V}|W_1^p W_2^p J_2^n \boldsymbol{U}) \tag{105}$$
$$= H(W_1^p, W_2^p) - I(\hat{Y}_r^n; \boldsymbol{V}|J_2^n \boldsymbol{U})$$
$$+ h(\boldsymbol{V}|W_1^p W_2^p J_2^n \boldsymbol{U}) - h(\boldsymbol{V}|W_1^p W_2^p J_2^n \boldsymbol{U}\hat{Y}_r^n) \tag{106}$$
$$\geq H(W_1^p, W_2^p) - I(\hat{Y}_r^n; \boldsymbol{V}|J_2^n \boldsymbol{U})$$
$$+ h(\boldsymbol{V}|W_1^p W_2^p J_2^n \boldsymbol{U}) - h(\boldsymbol{V}|W_1^p W_2^p J_2^n \boldsymbol{U}\hat{Y}_r^n) \tag{107}$$
$$\geq H(W_1^p, W_2^p) - nC\left(\frac{\alpha_1 h_1 P_1 + \alpha_2 h_2 P_2}{1 + P_{J1} + \sigma_Q^2}\right)$$
$$+ nR_1^{x2} + nR_2^{x2} - n\epsilon_5. \tag{108}$$

Note that with the knowledge of Y_r^n, and the bin index the eavesdropper at the relay is assumed to be able to decode the transmitted codeword. Here, whenever $P_{J2} \geq \sigma_Q^2$, the last term is bounded by Fano's inequality as with the knowledge of $\hat{Y}_r^n$, the 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 higher SNR than the aforementioned case. Also, observe that if $P_{J2} \leq \sigma_Q^2$, the rates of common secure messages will be 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,

$$H(W_1^p|Y_2^m J_2^n) \geq H(W_1^p) - nC\left(\frac{\alpha_1 h_1 P_1}{1+P_{J1}+\alpha_2 h_2 P_2+\sigma_Q^2}\right) + nR_1^{x2} - n\epsilon_6. \quad (109)$$

$$H(W_2^p|Y_2^m J_2^n) \geq H(W_2^p) - nC\left(\frac{\alpha_2 h_2 P_2}{1+P_{J1}+\alpha_1 h_1 P_1+\sigma_Q^2}\right) + nR_2^{x2} - n\epsilon_7. \quad (110)$$

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

$$\begin{aligned}
&H(W_1^s, W_2^s|Y_r^n) \\
&= H(W_1^s, W_2^s) - I(W_1^s W_2^s; Y_r^n) && (111)\\
&= H(W_1^s, W_2^s) - I(W_1^s W_2^s; Y_r^n) + I(W_1^s W_2^s; Y_r^n|\boldsymbol{U}) && (112)\\
&= H(W_1^s, W_2^s) - h(Y_r^n) \\
&\quad + h(Y_r^n|W_1^s W_2^s) + h(Y_r^n|\boldsymbol{U}) + h(Y_r^n|W_1^s W_2^s \boldsymbol{U}) && (113)\\
&= H(W_1^s, W_2^s) - I(\boldsymbol{U}; Y_r^n) + I(\boldsymbol{U}; Y_r^n|W_1^s W_2^s) && (114)\\
&= H(W_1^s, W_2^s) - I(\boldsymbol{U}; Y_r^n) \\
&\quad + h(\boldsymbol{U}|W_1^s W_2^s) - h(\boldsymbol{U}|Y_r^n W_1^s W_2^s) && (115)\\
&= H(W_1^s, W_2^s) + nR_1^{x1} + nR_2^{x1} - n\epsilon_8 \\
&\quad - nC\left(\frac{\bar{\alpha}_1 h_1 P_1 + \bar{\alpha}_2 h_2 P_2}{1+P_{J1}+P_{J2}+\alpha_1 h_1 P_1+\alpha_2 h_2 P_2}\right). && (116)
\end{aligned}$$

Again, similarly, we can get

$$H(W_1^s|Y_r^n) \geq H(W_1^s) + nR_1^{x1} - n\epsilon_9 - nC\left(\frac{\bar{\alpha}_1 h_1 P_1}{1+P_{J1}+P_{J2}+\alpha_1 h_1 P_1+h_2 P_2}\right). \quad (117)$$

$$H(W_2^s|Y_r^n) \geq H(W_2^s) + nR_2^{x1} - n\epsilon_{10} - nC\left(\frac{\bar{\alpha}_2 P_2}{1+P_{J1}+P_{J2}+\alpha_2 h_2 P_2+h_1 P_1}\right). \quad (118)$$

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

$$\begin{aligned}
&H(W_1^s, W_2^s, W_1^p, W_2^p|Y_r^n) \\
&= H(W_1^s, W_2^s, W_1^p, W_2^p) - I(W_1^s W_2^s W_1^p, W_2^p; Y_r^n) && (119)\\
&= H(W_1^s, W_2^s, W_1^p, W_2^p) - I(W_1^s W_2^s W_1^p, W_2^p; Y_r^n) \\
&\quad + I(W_1^s W_2^s W_1^p W_2^p; Y_r^n|\boldsymbol{U}\boldsymbol{V}) && (120)\\
&= H(W_1^s, W_2^s, W_1^p, W_2^p) + h(Y_r^n|W_1^s W_2^s W_1^p W_2^p) \\
&\quad - h(Y_r^n) + h(Y_r^n|\boldsymbol{U}\boldsymbol{V}) + h(Y_r^n|W_1^s W_2^s W_1^p W_2^p \boldsymbol{U}\boldsymbol{V}) && (121)\\
&= H(W_1^s, W_2^s, W_1^p, W_2^p) - I(\boldsymbol{V}\boldsymbol{U}; Y_r^n) \\
&\quad + I(\boldsymbol{V}\boldsymbol{U}; Y_r^n|W_1^s W_2^s W_1^p W_2^p) && (122)\\
&= H(W_1^s, W_2^s, W_1^p, W_2^p) + h(\boldsymbol{V}\boldsymbol{U}|W_1^s W_2^s W_1^p W_2^p) \\
&\quad - I(\boldsymbol{V}\boldsymbol{U}; Y_r^n) - h(\boldsymbol{V}\boldsymbol{U}|Y_r^n W_1^s W_2^s W_1^p W_2^p) && (123)\\
&= H(W_1^s, W_2^s, W_1^p, W_2^p) - nC\left(\frac{h_1 P_1 + h_2 P_2}{1+P_{J1}+P_{J2}}\right) \\
&\quad + nR_1^{x1} + nR_2^{x1} + nR_1^{x2} + nR_2^{x2} - n\epsilon_{11}. && (124)
\end{aligned}$$

By proper choice of the bin sizes, i.e., R_k^{x1} and R_k^{x2}, we get the achievable region stated in Theorem 1.

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

[3] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *2005 Asilomar Conf. on Signals, Systems, and Computers*, Nov. 2005, pp. 1747–1751.

[4] 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.

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

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

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

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

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

[10] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Info. Theory*, vol. 58, no. 5, pp. 2748–2765, 2012.

[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] A. A. Zewail and A. Yener, "The multiple access channel with an untrusted relay," to appear in Proceedings of Information Theory Workshop, ITW'14, Hobart, Tasmania, Australia, Nov. 2014.

[13] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[14] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Info. Theory*, vol. 57, no. 5, pp. 2730–2745, 2011.

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