This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings

A New Outer Bound for the Secrecy Capacity Region of the Gaussian Two-Way Wiretap Channel

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 investigate the fundamental communication limits when messages are sent via a Gaussian two-way channel, which must at the same time be kept secret from an external eavesdropper. In this two-way wiretap channel that models two legitimate transceivers and an eavesdropping receiver, there are two techniques to provide confidentiality for the messages: one entails the legitimate nodes to jam the eavesdropper, i.e., cooperative jamming, while the other entails generating keys from the feedback signals received by the two legitimate nodes and using them to encrypt the messages. Previous work has shown that both methods can be used concurrently to improve the secrecy rates of a channel with a degradedness condition. In this work, we consider the general case, and derive a new outer bound for the secrecy capacity region of this channel. A case is identified where the loss in secrecy rate, due to ignoring the backward (feedback) link at each legitimate transmitter from the other, is bounded by a constant which only depends on the channel gains. This is the case when the power of the two legitimate nodes increases proportionally. In all other cases, we show that ignoring feedback signals causes unbounded loss in the secrecy rate. The loss is measured as the gap between the achievable rate when the feedback signals are taken into account, and the upper bound when the feedback is not used, and hence is not affected by the choice of the achievable scheme. This result therefore establishes that, for the Gaussian two-way channel with an external eavesdropper, the encoders need to be designed with memory. This is in contrast to the result for this channel in the absence of an eavesdropper.**

I. Introduction

The notion of information theoretic secrecy was first proposed by Shannon in [1], which can be used to study the fundamental limits of reliable transmission rates when the message must be kept secret from an eavesdropper with unbounded computation power. Wyner studied the wiretap channel in [2] using this notion and showed that the characteristics of the underlying communication channel can help limit the information leaked to the eavesdropper and provide a secure rate guarantee.

This approach is recently taken to study a number of more sophisticated models. The most relevant work to this one is [3], which proposed the Gaussian two-way wiretap channel studied in this work. In this model, two transceivers exchange messages via a Gaussian two-way channel [4]. An eavesdropper has access to a noisy version of the sum of the channel inputs of the two transceivers. To protect the messages from being leaked to the eavesdropper, there are two methods the transceivers can use. We can ask one transceiver to transmit noise to jam the eavesdropper. We can also generate keys from the feedback signals received by the transceivers and use these keys to encrypt the messages. The first method, called cooperative jamming, is clearly effective in this model. However, whether it is necessary to use the second method is less clear, as its merit has only been established for models where the first method is not useful [5]–[7]. Moreover, it is known that, for a Gaussian two-way channel in the absence of eavesdroppers, the signals received by the transceivers are not needed for computing the transmitted signals [8]. Guided by these intuitions, most previous efforts on this model focus on studying the secrecy capacity when the channel is restricted to using the first method only. Reference [3] derived the achievable rate region of the model with cooperative jamming only. When only one node has a message to send, a computable upper bound on the secrecy rate was derived in [9] for a degraded case and recently in [10] for the general case. Again, both bounds only apply in the case where the sender of the message ignores all its received signals.

An insight obtained by [9] is that for the degraded case, it is actually possible to achieve a higher secrecy rate when the source node utilizes its received signals to encrypt its message, than the upper bound obtained without utilizing these signals. This result establishes the necessity of using both methods *concurrently* in the degraded case to achieve the secrecy capacity. Yet, it remains unclear if this is true for the general case. In addition, to justify the additional complexity at the source node required by using both methods, it is desirable to quantify the potential gain in secrecy rate from this approach. To answer these questions, clearly, we need an computable outer bound for the secrecy capacity region of this model when there is no restriction on the methods used by the transceivers.

The main contribution of this work is the derivation of this outer bound. The bound is applicable regardless of whether the two legitimate nodes utilizes the received signals to compute their transmitted signals, hence it is more general compared with all existing bounds. By comparing the bound with the achievable rate region, we identify one case where the impact is limited on the secrecy rates when the feedback signals are ignored by the transmitters. Specifically, when the channel is fully connected with independent link noise, the rate achieved using only cooperative jamming is within a constant from the

978-1-4244-6404-3/10/$26.00 ©2010 IEEE

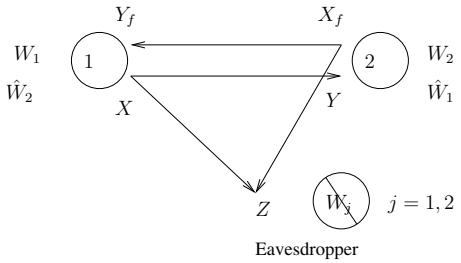

Fig. 1. Two-way wiretap channel

outer bound, if the powers of the two legitimate nodes increase proportionally. The constant is only a function of the channel gains. However, more strikingly, we prove that, in other cases, the loss caused by ignoring these feedback signals can be an unbounded function of the transmission power. Therefore, we conclude that utilizing feedback signals in the Gaussian two-way wiretap channel can be immensely beneficial in general.

Throughout the paper the notation $C(x)$ is defined as $C(x) = \frac{1}{2}\log_2(1+x)$. x_i denotes the ith component of vector x, while x^i denotes $\{x_1, ...x_i\}$.

II. System Model

The channel model is shown in Figure 1. The channel transitional probability is given by

$$\Pr(Z|X, X_f)\Pr(Y|X, X_f, Z)\Pr(Y_f|X_f, X, Z) \quad (1)$$

Let M_j represent the local randomness at node j. At the ith channel use, the encoding function of Node 1 is defined as:

$$X_i = f_i(Y_f^{i-1}, W_1, M_1) \quad (2)$$

The encoding function of Node 2 is defined as

$$X_{f,i} = g_i(Y^{i-1}, W_2, M_2) \quad (3)$$

Note that, since we have $M_j, j = 1, 2$, f_i and g_i are deterministic encoders.

Let n be the total number of channel uses. Node 2 must decode W_1 reliably from X_f^n, Y^n, M_2, W_2. Node 1 must decode W_2 reliably from Y_f^n, X^n, M_1, W_1. Let the decoder outputs be $\hat{W}_1$ and $\hat{W}_2$ respectively. Thus, we require

$$\lim_{n\to\infty} \Pr(W_j \neq \hat{W}_j) = 0, \quad j = 1, 2 \quad (4)$$

From Fano's inequality, this means:

$$H(W_1|X_f^n, Y^n, M_2, W_2) < n\varepsilon_1 \quad (5)$$

$$H(W_2|Y_f^n, X^n, M_1, W_1) < n\varepsilon_2 \quad (6)$$

where $\varepsilon_j > 0$ and $\lim_{n\to\infty} \varepsilon_j = 0$, $j = 1, 2$.

Both messages must be kept secret from the eavesdropper. Hence

$$I(W_1, W_2; Z^n) < n\varepsilon_3 \quad (7)$$

where $\varepsilon_3 > 0$ and $\lim_{n\to\infty} \varepsilon_3 = 0$.

Define $R_j, j = 1, 2$ as $\lim_{n\to\infty} \frac{1}{n} H(W_j)$. The secrecy capacity region is defined as all rate pairs $\{R_1, R_2\}$ for which (4) and (7) hold.

The Gaussian two-way wiretap channel model was first proposed in [3] and is defined as:

$$Y_f = X_f + N_3 + \sqrt{\alpha}X, \quad Y = X + N_1 + \sqrt{\beta}X_f \quad (8)$$

$$Z = \sqrt{h_1}X + \sqrt{h_2}X_f + N_2 \quad (9)$$

where $\sqrt{\alpha}, \sqrt{\beta}, \sqrt{h_1}, \sqrt{h_2}$ are channel gains. $N_i, i = 1, 2, 3$ are Gaussian random variables with zero mean and unit variance, representing the channel noise. We assume that given N_2, N_1 is independent from N_3:

$$p(N_1, N_2, N_3) = p(N_2)p(N_1|N_2)p(N_3|N_2) \quad (10)$$

We use ρ to denote the factor between N_1 and N_2. Similarly, η denotes the correlation between N_2 and N_3. Hence $-1 \leq \rho, \eta \leq 1$. From (1) and (10), we observe that the channel is a special case of the channel model in Figure 1.

Let the power constraint of Node 1 be P. Let the power constraint of Node 2 be P_r.

$$\frac{1}{n}\sum_{k=1}^{n} E\left[X_k^2\right] \leq P, \quad \frac{1}{n}\sum_{k=1}^{n} E\left[X_{f,k}^2\right] \leq P_r \quad (11)$$

Remark 1: When Y_f is ignored by Node 1, the channel becomes the so-called "relay channel with a confidential message to the relay", which was considered in [10], [11]. □

III. Outer Bounds

Theorem 1: For the channel model in Figure 1, R_1 is upper bounded by

$$\max_{\Pr(X,X_f)} \min\{I(X;Y), I(X;Y|Z,X_f) + I(X_f;Y_f,Z|X)\} \quad (12)$$

Proof: The proof is provided in Appendix A. ■

Remark 2: Ignoring Y_f at Node 1 is equivalent to viewing Y_f as a constant. From (12), R_1 in this case is upper bounded by

$$\max_{\Pr(X,X_f)} \min\{I(X;Y), I(X;Y|Z,X_f) + I(X_f;Z|X)\} \quad (13)$$

which is the upper bound in [10]. □

Corollary 1: The secrecy capacity region of the channel model in Figure 1 is bounded by

$$\cup_{\Pr(X,X_f)} \{(R_1, R_2) : \text{such that (15) (16) holds}\} \quad (14)$$

$$0 \leq R_1 \leq I(X;Y), \quad 0 \leq R_2 \leq I(X_f;Y_f) \quad (15)$$

$$R_1 + R_2 \leq \min\left\{ \begin{array}{l} I(X;Y|Z,X_f) + I(X_f;Z,Y_f|X), \\ I(X_f;Y_f|Z,X) + I(X;Z,Y|X_f) \end{array} \right\} \quad (16)$$

Proof Outline:

First, we add a public noiseless broadcast channel to the two-way wiretap channel as shown in Figure 2. The broadcast channel takes input from node 1 and provides outputs to node 2 and the eavesdropper. Since the channel is noiseless, the

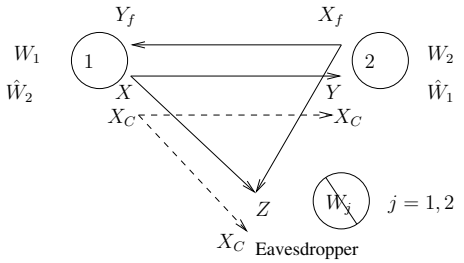

Fig. 2. Two-way wiretap channel with a public noiseless forward link

outputs equal the input, denoted by X_C. Then we apply the second term in Theorem 1 to this new channel model, and find that:

$$R_1 \leq I(X, X_C; Y, X_C | Z, X_C, X_f) + I(X_f; Y_f, Z, X_C | X, X_C) \tag{17}$$

It can be verified that (17) is upper bounded by:

$$I(X; Y | Z, X_f) + I(X_f; Y_f, Z | X) \tag{18}$$

This means introducing a public noiseless forward channel brings no change in the expression of the upper bound of R_1.

We next prove (18) is also an upper bound on $R_1 + R_2$. This is proved by showing if $R_1 = r_1, R_2 = r_2$ is achievable, then $R_1 = r_1 + r_2$ is also achievable. A rigorous proof is provided in [12]. The intuition is that we can use the message W_2 as a one-time pad to encrypt the data from node 1. The encrypted data is then transmitted over the public noiseless link. Since this link has unlimited rate, the additional number of channel uses required by this transmission is negligible. Hence we can show that (18) is an upper bound on the sum rate. ■

We next specialize these results to the Gaussian case.

Corollary 2: When Y_f is ignored by Node 1, the secrecy rate R_1 is upper bounded by

$$\inf_{\sigma^2 \geq 0} C\left(\frac{P\left(1+\sigma^2-\sqrt{h_1}\rho\right)^2}{\left(1+\sigma^2-\rho^2\right)\left(h_1 P+1+\sigma^2\right)}\right) + C\left(\frac{h_2 P_r}{1+\sigma^2}\right) \tag{19}$$

Proof Outline: Define N_4 as a Gaussian random variable such that $N_4 \sim \mathcal{N}(0, \sigma^2)$ and is independent from $N_i, i = 1, 2, 3$. Recall that Z is the signal received by the eavesdropper. We next consider a channel where the eavesdropper receives $Z + N_4$. Since $Z + N_4$ is a degraded version of Z, we can find an upper bound of the original channel by deriving an upper bound for this new channel.

This upper bound is then found by applying the bound (13). The corollary follows from the fact that all terms in the upper bound (13) is maximized when X, X_f are independent and each has a Gaussian distribution with zero mean and maximum possible variance. ■

Remark 3: When $\sigma^2 \to \infty$, (19) converges to $C(P)$, which corresponds to the first term in (13). Due to this fact, (19) is written as one term instead of the two terms as in (13). □

Remark 4: We introduce N_4 to further tighten the bound. For example, consider the case where $\rho = \eta = 0$. In this case the upper bound can be expressed as

$$\min_{0 \leq \alpha \leq 1} C\left(\frac{P}{\alpha h_1 P + 1}\right) + C\left(\alpha h_2 P_r\right) \tag{20}$$

where $\alpha = 1/(1+\sigma^2)$. Consider choosing the remaining parameters as $h_1 = 1, h_2 = 10$, $P = 100, P_r = 5$. It can be verified that the minimum is smaller than 2.96 and is attained around $\alpha = 0.09$. That is to say that the minimum is not attained at $\sigma^2 = 0$. □

Corollary 3: Define $R_{j,ub}, j = 1, 2$ as

$$R_{1,ub} = \inf_{\sigma^2 \geq 0} C\left(\frac{P\left(1+\sigma^2-\sqrt{h_1}\rho\right)^2}{\left(1+\sigma^2-\rho^2\right)\left(h_1 P+1+\sigma^2\right)}\right) + C\left(\frac{P_r\left(h_2+1+\sigma^2-2\sqrt{h_2}\eta\right)}{1+\sigma^2-\eta^2}\right) \tag{21}$$

$$R_{2,ub} = \inf_{\sigma^2 \geq 0} C\left(\frac{P_r\left(1+\sigma^2-\sqrt{h_2}\eta\right)^2}{\left(1+\sigma^2-\eta^2\right)\left(h_2 P_r+1+\sigma^2\right)}\right) + C\left(\frac{P\left(h_1+1+\sigma^2-2\sqrt{h_1}\rho\right)}{1+\sigma^2-\rho^2}\right) \tag{22}$$

The secrecy capacity region of the Gaussian two-way wiretap channel is upper bounded by

$$R_1 \leq \min\left\{C\left(P\right), R_{1,ub}\right\}, R_2 \leq \min\left\{C\left(P_r\right), R_{2,ub}\right\} \tag{23}$$

$$R_1 + R_2 \leq \min\left\{R_{1,ub}, R_{2,ub}\right\} \tag{24}$$

Proof Outline: Again we consider a channel where the eavesdropper receives $Z + N_4$ and derive an outer bound for this new channel. N_4 is as defined in the proof of Corollary 2.

The present corollary then follows from the fact that all terms in the outer bound in Corollary 1 are maximized simultaneously when X and X_f are independent, $X \sim \mathcal{N}(0, P)$, and $X_f \sim \mathcal{N}(0, P_r)$. The corollary then is a direct consequence of Corollary 1 when evaluated at this input distribution. ■

Remark 5: The introduction of N_4 is useful in tightening the bound. For example, consider the case where $\rho = \eta = 0$, $h_1 = 1, h_2 = 10$, $P = 100, P_r = 5$.

In this case the first term inside the minimum of the upper bound on R_1, which is $C(P)$, is about 3.3291. The second term inside the minimum of the upper bound on R_1 takes the form:

$$\min_{0 \leq \alpha \leq 1} C\left(\frac{P}{\alpha h_1 P + 1}\right) + C\left(P_r\left(\alpha h_2 + 1\right)\right) \tag{25}$$

where $\alpha = 1/(1+\sigma^2)$. It can be verified that the minimum is smaller than 3.24 and is attained around $\alpha = 0.32$. Hence the upper bound on R_1 is dominated by the second term inside the minimum and is not attained at $\sigma^2 = 0$. □

Remark 6: When $\eta = \rho = 1, h_1 = h_2 = 1$, Corollary 3 specializes to $R_1 + R_2 \leq \min\{C(P), C(P_r)\}$, which is the bound derived in [9] as a limiting case of the two-way relay-eavesdropper channel where the relay power goes to ∞. □

IV. Achievable Rates

Define the notation $[x]^+$ as $\max\{x, 0\}$. Define $f(P_1, P_2, h_1, h_2)$ and $R_j^*, j = 1, 2$ as:

$$f(P_1, P_2, h_1, h_2) = \alpha[C(P_1) - [C(\frac{h_1 P_1}{h_2 P_2 + 1}) - \frac{1-\alpha}{\alpha}[C(P_2) - C(\frac{h_2 P_2}{h_1 P_1 + 1})]^+]^+]^+ \quad (26)$$

$$R_1^* = \max_{0\le\alpha\le 1} f(P, P_r, h_1, h_2), R_2^* = \max_{0\le\alpha\le 1} f(P_r, P, h_2, h_1) \quad (27)$$

Define the region $\mathbf{R}$ as the convex hull of the rate pairs: $(0,0), (R_1^*, 0), (0, R_2^*)$. Then we have the following theorem:

Theorem 2: The rate region $\mathbf{R}$ is achievable.

Remark 7: The achievable scheme is composed of two phases. During phase one, with a time sharing factor of $1-\alpha$, Node 2 sends a key to Node 1. During phase two, Node 1 utilizes this key to encrypt its message and transmits the result to Node 2. Hence when $\alpha = 1$, $\mathbf{R}$ is achieved when both nodes ignore their received signals when computing their transmitting signals. The proof is omitted here due to space limitation and is provided in [12]. □

V. Comparison when $\rho = \eta = 0$

Corollary 4: When $\rho = \eta = 0$, $P_r = kP$, k is a positive constant, and $h_j \neq 0, j = 1, 2$, the loss in secrecy rates when received signals are not used to compute transmitting signals at Node j, $j = 1, 2$ is bounded by a constant, which is only a function of h_1 and h_2.

Proof is by letting $\alpha = 1$ in Theorem 2 and proving the corresponding R_1^* and R_2^* is within a constant from the sum rate upper bound. Details is omitted here due to space limitation and is provided in [12].

Corollary 5: Even in the case where cooperative jamming is possible ($h_j \neq 0, j = 1, 2$), when P is not proportionally increasing with P_r, ignoring Y_f at Node 1 can lead to unbounded loss in the secrecy rate.

Proof: We only need show that it is possible to achievable a secrecy rate for Node 1 that exceeds the upper bound given by Corollary 2 by an amount which is an unbounded function of P. Consider the case when $h_1 = h_2 = 1$. Then by evaluating (19) at $\sigma^2 = 0$ and $\sigma^2 \to \infty$ with $\rho = \eta = 0$, we find the secrecy rate R_1 is bounded by

$$\min\{C(P), C(P_r) + 0.5\} \quad (28)$$

when Y_f is ignored by Node 1. Choose P_r and P such that

$$C(P_r) + 0.5 < 0.4C(P) \quad (29)$$

For this power configuration, from (28), we observe that R_1 is upper bounded by $0.4C(P)$.

Let the α in Theorem 2 be 0.5. R_1^* then becomes:

$$0.5C(P) - 0.5\left[C\left(\frac{P}{P_r+1}\right) - C(P_r) + C\left(\frac{P_r}{P+1}\right)\right]^+ \quad (30)$$

A sufficient condition for $R_1^* = 0.5C(P)$ is that

$$C\left(\frac{P}{P_r+1}\right) + C\left(\frac{P_r}{P+1}\right) > C(P_r) \quad (31)$$

It can be verified that a sufficient condition it to hold is:

$$\left(\frac{P}{P_r+1} + 1\right)^2 / \left(\sqrt{P} + 1\right)^2 > 1 \quad (32)$$

which means $\sqrt{P} > P_r + 1$. Choose $P_r = P^{1/4}$. For sufficiently large P, both this requirement and (29) can be fulfilled. In this case, the achievable rate is $0.5C(P)$, which is greater than the upper bound $0.4C(P)$. The difference is $0.1C(P)$, which is not a bounded function of P. Hence we have proved the corollary. ■

VI. Conclusion

In this work, we have derived an outer bound for the two-way wiretap channel. By comparing it with the achievable rates for the Gaussian model, we have identified one case where the impact of ignoring feedback signals at the transmitters is limited. In the general case, we have proved that doing so leads to unbounded loss in secrecy rate. Therefore we conclude that utilizing feedback signals can be highly beneficial for two-way secure communication.

Appendix A
Proof of Theorem 1

Let $\varepsilon = \varepsilon_1 + \varepsilon_3$, where ε_1 and ε_3 were defined in (5) and (7). To simplify the notation, we use M_2' to denote $\{M_2, W_2\}$. Then we have:

$$\begin{aligned}
&H(W_1) - n\varepsilon && (33)\\
\le& H(W_1|Z^n) - H\left(W_1|Z^n, X_f^n, Y^n, M_2'\right) && (34)\\
=& I\left(W_1; M_2', X_f^n, Y^n|Z^n\right) && (35)\\
=& I\left(W_1; M_2', Y^n|Z^n\right) && (36)\\
\le& I\left(W_1, M_1, Y_f^n; M_2', Y^n|Z^n\right) && (37)\\
=& I\left(W_1, M_1, Y_f^n; M_2', Y^n, Z^n\right) - I\left(W_1, M_1, Y_f^n; Z^n\right) && (38)
\end{aligned}$$

where (34) follows from (5) and (7). (36) is because X_f^n is a deterministic function of Y^{n-1} and M_2', as shown in (3).

We next rewrite the first term in (38) as:

$$I\left(W_1, M_1, Y_f^n; Y_n|Z_n, M_2', Y^{n-1}, Z^{n-1}\right) + I\left(W_1, M_1, Y_f^n; Y^{n-1}, Z^n, M_2'\right) \quad (39)$$

The first term in (39) equals:

$$\begin{aligned}
&I\left(W_1, M_1, Y_f^n; Y_n|X_{f,n}, Z_n, M_2', Y^{n-1}, Z^{n-1}\right) && (40)\\
\le& h(Y_n|Z_n, X_{f,n}) - h\left(Y_n|X_{f,n}, X_n, M_2', Y^{n-1}, Z^n, W_1, M_1, Y_f^n\right) && (41)\\
=& h(Y_n|Z_n, X_{f,n}) - h(Y_n|X_{f,n}, X_n, Z_n) && (42)\\
=& I(X_n; Y_n|Z_n, X_{f,n}) && (43)
\end{aligned}$$

In (40), we use the fact that $X_{f,n}$ is a deterministic function of $\{M_2', Y^{n-1}\}$, as shown by (3). In (41), we use the fact that

X_n is a deterministic function of $\{W_1, M_1, Y_f^{n-1}\}$, as shown by (2). In (42), we use the fact that

$$Y_n - \{X_{f,n}, X_n, Z_n\} - \{M_2', Y^{n-1}, Z^{n-1}, W_1, M_1, Y_f^n\} \tag{44}$$

is a Markov chain. In particular, (1) allows us to remove $Y_{f,n}$ from the condition term. Applying this result, we find that (38) is upper bounded by

$$I\left(X_n; Y_n | Z_n, X_{f,n}\right) + I\left(W_1, M_1, Y_f^n; Y^{n-1}, M_2' | Z^n\right) \tag{45}$$

The second term in (45) can be rewritten as:

$$\begin{aligned} &I\left(W_1, M_1, Y_f^{n-1}; Y^{n-1}, M_2' | Z^n\right) + \\ &I\left(Y_{f,n}; Y^{n-1}, M_2' | W_1, M_1, Y_f^{n-1}, Z^n\right) \end{aligned} \tag{46}$$

The second term in (46) equals:

$$\begin{aligned} &I\left(Y_{f,n}; Y^{n-1}, M_2' | X_n, W_1, M_1, Y_f^{n-1}, Z^n\right) && (47)\\ \leq &h\left(Y_{f,n} | X_n, Z_n\right) - h(Y_{f,n} | X_{f,n}, X_n, Z_n, W_1, M_1, \\ &\qquad Y_f^{n-1}, Z^{n-1}, Y^{n-1}, M_2') && (48)\\ = &h\left(Y_{f,n} | X_n, Z_n\right) - h\left(Y_{f,n} | X_{f,n}, X_n, Z_n\right) && (49)\\ = &I(X_{f,n}; Y_{f,n} | X_n, Z_n) && (50) \end{aligned}$$

In (47), we use the fact that X_n is a deterministic function of $\{W_1, M_1, Y_f^{n-1}\}$, as shown by (2). In (48), we use the fact that $X_{f,n}$ is a deterministic function of $\{M_2', Y^{n-1}\}$, as shown by (3). In (49), we use the fact that

$$Y_{f,n} - \{X_{f,n}, X_n, Z_n\} - \{W_1, M_1, Y_f^{n-1}, Z^{n-1}, Y^{n-1}, M_2'\} \tag{51}$$

is a Markov chain. Applying this result, we find that that (45) is now upper bounded by

$$\begin{aligned} &I\left(X_n; Y_n | Z_n, X_{f,n}\right) + I(X_{f,n}; Y_{f,n} | X_n, Z_n) \\ &+ I\left(W_1, M_1, Y_f^{n-1}; Y^{n-1}, M_2' | Z^n\right) \end{aligned} \tag{52}$$

The last term in (52) can be rewritten as

$$\begin{aligned} &I\left(W_1, M_1, Y_f^{n-1}; Y^{n-1}, M_2' | Z^{n-1}\right) \\ &+ I\left(W_1, M_1, Y_f^{n-1}; Z_n | Y^{n-1}, M_2', Z^{n-1}\right) \\ &- I\left(W_1, M_1, Y_f^{n-1}; Z_n | Z^{n-1}\right) \end{aligned} \tag{53}$$

The second term and the last term in (53) can be upper bounded together as:

$$\begin{aligned} &- I\left(Z_n; M_2', Y^{n-1} | Z^{n-1}\right) \\ &- h\left(Z_n | W_1, M_1, Y_f^{n-1}, M_2', Y^{n-1}, Z^{n-1}\right) \\ &+ h\left(Z_n | Z^{n-1}, W_1, M_1, Y_f^{n-1}\right) && (54)\\ \leq &- h\left(Z_n | W_1, M_1, Y_f^{n-1}, M_2', Y^{n-1}, Z^{n-1}\right) \\ &+ h\left(Z_n | Z^{n-1}, W_1, M_1, Y_f^{n-1}\right) && (55)\\ = &- h\left(Z_n | X_n, X_{f,n}, W_1, M_1, Y_f^{n-1}, M_2', Y^{n-1}, Z^{n-1}\right) \\ &+ h\left(Z_n | X_n, Z^{n-1}, W_1, M_1, Y_f^{n-1}\right) && (56) \end{aligned}$$

$$\begin{aligned} \leq &- h\left(Z_n | X_n, X_{f,n}, W_1, M_1, Y_f^{n-1}, M_2', Y^{n-1}, Z^{n-1}\right) \\ &+ h\left(Z_n | X_n\right) && (57)\\ = &- h\left(Z_n | X_n, X_{f,n}\right) + h\left(Z_n | X_n\right) && (58)\\ = &I(X_{f,n}; Z_n | X_n) && (59) \end{aligned}$$

In (56), we use the fact that X_n is a deterministic function of $\{W_1, M_1, Y_f^{n-1}\}$, and $X_{f,n}$ is a deterministic function of $\{M_2', Y^{n-1}\}$. In (58), we use the fact that

$$Z_n - \{X_n, X_{f,n}\} - \{W_1, M_1, Y_f^{n-1}, M_2', Y^{n-1}, Z^{n-1}\} \tag{60}$$

is a Markov chain. Applying this result to (53), we find that that (52) is now upper bounded by:

$$\begin{aligned} &I\left(X_n; Y_n | X_{f,n}, Z_n\right) + I(X_{f,n}; Y_{f,n}, Z_n | X_n) \\ &+ I\left(W_1, M_1, Y_f^{n-1}; Y^{n-1}, M_2' | Z^{n-1}\right) \end{aligned} \tag{61}$$

Hence we have shown

$$\begin{aligned} H(W_1) - n\varepsilon &\leq I\left(W_1, M_1, Y_f^n; Y^n, M_2' | Z^n\right) \\ &\leq I\left(X_n; Y_n | X_{f,n}, Z_n\right) + I\left(X_{f,n}; Y_{f,n}, Z_n | X_n\right) \\ &\quad + I\left(W_1, M_1, Y_f^{n-1}; Y^{n-1}, M_2' | Z^{n-1}\right) \end{aligned} \tag{62}$$

Applying this result repeatedly for $n-1, n-2, ..., 1$, we have

$$H(W_1) - n\varepsilon \leq \sum_{i=1}^{n} (I(X_i; Y_i | X_{f,i}, Z_i) + I(X_{f,i}; Y_{f,i}, Z_i | X_i)) \tag{63}$$

The remaining steps follow from the standard single letterization of (63). For details, see [12].

REFERENCES

[1] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, September 1949.

[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] C. E. Shannon. Two-way Communication Channels. In *Proc. 4th Berkeley Symp. Math. Stat. Prob*, volume 1, pages 351–384, 1961.

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

[6] E. Ardetsanizadeh, M. Franceschetti, T. Javidi, and Y. H. Kim. The Secrecy Capacity of the Wiretap Channel with Rate-limited Feedback. Submitted to IEEE Transactions on Information Theory, 2008, Available online at http://circuit.ucsd.edu:16080/tjavidi/index_files/publications.html.

[7] D. Gunduz, D. R. Brown III, and H. V. Poor. Secure Communication with Feedback. In *IEEE International Symposium on Information Theory and its Applications*, December 2008.

[8] T. Han. A General Coding Scheme for the Two-way Channel. *IEEE Transactions on Information Theory*, 30(1):35–44, Januray 1984.

[9] X. He and A. Yener. On the Role of Feedback in Two Way Secure Communication. In *42nd Annual Asilomar Conference on Signals, Systems, and Computers*, October 2008.

[10] M. Bloch. Channel Scrambling for Secrecy. In *IEEE International Symposium on Information Theory*, June 2009.

[11] E. Ekrem and S. Ulukus. Secrecy in Cooperative Relay Broadcast Channels. Submitted to IEEE Transactions on Information Theory, October, 2008.

[12] X. He and A. Yener. The Role of Feedback in Two-Way Secure Communication. Submitted to IEEE Transactions on Information Theory, November, 2009, Available online at http://arxiv.org/abs/0911.4432.