Communications and Network, **2013, 5, 42-47**
http://dx.doi.org/10.4236/cn.2013.53B2009 Published Online September 2013 (http://www.scirp.org/journal/cn)

Secure Communications for Two-Way Relay Networks Via Relay Chatting

Jun Xiong[1], Dongtang Ma[1], Chunguo Liu[2], Xin Wang[1]
[1]School of Electronic Science and Engineering, National University of Defense Technology, Changsha, China
[2]National Key Laboratory of Blind Signals Processing, Chengdu, China
Email: xj8765@nudt.edu.cn, dongtangma@nudt.edu.cn, schg_liu@126.com, wxwirelss@nudt.edu.cn

Received May, 2013

ABSTRACT

In this paper, we investigate a two-way relay network consisting of two sources, multiple cooperative relays and an eavesdropper. To enhance secure communications, a new relay chatting based on transmission scheme is proposed. Specifically, the proposed scheme selects a best relay that maximize the sum mutual information among the sources to forward the sources' signals using an amplify-and-forward protocol, and the remaining relays transmit interference signals to confuse the eavesdropper via distributed beam forming. It can be found that the proposed scheme with relay chatting does not require the knowledge of the eavesdropper's channel, and outperforms the joint relay and jammer selection scheme, which introduces the interference into the sources. Numerical results show that the secrecy outage probability of the proposed scheme converges to zero as the transmit power increases.

Keywords: Two-way Relay Networks; Physical Layer Security; Relay Chatting

1. Introduction

Recently, there has been considerable interest in physical layer security, which exploits randomness properties of wireless channels. It was pioneered in the 1970s by Wyner [1], who introduced the wiretap channel and demonstrated that when the wiretap channel is a degraded version of the main channel, the source and the legitimate receiver can exchange secure messages at a non-zero rate. The result was later extended to the scalar Gaussian channels [2] and broadcast channels [3]. With the additional spatial degrees of freedom (DoF) provided by multi-antenna systems, the limitation that the main channel could be worse than the eavesdropper channel can be overcome. In particular, the secrecy capacity in Gaussian multiple-input multiple-output (MIMO) wiretap channel was studied in [4,5].

However, due to cost and size limitations, multiple antennas may not be available at network nodes. In these scenarios, cooperation is an effective way to enable single-antenna nodes to enjoy the benefits of multi-antenna systems. And some recent works have been proposed to obtain security using cooperative relays [6-11]. In these works, proper relay or jammer selection schemes seem to be interesting approaches, which provide a good trade-off between secrecy performance and system complexity [9-11].

Opportunistic relay selection in one-way relay networks with secrecy constraints was addressed in [9], where the proposed scheme involved the joint selection of a relay and a jamming node to enhance the security. Following a similar idea, a joint relay and jammer selection were investigated for two-way cooperative networks in [10]. Different from [9], the proposed algorithms in [10] selected three relay nodes to enhance security, where the first selected node operated in the conventional relay mode and forwarded the sources' signals, and the second and third nodes acted as jammers to confuse the eavesdropper in the first and second phase, respectively. However, the secrecy outage probability would converge to a fixed value as the transmit power increases since the selected single-antenna jammer nodes introduced interference into the legitimate receiver [9,10]. Most recently, a relay chatting based on transmission scheme was proposed to enhance secure communications for one-way relay networks in [11], where a best relay was selected to forward the source's signal using an amplify-and-forward (AF) protocol, and the remaining relays transmitted a jamming signal to confuse the eavesdropper via distributed beam forming. It was shown that the use of opportunistic relay chatting guaranteed that the outage probability converged to zero at high transmit power.

Motivated by [11], we extend relay chatting based transmission scheme to two-way relay networks in this paper. Specially, a best relay that maximize the sum mutual information among the two sources is selected to forward the sources' signals, and two chatting groups formed from the remaining relays transmit artificial interference to degrade the eavesdropper in the first and second phase, respectively. It can be found that the proposed relay chatting scheme does not require the knowledge of the eavesdropper's channel state information (CSI), and obtains better secrecy performance than the joint relay and jammer selection scheme proposed in [10].

The reminder of this paper is organized as follows. We present the system model and signal model in Section 2. In Section 3, the relay chatting based transmission scheme is presented. Numerical results are provided in Section 4, and the conclusions are drawn in Section 5.

Notations: Vectors and matrices are typed in boldface letters, and variables are italic letters; the transpose, complex conjugate, Hermitian, and inverse of $\boldsymbol{A}$ are $\boldsymbol{A}^T$, $\boldsymbol{A}^*$, $\boldsymbol{A}^H$ and $\boldsymbol{A}^{-1}$, respectively; $\boldsymbol{I}_N$ denotes a $N \times N$ identity matrix; $\boldsymbol{E}\{\bullet\}$ denotes statistical expectation while $\Pr\{\bullet\}$ denotes the probability of an input event; $[x]^+ \triangleq \max\{0, x\}$.

2. System Model and Signal Model

2.1. System Model

We assume a network configuration consisting of two sources S$_1$ and S$_2$, one eavesdropper E, and a relay node set $S_{in} = \{1, 2, \cdots, K\}$ with K nodes. Each node is equipped with a single omni-directional antenna and operates in a half-duplex mode. In **Figure 1**, it schematically shows the system model. As the relay nodes cannot transmit and receive simultaneously, the total communication process is performed by two phases. In the first phase, S$_1$ and S$_2$ broadcast their messages s_1 and s_2, and the best relay node R^* listens, where the criterion for the best relay selection will be discussed later. At the same time, a chatting group with size N_1, denoted by

$$\Re_1 = \left\{R_1, R_2, \cdots, R_{N_1}\right\},$$

is formed from the remaining $K-1$ relays and transmits a random messages x_1 via distributed beamforming. In the second phase, the best relay node forwards the source messages to the corresponding destinations based on AF protocol while a new chatting group of size N_2, denoted as $\Re_2 = \left\{R_1, R_2, \cdots, R_{N_2}\right\}$, transmits a random message x_2 using a new beam forming vector. We assume that the eavesdropper E can overhear the signals from the two phases.

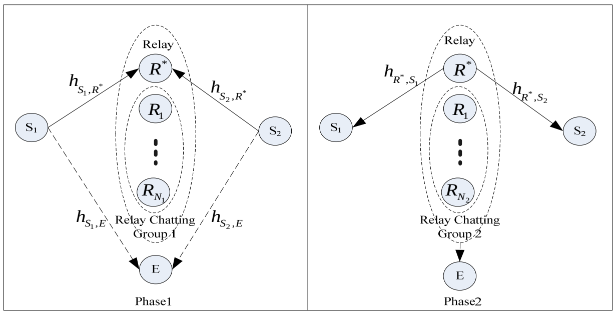

Figure 1. System model with two sources S$_1$ and S$_2$, a relay node set, and one eavesdropper E.

The channel gain from node i to node j is denoted by $h_{i,j}$, which is modeled as a zero-mean, independent, circularly-symmetric complex Gaussian random variable with the variance $\sigma_{i,j}^2$, where $\sigma_{i,j}^2 = d_{i,j}^{-\beta}$, $d_{i,j}$ denotes the Euclidean distance between node i and node j, and β represents the path-loss exponent. Furthermore, additive white Gaussian noise (AWGN) with zero mean and unit variance is assumed at each receiver.

2.2. Signal Model

In the first phase, the two sources send information symbols s_1 and s_2, respectively, which are mapped to a PSK set. The received signals at the best relay node R^* and eavesdropper E can be, respectively, expressed as

$$\begin{aligned} y_{R^*} &= \sqrt{P_{S_1}} h_{S_1,R^*} s_1 + \sqrt{P_{S_2}} h_{S_2,R^*} s_2 + \sqrt{P_{R_1}} \boldsymbol{h}_{R^*}^T \boldsymbol{f}_1 x_1 + n_{R^*}, \\ y_{E1} &= \sqrt{P_{S_1}} h_{S_1,E} s_1 + \sqrt{P_{S_2}} h_{S_2,E} s_2 + \sqrt{P_{R_1}} \boldsymbol{h}_{E1}^T \boldsymbol{f}_1 x_1 + n_{E1}, \end{aligned} \tag{1}$$

where $\boldsymbol{E}\left\{|s_i|^2\right\} = 1,\ i = 1, 2$, n_{R^*} and n_{E1} denote the noise at R^* and the eavesdropper E, respectively.

$$\boldsymbol{h}_{E_1} = \left[h_{R_1,E}, h_{R_2,E}, \cdots, h_{R_{N_1},E}\right]^T$$

with $h_{R_i,E}$ denoting the channel gain from the relay node R_i of the chatting group $\Re_1$ to the eavesdropper E. And

$$\boldsymbol{h}_{R^*} = \left[h_{R_1R^*}, h_{R_2R^*}, \cdots, h_{R_{N_1}R^*}\right]^T$$

with h_{R_i,R^*} denoting the channel gain from the relay node R_i of the chatting group $\Re_1$ to the best relay node R^*. $\boldsymbol{f}_1$ is the beamforming vector and x_1 is the interference signal with $\boldsymbol{E}\left\{|x_1|^2\right\} = 1$. In order to make the interference signal invisible to the best relay node while only degrading the eavesdropper's reception, $\boldsymbol{f}_1$ should be constructed to satisfy $\boldsymbol{h}_{R^*}^T \boldsymbol{f}_1 = 0$ and $\boldsymbol{f}_1^H \boldsymbol{f}_1 = 1$. P_{R_1} denotes the transmit power of the relay chatting group $\Re_1$.

In the second phase, R^* is selected to amplify its received signal, and forwards it to S$_1$ and S$_2$. At the same time, a new chatting group of size N_2, denoted by $\Re_2$, creates a new beamforming vector $\boldsymbol{f}_2$ to transmit interference signal. Similarly, we should make the interference signal invisible to the two sources. Hence, $\boldsymbol{f}_2$ should be located at its null space of the two sources' channels, i.e., $[\boldsymbol{h}_1,\boldsymbol{h}_2]^T \boldsymbol{f}_2=\boldsymbol{0}$ and $\boldsymbol{f}_2^H\boldsymbol{f}_2=1$, where $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$ denote the channels from the relay node of the chatting group $\Re_2$ to the sources S1 and S2, respectively. As such, the signals transmitted from the best relay node R^* can be expressed as

$$x_{R^*}=\alpha y_{R^*}, \tag{2}$$

where $\alpha=\sqrt{P_{R^*}}\Big/\sqrt{1+P_{S_1}\left|h_{S_1,R^*}\right|^2+P_{S_2}\left|h_{S_2,R^*}\right|^2}$ and P_{R^*} denotes the transmit power of the node R^*.

Since each source knows the own transmit signal $s_i\ (i=1,2)$, it can cancel the self-interference [10]. Thus, each source can extract the message from the other source. As such, the residual signals at S1 and S2 can be respectively expressed as

$$\begin{aligned} y_1&=\alpha\sqrt{P_{S_2}}h_{R^*,S_1}h_{S_2,R^*}s_2+\alpha h_{R^*,S_1}n_{R^*}+n_1,\\ y_2&=\alpha\sqrt{P_{S_1}}h_{R^*,S_2}h_{S_1,R^*}s_1+\alpha h_{R^*,S_2}n_{R^*}+n_2,\end{aligned} \tag{3}$$

where n_1 and n_2 denote the noise at the sources S1 and S2, respectively.

On the other hand, the received signal at the eavesdropper can be expressed as

$$\begin{aligned} y_{E2}&=\alpha\sqrt{P_{S_1}}h_{R^*,E}h_{S_1,R^*}s_1+\alpha\sqrt{P_{S_2}}h_{R^*,E}h_{S_2,R^*}s_2\\ &+\sqrt{P_{R_2}}\boldsymbol{h}_{E_2}^T\boldsymbol{f}_2x_2+\alpha h_{R^*,E}n_{R^*}+n_{E2},\end{aligned} \tag{4}$$

where $\boldsymbol{h}_{E_2}=\left[h_{R_1E},h_{R_2E},\cdots,h_{R_{N_2}E}\right]^T$ with $h_{R_i,E}$ denoting the channel gain from the relay node R_i of the chatting group $\Re_2$ to the eavesdropper E. P_{R_2} denotes the transmit power of the relay chatting group $\Re_2$. x_2 is the interference signal with $\boldsymbol{E}\left\{|x_2|^2\right\}=1$, and n_{E2} denotes the noise at the eavesdropper E.

3. Secure Communications with Relay Chatting

In this section, we discuss the relay selection for the proposed secure scheme with relay chatting. Then, we provide the secrecy outage probability as the metric of the secrecy performance.

3.1. Relay Selection

We define Γ_j as the signal to interference-plus-noise ratio (SINR) of the virtual channel $S_i\to S_j$ (for $i,j=1,2,\quad i\neq j$). They can be calculated as

$$\Gamma_1=\frac{\alpha^2P_{S_2}\left|h_{R^*,S_1}\right|^2\left|h_{S_2,R^*}\right|^2}{\alpha^2\left|h_{R^*,S_1}\right|^2+1}, \tag{5a}$$

$$\Gamma_2=\frac{\alpha^2P_{S_1}\left|h_{R^*,S_2}\right|^2\left|h_{S_1,R^*}\right|^2}{\alpha^2\left|h_{R^*,S_2}\right|^2+1}. \tag{5b}$$

Thus, the sum mutual information among the sources can be expressed as

$$\begin{aligned}\boldsymbol{I}_S&=\frac{1}{2}\boldsymbol{I}\left(y_1;s_2\right)+\frac{1}{2}\boldsymbol{I}\left(y_2;s_1\right)\\ &=\frac{1}{2}\log_2\left[\left(1+\Gamma_1\right)\left(1+\Gamma_2\right)\right],\end{aligned} \tag{6}$$

where $\boldsymbol{I}\left(y_i;s_j\right)=\frac{1}{2}\log_2\left(1+\Gamma_i\right)$ with $i,j=1,2,\ i\neq j$ and the scalar factor $1/2$ is due to the fact that two time units are required in two phases.

Equation (6) can be used as the criterion for the best relay selection, i.e.,

$$\begin{aligned}\left\{R^*\right\}&=\arg\max_{R\in S_{in}}\boldsymbol{I}_S\\ &=\arg\max_{R\in S_{in}}\left\{\left(1+\Gamma_1\right)\left(1+\Gamma_2\right)\right\}.\end{aligned} \tag{7}$$

We can find that the relay selection strategy based on Equation (7) is not dependent on the eavesdropper's CSI. In addition, the relay selection can be implemented in a distributed way [12], since each node only requires its local CSI to calculate Equation (7).

3.2. Secrecy Outage Probability

We use the secrecy outage probability as the metric of secrecy performance. The meaning of the secrecy outage probability is twofold. First, it provides the outage probability for the case where the intended destinations are unable to decode the messages from the sources reliably. It also gives the metric for the case where the message transmission is not perfectly secure, i.e., there exists some information leakage to the eavesdropper E [13].

In order to calculate the secrecy outage probability, we firstly have to get the SINR of the links $S_i\to E$ for $i=1,2$. We assume a simple case in which the eavesdropper applies maximal ratio combining (MRC), so as to examine the efficiency of the proposed scheme. According to MRC, the eavesdropper E combines the received signals by multiplying y_{E1} and y_{E2} with proper weighting factors.

$$y_E^i=\alpha_1^iy_{E1}+\alpha_2^iy_{E2}, \tag{8}$$

where y_E^i represents the combining signal for the source S_i and

$$\alpha_1^i=\frac{\sqrt{P_{S_i}}h_{S_i,E}^*}{\sigma_{N_{E1,S_j}}^2}, \tag{9}$$

$$\alpha_2^i=\frac{\alpha\sqrt{P_{S_i}}h_{R^*E}^*h_{S_iR^*}^*}{\sigma_{N_{E2,S_j}}^2}, \tag{10}$$

with $i,j=1,2,\ i\neq j$. $\sigma_{N_{E1,S_j}}^2$ and $\sigma_{N_{E2,S_j}}^2$ represent the total interference and noise power terms in y_{E1} and y_{E2}, denoted by respectively,

$$\sigma^2_{N_{E1,S_j}} = P_{S_j}\left|h_{S_j,E}\right|^2 + P_{R_1}\left|\boldsymbol{h}^T_{E_1}\boldsymbol{f}_1\right|^2 + 1, \tag{11}$$

$$\begin{aligned}\sigma^2_{N_{E2,S_j}} &= \alpha^2 P_{S_j}\left|h_{R^*,E}\right|^2\left|h_{S_j,R^*}\right|^2 + P_{R_2}\left|\boldsymbol{h}^T_{E_2}\boldsymbol{f}_2\right|^2 \\ &\quad + \alpha^2\left|h_{R^*,E}\right|^2 + 1.\end{aligned} \tag{12}$$

Thus, the SINR of the link $S_i \to E$ can be calculated as

$$\begin{aligned}\Gamma_{E_i} &= \frac{P_{S_i}\left|h_{S_i,E}\right|^2}{P_{S_j}\left|h_{S_j,E}\right|^2 + P_{R_1}\left|\boldsymbol{h}^T_{E_1}\boldsymbol{f}_1\right|^2 + 1} \\ &\quad + \frac{\alpha^2 P_{S_i}\left|h_{R^*E}\right|^2\left|h_{S_iR^*}\right|^2}{\alpha^2 P_{S_j}\left|h_{R^*,E}\right|^2\left|h_{S_j,R^*}\right|^2 + P_{R_2}\left|\boldsymbol{h}^T_{E_2}\boldsymbol{f}_2\right|^2 + \alpha^2\left|h_{R^*,E}\right|^2 + 1}.\end{aligned} \tag{13}$$

The instantaneous secrecy rate with the relay node set S_{in} for the source S_i can be expressed as [10]

$$R_{S_i} = \left[\frac{1}{2}\log_2\left(1+\Gamma_i\right) - \frac{1}{2}\log_2\left(1+\Gamma_{E_j}\right)\right]^+, \tag{14}$$

where $i, j = 1, 2,\ i \neq j$.

The overall secrecy performance of the two-way relay network is characterized by the sum of the two sources' secrecy rate, i.e.,

$$\begin{aligned}R_S &= R_{S_1} + R_{S_2} \\ &= \left[\frac{1}{2}\log_2\frac{1+\Gamma_1}{1+\Gamma_{E_2}} + \frac{1}{2}\log_2\frac{1+\Gamma_2}{1+\Gamma_{E_1}}\right]^+ \\ &= \frac{1}{2}\left[\log_2\frac{\left(1+\Gamma_1\right)\left(1+\Gamma_2\right)}{\left(1+\Gamma_{E_2}\right)\left(1+\Gamma_{E_1}\right)}\right]^+.\end{aligned} \tag{15}$$

For a target secrecy rate R_0, the secrecy outage probability can be expressed as follows [13,14]

$$\begin{aligned}P_{so}\left(R_S \le R_0\right) &= \Pr\left[R_S \le R_0\right] \\ &= \Pr\left[\frac{\left(1+\Gamma_1\right)\left(1+\Gamma_2\right)}{\left(1+\Gamma_{E_2}\right)\left(1+\Gamma_{E_1}\right)} \le 2^{2R_0}\right].\end{aligned} \tag{16}$$

3.3. Performance Analysis at High Transmit Power

In this subsection, we do some quantitative analysis on the asymptotic performance for the proposed scheme in high transmit power range.

Following the similar idea from [10], we assume that the transmit power for all nodes including two sources, the selected best relay and the relay chatting set is the same. In other words, as the source's transmit power $P_S \to \infty$, P_{S_i}, P_{R^*} and P_{R_i} also go to infinity. In this case, we can obtain

$$\lim_{P_S\to\infty}\Gamma_i = \frac{P_S\left|h_{R^*,S_i}\right|^2\left|h_{S_j,R^*}\right|^2}{\left|h_{R^*,S_i}\right|^2 + \left|h_{S_i,R^*}\right|^2 + \left|h_{S_j,R^*}\right|^2}, \tag{17}$$

$$\begin{aligned}\lim_{P_S\to\infty}\Gamma_{E_i} &= \frac{\left|h_{S_i,E}\right|^2}{\left|h_{S_j,E}\right|^2 + \left|\boldsymbol{h}^T_{E_1}\boldsymbol{f}_1\right|^2} \\ &\quad + \frac{\left|h_{R^*E}\right|^2\left|h_{S_iR^*}\right|^2}{\left|h_{R^*,E}\right|^2\left|h_{S_j,R^*}\right|^2 + \left(\left|h_{S_i,R^*}\right|^2 + \left|h_{S_j,R^*}\right|^2\right)\left|\boldsymbol{h}^T_{E_2}\boldsymbol{f}_2\right|^2},\end{aligned} \tag{18}$$

where $i, j = 1, 2,\ i \neq j$.

We can see that Γ_i grows rapidly as P_S increases, while Γ_{E_i} converges to a fixed value that depends on the corresponding channels. Therefore, based on Equation (16), the secrecy outage probability can go to zero at high transmit power, i.e., $P_{so}\left(R_S \le R_0\right) \to 0$ as $P_S \to \infty$.

4. Numerical Results

In this section, we provide numerical results in order to validate the effectiveness of the proposed scheme. The simulation environment consists of two sources S$_1$ and S$_2$, one eavesdropper E, and a relay node cluster. We assume that all nodes are located in a 2D square topology within a 1×1 unit square. We consider this scenario where S$_1$, S$_2$, and E are located at

$$\left(X_{S_1}, Y_{S_1}\right) = (0,1),\ \left(X_{S_2}, Y_{S_2}\right) = (1,1),$$

and $\left(X_E, Y_E\right) = (0.5, 0)$,

respectively. The K relay nodes spread randomly within the square space. For example, **Figure 2** gives the simulation scenario with $K = 8$ relays.

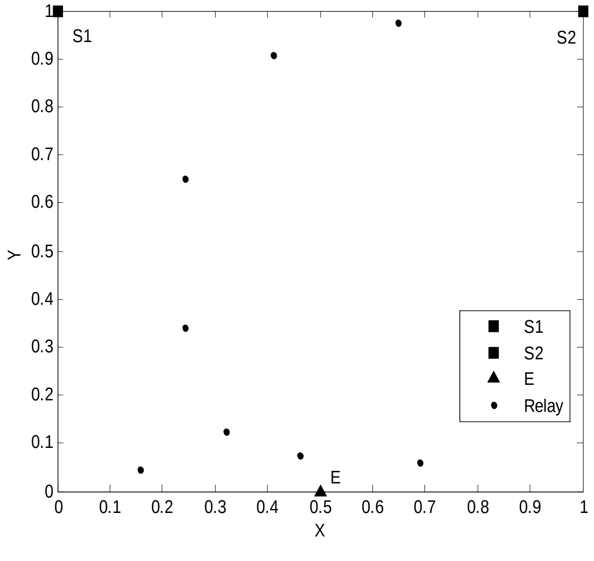

Figure 2. The 1 × 1 simulation scenario with K = 8 relays.

We assume that the sources, the best relay R^*, and the chatting group transmit with the same power, i.e., $P_{S_i} = P_{R^*} = P_{R_i} = P_S$, $i = 1,2$. The path-loss exponent is set to $\beta = 3$. All the remaining $K-1$ relay nodes are used as chatting relays, i.e., $N_1 = N_2 = K-1$.

In **Figure 3**, the secrecy outage probabilities have been shown as functions of the transmit power P_S. The target secrecy rate is set as $R_0 = 3$ bits/s/Hz. It can be seen that the relay chatting scheme can realize zero-appoaching outage probability as the transmit power increases. Meanwhile, as the number of the relay nodes increases, the secrecy outage probability profoundly decreases. A similar observation can be found in **Figure 4**, which presents the secrecy outage probability with different target secrecy rate R_0. The transmit power P_S is set to 10 dB. The secrecy performance can be improved by inviting more relays into cooperation due to the opportunistic use of the multiple relays.

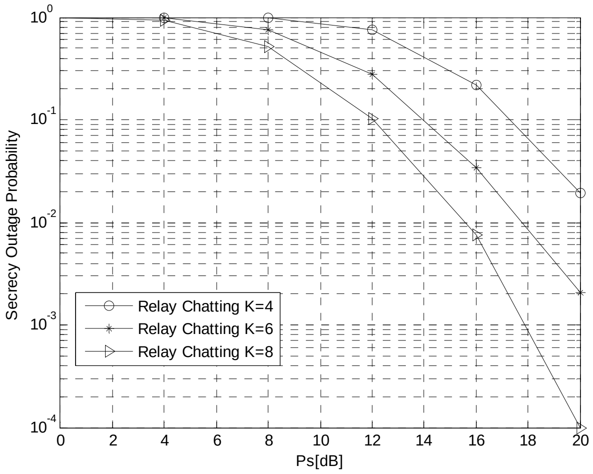

Figure 3. Secrecy outage probability versus the transmit power P_S with different number of relays K.

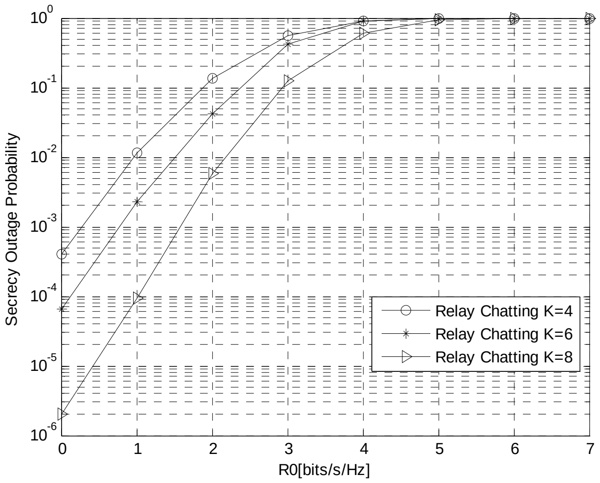

Figure 4. Secrecy outage probability versus the target secrecy rate R_0 with different number of relays K.

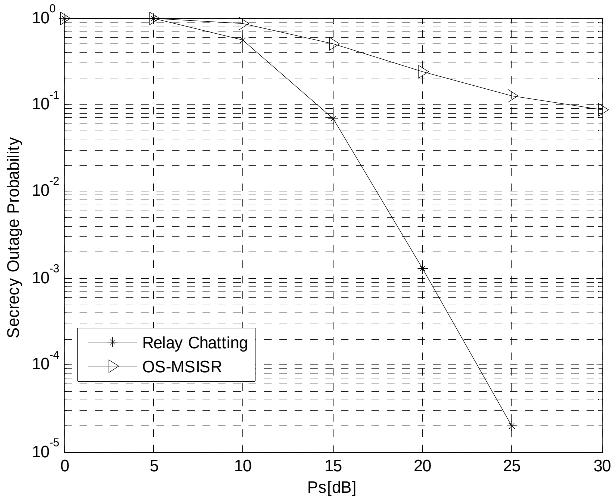

Figure 5. Secrecy outage probability versus the transmit power P_S..

Next, we compare the proposed relay chatting scheme with the joint relay and jammer selection scheme proposed in [10]. It is assumed in [10] that the jammers transmit with a power subject to the relay-jammer power ratio $L = 10$, i.e., $P_J = P_{R^*}/L$ where P_J denotes the transmit power of the selected jammer node. We give the simulation results of the optimal selection with maximum sum instantaneous secrecy rate (OS-MSISR) in Section III-A of [10]. It can be found that the OS-MSISR scheme requires the precise knowledge of the eavesdropper's channel, which is hard to obtain, e.g., a passive eavesdropper [14]. However, the proposed relay chatting in the previous section avoids the use of the eavesdropper's CSI.

Figure 5 presents the secrecy outage probability of both schemes, where the target secrecy rate is set to $R_0 = 3.5$ bits/s/Hz and the number of relay nodes is $K = 8$. As shown in $R_0 = 3.5$, the secrecy outage probability of OS-MSISR would converge to a fixed value as the transmit power P_S increases since the selected single-antenna jammer nodes introduce the interference into the sources. It can be also seen that the secrecy outage probability of our proposed relay chatting scheme can converge to zero as the transmit power P_S goes to infinity.

5. Conclusions

In this paper, a new relay chatting transmission scheme is proposed to enhance secure communications for two-way relay networks. The proposed scheme does not require the knowledge of the eavesdropper's channel and achieves better performance than the joint relay and jammer selection scheme. Performance analysis and simulation results show that the secrecy outage probability of the proposed scheme goes to zero as the transmit power increases.

6. Acknowledgements

This work was supported in part by the NSFC under Grants 61101096 and 61002032, and the NSF of Hunan Province under Grant 11jj4055.

REFERENCES

[1] A. D. Wyner, “The Wiretap Channel,” *Bell System Technical Journal*, Vol. 54, No. 8, 1975, pp. 1355-1367. doi:10.1002/j.1538-7305.1975.tb02040.x

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian Wiretap Channel,” *IEEE Transactions on Information Theory*, Vol. 24, No. 4, 1978, pp. 451-456. doi:10.1109/TIT.1978.1055917

[3] I. Csiszár and J. Körner, “Broadcast Channels With Confidential Messages,” *IEEE Transactions on Information Theory*, Vol. 24, No. 3, 1978, pp. 339-348. doi:10.1109/TIT.1978.1055892

[4] F. Oggier and B. Hassibi, “The Secrecy Capacity of The MIMO Wiretap Channel,” *IEEE Transactions on Information Theory*, Vol. 57, No. 8, 2011, pp. 4961-4972. doi:10.1109/TIT.2011.2158487

[5] T. Liu and S. Shamai, “A Note on The Secrecy Capacity of The Multiple Antenna Wiretap Channel,” *IEEE Transactions on Information Theory*, Vol. 55, No. 6, 2009, pp. 2547-2553. doi:10.1109/TIT.2009.2018322

[6] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays,” *IEEE Transactions on Signal Processing*, Vol. 58, No. 3, 2010, pp. 1875-1888. doi:10.1109/TSP.2009.2038412

[7] H. M. Wang, Q. Y. Yin and X. G. Xia, “Improving the Physical Layer Security of Wireless Two-Way Relaying via Analog Network Coding,” *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM)*, Texas, Houston, Dec. 2011.

[8] H. M. Wang, Q. Y. Yin and X. G. Xia, “Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks,” *IEEE Transactions on Signal Processing*, Vol. 60, No. 7, 2012, pp. 3532-3545. doi:10.1109/TSP.2012.2191543

[9] I. Krikidis, J. S. Thompson and S. McLaughlin, “Relay Selection for Secure Cooperative Networks With Jamming,” *IEEE Transactions on Wireless Communications*, Vol. 8, No. 10, 2009, pp. 5003-5011. doi:10.1109/TWC.2009.090323

[10] J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, “Joint Relay and Jammer Selection for Secure Two-Way Relay Networks,” *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, Jan. 2012, pp. 310-320. doi:10.1109/TIFS.2011.2166386

[11] Z. Ding, K. K. Leung, D. L. Goeckel and D. Towsley. “Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs. Relay Chatting,” *IEEE Transactions on Wireless Communications*, Vol. 10, No. 6, 2011, pp. 1725-1729. doi: /10.1109/TWC.2011.040511.101694

[12] A. Bletsas, A. Khisti, D. P. Reed and A. Lippman, “A Simple Cooperative Diversity Method Based On Network Path Selection,” *IEEE Journal Selected in Areas Communications*, Vol. 24, No. 3, Mar. 2006, pp. 659-672. doi:10.1109/JSAC.2005.862417

[13] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wireless Information-theoretic Security,” *IEEE Transactions on Information Theory*, Vol. 54, No. 6, 2008, pp. 2515-2534. doi:10.1109/TIT.2008.921908

[14] J. Xiong, K. K. Wong, D. Ma and J. Wei, “A Closed-Form Power Allocation for Minimizing Secrecy Outage Probability for MISO Wiretap Channels via Masked Beamforming,” *IEEE Communications Letters*, Vol. 16, No. 9, 2012, pp. 1496-1499. doi:10.1109/LCOMM.2012.073112.121254