Secure Communications over Wireless Channels

Lifeng Lai, Praveen Kumar Gopala and Hesham El Gamal
Department of Electrical and Computer Engineering
The Ohio State University
Columbus, OH 43210
Email: {lail,gopalap,helgamal}@ece.osu.edu

***Abstract*— In this work, we present new techniques that leverage the wireless medium in facilitating secure communications in the presence of eavesdroppers. First, we consider the secure transmission of information over an ergodic fading channel with long coherence intervals. The secrecy capacity of such a system is characterized under different assumptions on the available channel state information. We then propose a low-complexity on/off power allocation strategy which becomes asymptotically optimal as the average SNR grows. Remarkably, our results reveal the positive impact of fading on the secrecy capacity and establish the critical role of rate adaptation in enabling secure communications over slow fading channels. Moreover, we discuss the utility of user cooperation in establishing secure communication links. In particular, we construct novel cooperation strategies for the relay channel with an eavesdropper. One of the proposed strategies, i.e., noise forwarding, is used to illustrate the deaf helper phenomenon, where the relay is able to create a secure source-destination channel while being totally ignorant of the transmitted message.**

I. Introduction

The notion of information-theoretic secrecy was first introduced by Shannon [1]. This strong notion of secrecy does not rely on any assumptions on the computational resources of the eavesdropper. More specifically, perfect information-theoretic secrecy requires that $I(W;Z) = 0$, i.e., the signal Z received by the eavesdropper does not provide any additional information about the transmitted message W. Shannon considered a scenario where both the legitimate receiver and the eavesdropper have direct access to the transmitted signal. Under this model, he proved a negative result implying that the achievability of perfect secrecy requires the entropy of the private key K, used to encrypt the message W, to be larger than or equal to the entropy of the message itself (i.e., $H(K) \geq H(W)$ for perfect secrecy). Wyner [2] introduced the wiretap channel which accounts for the difference in the two noise processes, as observed by the destination and wiretapper. In this model, the wiretapper has no computational limitations and is assumed to know the codebook used by the transmitter. Under the assumption that the wiretapper's signal is a degraded version of the destination's signal, Wyner characterized the tradeoff between the information rate to the destination and the level of ignorance at the wiretapper (measured by its equivocation), and showed that it is possible to achieve a non-zero secrecy capacity. This work was later extended to non-degraded channels by Csiszár and Körner [3], where it was shown that if the main channel is less noisy than the wiretapper channel, then it is possible to achieve a non-zero secrecy capacity. However, if the wiretapper channel is less noisy than the main channel, the secrecy capacity will be zero. In this case, we will be unable to establish a secure link under Wyner's model. Motivated by this fact, we focus on the wireless setting and leverage the unique features of wireless channels to facilitate secure communications.

We first consider secure communications over fading channels and show that channel fading can be exploited to yield *opportunistic* secrecy, where one can achieve a perfectly secure non-zero rate even when the eavesdropper channel is more capable then the legitimate channel **on the average**. In particular, our work here characterizes the secrecy capacity of the slow fading channel in the presence of an eavesdropper. Our eavesdropper is the wireless counterpart of Wyner's wiretapper. We first assume that the transmitter knows the CSI of both the legitimate and eavesdropper channels, and derive the optimal power allocation strategy that achieves the secrecy capacity. Next we consider the case where the transmitter only knows the legitimate channel CSI and, again, derive the optimal power allocation strategy. We then propose an on/off power transmission scheme, with variable rate allocation, which approaches the optimal performance for asymptotically large average SNR. Interestingly, this scheme is also shown to attain the secrecy capacity under the full CSI assumption which implies that, at high SNR values, the additional knowledge of the eavesdropper CSI does not yield any gains in terms of the secrecy capacity for slow fading channels. Finally, our theoretical and numerical results are used to argue that rate adaptation plays a more critical role than power control in achieving the secrecy capacity of slow fading channels. This observation contrasts the scenario without secrecy constraints, where transmission strategies with constant rate are able to achieve capacity. Recent works on the effect of slow fading on the secrecy capacity could be found in [4], [5].

We then investigate the role of user-cooperation in secure communications and show that it can provide us with *cooperative* secrecy. Our main idea is to exploit user cooperation in facilitating the transmission of confidential messages from the source to the destination. More specifically, we consider a four-terminal relay-eavesdropper channel, where a source wishes to send messages to a destination while leveraging the help of a relay node to hide those messages from the eavesdropper. Here we identify a novel role of the relay node in establishing a secure link from the source to the destination. Towards this end, several cooperation strategies for the relay-eavesdropper channel are constructed and the corresponding achieved rate-equivocation regions are characterized. The proposed schemes are shown to achieve a positive perfect secrecy rate in several scenarios where the secrecy capacity in the absence of the relay node is zero. We then compute the perfect secrecy rates of the proposed schemes in the AWGN channel assuming gaussian inputs and show that the proposed schemes

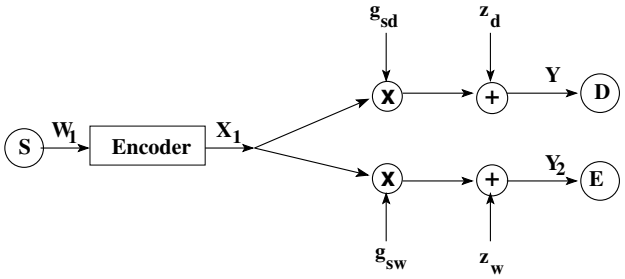

Fig. 1. The Fading Channel with an Eavesdropper

can provide us with a nonzero perfect secrecy rate even when both the destination and the relay are in disadvantageous positions.

Due to space limitations, we omit detailed proofs here. Interested readers can refer to [6], [7] for details.

II. Opportunistic secrecy

In this section, we consider the secure communication over fading channels. The system model is illustrated in Fig. 1. The source S communicates with a destination D in the presence of an eavesdropper E. During any coherence interval i, the signal received by the destination and the eavesdropper are given by, respectively

$$\begin{aligned} y(i) &= g_{sd}(i)x_1(i) + z_d(i), \\ y_2(i) &= g_{sw}(i)x_1(i) + z_w(i), \end{aligned}$$

where $g_{sd}(i), g_{sw}(i)$ are the channel gains from the source to the legitimate receiver (main channel) and the eavesdropper (eavesdropper channel) respectively, and $z_d(i), z_w(i)$ represent the i.i.d additive Gaussian noise with unit variance at the destination and the eavesdropper respectively. We denote the fading power gains of the main and eavesdropper channels by $h_{sd}(i) = |g_{sd}(i)|^2$ and $h_{sw}(i) = |g_{sw}(i)|^2$ respectively. We assume that both channels experience block fading, where the channel gains remain constant during each coherence interval and change independently from one coherence interval to the next. The fading process is assumed to be ergodic with a bounded continuous distribution. Moreover, the fading coefficients of the destination and the eavesdropper in any coherence interval are assumed to be independent of each other. We further assume that the number of channel uses n_1 within each coherence interval is large enough to allow for invoking random coding arguments.

The source wishes to send a message $W_1 \in \mathcal{W}_1 = \{1, 2, \cdots, M\}$ to the destination. The equivocation rate R_e at the eavesdropper is defined as the entropy rate of the transmitted message conditioned on the available CSI and the channel outputs at the eavesdropper, i.e.,

$$R_e \triangleq \frac{1}{n} H(W_1 | Y_2^n, h_{sd}^n, h_{sw}^n) \ , \tag{1}$$

where $h_{sd}^n = \{h_{sd}(1), \cdots, h_{sd}(n)\}$ and $h_{sw}^n = \{h_{sw}(1), \cdots, h_{sw}(n)\}$. It indicates the level of ignorance of the transmitted message W_1 at the eavesdropper. If the equivocation rate R_e is equal to the message rate, we get perfect secrecy. The secrecy capacity C_s is defined as the maximum achievable perfect secrecy rate.

Throughout the sequel, we assume that the CSI is known at the destination perfectly. Based on the available CSI, the transmitter adapts its transmission power **and rate** to maximize the perfect secrecy rate subject to a long-term average power constraint $\bar{P}$.

We first consider the case where at the beginning of each coherence interval, the transmitter knows the channel states of the legitimate receiver and the eavesdropper perfectly. When h_{sd} and h_{sw} are both known at the transmitter, one would expect the optimal scheme to allow for transmission only when $h_{sd} > h_{sw}$, and to adapt the transmitted power according to the instantaneous values of h_{sd} and h_{sw}. The following result formalizes this intuitive argument.

Theorem 1: When the channel gains of both the legitimate receiver and the eavesdropper are known at the transmitter, the secrecy capacity is given by

$$\begin{aligned} C_s^{(F)} &= \max_{P(h_{sd},h_{sw})} \int_0^\infty \int_{h_{sw}}^\infty \log\left(\frac{1+h_{sd}P(h_{sd},h_{sw})}{1+h_{sw}P(h_{sd},h_{sw})}\right) \\ &\qquad f(h_{sd})f(h_{sw})\mathrm{d}h_{sd}\mathrm{d}h_{sw}, \\ &\text{such that} \qquad \mathbb{E}\{P(h_{sd},h_{sw})\} \le \bar{P}. \end{aligned} \tag{2}$$

The optimal power allocation policy that achieves this secrecy capacity is given by

$$\begin{aligned} P(h_{sd},h_{sw}) = \frac{1}{2}\Bigg[\sqrt{\left(\frac{1}{h_{sw}}-\frac{1}{h_{sd}}\right)^2 + \frac{4}{\lambda}\left(\frac{1}{h_{sw}}-\frac{1}{h_{sd}}\right)} \\ - \left(\frac{1}{h_{sd}}+\frac{1}{h_{sw}}\right)\Bigg]^+, \end{aligned} \tag{3}$$

where $[x]^+ = \max\{0, x\}$, and the parameter λ is a constant that satisfies the power constraint in (2) with equality. We note that this power allocation is different from the celebrated water-filling solution.

Next, we consider the case where at the beginning of each coherence interval, the transmitter only knows the CSI of the main channel (legitimate receiver). The secrecy capacity under this scenario is characterized in the following theorem.

Theorem 2: When only the channel gain of the legitimate receiver is known at the transmitter, the secrecy capacity is given by

$$\begin{aligned} C_s^{(M)} &= \max_{P(h_{sd})} \iint \left[\log\left(\frac{1+h_{sd}P(h_{sd})}{1+h_{sw}P(h_{sd})}\right)\right]^+ \\ &\qquad f(h_{sd})f(h_{sw})\mathrm{d}h_{sd}\mathrm{d}h_{sw} \ , \\ &\text{such that} \qquad \mathbb{E}\{P(h_{sd})\} \le \bar{P}. \end{aligned} \tag{4}$$

The optimal power allocation policy that achieves this secrecy capacity is given as follows. For any main channel fading state h_{sd}, the optimal transmit power level $P(h_{sd})$ is determined from the equation

$$\frac{h_{sd}\Pr\left(h_{sw} \le h_{sd}\right)}{1+h_{sd}P(h_{sd})} - \int_0^{h_{sd}} \left(\frac{h_{sw}}{1+h_{sw}P(h_{sd})}\right) f(h_{sw})\mathrm{d}h_{sw} = \lambda,$$

where λ is a constant that satisfies the power constraint in (4) with equality. If the obtained power level turns out to be negative, then the optimal value of $P(h_{sd})$ is equal to 0. The solution to this optimization problem depends on the distributions $f(h_{sd})$ and $f(h_{sw})$.

We observe that, unlike the traditional ergodic fading scenario, achieving the optimal performance under a security constraint relies heavily on using a variable rate transmission strategy. This can be seen by evaluating the performance of a constant rate strategy where a single codeword is interleaved across infinitely many fading realizations. This interleaving will result in the eavesdropper **gaining more information**, than the destination, when its channel is better than the main channel, thereby yielding a perfect secrecy rate that is strictly smaller than that in (4). It is easy to see that the achievable perfect secrecy rate of the constant rate scheme, assuming a Gaussian codebook, is given by

$$\max_{P(h_{sd})} \iint \log\left(\frac{1+h_{sd}P(h_{sd})}{1+h_{sw}P(h_{sd})}\right) f(h_{sd})f(h_{sw})\mathrm{d}h_{sd}\mathrm{d}h_{sw} \ ,$$

$$\text{such that} \qquad \mathbb{E}\{P(h_{sd})\} \leq \bar{P}.$$

We now propose a transmission policy wherein the transmitter sends information only when the channel gain of the legitimate receiver h_{sd} exceeds a pre-determined constant threshold $\tau > 0$. Moreover, when $h_{sd} > \tau$, the transmitter always uses the same power level P. However, it is crucial to adapt the rate of transmission instantaneously as $\log(1+Ph_{sd})$ with h_{sd}. It is clear that for an average power constraint $\bar{P}$, the constant power level used for transmission will be

$$P \ = \ \frac{\bar{P}}{\Pr(h_{sd} > \tau)} \ .$$

Using a similar argument as in the achievable part of Theorem 2, we get the perfect secrecy rate achieved by the proposed scheme, using Gaussian inputs, as

$$R_s^{(CP)} = \int_0^\infty \int_\tau^\infty \left[\log\left(\frac{1+h_{sd}P}{1+h_{sw}P}\right)\right]^+ f(h_{sd})f(h_{sw})\mathrm{d}h_{sd}\mathrm{d}h_{sw}.$$

One can then optimize over the threshold τ to get the maximum achievable perfect secrecy rate.

Finally, as shown in [6], it is easy to establish the asymptotic optimality of this on/off scheme as the available average transmission power $\bar{P} \to \infty$. Moreover, the proposed on/off scheme also achieves the secrecy capacity $C_s^{(\bar{P})}$ under the full CSI assumption as $\bar{P} \to \infty$. Thus the absence of eavesdropper CSI at the transmitter does not reduce the secrecy capacity at high SNR values.

Now, we provide some numerical results to illustrate the opportunistic gains offered by channel fading, in facilitating secure communications. As an additional benchmark, we first obtain the performance when the transmitter does not have any knowledge of both the main and eavesdropper channels (only receiver CSI). In this scenario, the transmitter is unable to exploit rate/power adaptation and always transmits with power $\bar{P}$. It is straightforward to see that the achievable perfect secrecy rate in this scenario (using Gaussian inputs) is given by

$$R_s^{(R)} \ = \ \left[\iint \log\left(\frac{1+h_{sd}\bar{P}}{1+h_{sw}\bar{P}}\right) f(h_{sd})f(h_{sw})\mathrm{d}h_{sd}\mathrm{d}h_{sw}\right]^+$$

Thus when $\mathbb{E}\{h_{sw}\} \geq \mathbb{E}\{h_{sd}\}$, $R_s^{(R)} = 0$. The results for an asymmetric Rayleigh fading scenario, wherein the eavesdropper channel is more capable than the main channel, is provided in Fig. 2 (with $\mathbb{E}\{h_{sd}\} = 1$ and $\mathbb{E}\{h_{sw}\} = 2$). It is clear that the performance of the on/off power control scheme is very close to the secrecy capacity (with only main channel CSI) for a wide range of SNRs and, as expected, approaches the secrecy capacities, under both the full CSI and main channel CSI assumptions, at high values of SNR. The performance of the constant rate scheme is much worse than the other schemes that employ rate adaptation. Here we note that the performance curve for the constant rate scheme might be a lower bound to the secrecy capacity (since the KKT conditions are necessary but not sufficient for non-convex optimization).

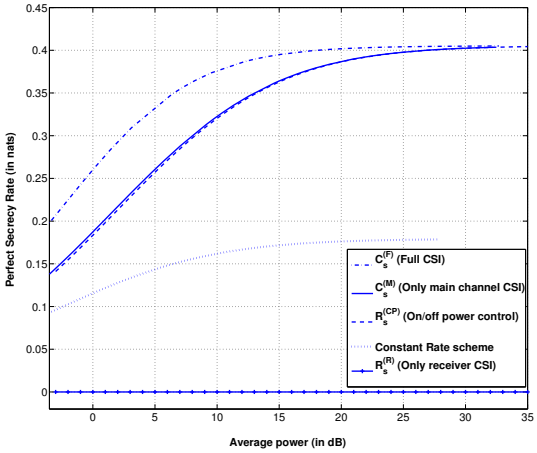

Fig. 2. Performance comparison for the asymmetric Rayleigh fading scenario with $\mathbb{E}\{h_{sd}\} = 1$ and $\mathbb{E}\{h_{sw}\} = 2$.

III. Cooperative Secrecy

In this section, we investigate the role of user-cooperation in secure communications. More specifically, we consider a four-terminal discrete 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 3. 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 destination, relay and eavesdropper respectively. We consider the memoryless channel. As in Section II, the source wishes to send the message $W_1 \in \mathcal{W}_1 = \{1, \cdots, M\}$ to the destination using a sequence of (M, n) codes consisting of: 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 encoder that maps the signals $(y_{1,1}, y_{1,2}, \cdots, y_{1,i-1})$ received before time i to the channel input $x_{2,i}$, 3) a decoding function ϕ: $\mathcal{Y}^n \to \mathcal{W}_1$. The average error probability of a (M, n) code is defined as

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

The equivocation rate at the eavesdropper is defined as $R_e = \frac{1}{n}H(W_1|\mathbf{Y}_2)$. The rate-equivocation pair (R_1, R_e), the trade-off among transmission rate and level of secrecy, 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

$$R_1 = \frac{1}{n}\log_2 M, \ P_e^n \leq \epsilon, \ \frac{1}{n}H(W_1|\mathbf{Y}_2) \geq R_e - \epsilon.$$

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

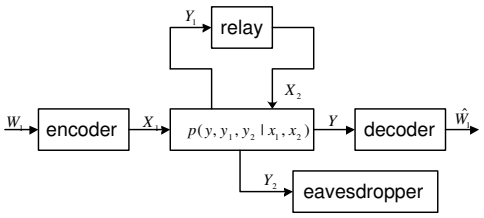

Fig. 3. The relay eavesdropper channel.

We first characterize the achievable rate-equivocation region of the Cover-El Gamal Decode and Forward (DF) Strategy [8]. In DF cooperation strategy, the relay node will first decode codewords and then re-encode the message to cooperate with the source. Here, we use the regular coding and backward decoding scheme developed in the classical relay setting [9], with the important difference that each message will be associated with many codewords in order to confuse the eavesdropper.

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

$$\begin{aligned} R_1 &< \min\{I(V_1, V_2; Y), I(V_1; Y_1|V_2)\}, \\ R_e &< R_1, \\ R_e &< [\min\{I(V_1, V_2; Y), I(V_1; Y_1|V_2)\} - I(V_1, V_2; Y_2)]^+, \end{aligned} \tag{5}$$

for some distribution $p(v_1, v_2, x_1, x_2, y_1, y_2, y) = p(v_1, v_2)p(x_1, x_2|v_1, v_2)p(y_1, y_2, y|x_1, x_2)$, are achievable using the DF strategy. Hence, for the DF scheme, the following perfect secrecy rate is achievable

$$R_s^{(DF)} = \sup_{p(v_1,v_2)} \big[\min\{I(V_1, V_2; Y), I(V_1; Y_1|V_2)\} - I(V_1, V_2; Y_2)\big]^+.$$

The channel between the source and the relay becomes a bottleneck for the DF strategy when it is noisier than the source-destination channel. This motivates our Noise-Forwarding (NF) scheme, where the relay node does not attempt to decode the message but sends codewords that are *independent* of the source's message. The enabling observation behind this scheme is that, in the wiretap channel, in addition to its own information, the source should send extra codewords to confuse the wiretapper. In our setting, this task can be accomplished by the relay by allowing it to send independent codewords, which aid in confusing the eavesdropper.

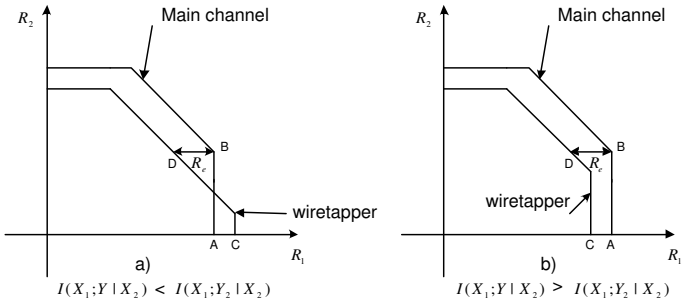

Fig. 4. The rate region of the compound MACs of the relay eavesdropper channel for a fixed input distribution $p(x_1)p(x_2)$.

Our NF scheme transforms the relay-eavesdropper channel into a compound multiple access channel (MAC), where the source/relay to the receiver is the first MAC and source/relay to the eavesdropper is the second one. Figure 4 shows the rate region of these two MACs for a fixed input distribution $p(x_1)p(x_2)$. In the figure, R_1 is the codeword rate of the source, and R_2 is the codeword rate of the relay. We can observe from Figure 2a) that if the relay node does not transmit, the perfect secrecy rate is zero for this input distribution since $R_1(A) < R_1(C)$. On the other hand, if the relay and the source coordinate their transmissions and operate at point B, we can achieve the equivocation rate R_e, which is strictly larger than zero. On the other hand, in Figure 2b), we can still get a positive perfect secrecy rate by operating at point A in the absence of the relay. But by moving the operating point to B, we can get a larger secrecy rate. This illustrates the main idea of our NF scheme.

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

$$\begin{aligned} R_1 &< I(V_1; Y|V_2), \\ R_e &< R_1, \\ R_e &< [I(V_1; Y|V_2) + \min\{I(V_2; Y), I(V_2; Y_2|V_1)\} \\ &\quad - \min\{I(V_2; Y), I(V_2; Y_2)\} - I(V_1; Y_2|V_2)]^+, \end{aligned} \tag{6}$$

for some distribution $p(v_1, v_2, x_1, x_2, y_1, y_2, y) = p(v_1)p(v_2)$ $p(x_1|v_1)p(x_2|v_2)p(y_1, y_2, y|x_1, x_2)$, are achievable using the NF scheme. Hence, for the NF scheme, the achievable perfect secrecy rate is

$$R_s^{(NF)} = \sup_{p(v_1)p(v_2)} [I(V_1; Y|V_2) + \min\{I(V_2; Y), I(V_2; Y_2|V_1)\} - \min\{I(V_2; Y), I(V_2; Y_2)\} - I(V_1; Y_2|V_2)]^+.$$

In the NF scheme, the relay node does not need to listen to the source, and hence, this scheme is also suited for relay nodes limited by the half-duplex constraint. In NF cooperation, each user sends independent messages to the destination, which resembles the MAC. Hence, NF cooperation can be adapted to the multiple access eavesdropper channel where the multiple users in the MAC channel can help each other in communicating securely with the destination without listening to each other.

In the following, we use the Gaussian relay-eavesdropper channel to illustrate the notion of cooperative secrecy. In this case, the signal received at each node is

$$y_j[n] = \sum_{i \neq j} g_{ij} x_i[n] + z_j[n], \tag{7}$$

here g_{ij} is the channel coefficient between node $i \in \{s, r\}$ and node $j \in \{r, w, d\}$, 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.

The secrecy capacity of the Gaussian eavesdropper channel with the absence of the relay node is given [10] by $\frac{1}{2}\big[\log_2(1 + |g_{sd}|^2 P_1) - \log_2(1 + |g_{sw}|^2 P_1)\big]^+$. Hence if $|g_{sw}|^2 \geq |g_{sd}|^2$ and the relay does not transmit, the secrecy capacity is zero, no matter how large P_1 is. On the other hand, as shown later, the relay can facilitate the source-destination pair to achieve a positive perfect secrecy rate under some conditions even when $|g_{sw}|^2 \geq |g_{sd}|^2$. In the following, we focus on such scenarios.

At this point, we do not know the optimal input distribution that maximizes $R_s^{(DF)}$, $R_s^{(NF)}$. Here, we let $V_1 = X_1, V_2 =$

X_2 and use a Gaussian input distribution to obtain an achievable lower bound.

For DF cooperation scheme, we let $X_2 \sim \mathcal{N}(0, P_2)$, $X_{10} \sim \mathcal{N}(0, P)$, where $\mathcal{N}(0, P)$ is the Gaussian distribution with zero mean and variance P. Also, we let $X_1 = c_1 X_2 + X_{10}$, where c_1 is a constant to be specified later. To satisfy the average power constraint at the source, we require $|c_1|^2 P_2 + P \leq P_1$.

Straightforward calculations show that

$$R_s^{(DF)} = \max_{c_1, P} \left[\min \left\{ \frac{1}{2} \log_2 \left(\frac{1 + |g_{sr}|^2 P}{1 + |g_{sw} c_1 + g_{rw}|^2 P_2 + |g_{sw}|^2 P} \right), \right. \right.$$
$$\left. \left. \frac{1}{2} \log_2 \left(\frac{1 + |g_{sd} c_1 + g_{rd}|^2 P_2 + |g_{sd}|^2 P}{1 + |g_{sw} c_1 + g_{rw}|^2 P_2 + |g_{sw}|^2 P} \right) \right\} \right]^+ . \quad (8)$$

For NF, we let $X_1 \sim \mathcal{N}(0, P_1)$, $X_2 \sim \mathcal{N}(0, P_2)$. Here X_1, X_2 are independent, resulting in

$$R_s^{(NF)} = \left[\min \left\{ \frac{1}{2} \log_2 \left(1 + |g_{sd}|^2 P_1 \right), \right. \right.$$
$$\frac{1}{2} \log_2 \left(\frac{1 + |g_{sd}|^2 P_1 + |g_{rd}|^2 P_2}{1 + |g_{sw}|^2 P_1 + |g_{rw}|^2 P_2} \right),$$
$$\left. \left. \frac{1}{2} \log_2 \left(\frac{(1 + |g_{rw}|^2 P_2)(1 + |g_{sd}|^2 P_1)}{1 + |g_{sw}|^2 P_1 + |g_{rw}|^2 P_2} \right) \right\} \right]^+ .$$

Figure 6 shows the achievable perfect secrecy rates 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 $g_{ij} = d_{ij}^{-\gamma} e^{j\theta_{ij}}$, 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[1]. The random phase will not affect the achievable perfect secrecy rate of NF since it does not depend on beam-forming between the source and relay. But, the rates of DF is different here. In this case, the source can adjust its phase according to the knowledge of the phase information about $\theta_{sr}, \theta_{sd}, \theta_{rd}$. In this way, the signals of the source and the relay will add up coherently at the destination, but not at the eavesdropper since θ_{sw}, θ_{rw} are independent of $\theta_{sd}, \theta_{rd}, \theta_{sr}$. The secrecy rate of DF could then be obtained by averaging (8) over the random phases. From the figure, we observe that when $x > 1$, DF cooperation does not offer any benefit. But NF and AF still enjoy non-zero perfect secrecy rates.

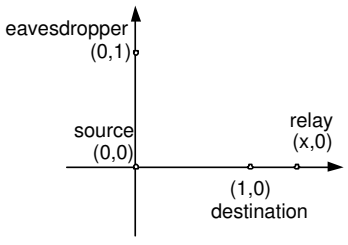

Fig. 5. The network topology.

[1]In the figure, the Amplify and Forward (AF) scheme corresponds to the case where the relay only sends a scaled version of its last received symbol, please refer to [7] for details.

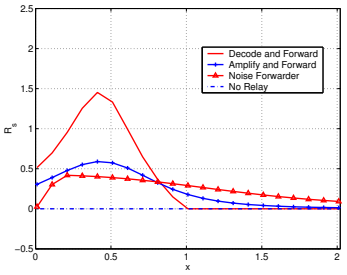

Fig. 6. The achievable perfect secrecy rate for various schemes in the Gaussian relay eavesdropper channel with phase fading.

IV. Conclusions

We have identified two novel methods to facilitate secure communication by leveraging the opportunities offered by wireless channels. In the opportunistic secrecy case, we have characterized the secrecy capacity of the slow fading channel with an eavesdropper under different assumptions on the available transmitter CSI. Our work establishes the interesting result that a non-zero perfectly secure rate is achievable in the fading channel even when the eavesdropper is more capable than the legitimate receiver (on the average). By contrasting this conclusion with the traditional AWGN scenario, one can see the positive impact of fading on **enhancing** the secrecy capacity. Our theoretical and numerical results established the critical role of main channel CSI and appropriate rate adaptation in facilitating secure communications over slow fading channels. In the cooperative secrecy case, we have devised several cooperation schemes that can provide non-zero perfect secrecy rate even when the secrecy capacity is zero in the absence of the relay node. Of particular interest is the novel and simple NF scheme, which is shown to be able to provide positive gains even in the cases where the relay node cannot provide any gain in the classical relay channel. The cooperative gains were proved theoretically and validated numerically in the AWGN channel.

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] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proc. IEEE Internat. Symposium on Information Theory*, pp. 2152–2155, Sep. 2005.

[5] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Internat. Symposium on Information Theory*, July 2006.

[6] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Information Theory*, Oct. 2006. Submitted.

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

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

[9] C.-M. Zing, F. Kuhlmann, and A. Buzo, "Achivability proof of some multiuser channel coding theorems using backward decoding," *IEEE Trans. on Information Theory*, vol. 35, no. 6, pp. 1160–1165, 1989.

[10] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Trans. on Information Theory*, vol. 24, pp. 451–456, Jul. 1978.