

Secure Communication with a Relay Helping the Wire-tapper

Melda Yuksel and Elza Erkip
 Department of Electrical and Computer Engineering
 Polytechnic University
 Brooklyn, New York 11201-3840
 Email: myukse01@utopia.poly.edu

Abstract—A four terminal Gaussian network, composed of a single source-destination pair, a relay and a wire-tapper is considered. Unlike the relay channel with a wire-tapper, it is assumed that the relay assists the wire-tapper, not the destination. The relay's objective is to decrease the achievable secrecy rates. However, since the destination is also allowed to listen to the relay's transmission, it also benefits from the relay in terms of achievable rates. Direct transmission, amplify-and-forward (AF), decode-and-forward (DF) and compress-and-forward (CF) relaying schemes are compared in terms of secrecy rates. It is shown that the best relaying strategy depends on relay's location. Comparison of relaying protocols and best power allocation schemes, when the relay assists the source-destination communication, do not readily extend to the case when the relay assists the wire-tapper.

I. INTRODUCTION

Today's communication systems are composed of multi-terminal networks, and the relay channel is a basic building block of this structure. The relay channel was introduced in [1], and investigated in detail in [2]. In [2], the capacity region of the physically degraded relay channel is found, different relaying schemes are suggested, and it is shown that the relay increases the achievable rates with respect to direct transmission. However, for the general relay channel, the capacity region is still unknown. Recently, the papers [3] and [4] have triggered a vast attention on the relay channel and resulted in extensive research on the subject.

Decode-and-forward (DF), and compress-and-forward (CF) are two of the relaying schemes proposed in [2]. In DF, the relay decodes its received message, re-encodes it, and forwards it to the destination. In CF, the relay first compresses its received signal and then assigns a channel codeword, which it sends through the relay-destination channel. The compression is Wyner-Ziv type; i.e. the relay compresses its received signal taking into account that the destination has side information, through its received signal. In amplify-and-forward (AF) relaying protocol [3], the relay simply forwards the noisy signal it has received after a power scaling.

Another recently emerging subject in communication networks is security. Security issues arise due to jammers, attackers or wire-tappers. In this work, we focus on the last case. A wire-tapper is an illegitimate, passive listener in the environment. In the presence of a wire-tapper, the source-destination pair needs to keep its confidential messages secret

from the wire-tapper. This model was firstly studied in [5] for the degraded wire-tapper, and extended to less noisy and more capable broadcast channels in [6]. The paper [7] studies the Gaussian wire-tap problem. Generalized multiple access channels with confidential messages are studied in [8], and in [9] K user multiple access channel with a degraded wire-tapper is investigated. Interference and broadcast channels, when each user has confidential messages, are studied in [10]. In [11], the relay channel is considered, and the relay itself is assumed to be the wire-tapper. In this case, the relay can obtain some information about the source message, in addition to helping the source-destination communication. The relay channel with a wire-tapper, in which the relay helps the source-destination communication, is studied in [12], [13].

In this paper, we approach the relay channel with a wire-tapper from a different perspective and assume the relay helps the wire-tapper. This is a possible scenario in a multi-terminal communication system, if an adversary captures a relay, and uses this relay to gather more information about the source message [14]. In this case, unlike a jamming scenario, the relay does not aim to hinder the source-destination communication, but to decrease the secrecy rate. To provide the largest benefit to the wire-tapper, the relay can employ the AF, DF, or CF protocols. On the other hand, because the destination also hears the relay's transmission, its achievable rates are higher. We compare these different relaying strategies for the Gaussian channel to observe their effect on the achievable secrecy rate. We observe that the CF protocol in this scenario is not a trivial extension of the CF protocol for the classical relay channel, as the destination cannot always reliably decode the relay signal tailored for the wire-tapper. In the relay channel, when the relay helps the source and the destination, it is well known that when the relay is closer to the source than the destination, DF is superior to CF, and similarly, when the relay is closer to the destination than the source, CF outperforms DF [15]. However, we argue that this well known result does not immediately apply to the case when the relay assists the wire-tapper. In addition to these, the relay power allocation significantly changes for the protocols under investigation.

The organization of the paper is as follows. Section II introduces the system model. Section III presents and compares the achievable secrecy rates for direct transmission, and for AF, DF, and CF relaying protocols. Section IV concludes the

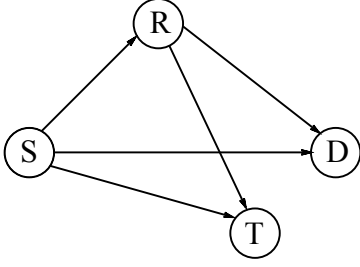


Fig. 1. The system model, the relay assists the wire-tapper.

paper.

II. SYSTEM MODEL

In this section we describe the system model. In the network under investigation, there is a single source-destination pair, a wire-tapper and a relay which aims to help the wire-tapper. S , D , R and T denote the source, the destination, the relay and the wire-tapper respectively. The system model is shown in Fig. 1.

We assume a time division multiple access system. The source transmits in the first time slot and the relay transmits in the second. This time division is imposed by the network, and even if the relay were silent, the source would not be able to use the second time slot for itself. Each time slot lasts for n channel uses. This is shown in Fig. 2.

In the classical wire-tap channel [5], the source knows that there is a wire-tapper in the system and assumes the wire-tapper uses the best decoding method possible. Similarly, the wire-tapper knows the source code book and the secrecy rate is calculated. Similar to the assumptions in the wire-tap channel, in this paper we assume both the source and the destination know the existence of a relay, who intends to help the wire-tapper. Moreover, they know which relaying scheme is going to be used. In other words, the encoding scheme at the source, the relaying protocol, and decoding methods at the destination and at the wire-tapper are all public information, only the message to be sent is to be kept confidential. Therefore, the source has to adjust its code book size to minimize its loss due to relay's actions.

The input-output relations are

$$Y_{l,i} = \frac{1}{\sqrt{d_{Sl}^\alpha}} X_{S,i} + Z_{l,i}$$

in the first time slot, $l = R, D, T$, $i = 1, \dots, n$, and

$$Y_{l,i} = \frac{1}{\sqrt{d_{Rl}^\alpha}} X_{R,i} + Z_{l,i}$$

in the second time slot, $l = D, T$, $i = n + 1, \dots, 2n$. Here $X_{S,i}$ denotes the signal the source transmits at time i in the first transmission slot, and $X_{R,i}$ denotes the signal the relay transmits at time i in the second slot. $Y_{l,i}$ and $Z_{l,i}$ denote the received signal and the noise at node l at time i respectively. We assume $Z_{l,i}$ are independent and identically distributed (i.i.d.) Gaussian with variance 1. In addition to these d_{kl} , $k = S, R$, $l = R, D, T$, $k \neq l$, denotes the Euclidian distance



Fig. 2. Orthogonal transmission between the source and the relay.

between the two nodes and α is the path loss exponent. We will use $Y_l^{(1)}$ and $Y_l^{(2)}$, $l = D, T$, to denote the destination and wire-tap observations in the first and the second time slots respectively. Note that the relay only listens in the first time slot.

The source sends message W , which is uniformly distributed over the message set $(1, \dots, 2^{2nR})$. Here R denotes the source rate. Note that the factor of 2 in the definition of R arises because the total number of channel uses in the system is equal to $2n$. The source maps the message W to the channel codeword $X_{S,1}^n$. The relay codeword $X_{R,n+1}^{2n}$ is a function of its received signal vector $Y_{R,1}^n$. The source and the relay have average power constraints P_S and P_R respectively. We also define

$$\gamma_{kl} = \frac{P_k}{d_{kl}^\alpha},$$

$k = S, R$, $l = R, D, T$, $k \neq l$.

The equivocation rate is defined as [6]

$$\frac{1}{2n} H(W | Y_{T,1}^{2n})$$

and $P_e^{(2n)}$ denotes the probability of error at the destination. The rate-equivocation rate pair (R, R_e) is achievable if there exists codes at rate R such that as $2n$ goes to infinity $P_e^{(2n)} \leq \epsilon$ and $H(W | Y_{T,1}^{2n}) / 2n \geq R_e - \epsilon$. Moreover, the secrecy rate R_s is achievable if (R_s, R_s) pair is achievable.

III. RELAYING SCHEMES

In this section we find achievable secrecy rates for direct transmission, and for relaying schemes AF, DF, and CF. We first concentrate on the direct transmission, because we will observe that depending on the relay location, all relaying schemes can display the same performance as direct transmission.

A. Direct Transmission

When the relay is turned off, the problem becomes equivalent to the classical wire-tap channel [5], [6], [7]. For this case an achievable secrecy rate is stated in the next theorem.

Theorem 1 ([5], [6], [7]): The secrecy rate

$$R_s^{(Dir)} = \frac{1}{2} \left[I_D^{(Dir)} - I_T^{(Dir)} \right]^+ \quad (1)$$

is achievable, where

$$I_D^{(Dir)} = \frac{1}{2} \log(1 + \gamma_{SD})$$

$$I_T^{(Dir)} = \frac{1}{2} \log(1 + \gamma_{ST}).$$

Proof: The proof can be found in [5], [6], [7]. Here we provide a brief sketch. We define $A = 2^{n(I_D^{(Dir)} - I_T^{(Dir)})}$, $B = 2^{nI_T^{(Dir)}}$ and the sets $\mathcal{A} = \{1, \dots, A\}$ and $\mathcal{B} = \{1, \dots, B\}$. The source chooses $2^{nI_D^{(Dir)}}$ channel codewords $X_{S,1}^n$ i.i.d.

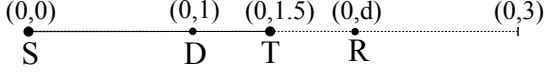


Fig. 3. Source (S), destination (D), wire-tapper (T) and relay (R) locations.

Gaussian with zero mean and variance P_S . In order to send a secret message $a \in \mathcal{A}$, the source chooses b uniformly from the set \mathcal{B} , forms $w = (a, b)$ and maps w into the channel codeword $X_{S,1}^n$. As the total number of codewords in the source code book is equal to $2^{nI_D^{(Dir)}}$, the destination can reliably decode w and hence a . However, the wire-tapper can only decode the index b and has no information about the secret message a . Thus perfect secrecy can be achieved. ■

B. Amplify and Forward

In the amplify and forward scheme, the relay simply forwards its received signal after a power scaling such that the transmitted signal satisfies the relay power constraint P_R . We denote this power scaling variable with β and write

$$X_{R,i+n} = \sqrt{\beta P_R} Y_{R,i},$$

$i = 1, \dots, n$, such that $0 \leq \beta \leq 1/(\gamma_{SR} + 1)$. The relay chooses β to minimize the secrecy rate. Note that unlike the relay channel, the relay may choose not to operate with full power. The secrecy rate for this case is stated in the next theorem.

Theorem 2: The AF scheme achieves the secrecy rate

$$R_s^{(AF)} = \min_{\beta \in [0, 1/(\gamma_{SR} + 1)]} \frac{1}{2} \left[I_D^{(AF)} - I_T^{(AF)} \right]^+, \quad (2)$$

where

$$I_D^{(AF)} = \frac{1}{2} \log(1 + \gamma_{SD} + f(\gamma_{SR}, \beta\gamma_{RD})) \quad (3)$$

$$I_T^{(AF)} = \frac{1}{2} \log(1 + \gamma_{ST} + f(\gamma_{SR}, \beta\gamma_{RT})), \quad (4)$$

and $f(x, y)$ is defined as

$$f(x, y) = \frac{xy}{x + y + 1}. \quad (5)$$

Proof: The encoding and the decoding method is very similar to the direct transmission. Similarly, the equivocation calculation easily follows from Theorem 1. ■

We next study the AF secrecy rate for different relay locations. We assume the source, the destination and the wire-tapper are located at $(0, 0)$, $(0, 1)$ and $(0, 1.5)$ respectively. The relay can be anywhere on the line from $(0, 0)$ to $(0, 3)$. This is shown in Fig. 3. We have $P_S = P_R = 10$ dB, and the path loss exponent $\alpha = 2$. Note that this constitutes an example topology; however, similar observations hold for other topologies.

Fig. 4 shows how the mutual information values $I_D^{(AF)}/2$, $I_T^{(AF)}/2$ with optimal β change with variable relay location. For comparison, we also show the same quantities for direct transmission ($\beta = 0$) and for full relay power ($\beta = 1$). The secrecy rate $R_s^{(AF)}$ is also plotted on the same graph. For secrecy rate when the relay is close to the source, $d_{SR} \leq$

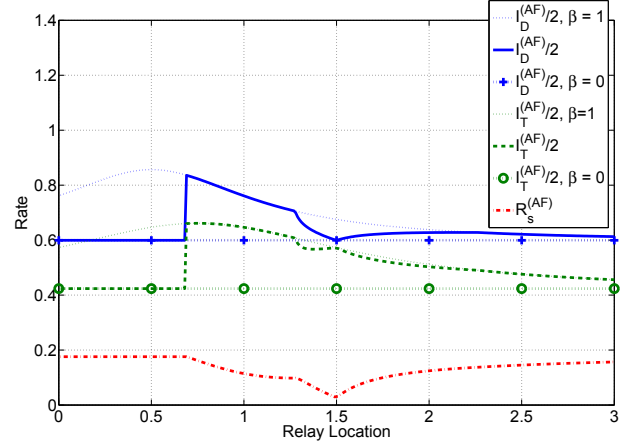


Fig. 4. The relay employs amplify and forward. The mutual information values at the destination and at the wire-tapper due to AF are equal to $I_D^{(AF)}/2$, equation (3), and $I_T^{(AF)}/2$, equation (4), respectively. The cases $\beta = 1$ (the relay transmits with full power) and $\beta = 0$ (the relay does not transmit), provide upper and lower bounds on $I_D^{(AF)}/2$ and $I_T^{(AF)}/2$ respectively. The secrecy rate $R_s^{(AF)}$ is given in (2).

0.68, we observe direct transmission behavior, the relay does not participate in the communication and sets $\beta = 0$. At these locations if the relay transmits, it unwillingly helps the destination more than it helps to the wire-tapper. If the relay were assisting the source-destination pair in the presence of a wire-tapper, then it would be operating at full power in this range.

When $0.68 < d_{SR} \leq 1.27$, the relay's contribution in terms of mutual information to the wire-tapper is more than its contribution to the destination. Here the relay transmits with full power, and the secrecy rate is smaller than direct transmission. If the relay were helping the source-destination pair, in this range, operating at full power would be suboptimal.

In the interval $1.27 < d_{SR} < 2.27$, the relay still decreases the secrecy rate but does not transmit with full-power. Especially when the relay is very close to the wire-tapper, the term $f(\gamma_{SR}, \beta\gamma_{RT})$ in (4) is close to γ_{SR} , whereas $f(\gamma_{SR}, \beta\gamma_{RD})$ in (3) is strictly smaller than $\min\{\gamma_{SR}, \beta\gamma_{RD}\}$. Therefore, by decreasing its power, the relay decreases γ_{RD} and ensures that destination does not take advantage of its transmission. When $d_{SR} \geq 2.27$, the relay again transmits with full power, and as the relay moves further, the secrecy rate converges to the direct transmission. This is because the relay's contribution to both the destination and the wire-tapper are minimal.

C. Decode and Forward

Instead of the AF protocol, the relay can choose to employ DF. The secrecy rate of DF is stated below.

Theorem 3: When the relay utilizes DF, the secrecy rate

$$R_s^{(DF)} = \begin{cases} \min_{\phi} \frac{1}{2} \left[I_D^{(DF)} - I_T^{(DF)} \right]^+ & \text{if } \mathcal{E}_{DF} \\ R_s^{(Dir)} & \text{if } \mathcal{E}_{DF}^c \end{cases}. \quad (6)$$

is achievable, where $\phi \in [0, 1]$ and

$$I_D^{(DF)} = \min \{I_{S,R}, I_{SR,D}\} \quad (7)$$

$$I_T^{(DF)} = \min \{I_{S,R}, I_{SR,T}\}, \quad (8)$$

with

$$I_{S,R} = \frac{1}{2} \log(1 + \gamma_{SR}) \quad (9)$$

$$I_{SR,D} = \frac{1}{2} \log(1 + \gamma_{SD}) + \frac{1}{2} \log(1 + \phi \gamma_{RD}) \quad (10)$$

$$I_{SR,T} = \frac{1}{2} \log(1 + \gamma_{ST}) + \frac{1}{2} \log(1 + \phi \gamma_{RT}). \quad (11)$$

The event \mathcal{E}_{DF} is defined as

$$\mathcal{E}_{DF} = \{I_{S,R} \geq I_{S,D}\}$$

with

$$I_{S,D} = \frac{1}{2} \log(1 + \gamma_{SD}).$$

The event \mathcal{E}_{DF}^c is the complement of \mathcal{E}_{DF} and $R_s^{(Dir)}$ is given in Theorem 1.

Proof: If \mathcal{E}_{DF} occurs, the received signal to noise ratio (SNR) at the relay is higher than at the destination, and the source can not prevent the relay from decoding. The best it can do is to comply with the relay. When the relay decodes the source signal, it uses an independent code book to encode the message W . Using Theorem 1 and the equivocation computation in [12], [13], one can easily conclude that the secrecy rate $\min_{\phi} [I_D^{(DF)} - I_T^{(DF)}]^+ / 2$ is achievable.

On the other hand, if the destination has higher received SNR than the relay, \mathcal{E}_{DF}^c occurs, the source simply chooses to send at the direct rate. The relay can not decode, the system reduces to direct transmission and achieves $R_s^{(Dir)}$. ■

We would like to note that the relay can also use a repetition code book, but as one would expect, an independent code book results in smaller secrecy rates, and we only present this case in this paper. In Section III-B, we have observed that the relay needs to adjust its power level to attain smaller secrecy rates. Therefore, when the relay does DF, we also assume that the relay can scale its power level with ϕ .

Fig. 5 presents $I_D^{(DF)}/2$, and $I_T^{(DF)}/2$ for optimal ϕ for the same locations as in Fig. 3. For comparison the mutual information expressions for are also plotted for $\phi = 0$, (direct transmission) and for full relay relay power $\phi = 1$. We also show $R_s^{(DF)}$ on the same graph.

We observe that when $d_{SR} > 1$, the source has no incentive to change its codebook structure, as the relay can not help the source-destination communication by DF. Therefore, the source sends at the direct transmission rate, and since the relay cannot decode this information, the wire-tapper has to rely on its direct signal received in the first time slot. This results in the direct transmission secrecy rate.

At $d_{SR} = 0.227$, $I_{S,R}$ becomes equal to $I_{SR,D}$. When $d_{SR} \leq 0.227$, the source-relay channel is very good, and $I_D^{(DF)} = I_{SR,D}$, and $I_T^{(DF)} = I_{SR,T}$. As in this range $I_{SR,D}$ is always larger than $I_{SR,T}$, the relay chooses not to transmit,

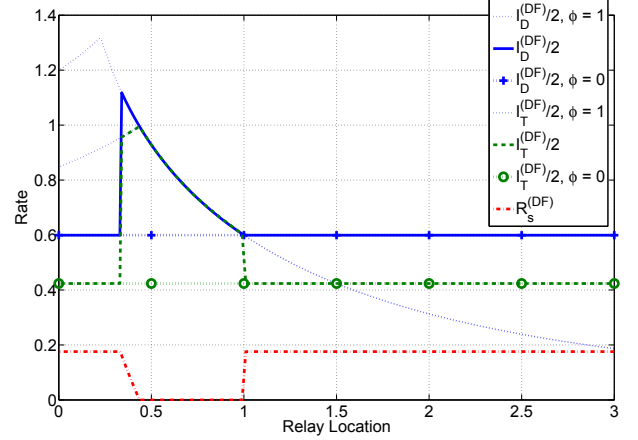


Fig. 5. The relay employs decode and forward. The mutual information values at the destination and at the wire-tapper due to DF are equal to $I_D^{(DF)}/2$, equation (7), and $I_T^{(DF)}/2$, equation (8), respectively. The cases $\phi = 1$ (the relay transmits with full power) and $\phi = 0$ (the relay does not transmit), provide upper and lower bounds on $I_D^{(DF)}/2$ and $I_T^{(DF)}/2$ respectively. The secrecy rate $R_s^{(DF)}$ is given in (6).

and sets $\phi = 0$, in order not to increase the secrecy rate above $R_s^{(Dir)}$. Note that if it was interested in helping the source and the destination, it would operate at full power. At $d_{SR} = 0.332$, $I_{S,R} = I_{SR,D}$, and the achievable secrecy rate is equal to $R_s^{(Dir)}$. Beyond this point, $R_s^{(DF)}$ starts decreasing below $R_s^{(Dir)}$. At $d_{SR} = 0.436$, the $I_{S,R} = I_{SR,T}$ and the DF protocol achieves zero secrecy rate. Therefore, in the range $0.332 < d_{S,R} < 0.436$ the relay transmits with full power. If the relay is in locations $0.436 \leq d_{SR} < 1$, for both the source-relay-destination and source-relay-wire-tapper relay channels, the source to relay channel is the bottleneck, $I_D^{(DF)} = I_T^{(DF)} = I_{S,R}$, and hence the achievable secrecy rate is zero.

D. Compress and Forward

In this subsection we assume the relay does CF. In the CF protocol, the relay compresses its received signal considering the wire-tapper's received signal $Y_T^{(1)}$ as side information. Moreover, the relay sends its compressed signal \hat{Y}_R at such a rate that it is reliably received at the wire-tapper.

Theorem 4: The CF scheme achieves the secrecy rate

$$R_s^{(CF)} = \min_{\psi \in [0,1]} \frac{1}{2} [I_D^{(CF)} - I_T^{(CF)}]^+, \quad (12)$$

where

$$I_D^{(CF)} = \begin{cases} \frac{1}{2} \log \left(1 + \gamma_{SD} + \frac{\gamma_{SR}}{\hat{N}_R + 1} \right) & \text{if } \mathcal{E}_{CF} \\ \frac{1}{2} \log(1 + \gamma_{SD}) & \text{if } \mathcal{E}_{CF}^c \end{cases} \quad (13)$$

$$I_T^{(CF)} = \frac{1}{2} \log \left(1 + \gamma_{ST} + \frac{\gamma_{SR}}{\hat{N}_R + 1} \right) \quad (14)$$

and

$$\hat{N}_R = \frac{1 + \gamma_{ST} + \gamma_{SR}}{(1 + \gamma_{ST})\psi\gamma_{RT}} \quad (15)$$

$$\mathcal{E}_{CF} = \{\gamma_{SD} \geq \gamma_{ST}, \text{ and, } \gamma_{RD} \geq \gamma_{RT}\}. \quad (16)$$

Moreover, the optimal $\psi = 1$.

Proof: The source codebook is formed using $X_S \sim \mathcal{N}(0, P_S)$. The relay compresses its received signal $Y_R^{(1)}$ according to the compression constraint

$$I(\hat{Y}_R; Y_R | Y_T^{(1)}) \leq I(X_R; Y_T^{(2)}), \quad (17)$$

We assume $\hat{Y}_R = Y_R + \hat{Z}_R$, $\hat{Z}_R \sim N(0, \hat{N}_R)$, and $X_R \sim N(0, \psi P_R)$. As in AF and DF we allow the relay not to transmit at full power.

The destination first attempts to decode X_R . Since the transmission rate of X_R is tailored to the wire-tapper, it will be able to do so if

$$I(X_R; Y_T^{(2)}) \leq I(X_R; Y_D^{(2)}),$$

which leads to the condition $\gamma_{RD} \geq \gamma_{RT}$. If decoding X_R is successful, the destination tries decoding \hat{Y}_R . This will happen with low probability of error, if

$$I(Y_T^{(1)}; \hat{Y}_R | X_R) \leq I(Y_D^{(1)}; \hat{Y}_R | X_R),$$

leading to $\gamma_{SD} \geq \gamma_{ST}$. Unless both of these conditions are satisfied, the destination ignores the relay signal, and only direct transmission rates are achievable at the destination. When the destination decodes \hat{Y}_R , it can achieve information rates $I(X_S; \hat{Y}_R, Y_D^{(1)})$ leading to the first term in $I_D^{(CF)}$.

The entropy at the wire-tapper given its observation is lower bounded as

$$\begin{aligned} & H(W | Y_{T,1}^{2n}) \\ & \stackrel{(a)}{\geq} H(W | Y_{T,1}^{2n}, \hat{Y}_{R,1}^n, X_{R,n+1}^{2n}) \\ & \stackrel{(b)}{=} H(W | Y_{T,1}^n, \hat{Y}_{R,1}^n, X_{R,n+1}^{2n}) \\ & = H(W, \hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) - H(\hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) \\ & = H(W, \hat{Y}_{R,1}^n, Y_{T,1}^n, X_{S,1}^n | X_{R,n+1}^{2n}) \\ & \quad - H(X_{S,1}^n | W, X_{R,n+1}^{2n}, \hat{Y}_{R,1}^n, Y_{T,1}^n) \\ & \quad - H(\hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) \\ & \stackrel{(c)}{=} H(W, X_{S,1}^n | X_{R,n+1}^{2n}) \\ & \quad + H(\hat{Y}_{R,1}^n, Y_{T,1}^n | W, X_{S,1}^n, X_{R,n+1}^{2n}) \\ & \quad - H(\hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) \\ & \stackrel{(d)}{=} H(W, X_{S,1}^n | X_{R,n+1}^{2n}) + H(\hat{Y}_{R,1}^n, Y_{T,1}^n | X_{S,1}^n, X_{R,n+1}^{2n}) \\ & \quad - H(\hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) \\ & = H(W, X_{S,1}^n | X_{R,n+1}^{2n}) - I(X_{S,1}^n; \hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) \\ & \stackrel{(e)}{\geq} H(X_{S,1}^n | X_{R,n+1}^{2n}) - I(X_{S,1}^n; \hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) \\ & \stackrel{(f)}{=} H(X_{S,1}^n) - I(X_{S,1}^n; \hat{Y}_{R,1}^n, Y_{T,1}^n) \\ & \stackrel{(g)}{=} nH(X_S) - nI(X_S; \hat{Y}_R, Y_T^{(1)}), \end{aligned} \quad (18)$$

where we have (a) because conditioning reduces entropy, (b) is because given $X_{R,n+1}^{2n}, Y_{T,n+1}^{2n}$ is independent from all other random variables, (c) follows as

$$H(X_{S,1}^n | W, X_{R,n+1}^{2n}, \hat{Y}_{R,1}^n, Y_{T,1}^n) \leq H(X_{S,1}^n | W) = 0,$$

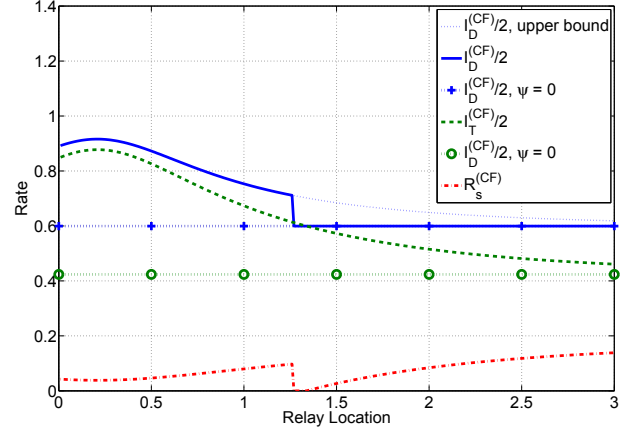


Fig. 6. The relay employs compress and forward. The mutual information values at the destination and at the wire-tapper due to CF are equal to $I_D^{(CF)}/2$, equation (13), and $I_T^{(CF)}/2$, equation (14), respectively. The case $\psi = 0$ (the relay does not transmit), provide a lower bound on $I_D^{(CF)}/2$ and $I_T^{(CF)}/2$ respectively. The upper bound on $I_D^{(CF)}/2$ assumes the destination can always decode the relay's signal. The secrecy rate $R_s^{(CF)}$ is given in (12).

(d) follows as $W \rightarrow (X_{S,1}^n, X_{R,n+1}^{2n}) \rightarrow (\hat{Y}_R, Y_{T,1}^n)$, we have (e) as $H(W, X_{S,1}^n | X_{R,n+1}^{2n}) \geq H(X_{S,1}^n | X_{R,n+1}^{2n})$, (f) follows because $p(x_S)$ and $p(x_R)$ are independent, and

$$I(X_{S,1}^n; \hat{Y}_{R,1}^n, Y_{T,1}^n | X_{R,n+1}^{2n}) = I(X_{S,1}^n; \hat{Y}_{R,1}^n, Y_{T,1}^n),$$

and finally (g) is because $X_{S,i}$ are i.i.d.

Using [8, Lemma 6], we have $nH(X_S) \geq nI_D^{(CF)} - 1$, and hence we obtain the secrecy rate $R_s^{(CF)}$ after normalizing the above lower bound with $2n$. Finally, as both for \mathcal{E}_{CF} and its complement, $R_s^{(CF)}$ is differentiable in ψ , one can easily prove that $R_s^{(CF)}$ is minimized for $\psi = 1$. ■

Note that in CF the relay signal (X_R, \hat{Y}_R) is especially tailored for the wire-tapper, and the destination has no guarantee of decoding the correct (X_R, \hat{Y}_R) . Moreover, even if the destination successfully decodes them, the compression noise variance \hat{N}_R satisfies the wire-tapper's compression constraint (17). If the relay was helping the destination, then the compression noise would have a smaller variance. Therefore, in CF protocol, the wire-tapper takes full advantage of the relay, while the destination cannot.

When the relay does CF for the wire-tapper, the equivocation lower bound becomes tight as the wire-tapper can reliably decode X_R and \hat{Y}_R using its observation in the second time slot. If the relay did CF for the destination, the bound would not be tight anymore and finding a lower bound on the equivocation rate would be more difficult. This is because equivocation is a soft metric, and the wire-tapper does not need to decode X_R and \hat{Y}_R reliably to lower its confusion.

In Fig. 6, we plot $R_s^{(CF)}$, $I_D^{(CF)}/2$, $I_T^{(CF)}/2$. The upper bound on $I_D^{(CF)}/2$ assumes that the destination can always decode the relay's signal X_R and also obtains \hat{Y}_R . We also plot $I_D^{(CF)}/2$ and $I_T^{(CF)}/2$ for $\psi = 0$, which is equivalent to direct

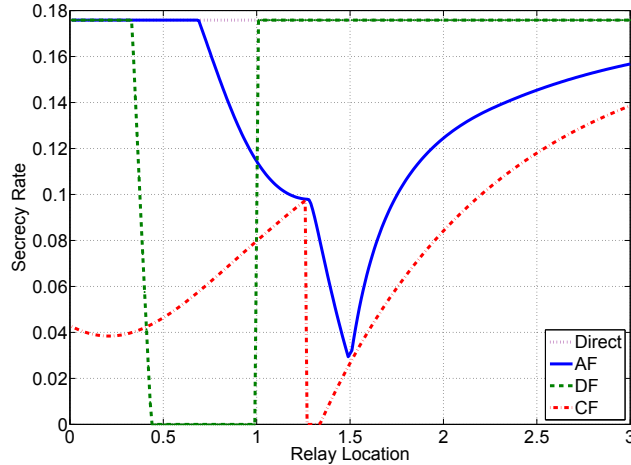


Fig. 7. Secrecy rates for direct transmission, amplify and forward, decode and forward, and compress and forward protocols as a function of relay location.

transmission. When the relay is in the range $0 < d_{SR} \leq 1.25$, the destination can decode X_R and \hat{Y}_R successfully and we obtain secrecy rates smaller than $R_s^{(Dir)}$. When $d_{SR} > 1.25$, the destination can no longer decode (X_R, \hat{Y}_R) , thus ignores the relay signal. That's why in this range the $I_D^{(CF)} = I_D^{(Dir)}$. However, the wire-tapper continues to make use of the relay.

E. Discussion

Fig. 7 compares the achievable secrecy rates by direct transmission, AF, DF, and CF protocols. We observe that when the relay is very close to the source, the CF protocol achieves the smallest secrecy rate. Note that, if the destination did not hear the relay, this would not be the case. This is because for the source-relay-wire-tap channel, whenever the relay is close to the source, DF results in larger mutual information at the wire-tapper than CF [15]. (This can also be observed comparing $I_T^{(CF)}/2$ and the upper bound on $I_T^{(DF)}/2$ from Fig. 6 and Fig. 5.) When the relay is closer to the destination than the source, and has a better channel than the destination, the DF protocol is optimal from the perspective of the wire-tapper and achieves zero secrecy rate. Whenever the relay has a worse channel to the source than the destination, then the CF protocol achieves the smallest secrecy rate.

When the relay helps the source-destination communication in the presence of a wire-tapper, the noise forwarding strategy is suggested to improve secrecy rates [16]. In this scheme the relay simply sends noise, which weakens the wire-tapper's received SNR more than the destination's. In our setup a noise forwarding scheme is not meaningful because of time-division. If the relay transmits noise, then it will not be useful to the wire-tapper, and the destination will always ignore the relay signal. For a non-orthogonal channel allocation, in which the source transmits all the time, relay listens for a fraction of it and transmits in the remaining, noise forwarding can be useful.

IV. CONCLUSION

In this work we studied a four terminal Gaussian network, composed of a source, a destination, a relay and a wire-tapper, in which the relay assists the wire-tapper. We compared direct transmission, AF, DF, and CF protocols in terms of achievable secrecy rates. We observed that the comparison between these protocols is not a trivial extension of the results for the classical relay channel. Also unlike the classical relay channel, where the relay always transmits with full power, power allocation at the relay is essential for optimizing secrecy rates in the presence of a wire-tapper.

ACKNOWLEDGMENT

This material is based upon work partially supported by the NSF under Grant No. 0093163.

REFERENCES

- [1] E. C. van der Meulen, "Three-terminal communication channels," *Advances in Applied Probability*, vol. 3, p. 121, 1971.
- [2] T. M. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, p. 572, September 1979.
- [3] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, p. 3062, December 2004.
- [4] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity-Part I, Part II," *IEEE Transactions on Communications*, vol. 51, no. 11, p. 1927, November 2003.
- [5] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, p. 1355, October 1975.
- [6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, p. 339, May 1978.
- [7] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, p. 451, July 1978.
- [8] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," April 2006, submitted to IEEE Transactions on Information Theory.
- [9] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," May 2006, submitted to IEEE Transactions on Information Theory.
- [10] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proceedings of 44th Allerton Conference on Communication, Control and Computing*, September 2006.
- [11] Y. Oohama, "Coding for relay channels with confidential messages," in *Proceedings of IEEE Information Theory Workshop*, 2001.
- [12] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proceedings of 41st Conference of Information Sciences and Systems*, 2007.
- [13] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," December 2006, submitted to IEEE Transactions on Information Theory.
- [14] K. Lu, Y. Qian, and H. Chen, "A secure and service-oriented network control framework for WiMAX networks," *IEEE Communications Magazine*, vol. 45, no. 5, p. 124, May 2007.
- [15] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Transactions on Information Theory*, vol. 51, no. 9, p. 3037, 2005.
- [16] L. Lai, K. Liu, and H. E. Gamal, "The three node wireless network: Achievable rates and cooperation strategies," *IEEE Transactions on Information Theory*, vol. 52, no. 3, p. 805, March 2006.