Two-hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming

Xiang He Aylin Yener
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xxh119@psu.edu *yener@ee.psu.edu*

***Abstract*—We consider a source-destination pair that can communicate only through an unauthenticated intermediate relay node. In this two-hop communication scenario, where the cooperation from the relay node is essential, we investigate whether achieving non-zero secrecy rate is possible. Specifically, we treat the relay node as an eavesdropper from whom the source information needs to be kept secret, despite the fact that its cooperation in relaying this information is needed. We find that a positive secrecy rate is indeed achievable, with the aid of the destination node or an external node that jams the relay, i.e., by cooperative jamming. We derive an upper bound on the secrecy rate by means of an eavesdropper-relay separation argument. We remark that this upper bound is the first of its kind in Gaussian channels with cooperative jamming. The upper bound is strictly smaller than the channel capacity without secrecy constraints. The achievable secrecy rates are found using stochastic encoding and compress-and-forward at the relay. Numerical results show that the gap between the bound and the achievable rate is small when the relay's power is larger than the power of the jammer and the source. In essence, this paper shows that a cooperative jammer enables secure communication to take place using an untrusted relay which would be otherwise impossible.**

I. Introduction

Recent advances in wireless ad hoc networking have led to sophisticated physical layer strategies to improve reliable communication rates and range of communication. Many of these approaches rely on cooperation from neighboring nodes in relaying information for source-destination pair(s) [1]. Cooperative communication scenarios typically assume a complete trust between cooperating nodes and allow the information to potentially be decoded at the cooperating nodes. On the other hand, in practice, it is likely to encounter public ad hoc networks where relays needed for connectivity may be unauthenticated despite operating with known protocols. In such cases, secrecy of the information flowing through the relay needs to be guaranteed, despite the fact that the relay is a cooperating node.

It was first recognized in [2] that information transmitted from a source to a destination can be protected from an eavesdropping node -even if it has access to codebooks and has unlimited computational capability- as a consequence of the relative quality of the channels to the legitimate receiver and the eavesdropper. The field of information theoretic secrecy has recently been rejuvenated primarily due to its potential impact on information security for wireless communication scenarios, see for example [3], [4]. The majority of communication models in information theoretic secrecy, including the aforementioned references, assume the existence of an external eavesdropper from whom the information must be kept secret. Reference [5] considers the classical three node relay channel where the relay is treated as the eavesdropper. While the results presented in [5] mostly lead to the conclusion that an untrusted relay should not be employed, recent work showed that in relay channels with orthogonal components, the untrusted relay can help increase the achievable secrecy rates [6], establishing that cooperation is useful even with unauthenticated nodes.

In this work, we consider a communication model in which the assistance of the intermediate relaying node is essential in communication. That is, unlike the classical relay channel, there exists no direct link between the source and the destination. At the same time, the relay node is unauthenticated and we wish to treat it as an eavesdropper. Such a Gaussian relay channel is degraded, and treating the relay as an eavesdropper, the secrecy capacity of this system is zero [5].

While, at the outset, this pessimistic result seemingly closes this problem, in this work, we will show that this is not the case. Specifically, we will show that by enlisting the help of a third party who is friendly, whether it be the destination node itself, or an external node, the secrecy capacity of this two-hop relay network indeed can be made strictly positive.

The technique with which we will accomplish this is "cooperative jamming" [7], which deliberately introduces noise into the communication medium with the intent of hurting the eavesdropper *more* than the legitimate receiver. Cooperative jamming has been used up to date in several single hop problems, including multiple access, two-way and relay wiretap channels [3], [4]. Other recent work that use similar ideas include [8], [9], [10]. In [8], 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 achieved. Reference [10] 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. References [9], [3] consider the case where the destination carries out the jamming. In all these cases, no upper bound on the secrecy rate is known for the Gaussian case.

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

In this work, we derive an upper bound for the secrecy rate of a relay channel, which does not have a direct link but enjoys the help of a cooperative jammer. A key assumption we made is the "independent encoding assumption", which means neither the source nor the jammer uses the signals they received in the past to compute the transmitted signal in the future. This essentially simplifies the system, and is likely representative of a more practical scenario.

Under this assumption, the bound we found is strictly smaller that the capacity without secrecy constraints. We also compare it with the achievable rates based on compress-and-forward at the relay. We find that the gap between the achievable rates and the upper bound becomes smaller as the relay has more power.

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

II. Channel Model

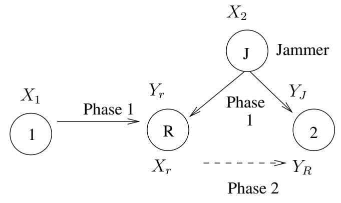

Fig. 1. A Two-Hop Network with a Cooperative Jammer

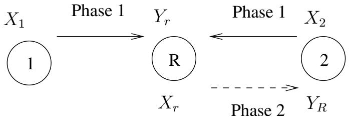

Fig. 2. Cooperative Jammer is co-located with node 2 (destination)

The system model is shown in Figure 1. We assume the nodes are half-duplex and communication takes place over two phases. During the first phase, shown with solid lines, the source transmits. The jammer also transmits in order to confuse the relay node. In the second phase, shown with dashed lines, the relay transmits. The destination (node 2) receives the jamming signal over a noisy channel during the first phase and uses it as side information during phase two to decode the message W. Note that if the destination has perfect knowledge of the jamming signal instead of a noisy one during the first phase, then the channel becomes the two-way relay channel model shown in Figure 2.

Under the independent encoding assumption, Figure 1 can be expressed with the channel model shown in Figure 3. After we normalize the channel gains, the relationship between the transmitted and the received signals is given below:

$$Y_r = X_1 + X_2 + Z_r \tag{1}$$

$$Y_R = X_r + Z_R \tag{2}$$

$$Y_J = X_2 + Z_2 \tag{3}$$

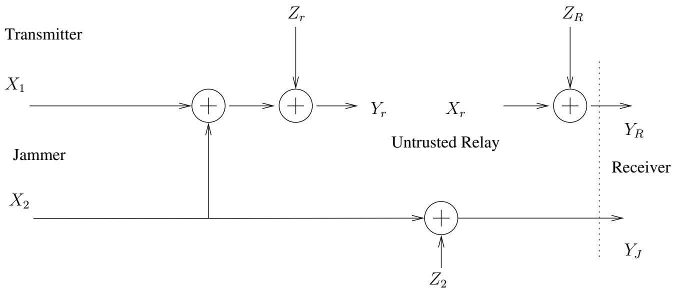

Fig. 3. Equivalent Channel Model for Figure 1.

where $X_i, i = 1, 2$ are signals transmitted by node i; Y_r, X_r are received and transmitted signals by the relay respectively, and Z_2, Z_r, Z_R are independent Gaussian random variables. Z_r, Z_R has unit variance. Z_2 has variance σ_2^2. Y_J, Y_R are signals received by the destination in phase 1 and phase 2 respectively, with Y_J resulting from the jamming signal. We further assume the transmitters have the following power constraints:

$$\frac{1}{n}\sum_{k=1}^{n} E\left[X_{i,k}^2\right] \le P_i, i = 1, 2 \quad \frac{1}{n}\sum_{k=1}^{n} E\left[X_{r,k}^2\right] \le P_r \tag{4}$$

III. Upper Bound on Secrecy Rate

In this section, we derive the upper bound for the secrecy rate of the channel shown in Figure 3. The upper bound is obtained via the following transformation steps:

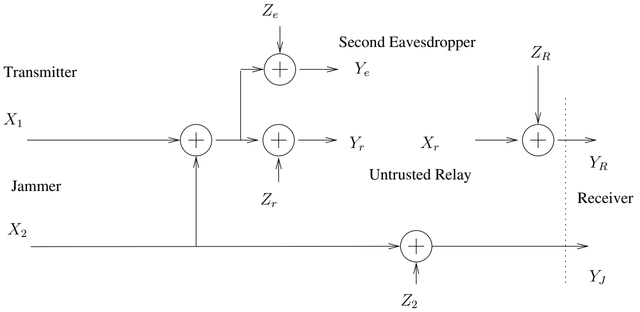

Fig. 4. Two-Eavesdropper Channel

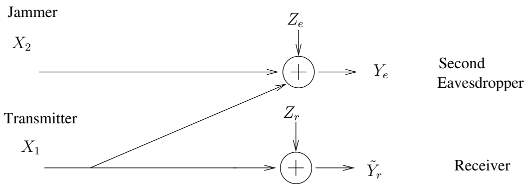

Fig. 5. Channel Model After Transformation

1) First, we add a second eavesdropper to the channel, as shown by Figure 4. Its received signal Y_e is given by $Y_e = X_1 + X_2 + Z_e$. Here Z_e is a Gaussian noise with the same distribution as Z_r. Z_e can be arbitrarily correlated with Z_r. It can be proved by following a

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.

slightly modified version of [11, Theorem 3] that doing so will not decrease the secrecy rate. In essence, this is because any coding scheme that works in the original system will still work in the new two-eavesdropper system.

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.

Remark 1: A key condition for the argument above to work is that the two eavesdroppers cannot hear each other [11]. This argument would not work if the jamming signal X_2 were allowed to depend on the signals received previously. In this case, there would be a feedback link from Y_R to X_2 in Figure 4. The eavesdroppers could hear each other via this feedback link and we would not be able to guarantee that the secrecy rate would not decrease.

Next, the signal X_r^n is provided to the destination by a genie. Similarly, the signal X_2^n is revealed to both the relay and the destination. The secrecy rate is then bounded by:

$$
\begin{aligned}
& H\left(W|Y_e^n\right) \\
\leq & H\left(W|Y_e^n\right) - H\left(W|X_r^n Y_R^n Y_J^n\right) + n\varepsilon && (5)\\
= & H\left(W|Y_e^n\right) - H\left(W|X_r^n Y_J^n\right) + n\varepsilon && (6)\\
\leq & H\left(W|Y_e^n\right) - H\left(W|Y_r^n X_r^n Y_J^n\right) + n\varepsilon && (7)\\
= & H\left(W|Y_e^n\right) - H\left(W|Y_r^n Y_J^n\right) + n\varepsilon && (8)\\
\leq & H\left(W|Y_e^n\right) - H\left(W|Y_r^n X_2^n Y_J^n\right) + n\varepsilon && (9)\\
= & H\left(W|Y_e^n\right) - H\left(W|Y_r^n X_2^n\right) + n\varepsilon && (10)\\
= & H\left(W|Y_e^n\right) - H\left(W|X_1^n + Z_r^n\right) + n\varepsilon && (11)\\
\leq & H\left(W|Y_e^n\right) - H\left(W|Y_e^n, X_1^n + Z_r^n\right) + n\varepsilon && (12)
\end{aligned}
$$

The genie information X_r causes the signal Y_R to be useless to the relay, as shown by (5)-(6). Revealing the genie information X_2 to the relay and the destination essentially removes the influence of the jamming signal from the relay link, as shown by (7)-(12). These are essentially a consequence of the link noises being independent. The resulting channel is equivalent to the one shown in Figure 5. It can be viewed as a special case of the channel in [3], [10], and similar techniques can be used here to bound its secrecy rate. Let $\tilde{Y}_r^n = X_1^n + Z_r^n$. Then we have:

$$
\begin{aligned}
& H\left(W|Y_e^n\right) - H\left(W|Y_e^n \tilde{Y}_r^n\right) = I\left(W; \tilde{Y}_r^n | Y_e^n\right) && (13)\\
\leq & I\left(W X_1^n; \tilde{Y}_r^n | Y_e^n\right) && (14)\\
= & I\left(X_1^n; \tilde{Y}_r^n | Y_e^n\right) && (15)\\
= & h\left(\tilde{Y}_r^n | Y_e^n\right) - h\left(Z_r^n | X_2^n + Z_e^n\right) && (16)\\
\leq & h\left(\tilde{Y}_r^n | Y_e^n\right) - h\left(Z_r^n | X_2^n + Z_e^n, X_2^n\right) && (17)\\
= & h\left(\tilde{Y}_r^n | Y_e^n\right) - h\left(Z_r^n | Z_e^n\right) && (18)
\end{aligned}
$$

Here (15) follows from the fact that X_1^n determines W. The first term in (18) is maximized when X_1^n and X_2^n are i.i.d. Gaussian sequences. Let the variance of each component of X_i^n be P_i,$i = 1, 2$ Let ρ be the correlation factor between Z_r and Z_e. Then (18) is equal to

$$\frac{1}{2}\log_2 \frac{\left(P_1+1\right)\left(P_1+P_2+1\right) - \left(P_1+\rho\right)^2}{\left(P_1+P_2+1\right)\left(1-\rho^2\right)} \tag{19}$$

It can be verified that, for arbitrary ρ, equation (18) is an increasing function of P_1 and P_2. Therefore, the upper bound is maximized with maximum average power. Equation (19) can then be tightened by minimizing it over ρ. The optimal ρ is given below:

$$\frac{2P_1 + P_1P_2 + P_2 - \sqrt{4P_2P_1^2 + 4P_2P_1 + P_2^2P_1^2 + 2P_2^2P_1 + P_2^2}}{2P_1} \tag{20}$$

As a result, we have the following theorem:

Theorem 1: The secrecy rate of the channel in Figure 3 is upper bounded by (19), where ρ is given by (20). P_1 and P_2 are the average power constraints of the transmitter and the jammer.

Remark 2: The bound (19) is strictly smaller than the trivial bound $C(P_1)$ obtained by removing the secrecy constraints. To show that, simply let $\rho = 0$. (19) becomes

$$C\left(P_1\right) + \frac{1}{2}\log_2 \frac{1 + \frac{P_1}{(P_1+1)(P_2+1)}}{1 + \frac{P_1}{(P_2+1)}} \tag{21}$$

The second term is always negative.

Remark 3: Fix P_2, and increase P_1. The bound (19) can be approximated by

$$\frac{1}{2}\log_2\left(\frac{P_2 + 2(1-\rho)}{1-\rho^2}\right) \tag{22}$$

$$\text{where } \rho = 1 + P_2/2 - \sqrt{P_2 + P_2^2/4} \tag{23}$$

On the other hand, if we let $P_2 = cP_1$, and increase P_1 (and hence P_2), then the bound (19) can be approximated by $C(P_1) - C\left(1/c\right)$. In other words, the difference between the bound and its approximation converges to 0 as $P_1 \rightarrow \infty$.

IV. Comparison with Achievable Rates

In this section, we find an achievable secrecy rate and compare it with the upper bound. We begin by considering the general relay channel and then specialize it to the two phase half-duplex model in Figure 2.

Theorem 2: Consider the general relay channel defined by $p(Y_r, Y|X_1, X_2, X_r)$, where X_1, X_2, X_r are the signals transmitted by the source, the jammer, and the relay respectively. Y_r is the signal received by the relay. Y is the signal received by the destination. Then the following secrecy rate is achievable using compress-and-forward:

$$0 \leq R_1 \leq \max_{p(X_1)p(X_2)p(X_r)} \begin{bmatrix} I\left(X_1; Y\hat{Y}_r|X_r\right) \\ -I\left(X_1; Y_r|X_r\right) \end{bmatrix}^+ \tag{24}$$

where $\hat{Y}_r$ is chosen such that $I\left(\hat{Y}_r; Y_r|X_rY\right) < I\left(X_r; Y\right)$

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

Remark 4: The coding scheme is the same as the coding scheme in [6]. The expression is the same except that it is maximized over $p(X_1)p(X_2)p(X_r)$.

For the Gaussian case, we have the following corollary:

Corollary 1: For the channel in Figure 3, the following secrecy rate is achievable:

$$0 \leq R_e \leq \max_{0\leq P_i' \leq P_i, i=1,2} \tag{25}$$

$$\left[C\left(\frac{P_1'}{(1+\sigma_2^2+\sigma_c^2)-\sigma_2^4/\left(P_2'+\sigma_2^2\right)}\right)-C\left(\frac{P_1'}{(1+P_2')}\right)\right]^+$$

$$\text{where } \sigma_c^2 = \frac{P_1'+1+P_2'\sigma_2^2/\left(P_2'+\sigma_2^2\right)}{P_r} \tag{26}$$

Proof: Proof follows from Theorem 2 by replacing Y with Y_J, Y_R. We then have the following facts:

$$I\left(X_1; Y_J Y_R \hat{Y}_r | X_r\right) = I\left(X_1; Y_R \hat{Y}_r | X_r Y_J\right) \tag{27}$$

$$I\left(X_r; Y\right) = I\left(X_r; Y_R Y_J\right) = I\left(X_r; Y_R | Y_J\right) \tag{28}$$

Then letting $X_1 \sim \mathcal{N}(0, P_1')$,$X_2 \sim \mathcal{N}(0, P_2')$, $\hat{Y}_r = Y_r + Z_Q$, $Z_Q \sim \mathcal{N}(0, \sigma_c^2)$, we get the desired result. ■

Remark 5: It can be seen from (26) that 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 infinity, the optimal transmission power is actually finite. Let this value be P_1^*. P_1^* may or may not fall into the interval $[0, P_1]$. 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 6: If the power of the relay $P_r \to \infty$, and the jammer is close to the destination, which means $\sigma_2^2 \to 0$, then the achievable rate converges to

$$C(P_1) - C(\frac{P_1}{1+P_2}) \tag{29}$$

1) If we further fix P_2 , and let $P_1 \to \infty$, then difference of the upper bound and the achievable rate converges to

$$C\left(\frac{P_2 + (\rho-1)^2}{1-\rho^2}\right) - C\left(P_2\right) \tag{30}$$

where ρ is given by (23). We observe that the difference is only a function of P_2. By comparison, the gap between the achievable rate and the trivial upper bound $C(P_1)$ is $C(\frac{P_1}{1+P2})$, which is unbounded.

2) If we instead fix $P_2 = cP_1$, and let $P_1 \to \infty$, then the difference of the upper bound and the achievable rate converges to 0. In this case, our upper bound is asymptotically tight.

	Relay's Power	Jammer's Power
Fig. 6	Large	Proportional
Fig. 7	Large	Fixed
Fig. 8	Limited	Proportional
Fig. 9	Limited	Fixed

TABLE I
SCENARIOS CONSIDERED IN THE NUMERICAL RESULTS

V. NUMERICAL RESULTS

Shown in Table I are the four cases of interest in practice, corresponding to different power budgets of the relay and the jammer. The numerical result of each case is shown in the figure listed in the table. We assume that the jammer and the destination are co-located as shown in Figure 2. For the external cooperative jammer case, the upper bound still holds, but the gap between the upper bound and achievable rates would be wider.

As illustrated by all the four figures, 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. Figure 6 and Figure 7 demonstrate the asymptotic behavior described in Remark 6. 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 (29), equals 9.98×10^{-4} bits/channel use.

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

Figure 8 and Figure 9 demonstrate the behavior of the achievable rates when the relay power is finite. Because the upper bound does not reflect the power of relay, the cut set bound without secrecy constraint is still needed to bound the secrecy rate in these cases. Figure 9 illustrates the power control problem described in Remark 5. 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.

VI. 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

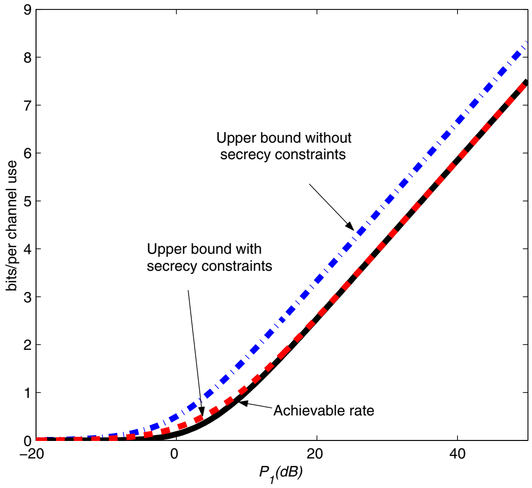

Fig. 6. Secrecy Rates, P_r is ∞,$P_2 = 0.5P_1$

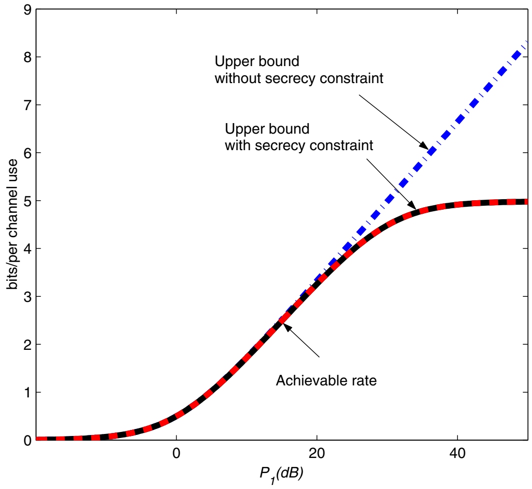

Fig. 7. Secrecy Rates, P_r is ∞,$P_2 = 30$dB

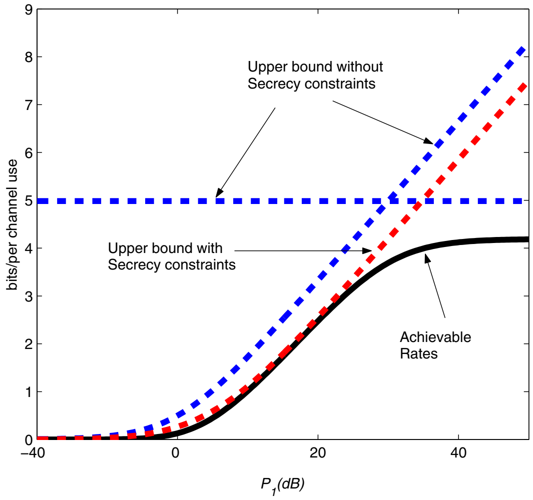

Fig. 8. Secrecy Rates, $P_r = 30$dB $P_2 = 0.5P_1$

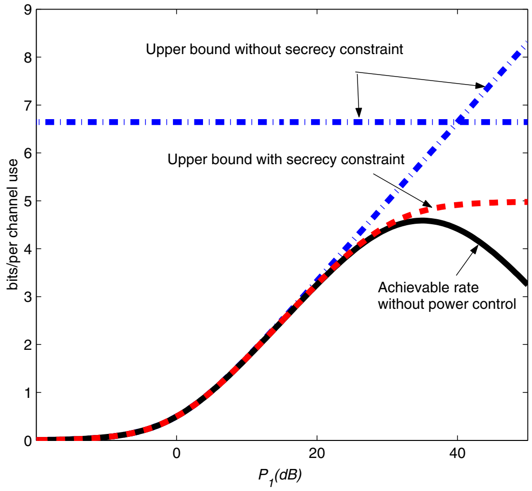

Fig. 9. Secrecy Rates, $P_r = 30$dB, $P_2 = 40$dB

for the secrecy rate under 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. Numerical results show that our upper bound is in general close to the achievable rate, and is indistinguishable from it, when the relay 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. Finding upper bound for the secrecy rate when feedback is used for encoding is of current interest to us. This would serve to quantify the rate loss when feedback is not used for encoding.

References

[1] G. Kramer, M. Gastpar, and P. Gupta. Cooperative Strategies and Capacity Theorems for Relay Networks. *IEEE Transactions on Information Theory*, 51(9):3037–3063, 2005.

[2] A.D. Wyner. The Wire-tap Channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[3] E. Tekin and A. Yener. The General Gaussian Multiple Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, June 2008.

[4] L. Lai and H. El Gamal. The Relay-Eavesdropper Channel: Cooperation for Secrecy. 2006. Submitted to IEEE Transactions on Information Theory.

[5] Y. Oohama. Relay Channels with Confidential Messages. Submitted to IEEE Transactions on Information Theory, 2007.

[6] X. He and A. Yener. On the Equivocation Region of Relay Channels with Orthogonal Components. *Annual Asilomar Conference on Signals, Systems, and Computers*, 2007.

[7] E. Tekin and A. Yener. Achievable Rates for the General Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy. *Allerton Conference on Communication, Control, and Computing*, 2006.

[8] M.L. Jorgensen, B.R. Yanakiev, G.E. Kirkelund, P. Popovski, H. Yomo, and T. Larsen. Shout to Secure: Physical-Layer Wireless Security with Known Interference. *IEEE Global Telecommunication Conference*, 2007.

[9] L. Lai, H. El Gamal, and H.V. Poor. The Wiretap Channel with Feedback: Encryption over the Channel. 2007. submitted to IEEE Transaction on Information Theory.

[10] X. Tang, R. Liu, P. Spasojevic, and H.V. Poor. Interference-Assisted Secret Communication. *IEEE Information Theory Workshop*, 2008.

[11] X. He and A. Yener. Cooperation with an Untrusted Relay: A Secrecy Perspective. 2008. submitted to IEEE Transaction on Information Theory.