Achievable Rates for Two-Way Wire-Tap Channels

Ender Tekin
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University
University Park, PA 16802
tekin@psu.edu

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

***Abstract*—We consider two-way wire-tap channels, where two users are communicating with each other in the presence of an eavesdropper, who has access to the communications through a multiple-access channel. We find achievable rates for two different scenarios, the *Gaussian two-way wire-tap channel*, (GTW-WT), and the *binary additive two-way wire-tap channel*, (BATW-WT). It is shown that the two-way channels inherently provide a unique advantage for wire-tapped scenarios, as the users know their own transmitted signals and in effect help encrypt the other user's messages, similar to a one-time pad. We compare the achievable rates to that of the Gaussian multiple-access wire-tap channel (GMAC-WT) to illustrate this advantage.**

I. Introduction

Information theoretic secrecy was first developed by Shannon in [1]. In this work, Shannon showed that to achieve *perfect secrecy* in communications, which is equivalent to providing no information to an enemy cryptanalyst, the *a posteriori* probability of a message must be equivalent to its *a priori* probability.

In [2], Wyner applied this concept to the discrete memoryless channel by defining the *wire-tap channel*, where there is a wire-tapper who has access to a degraded version of the intended receiver's signal. Using the normalized conditional entropy of the transmitted message given the received signal at the wire-tapper as the secrecy measure, he found the region of all possible rate/equivocation pairs, and the existence of a *secrecy capacity*, C_s, the rate up to which it is possible to transmit zero information to the wire-tapper.

Reference [3] extended Wyner's results to Gaussian channels. Csiszár and Körner, [4], improved Wyner's results to weaker, "less noisy" and "more capable" channels. Furthermore, they examined sending common information to both the receiver and the wire-tapper, while maintaining the secrecy of private information that is communicated to the receiver only.

In [5], it is shown that the existence of a "public" feedback channel can enable the two parties to be able to generate a secret key even when the wire-tap capacity is zero. More recently, the notion of the wire-tap channel has been extended to parallel channels, [6], relay channels, [7], and fading channels, [8]. Broadcast and interference channels with confidential messages are considered in [9]. References [10], [11] examine the multiple access channel with confidential messages where two transmitters try to keep their messages secret from each other while communicating with a common receiver. Gaussian multiple-access wire-tap (GMAC-WT) channels are considered in [12]–[15], where transmitters communicate with an intended receiver in the presence of an external wire-tapper. In [13], [14], we considered the case where the wire-tapper gets a degraded version of the signal at the legitimate receiver, and found the secrecy-sum capacity for the *collective* set of constraints using Gaussian codebooks and stochastic encoders. In [15], the general (non-degraded) GMAC-WT was considered, and an achievable rate region for perfect secrecy with collective secrecy measures was found.

In this paper, we consider the two-way channel where two nodes communicate with each other, [16]. We introduce the two-way wire-tap (TW-WT) channel where an external *eavesdropper* receives the transmitters' signals through a general MAC. In particular, we consider the Gaussian Two-Way Wire-Tap Channel (GTW-WT), and the Binary Additive Two-Way Wire-Tap Channel (BATW-WT). We utilize as our secrecy constraint, the normalized conditional entropy of the transmitted secret messages given the eavesdropper's signal, as in [2]. We show that satisfying this constraint implies the secrecy of the messages for both users. In both scenarios, transmitters are assumed to have one secret and one open message to transmit. We find an achievable *secure rate region*, for both cases, where users can communicate with arbitrarily small probability of error with the intended receiver under *perfect secrecy* from the eavesdropper.

We also show that in cases where a user is not able to achieve secrecy, that user may help the other user increase its secrecy rate or achieve secrecy if it was not possible before, by jamming the eavesdropper. Thus, similar to the Gaussian multiple-access wire-tap channel, [15], *cooperative jamming* helps increase the secrecy rate.

II. System Model and Problem Statement

We consider two users communicating in the presence of an intelligent and informed eavesdropper. Each transmitter $k \in \mathcal{K} \triangleq \{1,2\}$ has a secret message, W_k, from a set of equally likely messages $\mathcal{W}_k = \{1,\ldots,M_k\}$. The messages are encoded using $(2^{nR_k},n)$ codes into $\{\tilde{X}_k^n(W_k)\}$, where $R_k = \frac{1}{n}\log_2 M_k$. The encoded messages $\{\tilde{\mathbf{X}}_k\} = \{\tilde{X}_k^n\}$ are then transmitted. Each receiver $k=1,2$ gets $\mathbf{Y}_k = Y_k^n$ and the eavesdropper $\mathbf{Z} = Z^n$. Receiver k decodes $\mathbf{Y}_k$ to get an estimate of the transmitted message of the other user. The users would like to communicate with arbitrarily low probability of error, while maintaining perfect secrecy of the messages, $\mathbf{W}$. We assume the channel parameters are universally known, including at the eavesdropper, and that the eavesdropper also

1-4244-1429-6/07/$25.00 ©2007 IEEE

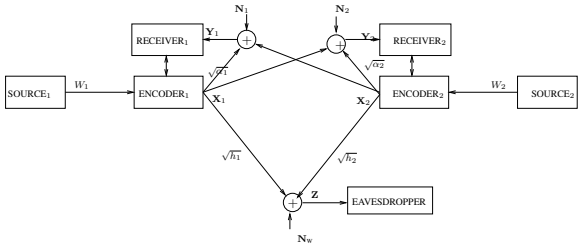

Fig. 1. The standardized GTW-WT system model

knows the codebooks and coding scheme. We first define *achievability* for this wire-tap channel:

Definition 1 (Achievable secrecy rates). The rate pair (R_1, R_2) is said to be *achievable* for the TW-WT, if for $\epsilon > 0$ there exists a code of sufficient length n such that

$$\frac{1}{n}\log_2 M_k \geq R_k - \epsilon \quad k = 1, 2 \tag{1a}$$

$$P_e \leq \epsilon \tag{1b}$$

$$\frac{H(\mathbf{W}|\mathbf{Z})}{H(\mathbf{W})} \geq 1 - \epsilon \tag{1c}$$

where

$$P_e = \frac{1}{M_1 M_2} \sum_{\mathbf{W} \in \mathcal{W}_1 \times \mathcal{W}_2} \mathrm{P}\{\hat{\mathbf{W}} \neq \mathbf{W} | \mathbf{W} \text{ was sent}\}. \tag{2}$$

is the average probability of error for a given code.

A. The Gaussian Two-Way Wire-Tap Channel

We describe the Gaussian Two-Way Wire-Tap Channel (GTW-WT), which corresponds to a two-way wireless communications system. We assume slow fading, such that each codeword experiences the same channel coefficient, and also that all parties know the channel coefficients. The signals at the intended receiver and the eavesdropper are given by

$$\mathbf{Y}_1 = \tilde{\mathbf{X}}_1 + \sqrt{h_2^{\mathrm{M}}}\tilde{\mathbf{X}}_2 + \tilde{\mathbf{N}}_1 \tag{3a}$$

$$\mathbf{Y}_2 = \sqrt{h_1^{\mathrm{M}}}\tilde{\mathbf{X}}_1 + \tilde{\mathbf{X}}_2 + \tilde{\mathbf{N}}_2 \tag{3b}$$

$$\mathbf{Z} = \sqrt{h_1^{\mathrm{w}}}\tilde{\mathbf{X}}_1 + \sqrt{h_2^{\mathrm{w}}}\tilde{\mathbf{X}}_2 + \tilde{\mathbf{N}}_{\mathrm{w}} \tag{3c}$$

such that $\frac{1}{n}\sum_{i=1}^{n} \tilde{X}_{ki}^2 \leq \tilde{\bar{P}}_k$, for $k = 1, 2$ and $\tilde{\mathbf{N}}_k \sim \mathcal{N}\left(0, \sigma_k^2\right)$ and $\tilde{\mathbf{N}}_{\mathrm{w}} \sim \mathcal{N}\left(0, \sigma_{\mathrm{w}}^2\right)$. For simplicity, without loss of generality, we consider an equivalent standard form as in [14] as illustrated in Figure 1.

$$\mathbf{Y}_1 = \sqrt{\alpha_1}\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{N}_1 \tag{4a}$$

$$\mathbf{Y}_2 = \mathbf{X}_1 + \sqrt{\alpha_2}\mathbf{X}_2 + \mathbf{N}_2 \tag{4b}$$

$$\mathbf{Z} = \sqrt{h_1}\mathbf{X}_1 + \sqrt{h_2}\mathbf{X}_2 + \mathbf{N}_{\mathrm{w}} \tag{4c}$$

where, for $k = 1, 2$,

- the codewords $\{\tilde{\mathbf{X}}\}$ are scaled to get $\mathbf{X}_1 = \sqrt{\frac{h_1^{\mathrm{M}}}{\sigma_2^2}}\tilde{\mathbf{X}}_1$ and $\mathbf{X}_2 = \sqrt{\frac{h_2^{\mathrm{M}}}{\sigma_1^2}}\tilde{\mathbf{X}}_2$;
- the maximum powers are scaled to get $\bar{P}_1 = \frac{h_1^{\mathrm{M}}}{\sigma_2^2}\tilde{\bar{P}}_1$ and $\bar{P}_2 = \frac{h_2^{\mathrm{M}}}{\sigma_1^2}\tilde{\bar{P}}_2$;
- the transmitters' new channel gains are given by $\alpha_1 = \frac{\sigma_2^2}{h_1^{\mathrm{M}}\sigma_1^2}$ and $\alpha_2 = \frac{\sigma_1^2}{h_2^{\mathrm{M}}\sigma_2^2}$;
- the wiretapper's new channel gains are given by $h_1 = \frac{h_1^{\mathrm{w}}\sigma_2^2}{h_1^{\mathrm{M}}\sigma_{\mathrm{w}}^2}$ and $h_2 = \frac{h_2^{\mathrm{w}}\sigma_1^2}{h_2^{\mathrm{M}}\sigma_{\mathrm{w}}^2}$;
- the noises are normalized by $\mathbf{N}_k = \frac{\tilde{\mathbf{N}}_k}{\sigma_k^2}$ and $\mathbf{N}_{\mathrm{w}} = \frac{\tilde{\mathbf{N}}_{\mathrm{w}}}{\sigma_{\mathrm{w}}^2}$.

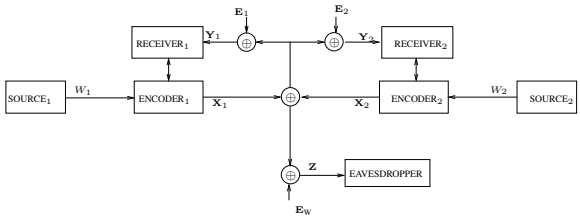

Fig. 2. BATW-WT system model

B. The Binary Additive Two-Way Wire-Tap Channel

This model, shown in Figure 2, corresponds to a more classical wire-tapped channel, where the binary signals of two transmitters are superimposed on a common wire, as in [16], and random bit errors are produced as in a binary symmetric channel. For the BATW-WT, the received signals are given by

$$\mathbf{Y}_1 = \mathbf{X}_1 \oplus \mathbf{X}_2 \oplus \mathbf{E}_1 \tag{5a}$$

$$\mathbf{Y}_2 = \mathbf{X}_1 \oplus \mathbf{X}_2 \oplus \mathbf{E}_2 \tag{5b}$$

$$\mathbf{Z}_1 = \mathbf{X}_1 \oplus \mathbf{X}_2 \oplus \mathbf{E}_{\mathrm{w}} \tag{5c}$$

where $\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_{\mathrm{w}}$ are n-vectors of binary random variables representing errors such that $\mathrm{P}\{E_{ki} = 1\} = \varepsilon_k < \frac{1}{2}$ and $\mathrm{P}\{E_{\mathrm{w}i} = 1\} = \varepsilon_{\mathrm{w}} < \frac{1}{2}$;$\varepsilon_k$ is the error probability at receiver $k = 1, 2$; ε_{w} is the error probability at the wiretapper.

III. Achievable Rates

In this section, we give our results on some achievable rates for the TW-WT channels considered in this paper. The proofs for both the GTW-WT and BATW-WT are similar and are summarized in Appendix I. For details, please see [17]. We first define a few quantities:

$$[\xi]^+ \triangleq \max\{\xi, 0\}, \qquad g(\xi) \triangleq \frac{1}{2}\log(1+\xi)$$

$$h(\xi) \triangleq -\xi\log\xi - (1-\xi)\log(1-\xi), \quad 0 \leq \xi \leq 1$$

$$\mathcal{P} \triangleq \left\{(P_1, P_2) \colon 0 \leq P_1 \leq \bar{P}_1,\, 0 \leq P_2 \leq \bar{P}_2\right\}$$

and

$$C_k = \begin{cases} g\left(P_k\right), & \text{if GTW-WT} \\ 1 - h(\varepsilon_k), & \text{if BATW-WT} \end{cases} \tag{6}$$

$$C_{\mathrm{w}} = \begin{cases} g\left(h_1 P_1 + h_2 P_2\right), & \text{if GTW-WT} \\ 1 - h(\varepsilon_{\mathrm{w}}), & \text{if BATW-WT} \end{cases} \tag{7}$$

We now give achievable secret-rate regions for the two channels. In both channels under consideration, capacity without secrecy constraints can be achieved using independent inputs: for the GTW-WT, this was shown in [18]. For the BATW-WT, it is easily checked that the symmetry conditions in [16] apply, and the capacity region is a rectangle obtained by equiprobable inputs. The achievable secrecy rate regions in this paper are obtained using independent channel inputs.

Theorem 1. Let

$$\begin{aligned}\mathcal{R}^{\text{GTW}}(P_1,P_2) = \{(R_1,R_2)&: \\ R_k &\le g(P_k) \quad k=1,2 \\ R_1+R_2 &\le [g(P_1)+g(P_2)-g(h_1P_1+h_2P_2)]^+\}\end{aligned} \tag{8}$$

The rate region given below is achievable for the GTW-WT:

$$\mathcal{R}^{\text{GTW}} = \text{convex closure of } \bigcup_{\mathbf{P}\in\mathcal{P}} \mathcal{R}^{\text{GTW}}(\mathbf{P}) \tag{9}$$

Proof: See Appendix I. □

Theorem 2. For the BATW-WT, we can achieve the following set of rates:

$$\begin{aligned}\mathcal{R}^{\text{BATW}} = \{(R_1,R_2)&: \\ R_k &\le 1-h(\varepsilon_k) \quad k=1,2 \\ R_1+R_2 &\le [1+h(\varepsilon_{\text{w}})-h(\varepsilon_1)-h(\varepsilon_2)]^+\}\end{aligned} \tag{10}$$

Proof: See Appendix I. □

IV. Maximization of Sum Rate for GTW-WT

The achievable regions given in Theorem 1 depends on the transmit powers. We are naturally interested in the power allocation $\mathbf{P}^* = (P_1^*, P_2^*)$ that would maximize the total secrecy sum-rate. Without loss of generality, we will assume that $h_1 \le h_2$. We formally state the problem as:

$$\begin{aligned}&\max_{\mathbf{P}\in\mathcal{P}} \; C_1 + C_2 - C_{\text{w}} \\ &\quad = \max_{\mathbf{P}\in\mathcal{P}} \; g(P_1) + g(P_2) - g(h_1P_1+h_2P_2) &(11)\\ &\quad \equiv \min_{\mathbf{P}\in\mathcal{P}} \; \rho(\mathbf{P}) &(12)\end{aligned}$$

where

$$\rho(\mathbf{P}) \triangleq \frac{1+h_1P_1+h_2P_2}{(1+P_1)(1+P_2)} \tag{13}$$

The optimum power allocation is stated below:

Theorem 3. The secrecy sum-rate maximizing power allocation for the GTW-WT is given by:

$$(P_1^*,P_2^*) = \begin{cases}(\bar{P}_1,\bar{P}_2), & \text{if } h_1 \le 1+h_2\bar{P}_2,\ h_2 < 1+h_1\bar{P}_1 \\ (\bar{P}_1,0), & \text{if } h_1 < 1,\ h_2 \ge 1+h_1\bar{P}_1 \\ (0,0), & \text{otherwise}\end{cases} \tag{14}$$

Proof: See Appendix II. □

Note that the solution is such that as long as a user is not single-user decodable, it should be transmitting with maximum power. Comparing this with the GGMAC-WT region found in [15], we note the same structure, namely, that secrecy is achievable for both users, as long as neither can be decoded by treating the other user as noise.

V. Cooperative Jamming

In [15], it was shown that for the GGMAC-WT, a user who ceases transmission to maximize the secrecy sum-rate may jam the eavesdropper and allow an increase in the remaining users' secrecy rate, or even allow a user to achieve a positive secrecy rate. Similarly, in Theorem 3, we see that when user 2 is single-user decodable, i.e. $h_2 \ge 1+h_1\bar{P}_1$, it must cease transmission in order to maximize sum rate. We show that in this case, user 2 can similarly help user 1 increase its secret rate and/or achieve a positive secrecy rate. This is achieved by letting user 2 transmit white Gaussian noise instead of actual codewords. Since receiver 2 knows the transmitted codewords, it can subtract these from its received sequence to get a clear channel from user 1. However, the eavesdropper, devoid of this *side information*, sees more noise and the achievable secrecy capacity for user 1 (since we are reduced to the single user case, [3] established that this is indeed the capacity) is increased as it is the difference of the capacity to user 1's channel to receiver 2 and its channel to the eavesdropper. This is stated below:

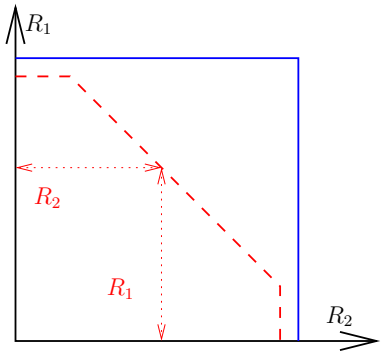

Fig. 3. Example region for a TW-WT

Theorem 4. The optimum power allocations for the cooperative jamming scheme described is

$$(P_1^*,P_2^*) = \begin{cases}(\bar{P}_1,\bar{P}_2), & \text{if } h_1 < 1+h_2\bar{P}_2 \\ (0,0), & \text{otherwise}\end{cases} \tag{15}$$

Proof: See Appendix III. □

This can be interpreted as "jam with maximum power if it is possible to change user 1's effective channel gain such that it is no longer single-user decodable". If $h_2 < 1+h_1\bar{P}_1$, then user 2 must be transmitting instead of jamming.

We can similarly consider a scheme for the BATW-WT. Note that the achievable secret-sum rate is 0 when $h(\varepsilon_1)+h(\varepsilon_2) \ge 1+h(\varepsilon_{\text{w}})$. This implies that $\varepsilon_k \ge \varepsilon_{\text{w}}$, $k=1,2$. Let $\varepsilon_1 \le \varepsilon_2$. Then, user 2 can randomly transmit bits drawn according to the binary distribution with $\text{P}\{X_{2i}=1\} = \frac{1}{2}$. This is equivalent to randomly adding a bit to the eavesdropper's signal. Hence the probability of error at the eavesdropper for user 2's codeword becomes $\frac{1}{2}$, and the eavesdropper cannot gain any information about user 1's transmitted codeword. Receiver 2, however, knows the jamming sequence, which it can subtract from its received sequence. Thus, user 1 can transmit to user 2 at a rate $1-h(\varepsilon_1)$, which is its capacity.

VI. Numerical Results and Conclusions

We now illustrate our results via numerical examples. A typical region for the TW-WT channels considered is shown in Figure 3. Figure 4 shows an achievable region as a function of the power allocations. We can see that the optimum power allocation is given by Theorem 3. Finally, Figure 5 shows the

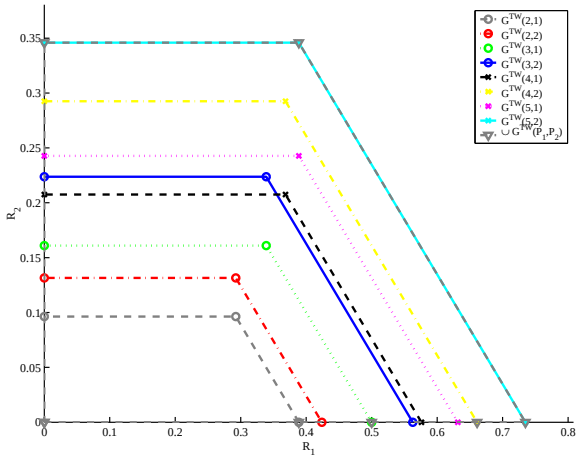

Fig. 4. GTW-WT achievable secrecy region when $\bar{P}_1 = 5, \bar{P}_2 = 2, h_1 = .5, h_2 = 1.5$.

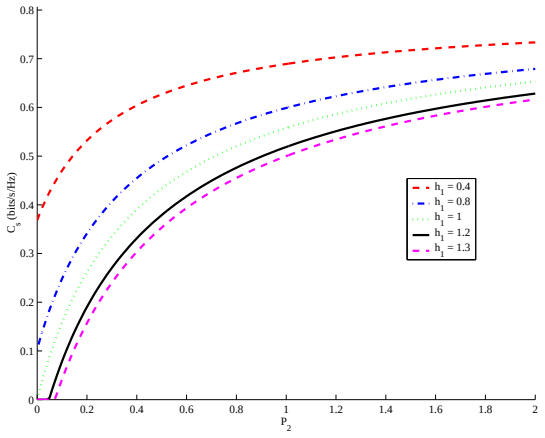

Fig. 5. GTW-WT cooperative jamming secrecy capacity as a function of P_2 with different h_1 for $\bar{P} = 2$, $h_2 = 4.2$

secrecy capacity increase for user 1 as a function of user 2's jamming power.

Comparing the GTW-WT region to the achievable region for the GGMAC-WT, [15], we can see the enlargement of the rate region due to the two-way communications scenario. Even though the signal received by the eavesdropper is the same, the two-way channel effectively provides a shared secret, namely the transmitters' knowledge on their own codewords, and hence enlarges the rate region. In addition, unlike the GGMAC-WT, sum secret rate is not limited by the channel gains as the power limitations are relaxed for the GTW-WT. In fact, we see that $\lim_{\bar{P}\to\infty} R_1 + R_2 = g(\frac{1}{2}\bar{P})$.

An important thing to note is that in both channels, the achievability proof uses a scheme that requires the receivers to decode one of $2^{n(R_k+R_k^x)}$ codewords. Thus, the actual rate of communication is $R_k + R_k^x$, although only a rate R_k is "secret" information. We can utilize the extra codewords to communicate at an additional rate R_k^x, although the secrecy of these messages is not guaranteed. Thus, we may use the channel to its full capacity, but are limited in rate by how much of the communication can be kept secret as in [3], [14].

In conclusion, we see that two-way channels provide an extra advantage for wire-tap scenarios as the receivers, knowing their own transmitted codewords, gain an advantage over the eavesdropper that is not possible for multiple-access wire-tap channels. As a result, a larger achievable region is found, and for the scenarios considered cooperative jamming proves to be even more useful as it does not hurt the transmitting user's rate as it does for the GMAC-WT.

Appendix I
Achievability Proofs

The proofs follow along the same line as the proof in [15] for the achievability of the general GMAC-WT. Let $\mathbf{P} \in \mathcal{P}$ and $\mathbf{R} \in \mathcal{R}^{\text{GTW}}$ for the GTW-WT, and let $\mathbf{R} \in \mathcal{R}^{\text{BATW}}$ for the BATW-WT. Consider user $j = 1$, and the following scheme (the other user does exactly the same):

1) Generate 2 codebooks $\mathfrak{X}_1, \tilde{\mathfrak{X}}_1$. $\mathfrak{X}_1$ consists of M_1 codewords, and codebook $\tilde{\mathfrak{X}}_1$ has M_1^x codewords. The codebooks are generated such that
   a) For the GTW-WT, each component of the codes in $\mathfrak{X}_1$ is drawn $\sim \mathcal{N}(0, \lambda_1 P_1 - \varepsilon)$, and each component of $\tilde{\mathfrak{X}}_1$ is drawn $\sim \mathcal{N}(0, (1-\lambda_1)P_1 - \varepsilon)$ where ε is an arbitrarily small number to ensure that the power constraints on the codewords are satisfied with high probability.
   b) For the BATW-WT, codewords in $\mathfrak{X}_1$ and $\tilde{\mathfrak{X}}_1$ are drawn uniformly according to a binary distribution with $p = \frac{1}{2}$.
2) To transmit message $W_1 \in \mathcal{W}_1$, user 1 finds the codeword corresponding to W_1 in $\mathfrak{X}_1$ and also uniformly chooses a codeword from $\tilde{\mathfrak{X}}_1$. User 1 then adds (xor's for the binary case) these codewords and transmits the resulting codeword, $\mathbf{X}_1$, so that we are actually transmitting (uniformly) one of $M_1 M_1^x$ codewords, and the rate of transmission is $R_1 + R_1^x$, where $R_1^x = \frac{1}{n}\log M_1^x$.

We choose the rates to satisfy

$$R_k + R_k^x \le C_k, \quad k = 1, 2 \tag{16}$$
$$R_1 + R_2 \le C_1 + C_2 - C_{\text{w}} \tag{17}$$
$$R_1^x + R_2^x = C_{\text{w}} \tag{18}$$

The first set of conditions for both channels guarantee that receiver 1 can reliably decode the $2^{n(R_2+R_2^x)}$ codewords from user 2 since it knows its own transmitted codeword, $\mathbf{X}_1$, and can subtract (or xor for the binary case) this with its received sequence $\mathbf{Y}_1$ to get a single-user channel from the other transmitter such that for the GTW-WT, it has $\mathbf{X}_2 + \mathbf{N}_1$ and for the BATW-WT, it has $\mathbf{X}_2 \oplus \mathbf{E}_1$. Then, the standard channel coding arguments, see [19], can be used to establish that rates of C_k can be achieved for user k. Define

$$\mathbf{X}_\Sigma = \begin{cases} \sqrt{h_1}\mathbf{X}_1 + \sqrt{h_2}\mathbf{X}_2, & \text{if GTW-WT} \\ \mathbf{X}_1 \oplus \mathbf{X}_2, & \text{if BATW-WT} \end{cases} \tag{19}$$

Then,

$$H(\mathbf{W}|\mathbf{Z}) = H(\mathbf{W},\mathbf{Z}) - H(\mathbf{Z}) \tag{20}$$
$$= H(\mathbf{W},\mathbf{X}_\Sigma,\mathbf{Z}) - H(\mathbf{X}_\Sigma|\mathbf{W},\mathbf{Z}) - H(\mathbf{Z}) \tag{21}$$
$$= H(\mathbf{W}) + H(\mathbf{Z}|\mathbf{W},\mathbf{X}_\Sigma) - H(\mathbf{Z}) + H(\mathbf{X}_\Sigma|\mathbf{W}) - H(\mathbf{X}_\Sigma|\mathbf{W},\mathbf{Z}) \tag{22}$$

$$= H(\mathbf{W}) - I(\mathbf{X}_\Sigma;\mathbf{Z}) + I(\mathbf{X}_\Sigma;\mathbf{Z}|\mathbf{W}) \quad (23)$$

where the key observation is that the eavesdropper's information on $\mathbf{W}$ only depends on $\mathbf{X}_\Sigma$, i.e. $\mathbf{W} \to \mathbf{X}_\Sigma \to \mathbf{Z}$, and hence $H(\mathbf{Z}|\mathbf{W},\mathbf{X}_\Sigma) = H(\mathbf{Z}|\mathbf{X}_\Sigma)$.

Note that we have $I(\mathbf{X}_\Sigma;\mathbf{Z}) \le nC_{\rm w}$, from the capacity of the standard single user binary additive channel. We can also write $I(\mathbf{X}_\Sigma;\mathbf{Z}|\mathbf{W}) = H(\mathbf{X}_\Sigma|\mathbf{W}) - H(\mathbf{X}_\Sigma|\mathbf{W},\mathbf{Z})$. Since, given each pair of messages, $\mathbf{W}$, we uniformly send one of $M_1^x M_2^x$ random sum-codewords, we have $H(\mathbf{X}_\Sigma|\mathbf{W}) = \log(M_1^x M_2^x) = n\left(R_1^x + R_2^x\right) = nC_{\rm w}$. In addition, we have $H(\mathbf{X}_\Sigma|\mathbf{W},\mathbf{Z}) \le \epsilon$, since given $\mathbf{W}$, we transmit one of only $nC_{\rm w}$ codewords, and the eavesdropper can reliably decode these. Thus, we also have $I(\mathbf{X}_\Sigma;\mathbf{Z}|\mathbf{W}) \ge nC_{\rm w} - n\epsilon$. Using these in (23), we see that

$$H(\mathbf{W}|\mathbf{Z}) \ge H(\mathbf{W}) - nC_{\rm w} + nC_{\rm w} - n\epsilon = H(\mathbf{W}) - n\epsilon \quad (24)$$

Appendix II
Proof of Theorem 3

The Lagrangian is given by,

$$\mathcal{L}(\mathbf{P},\boldsymbol{\mu}) = \rho(\mathbf{P}) - \textstyle\sum_{k=1}^2 \mu_{1k}P_k + \sum_{k=1}^2 \mu_{2k}(P_k - \bar{P}_k) \quad (25)$$

Equating the derivative of the Lagrangian to zero,

$$\frac{\partial \mathcal{L}(\mathbf{P}^*,\boldsymbol{\mu})}{\partial P_j^*} = \dot{\rho}_j(\mathbf{P}^*) - \mu_{1j} + \mu_{2j} = 0 \quad (26)$$

where

$$\dot{\rho}_j(\mathbf{P}) \triangleq \frac{h_j - \Phi_j(\mathbf{P})}{(1+P_1)(1+P_2)} \quad (27)$$

$$\Phi_j(\mathbf{P}) \triangleq \frac{1 + h_1P_1 + h_2P_2}{1+P_j} \quad (28)$$

It is easy to see that if $h_j > \Phi_j(\mathbf{P})$, then $\mu_{1j} > 0$, and we have $P_j^* = \bar{P}_j$. If $h_j < \Phi_j(\mathbf{P})$, then we similarly find that $P_j^* = 0$. Finally, if $h_j = \Phi_j(\mathbf{P})$, we can have $0 < P_j^* < \bar{P}_j$. However, such a user has $\dot{\rho}_j(\mathbf{P}^*) = 0$, so we can set $P_j^* = 0$ with no effect on the secrecy sum-rate. Thus, we have $P_j^* = \bar{P}_j$ if $h_j < \phi_j(\mathbf{P})$, and $P_j^* = 0$ if $h_j \ge \phi_j(\mathbf{P})$.

Now consider user 1. If $P_1^* = 0$, then $h_2 \ge h_1 \ge 1 + h_2P_2^*$, but if $P_2^* > 0$, this implies that $h_2 > \frac{1+h_2P_2^*}{1+P_2^*}$ and $P_2^* = 0$. This contradiction shows that if $P_1^* = 0$, then $P_2^* = 0$. Assume $P_1^* = \bar{P}_1$, i.e. $h_1 < 1 + h_2P_2^*$. If $h_2 > 1 + h_1\bar{P}_1$, then $P_2^* = 0$. If $h_2 < 1 + h_1\bar{P}_1$, then $P_2^* = \bar{P}_2$.

Appendix III
Proof of Theorem 4

We can write the problem formally as:

$$\max_{\mathbf{P}\in\mathcal{P}} \quad g\left(P_1\right) - g\left(\frac{h_1P_1}{1+h_2P_2}\right) \equiv \min_{\mathbf{P}\in\mathcal{P}} \frac{\rho(\mathbf{P})}{\phi_2(P_2)} \quad (29)$$

where ρ is given in (13) and $\phi_2(P_2) \triangleq \frac{1+h_2P_2}{1+P_2}$.

The Lagrangian is given by

$$\mathcal{L}(\mathbf{P},\boldsymbol{\mu}) = \frac{\rho(\mathbf{P})}{\phi_2(P_2)} - \textstyle\sum_{k=1}^2 \mu_{1k}P_k + \sum_{k=1}^2 \mu_{2k}(P_k - \bar{P}_k) \quad (30)$$

Taking the derivative with respect to P_1^*, P_2^*, we get:

$$\frac{\dot{\rho}_1(\mathbf{P}^*)}{\phi_2(P_2^*)} - \mu_{11} + \mu_{21} = 0 \quad (31)$$

$$\frac{\dot{\rho}_2(\mathbf{P})\phi_2(P_2^*) - \rho(\mathbf{P})\dot{\phi}_2(P_2^*)}{\phi_2^2(P_2^*)} - \mu_{12} + \mu_{22} = 0 \quad (32)$$

where $\dot{\rho}$ is as given in (27) and $\dot{\phi}_2(P) \triangleq \frac{h_2 - \phi_2(P)}{1+P}$.

Consider user 1. If we have $h_1 > 1 + h_2P_2^*$, then we must have $\mu_{11} > 0$ since the first and last terms in (31) would be positive, making $P_1^* = 0$. Assume $P_1^* > 0 \Rightarrow \mu_{11} = 0$. If $h_1 < 1 + h_2P_2^*$, then the first term is negative, and $P_1^* = \bar{P}_1$. If $h_1 = 1 + h_2P_2^*$, then the sum rate is zero, and we can set $P_1^* = 0$. For user 2, it is very easy to see that since it only harms the jammer, the optimal jamming strategy should have $P_2^* = \bar{P}_2$, as long as user 1 has $P_1^* > 0$. This can also be seen by noting that $\dot{\rho}_2(\mathbf{P})\phi_2(P_2^*) - \rho(\mathbf{P})\dot{\phi}_2(P_2^*) < 0$ for $P_1^* > 0$.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. J.*, vol. 28, pp. 656–715, 1949.

[2] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, no. 24(4), pp. 451–456, Jul 1978.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, no. 24(3), pp. 339–348, May 1978.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, no. 39(3), pp. 733–742, May 1993.

[6] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. Inform. Theory*, no. 32(3), pp. 387 – 393, May 1986.

[7] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inform. Theory Workshop (ITW)*, 2001, pp. 87 – 89.

[8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jul 2006.

[9] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. Allerton Conf. Commun., Contr., Comput.*, Sep 2006.

[10] Y. Liang and V. Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. Inform. Theory*, submitted for publication, conference version presented at ISIT'06. [Online.] Available: http://arxiv.org/format/cs.IT/0605014.

[11] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jul 2006.

[12] E. Tekin, S. Şerbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. ASILOMAR Conf. Sig., Syst., Comp.*, Oct 2005.

[13] E. Tekin and A. Yener, "The Gaussian multiple-access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jul 2006.

[14] ——, "The Gaussian multiple-access wire-tap channel," *IEEE Trans. Inform. Theory*, submitted for publication, [Online.] Available: http://arxiv.org/format/cs.IT/0605028.

[15] ——, "Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy," in *Proc. Allerton Conf. Commun., Contr., Comput.*, Sep 2006, [Online.] Available: http://arxiv.org/abs/cs/0612088.

[16] C. E. Shannon, "Two-way communication channels," in *Proc. 4th Berkeley Symposium Math. Stat. Prob. Vol. 1*, 1961, pp. 611–644.

[17] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, submitted for publication November 2006, [Online.] Available: http://arxiv.org/abs/cs/0702112.

[18] T. S. Han, "A general coding scheme for the two-way channel," *IEEE Trans. Inform. Theory*, vol. 30, no. 1, pp. 35–44, Jan 1984.

[19] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, 1991.