Power Allocation in One-Way Untrusted AF Relay System with Friendly Jamming

Ronghua Luo[1(✉)], Chao Meng[1], Guobing Hu[2], and Hua Shi[1]

[1] School of Networks and Telecommunications Engineering in Jinling Institute of Technology, Nanjing, China
{lrh, mengchao, shihuawindy}@jit.edu.cn
[2] School of Electronical and Information Engineering in Jinling Institute of Technology, Nanjing, China
s0304152@jit.edu.cn

Abstract. In this paper, the physical layer security in one-way untrusted AF relay system is considered. For improving the physical layer security, external friendly jammers offer help through transmitting interference signal to the untrusted relay. It is indicated that a nonzero secrecy rate is achievable in one-way untrusted AF relay system with the help of friendly jammers. The source optimization problem is further formulated. In this optimization problem, in order to increasing the secrecy rate, the source must pay the jammers for exchanging their service of jamming. Finally, an optimal transmit power allocation of all the nodes is provided for the system. And simulation results verify the properties.

Keywords: Physical layer security · Secrecy rate · Friendly jammer
Source optimization problem · Power allocation

1 Introduction

Recently, physical layer based security attracting much attention due to the broadcasting nature of wireless communication. The theoretical foundation to study the secure communication at the physical layer is the wiretap channel and the information-theoretic notion of secrecy introduced by Wyner [1]. It has been proved that if the main channel condition is worse than the wiretap channel, the secrecy capacity will be zero [2], in order to overcoming this limitation, cooperative relaying [3, 4] and cooperative jamming [5, 6] has been proposed in wireless communication networks. And, physical layer security is also very important in 5G networks, such as ultra dense networks [7], LTE-U [8], and network slicing [9].

When the channel between the source and destination is worst, the relay node must be utilized to forward the information of source. However, in some cases, the relay node is untrusted. For example, the relay has a lower sense of security, and so, it does not trust the confidential messages it is relaying. How to communicate securely with the untrusted relay has been studied in [10, 11]. In [12], the destination can perform cooperative jamming, and which disable the untrusted relay from deciphering what it relaying. And recently, considering physical layer security in two-way untrusted relay

K. Long et al. (Eds.): 5GWN 2017, LNICST 211, pp. 589–596, 2018.
https://doi.org/10.1007/978-3-319-72823-0_54

system was also studied in [13]. In this paper, with the help of friendly jammers, the secrecy rate of the sources can be effectively improved.

In this paper, the physical layer security of AF untrusted one-way relay system with friendly jamming is investigated. Because there is no direct communication link between the source and the destination, an essential relay is needed, meanwhile, this relay is also a malicious eavesdropper. In [14], it is indicated that the secrecy rate is zero. Because that the untrusted relay can decipher the confidential message from the source. Therefore, the destination can only receive the signals from the untrusted relay who knows all the confidential message the destination knows. And then, it is impossible to make the source-destination pairs keeping secret from the untrusted relay. So, in this paper, we utilize the jammers as helpers that confusing the eavesdropping relay. After more analysis, it is indicated that a non-zero secrecy rate is indeed available by utilizing proper jamming power from the friendly jammers. The source optimization problem is further formulated. In the optimization problem, in order to improve the secrecy rate, the source must pay the jammers for interfering the malicious relay. The friendly jammers charge the sources with a certain price for their service of jamming. And the simulation results verify the properties.

The paper is organized as follows. Section 2 presents the channel model, two-phase protocol that utilizes cooperative jamming and the secrecy rate for the destination is defined. In Sect. 3, we formulate the source optimization problem and analyze the optimizing problem of physical layer security with jammers. In Sect. 4, simulation results are presented. And main conclusions are drawn in Sect. 5.

2 System Model

As shown in Fig. 1, we consider a one-way AF relay network consisting of one source node, one untrusted relay node, one destination and N friendly jammer nodes, which are denoted by S, R, D and FJ_i, $i = 1, 2, \ldots, N$, respectively. It is assumed that all nodes are half-duplex and there includes two phases, called phase one and phase two respectively. In phase one, the source transmits signal X_s with power p_s. At the same time, the jammer nodes transmit jamming signals X_{J_i} with $p_i^J, j = 1, 2, \ldots, N$ for confusing the relay node. We define the received signal at the relay in phase one as X_R

$$X_R = \sqrt{p_s} X_s h_{S,R} + \sum_{i=1}^{N} \sqrt{p_i^J} X_{J_i} h_{J_i,R} + Z_1 \tag{1}$$

Where Z_1 is an additive white Gaussian noise (AWGN), the mean is zero and variance is σ^2.

In phase two, the relay node amplifies and forward (AF) the received signal X_R with a factor β. And β is defined as

$$\beta = \left(p_s \left|h_{S,R}\right|^2 + \sum_{i=1}^{N} p_i^J \left|h_{J_i,R}\right|^2 + \sigma^2\right)^{-1/2} \tag{2}$$

The received signal at the destination in phase two is defined as Y_D, which is expressed as

$$Y_D = \beta\sqrt{p_r}X_R h_{R,D} + \sum_{i=1}^{N}\sqrt{p_i^J}X_{J_i}h_{J_i,D} + Z_2 \tag{3}$$

Where Z_2 is also an AWGN with zero-mean and variance of σ^2. Assuming that the signal X_{J_i} is known to the destination. After calculation, Y_D can be given as

$$Y_D = \beta\sqrt{p_s p_r}X_s h_{S,R}h_{R,D} + \beta\sqrt{p_r}h_{R,D}Z_1 + Z_2 \tag{4}$$

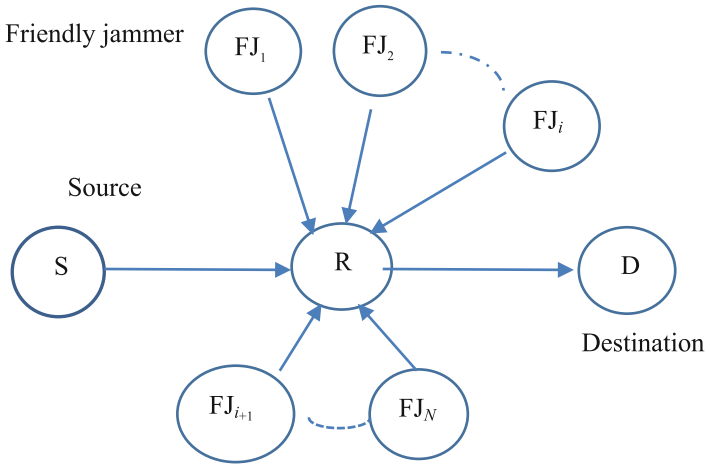

Fig. 1. System model of the one-way relay network

Then, the corresponding SINR (signal-to-interference-and-noise ratio) at the relay, defined as γ_R, can be given by

$$\gamma_R = \frac{p_s\left|h_{S,R}\right|^2}{\sigma^2 + \sum_{i=1}^{N}p_i^J\left|h_{J_i,R}\right|^2} \tag{5}$$

The corresponding SINR at the destination defined as γ_D, can be given by

$$\gamma_D = \frac{p_r p_s\left|h_{S,R}\right|^2\left|h_{R,D}\right|^2}{\sigma^2(p_s\left|h_{S,R}\right|^2 + \sum_{i=1}^{N}p_i^J\left|h_{J_i,R}\right|^2 + \sigma^2 + p_r\left|h_{R,D}\right|^2)} \tag{6}$$

And then, the untrusted relay node has the capacity as

$$C_R = \frac{W}{2}\log_2(1+\gamma_R) \tag{7}$$

The destination has the capacity as

$$C_D = \frac{W}{2}\log_2(1+\gamma_D) \tag{8}$$

Then, the secrecy rate for the destination can be defined as

$$C_D^s = (C_D - C_R)^+ \tag{9}$$

Where $(x)^+$ denotes $\max\{x, 0\}$.

3 Physical Layer Security with Jammers

From [14], we know that the secrecy rate of the destination is zero without friendly jammers. However, when using friendly jammers, these jammers can transmit interference signal to confuse the malicious relay, meanwhile, the interference signal is known for the destination. Then, a non-zero secrecy rate of the destination with the help of friendly jammers may be indeed available at some power vectors of (p_s, p_r, p_i^J). In this section, after further analyzing, it is found that the secrecy rate of the destination can be effectively improved through buying jamming power from the friendly jammers. And then, the problem comes to how to optimize the secrecy rate of the destination by allocating the jamming power from different friendly jammers.

From (7), (8) and (9), we have

$$C_D^s = \frac{W}{2}\left[\log_2\left(1+\frac{p_r p_s |h_{S,R}|^2 |h_{R,D}|^2}{\sigma^2(p_s|h_{S,R}|^2 + \sum_{i=1}^{N} p_i^J |h_{J_i,R}|^2 + \sigma^2 + p_r|h_{R,D}|^2)}\right) - \log_2\left(1+\frac{p_s|h_{S,R}|^2}{\sigma^2 + \sum_{i=1}^{N} p_i^J |h_{J_i,R}|^2}\right)\right]^+ \tag{10}$$

From (10), we can find that if $\frac{\sigma^2}{p_r|h_{R,D}|^2} < 1$, in some region of the jamming power p_i^J, the secrecy rate will be positive, which implies that the secrecy rate can be improved with friendly jammers' help compared to the secrecy rate without friendly jammers.

And $\frac{\partial C_D^s}{\partial p_r} > 0$ is always hold, which means that C_D^s is a monotonically increasing function of p_r. Thus, when $p_r = p_{\max}$, the secrecy rate C_D^s reaches the maximum, where $p_{\max}$ denotes the optimal relay power. In this paper, our main interested thing is how to

optimize the utility value of the source by allocating the jamming power, and meanwhile, all the nodes transmit with independent power, we can consider the source power p_s as a constant. If the source wants to improve the secrecy rate with the help of jammers, they must pay the cost to the jammers. So, in this paper, the utility function of the source is defined as

$$U_s = \alpha C_D^s - M \tag{11}$$

Where the constant $\alpha > 0$ is a factor that converts utility units to currency. M is the cost to pay for the jammers, which is defined as

$$M = \sum_{i=1}^{N} \lambda_i p_i^J \tag{12}$$

Where λ_i is the price per unit power charged by the friendly jammer *i.*

So, subject to the secrecy rate constraint and individual power constraint, the source optimization problem can be formulated as

$$\begin{array}{ll} \max & U_s = \alpha C_D^s - M \\ st. & C_D^s > 0 \\ & 0 \le p_i^J \le p_{\max}, fixed \quad p_r, p_s \end{array} \tag{13}$$

For maximizing the optimization problem, we can calculate the first derivative of U_s, we have

$$\begin{aligned} \frac{\partial U_s}{\partial p_i^J} = \frac{\alpha W}{2\ln 2}\Big[& \frac{A\left|h_{J_i,R}\right|^2}{(B+\sum_{i=1}^{N} p_i^J\left|h_{J_i,R}\right|^2 + A)(B+\sum_{i=1}^{N} p_i^J\left|h_{J_i,R}\right|^2)} \\ & - \frac{p_s\left|h_{S,R}\right|^2\left|h_{J_i,R}\right|^2}{(\sigma^2+\sum_{i=1}^{N} p_i^J\left|h_{J_i,R}\right|^2 + p_s\left|h_{S,R}\right|^2)(\sigma^2+\sum_{i=1}^{N} p_i^J\left|h_{J_i,R}\right|^2)}\Big] - \lambda_i \end{aligned} \tag{14}$$

Where $A = p_r p_s\left|h_{S,R}\right|^2\left|h_{R,D}\right|^2$, $B = p_s\left|h_{S,R}\right|^2 + p_r\left|h_{R,D}\right|^2 + \sigma^2$. When $\partial U_s/\partial p_i^J = 0$, we can obtain the forth-order polynomial equation as

$$\left(p_i^J\right)^4 + C_{i,3}\left(p_i^J\right)^3 + C_{i,2}\left(p_i^J\right)^2 + C_{i,1}p_i^J + C_{i,0} = 0 \tag{15}$$

Where $C_{i,n}, n = 0, 1, 2, 3$ are formulas of A, B, λ_i and p_i^J. Because that the solutions of the forth-order polynomial equation are very complex and not necessary for our following work, so our main interest is the parameters that affect these optimalsolutions. Then, the optimal power solutions of the friendly jammer i can be denoted as

$$p_i^{J^*} = p_i^{J^*}(A, B, \{P_j^J\}_{j \neq i}, \lambda_i) \tag{16}$$

Further, subject to the constraints, the optimal jamming power can be denoted as

$$p_{i\_opt}^J = \min(\max(p_i^{J^*}, 0), p_{\max}) \tag{17}$$

4 Simulation Results

The proposed scheme has been simulated numerically using MATLAB software. In the simulation, we consider a one-way AF relay network with one source, one relay, one destination which are located at (−1, 0), (0, 0) and (1, 0) respectively. The other parameters are defined as: $p_{\max} = 10$, the transmission bandwidth $W = 1$, the noise variance $\sigma^2 = 0.01$,the path loss factor is 2, and $\alpha = 1$.

When only one friendly jammer helps to the source, the two friendly jammer locations are considered as (0.3, 0.4) and (0.6, 0.8). In Fig. 2, the power of source is set up to $p_{\max} = 10$ and $\lambda = 0.1$, we can find that the utility of source can be maximized, when the jammers power is 2 and 4 respectively. And we can see, if the friendly jammer is close to the untrusted relay, the utility function can be improved more effectively. Figure 3 shows that the optimal jamming power is decreased with the asking price creasing, and it is foreseeable that the jamming power which buys from the jammer will be zero. So, when setting the price λ, a tradeoff must be considered for the friendly jammer.

In Fig. 4, two different scenarios are considered in simulations. On the one hand, there is no sufficiently effective friendly jammer, which implies that maximum secrecy rate cannot be achieved with the help of only one friendly jammer. And meanwhile, in this scenario, the secrecy rate increases with the number of friendly jammers. When the

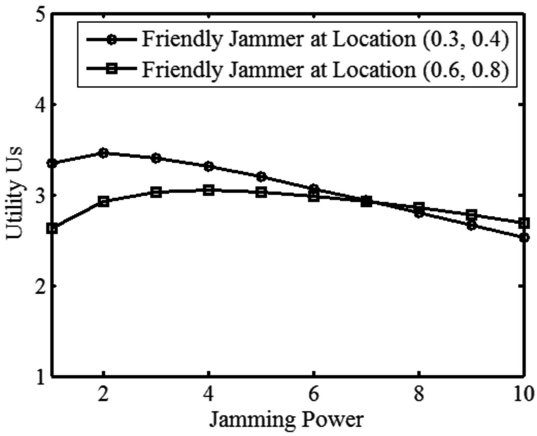

Fig. 2. The source's utility versus the jamming power

number of friendly jammers is 20, the secrecy rate can reach the maximum. However, on the other hand, when there is at least one sufficiently effective friendly jammer, which means that multiple friendly jammers can offer sufficiently effective help, we can see that the secrecy rate remains unchanged with the number of friendly jammers increasing.

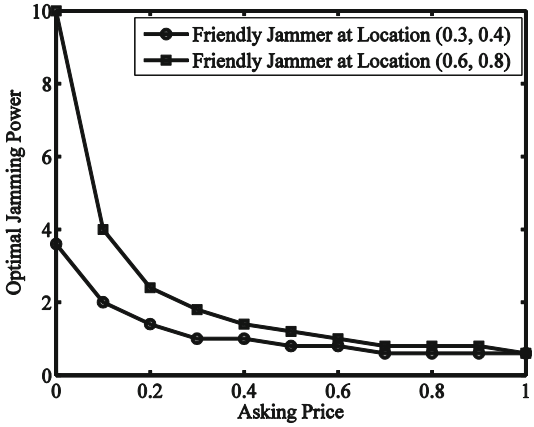

Fig. 3. The optimal jamming power versus asking price

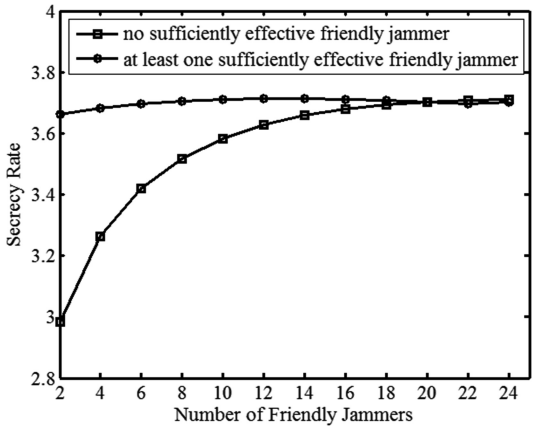

Fig. 4. Secrecy rate versus the number of friendly jammers

5 Conclusions

In this paper, we have investigated the one-way untrusted relay communications with friendly jammers. The source optimization problem is defined, and the optimal solution of jammer power is obtained. Simulation results show that the utility function of the

source can be improved with friendly jammers' help. And there exists a tradeoff for the price of jammers, otherwise, the source will not select the jammers as cooperators.

Acknowledgement. This work was supported by the Natural Science Foundation of Jiangsu Province (Grants No. BK20161104), The Scientific Research Fund Project of JIT (2016 incentive program, jit-2016-jlxm-24), the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (16KJB510011), the Doctoral Scientific Research Foundation of JIT (jit-b-201409, jit-b-201408, jit-b-201633) and Incubation Project of Science Foundation of JIT (jit-fhxm-201605).

References

1. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
2. Csiszar, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (1978)
3. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Amplify-and-forward based cooperation for secure wireless communications. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei, Taiwan, pp. 2613–2616. IEEE Press (2009)
4. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
5. Tekin, E., Yener, A.: The general gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming. IEEE Trans. Inf. Theory **54**(6), 2735–2751 (2008)
6. Zheng, G., Choo, L.-C., Wong, K.-K.: Optimal cooperative jamming to enhance physical layer security using relays. IEEE Trans. Signal Process. **59**(3), 1317–1322 (2011)
7. Zhang, H., Dong, Y., Cheng, J., Hossain, M., Leung, V.C.M.: Fronthauling for 5G LTE-U ultra dense cloud small cell networks. IEEE Wirel. Commun. **23**(6), 48–56 (2016)
8. Zhang, H., Chu, X., Guo, W., Wang, S.: Coexistence of Wi-Fi and heterogeneous small cell networks sharing unlicensed spectrum. IEEE Commun. Mag. **53**(3), 158–164 (2015)
9. Zhang, H., Liu, N., Chu, X., Long, K., Aghvami, A., Leung, V.: Network slicing based 5G and future mobile networks: mobility, resource management, and challenges. IEEE Commun. Magazine **55**(8), 138–145 (2017)
10. Oohama, Y.: Coding for relay channels with confidential messages. In: Proceedings of IEEE Information Theory Workshop, Caims, Australia, pp. 87–89. IEEE Press (2001)
11. Oohama, Y.: Capacity theorems for relay channels with confidential messages. In: Proceedings IEEE International Symposium Information Theory, Nice, France, pp. 926–930. IEEE Press (2007)
12. He, X., Yener, A.: Two-hop secure communication using an untrusted relay: a case for cooperative jamming. In: Proceedings of IEEE Global Communications Conference, New Orleans, LA, pp. 1–5. IEEE Press (2008)
13. Zhang, R., Song, L., Han, Z., Jiao, B., Debbah, M.: Physical layer security for two-way untrusted relaying with friendly jammers. IEEE Trans. Veh. Technol. **61**(8), 3693–3703 (2012)
14. He, X., Yener, A.: Cooperation with untrusted relay: a secrecy perspective. IEEE Trans. Inf. Theory **56**(8), 3807–3827 (2010)