On the Role of Feedback in Two-Way Secure Communication

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*—For bi-directional communication, the most general form of encoders should consider the signals received in the past as inputs. However, in practice, it would also be highly desirable if feedback could be ignored for encoding purposes since this would lead to a simple system design. In this work, we investigate the question of whether and how much loss in secrecy rate would be incurred, if such an approach were taken. To do so, we investigate the role of feedback in secrecy for two three-node two-way channel models. First, we show that feedback is indeed *useful* for a class of full-duplex two-way wire-tap channels. In this case, when feedback is ignored, the channel is equivalent to a Gaussian degraded relay channel with confidential messages to the relay. The usefulness of feedback is demonstrated by deriving an upper bound for this channel when feedback is ignored, and then proving that, when feedback is used, a secrecy rate higher than this upper bound is achievable. Secondly, we consider the half-duplex Gaussian two-way relay channel where there is an eavesdropper co-located with the relay node, and find that the impact of feedback is less pronounced compared to the previous scenario. Specifically, the loss in secrecy rate, when ignoring the feedback, is quantified to be less than 0.5 bit per channel use when the power of the relay goes to infinity. We also show that this rate region is achievable under a simple time sharing scheme with cooperative jamming, which, with its simplicity and near-optimum performance, is a viable alternative to an encoder using feedback.**

I. Introduction

Most communication links are bi-directional. In secure communication, the benefit of having a secure reverse link were previously shown in several cases. In [1], Shannon showed a secure reverse link can be be used to send a key termed one-time pad to increase the secrecy capacity of the forward link. The same idea was extended to prove achievability results for the wire-tap channel with rate limited feedback link in [2] and [3]. References [4], [5] provided a scheme for channels with binary symmetric links.

One common feature shared by the channel models of all these works is that the feedback link is orthogonal to the forward link. In most wireless systems, this is achieved via sharing in time or frequency. On second thought however, it could be overly optimistic to assume that the eavesdropper only monitors time slots or frequency bands corresponding to the traffic in one direction and completely ignores the other. Also, separating these two flows artificially, might inadvertently give the eavesdropper an advantage, as compared to superimposing them together. Alternatively, when flow separation is not done, introducing artificial noise into the system via cooperative jamming has been shown to improve secrecy rates in the two-way communication against an external eavesdropper [6]. Yet in reference [6], feedback is ignored for encoding purposes.

In light of these works, it is important to consider “cooperative jamming” and feedback together when the fundamental information theoretic limit of bi-directional communication is of interest. In this work, we focus on two models where both techniques are potentially useful: (i) a class of Gaussian full-duplex two-way wire-tap channels, (ii) the Gaussian half-duplex two-way relay channel with an untrusted relay.

For the first model, if the feedback is ignored at one node, the model becomes the relay channel with confidential message to the relay [7]. We focus on the case where the relay channel is physically degraded and derive a computable upper bound. This upper bound, derived when feedback is ignored, is then shown to be smaller than the achievable rate when feedback is used. Hence, we prove that ignoring feedback is strictly suboptimal for this channel.

For the second model, we prove that if the power of the relay goes to ∞, then the loss of ignoring the feedback is bounded by 0.5 bit per channel use. Interestingly, a simple TDMA scheme with cooperative jamming yields the achievable rate, contrary to the case without any eavesdropper, where compute and forward is shown to be a superior scheme [8].

We emphasize that the key to the approach we used in deriving the outer bounds in this work is to recognize cooperative jamming as a special form of feedback, except that the feedback functionality exists physically in the channel rather than the node.

Finally, the notation $C(x) = \frac{1}{2}\log_2(1+x)$ is used throughout this work.

II. Preliminary Results

In this section, we list some results that are used extensively in the sequel. Proofs are given in [9] and are omitted here due to the space limitation.

A. A $\frac{1}{2}$ Bit Result

Lemma 1:

$$f(x,y) = \frac{1}{2}\log_2\left(\frac{(1+x)(1+y)}{1+x+y}\right) \tag{1}$$

978-1-4244-2941-7/08/$25.00 ©2008 IEEE

$$g(x,y) = \min\{C(x), C(y)\} \tag{2}$$

Then $0 \le g(x,y) - f(x,y) \le 0.5$.

B. A Noiseless Wire-Tap Channel with Noisy Feedback

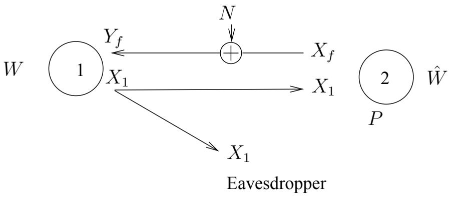

Fig. 1. The theoretical channel model with feedback

Consider a noiseless wire-tap channel with noisy feedback, shown in Figure 1. In this model, which is of theoretical interest, node 1 wants to sent a secret message W to node 2. The forward link is noiseless. Hence the eavesdropper has perfect knowledge of the signal sent by the transmitter. The backward link is a noisy channel defined as $Y_f = X_f + N$, where N is a zero mean Gaussian noise with unit variance.

The average power constraint of node 2 is P. Node 1 is not power constrained.

The stochastic encoding function at node 1 is defined as

$$X_{1,i} = h_i(X_1^{i-1}, Y_f^i, W) \tag{3}$$

Node 2 uses a stochastic feedback function defined as

$$X_{f,i} = g_i(X_f^{i-1}, X_1^{i-1}) \tag{4}$$

We assume node 2 talks first while node 1 listens. Next, node 1 talks and node 2 listens. Therefore, node 1 always has one more sample available when it computes its transmission signal $X_{1,i}$, which leads to Y_f^i on the right hand side of (3) instead of Y_f^{i-1}.

Since the eavesdropper receives X_1^n, the secrecy constraint of this model is defined as

$$\lim_{n\to\infty} \frac{1}{n} H\left(W|X_1^n\right) = \lim_{n\to\infty} \frac{1}{n} H\left(W\right) \tag{5}$$

The destination knows X_1^n and X_f^n. From Fano's inequality, reliable transmission dictates:

$$H\left(W|X_f^n, X_1^n\right) < n\varepsilon \tag{6}$$

where $\varepsilon > 0$, $\lim_{n\to\infty} \varepsilon = 0$.

The source node knows Y_f^n and X_1^n. From (6), it can be shown the following lemma holds [9]:

Lemma 2: Equation (6) implies $H\left(W|Y_f^n, X_1^n\right) < n\varepsilon$

Remark 1: Lemma 2 says for any coding scheme that reliably transmits message W, it also conforms to the secret key generation protocol defined in [4], because both nodes can determine W almost surely from the signals available to them. Suppose a secret key rate is achievable, then, because of the existence of infinite rate public forward channel in this model, the key can be used to transmit secret message over the forward channel with arbitrarily small number of channel uses. Therefore, for this channel, the upper bound for the secret key capacity given by [4] is also an upper bound for the secrecy capacity. The channel defined by the probability distribution $p(Y,Z|X)$ in [4] corresponds to $p(Y_f|X_f)$. The forward link here corresponds to the public discussion link in [4]. The upper bound for the secrecy rate follows immediately from the upper bound for the secrecy key capacity in [4] as $I(X_f, Y_f) = C(P)$. This is stated as the following theorem:

Theorem 1: The secrecy capacity of the model in Figure 1 is bounded by $C(P)$.

III. Feedback in Full Duplex Two-way Wire-Tap Channel

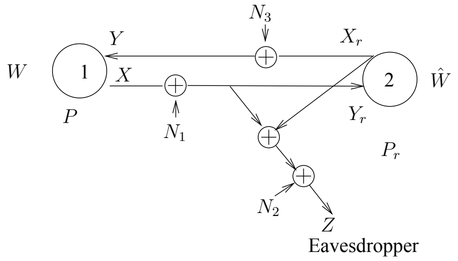

Fig. 2. The degraded two-way wire-tap channel

The two way wire-tap channel we consider is shown in Figure 2. The forward link can be expressed as:

$$Y_r = X + N_1 \tag{7}$$

The backward link is defined as:

$$Y = X_r + N_3 \tag{8}$$

The signal received by the eavesdropper is:

$$Z = X + X_r + N_1 + N_2 \tag{9}$$

where N_1, N_2, N_3 are independent zero mean Gaussian random variables. $E[N_1^2] = 1$. $E[N_i^2] = \sigma_i^2, i = 2, 3$.

Unlike the channel model in section II-B, we assume node 1 and node 2 transmit simultaneously at each time slot, so that node 2 can jam the eavesdropper and protect the secret message transmitted by node 1. The average transmission power constraints of node 1 and node 2 are P and P_r respectively.

A. Upper bound of Secrecy Rate when Feedback is Ignored

When the feedback Y is ignored by the source node, the channel is the same as a physically degraded Gaussian relay channel, where node 2 corresponds to the relay node, the eavesdropper corresponds the destination. The secret message W is transmitted from node 1 to node 2 rather than to the destination, hence we have a relay channel with confidential messages to the relay.

When feedback is ignored at node 1, the stochastic encoding function at node 1 is simply:

$$X_i = t_i\left(X^{i-1}, W\right) \tag{10}$$

The stochastic relaying function at node 2 is: $X_{r,i} = f_i\left(X_r^{i-1}, Y_r^{i-1}\right)$. The secrecy rate for this case can be upper bounded by the following theorem:

Theorem 2: The secrecy rate of the channel in Figure 3 is bounded by $\min\{C(P), C(\bar{P}_r)\}$, where $\bar{P}_r = P_r + \sigma_2^2$.

Proof: The first term $C(P)$ follows by removing the eavesdropper. In order to obtain the second term, we consider the network in Figure 3. In this new model, N_2 is removed but the power constraint of node 2 is increased from P_r to $\bar{P}_r = P_r + \sigma_r^2$. It is easy to see that the secrecy capacity of this model is greater or equal to the secrecy capacity of the degraded Gaussian channel.

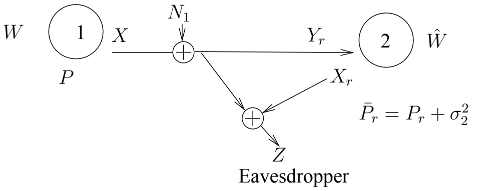

Fig. 3. The model with cooperative jamming

We next prove that under the same power constraint, the secrecy capacity of the model in Figure 1 must be greater or equal to the secrecy capacity of the channel model in Figure 3. The theorem then follows from Theorem 1. In the remaining part of this proof, we call Figure 1 the *feedback model*, and Figure 3 the *jamming model*. We prove that any signaling scheme in the jamming model can be simulated by the feedback model.

First, we choose the feedback function g_i in the feedback model as $X_{f,i} = f_i(X_f^{i-1}, X_1^{i-1} - X_f^{i-1})$. The encoding function in the feedback model h_i is chosen to be:

$$X_{1,i} = Y_{f,i} + t_i\left(X^{i-1}, W\right) \tag{11}$$

where X^{i-1} is governed by (10).

It can be verified that, for any $i > 1$, if $X_f^{i-1} = X_r^{i-1}$, then $X_{f,i} = X_{r,i}$. Using this result, from (11) we have

$$\begin{aligned} X_{1,i} &= X_{f,i} + N_i + t_i\left(X^{i-1}, W\right) && (12)\\ &= X_{r,i} + N_{1,i} + t_i\left(X^{i-1}, W\right) = Z_i && (13)\end{aligned}$$

Therefore the signals received by the eavesdropper in these two models are identical.

The destination in the feedback model knows $X_{f,i}$. Therefore, it can compute $t_i\left(X^{i-1}, W\right) + N_i$ from $X_{1,i} - X_{f,i}$ which is the signal received by node 2 in jamming model. This, along with the fact $X_{r,i} = X_{f,i}$, tells us that the destination in the feedback model can compute any signals known by the destination in the jamming model. This means, if W can be reliably received in the jamming model, it can also be reliably received in the feedback model. Hence we have the theorem. ■

Remark 2: If node 2 transmits i.i.d. Gaussian noise to jam the eavesdropper, then a secrecy rate of $C(P) - C(P/\bar{P}_r)$ is achievable. From Lemma 1, we see the gap between this achievable rate and the upper bound given by Theorem 2 is less than 0.5 bit per channel.

Remark 3: The relay channel with confidential message to the relay can be viewed as a special case of the model studied in [7], where the secrecy rate to use 2 is 0. An upper bound for the general discrete memoryless relay channel was derived therein. In Theorem 2 we provided a computable upper bound for the degraded Gaussian case.

B. Achievable Secrecy Rate when Feedback is Used

We next provide an achievable secrecy rate when the feedback at node 1 is used for encoding purpose.

Theorem 3: The following secrecy rate is achievable.

$$\begin{aligned} 0 \le R_e \le \frac{1}{2}[C(P)-\\ [C(\frac{P}{P_r + \sigma_2^2}) - [C(\frac{P_r}{\sigma_3^2}) - C(\frac{P_r}{P + \sigma_2^2})]^+]^+]^+ \end{aligned} \tag{14}$$

The complete proof is given in [9]. Briefly, the achievable scheme is as follows. The communication is divided into two phases. During the first phase, node 2 sends a key K to node 1. The rate of the key is chosen to be $[C(\frac{P_r}{\sigma_3^2}) - C(\frac{P_r}{P+\sigma_2^2})]^+$. At the same time, node 1 performs cooperative jamming. During the second phase, node 1 encrypts its data W with this key K, and sends the result back to node 2. At the same time, node 2 does cooperative jamming.

Remark 4: It is easy to see that for certain channel parameters, the achievable rate given by Theorem 3 can be greater than the upper bound given by Theorem 2. This shows the necessity of using feedback in encoder design at node 1. Consider, for example, the case $C(\bar{P}_r) < 0.5C(P)$. The upper bound then becomes $C(\bar{P}_r)$. We know that, there must exist a σ_3^2 small enough to drive the achievable rate in (14) to $0.5C(P)$, which is larger than the upper bound. That is to say, if the channel condition from node 2 to node 1 is good, the signal received by node 1 should not be ignored.

IV. Feedback in Half Duplex Two-way Relay Channel with An Untrusted Relay

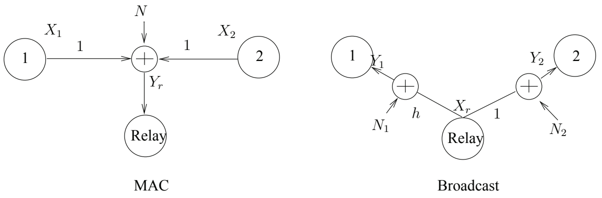

Fig. 4. Gaussian two-way half-duplex relay channel with untrusted relay

The Gaussian half-duplex two-way relay channel is shown in Figure 4. At any time slot, the channel either behaves as a MAC channel, shown on the left, or as a broadcast channel, shown on the right. After normalizing the channel gains, the MAC channel can be expressed as: $Y_r = X_1 + X_2 + N$ The broadcast channel can be expressed as: $Y_1 = hX_r + N_1$, $Y_2 =$

$X_r + N_2$, where h is the channel gain. $h \neq 0$, and N, N_1, N_2 are zero mean Gaussian random variables with unit variance.

Like in Section III, we assume node 1 and node 2 transmit simultaneously during the MAC phase. We use $X_{j,i}, j = 1, 2$ to denote the set of signals transmitted by node j during the ith time $i \geq 1$ that the channel is under MAC mode. The notation X_j^i denotes the set of signals: $\{X_{j,k}, k = 1...i\}$. Similarly $X_{r,i}$ denotes the set of signals transmitted by the relay node during the ith time $i \geq 1$ that the channel is under broadcast mode. $Y_{1,i}, Y_{2,i}, Y_{r,i}$ are sets of received signals defined in the same fashion.

The channel switches between MAC and broadcast mode according to a globally known schedule. We assume the schedule is independent from the stochastic encoders, the message, or the channel noise. The first mode is MAC. [1]

Suppose the MAC mode is activated $\bar{n}$ times, lasting n channel uses. The broadcast mode is activated $\bar{m}$ times, lasting m channel uses. Overall, $n + m$ time slots are used. The time sharing factor α is then computed as $\alpha = \frac{n}{m+n}$. $\bar{\alpha} = 1 - \alpha$.

After normalization, the average power constraints of node $1, 2$ over the MAC mode are $P_1 = \bar{P}_1/\alpha$, $P_2 = \bar{P}_2/\alpha$ respectively. The average power constraint of the relay over the broadcast mode is $P_r = \bar{P}_r/\bar{\alpha}$.

Let W_1 be the secret message from node 1 to node 2. Let W_2 be the secret message from node 2 to node 1.

For the ith MAC mode, the stochastic encoding functions at node 1 $f_{1,i}$ are defined as: $X_{1,i} = f_{1,i}(Y_1^{i-1}, W_1, X_1^{i-1})$ Similarly, the stochastic encoding functions at node 2 $f_{2,i}$ are defined as: $X_{2,i} = f_{2,i}(Y_2^{i-1}, W_2, X_2^{i-1})$. If the ith MAC mode involves multiple channel uses, then the functions $f_{1,i}, f_{2,i}$ are vector valued.

Without loss of generality, the stochastic relay functions at node 3 $\{g_i, C_i\}$ are defined as: $X_{r,i} = g_i(Y_r^{i-1}, X_r^{i-1}, C_i)$, where g_i is a deterministic function. $\{C_i\}$ is a sequence of random variables which models the stochastic mapping.

The secrecy constraint is expressed as

$$\begin{aligned} &\lim_{m,n\to\infty} \frac{1}{m+n} H(W_1, W_2 | Y_r^{\bar{n}}, X_r^{\bar{m}}) \\ &= \lim_{m,n\to\infty} \frac{1}{m+n} H(W_1, W_2) \end{aligned} \tag{15}$$

The secrecy rate R_1, R_2 is defined as

$$R_j = \lim_{m,n\to\infty} \frac{1}{n+m} H(W_j), j = 1, 2 \tag{16}$$

when W_j can be transmitted reliably. The secrecy capacity region is defined as all achievable rate pairs (R_1, R_2) that satisfy (15).

In order to bound the secrecy rate region of this channel, we consider the channel in Figure 5. X_1 and X_2 have the same power constraint as the X_1, X_2 in Figure 4.

First, the public link is activated, which sends out the stochastic mapping C_i used at the relay. The encoding function at the public forward link is defined as follows: $C_i = q_i(C^{i-1})$.

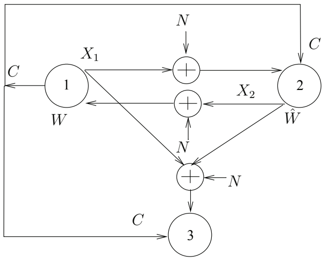

Fig. 5. Two way wire-tap channel with public noiseless forward link

The rest part of the channel is activated next for the same number of time slots when the original channel is under MAC mode. After that, the nodes remain silent for the time slots when the original two-way relay channel model is under broadcast mode. Doing so ensures the overall number of channel uses to be the same between these two models. Under these assumptions, we have the following theorem:

Theorem 4: The secrecy rate region of the channel in Figure 5 includes the secrecy capacity region of the two way relay channel in Figure 4.

The proof is given in [9]. The key is to provide the received signal of the relay and its stochastic mapping to nodes $1, 2$ as genie information.

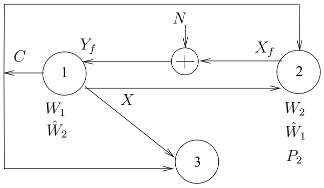

Fig. 6. Two-way model with one-sided secure link

Next, we consider the channel in Figure 6. We assume this channel is activated in the same way in that it is silent if the original channel model is in broadcast mode. Under this assumption, we have the following theorem:

Theorem 5: The secrecy capacity region of the channel in Figure 6 under a serial protocol where node 2 talks first includes the secrecy rate region of the channel in Figure 5.

The proof is given in [9]. Like in Theorem 2, the essence of the proof comes from showing the channel in Figure 6 can simulate the channel in Figure 5.

Theorem 6: An outer bound for the secrecy capacity region of the channel in Figure 6 is given by

$$R_1 + R_2 \leq \alpha C\left(P_2\right), \quad R_i \geq 0, i = 1, 2 \tag{17}$$

Proof: We first prove the following result: For the channel in Figure 6, any bound on R_1 is a bound on $R_1 + R_2$. We prove this statement by showing if $R_1 = r_1, R_2 = r_2$ is achievable, then $R_1 = r_1 + r_2$ is also achievable.

[1] The case where the first mode is a broadcast mode can be viewed as a special case of invoking MAC mode first by transmitting nothing during the first MAC mode. The rate loss caused by the wasted channel uses is negligible as the number of channel uses goes to ∞.

Construct a message set $\{W_a\}$ which has the same cardinality of the message set $\{W_2\}$. Let part of the secret message be transmitted via W_a, and the remaining part of the secret message be transmitted via W_1. The role of W_2 is serving as the secret key. Let W_2 be taken from the set $\{W_2\}$ under a uniform distribution. W_2 is independent from W_a and W_1.

Let $\oplus$ be the modulus addition defined over $\{1, ... \|W_2\|\}$. Node 1, after decoding W_2, transmits $W_2 \oplus W_a$ over the public channel. Since the public channel is noiseless with continuous input, it can transmit $W_2 \oplus W_a$ with less than n channel uses. Because node 2 knows W_2, it can recover W_a from $W_2 \oplus W_a$.

The signal available to the eavesdropper now becomes the output of the wiretap channel X^n, and the output of the public link $W_a \oplus W_2$. Conditioned on these signals, the equivocation of W_1, W_a can be computed as:

$$H\left(W_1, W_a | X^n, W_a \oplus W_2\right) \tag{18}$$

$$= H\left(W_a | X^n, W_a \oplus W_2\right) + H\left(W_1 | X^n, W_a, W_a \oplus W_2\right) \tag{19}$$

$$= H\left(W_a | X^n, W_a \oplus W_2\right) + H\left(W_1 | X^n, W_a, W_2\right) \tag{20}$$

$$= H\left(W_a | W_a \oplus W_2\right) + H\left(W_1 | X^n, W_a, W_2\right) \tag{21}$$

$$= H\left(W_a | W_a \oplus W_2\right) + H\left(W_1 | X^n, W_2\right) \tag{22}$$

$$= H\left(W_a\right) + H\left(W_1 | X^n, W_2\right) \tag{23}$$

$$\geq H\left(W_a\right) + H\left(W_1\right) - n\varepsilon \tag{24}$$

$$\geq H\left(W_1, W_a\right) - n\varepsilon \tag{25}$$

Equation (21) follows from the fact that X^n is independent from W_a, W_2. Equation (22) follows from the fact that W_a is independent from X^n,W_1,W_2. Equation (24) follows from the fact that collective secrecy implies one message is secure even if the other message is revealed to the eavesdropper [6].

The argument above shows the rate of W_1, W_a is the secrecy rate R_1. Since W_a is chosen from the message set $\{W_a\}$ under a uniform distribution, we have $R_1 = r_1 + r_2$.

From Lemma 1, we know $R_1 \leq \alpha C(P_2)$, hence, by the preceding argument, we have $R_1 + R_2 \leq \alpha C(P_2)$. This completes the proof. ■

Theorem 6 leads to our main result [9]:

Theorem 7: Define region $\mathbf{A}$ as

$$R_1 + R_2 \leq \alpha \min\left\{C\left(\bar{P}_1/\alpha\right), C\left(\bar{P}_2/\alpha\right)\right\} \tag{26}$$

Define region $\mathbf{B}$ as

$$0 \leq R_1 \leq \bar{\alpha} C(\bar{P}_r/\bar{\alpha}), 0 \leq R_2 \leq \bar{\alpha} C(h^2 \bar{P}_r/\bar{\alpha}) \tag{27}$$

An outer bound for the secrecy capacity of two way relay channel is given by $\cup_{0 \leq \alpha \leq 1}\{\mathbf{A} \cap \mathbf{B}\}$.

Remark 5: When $\bar{P}_r \to \infty$, and $h \neq 0$, then the region is maximized when $\alpha \to 1$. The outer bound becomes:

$$R_1 + R_2 \leq \min\left\{C\left(\bar{P}_1\right), C\left(\bar{P}_2\right)\right\}, R_i \geq 0, i = 1, 2 \tag{28}$$

A. Comparison with Achievable Rates

In this section, we derive the achievable secrecy rate region. We begin by deriving the achievable region for R_1. The whole region then follows from time sharing.

Lemma 3:

$$0 \leq R_1 \leq \max_{0 \leq P_1' \leq \bar{P}_1/\alpha} \alpha \left[C\left(\frac{P_1'}{(1+\sigma_c^2)}\right) - C\left(\frac{P_1'}{(1+\bar{P}_2/\alpha)}\right)\right]^+ \tag{29}$$

where $\sigma_c^2 = \frac{P_1'+1}{\bar{P}_r/\bar{\alpha}}$
The proof is given in [9]. The relay node performs compress-and-forward while node 2 performs cooperative jamming by transmitting an i.i.d. Gaussian sequence.

Remark 6: If the power of the relay $\bar{P}_r \to \infty$, then $\alpha \to 1$, the achievable rate converges to $C(\bar{P}_1) - C(\frac{\bar{P}_1}{1+\bar{P}_2})$. The secrecy rate region is obtained with time sharing and it converges to $R_1 + R_2 \leq C(\bar{P}_1) - C(\frac{\bar{P}_1}{1+\bar{P}_2})$, $R_i \geq 0, i = 1, 2$. Compared it with the outer bound, using Lemma 1, we notice the gap between the upper bound and lower bound is less than 0.5 bit per channel use.

V. Conclusion

In this work, we have investigated the relationship between two important techniques to achieve secrecy: cooperative jamming and feedback. The former is usually regarded as a "keyless" technique, while the latter is typically used to send the "secret key". In this work, we showed that these two techniques are not so different from each other after all: Cooperative jamming can be viewed as a special case of feedback, except that the feedback functionality is performed by the channel itself. Recognizing this relation enables us to investigate the necessity of using feedback for encoding in two models: (i) a class of Gaussian full-duplex two-way wiretap channel, where use of feedback is found to be indeed beneficial; (ii) the Gaussian half-duplex two-way relay channel with untrusted relay, where feedback can be safely ignored, if the power of the relay is abundant.

References

[1] C. E.. Shannon. *Communication Theory and Secrecy Systems*. Bell Telephone Laboratories, September 1949.

[2] E. Ardetsanizadeh, M. Franceschetti, T. Javidi, and Y.H. Kim. Wiretap Channel with Rate-limited Feedback. *IEEE International Symposium on Information Theory*, July 2008.

[3] D. Gunduz, D. R. Brown III, A. Goldmith, and H. V. Poor. Secrecy Capacity of Wiretap Channels with Noisy Feedback. 2008. http://spinlab.wpi.edu/publications.html.

[4] U. M. Maurer. Secret Key Agreement by Public Discussion from Common Information. *IEEE Transactions on Information Theory*, 39(3):733–742, May 1993.

[5] G. T. Amariucai and S. Wei. Strictly Positive Secrecy Rates of Binary Wiretapper Channels Using Feedback Schemes. *Annual Conference on Information Sciences and Systems*, March 2008.

[6] 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.

[7] E. Ekrem and S. Ulukus. Secrecy in Cooperative Relay Broadcast Channels. *IEEE International Symposium on Information Theory*, July 2008.

[8] B. Nazer and M. Gastpar. The Case for Structured Random Codes in Network Capacity Theorems. *European Transactions on Telecommunications, Special Issue on New Directions in Information Theory*, 19(4):455–474, June 2008.

[9] X. He and A. Yener. The Role of Feedback in Two-Way Secure Communication. Submitted for publication. Available at http://labs.ee.psu.edu/labs/wcan, 2008.