The Multiple Access Channel with an Untrusted Relay

Ahmed A. Zewail and Aylin Yener

Department of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802

***Abstract*—This paper considers a Gaussian multiple access channel aided by a relay. Specifically, the relay facilitates communication between multiple sources and a destination to which the sources have no direct link. In this set up, the relay node is considered to be untrusted, i.e., honest but curious, from whom the source messages need to be kept secret. We identify an achievable secrecy rate region utilizing cooperative jamming from the destination, and using compress-and-forward at the relay. Additionally, an outer bound on the secrecy rate region is derived. Numerical results indicate that the outer bound is tight in some cases of interest.**

I. Introduction

The broadcast nature of wireless communications enables transmitted signals to be overheard by unauthorized nodes, making the medium vulnerable to eavesdropping attacks. Information theoretic secrecy overcomes this vulnerability and provides absolute confidentiality with transmission and network design strategies. The secrecy capacity of a noisy channel was defined by Wyner [1], where he proved, using stochastic encoding, the possibility of having confidential data transmission in the presence of a wiretapper[1], if the received signal at the wiretapper is a degraded version of the one at the legitimate receiver. This result was extended to general discrete memoryless channels, where the wiretapper observation is not necessarily degraded [2].

The past decade has witnessed a significant effort in information theoretic secrecy research in a variety of network models, offering various design insights into the physical layer, see for example [3]–[13] and many others. Previous work of particular relevance to the problem studied in this paper includes the model where multiple sources securely communicate to a receiver in a Gaussian channel in the presence of an eavesdropper [3]–[5]. For this, the multiple access wiretap channel, it has been shown that *cooperative jamming* where a transmitter sacrifices its own rate, and instead uses its resources to judiciously interfere with the wiretapper, improves the achievable secure sum rate of the system [5].

The impact of confidentiality (secrecy) requirements on cooperative communications has been studied in various references, notably on various channel models where a single legitimate transmitter receiver pair communicates through one or more relay nodes see for example [6], [8]–[11]. In particular, the model where a relay node helping in communication while simultaneously being untrusted with the secret information has been proposed in [10], [13]. A two-hop scenario where the untrusted relay is the only means of communicating between a single source and the destination has been considered in [9].

This paper extends the secure cooperative communications model in [9] to a scenario where multiple sources wish to communicate to a destination through an untrusted relay keeping the messages secret from it. This could be a valid scenario for instance for the uplink of a dynamic small cell whose access point is an unauthenticated router, e.g., a device that forms a hot spot and is willing to relay the signals it receives to a base station. Modeling this set up as a K-user multiple access relay channel with no direct link, where the relay is assumed to be an honest but curious node on which the secrecy constraints must be imposed, we seek to understand the end-to-end secure communication rates. We first define an achievable secure rate region using Gaussian signaling and compress-and-forward at the relay with the aid of the cooperative jamming from the destination. Next, we derive a genie aided outer bound on the secure rate region by adding a new eavesdropper to the network that has the same channel statistics of the relay, after which the relay can be assumed to be trusted. We find that in some scenarios of interest the bound is tight. We also observe that in this set up, it is essential to seek the destination node's help in improving secrecy, as opposed to a source node to serve as a cooperative jammer.

The remainder of the paper is organized as follows. Section II describes the model. Then, an achievable region is provided in Section III, while we develop the outer bound in Section IV. Section V provides the numerical results and the related observations. Section VI summarizes our conclusions.

II. System model

We consider a network consisting of K sources, $\{S_k\}$ $k \in \{1, 2, \ldots, K\}$ that send messages to the destination (D) over an untrusted relay (R) as shown in Fig. 1. All nodes are assumed to operate in half-duplex mode, with communication taking place over two phases. In the first phase, sources transmit their signals $\{X_k\}$ to the relay, and in the second phase, the relay transmits to the destination. The destination is assumed to be willing to participate in communication as a cooperative jammer node in the first phase. More specifically, during the sources' transmission to the relay, the destination

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

[1]The terms "wiretapper" and "eavesdropper" are used interchangeably.

978-1-4799-5999-0/14/$31.00 ©2014 IEEE

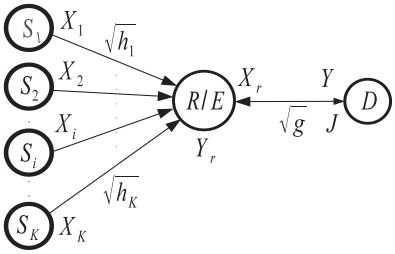

Fig. 1. K-user multiple access channel with untrusted relay.

simultaneously jams the relay with a Gaussian signal (J). The received signal at the relay in channel use i of the first phase is given by

$$Y_r(i) = \sum_{k=1}^{K} \sqrt{h_k} X_k(i) + \sqrt{g} J(i) + Z_r(i) \tag{1}$$

where $\sqrt{h_k}$ is the channel gain from user k to the relay node, and $\sqrt{g}$ represents the channel gain between the relay and the destination. We assume the channel between the relay and the destination to be reciprocal. Z_r is the additive zero mean Gaussian noise with unit variance. The received signal at D at the channel use j of the second phase is expressed as

$$Y(j) = \sqrt{g} X_r(j) + Z(j) \tag{2}$$

where X_r is sent from the relay and Z is the additive zero mean Gaussian noise with unit variance. Define n as the number of channel uses for the first phase, and m as the number of channel uses for the second phase. Let $N = n+m$ be the total number of channel uses. The transmitted signal from each source has to satisfy the average power constraint

$$\frac{1}{N} \sum_{i=1}^{N} E[X_k^2(i)] \leq \bar{P}_k, \quad k \in \{1, 2, \ldots, K\}. \tag{3}$$

The jamming signal from the destination, and the transmitted signal by the relay have the following average power constraints

$$\frac{1}{N} \sum_{i=1}^{N} E[J^2(i)] \leq \bar{P}_J \quad \text{and} \quad \frac{1}{N} \sum_{i=1}^{N} E[X_r^2(i)] \leq \bar{P}_r. \tag{4}$$

Define the time sharing parameter of the first phase, i.e., $\alpha = \frac{n}{n+m}$. Since each node remains silent over one of the two phases, source k, $(k = 1, \cdots, K)$, the destination, and the relay have the following *effective* average powers:

$$P_k = \frac{\bar{P}_k}{\alpha}, \quad P_J = \frac{\bar{P}_J}{\alpha}, \quad P_r = \frac{\bar{P}_r}{1-\alpha}. \tag{5}$$

Remark 1 *Observe that the model is equivalent to the one with an external jammer, which jams the relay in the first phase and is heard by the destination over a noiseless link. Thus, we can consider the received signal at D over the two phases to be* $\boldsymbol{Y} = \{J(1) \cdots J(n), Y(1) \cdots Y(m)\}$.

Each source S_k wishes to communicate secret message (W_k) from the set $\{1, \ldots, M_k^s\}$ to D, while keeping it confidential from the relay, i.e., we have to have

$$\frac{1}{N} H(\boldsymbol{W}_{\mathcal{S}}^s | Y_r^n) \geq \frac{1}{N} H(\boldsymbol{W}_{\mathcal{S}}^s) - \epsilon \qquad \forall \mathcal{S} \tag{6}$$

where $\mathcal{S} \subseteq \mathcal{K}$, $\mathcal{K} \triangleq \{1, 2, \ldots, K\}$ is the set that contains all source nodes and $\boldsymbol{W}_{\mathcal{S}}^s \triangleq \{W_k, k = 1, \cdots, K, \exists k \in \mathcal{S}\}$. Source S_k encodes the messages into $\{X_k^n(W_k)\}$ using $(2^{nR_k}, n)$ codebook, where $R_k = \frac{1}{n} \log_2 M_k^s$. In the remainder of this paper, $H(X)$ and $h(X)$ represent the entropy and the differential entropy of the random variable X, respectively. Also, we use $C(x) \triangleq 0.5 \log_2(1+x)$, $[x]^+ = \max(0, x)$ and $\boldsymbol{X}_{\mathcal{S}} \triangleq \{X_k, k = 1, \cdots, K, \exists k \in \mathcal{S}\}$. We omit the channel use index whenever it is clear from the context.

III. Achievable secure rate region

The key elements of our achievability scheme are random binning at the sources [12] and compress-and-forward at the relay [9]. The achievable scheme is described as follows.

1) At the sources: Define $R_k^x = \frac{1}{n} \log_2 M_k^x$ and $M_k = M_k^x M_k^s$. The source S_k generates M_k codewords. The components of each of them are drawn randomly from $\mathcal{N}(0, P_k - \delta_k)$, where δ_k is an arbitrary positive number to ensure that the power constraint is satisfied. Then, S_k randomly distributes them to M_k^s bins, each of which is indexed by W_k and contains M_k^x codewords. To transmit a message W_k, the source S_k uniformly picks a codeword from the bin indexed by W_k, and transmits the signal X_k.

2) At the relay: The relay compresses the received signal Y_r into a quantized version $\hat{Y}_r$ and transmits the corresponding signal X_r. The eavesdropper, associated with the relay, receives the source signals through a multiple access channel [4], [5]. It follows from [4], [5], [10], [14] and [15] that the following region is achievable

$$\sum_{k \in \mathcal{S}} (R_k^s + R_k^x) \leq I(\boldsymbol{X}_{\mathcal{S}}; Y, \hat{Y}_r | X_r, \boldsymbol{X}_{\mathcal{S}^c}) \tag{7}$$

$$\sum_{k \in \mathcal{S}} R_k^s \leq [I(\boldsymbol{X}_{\mathcal{S}}; Y, \hat{Y}_r | X_r, \boldsymbol{X}_{\mathcal{S}^c}) - I(\boldsymbol{X}_{\mathcal{S}}; Y_r | X_r)]^+ \tag{8}$$

$$I(X_r; Y) \geq I(Y_r; \hat{Y}_r | X_r, Y). \tag{9}$$

More details for the compress-and-forward scheme and the decoding at D can be found in [10], [14] and [15].

By evaluating the above secrecy rate region for the Gaussian case, we get the following theorem.

Theorem 1 *The rate region that satisfies the following inequalities is achievable for all* $\mathcal{S} \subseteq \mathcal{K}$, $\mathcal{K} \triangleq \{1, \ldots, K\}$

$$\sum_{k \in \mathcal{S}} (R_k^s + R_k^x) \leq \alpha C \left(\frac{\sum_{k \in \mathcal{S}} h_k P_k}{1 + \sigma_Q^2} \right) \tag{10}$$

$$\sum_{k \in \mathcal{S}} R_k^s \leq \alpha \left[C \left(\frac{\sum_{k \in \mathcal{S}} h_k P_k}{1 + \sigma_Q^2} \right) - C \left(\frac{\sum_{k \in \mathcal{S}} h_k P_k}{1 + g P_J + \sum_{j \in \mathcal{S}^c} h_j P_j} \right) \right]^+ \tag{11}$$

where $0 < \alpha \leq 1$ *and* $\forall \alpha$, σ_Q^2 *satisfies*

$$\alpha C\left(\frac{1+\sum_{k=1}^{K} h_k P_k}{\sigma_Q^2}\right) = (1-\alpha) C\left(g P_r\right). \quad (12)$$

The proof can be found in the appendix.

Remark 2 *It can be seen from Theorem 1 that the achievable rates are proportional to the time sharing factor* α*. Thus, the relay should always transmit with its maximum power. However, it can be readily observed that if* $\sum_k^K h_k P_k \to 0$*, or* ∞*, then the secure sum rate will diminish. Thus, the rate is not monotonically increasing in the total source power,* $\sum_k^K h_k P_k$*. This implies that for a fixed jamming power, we have to find the optimum value* P_T^* *for* $\sum_k^K h_k P_k$*, which may require some users to transmit with less than their maximum power. We will support this remark with numerical results in Section V.*

Remark 3 *It is worth mentioning that if* $P_r \to \infty$*, the optimal* $\alpha = 1$ *and* $\sigma_Q^2 = 0$*. Hence, we have the following region:*

$$\sum_{k\in\mathcal{S}} (R_k^s + R_k^x) \leq C\left(\sum_{k\in\mathcal{S}} h_k P_k\right) \quad (13)$$

$$\sum_{k\in\mathcal{S}} R_k^s \leq \left[C\left(\sum_{k\in\mathcal{S}} h_k P_k\right) - C\left(\frac{\sum_{k\in\mathcal{S}} h_k P_k}{1+gP_J+\sum_{j\in\mathcal{S}^c} h_j P_j}\right)\right]^+. \quad (14)$$

Remark 4 *There is no need for cooperative jamming from the source nodes to maximize the achievable secure sum rate. To prove this, consider the case where each user can divide its signal into two parts:* X_k *with power* $a_k \bar{P}_k$ *for the data message and* J_k *with power* $(1-a_k)\bar{P}_k$ *for a random jamming signal to confuse the relay and* $a_k \in [0,1]$*. Then, we have*

$$\sum_{k=1}^{K} R_k^{sCJ} \leq \frac{\alpha}{2}\log_2\left(\frac{1+\sigma_Q^2+\sum_{k=1}^{K} h_k P_k}{1+gP_J+\sum_{k=1}^{K} h_k P_k}\cdot \frac{1+gP_J+\sum_{k=1}^{K}(1-a_k)h_k P_k}{1+\sigma_Q^2+\sum_{k=1}^{K}(1-a_k)h_k P_k}\right). \quad (15)$$

Also, (11) can be expressed as

$$\sum_{k=1}^{K} R_k^s \leq \frac{\alpha}{2}\log_2\left(\frac{1+\sigma_Q^2+\sum_{k=1}^{K} h_k P_k}{1+gP_J+\sum_{k=1}^{K} h_k P_k}\cdot\frac{1+gP_J}{1+\sigma_Q^2}\right). \quad (16)$$

It is clear that the difference between (15) and (16) is in the second fraction in the $\log_2$ *function. We can conclude that as long as* $1+gP_J \geq 1+\sigma_Q^2$ *the sum rate in (16) is higher than the one in (15). Observe that this is also the condition for the achievable secure sum rate to be positive.*

IV. Outer bound on the secure rate region

In this section, we derive an outer bound on the secure rate region. We use the relay/eavesdropper separation technique presented in [9]. First, we add an external eavesdropper to our network, which has the same channel statistics as the relay. The received signal at this external eavesdropper is given by

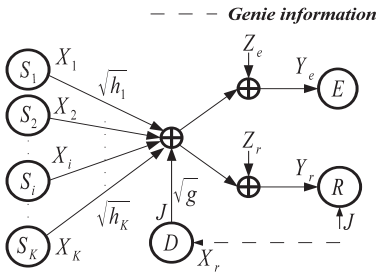

Fig. 2. An equivalent network used to calculate the outer bound.

$$Y_e = \sum_{k=1}^{K} \sqrt{h_k} X_k + \sqrt{g} J + Z_e \quad (17)$$

where Z_e is zero mean Gaussian noise with unit variance and it is correlated with Z_r with a coefficient ρ.

Second, we remove the eavesdropper at the relay, i.e., consider the relay to be trusted, and assume a genie transfers the jamming signal J from the destination D to the relay. Moreover, we assume a genie provides X_r to the destination. In other words, we consider the destination to have X_r, as shown in Fig. 2. Note that none of the assumptions above reduce the secrecy rate region of the model. Observe that we have $p(\boldsymbol{W}_k, Y_e^n) = p(\boldsymbol{W}_k, Y_r^n)$. Thus if we guarantee the secrecy of messages at this additional eavesdropper, they are kept secret at the relay in the original model.

$$\begin{aligned}
&H(\boldsymbol{W}_{\boldsymbol{S}}^s|Y_e^n)\\
&\leq H(\boldsymbol{W}_{\boldsymbol{S}}^s|Y_e^n) - H(\boldsymbol{W}_{\boldsymbol{S}}^s|\boldsymbol{X}_{\mathcal{S}^c}^n X_r^m Y^m J^n) + n\epsilon_1 && (18)\\
&= H(\boldsymbol{W}_{\boldsymbol{S}}^s|Y_e^n) - H(\boldsymbol{W}_{\boldsymbol{S}}^s|\boldsymbol{X}_{\mathcal{S}^c}^n X_r^m J^n) + n\epsilon_1 && (19)\\
&\leq H(\boldsymbol{W}_{\boldsymbol{S}}^s|Y_e^n) - H(\boldsymbol{W}_{\boldsymbol{S}}^s|\boldsymbol{X}_{\mathcal{S}^c}^n Y_r^n X_r^m J^n) + n\epsilon_1 && (20)\\
&= H(\boldsymbol{W}_{\boldsymbol{S}}^s|Y_e^n) - H(\boldsymbol{W}_{\boldsymbol{S}}^s|\boldsymbol{X}_{\mathcal{S}^c}^n Y_r^n J^n) + n\epsilon_1 && (21)\\
&= H(\boldsymbol{W}_{\boldsymbol{S}}^s|Y_e^n) - H(\boldsymbol{W}_{\boldsymbol{S}}^s|\sum_{k\in\mathcal{S}}\sqrt{h_k}X_k^n + Z_r^n) + n\epsilon_1 && (22)\\
&\leq H(\boldsymbol{W}_{\boldsymbol{S}}^s|Y_e^n) - H(\boldsymbol{W}_{\boldsymbol{S}}^s|\sum_{k\in\mathcal{S}}\sqrt{h_k}X_k^n + Z_r^n, Y_e^n) + n\epsilon_1. && (23)
\end{aligned}$$

Equation (18) follows from Fano's inequality. Since, X_r^m is given to the destination, Y^m can be removed as is done in (19). (18)-(21) follow since J^n is provided to the relay. Let $G^n = \sum_{k\in\mathcal{S}}\sqrt{h_k}X_k^n + Z_r^n$. We have

$$\begin{aligned}
&I(\boldsymbol{W}_{\boldsymbol{S}}^s; G^n|Y_e^n)\\
&\leq I(\boldsymbol{W}_{\boldsymbol{S}}^s, \boldsymbol{X}_{\mathcal{S}}^n; G^n|Y_e^n) && (24)\\
&= I(\boldsymbol{X}_{\mathcal{S}}^n; G^n|Y_e^n) && (25)\\
&= h(G^n|Y_e^n) - h(G^n|Y_e^n, \boldsymbol{X}_{\mathcal{S}}^n) && (26)\\
&= h(G^n|Y_e^n) - h(Z_r^n|\sum_{k\in\mathcal{S}^c}\sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_e^n) && (27)\\
&\leq h(G^n|Y_e^n) - h(Z_r^n|\sum_{k\in\mathcal{S}^c}\sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_e^n, J^n) && (28)\\
&= h(G^n|Y_e^n) - h(Z_r^n|\sum_{k\in\mathcal{S}^c}\sqrt{h_k}X_k^n + Z_e^n). && (29)
\end{aligned}$$

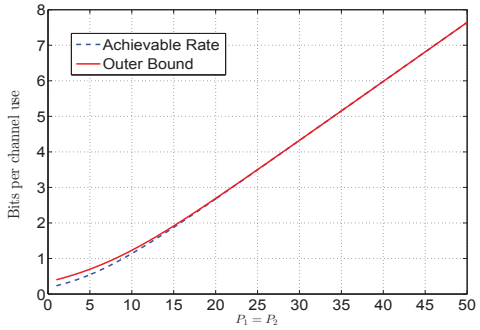

Fig. 3. The secure sum rate vs the transmitted power when $P_r \to \infty$, $P_J = 0.5P_1$, $h_1 = h_2 = 1$ and optimal α.

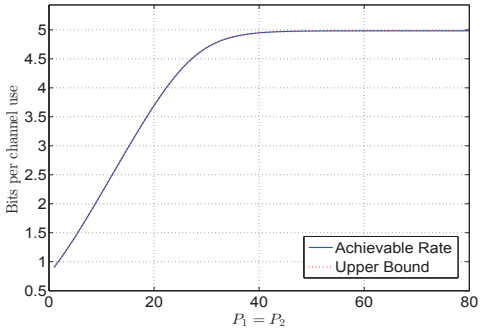

Fig. 4. The secure sum rate vs the transmitted power when $P_r \to \infty$, $P_J = 30$ dB, $h_1 = h_2 = 1$ and optimal α.

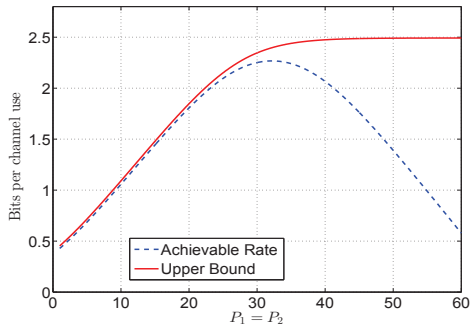

Fig. 5. The secure sum rate vs the transmitted power when $\bar{P}_r = 40$ dB and $\bar{P}_J = 30$ dB, $h_1 = h_2 = 1$ and optimal α.

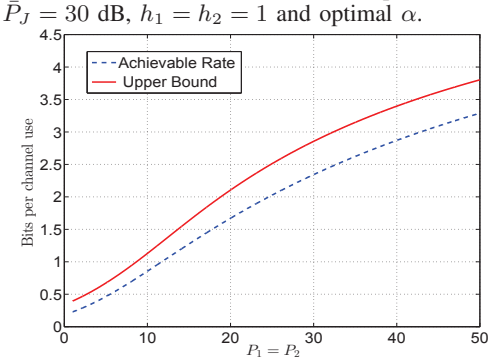

Fig. 6. The secure sum rate vs the transmitted power when $\bar{P}_r = 40$ dB and $\bar{P}_J = 0.5\bar{P}_1$, $h_1 = h_2 = 1$ and optimal α.

(25) results from the fact that $\boldsymbol{W}_{\mathcal{S}}^s$ is determined from $\boldsymbol{X}_{\mathcal{S}}^n$. Now, (29) is maximized when the channel inputs X_k^n's and J^n are i.i.d. Gaussian sequences. Next, we tighten this upper bound by minimizing it over the correlation coefficient of Z_r and Z_e ρ. We can state the following theorem.

Theorem 2 *The secure rate region of is upper bounded by (30).*

$$\sum_{k\in\mathcal{S}} R_k^s \leq \max_{0<\alpha<1} \min_{-1\leq\rho\leq 1} f(\alpha,\rho) \tag{30}$$

where

$$f(\alpha,\rho) = \min\left(\frac{\alpha}{2}\log_2(V), (1-\alpha)C\left(gP_r\right)\right) \tag{31}$$

and

$$V = \frac{[(1+\boldsymbol{P}_s)(1+\boldsymbol{P}_t) - (\boldsymbol{P}_s+\rho)^2](\sum_{k\in\mathcal{S}^c} h_k P_k + 1)}{[(1+\sum_{k\in\mathcal{S}^c} h_k P_k) - \rho^2](1+\boldsymbol{P}_t)} \tag{32}$$

with $\boldsymbol{P}_t = \sum_{k=1}^K h_k P_k + gP_J$ *and* $\boldsymbol{P}_s = \sum_{k\in\mathcal{S}} h_k P_k$.

Remark 5 *For $K = 1$, the analysis above reduces to that of a single source single destination two-hop network [9].*

V. Numerical Results

In this section, we present numerical results to illustrate the performance of the proposed achievable scheme. We consider a network with two sources, i.e., $K = 2$, and focus on the secure sum rate.

In Fig.s 3 and 4, we consider the case where $P_r \to \infty$. If the jamming power P_J is proportional to P_1+P_2, we observe that the secure sum rate is an increasing function in the transmitting powers, and it approaches ∞ as $P_1+P_2 \to \infty$, as illustrated in Fig. 3. Furthermore, the gap between the upper bound and the achievable secure sum rate converges to zero, as the transmit powers increase.

On the other hand, if we fix the jamming power P_J when $P_r \to \infty$, we observe that the secure sum rate increases with the transmit powers but is bounded, as shown in Fig. 4. From Fig.s 3 and 4, we can conclude that the upper bound on the secure sum rate is tight when $P_r \to \infty$.

In Fig.s 5 and 6, we consider the case where the relay power is limited. It is evident that the achievable secure sum rate is not an increasing function of the transmit powers when the jamming power is fixed as shown in Fig. 5. The source powers need to be chosen so as to yield the maximum of the sum rate curve. Fig. 6 shows the case where the jamming power is proportional to the sum of the source powers, we can observe that in the high power region the upper bound is not tight.

VI. Conclusion

We have considered a K-user multiple access relay channel with no direct link between the sources and the destination. The relay is considered to be honest but curious and needs to be treated as an eavesdropper. We have shown that positive secure communication rates are achievable for all sources using

cooperative random binning at the sources and compress-and-forward at the relay with the help of a cooperative jamming from the destination. We have found that the relay and the destination should operate with maximum power while the transmitted powers from the sources need to be optimized. Additionally, we have found an outer bound on the secure rate region. Future directions include considering untrusted relays in multicast transmission to multiple (untrusted) destinations. Recent partial results in this direction can be found in [16].

APPENDIX

Recall that $\boldsymbol{Y} = \{J(1)\cdots J(n), Y(1)\cdots Y(m)\}$. As in [9], the input distributions are such that

$$p(X_1^n,\ldots,X_K^n,J^n,X_r^m) = p(X_1^n)\ldots p(X_K^n)p(J^n)p(X_r^m). \quad (33)$$

We calculate the terms in (7)-(9) as follows.

$$\begin{aligned} &I(\boldsymbol{X}_{\boldsymbol{\mathcal{S}}}^n; \sum_{k=1}^K \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n | X_r^m, \boldsymbol{X}_{\boldsymbol{\mathcal{S}}^c}^n) \\ &= I(\boldsymbol{X}_{\boldsymbol{\mathcal{S}}}^n; \sum_{k\in\mathcal{S}} \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n | X_r^m) \quad (34) \\ &= I(\boldsymbol{X}_{\boldsymbol{\mathcal{S}}}^n; \sum_{k\in\mathcal{S}} \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n) = nC\left(\frac{\sum_{k\in\mathcal{S}} h_kP_k}{1+gP_J}\right) \quad (35) \end{aligned}$$

Next,

$$\begin{aligned} &I(\boldsymbol{X}_{\mathcal{S}}^n; J^n, Y^m, \hat{Y_r}^n | X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; Y^m, \hat{Y_r}^n | X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) + I(\boldsymbol{X}_{\mathcal{S}}^n; J^n | X_r^m, \boldsymbol{X}_{\mathcal{S}^c}) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; Y^m, \hat{Y_r}^n | X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) \quad (36) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; \hat{Y_r}^n | Y^m, X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) + I(\boldsymbol{X}_{\mathcal{S}}^n; Y^m | X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; \hat{Y_r}^n | Y^m, X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) + I(\boldsymbol{X}_{\mathcal{S}}^n; Z^m | X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; \hat{Y_r}^n | Y^m, X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) \quad (37) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; Y_r^n + Z_Q^n | Y^m, X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) \quad (38) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; \sum_{k=1}^K \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n + Z_Q^n | X_r^m, \boldsymbol{X}_{\mathcal{S}^c}^n, J^n) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; \sum_{k\in\mathcal{S}} \sqrt{h_k}X_k^n + Z_r^n + Z_Q^n) = nC\left(\frac{\sum_{k\in\mathcal{S}} h_kP_k}{1+\sigma_Q^2}\right). \quad (39) \end{aligned}$$

Next, we have

$$\begin{aligned} &I(\boldsymbol{X}_{\mathcal{S}}^n; Y_r^n | X_r^m) = I(\boldsymbol{X}_{\mathcal{S}}^n; \sum_{k=1}^K \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n | X_r^m) \\ &= I(\boldsymbol{X}_{\mathcal{S}}^n; \sum_{k=1}^K \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n) \quad (40) \\ &= nC\left(\frac{\sum_{k\in\mathcal{S}} h_kP_k}{1+gP_J+\sum_{j\in\mathcal{S}^c} h_jP_j}\right). \quad (41) \end{aligned}$$

Then, we have

$$\begin{aligned} I(X_r^m; Y^m, J^n) &= I(X_r^m; \sqrt{g}X_r^m + Z^m, J^n) \\ &= I(X_r^m; \sqrt{g}X_r^m + Z^m) = mC\left(gP_r\right). \quad (42) \end{aligned}$$

Finally, we have

$$\begin{aligned} &I(Y_r^n; \hat{Y_r}^n | X_r^m, Y^m, J^n) \\ &= I(\sum_{k=1}^K \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n; \\ &\quad \sum_{k=1}^K \sqrt{h_k}X_k^n + \sqrt{g}J^n + Z_r^n + Z_Q^n | X_r^m, Y^m, J^n) \\ &= I(\sum_{k=1}^K \sqrt{h_k}X_k^n + Z_r^n; \sum_{k=1}^K \sqrt{h_k}X_k^n + Z_r^n + Z_Q^n) \quad (43) \\ &= nC\left(\frac{1+\sum_{k=1}^K h_kP_k}{\sigma_Q^2}\right). \quad (44) \end{aligned}$$

Equations (35), (36), (37), (39), (40) and (43) follow from the condition of independence on the channel inputs in (33) and the noise signals, while (35), (39), (41), (42) and (44) result from considering i.i.d. Gaussian signals.

Substituting these quantities in (7)-(9), and dividing both sides by $n+m=N$ an taking the limit as $N\to\infty$, we get the achievable region stated in Theorem 1.

REFERENCES

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

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–3487, 1978.

[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 Gaussian multiple access wire-tap channel," *IEEE Trans. Info. Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[5] ——, "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.

[6] 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.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel," *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

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

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

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

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

[12] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Info. Theory*, vol. 57, no. 9, pp. 5682–5694, 2011.

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

[14] 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.

[15] T. M. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Info. Theory*, vol. 25, no. 9, pp. 572–584, September 1979.

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