Analyzing Amplify-and-Forward and Decode-and-Forward Cooperative Strategies in Wyner's Channel Model

Pengyu Zhang[1], Jian Yuan[1], Jianshu Chen[1], Jian Wang[1], Jin Yang[2]
[1]Tsinghua National Laboratory for Information Science and Technology
Department of Electrical Engineering, Tsinghua University, Beijing, China
[2]China Broadband Wireless Research Center, Motorola Lab, Beijing, China
Email: zhangpengyu@tsinghua.org.cn Fax/Phone: 86-10-62781447

***Abstract*—The benefits of Amplify-and-Forward (AF) and Decode-and-Forward (DF) cooperative relay for secure communication are investigated within Wyner's wiretap channel. We characterize the secrecy rate when source, destination, relay and eavesdropper all use single antenna and the channel conditions are fix. Both AF and DF cooperative strategies are proved theoretically to be able to facilitate secure communication. Detailed analysis of AF and DF scheme reveals a trade off between secrecy area and request secrecy rate. In addition, secrecy constraints in cooperative secure communication are discussed and are used to explain the differences in AF and DF scheme. Overall, our work establishes the utility of cooperation and compares each advantage of AF and DF scheme in facilitating secure communication over wireless channel.**

I. Introduction

The broadcast nature of wireless communication calls for careful security considerations. Information theoretic security of wireless channels has received a great deal of attention recently. In [1], Wyner introduced wiretap channel model to evaluate secure information transmission at the physical layer. In the basic wiretap channel, Wyner established the secrecy capacity for the case where the eavesdropping channel is a degraded one of the user's channel, shown in Fig. 1. In [2], Csiszar generalized this result to the nondegraded discrete memoryless broadcast channel and Leung-Yan-Cheong applied it to the basic Gaussian channel in [3].

In [2], Csiszar shows that the capacity-equivocation region of the nondegraded channel is as Wyner's when the user's channel is more capable compared to the eavesdropper's channel. However, the conditions in [1] [2], such as degradedness, less noisy or more capable, are not always true in real system. In this situation, the secrecy capacity of the channel is zero, implying the infeasibility of secure communication. Many techniques, such as multiple antennas used in [4] [5] [6], have been developed to solve this problem.

Motivated by emerging wireless communication application, there is another growing interests in exploiting the benefits of relay to solve the problem mentioned above. In [7], a transmitter sends a confidential message to its intended receiver with the help of an independent interferer in the presence of a passive eavesdropper. An achievable secrecy rate for this channel is given. This result shows that a relay with interference can be exploited to assist secrecy in wireless communications. In [8], Lai considers user cooperation to enable secure communication. The rate-equivocation region of the compound MAC of the relay wiretap channel is characterized.

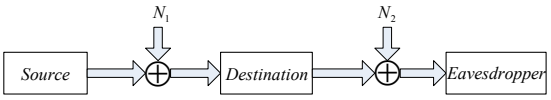

Fig. 1. Degraded wiretap channel

In [9], Laneman analyzed the limitations of the cooperative strategies in [8]. Different from [8], half-duplex cooperative relay proposed by Laneman is introduced to facilitate secure communication. Theoretical analysis proves that both two cooperative strategies, Amplify-and-Forward and Decode-and-Forward, can facilitate secure communication. The existence of relay provides additional channels to transmit secret information and nonzero secrecy rate is achieved. Detailed calculation reveals a secrecy area-rate trade off in AF and DF scheme. Cooperative AF relay can be deployed in larger area with lower secrecy rate. In contrary, the deployment area of cooperative DF relay is smaller but the secrecy rate is higher. The differences of AF and DF scheme are explained by the secrecy constraints on cooperative secure communication. Secrecy constraints we obtained indicate that channel condition between source and relay is of significant importance in cooperative secure communication.

The organization of the paper is as follows. Section II describes the channel and system model of interest. Section III states all the main results of the paper. Calculation results and analysis of cooperative secure communication scheme is provided in section IV. Section V contains some concluding remarks.

II. Channel and system model

Because of the limitations of the cooperative strategies in [8], half-duplex cooperative strategies are introduced to facilitate secure communication. To ensure half-duplex operation and without loss of generality, we characterize our channel

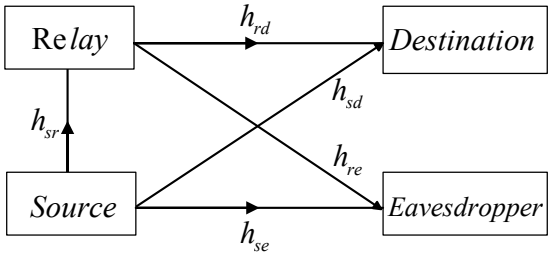

Fig. 2. Channel and system model

model using a time-division notation. The channel and system model is shown in Fig. 2. All terminals use single antenna to transmit and receive.

In the first half of transmission, source transmits its information while both relay and destination receive information in the presence of an eavesdropper. We model the channel during the first half of block as

$$y_{\rm r}[n] = h_{\rm sr}x_{\rm s}[n] + z_{\rm r}[n] \quad (1)$$

$$y_{\rm d}[n] = h_{\rm sd}x_{\rm s}[n] + z_{\rm d}[n] \quad (2)$$

$$y_{\rm e}[n] = h_{\rm se}x_{\rm s}[n] + z_{\rm e}[n] \quad (3)$$

for $n = 1, 2, \ldots, N/2$, where $x_{\rm s}$ is the source transmitted signal and $y_{\rm r}$, $y_{\rm d}$ and $y_{\rm e}$ are the relay, destination and eavesdropper received signals, respectively.

In the second half of transmission, the relay transmits information it received in the first half of block while destination receives information in the presence of an eavesdropper. For the second half of block, we model the received signal as

$$y_{\rm d}[n] = h_{\rm rd}x_{\rm r}[n] + z_{\rm d}[n] \quad (4)$$

$$y_{\rm e}[n] = h_{\rm re}x_{\rm r}[n] + z_{\rm e}[n] \quad (5)$$

for $n = N/2 + 1, N/2 + 2, \ldots, N$, where $x_{\rm r}$ is the relay transmitted signal and $y_{\rm d}$ and $y_{\rm e}$ are the destination and eavesdropper received signals.

In (1)-(5), $h_{\rm ij}$ captures the effects of path-loss, and $z_{\rm j}$ captures the effects of receiver noise and other forms of interferences in the system, where $i \in \{s, r\}$ and $j \in \{r, d, e\}$. We consider the scenario in which $h_{\rm ij}$ is accurately measured by the appropriate receivers. Statistically, we model $z_{\rm j}[n]$ as zero-mean mutually independent, circularly symmetric, complex Gaussian random sequences with unit variance.

III. Cooperative secure communication

A. Secrecy capacity

Communication takes place at a rate R in bits per channel use over a transmission interval of length n. Specifically, a $(2^{\rm nR}, n)$ code for the channel consists of a message w uniformly distributed over the index set $w_{\rm n} = 1, 2, \ldots, 2^{\rm nR}$. An encoder $u_{\rm n}$ maps the message w to the transmitted sequence $\{x(t)\}^n$, and a decoding function $v_{\rm n}$ maps the received sequence $\{y(t)\}^n$ to a message estimate $\hat{w}$. The error event is $\varepsilon_{\rm n} = \{v_{\rm n}(u_{\rm n}(w)) \neq w\}$, and the amount of information obtained by the eavesdropper from the transmission is measured via the equivocation $I(w; y_{\rm e}^n)$.

According to [6], a secrecy rate $R_{\rm e}$ is achievable if there exists a sequence of $(2^{nR_{\rm e}}, n)$ codes such that $Pr(\varepsilon_{\rm n}) \to 0$ and $I(w; y_{\rm e}^n)/n \to 0$ as $n \to \infty$. The secrecy capacity is the supremum of all achievable secrecy rates.

According to [2], the secrecy capacity of the nondegraded discrete memoryless broadcast channel is expressed in the form

$$C_{\rm S} = \max_{w \to x \to y_{\rm d} y_{\rm e}} \{I(w; y_{\rm d}) - I(w; y_{\rm e})\} \quad (6)$$

Ideally, one should solve (6) for the optimal joint distribution of w and x. Following [5], we restrict ourselves to the potentially sub-optimal assumption that $x = w$, under which, the following secrecy rate is achievable

$$R_{\rm S} = \max_{p(x)} \{I(x; y_{\rm d}) - I(x; y_{\rm e})\} \quad (7)$$

In [2], Csiszar pointed out that $R_{\rm S}$ would have been equivalent to the secrecy capacity $C_{\rm S}$, if the main channel was "more capable" than the eavesdropping channel. $p(x)$ must be chosen to maximize (7), but following [5], we restrict ourselves to the class of Gaussian pdfs. Our aim is to characterize the benefits of secrecy rate brought by cooperative relay under this restriction and the input power constraint. We limit our discussion to the scenario that all terminals use unit power and single antenna to transmit. The problem of power allocation in cooperative secure communication is another research topic.

B. Cooperative relays facilitate secure communication

In this section, we analyze the secrecy gain brought by cooperative relay. The basic idea of cooperative secure communication is that after amplifying the signals or decoding the codewords, the relay and source can "beam-form" towards the destination to enable a larger rate gain in the main channel than the wiretap channel.

1) Cooperative AF scheme: In AF scheme, the relay first amplifies signals from the source and then cooperates with source to transmit secret information to the destination. According to [9], mutual information of AF scheme between source and destination and eavesdropper are

$$I_{\rm SD_{AF}} = \log(1 + P_{\rm S}|h_{\rm sd}|^2 + \frac{P_{\rm S}|h_{\rm sr}|^2 P_{\rm R}|h_{\rm rd}|^2}{1 + P_{\rm S}|h_{\rm sr}|^2 + P_{\rm R}|h_{\rm rd}|^2}) \quad (8)$$

$$I_{\rm SE_{AF}} = \log(1 + P_{\rm S}|h_{\rm se}|^2 + \frac{P_{\rm S}|h_{\rm sr}|^2 P_{\rm R}|h_{\rm re}|^2}{(1 + P_{\rm S}|h_{\rm sr}|^2 + P_{\rm R}|h_{\rm re}|^2)}) \quad (9)$$

Secrecy rate $R_{\rm S}$ of cooperative AF strategy is

$$\begin{aligned} R_{\rm S_{AF}} &= I_{\rm SD_{AF}} - I_{\rm SE_{AF}} \quad (10) \\ &= \log(\frac{1 + |h_{\rm sd}|^2 + \frac{|h_{\rm sr}|^2|h_{\rm rd}|^2}{1+|h_{\rm sr}|^2+|h_{\rm rd}|^2}}{1 + |h_{\rm se}|^2 + \frac{|h_{\rm sr}|^2|h_{\rm re}|^2}{1+|h_{\rm sr}|^2+|h_{\rm re})|^2}}) \end{aligned}$$

To investigate the benefits brought by cooperative AF relay, we consider the scenario that eavesdropper's channel is better than user's channel ($h_{\rm sd} < h_{\rm se}$). Through direct transmission without relay, the secrecy rate is zero when $h_{\rm sd} < h_{\rm se}$. However, cooperative AF relays that satisfy the following channel condition can achieve nonzero secrecy rate.

$$\frac{|h_{\rm sr}|^2(|h_{\rm sr}|^2+1)(|h_{\rm rd}|^2-|h_{\rm re}|^2)}{(|h_{\rm sr}|^2+|h_{\rm rd}|^2+1)(|h_{\rm sr}|^2+|h_{\rm re}|^2+1)} > |h_{\rm se}|^2-|h_{\rm sr}|^2 \quad (11)$$

$h_{\rm sr}$ provides additional channel to transmit secret information and $h_{\rm rd}$ compensates the secret information loss at the source. With large $h_{\rm sr}$ and enough secret information compensation ($|h_{\rm rd}|^2-|h_{\rm re}|^2 \gg |h_{\rm se}|^2-|h_{\rm sd}|^2$), we can achieve nonzero secrecy rate in AF scheme.

2) Cooperative DF scheme: In DF scheme, relay first decodes the codewords transmitted by source, then cooperates with source to transmit secret message to the destination. Similar with AF relay, DF relay can also promote secrecy rate. According to [9], mutual information of DF scheme between source and destination and eavesdropper are

$$I_{\rm SD_{DF}} = \min\{\log(1+P_{\rm S}|h_{\rm sr}|^2), \log(1+P_{\rm S}|h_{\rm sd}|^2+P_{\rm R}|h_{\rm rd}|^2)\} \quad (12)$$

$$I_{\rm SE_{DF}} = \min\{\log(1+P_{\rm S}|h_{\rm sr}|^2), log(1+P_{\rm S}|h_{\rm se}|^2+P_{\rm R}|h_{\rm re}|^2)\} \quad (13)$$

Secrecy rate $R_{\rm S}$ of cooperative DF strategy is

$$\begin{aligned} R_{\rm S_{DF}} &= I_{\rm SD_{DF}} - I_{\rm SE_{DF}} \quad (14)\\ &= \min\{\log(1+|h_{\rm sr}|^2), \log(1+|h_{\rm sd}|^2+|h_{\rm rd}|^2)\}\\ &\quad -\min\{\log(1+|h_{\rm sr}|^2), \log(1+|h_{\rm se}|^2+|h_{\rm re}|^2)\} \end{aligned}$$

Also, we investigate the benefits brought by cooperative DF relay when $h_{\rm sd} < h_{\rm se}$. Cooperative DF relays that satisfy the following channel condition can achieve nonzero secrecy rate.

$$\begin{cases} |h_{\rm sr}|^2 > |h_{\rm se}|^2+|h_{\rm re}|^2 \\ |h_{\rm rd}|^2-|h_{\rm re}|^2 > |h_{\rm se}|^2-|h_{\rm sd}|^2 \end{cases}$$

$h_{\rm sr}$ and $h_{\rm rd}$ associated with DF relay has the same function as in AF scheme.

C. Secrecy constraints on secure communication

In this section, we investigate the secrecy constraints on cooperative relay in secure communication.

1) Secrecy constraint on DF:

Theorem 1: Cooperative DF relay can not achieve nonzero secrecy rate under the channel condition:

$$|h_{\rm sr}|^2 \le |h_{\rm se}|^2+|h_{\rm re}|^2$$

Proof: To achieve nonzero secrecy rate

$$\begin{aligned} R_{\rm S_{DF}} > 0 \quad &\Rightarrow \quad I_{\rm SD_{DF}} - I_{\rm SE_{DF}} > 0 \quad (15)\\ &\Rightarrow \quad \min\{\log(1+|h_{\rm sr}|^2), \log(1+|h_{\rm sd}|^2+|h_{\rm rd}|^2)\}\\ &\quad -\min\{\log(1+|h_{\rm sr}|^2), \log(1+|h_{\rm se}|^2+|h_{\rm re}|^2)\} > 0 \end{aligned}$$

We discuss the following four possible channel combinations to analyze the inequation above:

$$\begin{cases} |h_{\rm sr}|^2 > |h_{\rm sd}|^2+|h_{\rm rd}|^2, |h_{\rm sr}|^2 > |h_{\rm se}|^2+|h_{\rm re}|^2 \\ |h_{\rm sr}|^2 < |h_{\rm sd}|^2+|h_{\rm rd}|^2, |h_{\rm sr}|^2 > |h_{\rm se}|^2+|h_{\rm re}|^2 \\ |h_{\rm sr}|^2 > |h_{\rm sd}|^2+|h_{\rm rd}|^2, |h_{\rm sr}|^2 < |h_{\rm se}|^2+|h_{\rm re}|^2 \\ |h_{\rm sr}|^2 < |h_{\rm sd}|^2+|h_{\rm rd}|^2, |h_{\rm sr}|^2 < |h_{\rm se}|^2+|h_{\rm re}|^2 \end{cases}$$

Under the four channel conditions, $R_{\rm S_{DF}} > 0$ can be simplified as

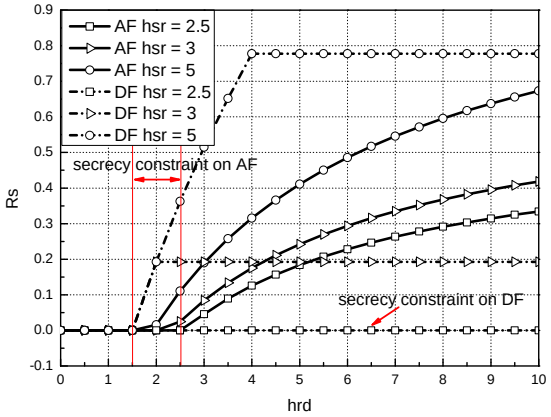

Fig. 3. Secrecy gain and secrecy constraints

$$\begin{cases} R_{\rm S_{DF}} = \log(1+|h_{\rm sd}|^2+|h_{\rm rd}|^2)-\log(1+|h_{\rm se}|^2+|h_{\rm re}|^2) > 0 \\ R_{\rm S_{DF}} = \log(1+|h_{\rm sr}|^2)-\log(1+|h_{\rm se}|^2+|h_{\rm re}|^2) > 0 \\ R_{\rm S_{DF}} = \log(1+|h_{\rm sd}|^2+|h_{\rm rd}|^2)-\log(1+|h_{\rm sr}|^2) > 0 \\ R_{\rm S_{DF}} = \log(1+1+|h_{\rm sr}|^2)-\log(1+|h_{\rm sr}|^2) > 0 \end{cases} \Rightarrow$$

$$\begin{cases} |h_{\rm sr}|^2 > |h_{\rm se}|^2+|h_{\rm re}|^2, |h_{\rm rd}|^2-|h_{\rm re}|^2 > |h_{\rm se}|^2-|h_{\rm sd}|^2 \\ |h_{\rm sr}|^2 > |h_{\rm se}|^2+|h_{\rm re}|^2, |h_{\rm rd}|^2-|h_{\rm re}|^2 > |h_{\rm se}|^2-|h_{\rm sd}|^2 \\ |h_{\rm sd}|^2+|h_{\rm rd}|^2 > |h_{\rm sr}|^2, |h_{\rm sd}|^2+|h_{\rm rd}|^2 < |h_{\rm sr}|^2 \\ 0 > 0 \end{cases}$$

Under the later two channel condition, $|h_{\rm sr}|^2 \le |h_{\rm se}|^2+|h_{\rm re}|^2$, cooperative DF relay can not achieve nonzero secrecy rate. Thus channel condition $h_{\rm sr}$ is of significant importance for DF scheme in cooperative secure communication.

2) Secrecy constraint on AF:

Theorem 2: Cooperative AF relay can achieve nonzero secrecy rate only under the following channel condition:

$$\frac{|h_{\rm sr}|^2(|h_{\rm sr}|^2+1)(|h_{\rm rd}|^2-|h_{\rm re}|^2)}{(|h_{\rm sr}|^2+|h_{\rm rd}|^2+1)(|h_{\rm sr}|^2+|h_{\rm re}|^2+1)} > |h_{\rm se}|^2-|h_{\rm sr}|^2$$

Proof can be obtained by calculating $C_{\rm S_{AF}} > 0$.

Secrecy constraint on AF indicates that AF relay can not achieve nonzero secrecy rate with low $h_{\rm sr}$ because of the fractional structure of $h_{\rm sr}$. Thus $h_{\rm sr}$ is also important for AF scheme.

IV. Numerical Results and Discussion

In this section's calculation, we exhibit the gain in secrecy rate brought by AF and DF cooperative relay and a secrecy area-rate trade off is exhibited. Also, our calculation analyzes the differences of the two schemes caused by secrecy constraints.

A. Theoretical analysis of secrecy gain and constraints

In Fig. 3, we evaluate the performance of cooperative relay under different channel conditions. In our analysis, for convenient comparison, we assume $h_{\rm sd}=1$, $h_{\rm re}=1$ and $h_{\rm se}=1.5$. This means eavesdropper's channel is better than user's channel and secrecy rate is zero under this channel

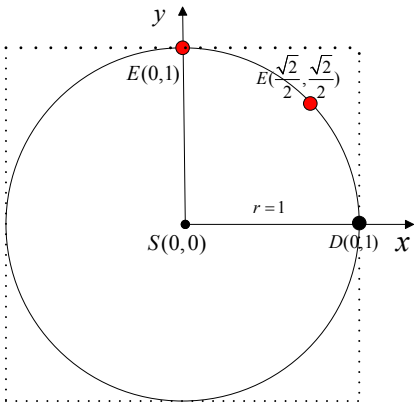

Fig. 4. Eavesdropping scenario

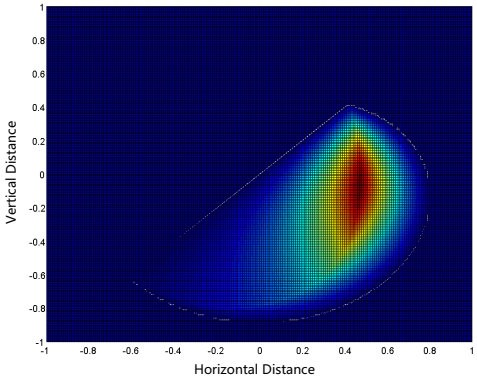

Fig. 6. DF relay deployment in $\{x \in [-1,1], y \in [-1,1]\}$ when $E(0,1)$

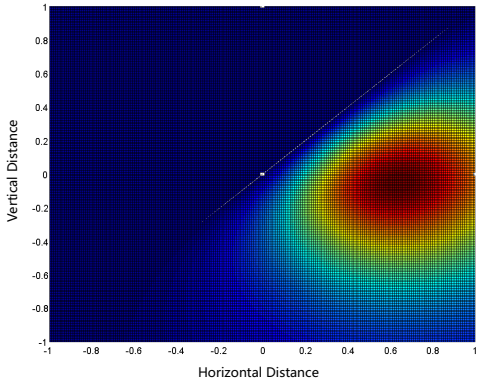

Fig. 5. AF relay deployment in $\{x \in [-1,1], y \in [-1,1]\}$ when $E(0,1)$

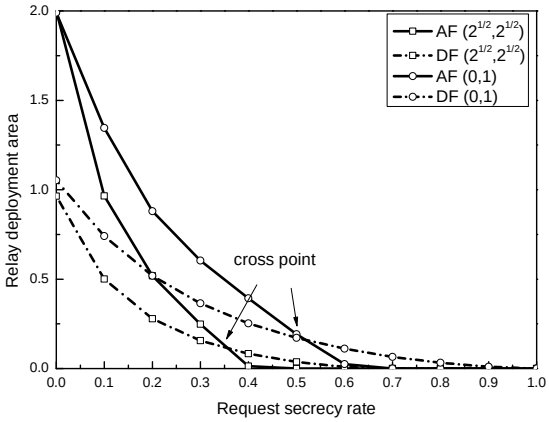

Fig. 7. Secrecy area-rate trade off in AF and DF

condition through direct transmission with single antenna. However, in Fig. 3, both cooperative AF and DF relay can help source achieve nonzero secrecy rate when $h_{\mathrm{rd}} > 3$ and $h_{\mathrm{sr}} = 3$ or $h_{\mathrm{sr}} = 5$. In Fig. 3, we can see h_{sr} is important for both AF and DF strategies. AF and DF relays with $h_{\mathrm{sr}} = 5$ achieve higher secrecy rate than relays with $h_{\mathrm{sr}} = 3$ in the same h_{rd}. Thus with larger h_{sr}, it is easier to achieve higher secrecy rate.

However, limited by secrecy constraints, cooperative relay is unable to facilitate secure communication under some channel conditions. In Fig. 3, because of the secrecy constraint on DF scheme, cooperative DF relay are unable to achieve nonzero secrecy rate if h_{sr} is not so good, e.g. $h_{\mathrm{sr}} = 2.5$ ($h_{\mathrm{sr}} <= h_{\mathrm{se}} + h_{\mathrm{re}}$). In the area between the vertical line, secrecy constraint on AF scheme prevents relay achieving nonzero secrecy rate. Thus, h_{sr} is important for cooperative secure communication.

B. Secrecy gain and constraints in large scale model

1) Secrecy area-rate trade off in AF and DF: In this section, we analyze the secrecy gain of AF and DF scheme under large scale model. We consider the scenario shown in Fig. 4. Large-scale model of signals is used and the distance between source and destination is assume to be unit ($r_{sd} = 1$). Without cooperative relay, eavesdropper must be excluded out of the circle to guarantee nonzero secrecy rate. So two special positions of eavesdropper, $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$ and (0,1), are selected to investigate the secrecy gain of cooperative AF and DF relay. In this section, we limit our discussion to the area of $\{x \in [-1,1], y \in [-1,1]\}$. Larger area will lead to same conclusion.

Fig. 5 and Fig. 6 show the deployment of AF and DF relays in the area $\{x \in [-1,1], y \in [-1,1]\}$ when eavesdropper is at $(0,1)$. Red area represents the position with high nonzero secrecy rate and deep blue area represents the position with zero secrecy rate. We can observe that the deployment area of AF relay is larger than DF relay.

Fig. 7 introduces the secrecy area-rate trade off in AF and DF. Horizontal axis represents request secrecy rate and vertical axis is the area that relay can be deployed to guarantee nonzero secrecy rate. When request secrecy rate is low, cooperative AF relay is able to be deployed in larger area than DF relay to achieve nonzero secrecy rate, such as the area on the left side of the cross point. This is due to the reason that the secrecy constraint on AF relay is not as strict as DF relay. Secrecy constraint on AF scheme allows relay working under more channel conditions. Channel combination of h_{sr}, h_{rd} and h_{re} makes AF relay work in larger scope of h_{sr}. However, secrecy

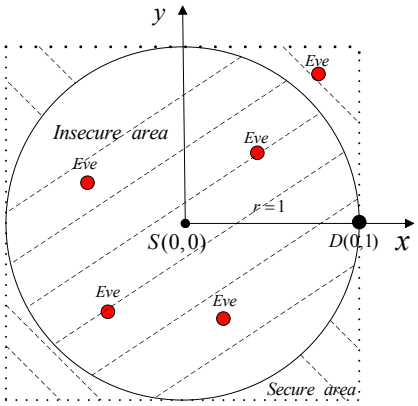

Fig. 8. Search secure area model

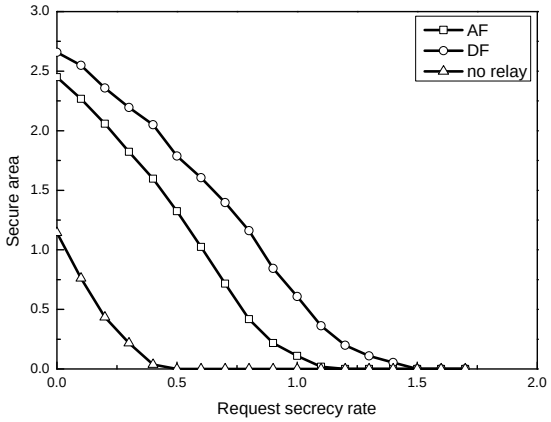

Fig. 9. Search secure area

constraint on DF scheme is stricter. DF relay can work only when $|h_{\rm sr}|^2 > |h_{\rm se}|^2 + |h_{\rm re}|^2$. Thus, the deployment area of DF relay is smaller, such as the line on the left side of the cross point.

In contrary, the maximal request secrecy rate that DF relay achieves is larger than AF relay, such as the area on the right side of the cross point. Because of the fractional structure of $h_{\rm sr}$ in AF secrecy constraint, compensated information (provided by $|h_{\rm rd}|^2 - |h_{\rm re}|^2$) of AF scheme is limited by $h_{\rm sr}$ and is smaller than DF scheme. Thus, the maximal request secrecy rate AF achieves is smaller in the same $h_{\rm sr}$. In contrary, as the minimum structure of $h_{\rm sr}$ in DF secrecy constraint, DF scheme acquires full compensated information and can achieve higher maximal request secrecy rate.

2) Secrecy gain without eavesdropper's information: In this section, we analyze the secrecy gain in the scenario without eavesdropper's information Fig. 8. The area out of which eavesdropper must be excluded to guarantee secure communication is defined as insecure area and secure area is the result of the subtraction of total area and insecure area.

In Fig. 9, horizontal axis represents the request of secrecy rate and vertical axis represents secure area. Without relay, eavesdropper must be excluded out of the circle with radius 1 in Fig. 8 to guarantee nonzero secrecy rate. The introduction of relay enhances secure area. In our calculation, we put eavesdropper on every position of the area $\{x \in [-1,1], y \in [-1,1]\}$. For each eavesdropping position, we search all possible relays in $\{x \in [-1,1], y \in [-1,1]\}$ to find out whether there is a relay that can help source achieve nonzero secrecy rate. For one eavesdropping position, if we can find one relay in $\{x \in [-1,1], y \in [-1,1]\}$ that helps achieve nonzero secrecy rate, this eavesdropping position is included in secure area.

In Fig. 9, our calculation shows that both cooperative AF and DF relay can increase secure area. In the system without relay, the line declines to zero quickly and the maximal request secrecy rate is small. Cooperative relays (two lines on the right) help source achieve larger secure area on the same request secrecy rate, e.g., secure area of AF and DF are 2.45 and 2.6 when request secrecy rate is 0. And the maximal request secrecy rates of AF and DF that can be achieved in $\{x \in [-1,1], y \in [-1,1]\}$ are 1.1 and 1.5. Thus, cooperative relay facilitates secure communication even without eavesdropper's information. The line of DF relay is on the right of AF relay. This indicates that cooperative DF relay performs better in increasing secure area than AF relay.

V. Conclusion

We have introduced two cooperative relaying strategies to facilitate secure communication. The introduction of cooperative relays provides additional channels to transmit secret information. Calculation results demonstrate that cooperative relay can promote secrecy rate and there is a secrecy area-rate trade off in AF and DF scheme. Moreover, secrecy constraints on secure communication are discussed and are used explain the differences of the two cooperative schemes.

In future research, we will discuss the cooperation of two weak user (with zero secrecy capacity each) in secure communication. We are trying to find out whether their cooperation can achieve nonzero secrecy rate.

Acknowledgment

The authors would like to thank China Broadband Wireless Research Center, ARTC, Motorola, for her kind support.

References

[1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–87, 1975.

[2] I. Csiszar and J. Korner, Broadcast Channels with Confidential Messages, *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] R. Negi and S. Goel, Secret Communication Using Artificial Noise, *IEEE Vehicular Technology Conference*, vol. 3, pp. 1906-1910, September 2005.

[5] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," *IEEE International Symposium on Information Theory*, pp. 2466 - 2470, June 2007.

[6] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel," *http://arxiv.org/abs/0708.4219*, Aug 2007.

[7] X. Tang, R. Liu, P. Spasojevic and H.V. Poor, "Interference-Assisted Secret Communication," http://arxiv.org/abs/0804.1382, May 2008.

[8] L. Lai and H. El Gamal, "Cooperation for Secure Communication: The Relay Wiretap Channel," *IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 3, pp. 149 - 152, April 2007.

[9] 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, pp. 3062 - 3080, December 2004.