Joint Source-Relay Selection Scheme for Cooperative Networks under Eavesdropping Environment

Jianbin Xue[1], Heng Zhu[1], Xiaoming Liao[1], and Zhe Su[2]
(Corresponding author: Heng Zhu)
School of Computer and Communication, Lanzhou University of Technology[1]
No. 287, Langongping Road, Qilihe District, Lanzhou 730050, China
School of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics[2]
No. 29, Jiangjun Avenue, Jiang Ning District, Nanjing 210096, China
(Email: 490853309@qq.com)
(Received Mar. 27, 2018; Revised and Accepted Aug. 18, 2018; First Online June 24, 2019)

Abstract

In this paper, we propose a low complexity opportunistic source-relay selection algorithm based on power allocation for multi-source multi-relay cooperative network. We consider that the channel state information of both the main channels and the wiretap channels to minimize the system secrecy outage probability. First of all, the optimal power allocation factor for each link is given when the total transmission power is limited. Secondly, the optimal selection algorithm is designed based on power allocation and the approximate expression of the secrecy outage probability is derived in the high signal-to-noise ratio regime. Numerical experimental results demonstrate that the system secrecy outage probability of the proposed algorithm is related to the number of relay nodes but has no relation with the number of relay nodes. The proposed a low complexity opportunistic source-relay selection algorithm in this paper not only reduces the computational complexity but also has lower secrecy outage probability compared with the traditional source-relay selection algorithm.

Keywords: Cooperative Communication; Decode-and-Forward; Physical Layer Security; Secrecy Outage Probability; Source-Relay Selection

1 Introduction

With the explosive development of modern digital wireless communication technology and the continual emergence of new networks, the complexity of the wireless network security [5] problem has increasingly become the focus that people concern. Meanwhile, the open channel environment of the wireless network and the mobility of the terminal equipment also bring serious potential dangers to the information security, which makes more vulnerable to malicious attacks than the wired network. How to ensure the secure transmission of confidential information in wireless network is facing a severe test, and the security of the user information is confronting with new serious challenges.

Traditional encryption methods with secret key cryptography can obtain better safely performance, nevertheless, the encryption algorithm is too complex frequently, which need at the expense of great computation cost and increase signaling overheads undoubtedly [7]. Unlike the traditional cryptographic system, physical layer security is based on Shannon theory using the uncertain characteristics of noise channel, which does not require sophisticated algorithm to present being eavesdropped and it can theoretically analyze the degree of the information leakage easily. In recent years, scholars have paid more and more attention to the physical layer security technology [3, 6]. In [16], the authors first proposed the concept of the physical layer security and pointed out that it can also ensure data transmission security when the channel condition of legitimate users is better than the wiretap channel without need to create the keys. The authors in the literature [15] investigated the physical layer security of the multiple access Gauss wiretap channel.

It is known that there is a close connection between the secrecy transmission rate and the channel quality under eavesdropping environment, the secrecy transmission rate will be extremely low even may be to zero when the quality condition of the main channel and the eavesdropper channel is approximately equal. Cooperative relay technology has been recognized as an effective technique to achieve space diversity gain by using a virtual antenna array, which can combat channel fading effectively and increase the reliability and information rate of the transmission system. On the other hand, cooperative com-

munication technology can improve the network coverage and have been adopted in industry standard, *e.g.*, the IEEE802.16j [9] standard for relay-based wireless access networks.

Recently, a lot of works in the literature [2, 8, 11, 14] focused on improving the transmission reliability of wireless communication network by multi-user diversity and multi-relay diversity. The authors of literature [14] studied the network security by combining cooperative diversity in multi-users multi-relay cooperation network scenario. In the literature [2], three opportunistic relay selection algorithms were proposed with privacy constraints in cooperative network. Cooperative communication technology is widely used, and it can be applied to mobile communication in conjunction with D2D technology, and can also be applied to ad hoc networks [1, 12] and wireless Mesh networks. Although cooperative diversity gain has the ability to improve the reliability of wireless communication network, but with the number of users and cooperative relay nodes increases, it is also more vulnerable to illegal attack because of the same information to be sent two times or more. To solve this problem, a new multi-user multi-relay scheme based on cooperative jamming was proposed aim at maximizing the secrecy transmission rate in literature [10].

For the scenario of multiple emission sources or multiple relays, the choice of source node and relay node has a decisive influence on the system performance, so it is extremely important to select the optimal source node and relay node from plenty of potential nodes. The authors of [13] proposed the relay selection strategy by adopting decode-and-forward (DF) protocol based on the minimum secrecy outage probability (SOP) under the eavesdropping environment, which has lower outage probability compare with direct communication. In [17], the physical layer security of a multi-user system was studied in cognitive radio network. In [18], the optimal relay selections scheme for DF and amplify-and-forward (AF) relay protocols were given respective and the outage probability was analyzed. The authors of [4] discussed the performance of the optimal source-relay selection.

However, all of the above researches were assumed that the secrecy transmission rate was the fixed value zero, which lack generality. In this paper, we investigate the network physical layer security of the multi-source multi-relay cooperation network under the eavesdropping environment, and propose a source-relay selection algorithm based on power allocation aim at minimizing the system SOP. Firstly, we obtain the optimal power allocation factor for any link when the total power of the source node and relay node is limited. Basis of this, we derive the optimal source-relay selection algorithm. Subsequently, we evaluate the closed-form expression of the system SOP. Simulation results show that the proposed source-relay selection algorithm has better security performance than the traditional selection algorithm.

The remainder of this paper is organized as follows. In Section 2, we give the system model of multi-source multi-relay with an eavesdropper. In Section 3, we present the traditional source-relay selection algorithms and propose the optimal selection algorithm base on power allocation. Subsequently, we give the SOP of three selection algorithms. Finally, the related conclusion is drawn in Section 4.

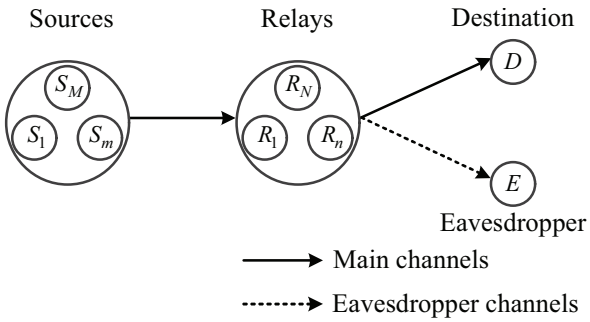

Figure 1: System model of multi-source multi-relay cooperative networks with an eavesdropper

2 System Model

As shown in Figure 1, we consider a multi-source multi-relay cooperation network, which consists of M source nodes $S_m(m = 1, 2 \cdots M)$, N candidate relay nodes $R_n(n = 1, 2 \cdots N)$, a destination node D and an eavesdropper E. In the actual communication, it is difficult for relays to transmit and receive message at the same frequency band simultaneously because of the impact of relay radio frequency devices. Therefore, all the relay nodes in this paper are equipped with a single antenna and adopt half-duplex communication mode. That is to say, the transmitted signal and the received signal must be conducted at the different time-slot.

It is assumed that there is no direct link from the source nodes to the destination node and eavesdropper, all communications must be assisted for relay and all the links follow independent flat Rayleigh fading distribution. The whole communication process is divided into two phases. In the first phase, in order to prevent the wiretap as much as possible, the optimal source-relay pair (S_{m^*}, R_{n^*}) is selected to maximum the system secrecy transmission rate. Then the selected source node S_{m^*} sends the message to the relay node R_{n^*} during this phase. In the second phase, the source sends any information no longer. The relay node R_{n^*} forwards the information received in the first phase to the destination node D as well as the eavesdropper E may overhear the information simultaneously.

In the first phase, the source S_{m^*} broadcasts the signal x_0 and the relay R_{n^*} receives the signal as:

$$y_{S_m R_n} = \sqrt{P_s} h_{S_m R_n} x_0 + n_{S_m R_n}$$

Where P_s represents the transmission power of the source S_m; $h_{S_m R_n}$ represents the channel coefficient of the link

between the source S_m and the relay R_n,which is modeled as a zero-mean complex Gaussian fading distributed with variances $\sigma^2_{R_n}$; $n_{S_m R_n}$ represents the additive Gauss white noise (AGWN) at R_n with zero-mean and variance $\sigma^2_{R_n}$.Therefore, the instantaneous signal-to-noise ratio (SNR) at R_n can be expressed as:

$$\gamma_{S_m R_n} = \frac{P_s |h_{S_m R_n}|^2}{\sigma^2_{R_n}} \tag{1}$$

In the second phase, it is assumed that the eavesdropper E knows the instantaneous channel state information (CSI) of all the relay nodes. The selected optimal relay using DF protocol to transmit data, thus the receive information at D and E can be written respectively as:

$$\begin{aligned} y_D &= \sqrt{P_i} h_{R_n D} \hat{x} + n_{R_n D} \\ y_E &= \sqrt{P_i} h_{R_n E} \hat{x} + n_{R_n E}. \end{aligned}$$

Where $\hat{x}$ represents the re-encode data symbol of the relay R_n; P_i is the transmission power of the relay R_n; $h_{R_n D}$ and $h_{R_n E}$ represent the channel coefficients of the links from to D and E respectively, which are modeled as the zero-mean complex Gaussian distribution with variances $\Omega_{R_n D}$ and $\Omega_{R_n E}$; $n_{R_n D}$ and $n_{R_n E}$ represents the AWGN at R_n with zero-mean and variances $\sigma^2_{R_n}$ and σ^2_E, respectively. Therefore, the instantaneous SNR at D and E are expressed respectively as:

$$\gamma_{R_n D} = \frac{P_i |h_{R_n D}|^2}{\sigma^2_D} \tag{2}$$

$$\gamma_{R_n E} = \frac{P_i |h_{R_n E}|^2}{\sigma^2_E}$$

For the calculation convenience, in this paper, we let $\sigma^2_{R_n} = \sigma^2_D = \sigma^2_E = N_0$. In the cooperative communication network under eavesdropping environment, the channel $S_m \to R_n$ and $R_n \to D$ are called the main channels, and the channel $R_n \to E$ is called the eavesdropper channels. When the relay node is used DF protocol to transmit data, the relay has a certain probability of decoding errors from the source node information. Combining Equations (1) and (2), the SNR of the main channel can be expressed as $\gamma_{S_m R_n D} = \min(\gamma_{S_m R_n}, \gamma_{R_n D})$, so the information transmission rate at the node D and E can be written as:

$$\begin{aligned} C_{S_m R_n D} &= \frac{1}{2} \log_2 \left[1 + \min(\gamma_{S_m R_n}, \gamma_{R_n D})\right] \\ C_{R_n E} &= \frac{1}{2} \log_2 (1 + \gamma_{R_n E}) \end{aligned} \tag{3}$$

It is known that the system secrecy transmission rate is defined as the information rate difference between the main channel and the eavesdropper channel. So the system secrecy transmission rate can be expressed as:

$$C_{\text{sec}} = \frac{1}{2} \log_2 \left[\frac{1 + \min(\gamma_{S_m R_n}, \gamma_{R_n D})}{1 + \gamma_{R_n E}} \right]^+ \tag{4}$$

Where $[x]^+ = \max(0, x)$, thus the system SOP can be defined as:

$$P^{\text{out}}_{\text{sec}} = \Pr(C_{\text{sec}} < R). \tag{5}$$

Where R indicates the system secrecy transmission rate threshold.

3 Joint Source-Relay Selection and Performance Analysis

In the process of source-relay pair selection, for each communication, the choice of the optimal source-relay should satisfy the maximum system secrecy transmission rate from Equation (3). In this section, we mainly explore the selection algorithm. Firstly, we give the average SOP of the random source-relay selection algorithm and the traditional source-relay selection algorithm. Secondly, we and derive the closed form expression of the system SOP. It's assumed that the total power of all nodes is P_T, let $P_T/N_0 = \gamma$. The transmission power between source node and relay is equal when using the random selection algorithm and the traditional selection algorithm, that is $P_s = P_i = P_T/2$.

3.1 Random Source-Relay Selection algorithm

There are $M \cdot N$ combinations of the random source-relay selection algorithm, one of which can be chosen with equal probability $1/(M \cdot N)$. When (S_m, R_n) is selected for communication, combining Equations (4) and (5), at the high SNR regime, the system SOP can be derived as:

$$\begin{aligned} P^{\text{out}}_{\text{sec},S_m R_n} &= \Pr\{\min(h_{S_m R_n}, h_{R_n D}) < g(R) h_{R_n E}\} \\ &= \int_0^\infty \{1 - \exp(-\frac{g(R)x}{\Omega_{S_m R_n}} - \frac{g(R)x}{\Omega_{R_n D}})\} f_{h_{R_n E}}(x) dx \\ &= 1 - \frac{1}{\Omega_{R_n E}} (\frac{g(R)}{\Omega_{S_m R_n}} + \frac{g(R)}{\Omega_{R_n D}} + \frac{1}{\Omega_{R_n E}})^{-1} \end{aligned}$$

Where $g(R) = 2^{2R}$, when adopt the random selection algorithm, the system average SOP can be derived as:

$$\begin{aligned} P^{\text{out}}_{\text{sec,ave}} &= \frac{1}{M \cdot N} \sum_{m=1}^{M} \sum_{n=1}^{N} P^{\text{out}}_{\text{sec},S_m R_n} \\ &= \frac{1}{M \cdot N} \sum_{m=1}^{M} \sum_{n=1}^{N} \{1 \\ &\quad - \frac{1}{\Omega_{R_n E}} \left(\frac{g(R)}{\Omega_{S_m R_n}} + \frac{g(R)}{\Omega_{R_n D}} + \frac{1}{\Omega_{R_n E}} \right)^{-1} \} \end{aligned} \tag{6}$$

3.2 Traditional Source-Relay Selection algorithm

Similarly to the random selection algorithm, the traditional source-relay selection algorithm is chosen under the equal power transmission of each node. In order to reduce

the probability of eavesdropping in the transmission process, the traditional scheme selects the best source-relay pair for each communication to meet the maximum secrecy transmission rate, so (S_{m^*}, R_{n^*}) can be expressed as:

$$(S_{m^*}, R_{n^*}) = \arg\max \frac{1+\min(\gamma_{S_m R_n}, \gamma_{R_n D})}{1+\gamma_{R_n E}} \quad (7)$$

Combining Equations (3) and (5), when (S_{m^*}, R_{n^*}) is selected to participant in communication and the system SOP can be expressed as:

$$\begin{aligned} P_{\text{sec}}^{\text{out}} &= \Pr\left[\max_n \frac{\min(h_{S_{m^*}R_n}, h_{R_n D})}{h_{R_n E}} < g(R)\right] \\ &= \prod_{n=1}^{N} \underbrace{\Pr\left[\min(\max_m h_{S_m R_n}, h_{R_n D}) < g(R) h_{R_n E}\right]}_{\Phi} \end{aligned}$$

Let $U = \min(\max_m h_{S_m R_n}, h_{R_n D})$, the CDF of U can be derived as:

$$\begin{aligned} &\Pr(U<u) = \Pr\left[\min(\max_m h_{S_m R_n}, h_{R_n D}) < u\right] \\ &= 1 - \Pr(h_{R_n D} > u)\Pr\left(\max_m h_{S_m R_n} > u\right) \\ &= 1 - \exp\left(-\frac{u}{\Omega_{R_n D}}\right) \\ &\quad + \exp\left(-\frac{u}{\Omega_{R_n D}}\right) \prod_{m=1}^{M}\left[1-\exp\left(-\frac{u}{\Omega_{S_m R_n}}\right)\right] \end{aligned}$$

By polynomial theory, $\prod_{m=1}^{M}\left[1-\exp\left(-\frac{u}{\Omega_{S_m R_n}}\right)\right]$ can be expanded as:

$$\begin{aligned} &\prod_{m=1}^{M}\left[1-\exp\left(-\frac{u}{\Omega_{S_m R_n}}\right)\right] \\ &\quad = 1 + \sum_{m=1}^{2^M-1} (-1)^{|S_j|} \exp(-\sum_{m\in S_j} \frac{u}{\Omega_{S_m R_n}}). \end{aligned}$$

Where S_j represents the j-th non-empty collection, $|S_j|$ denotes the cardinality of set S_j. Substituting Equation (7) into (6), we can have Equation (8):

$$\begin{aligned} \Phi &= \int_0^{\infty} [1-\exp\left(-\frac{g(R)u}{\Omega_{R_n D}}\right) + \exp\left(-\frac{g(R)u}{\Omega_{R_n D}}\right) \\ &\quad \cdot \left(1 + \sum_{j=1}^{2^M-1} (-1)^{|S_j|} \exp(-\sum_{m\in S_j} \frac{g(R)u}{\Omega_{S_m R_n}}\right)] \\ &\quad \cdot f_{\gamma_{R_n E}}(u)\, du \\ &= 1 + \frac{1}{\Omega_{R_n E}} \sum_{j=1}^{2^M-1} (-1)^{|S_j|} \\ &\quad \cdot \left(\frac{g(R)}{\Omega_{R_n D}} + \frac{g(R)}{\Omega_{R_n E}} + \sum_{m\in S_j} \frac{g(R)}{\Omega_{S_m R_n}}\right)^{-1} \end{aligned} \quad (8)$$

3.3 Optimal Source-Relay Selection algorithm

The above two selection algorithms were designed by minimizing the system SOP in the case of equal power transmission for all nodes, which was a sub-optimal selection method with high computational complexity. In this section, we propose a lower complexity source-relay selection algorithm, which based on power allocation to search the optimal source and relay. That is, we obtain the power allocation factor of each link potential participation nodes firstly and then select the optimum source-relay (S_{m^*}, R_{n^*}).

3.3.1 Power Allocation Process

When $(S_m R_n)$ is selected to participate in cooperation communication, if the transmission power of the source node S_m is $\mu P_T (0<\mu<1)$, so the transmission power of the relay node R_n is $(1-\mu)P_T$. Thus the system SOP can be expressed as:

$$C_{(m,n)} = \frac{1+\min(\gamma_{S_m R_n}, \gamma_{R_n D})}{1+\gamma_{R_n E}}$$

When $\gamma_{S_m R_n} < \gamma_{R_n D}$, $C_{(m,n)} = \frac{1+\mu\gamma|h_{S_m R_n}|^2}{1+(1-\mu)\gamma|h_{R_n E}|^2}$. Because $\frac{\partial C_{(m,n)}}{\partial \mu}$ is true forever $C_{(m,n)}$ is a strictly monotone increasing function. We can enhance μ until $\gamma_{S_m R_n} = \gamma_{R_n D}$, the function $C_{(m,n)}$ can get the maximum value now.

When $\gamma_{S_m R_n} > \gamma_{R_n D}$, $C_{(m,n)} = \frac{1+(1-\mu)\gamma|h_{R_n D}|^2}{1+(1-\mu)\gamma|h_{R_n E}|^2}$.Thus $\frac{\partial C_{(m,n)}}{\partial \mu} = A(|h_{R_n E}|^2 - |h_{R_n D}|^2)$, the variable A is a factor greater than 0 in the formula. If $|h_{R_n D}|^2 > |h_{R_n E}|^2$, $C_{(m,n)}$ is a monotonically decreasing function. We can enhance μ until $\gamma_{S_m R_n} = \gamma_{R_n D}$, the function $C_{(m,n)}$ gets the maximum value now. If $|h_{R_n D}|^2 < |h_{R_n E}|^2$, no matter how we change μ, the system secrecy transmission rate is 0 because of $C_{(m,n)} < 1$.

To summarize, if the source-relay pair (S_m, R_n) is selected to participates in cooperative communication, the optimal power allocation of each transmission can be expressed as:

$$\gamma_{S_m R_n} = \gamma_{R_n D}, \texttt{that is } \mu = \frac{|h_{R_n D}|^2}{|h_{S_m R_n}|^2 + |h_{R_n D}|^2} \quad (9)$$

3.3.2 Optimal Source-Relay Selection Process

Substituting Equation (9) into (7), the optimal source-relay pair (S_{m^*}, R_{n^*}) is given in Equation (10):

$$\begin{aligned} &(S_{m^*}, R_{n^*}) = \\ &\arg\max_{m,n}\left\{\frac{1}{2}\log_2 \frac{1+\gamma|h_{S_m R_n}|^2|h_{R_n D}|^2/(h_{S_m R_n}|^2+|h_{R_n D}|^2)}{1+\gamma|h_{S_m R_n}|^2|h_{R_n E}|^2/(h_{S_m R_n}|^2+|h_{R_n D}|^2)}\right\} \end{aligned} \quad (10)$$

Combining Equations (5) and (10), when SNR is large

enough, the system SOP can be expressed as:

$$P_{\text{sec}}^{\text{out}} = \Pr\left[\max_{n}\left(|h_{R_nD}|^2/|h_{R_nE}|^2\right) < g(R)\right] = \prod_{n=1}^{N} \underbrace{\Pr\left(|h_{R_nD}|^2 < g(R)|h_{R_nE}|^2\right)}_{\Psi} \tag{11}$$

Where Ψ can be obtained as:

$$\Psi = \int_0^{\infty} \Pr\left[|h_{R_nD}|^2 < xg(R)\right] f_{h_{R_nE}}(x)dx = \frac{g(R)\Omega_{R_nE}}{\Omega_{R_nD} + g(R)\Omega_{R_nE}} \tag{12}$$

Therefore, when the source-relay pair (S_{m^*}, R_{n^*}) is selected and the system SOP of the proposed algorithm can be expressed as

$$P_{\text{sec}}^{\text{out}} = \prod_{i=1}^{N} \frac{g(R)\Omega_{R_nE}}{\Omega_{R_nD} + g(R)\Omega_{R_nE}} \tag{13}$$

In conclusion, when the number of source nodes is M and the number of relay nodes is N, the traditional selection algorithm need to compare the performance of the $M \cdot N$ links, and also need to calculate the integral polynomial multiplication with high computational complexity.

In our proposed algorithm, the optimal allocation factor among the source node and relay node of any link is obtained by power allocation and we can obtain the system SOP easily. It can be seen from Expression (13) that the SOP of the proposed scheme is independent function of the source node. The relay nodes can decode correctly by regulating the transmission power of source node and reduce the computational complexity to a great extent.

3.4 Numerical Results and Discussions

In this section, we analyze the SOP performance of the proposed source-relay selection algorithm by Monte-Carlo simulation, and compared it with the random selection and the traditional selection of two source-relay selection algorithms. In the simulations, we simulate a line network and assume that not only M source nodes but also N relay nodes are distributed in the same position respectively. The distance between the source and the destination is normalized to one, and all the relay nodes are located at the precise middle between the source and the destination. Therefore, the channel coefficient of any link follows the complex Gauss random distribution with zero-mean and variance d_{ij}^{-v}, where d_{ij} denotes the distance between any two nodes and stands for the path-loss factor. Here, we set $v = 4$ for an urban environment. The main-to-eavesdropper ratio was defined as the ratio of the main channel gain over the eavesdropper channel gain (*i.e.*, MER=$\Omega_{S_mR_n}/\Omega_{R_nE}$). In addition, the system target secrecy information rate is supposed as $R = 1\text{bit}/(s \cdot \text{Hz})$.

Figure 2 shows the theoretical value curves and the simulation values of the system SOP for different number

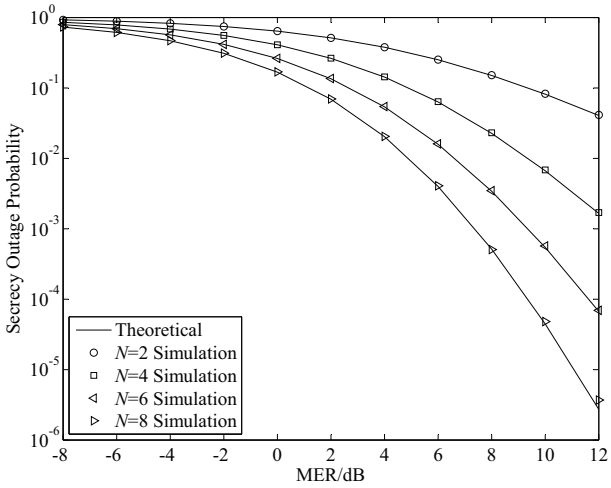

Figure 2: Theoretical values and simulation values of the secrecy outage probability with the different relays number

of candidate relays with the same source nodes number M=4. It can be seen from the figure, the theoretical value curve of the proposed algorithm are approximately coincidence with the simulation curve for the case of N=2, N=4, N=6 and N=8. Thus we prove the positive solution of the proposed algorithm. As well with the same number of nodes, the SOP of the four curves shows descend trend along with the increasing of MER. This is because the quality of the wiretap channel get worse compare with the main channel when increases, so the secrecy transmission rate is becoming larger. Therefore, in order to ensure the transmission more secure, one way is to move the eavesdroppers far away from the sources. Meanwhile, with the same channel condition, the more the number of candidate relays, the smaller the SOP.

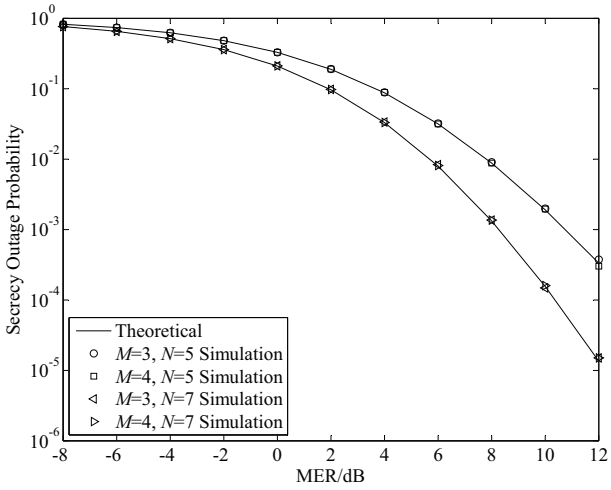

Figure 3: Comparison of the SOP under different channel conditions

Figure 3 gives the theoretical value curves and the simulation values of the system SOP when the number of source nodes and relay nodes is different. It can be seen

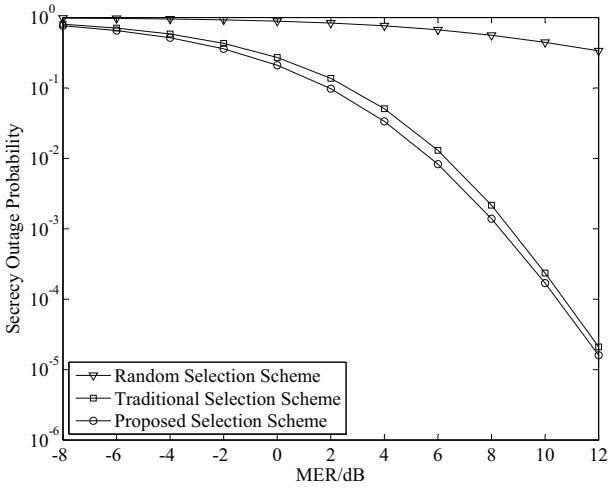

Figure 4: Comparison of secrecy outage probability between the different source-relay selection algorithms (M=4, N=5)

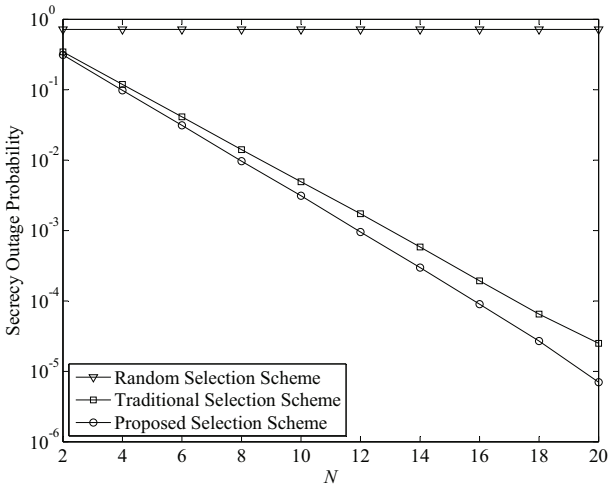

Figure 5: Comparison of secrecy outage probability between different schemes with the same candidate relay number (M=5, MER=5dB)

that the theoretical value curve of the proposed source-relay selection algorithm approximately coincides with the simulation curve when the number of candidate source nodes and relay nodes is constant. Thus the correctness of the proposed algorithm is further verified. At the same time, we can see that the system SOP decreases with the increasing of MER. When the number of relay nodes remain unchanged, the SOP of the algorithm are constant no matter how many the number of the candidate source nodes, which shows that the proposed selection algorithm related to the number of candidate relays but independent of the number of source nodes. This is because when the number of candidate relay nodes is fixed, we can adjust the power of each link in the proposed algorithm, and by calculating the system secrecy transmission rate is a function which independent of the source node channel.

Figure 4 illustrates the system SOP curves of the different source-relay selection algorithms under the same channel quality condition. We can see that the SOP of the three selection algorithms turn out descend trend with the increasing of MER. In the same channel condition, the random selection algorithm has the highest outage probability. However, the traditional selection algorithm chooses the source-relay with the highest security transfer rate to participate in cooperative communication under equal power allocation and the system SOP is significantly reduced compared with the random selection algorithm. The proposed scheme in this paper has the lowest outage probability, the optimal power allocation is firstly carried out for each link, and the source-relay pair is selected according to the quality of the main channel and the wiretap channel subsequently.

Figure 5 presents the system SOP curves of the different source-relay selection algorithms under the same candidate relays condition. We can see from the figure, when the number of source nodes is fixed, the SOP of the random selection algorithm is independent of the number of candidate relay nodes because the source nodes and relay nodes are distributed in the same position, which is linear. Meanwhile, the system SOP of the traditional scheme and the proposed scheme turn out descend trend with the increasing of candidate relay node N. In the same number of resource nodes and relay nodes, the random source-relay selection algorithm has the highest SOP, and the traditional selection algorithm is secondary. The SOP of the proposed scheme in this paper is the lowest.

4 Conclusions

In this paper, a new opportunistic source-relay selection algorithm is proposed for the multi-source multi-relay cooperative networks, which aims at minimizing the system SOP. We joint considering the CSI of the main channel and the wiretap channel. Firstly, the optimal power allocation factor for any link is obtained when the total transmitted power is limited, which is a function of the channel statistics .On the basis of this, the selection algorithm of the optimal source-relay is given and the closed-form expression of the system SOP is derived. The simulation results verify the proposed scheme has lower SOP performance compared with the traditional selection algorithm and reduce the computational complexity.

In addition, this work is assumed that there is no direct link between all source nodes and destination node. In the future work, we will continue to explore the physical layer security for the multi-source multi-relay networks with direct link.

Acknowledgments

This study was supported in part by National Natural Science Foundation of China (NO. 61461026), and Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (N0.

2014D13).The authors would like to thank the anonymous reviewers and the editors for their suggestions.

References

[1] T. Alam and M. Aljohani, "Design a new middleware for communication in Ad Hoc network of Android smart devices," in *International Conference on Information and Communication Technology for Competitive Strategies*, Dec. 2016. (https://www.researchgate.net/publication/307080049_Design_a_New_Middleware_for_Communication_in_Ad_Hoc_Network_of_Android_Smart_Devices)

[2] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection algorithms for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 12, pp. 6076-6085, 2013.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering (1st ed)*, 2011. (https://www.cambridge.org/core/books/physicallayer-security/543CF3D1431805B6AE04A7AA72903D09)

[4] W. F. Cao, Y. L. Zou, and Z. Yang, "Joint source-relay selection for improving wireless physical-layer security," in *Proceedings of The 59th IEEE Global Communications Conference (GLOBECOM'16)*, Dec. 2016. (https://ieeexplore.ieee.org/abstract/document/7841935)

[5] G. J. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the Full-Duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574-583, 2015.

[6] J. S. Chen, C. Y. Yang, and M. S. Hwang, "The capacity analysis in the secure cooperative communication system," *International Journal of Network Security*, vol. 19, no. 6, pp. 863-869, 2017.

[7] K. Emura, G. Hanaoka, Y. Sakai, and J. C. N. Schuldt, "Group signature implies public-key encryption with non-interactive opening," *International Journal of Information Security*, vol. 13, no. 1, pp. 51-62, 2014.

[8] L. S. Fan, X. F. Lei, T. Q. Duong, E. Maged, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3299-3310, 2014.

[9] V. Genc, S. Murphy, Y. Yu, and J. Murphy, "IEEE 802.16J relay-based wireless access networks: An overview," *IEEE Wireless Communications*, vol. 15, no. 5, pp. 56-63, 2008.

[10] S. I. Kim, I. M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3724-3737, 2015.

[11] X. F. Lei, L. S. Fan, R. Q. Hu, D. S. Michalopoulos, and P. Z. Fan, "Secure multiuser communications in multiple decode-and-forward relay networks with direct links," in *IEEE Global Communications Conference (GLOBECOM'14)*, pp. 3180-3185, Dec. 2014.

[12] V. S. Naresh, and N. V. E. S. Murthy, "Elliptic curve based dynamic contributory group key agreement protocol for secure group communication over Ad-hoc networks," *International Journal of Network Security*, vol. 17, no. 5, pp. 588-596, 2015.

[13] P. N. Son and H. Y. Kong, "Exact outage probability of a decode-and-forward scheme with best relay selection under physical layer security," *Wireless Personal Communications*, vol. 4, no. 2, pp. 325-342, 2014.

[14] L. Sun, T. Y. Zhang, L. Lu, and H. Niu, "On the combination of cooperative diversity and multiuser diversity in multi-source multi-relay wireless networks," *IEEE Signal Processing Letters*, vol. 17, no. 6, pp. 535-538, 2010.

[15] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Information Theory and Applications Workshop (ITA'07)*, pp. 404-413, Feb. 2007.

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

[17] Y. L. Zou, X. B. Wang, and W. M. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103-5113, 2013.

[18] Y. L. Zou, X. B. Wang, and W. M. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no.10, pp. 2099-2111, 2013.

Biography

Jianbin Xue is a professor and deputy dean of school of computer and communication, Lanzhou University of Technology, China. He received the B.S. degree in communication engineering from Sichuan University, in 1997. He received the M.S. degree and the Ph.D. degree both from Lanzhou University of Technology, Lanzhou, China, in 2005 and 2009, respectively. His main research interests include wireless communication theory and technology, wireless network theory and technology.

Heng Zhu received the B.S. degree in electronic and information engineering from Shihezi University, China, in 2010. He is currently pursuing his M.S. degree in the school of Computer and Communication, Lanzhou University of Technology. His research interests include cooperative communication and D2D communication.

Xiaoming Liao received the B.S. degree from Wuhan University of Science and Technology, in 2014. He is currently pursuing his M.S. degree in the school of Computer and Communication, Lanzhou University of Technology.

His main research interests is wireless heterogeneous network.

Zhe Su was born in Inner Mongolia Province, China, in 1993. He is currently pursuing his Ph.D. degree in the school of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics. His major is Communication and Information System.