Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2009, Article ID 305146, 13 pages
doi:10.1155/2009/305146

Research Article

Two-Hop Secure Communication Using an Untrusted Relay

Xiang He and Aylin Yener

Wireless Communications and Networking Laboratory, Electrical Engineering Department, The Pennsylvania State University, University Park, PA 16802, USA

Correspondence should be addressed to Aylin Yener, yener@engr.psu.edu

Received 4 December 2008; Revised 8 August 2009; Accepted 8 October 2009

Recommended by Hesham El-Gamal

We consider a source-destination pair that can only communicate through an *untrusted* intermediate relay node. The intermediate node is willing to employ a designated relaying scheme to facilitate reliable communication between the source and the destination. Yet, the information it relays needs to be kept secret from it. In this two-hop communication scenario, where the use of the untrusted relay node is essential, we find that a positive secrecy rate is achievable. The center piece of the achievability scheme is the help provided by either the destination node with transmission capability, or an external "good samaritan" node. In either case, the helper performs cooperative jamming that confuses the eavesdropping relay and disables it from being able to decipher what it is relaying. We next derive an upper bound on the secrecy rate for this system. We observe that the gap between the upper bound and the achievable rate vanishes as the power of the relay node goes to infinity. Overall, the paper presents a case for intentional interference, that is, cooperative jamming, as an enabler for secure communication.

1. Introduction

Information theoretic security was proposed by Shannon [1]. The idea of measuring secrecy using mutual information lends itself naturally to the investigation of how the channel can influence secrecy and further to the characterization of the fundamental limit of secure transmission rate. Wyner, in [2], defined the wiretap channel, and showed that secure communication from a transmitter to a "legitimate" receiver is possible when the signal received by the wiretapper (eavesdropper) is degraded with respect to that received by the legitimate receiver. Reference [3] identified the *secrecy capacity* of the general discrete memoryless wiretap channel. The secrecy capacity of the Gaussian wiretap channel is found in [4].

Recent progress in this area has extended classical information theory channel models to include secrecy constraints. Examples are the multiple access channel, the broadcast channel, the two-way channel, the three-node relay channel and the two-user interference channel [5–13]. These studies are beginning to lead to insights for designing secure wireless communication systems from the physical layer up. Prominent such examples include using multiple antennas to steer the transmitted signal away from an eavesdropper [14–16], transmitting with the intention of jamming the eavesdropper [8, 10, 17], and taking advantage of variations in channel state to provide secrecy [18–20].

The focus of this work is on a class of relay networks where the source and the destination have no direct link and thus can only communicate utilizing an intermediate relay node. This models the practical scenario where direct communication between the source and the destination is too "expensive" in terms of power consumption: direct communication may be used to send some very low rate control packages, for example to initialize the communication, but it is infeasible to sustain a nontrivial reliable communication rate due to the power constraint.

In such a scenario, the source-destination pair *needs* the relay to communicate. On the other hand, more often than not, this relay node may be "untrusted" [11]. This does not mean the relay node is malicious, in fact quite the opposite, it may be part of the network and we will assume that it is willing to faithfully carry out the designated relaying scheme. The relay simply has a lower security clearance in the network and hence is not trusted with the confidential message it is relaying. Equivalently, we can assume the confidential

message is one used for identification of the source node for authentication, which should never be revealed to a relay node in order not to be vulnerable to an impersonation attack. In all these cases, we must assume there is an eavesdropper colocated at the relay node when designing the system.

The "untrusted" relay model, or the eavesdropper being colocated with the relay node, was first studied in [9] for the general relay channel, with a rather pessimistic outlook, finding that for the degraded or the reversely degraded relay channel the relay node should not be deployed. More optimistic results for the relay channel with a colocated eavesdropper have been identified recently in [11, 21, 22]. Specifically, it has been shown that the cooperation from the relay may, in fact, be essential to achieving nonzero secrecy rate [11, 21]. The model is later extended to the more symmetric case in [23, 24] where the relay also has a confidential message of its own, which must be kept secret from the destination.

All these models assume that a direct link between the source and the destination is present including our previous work [11]. In contrast, when there is no direct link, it is impossible for this network to convey a confidential message from the source to the destination while keeping it secret from the relay [9]. This is because the destination can only receive signals from the relay resulting in a physically degraded relay channel [25]. Therefore, the relay knows everything the destination knows regarding the confidential message, and the secrecy capacity is zero.

The differentiating feature of the model studied in this work from those described above including [11] is that the destination has transmission capability. This opens the possibility of the destination node to actively participate in ensuring the secrecy of the information it wants to obtain. In an effort to address a practical two-hop communication scenario, we shall consider each node to be half-duplex, which leads to a two-phase communication model. In addition, feedback to the source is not considered in the channel model. Interestingly, in this model, the transmission capability of the destination proves to be the *enabler* of secure communication. By recruiting the help of the destination to do "cooperative jamming", positive secrecy rate can be achieved that would not have been possible otherwise. We also remark that in case the transmission by the destination is not possible or desired, the help from an external cooperative jammer will do as well.

The idea of using a helpful jammer goes back to [17, 26, 27] and has since been used in many different models. Besides the multiple access, two-way [8] and relay wiretap channels [10], other recent results that use "cooperative jamming" as the part of the achievability scheme, include [28–30]. In [28], a separate jammer is added to the classical Gaussian wiretap channel model. The jamming signal is revealed to the legitimate receiver via a wired link so that an advantage over the eavesdropper is gained. Reference [30] does not assume the wired connection, and employs a scheme tantamount to the two user multiple access channel with an external eavesdropper where one of the users perform cooperative jamming. Reference [29] considers the case where both the eavesdropper and the legitimate receiver observes a modulus Λ channel and the destination carries out the jamming. We note that all these works deal with an external eavesdropper, in contrast to the focus of this work, which is an untrusted (but legitimate) node in the network.

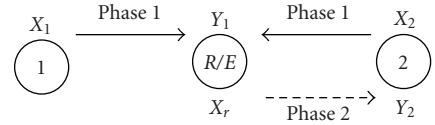

Figure 1: Two-hop communication using an untrusted relay.

In general, the optimality of recruiting a helpful jammer remains open as the converse results are limited. For the Gaussian case, the main difficulty is to find a upper bound for which the optimal input distribution can be found and evaluated. Doing so usually involves the introduction of genie information, as in the converse for the Gaussian wiretap channel [4], MIMO wiretap channel [14] and MAC wiretap channel [31]. The proofs then typically invoke the entropy power inequality, as in [4], or the generalized entropy power inequality, as in [32].

In this work, we derive a computable upper bound for the model in consideration by first introducing a second eavesdropper, an approach first used for a three-node relay channel in [11]. Next, after several steps of genie arguments, the channel is transformed into a wiretap channel with a helpful jammer, whose outer bound is then evaluated. The resulting bound is nontrivial in the sense that it is strictly tighter than the bound for the same channel without secrecy constraints. We also prove that it is tighter than an upper bound derived using the generalized entropy power inequality following a similar approach to [32], when the maximum sum received SNR at the relay is greater than 0 dB. We show that the gap between the bound and the achievable rates converges to zero when the power of the relay goes to infinity.

The paper is organized as follows. Section 2 presents the channel model and the two-phase protocol that utilizes cooperative jamming. In Section 3, we derive the achievable rates. Section 4 presents our upper bound and compares with other known upper bounds. Section 5 presents the numerical results. Finally, Section 6 presents the conclusion.

The following notation is used throughout this work: We use H to denote the entropy, h to denote the differential entropy, and ε_k to denote any variable that goes to 0 when n goes to ∞. We define $C(x) = (1/2)\log_2(1+x)$.

2. Channel Model

The system model is shown in Figure 1. We assume all nodes are half-duplex and the communication alternates between two phases, called phase one and phase two respectively. During phase one, shown with solid lines in Figure 1, the source transmits signal X_1. At the same time, the destination node transmits jamming signal X_2 in order to confuse the

relay node. The signal received by the relay in phase one, Y_1, is given by

$$Y_1 = X_1 + X_2 + Z_1, \tag{1}$$

where Z_1 is a zero mean Gaussian random variable with unit variance. In an effort to reflect on the design of a practical system, we assume that the computation of X_i, $i = 1, 2$ does not rely on the signals received by node i in the past.

In phase two, shown with dashed lines, the relay transmits signal X_r, which is computed from the local randomness at the relay, the signal transmitted and received by the relay in the past.

The signal received by the destination in phase two is denoted by Y_2, which is given below:

$$Y_2 = X_r + Z_2, \tag{2}$$

where Z_2 is a zero mean Gaussian random variable with unit variance.

The channel alternates between these two phases according to a random or deterministic schedule, which is generated by a global controller independently from the signals associated with the channel model. Hence here the term "schedule" is simply a finite number of channel uses which are either marked as phase one or phase two. We use n to denote the number of channel uses marked as phase one, and m to denote the number of channel uses marked as phase two. It should be noted that in general the n channel uses of phase one are not consecutive. Neither are the m channel uses of phase two. We assume the schedule is stable, in the sense that the following limit exists:

$$\alpha = \lim_{n+m\to\infty} \frac{n}{m+n}. \tag{3}$$

For a given α, we use $\{T(\alpha)\}$ to denote a sequence of schedules with increasing number of channel uses $n+m$ such that (3) holds. According to this definition, α becomes the limit of the time sharing factor of phase one in the schedule $T(\alpha)$ as $n+m \to \infty$.

When transmitting signals, the source, the destination, and the relay must satisfy certain power constraints. The average power constraints for the source, the jammer and the relay can be expressed as follows:

$$\frac{1}{N}\sum_{k=1}^{N} E\left[X_{i,k}^2\right] \le \overline{P}_i, \quad i = 1, 2, \tag{4}$$

$$\frac{1}{N}\sum_{k=1}^{N} E\left[X_{r,k}^2\right] \le \overline{P}_r, \tag{5}$$

where

$$N = n + m \tag{6}$$

is the total number of channel uses.

For the purpose of completeness, we also introduce the notation P_i, $i = 1, 2$ to denote the average power of node i during phase one. Since node 1 and 2 are only transmitting during phase one, P_i and $\overline{P}_i$ are related as

$$P_i = \frac{\overline{P}_i}{\alpha}, \quad i = 1, 2. \tag{7}$$

Similarly, we use P_r to denote the average power of the relay node during phase two. Since the relay node only transmits during the second phase, P_r is related to $\overline{P}_r$ as follows:

$$P_r = \frac{\overline{P}_r}{1-\alpha}. \tag{8}$$

After a number of phases, the destination node (node 2) decodes a message $\widehat{W}$ from the signals it transmitted during the periods of phase one and the signals it received during the periods of phase two. For reliable communication, $\widehat{W}$ should equal the message W from the source node with high probability. Hence we have the following requirement:

$$\lim_{n+m\to\infty} \Pr\left(W \ne \widehat{W}\right) = 0. \tag{9}$$

The message W must also be kept secret from the eavesdropper at the relay node, who can infer the value of W based on the following knowledges available to it.

(1) The local randomness at the relay, denoted by A.

(2) The n signals the relay transmitted during the periods of phase one, denoted by Y_1^n.

(3) The m signals the relay transmitted during the periods of phase two, denoted by X_r^m.

The information on W that the eavesdropper can extract from these knowledges should be limited. Hence we have the following secrecy constraint:

$$\begin{aligned}&\lim_{n+m\to\infty} \frac{1}{n+m} H(W)\\ &\quad = \lim_{n+m\to\infty} \frac{1}{n+m} H(W \mid X_r^m, Y_1^n, A).\end{aligned} \tag{10}$$

Since $W - \{X_r^m, Y_1^n\} - A$ is a Markov chain, we have

$$\begin{aligned}&\lim_{n+m\to\infty} \frac{1}{n+m} H(W \mid X_r^m, Y_1^n, A)\\ &\quad = \lim_{n+m\to\infty} \frac{1}{n+m} H(W \mid X_r^m, Y_1^n).\end{aligned} \tag{11}$$

Therefore, the secrecy constraint can be expressed as

$$\begin{aligned}&\lim_{n+m\to\infty} \frac{1}{n+m} H(W)\\ &\quad = \lim_{n+m\to\infty} \frac{1}{n+m} H(W \mid X_r^m, Y_1^n).\end{aligned} \tag{12}$$

For a given α, and sequences of schedule $\{T(\alpha)\}$, the secrecy rate R_e is defined as

$$R_e = \lim_{n+m\to\infty} \frac{1}{n+m} H(W) \tag{13}$$

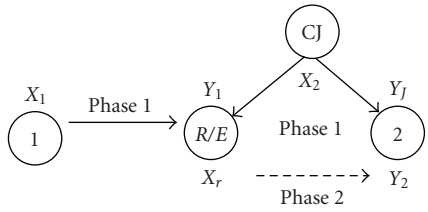

Figure 2: Two-hop network with an external cooperative jammer, CJ.

such that (9) and (12) are fulfilled. When deriving achievable rate, we will focus on a specific sequence of schedules $\{T(\alpha)\}$, and maximize the secrecy rate over α. When deriving the upper bound, we will consider all possible sequences of $\{T(\alpha)\}$.

Remark 1. Since the signals transmitted by node 1 and 2 do not depend on the signals they received in the past, $W \to Y_1^n \to X_r^m$ is a Markov chain. Therefore,

$$\lim_{n+m\to\infty} \frac{1}{n+m} H(W \mid X_r^m, Y_1^n) = \lim_{n+m\to\infty} \frac{1}{n+m} H(W \mid Y_1^n). \tag{14}$$

Hence, the following secrecy constraint can be used instead:

$$\lim_{n+m\to\infty} \frac{1}{n+m} H(W) = \lim_{n+m\to\infty} \frac{1}{n+m} H(W \mid Y_1^n). \tag{15}$$

Remark 2. We observe that in the system model shown in Figure 1, the destination, as the sender of the jamming signal during the periods of phase one, has perfect knowledge of this signal. This can be viewed as a special case of the model shown in Figure 2, where the destination only has a noisy copy of the jamming signal $Y_J = X_2 + Z_J$. If the jamming signal is corrupted by a noise sequence Z_J that is independent of the noise sequences at the other receivers, then the secrecy capacity of the model in Figure 2 can not be larger than the secrecy capacity of the model in Figure 1. This is because giving this noise sequence to the destination as genie information would simply reveal the jamming signal X_2 to it. Therefore, any upper bound we derive for Figure 1 is also an upper bound for Figure 2.

Remark 3. An apparent vulnerability of the described two phase protocol is that the destination may not be aware that the source has initiated its transmission. In this case, without the protection of the jamming signal from the destination, the message from the source would be revealed to the relay node and hence compromised. To prevent this from happening, proper initialization of the protocol is necessary.

3. Achievable Rate

In this section, we derive the achievable secrecy rate with the following sequence of deterministic periodic schedules.

The channel alternates between n' channel uses for phase one and m' channel uses for phase two, where n' and m' are two positive integers. The alternation takes M times. Hence $n = n'M$ and $m = m'M$. For a given α, the sequence of schedules is obtained by letting $M, n', m' \to \infty$ and

$$\lim_{n',m'\to\infty} \frac{n'}{m'+n'} = \alpha. \tag{16}$$

With this sequence of schedules, we have the following theorem.

Theorem 1. *The following secrecy rate is achievable for the model in Figure 1:*

$$0 \le R \le \max_{0\le P_1'\le \overline{P}_1/\alpha, 0<\alpha<1} \alpha\left[C\left(\frac{P_1'}{(1+\sigma_c^2)}\right) - C\left(\frac{P_1'}{(1+P_2)}\right)\right]^+, \tag{17}$$

where σ_c^2 is the variance of the Gaussian quantization noise determined by:

$$\alpha C\left(\frac{P_1'+1}{\sigma_c^2}\right) = (1-\alpha)C(P_r), \tag{18}$$

where P_2 is defined in (7)*, P_r is defined in* (8)*.*

Proof. The proof is given in the appendix. □

Remark 4. It can be seen from (17) that, for any fixed time sharing factor α the relay should always transmit at maximum power P_r. However, the optimal transmission power of the source may be less than P_1. This can be seen as follows: For a given jamming power P_2, the achievable rate is not a monotonically increasing function of P_1'. This is because, if $P_1' \to 0$ or $P_1' \to \infty$, $R_e \to 0$, indicating that even if the source power budget is ∞, the optimal transmission power is actually finite. Let this value be P_1^*. P_1^* may or may not fall into the interval $[0, P_1]$, which is the range of power consumption allowed for phase one. If it does, then the source should transmit with power P_1^* rather than P_1. If not, then the corresponding optimal value needs to be determined.

Remark 5. If the power constraint of the relay $\overline{P}_r \to \infty$, then $\sigma_c^2 \to 0, \alpha \to 1$. The achievable rate converges to

$$C\left(\overline{P}_1\right) - C\left(\frac{\overline{P}_1}{1+\overline{P}_2}\right). \tag{19}$$

4. Upper Bound

In this section, we derive an upper bound for the secrecy rate.

We first need to determine the optimal schedule. It turns out that it is easy to find: We simply let the first n channel uses be phase one, and the remaining m channel uses be phase two. The optimality of this schedule can be proved as follows.

Suppose a different schedule is used. Since the signals received in the past are not used for encoding purposes at node 1 and 2, we can always move the channel uses of phase

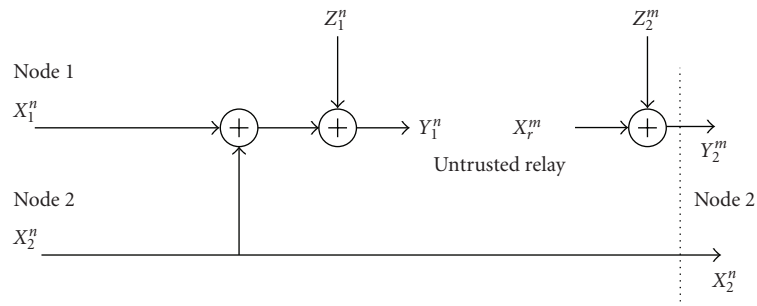

Figure 3: Equivalent Channel Model for Deriving the Upper Bound.

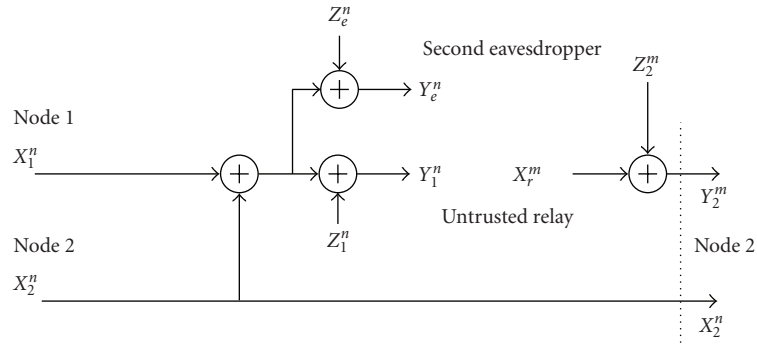

Figure 4: Two-eavesdropper channel.

one to the front without affecting the signals transmitted by these two nodes. On the other hand, we notice that the relay can only use signals received in the past to compute its transmission signals. However, during phase one, the relay only receives signals. Since moving phase one ahead only means the relay could receive signals sooner, doing so will not limit the capability of the relay to calculate its transmitted signals. Consequently, we observe that no matter what schedule is used to achieve a secrecy rate, we can always modify this schedule such that all channel uses of phase one are ahead of those of phase two and still achieve the same secrecy rate. Hence in the following we only consider the optimal schedule.

We also observe we can transform the channel into the one shown in Figure 3. The jammer and the receiver are now drawn separately, since the jammer does not use the signal received in the past to compute the jamming signal. Note that Figure 3 is similar to Figure 12 used in the achievability proof except that the dimension of the signals is changed from m', n' to m, n.

We next leverage a technique first used in [11, 22] to derive the upper bound. Specifically, the upper bound is obtained via the following transformations.

(1) First, we add a second eavesdropper to the channel, as shown by Figure 4. Its received signal is denoted by Y_e and over n channel uses Y_e^n is given by

$$Y_e^n = X_1^n + X_2^n + Z_e^n. \tag{20}$$

Here Z_e^n is a Gaussian noise with the same distribution as Z_1^n. Z_e^n can be arbitrarily correlated with Z_1^n. Since

$$Y_1^n = X_1^n + X_2^n + Z_1^n. \tag{21}$$

we have

$$\Pr(W, Y_e^n) = \Pr(W, Y_1^n). \tag{22}$$

Therefore,

$$H(W \mid Y_e^n) = H(W \mid Y_1^n). \tag{23}$$

From (15), this means

$$\begin{aligned} &\lim_{n+m\to\infty} \frac{1}{m+n} H(W). \\ &\quad = \lim_{n+m\to\infty} \frac{1}{m+n} H(W \mid Y_e^n). \end{aligned} \tag{24}$$

Hence the message W is kept secret from the second eavesdropper. This means, for a given coding scheme that achieves secrecy rate in Figure 3, the same secrecy rate is achievable with the introduction of this additional eavesdropper.

(2) Next, we remove the first eavesdropper at the relay. Doing so will not decrease secrecy rate either, since we have one less secrecy constraint.

From (24), the secrecy rate can be upper bounded via $H(W \mid Y_e^n)$. To do that, we provide the signal X_r^m to the destination by a genie. Similarly, the signal X_2^n is revealed

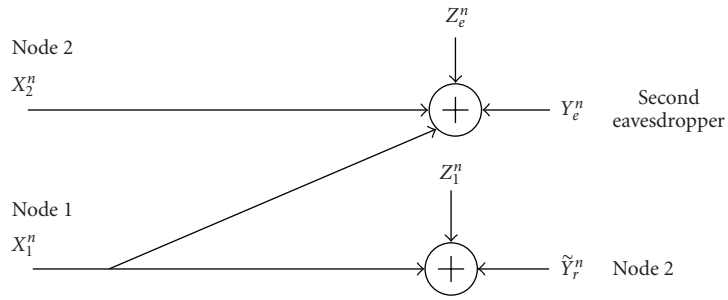

Figure 5: Channel model after transformation.

to both the relay and the destination. $H(W \mid Y_e^n)$ is then bounded by

$$\begin{aligned} &H(W \mid Y_e^n) \\ &\quad \le H(W \mid Y_e^n) - H(W \mid X_r^m Y_2^m X_2^n) + n\varepsilon \qquad (25)\\ &\quad = H(W \mid Y_e^n) - H(W \mid X_r^m X_2^n) + n\varepsilon \qquad (26)\\ &\quad \le H(W \mid Y_e^n) - H(W \mid Y_1^n X_r^m X_2^n) + n\varepsilon \qquad (27)\\ &\quad = H(W \mid Y_e^n) - H(W \mid Y_1^n X_2^n) + n\varepsilon \qquad (28)\\ &\quad = H(W \mid Y_e^n) - H(W \mid X_1^n + Z_1^n) + n\varepsilon \qquad (29)\\ &\quad \le H(W \mid Y_e^n) - H(W \mid Y_e^n, X_1^n + Z_1^n) + n\varepsilon. \qquad (30)\end{aligned}$$

The genie information X_r^m causes the signal Y_2^m to be useless to the relay, as shown by (25)-(26). Equation (28) is due to the fact that once the signal received by the relay Y_1^n is given, the signal transmitted by the relay X_r^m, which is computed from Y_1^n, is independent from the jamming signal X_2^n and the confidential message W. Finally, revealing the genie information X_2^n to the relay and the destination essentially removes the influence of the jamming signal from the relay link, as shown by (28)–(30). These are essentially a consequence of the link noises being independent. The resulting channel is equivalent to the one shown in Figure 5, and can be viewed as a special case of the channel in [8, 33]. Similar techniques to those in [31, 33] can be used here to bound the secrecy rate. Let $\widetilde{Y}_r^n = X_1^n + Z_1^n$. Then (30) becomes

$$\begin{aligned} &H(W \mid Y_e^n) - H\left(W \mid Y_e^n \widetilde{Y}_r^n\right) \qquad (31)\\ &\quad = I\left(W; \widetilde{Y}_r^n \mid Y_e^n\right) \qquad (32)\\ &\quad \le I\left(WX_1^n; \widetilde{Y}_r^n \mid Y_e^n\right) \qquad (33)\\ &\quad = I\left(X_1^n; \widetilde{Y}_r^n \mid Y_e^n\right) \qquad (34)\\ &\quad = h\left(\widetilde{Y}_r^n \mid Y_e^n\right) - h(Z_1^n \mid X_2^n + Z_e^n) \qquad (35)\\ &\quad \le h\left(\widetilde{Y}_r^n \mid Y_e^n\right) - h(Z_1^n \mid X_2^n + Z_e^n, X_2^n) \qquad (36)\\ &\quad = h\left(\widetilde{Y}_r^n \mid Y_e^n\right) - h(Z_1^n \mid Z_e^n). \qquad (37)\end{aligned}$$

Here (34) follows from the fact that X_1^n determines W. The first term in (37) is maximized when X_1^n and X_2^n are i.i.d. Gaussian sequences [14]. Let the variance of each component of X_i^n be $P_i = \overline{P}_i/\alpha$, $i = 1, 2$. Let ρ be the correlation factor between Z_1 and Z_e. Then (37) is equal to

$$\frac{n}{2}\log_2 \frac{(P_1+1)(P_1+P_2+1) - (P_1+\rho)^2}{(P_1+P_2+1)(1-\rho^2)}. \qquad (38)$$

It can be verified that, for any fixed ρ, equation (37) is an increasing function of P_1 and P_2. Therefore, the upper bound is maximized with maximum average power. Equation (38) can then be tightened by minimizing it over ρ. The optimal ρ is given below:

$$\frac{2P_1 + P_1P_2 + P_2 - \sqrt{A}}{2P_1}, \qquad (39)$$

where

$$A = 4P_2P_1^2 + 4P_2P_1 + P_2^2P_1^2 + 2P_2^2P_1 + P_2^2. \qquad (40)$$

As a result, we have the following theorem.

Theorem 2. *The secrecy rate of the channel in Figure 12 is upper bounded by*

$$\max_{0<\alpha<1} \min\left\{\begin{array}{c} \dfrac{\alpha}{2}\log_2 \dfrac{(P_1+1)(P_1+P_2+1) - (P_1+\rho)^2}{(P_1+P_2+1)(1-\rho^2)}, \\ (1-\alpha)C(P_r) \end{array}\right\} \qquad (41)$$

where ρ is given by (39). $P_1 = \overline{P}_1/\alpha$, $P_2 = \overline{P}_2/\alpha$, *and* $P_r = \overline{P}_r/(1-\alpha)$ *are the average power constraints of node* 1, 2 *and the relay for the time sharing factor* α.

Remark 6. If we further fix $\overline{P}_2$, and let $\overline{P}_r, \overline{P}_1 \to \infty$, then $\alpha \to 1$. ρ converges to $\overline{\rho}$ given by

$$\overline{\rho} = 1 + \frac{\overline{P}_2}{2} - \sqrt{\overline{P}_2 + \frac{\overline{P}_2^2}{4}}. \qquad (42)$$

The difference of the upper bound and the achievable rate converges to

$$C\left(\frac{\overline{P}_2 + (\overline{\rho}-1)^2}{1-\overline{\rho}^2}\right) - C\left(\overline{P}_2\right). \qquad (43)$$

We observe that the difference is only a function of $\overline{P}_2$. By comparison, the gap between the achievable rate and the trivial upper bound $C(\overline{P}_1)$ is $C(\overline{P}_1/(1+\overline{P}_2))$, which is unbounded.

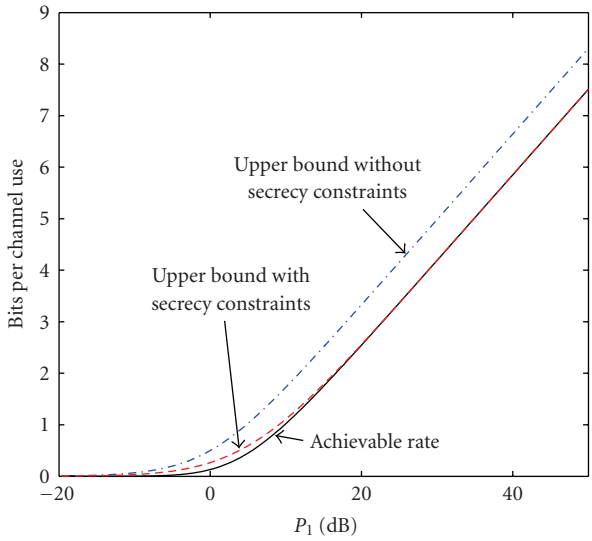

FIGURE 6: Secrecy Rate, $P_r \to \infty$, $P_2 = 0.5\,P_1$, optimal α.

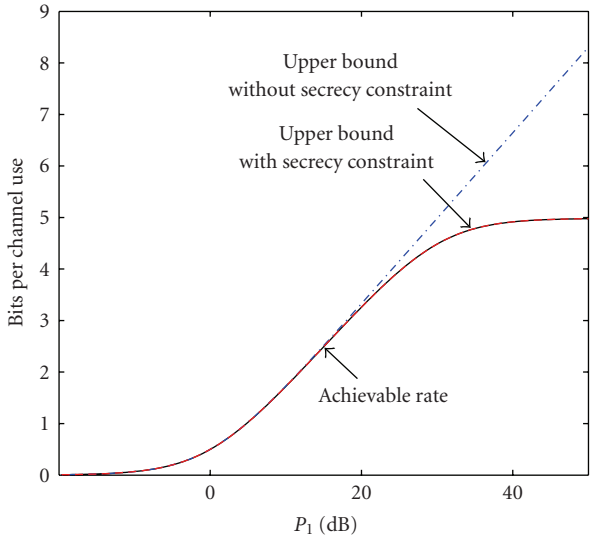

FIGURE 7: Secrecy Rate, $P_r \to \infty$, $P_2 = 30$ dB, optimal α.

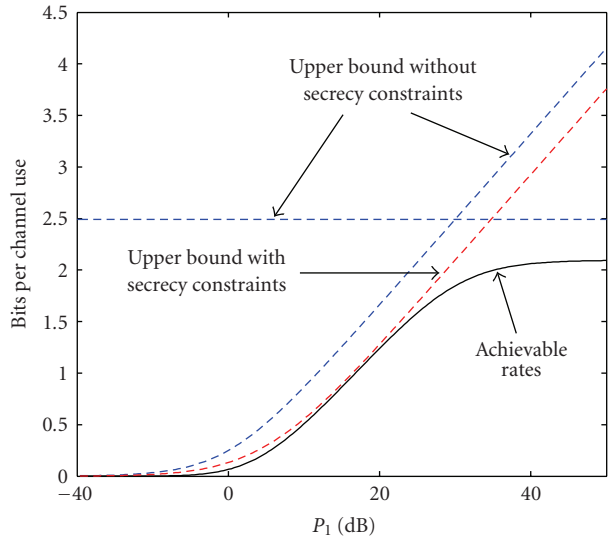

FIGURE 8: Secrecy Rate, $P_r = 30$ dB, $P_2 = 0.5\,P_1$, $\alpha = 0.5$.

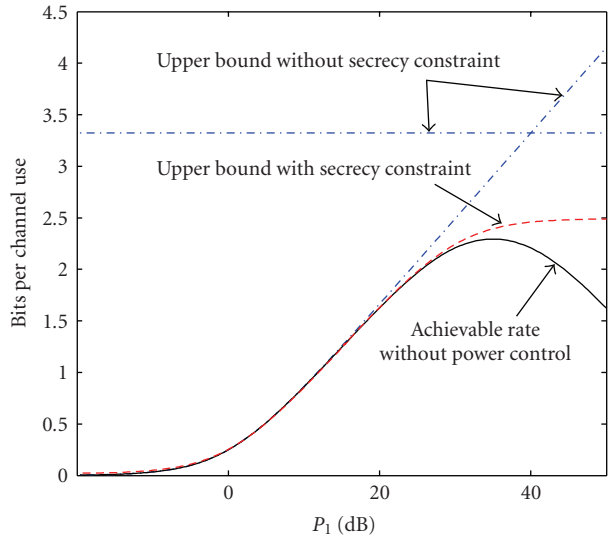

FIGURE 9: Secrecy Rate, $P_r = 30$ dB, $P_2 = 40$ dB, $\alpha = 0.5$.

Remark 7. If we instead fix $\overline{P}_2 = \beta\overline{P}_1$, and let $\overline{P}_r \to \infty$, then $\alpha \to 1$. The achievable rate converges to (19). In this case, if we further let $\overline{P}_1 \to \infty$, the upper bound given by (41) converges to

$$C\left(\overline{P}_1\right) - C\left(\frac{1}{\beta}\right). \tag{44}$$

Comparing it with (19), we observe the difference of the upper bound and the achievable rate converges to 0. Hence, in this case, our upper bound is asymptotically tight.

Remark 8. The first term in the bound (41) is strictly smaller than the trivial bound $\alpha C(P_1)$ obtained by removing the secrecy constraints. To show that, simply let $\rho = 0$. Equation (41) becomes

$$\alpha C(P_1) + \frac{\alpha}{2}\log_2 \frac{1 + P_1/((P_1+1)(P_2+1))}{1 + P_1/(P_2+1)}. \tag{45}$$

The second term in (45) is always negative.

4.1. Comparison with the Bound Derived with Generalized Entropy Power Inequality. Recently the generalized entropy power inequality [34] was used to derive a computable upper bound for the Gaussian multiple access channel with secrecy constraints [32]. Here the same technique is applicable and another computable upper bound for the model in Figure 1 can be derived. It is of interest to know which bound is tighter. Next, we prove that as long as $P_1 + P_2 > 1$, this upper bound is always looser than the bound given by (38)-(39).

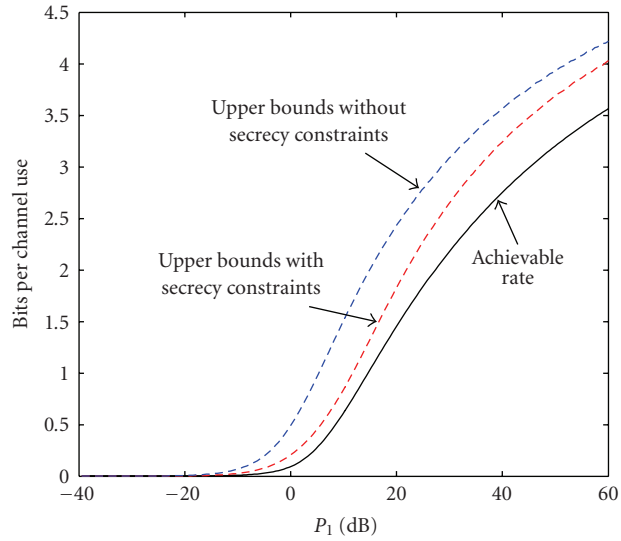

FIGURE 10: Secrecy Rate, $P_r = 40$ dB, $P_2 = 0.25\,P_1$, optimized over α.

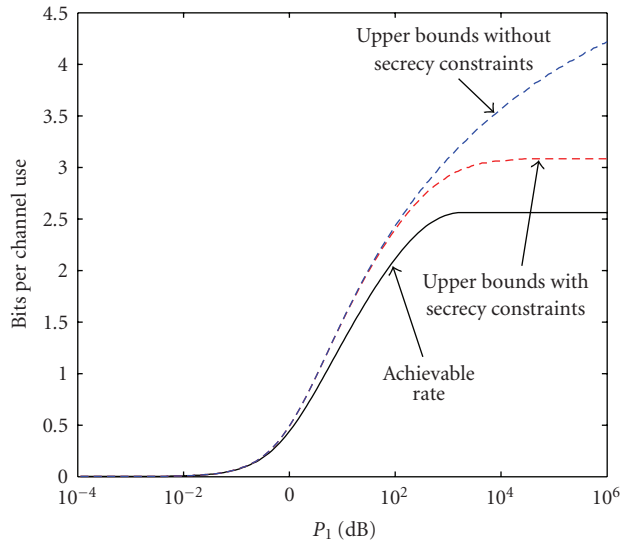

FIGURE 11: Secrecy Rate, $P_r = 40$ dB, $P_2 = 30$ dB, optimized over α, power control at the source node enabled.

First, we briefly describe the derivation of the bound based on the approach in [32]:

$$H(W \mid Y_1^n) \tag{46}$$

$$\overset{(a)}{=} H(W \mid Y_1^n) - H(W \mid Y_1^n X_2^n) + n\varepsilon$$

$$= I(W; X_2^n \mid Y_1^n) + n\varepsilon \tag{47}$$

$$\leq I(WX_1^n; X_2^n \mid Y_1^n) + n\varepsilon \tag{48}$$

$$= I(X_1^n; X_2^n \mid Y_1^n) + n\varepsilon. \tag{49}$$

Here step (a) follows from Fano's inequality. (49) can be written as:

$$I(X_1^n; Y_1^n \mid X_2^n) + I(X_1^n; X_2^n) - I(X_1^n; Y_1^n) + n\varepsilon \tag{50}$$

$$\overset{(b)}{=} I(X_1^n; Y_1^n \mid X_2^n) - I(X_1^n; Y_1^n) + n\varepsilon \tag{51}$$

$$= h(X_1^n + Z_1^n) + h(X_2^n + Z_1^n) - h(Z_1^n) - h(X_1^n + X_2^n + Z_1^n) + n\varepsilon \tag{52}$$

Step (b) follows from X_1^n, X_2^n being independent.

Next, like [32, equation (76)], we invoke the inequality from [34] and obtain

$$2^{(2/n)h\left(X_1^n+X_2^n+Z_1^n\right)} \geq \frac{2^{(2/n)h(X_1^n+Z_1^n)} + 2^{(2/n)h\left(X_2^n+Z_1^n\right)}}{2}. \tag{53}$$

Hence (52) can be upper bounded with

$$h(X_1^n + Z_1^n) + h(X_2^n + Z_1^n) - \frac{n}{2}\log_2\left(2^{(2/n)h\left(X_1^n+Z_1^n\right)} + 2^{(2/n)h\left(X_2^n+Z_1^n\right)}\right) + \frac{n}{2}\log_2(2). \tag{54}$$

This expression is maximized when X_1^n, X_2^n are chosen to be i.i.d. Gaussian sequences. Dividing by the total number of channel uses $n + m$, the final expression of the upper bound is given by

$$\frac{\alpha}{2}\log_2\left(\frac{2(P_1+1)(P_2+1)}{P_1+P_2+2}\right). \tag{55}$$

Remark 9. Note that (55) is also tighter than the bound $\alpha C(P_1)$ when $P_1 > P_2$. Hence it is a nontrivial bound when $P_1 > P_2$.

Remark 10. When $\overline{P}_r \to \infty$, then $\alpha \to 1$, $P_i \to \overline{P}_i$, $i = 1, 2$. Comparing (19) with (55), the gap between the achievable rates and the bound given by (55) is

$$\frac{1}{2}\log_2\left(1 + \frac{\overline{P}_1 + \overline{P}_2}{2 + \overline{P}_1 + \overline{P}_2}\right). \tag{56}$$

which is smaller than 0.5 bit/channel use.

We next show that for any given α, if $P_1 + P_2 > 1$, (55) is always bigger than the first term in (41). We omit the time sharing factor α in the front since they are present in both expressions. Then we pick ρ such that

$$1 - \rho^2 = \frac{P_1 + P_2 + 2}{2(P_1 + P_2 + 1)}. \tag{57}$$

Note that this is a valid choice for ρ since the right hand side is within the interval $(0, 1)$. Then (41), after canceling α in the front, becomes

$$\frac{1}{2}\log_2 \frac{2\left(\begin{matrix}(P_1+1)(P_1+P_2+1)\\ -(P_1+\rho)^2\end{matrix}\right)}{P_1+P_2+2}. \tag{58}$$

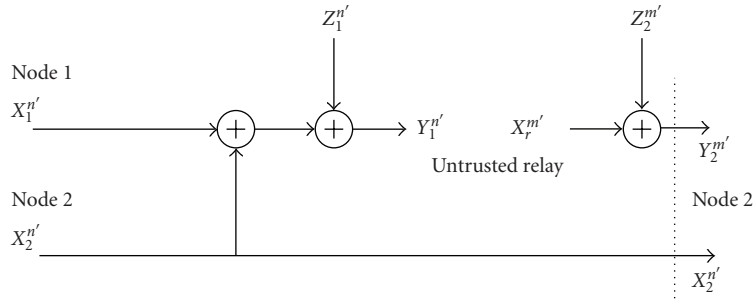

Figure 12: Equivalent channel model.

Table 1: Scenarios considered in the numerical results.

	Relay's power	Jammer's power	α
Figure 6	∞	Proportional	Optimal
Figure 7	∞	Fixed	Optimal
Figure 8	Limited	Proportional	0.5
Figure 9	Limited	Fixed	0.5
Figure 10	Limited	Proportional	Optimal
Figure 11	Limited	Fixed	Optimal

Hence we only need to verify that (55) is greater than (58) when $P_1 + P_2 > 1$. This is equivalent to verifying

$$(P_1 + 1)(P_2 + 1) > (P_1 + 1)(P_1 + P_2 + 1) - (P_1 + \rho)^2 \quad (59)$$

or $(2\rho - 1)P_1 + \rho^2 > 0$. A sufficient condition for this to hold is to require $2\rho - 1 > 0$. Substitute (57) into this requirement we get $P_1 + P_2 > 1$.

Remark 11. Since the gap between the achievable rates and the bound given by (55) is bounded by 0.5 bit/channel use when $\overline{P}_r \to \infty$, the gap between the achievable rates and the bound given by (41) is also bounded by 0.5 bit/channel use when $\overline{P}_r \to \infty$ and $\overline{P}_1 + \overline{P}_2 > 1$. Note that since when $\overline{P}_r \to \infty$ we have $\alpha \to 1$, the condition $P_1 + P_2 > 1$ is equivalent to $\overline{P}_1 + \overline{P}_2 > 1$.

Remark 12. For the case that $P_1 + P_2 < 1$, it is not clear between (55) and (41) which bound is tighter. However, for these cases, the secrecy capacity is so small that the bounds are of no consequence.

5. Numerical Results

Shown in Table 1 are the six cases of interest, corresponding to different power budgets of the relay and the jammer and whether time sharing factor α is fixed. We included the cases with fixed time sharing factor because in a real system, for simplicity the time sharing factor may not be dynamically adjusted according to power budgets. The numerical result of each case is shown in the figures listed in the table. We stress that, though not explicitly considered in the numerical results, for the more general case where the cooperative jammer is external, as shown in Figure 2, the upper bound still holds, but the gap between the upper bound and achievable rates would be wider.

Figures 6 and 7 demonstrate the asymptotic behavior described in Remark 6 when the power of relay goes to ∞. Note that in this case the optimal time sharing factor α converges to 1. Figures 8 and 9 demonstrate the case where the power the relay is finite, and the time sharing factor α is fixed. In all four cases, we observe the upper bound is close to the achievable rate when relay's power is larger than the power of the source and the jammer. In this region, typically, the achievable rate increases linearly with the source SNR. In Figure 6, the gap between the upper bound and achievable rate goes to zero as $P_1 \to \infty$. In Figure 7, the upper bound almost coincides with the achievable rate. The gap, given by (43), equals 9.98×10^{-4} bits/channel use.

Also shown in each figure is the cut-set bound without secrecy constraints. The improvement provided by the new bounds depends on the power budget. In general, the improvement is small if the power of the jammer is large. Note that since we have normalized all channel gains and included them into the power constraint, the power budget difference can be considered a consequence of the difference in link gains.

Figure 9 also illustrates the power control problem described in Remark 4. Without power control at the source node, the achievable rate will eventually decrease to zero. Note that this behavior crystallizes only when the relay's power is limited.

Finally, in Figures 10 and 11, we compare the achievable rates and the upper bound when each are maximized over the time sharing factor α. The gap between the upper bound and the achievable rate is now wider because the second term in the upper bound (41) is the same as the upper bound without secrecy constraint. The role played by the second

term (41) becomes significant when the bound is optimized over the time sharing factor, which as pointed out in [35], has a tendency to balance the two terms in the bound (41). However, as shown in these figures, compared to the upper bound without secrecy constraints, the new bound still offers significant improvement.

6. Conclusion

In this paper, we have considered a relay network without a direct link, where relaying is essential for the source and the destination to communicate despite the fact that the relay node is untrusted. Imposing secrecy constraints at the relay node, contrary to the previous work, we have shown that a nonzero secrecy rate is indeed achievable. This is accomplished by enlisting the help of the destination (or another dedicated node) who transmits to jam the relay, and uses the jamming signal as side information. We have derived an upper bound for the secrecy rate with the assumption that no feedback is used for encoding at the source or destination. The new upper bound is strictly tighter than the upper bound without secrecy constraints. We have also proved that it is tighter than an upper bound derived from generalized entropy power inequality when the maximum sum received SNR at the relay is greater than 0 dB. The gap between the bound and the achievable rates converges to 0 when the power of the transmitter, the relay and the jammer goes to ∞. Numerical results show that our upper bound is in general close to the achievable rate, and is indistinguishable from it for a fixed time sharing factor with a relay whose power is in abundance.

In this work, we considered the case where the source or the jammer does not make use of the relay transmission for encoding purposes. An upper bound for the secrecy rate when feedback is used is recently found in [36]. A gap exists between the upper bound and the achievable rate in [36], which is bounded by 0.5 bit per channel use but does not vanish when the power of the transmitter, the relay and the jammer goes to infinity. By comparison, the bound presented in this work is asymptotically tighter in this case.

We conclude by reiterating that our findings in this paper presents cooperative jamming as an enabler for secrecy from an *internal* eavesdropper, and motivates further investigation of such cooperation ideas in more general settings including those in larger networks. We also comment whether and when cooperative jamming actually yields the secrecy capacity (region) for various multiuser channels remain open problems in information theory.

Appendix

Proof of Theorem 1

We first introduce several supporting results used in proving Theorem 1.

In [11, 21], we presented the following achievable secrecy rate for a general relay channel.

Theorem 3. *Consider a relay network with conditional distribution $p(Y, Y_r \mid X, X_r)$, with X, X_r being the input from the source and the relay respectively, and Y_r, Y being the signals received by the relay and the destination, respectively. For the distribution*

$$p(X)p(X_r)p(Y, Y_r X, X_r)p\left(\hat{Y}_r Y_r, X_r\right), \tag{A.1}$$

the following range of rates R is achievable:

$$0 \le R < \left[I\left(X; Y\hat{Y}_r \mid X_r\right) - I(X; Y_r \mid X_r)\right]^+ \tag{A.2}$$

with

$$I(X_r; Y) > I\left(\hat{Y}_r; Y_r Y X_r\right). \tag{A.3}$$

Theorem 3 follows from the achievable equivocation region given in [11, Theorem 1] by simply considering rates R that equal the equivocation rate R_e. The proof of Theorem 3 is given in [11]. The outline of the achievable scheme is as follows: The relay does compress-and-forward as described in [25]. Therefore, as in [25], X_r is independent from X in the input distribution expression (A.1). The same decoder in [25] is used at the destination. The same codebook as [25] is used at the source node. However, instead of mapping the message to the codeword deterministically as in [25], a stochastic encoder is used at the source node. In this encoder, the codewords are randomly binned into several bins. The size of each bin is $2^{NI(X;Y_r|X_r)}$ where N is the total number of channel uses. The message W determines which bin to use by the encoder. The actual transmitted codeword is then randomly chosen from the bin according to a uniform distribution. This randomness serves to confuse the eavesdropper at the relay node at the cost of the rate as shown by the term $-I(X; Y_r \mid X_r)$ in (A.2).

We next extend this result by considering a relay channel with a jammer defined by

$$p(Y_r, Y \mid X, X_2, X_r), \tag{A.4}$$

where X_2 is the signal transmitted by the jammer and the notation Y, Y_r, X, X_2 follows the definition above. Then, if the jammer transmits an i.i.d. signal according to distribution $p(X_2)$ and $p(X, X_2, X_r) = p(X)p(X_2)p(X_r)$, the induced channel $p(Y_r, Y \mid X, X_r)$ is given below:

$$p(Y_r, Y \mid X, X_r) = \sum_{X_2} p(X_2)p(Y_r, Y \mid X, X_2, X_r) \tag{A.5}$$

and it is also a memoryless relay channel. Hence, we can use Theorem 3 and obtain the following corollary.

Corollary 1. *The following secrecy rate is achievable:*

$$\begin{aligned} 0 \le R \le & \max_{p(X)p(X_2)p(X_r)p(Y,Y_r|X,X_2,X_r)p(\hat{Y}_r|Y_r,X_r)} \\ & \times\left[I\left(X; Y\hat{Y}_r \mid X_r\right) - I(X; Y_r \mid X_r)\right]^+ \end{aligned} \tag{A.6}$$

with

$$I(X_r; Y) > I\left(\hat{Y}_r; Y_r \mid Y X_r\right). \tag{A.7}$$

We next reformulate our channel in Figure 1 in a way such that Corollary 1 can be applied. This is shown in Figure 12. Here we can draw the jammer and the receiver separately, since the jammer does not use the signal received in the past to compute the jamming signal. The m' and n' are the parameters of the schedule described in Section 3. We then observe Figure 12 can be viewed as a three node relay network with a jammer, defined as follows:

$$p(\mathrm{Y}, \mathrm{Y_r} \mid \mathrm{X}, \mathrm{X_2}, \mathrm{X_r}), \tag{A.8}$$

where

$$\begin{aligned} \mathrm{Y} &= \left\{ Y_2^{m'}, X_2^{n'} \right\}, \\ \mathrm{Y_r} &= Y_1^{n'}, \qquad \mathrm{X} = X_1^{n'}, \\ \mathrm{X_r} &= X_r^{m'}, \qquad \mathrm{X_2} = X_2^{n'}. \end{aligned} \tag{A.9}$$

The input distributions to this vector input channel are chosen as

$$p\left(X_1^{n'}, X_2^{n'}, X_r^{m'}\right) = p\left(X_1^{n'}\right) p\left(X_2^{n'}\right) p\left(X_r^{m'}\right), \tag{A.10}$$

where $p(X_1^{n'})$, $p(X_2^{n'})$ and $p(X_r^{m'})$ are given below.

(1) Let $X_1^{n'} \sim \mathcal{N}(0, P_1' \mathbf{I}_{n' \times n'})$, where P_1' is the average power consumption of node 1 during the periods of phase one. Hence $0 < P_1' < P_1$.

(2) Let the auxiliary random variable in compress-and-forward $\hat{\mathrm{Y}}_\mathrm{r}$ be $\hat{Y}_1^{n'}$. Let $\hat{Y}_1^{n'} = Y_1^{n'} + Z_Q^{n'}$, where $Z_Q^{n'} \sim \mathcal{N}(0, \sigma_c^2 \mathbf{I}_{n' \times n'})$,

(3) Let $X_r^{m'} \sim \mathcal{N}(0, P_r \mathbf{I}_{m' \times m'})$ and $X_2^{n'} \sim \mathcal{N}(0, P_2 \mathbf{I}_{n' \times n'})$,

where $\mathbf{I}_{n' \times n'}$ denotes an $n' \times n'$ identity matrix. With (1)–(3), we have

$$I\left(\mathrm{X}; \mathrm{Y}\hat{\mathrm{Y}}_\mathrm{r} \mid \mathrm{X_r}\right) \tag{A.11}$$

$$= I\left(X_1^{n'}; Y_2^{m'} X_2^{n'} \hat{Y}_1^{n'} \mid X_r^{m'}\right) \tag{A.12}$$

$$\begin{aligned} &= I\left(X_1^{n'}; Y_2^{m'} \hat{Y}_1^{n'} \mid X_r^{m'} X_2^{n'}\right) \\ &\quad + I\left(X_1^{n'}; X_2^{n'} \mid X_r^{m'}\right). \end{aligned} \tag{A.13}$$

From (A.10), $I(X_1^{n'}; X_2^{n'} \mid X_r^{m'}) = 0$. Therefore (A.13) equals

$$I\left(X_1^{n'}; Y_2^{m'} \hat{Y}_1^{n'} \mid X_r^{m'} X_2^{n'}\right) \tag{A.14}$$

$$\begin{aligned} &= I\left(X_1^{n'}; \hat{Y}_1^{n'} \mid X_r^{m'} Y_2^{m'} X_2^{n'}\right) \\ &\quad + I\left(X_1^{n'}; Y_2^{m'} \mid X_r^{m'} X_2^{n'}\right) \end{aligned} \tag{A.15}$$

$$\begin{aligned} &= I\left(X_1^{n'}; \hat{Y}_1^{n'} \mid X_r^{m'} Y_2^{m'} X_2^{n'}\right) \\ &\quad + I\left(X_1^{n'}; Z_2^{m'} \mid X_r^{m'} X_2^{n'}\right) \end{aligned} \tag{A.16}$$

$$= I\left(X_1^{n'}; \hat{Y}_1^{n'} \mid X_r^{m'} Y_2^{m'} X_2^{n'}\right), \tag{A.17}$$

(A.17) equals:

$$I\left(X_1^{n'}; Y_1^{n'} + Z_Q^{n'} \mid X_r^{m'} Y_2^{m'} X_2^{n'}\right) \tag{A.18}$$

$$\begin{aligned} &= I\left(X_1^{n'}; X_1^{n'} + X_2^{n'} + Z_1^{n'} + Z_Q^{n'} \right. \\ &\qquad \left. \mid X_r^{m'}, X_r^{m'} + Z_2^{m'}, X_2^{n'}\right) \end{aligned} \tag{A.19}$$

$$= I\left(X_1^{n'}; X_1^{n'} + X_2^{n'} + Z_1^{n'} + Z_Q^{n'} \mid X_2^{n'}\right) \tag{A.20}$$

$$= I\left(X_1^{n'}; X_1^{n'} + Z_1^{n'} + Z_Q^{n'}\right) \tag{A.21}$$

$$= n' C\left(\frac{P_1'}{1 + \sigma_c^2}\right), \tag{A.22}$$

$$I(\mathrm{X}; \mathrm{Y_r} \mid \mathrm{X_r}) \tag{A.23}$$

$$= I\left(X_1^{n'}; Y_1^{n'} \mid X_r^{m'}\right) \tag{A.24}$$

$$= I\left(X_1^{n'}; X_1^{n'} + X_2^{n'} + Z_1^{n'} \mid X_r^{m'}\right) \tag{A.25}$$

$$= I\left(X_1^{n'}; X_1^{n'} + X_2^{n'} + Z_1^{n'}\right) \tag{A.26}$$

$$= n' C\left(\frac{P_1'}{1 + P_2}\right), \tag{A.27}$$

$$I(\mathrm{X_r}; \mathrm{Y}) \tag{A.28}$$

$$= I\left(X_r^{m'}; Y_2^{m'}, X_2^{n'}\right) \tag{A.29}$$

$$= I\left(X_r^{m'}; Y_2^{m'}\right) \tag{A.30}$$

$$= m' C(P_r), \tag{A.31}$$

$$I\left(\hat{\mathrm{Y}}_\mathrm{r}; \mathrm{Y_r} \mid \mathrm{Y}, \mathrm{X_r}\right) \tag{A.32}$$

$$= I\left(\hat{Y}_1^{n'}; Y_1^{n'} \mid Y_2^{m'} X_2^{n'} X_r^{m'}\right) \tag{A.33}$$

$$= I\left(Y_1^{n'} + Z_Q^{n'}; Y_1^{n'} \mid X_2^{n'} X_r^{m'} Z_2^{m'}\right) \tag{A.34}$$

$$\begin{aligned} &= I\left(X_1^{n'} + X_2^{n'} + Z_1^{n'} + Z_Q^{n'}; \right. \\ &\qquad \left. X_1^{n'} + X_2^{n'} + Z_1^{n'} \mid X_2^{n'}, X_r^{m'}\right) \end{aligned} \tag{A.35}$$

$$\begin{aligned} &= I\left(X_1^{n'} + X_2^{n'} + Z_1^{n'} + Z_Q^{n'}; \right. \\ &\qquad \left. X_1^{n'} + X_2^{n'} + Z_1^{n'} \mid X_2^{n'}\right) \end{aligned} \tag{A.36}$$

$$= I\left(X_1^{n'} + Z_1^{n'} + Z_Q^{n'}; X_1^{n'} + Z_1^{n'}\right) \tag{A.37}$$

$$= n' C\left(\frac{P_1' + 1}{\sigma_c^2}\right). \tag{A.38}$$

In (A.14), (A.20), (A.26), (A.30), (A.36), and (A.37), we use (A.10) repeatedly, which says that with compress-and-forward, the input distribution are chosen such that $X_1^{n'}, X_2^{n'}, X_r^{m'}$ are independent.

Substituting the values of $I(X; Y\hat{Y}_r \mid X_r)$, $I(X; Y_r \mid X_r)$, $I(X_r; Y)$ and $I(\hat{Y}_r; Y_r \mid Y, X_r)$ into Corollary 1, dividing both sides by $m' + n'$, and taking the limit $m' + n' \to \infty$, we proved the theorem.

Acknowledgments

This work was presented in part at the IEEE Globecom Conference, December 2008. This work is supported in part by the National Science Foundation with Grants CCR-0237727, CCF-051483, CNS-0716325, CNS-0721445, and the DARPA ITMANET Program with Grant W911NF-07-1-0028.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

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

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[5] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[6] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proceedings of the 39th Asilomar Conference on Signals, Systems and Computers (ACSSC '05)*, pp. 1747–1751, Pacific Grove, Calif, USA, October-November 2005.

[7] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

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

[9] Y. Oohama, "Relay channels with confidential messages," submitted to *IEEE Transactions on Information Theory* http://arxiv.org/abs/cs/0611125.

[10] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[11] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," 2008, submitted to *IEEE Transactions on Information Theory* http://arxiv.org/abs/0910.1511.

[12] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[13] R. Liu and H. V. Poor, "Multi-antenna Gaussian broadcast channels with confidential messages," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '08)*, pp. 2202–2206, Toronto, Canada, July 2008.

[14] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: the MISOME wiretap channel," to appear in *IEEE Transactions on Information Theory* http://allegro.mit.edu/pubs/posted/journal/2007-khisti-wornell-it.pdf.

[15] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proceedings IEEE International Symposium on Information Theory (ISIT '08)*, pp. 524–528, Toronto, Canada, July 2008.

[16] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: the 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, 2009.

[17] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proceedings of the 44th Annual Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, Ill, USA, September 2006.

[18] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[19] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[20] O. Koyluoglu, H. El-Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," 2008, submitted to *IEEE Transactions on Information Theory* http://arxiv.org/abs/0810.1187.

[21] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Proceedings of the 41st Asilomar Conference on Signals, Systems and Computers (ACSSC '07)*, pp. 883–887, Pacific Grove, Calif, USA, November 2007.

[22] X. He and A. Yener, "The role of an untrusted relay in secret communication," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '08)*, pp. 2212–2216, Toronto, Canada, July 2008.

[23] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '08)*, pp. 2217–2221, Toronto, Canada, July 2008.

[24] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," 2008, submitted to *IEEE Transactions on Information Theory* http://www.ece.umd.edu/ ulukus/papers/journal/crbc-secrecy.pdf.

[25] T. M. Cover and A. A. El Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, 1979.

[26] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proceedings of IEEE Military Communications Conference (MILCOM '05)*, Atlatnic City, NJ, USA, October 2005.

[27] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proceedings of the 62nd IEEE Vehicular Technology Conference (VTC '05)*, vol. 3, pp. 1906–1910, Stockholm, Sweden, September 2005.

[28] M. L. Jørgensen, B. R. Yanakiev, G. E. Kirkelund, P. Popovski, H. Yomo, and T. Larsen, "Shout to secure: physical-layer wireless security with known interference," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 33–38, Washington, DC, USA, November 2007.

[29] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: encryption over the channel," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, 2008.

[30] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proceedings of IEEE*

Information Theory Workshop (ITW '08), pp. 164–168, Porto, Portugal, May 2008.

[31] E. Tekin and A. Yener, "Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, Ill, USA, September 2007.

[32] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1014–1021, Urbana-Champaign, Ill, USA, September 2008.

[33] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '08)*, pp. 389–393, Toronto, Canada, July 2008.

[34] M. Madiman and A. Barron, "Generalized entropy power inequalities and monotonicity properties of information," *IEEE Transactions on Information Theory*, vol. 53, no. 7, pp. 2317–2329, 2007.

[35] Y. Liang, V. V. Veeravalli, and H. V. Poor, "Resource allocation for wireless fading relay channels: max-min solution," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3432–3453, 2007.

[36] X. He and A. Yener, "On the role of feedback in two-way secure communication," in *Proceedings of the 42nd Asilomar Conference on Signals, Systems and Computers (ACSSC '08)*, pp. 1093–1097, Pacific Grove, Calif, USA, October 2008.