COOPERATION FOR SECURE COMMUNICATION: THE RELAY WIRETAP CHANNEL

Lifeng Lai and Hesham El Gamal

Department of Electrical and Computer Engineering
Ohio State University
Columbus, OH 43202, USA
Email: {lail,helgamal}@ece.osu.edu

ABSTRACT

It is well known that a non-zero secrecy capacity of the wiretap channel is only possible when the legitimate receiver is less noisy than the wiretapper. This work shows that user cooperation is an efficient solution to this limitation. In particular, the four-terminal wiretap relay channel is considered in our work where several cooperation strategies, that enable secure communication, are constructed and the corresponding rate-equivocation regions are characterized. Of particular interest is the novel *noise forwarding* strategy which establishes the *deaf helper phenomenon*. Here, the relay is able to facilitate secure communication over the main channel while being totally ignorant of the transmitted message. The gain offered by the proposed strategies is proved theoretically and validated numerically in the additive white Gaussian noise (AWGN) channel. Overall, our work establishes the utility of user cooperation in facilitating secure communication over wireless channels.

Keywords: cooperation, wiretapper, relay, secure communication

1. INTRODUCTION

Most, if not all, of the cryptosystems widely used nowadays are based on the unproved difficulty of solving some mathematic problems. For example, the RSA scheme is based on the assumption that it is difficult to factorize big prime numbers. These systems are only computational secure since the proper operation of these system depends on the difficulty of solving some mathematical problems and the limited computation ability assumption of the wiretapper. With the rapid developments of computing technologies and algorithm design techniques, cryptosystems that are based on assumptions of enemies' computation ability and unproved mathematical problems will eventually be outdated.

The strong notion of information theoretic security was introduced by Shannon [1]. Perfect information theoretic secrecy requires $I(W;Z) = 0$, which means that the signal Z that the wiretapper receives provides no further information about the message W sent by the source than its *a prior* information about W. The model in [1] assumed that the transmission is noiseless, hence the signal Z that the wiretapper receives and the signal Y received by the legitimate destination are identical with the signal X. Under this model, Shannon proved a negative result stating that perfect secrecy requires the entropy of the private key K, used to encrypt the message W, to be larger than the entropy of the message, that is $H(K) \geq H(W)$. Taking the channel uncertainty into consideration, Wyner introduced the wiretap channel in [2]. In this model, a source wishes to transmit confidential messages to a destination while keeping the message as secret as possible from a wiretapper, who has unlimited computation ability and knows the coding/decoding scheme used in the main channel. Wyner characterized the trade-off between the information rate to the receiver and the level of secrecy, as measured by equivocation, under the assumption that the wiretapper channel is a degraded version of the main channel. In particular, Wyner showed that the secrecy capacity (i.e., perfectly secure rate) is nonzero. Csiszár and Körner [3] extended this work to the broadcast channel, where the source sends a common message to both the receiver and the wiretapper, and a confidential message only to the receiver. They showed that if the main channel is less noisy than the wiretap channel, it is possible to achieve a positive perfect secrecy capacity. The relay channel with confidential messages was studied in [4], where the relay node acts both as wiretapper and helper. The source sends common message to the receiver under the help of the relay node, but sends a private message to the receiver while keeping it secret from the relay.

This paper investigates the role of user cooperation in enhancing network security. This work is stimulated by the fact that the conditions in [2, 3], such as degradedness, less noisy or more capable, are **not** always true. In this situation, the perfect secrecy capacity of the channel is zero, implying the **infeasibility** of secure communication. Here, we show that that a relay (helper) node can play a critical role in facilitating secure communication under this assumption. In our model, contrary to [4], the relay node is a trusted partner different from the wiretapper. Therefore, this model generalizes the relay channel [5] and the wiretap channel [2].

2. MODEL

We consider a discrete relay wiretap channel consisting of finite sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, \mathcal{Y}_1, \mathcal{Y}_2$ and a transition probability distribution $p(y, y_1, y_2|x_1, x_2)$, as shown in Figure 1. Here, $\mathcal{X}_1, \mathcal{X}_2$ are the channel inputs from the source and the relay respectively, while $\mathcal{Y}, \mathcal{Y}_1, \mathcal{Y}_2$ are the channel outputs at the receiver,

the relay and the wiretapper respectively. We consider the memoryless channel, hence the channel outputs $(y_i, y_{1,i}, y_{2,i})$ at time i only depend on the channel inputs $(x_{1,i}, x_{2,i})$ at time i. The source wishes to send message $W_1 \in \mathcal{W}_1 =$

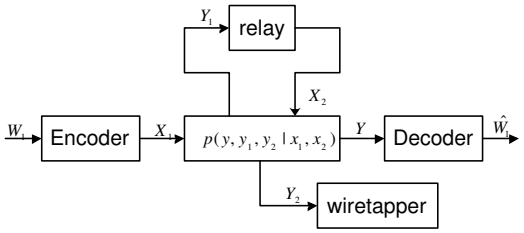

Fig. 1. The relay wiretap channel.

$\{1, 2, \cdots, M\}$ to the destination. An (M, n) code consists of the following elements: 1) a stochastic encoder f_n at the source that maps the message w_1 to a codeword $\mathbf{x}_1 \in \mathcal{X}_1^n$, 2) a relay function at the relay node that maps the signals $(y_{1,1}, y_{1,2}, \cdots, y_{1,i-1})$ received before time i into the channel input $x_{2,i}$, using the mapping φ_i: $(Y_{1,1}, Y_{1,2}, \cdots, Y_{1,i-1}) \rightarrow X_{2,i}$, 3) a decoding function ϕ: $\mathcal{Y}^n \rightarrow \mathcal{W}_1$. The average error probability of a (M, n) code is defined as

$$P_e^n = \sum_{w_1 \in \mathcal{W}_1} \frac{1}{M} \Pr\{\phi(\mathbf{y}) \neq w_1 | w_1 \text{ was sent}\}. \quad (1)$$

The equivocation rate at the wiretapper is $R_e = \frac{1}{n} H(W_1|\mathbf{Y}_2)$.

The rate-equivocation pair (R_1, R_e) is said to be achievable if for any $\epsilon > 0$, there exists a sequence of codes (M, n) such that for any $n \geq n(\epsilon)$, we have

$$R_1 = \frac{1}{n} \log_2 M, \quad (2)$$

$$P_e^n \leq \epsilon, \quad (3)$$

$$\frac{1}{n} H(W_1|\mathbf{Y}_2) \geq R_e - \epsilon. \quad (4)$$

We further say that the perfect secrecy rate R_1 is achievable if the rate-equivocation pair (R_1, R_1) is achievable.

3. COOPERATION STRATEGIES

Due to space limitation, we limit our discussion in this section to the Decode and Forward (DF) and Noise Forwarding (NF) schemes. In [6], we derive an outer bound on the rate-equivocation region and characterize the region achieved by Compress and Forward (CF) cooperation. Interested readers can also refer [6] for the proofs of the theorems in this paper.

3.1. Decode and Forward

In DF cooperation, the relay node will first decode codewords from the source and then cooperate with source to send secret messages to the destination. The basic idea is that after decoding, the relay and the source can beam-form toward the destination to enable a larger rate gain in the main channel than the wiretap channel.

Theorem 1 *The rate pairs in the closure of the convex hull of all (R_1, R_e) satisfying*

$$\begin{aligned} R_1 &< \min\{I(X_1, X_2; Y), I(X_1; Y_1|X_2)\}, \\ R_e &< R_1, \\ R_e &< \min\{I(X_1, X_2; Y), I(X_1; Y_1|X_2)\} - I(X_1, X_2; Y_2), \end{aligned} \quad (5)$$

for some distribution $p(x_1, x_2, y_1, y_2, y) = p(y_1, y_2, y|x_1, x_2)$ $p(x_1, x_2)$ are achievable in the relay wiretap channel when the relay node uses DF scheme.

3.2. Noise-Forwarding

When the source-relay channel is very noisy, it becomes the **bottleneck** in the DF scheme. In this section, we design a novel scheme which facilitates perfectly secure communication without requiring the relay to **listen** to the message transmitted by the source (i.e., deaf relay). The enabling observation is that, in the wiretap channel, besides its own information, the source should send extra codewords to confuse the wiretapper. In our setting, this task can be done partially by the relay node. Hence, the relay node can help the transmitter without even attempting to listen to the transmitted message. Here, we assume that the **noise codebook** used by the relay is known everywhere. With NF, the relay wiretap channel reduces to a compound MAC channel, where the (source/relay)- receiver link is the first MAC channel and (source/relay)-wiretapper link is the second one. Figure 2 shows the rate region of these two MACs for a fixed input distribution $p(x_1)p(x_2)$. In the figure, we let the source rate be R_1, and the relay rate be R_2. From this figure, we can see that if the relay node doesn't transmit, it is impossible for the source to transmit any confidential message, since $R_1(A) < R_1(C)$. On the other hand, if the relay and the source coordinate their transmission and operate at the point B, we can achieve equivocation rate R_e, which is strictly larger than zero. This illustrates the main idea behind the NF scheme.

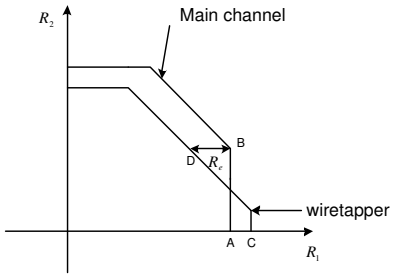

Fig. 2. The compound MAC of the relay wiretap channel.

The following theorem characterizes the achievable rate-equivocation region of this scheme, when $I(X_1; Y|X_2) < I(X_1; Y_2|X_2)$, *i.e.*, the channel between the source and the wiretapper is better than the channel between the source and the destination (a situation of primary interest to this paper).

Theorem 2 *The rate pairs in the closure of the convex hull of all (R_1, R_e) satisfying*

$$\begin{aligned} R_1 &< I(X_1;Y|X_2), \\ R_e &< R_1, \\ R_e &< \min\{I(X_2;Y), I(X_2;Y_2|X_1)\} + I(X_1;Y|X_2) \\ &\quad -I(X_1,X_2;Y_2), \end{aligned} \tag{6}$$

for some distribution $p(x_1,x_2,y_1,y_2,y) = p(y_1,y_2,y|x_1,x_2)$ $p(x_1)p(x_2)$, are achievable.

4. THE AWGN CHANNEL

In this case, the signal seen by each receiver is given

$$y_j = \sum_{i\neq j} h_{ij}x_i + z_j,$$

here h_{ij} is the channel coefficient between node i and node j, and z_j is the i.i.d Gaussian noise with unit variance at node j. The source and the relay have average power constraint P_1, P_2 respectively. We know that if $h_{sw}^2 \geq h_{sd}^2$ and there is no relay, it is impossible for the source to send confidential messages to the receiver, no matter how large the power P_1 is. Hence $R_s = 0$. On the other hand, if the relay node can join in the transmission, we can get positive perfect secrecy rate under some conditions even when $h_{sw}^2 \geq h_{sd}^2$. In the following, we consider the case $h_{sw}^2 \geq h_{sd}^2$, hence the secrecy capacity of the channel without relay is 0. In this paper, we use Gaussian input distribution to obtain an achievable lower bound (characterizing the optimal input distribution is beyond the scope of this work).

First consider the DF scheme, and we let $X_2 \sim \mathcal{N}(0,\beta P_2)$, $X_{10} \sim \mathcal{N}(0,P)$, where $\mathcal{N}(0,P)$ means Gaussian distribution with zero mean and variance P. Also, let

$$X_1 = c_1X_2 + X_{10}, \tag{7}$$

where c_1 is a constant to be specified later. This equation means that, besides injecting new information through X_{10}, the source also spends some of its available energy in cooperating with the relay to do beam-forming toward the receiver at each block. To satisfy the average power constraint at the source, we require $c_1^2\beta P_2 + P \leq P_1$. Here, $0 \leq \beta \leq 1$ is the part of the available power that the relay uses to transmit. Since in the DF scheme, the relay decodes the codewords sent by the source, hence, it is possible for them to do beam-forming toward the receiver while cancelling out the signal at the wiretapper. This could be done by appropriately choosing the parameter c_1. Straight forward calculation shows that

$$I(X_1;Y_1|X_2) = \frac{1}{2}\log_2(1+h_{sr}^2P),$$

$$I(X_1,X_2;Y) = \frac{1}{2}\log_2(1+(h_{sd}c_1+h_{rd})^2\beta P_2 + h_{sd}^2P),$$

$$I(X_1,X_2;Y_2) = \frac{1}{2}\log_2(1+(h_{sw}c_1+h_{rw})^2\beta P_2 + h_{sw}^2P).$$

Hence, we have $R_{s,DF} = \max\limits_{\beta,c_1,P} \min\{R_{1,e}, R_{2,e}\}$, where

$$R_{1,e} = \frac{1}{2}\log_2\Big(\frac{1+h_{sr}^2P}{1+(h_{sw}c_1+h_{rw})^2\beta P_2 + h_{sw}^2P}\Big),$$

$$R_{2,e} = \frac{1}{2}\log_2\Big(\frac{1+(h_{sd}c_1+h_{rd})^2\beta P_2 + h_{sd}^2P}{1+(h_{sw}c_1+h_{rw})^2\beta P_2 + h_{sw}^2P}\Big).$$

For the NF, we let $X_1 \sim \mathcal{N}(0,\alpha P_1)$, $X_2 \sim \mathcal{N}(0,\beta P_2)$, where $0 \leq \alpha \leq 1, 0 \leq \beta \leq 1$. Here X_1, X_2 are independent, and hence, we have

$$\begin{aligned} &I(X_1;Y|X_2) = \frac{1}{2}\log_2\Big(1+\alpha h_{sd}^2P_1\Big), \\ &I(X_1,X_2;Y) - I(X_1,X_2;Y_2) \\ &\quad = \frac{1}{2}\log_2\Big(\frac{1+\alpha h_{sd}^2P_1+\beta h_{rd}^2P_2}{1+\alpha h_{sw}^2P_1+\beta h_{rw}^2P_2}\Big), \\ &I(X_2;Y_2|X_1) + I(X_1;Y|X_2) - I(X_1,X_2;Y_2) \\ &\quad = \frac{1}{2}\log_2\Big(\frac{(1+h_{rw}^2\beta P_2)(1+h_{sd}^2\alpha P_1)}{1+\alpha h_{sw}^2P_1+\beta h_{rw}^2P_2}\Big). \end{aligned}$$

Hence, we have

$$\begin{aligned} R_{s,NF} &= \max_{\alpha,\beta} \min\Big\{\frac{1}{2}\log_2\Big(1+\alpha h_{sd}^2P_1\Big), \\ &\quad \frac{1}{2}\log_2\Big(\frac{1+\alpha h_{sd}^2P_1+\beta h_{rd}^2P_2}{1+\alpha h_{sw}^2P_1+\beta h_{rw}^2P_2}\Big), \\ &\quad \frac{1}{2}\log_2\Big(\frac{(1+h_{rw}^2\beta P_2)(1+h_{sd}^2\alpha P_1)}{1+\alpha h_{sw}^2P_1+\beta h_{rw}^2P_2}\Big)\Big\}. \end{aligned} \tag{8}$$

In the following, we consider the amplify and forward cooperation scheme (we did not consider this scheme is the discrete case since, in general, it does not lend itself to a single letter characterization). In this scheme, the source encodes its messages into codewords with length ML each and divides each codeword into L sub-blocks each with M symbols, where L is chosen to be sufficiently large. At each sub-block, the relay sends a linear combination of the received noisy signal of this sub-block so far. For simplicity, we limit our discussion to the simple case with $M = 2$. In this case, the source sends $X_1(1)$ at the first symbol of each sub-block, the relay receives $Y_1(1) = h_{sr}X_1(1) + Z_1(1)$; At the second symbol, the source sends $\alpha X_1(1) + \beta X_1(2)$, while the relay sends $\gamma Y_1(1)$. Here α, β, γ are chosen to satisfy the average power constraints at the source and the relay. Thus, this scheme allows beam-forming between the source and relay without requiring the relay to fully decode.

Writing the signal received at the destination and the wiretapper in matrix form, we have $\mathbf{Y} = \mathbf{H}_1\mathbf{X}_1 + \mathbf{Z}$, $\mathbf{Y}_2 = \mathbf{H}_2\mathbf{X}_1 + \mathbf{Z}_2$, where

$$\begin{aligned} \mathbf{H}_1 &= \begin{bmatrix} h_{sd} & 0 \\ \beta h_{sd} + \gamma h_{sr}h_{rd} & \alpha h_{sd} \end{bmatrix}, \\ \mathbf{H}_2 &= \begin{bmatrix} h_{sw} & 0 \\ \beta h_{sw} + \gamma h_{sr}h_{rw} & \alpha h_{sw} \end{bmatrix}, \end{aligned} \tag{9}$$

$\mathbf{X}_1 = [X_1(1), X_1(2)]^T, \mathbf{Z} = [Z(1), \gamma h_{rd}Z_1(1)+Z(2)]^T, \mathbf{Z}_2 = [Z_2(1), \gamma h_{rw}Z_1(1)+Z_2(2)]^T$. Hence, the channel under consideration can be viewed as an equivalent standard memoryless wiretap channel with input $\mathbf{X}_1$ and outputs $\mathbf{Y}, \mathbf{Y}_2$ at the

destination and the wiretapper respectively. Then, based on the result of [3], an achievable perfect secure rate is $I(\mathbf{X}_1;\mathbf{Y})-I(\mathbf{X}_1;\mathbf{Y}_2)$.

Choosing Gaussian input with covariance matrix $\mathbb{E}\{\mathbf{X}\mathbf{X}^T\}=P\mathbf{I}$, we get the following achievable perfect secrecy rate

$$\begin{aligned} R_{s,AF} &= \max_{\alpha,\beta,\gamma,P}\Big[\frac{1}{4}\log_2\frac{|\det\{P\mathbf{H}_1\mathbf{H}_1^T+\mathbb{E}\{\mathbf{Z}\mathbf{Z}^T\}\}|}{|\det\{\mathbb{E}\{\mathbf{Z}\mathbf{Z}^T\}\}|} \\ &\quad -\frac{1}{4}\log_2\frac{|\det\{P\mathbf{H}_2\mathbf{H}_2^T+\mathbb{E}\{\mathbf{Z}_2\mathbf{Z}_2^T\}\}|}{|\det\{\mathbb{E}\{\mathbf{Z}_2\mathbf{Z}_2^T\}\}|}\Big] \\ &= \max_{\alpha,\beta,\gamma,P}\frac{1}{4}\log_2\frac{|\det\{P\mathbf{H}_1\mathbf{H}_1^T+\mathbf{A}\}\det\mathbf{B}|}{|\det\{P\mathbf{H}_2\mathbf{H}_2^T+\mathbf{B}\}\det\mathbf{A}|}, \end{aligned} \quad (10)$$

where

$$\mathbf{A}=\begin{bmatrix}1 & 0\\ 0 & 1+\gamma^2h_{rd}^2\end{bmatrix},\mathbf{B}=\begin{bmatrix}1 & 0\\ 0 & 1+\gamma^2h_{rw}^2\end{bmatrix},$$

and the maximization is over the set of power constraints: $(1+\alpha^2+\beta^2)P\le 2P_1, \gamma^2(h_{sr}^2P+1)\le 2P_2$.

Figure 3 shows the achievable perfect secrecy capacity of various schemes when we put a source at $(0,0)$, a destination at $(1,0)$, a wiretapper at $(0,1)$, and a relay node at $(x,0)$. We let $P_1=1, P_2=8$. In generating this figure, we assume that in addition to path loss, each channel also has an independent phase fading, that is $h_{ij}=d_{ij}^{-\gamma}e^{j\theta_{ij}}$, where θ_{ij} is uniformly distributed over $[0,2\pi)$. We assume that before transmission, the source knows the phase of $\theta_{sr},\theta_{sd},\theta_{rd}$, but doesn't know θ_{sw},θ_{rw}. Since $d_{sd}=d_{sw}$, the perfect secrecy capacity of the wiretap channel without the relay node is zero, no matter how large the power the source has.

The random phase will only affect the performance of schemes that depend on beam-forming between the source and the relay (i.e., DF and AF). Consider the DF scheme, and let c_1 in (7) be $d_1e^{j(\theta_{rd}-\theta_{sd})}$, where d_1 is a real number. In this way, the signals of the source and the relay will add up coherently at the destination, but not at the wiretapper since θ_{sw},θ_{rw} are independent with θ_{sd},θ_{rd}. To satisfy the average power constraint at the source, we need $d_1^2\beta P_2+P\le P_1$. Straight forward calculation shows

$$R_{s,DF}=\max_{\beta,d_1,P}\min\Big\{\frac{1}{2}\log_2(1+|h_{sr}|^2P)-R_w,$$
$$\frac{1}{2}\log_2(1+(|h_{sd}|d_1+|h_{rd}|)^2\beta P_2+|h_{sd}|^2P)-R_w\Big\}, \quad (11)$$

where $R_w=\frac{1}{2}\mathbb{E}_{\theta_{sw},\theta_{rd},\theta_{sd},\theta_{rw}}\Big\{\log_2\Big(1+(|h_{sw}|^2d_1^2+|h_{rw}|^2+2d_1|h_{sw}h_{rw}|\cos\theta)\beta P_2+|h_{sw}|^2P\Big)\Big\}$, in which $\theta=\theta_{sw}+\theta_{rd}-\theta_{sd}-\theta_{rw}$.

Similarly, we can get the perfectly secure rate achieved by the AF scheme under this channel model.

The gain offered by the three proposed cooperation strategies is evident in the figure. Moreover, it is shown that when $x>1$ the DF scheme doesn't offer any benefits since the bottleneck is at the relay node. But both NF and AF still offer positive gains. Finally, we wish to stress the **uniqueness** of the NF strategy in the sense that 1) it does not require the relay to listen to the source transmission and 2) it only offers a performance gain in the presence of the wiretapper.

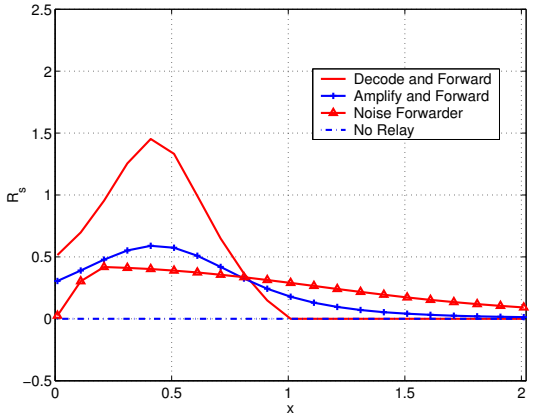

Fig. 3. The achievable perfect secrecy capacity for various schemes in the Gaussian relay wiretap channel with phase fading.

5. CONCLUSIONS

Here, we established a novel utility of user cooperation in facilitating secure communication in wireless networks wiretappers (eavesdroppers). Towards this end, we constructed several cooperation strategies for the relay wiretap channel and characterized the corresponding achievable performance. Our analysis, and numerical results, showed that the proposed schemes offer non-zero secrecy when the wiretap channel is more capable (less noisy) than the main channel. Of particular interest is the proposed noise forwarding strategy which shows that the relay can help in creating a secure source-destination link without listening to the source signal.

6. REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, pp. 339–348, May 1978.

[4] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, (Cairns, Australia), pp. 87 – 89, Sept. 2-7, 2001.

[5] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. on Information Theory*, vol. 25, pp. 572–584, Sep. 1979.

[6] L. Lai and H. El-Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. on Information Theory*, Dec 2006. Submitted.