Cooperative Jamming and Power Allocation in Three-Phase Two-Way Relaying System with Untrusty Relay Node

Hang Long[1], Wei Xiange[2], Xiaoli Zhang[1], Jing Wang[1], and Wenbo Wang[1]*

[1]Wireless Signal Processing and Network Lab, Key Laboratory of Universal Wireless Communication, Ministry of Education, Beijing University of Posts & Telecommunications, Beijing 100876 China

e-mail: lhrzrzlh@bupt.edu.cn

[2]Faculty of Engineering and Surveying, University of Southern Queensland, Toowoomba, QLD 4350, Australia

e-mail: Wei.Xiang@usq.edu.au

Abstract

This paper investigates the physical layer security issue of the three-phase two-way relaying system with an untrusty relay node. New cooperative jamming schemes are proposed for the three-phase bi-directional secrecy communications. The transmit power of each source node is divided into two parts corresponding to the user and jamming signals, respectively. The minimum jamming signal power at each source node is analyzed. An iterative power allocation algorithm is proposed for the three-phase protocol. Numerical results demonstrate the superiority of the proposed cooperative jamming scheme with power allocation.

1. Introduction

Recently, the attention to physical layer security techniques is increasing. In this area, cooperative jamming is a special technique, where artificial noise is introduced by a helpful interferer to confuse the eavesdropper [3-6]. In [3], the idea of cooperative jamming is proposed for the multiple-input single-output system, where additional artificial noise is introduced into the transmitted signal and a beamformer for the artificial noise is employed to avoid the interference at the legitimate receiver. In [4], a non-transmitting user is utilized as a cooperative jamming node to interfere with the eavesdropper and to increase the secrecy capacity.

Artificial jamming signals in cooperative jamming can be divided into four general categories [5-6]. Cooperative jamming schemes of the second category perform better than those of the first category since the jamming signal does not affect the performance of the legitimate receiver. Cooperative jamming in relay wiretap systems has been widely studied in the literature. However, the security of the two-way relaying system still remains an open problem. Cooperative jamming can also be utilized in the two-way relaying system. In [9], several cooperative jamming nodes with a payment price are introduced into the system to interfere with the untrusty relay node (eavesdropper node) in the multi-access phase. The problem of relay and jamming nodes selection in two-way relaying systems is investigated. Nearly all the work in the literature to date on cooperative jamming in two-way relaying systems [9] have been focusing on the scenario of external jamming nodes. Actually, cooperative jamming signals can be introduced without the use of external jamming nodes. The source nodes in the system can also transmit jamming signals to interfere with the eavesdropper [5], [6].

In this paper, a new cooperative jamming scheme is proposed to enhance the secrecy capacity of the two-way relaying system with an untrusty relay node (eavesdropper) without the use of external jammer nodes. The three-phase two-way relaying protocol is considered, where the two source nodes transmit the user and jamming signals alternatively. The minimum jamming signal power at each source node is derived. An iterative greedy algorithm is proposed for power allocation. Simulation results demonstrate that secrecy communications for the two-way relaying system are attainable with cooperative jamming.

2. System Model

A two-way relaying system is considered, where two source nodes (S_1 and S_2) and an untrusty relay node (R) are present. The bi-directional communications between S_1 and S_2 are aided by R, which also intercepts the source information transmitted from S_1 and S_2. That is, R is regarded as an eavesdropper (a.k.a. a wiretapper, E).

Block fading channels and the time-division duplex mode are assumed. The channels among the nodes are invariant during a complete transmission cycle. The channel coefficients of the S_1-R (R- S_1) and S_2-R (R- S_2) links are h_1 and h_2, respectively.

The overall transmit power constraints at S_1, S_2 and R are P_1, P_2 and P_R, respectively. Additive Gaussian noise at S_1, S_2 and R is assumed, and the noise variances are σ_{S1}^2, σ_{S2}^2 and σ_R^2, respectively. Without loss of generality, it is assumed in the sequel that $\sigma_{S1}^2 = \sigma_{S2}^2 = \sigma_R^2 = \sigma^2$ and $P_1 = P_2 = P_R = 1$. The average signal-to-noise ratios (SNRs) of the two links are defined as

$$\rho_1 = \mathcal{E}(|h_1|^2)/\sigma^2, \rho_2 = \mathcal{E}(|h_2|^2)/\sigma^2 \tag{1}$$

where $\mathcal{E}(\cdot)$ denotes mathematical expectation.

978-1-4673-5225-3/14/$31.00 ©2014 IEEE

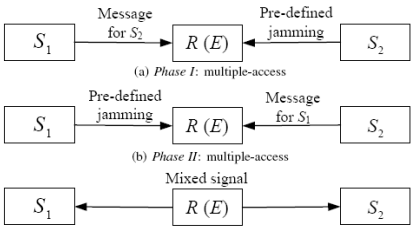

Fig. 1. Illustration of the three-phase protocol flow.

3. Cooperative Jamming and Power Allocation

In the three-phase protocol, the signals from S1 and S2 arrive at R in two separate phases. Hence, the equivalent SNR of a two-hop transmission (S1-R-S2 or vice versa) is potentially no greater than the SNR at R, which makes secrecy communications through R (E) virtually infeasible. Therefore, the system secrecy capacity without cooperative jamming is zero. As a consequence, the cooperative jamming technique in the three-phase protocol is necessary.

3.1 Three-phase two-way relaying with cooperative jamming

As illustrated in Fig. 1, the three-phase two-way relaying protocol with cooperative jamming can be summarized as follows:

Phase I: S1 transmits x_{S1} to R with the power allocation of $\mathcal{E}(|x_{S1}|^2) = P_{11}$. At the same time, S2 transmits I2 to R with the power allocation of $\mathcal{E}(|I_2|^2) = P_{21}$. The received signal at R is

$$y_{R_1} = h_1 x_{S1} + h_2 I_2 + n_{R1} \tag{2}$$

Phase II: S2 transmits x_{S2} to R with the power allocation of $\mathcal{E}(|x_{S2}|^2) = P_{22}$. S1 transmits I1 to R with the power allocation of $\mathcal{E}(|I_1|^2) = P_{12}$ simultaneously. The received signal at R is

$$y_{R_2} = h_1 I_1 + h_2 x_{S2} + n_{R2} \tag{3}$$

Phase III: R combines the received signals in Phases I and II and broadcasts them to S1 and S2 with the amplify-and-forward (AF) protocol

$$x_R = \beta(y_{R_1} + y_{R_2}) \tag{4}$$

The received signals at $\mathcal{S}1$ and $\mathcal{S}2$ are

$$y_{S1} = h_1 x_R + n_{S1} \tag{5}$$

and

$$y_{S2} = h_2 x_R + n_{S2} \tag{6}$$

respectively.

3.2 Power Allocation

As defined in Section II, the overall transmit power constraints at S1 and S2 in the first two phases are P1 = P11+P12 and P2 = P21 + P22, respectively. The transmit power at each source node is divided into two parts corresponding to information transmission and jamming. Note that if P12 = 0 and P21 = 0 (P11 = P1 and P22 = P2), the system degrades to the conventional three-phase two-way relaying system without cooperative jamming, which can not achieve a positive secrecy capacity.

Substituting (2) and (3) into (4), we arrive at

$$\beta^{-2} = |h_1|^2 + |h_2|^2 + 2\sigma^2 \tag{7}$$

Integrating (2)-(4) into (5), the received signal at $\mathcal{S}1$ can be rewritten as

$$y_{S1} = \beta h_1^2 x_{S1} + h_1 \beta h_2 I_2 + h_1 \beta n_{R1} + \beta h_1^2 I_1 + h_1 \beta h_2 x_{S2} + h_1 \beta n_{R2} + n_{S1} \tag{8}$$

It is assumed that xS1, I1 and I2 are all a priori known at S1 and can thus be canceled out with an SIC receiver. After the SIC receiver, the received SNR at S1 is given by

$$\gamma_{21} = a_2 P_{22}, a_2 = \frac{\beta^2 |h_1 h_2|^2}{(2\beta^2 |h_1|^2 + 1)\sigma^2} \tag{9}$$

According to (3), the received signal-to=interference-and-noise ratio (SINR) at $\mathcal{R}$ with respect to $x_{\mathcal{S}2}$ is

$$\gamma_{2E} = \frac{P_{22}}{cP_{12} + b_2}, b_2 = \frac{\sigma^2}{|h_2|^2}, c = \frac{|h_1|^2}{|h_2|^2} \tag{10}$$

Similarly, the received SNR at $\mathcal{S}2$ can be written as

$$\gamma_{12} = a_1 P_{11}, a_1 = \frac{\beta^2 |h_2 h_1|^2}{(2\beta^2 |h_2|^2 + 1)\sigma^2} \tag{11}$$

The received SINR at R with respect to xS1 is

$$\gamma_{1E} = \frac{P_{11}}{\frac{1}{c} P_{21} + b_1}, b_1 = \frac{\sigma^2}{|h_1|^2} \tag{12}$$

The secrecy capacity of the two-way relaying wiretap system is defined as

$$R_S = (R_{S12} + R_{S21}) / 3 \tag{13}$$

where

$$R_{S12} = \left[\log_2(1+\gamma_{12}) - \log_2(1+\gamma_{1E})\right]^{\dagger} \tag{14}$$

and

$$R_{S21} = \left[\log_2(1+\gamma_{21}) - \log_2(1+\gamma_{2E})\right]^{\dagger} \tag{15}$$

are related to the S1-S2 and S2-S1 links, respectively. Note that $x^{\dagger}$ denotes max(x, 0).

It is notable that the SINRs at E are also treated as the SNR in the secrecy capacity defined in (13)-(15), which is a common treatment if the interference is assumed to be Gaussian and independent to the user signals.

As can be seen from (7), $\beta^2 |h_1|^2 < 1$ and $\beta^2 |h_2|^2 < 1$. We then have

$$a_1 b_1 = \frac{\beta^2 |h_2|^2}{2\beta^2 |h_2|^2 + 1} < \frac{1}{3}, a_2 b_2 < \frac{1}{3} \tag{16}$$

If the cooperative jamming scheme is not used, namely, P12 = 0 and P21 = 0, we have

$$\frac{1+\gamma_{12}}{1+\gamma_{1E}} = \frac{b_1 + a_1 b_1}{b_1 + 1} < 1, \frac{1+\gamma_{21}}{1+\gamma_{2E}} < 1 \tag{17}$$

This suggests that secrecy communications are impossible without cooperative jamming. Hence, a small amount of jamming signal power should be adopted at each source node. We take the S2-S1 link as an example. The jamming signal power P12 should guarantee that

$$\gamma_{21} > \gamma_{2E} \Leftrightarrow a_2 P_{22} > \frac{P_{22}}{cP_{12} + b_2} \Leftrightarrow P_{12} > \frac{1}{a_2 c} - \frac{b_2}{c} = \frac{(\beta^2 |h_1|^2 + 1)\sigma^2}{\beta^2 |h_1|^4} = P_{I1,\text{th}} \tag{18}$$

If $|h_1|^2$ is small, the minimum jamming power at S1 ($P_{I1,\text{th}}$) calculated by (18) might be larger than P1, so that secrecy communications from S2 to S1 are impossible. Fortunately, if the channel of the S1-R link is good enough, $P_{I1,\text{th}} \to 0$. Similarly, the minimum jamming power at S2 is given by

$$P_{I2,\text{th}} = \frac{(\beta^2 |h_2|^2 + 1)\sigma^2}{\beta^2 |h_2|^4} \tag{19}$$

According to the values of $P_{I1,\text{th}}$ and $P_{I2,\text{th}}$, we can discuss the problem of power allocation as follows:

If $P_{I1,\text{th}} \geq 1$ and $P_{I2,\text{th}} \geq 1$, secrecy communications between S1 and S2 are impossible and RS = 0;

If $P_{I1,\text{th}} \geq 1$ and $P_{I2,\text{th}} < 1$, we have $\gamma_{21} < \gamma_{2E}$ and RS21 = 0. Hence, secure communications from S2 to S1 are impossible and all the available transmit power at the two source nodes should be allocated to the S1-S2 link, i.e., P11 = 1, P12 = 0, P21 = 1, and P22 = 0. Similar conclusions can be made for the case of $P_{I1,\text{th}} < 1$ and $P_{I2,\text{th}} \geq 1$; and

If $P_{I1,\text{th}} < 1$ and $P_{I2,\text{th}} < 1$, the optimum power allocation ensuring the minimum jamming power at S_1 and S_2 can be achieved alternatively by

$$\{P_{11'}, P_{22'}\} = \underset{0 \leq P_{11} \leq 1 - P_{I1,\text{th}}, 0 \leq P_{22} \leq 1 - P_{I2,\text{th}}}{\arg\max} f(P_{11}, P_{22}) g(P_{11}, P_{22}) \tag{20}$$

where

$$f(P_{11}, P_{22}) = \frac{1+\gamma_{12}}{1+\gamma_{1E}}, g(P_{11}, P_{22}) = \frac{1+\gamma_{21}}{1+\gamma_{2E}} \tag{21}$$

If $P_{11}' = 1 - P_{I1,\text{th}}$ ($P_{22}' = 1 - P_{I2,\text{th}}$), the optimum power allocation is the same as in the second case discussed earlier. Otherwise, P_{11}' and P_{22}' achieved with (20) are globally optimum.

The objective function of (20) is a convex function of P11 and P22 which will be revealed in the sequel. A greedy power allocation algorithm is proposed in the next subsection to solve the optimization problem of (20), which is able to approximately achieve the solution.

We can analyze f(P11, P22) and the analysis can be directly extended to g(P11, P22). It is easy to show that $f(P_{11}, P_{22})$ is a convex function of P_{11} only if $a_1(1-P_{22})/c + a_1 b_1 > 1$. This requirement is the same as that of the minimum jammin P_{22} in the intervals of $0 \le P_{11} \le 1 - P_{I1,\text{th}}$ and $0 \le P_{22} \le 1 - P_{I2,\text{th}}$.

4. Simulation Results

The proposed cooperative jamming scheme with the greedy power allocation algorithm is evaluated, which is denoted by "Greedy PA" in the following figures. Two baseline schemes are adopted for comparison: 1) the power at each source node is equally divided between the user and jamming signals, i.e., P11 = P12 = 0.5 and P21 = P22 = 0.5, which is denoted by "Equal PA"; and 2) the selective uni-directional transmission (SUDT) scheme, where the powers of the two source nodes are all allocated to one of the two uni-directional links with a larger secrecy capacity, i.e., the secrecy capacity is max[RS(1, 0), RS(0, 1)].

Fig. 2 plots the secrecy capacity results when $\rho_1 = \rho_2 = \rho$. The curves of the two baseline schemes intersect around $\rho = 12$ dB. However, the proposed cooperative jamming scheme always outperforms the two baseline schemes over the entire range of the average SNR. When the channels are both in very poor condition, secrecy bi-directional communications cannot be attained, and all the power should be allocated to only one direction. Hence, the proposed cooperative jamming and SUDT schemes perform similarly when ½ is very small. However, if the channels are in good conditions, secrecy bidirectional communications are possible, and the equal power allocation scheme outperforms SUDT and performs close to the proposed cooperative jamming scheme with power allocation.

The results when ρ_1 is fixed are given in Figs. 3 and 4. If the S1-R link is poor (e.g., the assumption of Fig. 3), the gain in ρ_2 given by the proposed cooperative jamming scheme with power allocation is about 1 dB over SUDT. In Fig. 4, when the channels are in good conditions, the gain is more evident and larger than 4 dB.

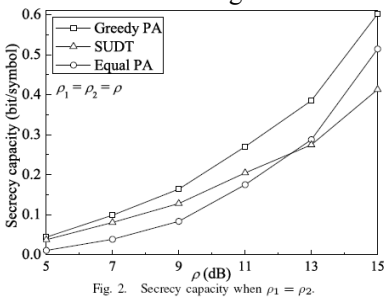

Fig. 2. Secrecy capacity when $\rho_1 = \rho_2$.

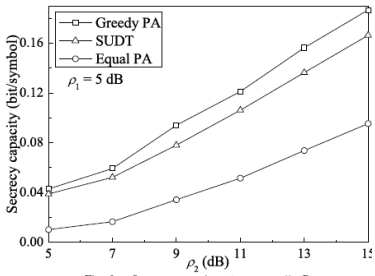

Fig. 3. Secrecy capacity when $\rho_1 = 5$ dB.

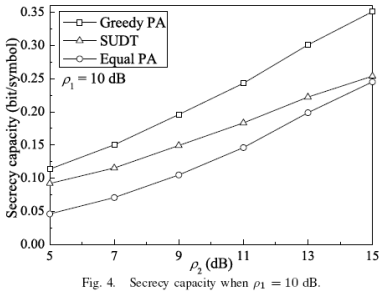

Fig. 4. Secrecy capacity when $\rho_1 = 10$ dB.

5. Conclusion

In this paper, we have investigated the cooperative jamming in the three-phase two-way relaying system with an untrusty relay node. Pre-defined jamming signals are introduced at the source nodes to interfere with the untrusty relay node. The power allocation between the user and jamming signals at the source nodes is analyzed. Simulation results suggest that the secrecy capacity gain achieved by the proposed cooperative jamming scheme is more evident if the links are in good condition.

6. References

2. H. Long, W. Xiang, Y. Zhang, et al., "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 229-238, Jan. 2013.

3. R. Negi and S. Goel, "Secret communications using artificial noise," in Proc. IEEE Vehicular Technology Conference (VTC), Dallas, TX, Sept. 2005, pp. 1906-1910.

4. E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in Proc. Allerton Conference on Communication, Control, and Computing (ACCCC), Monticello, IL, Sep. 2006, pp. 1-8.

5. H. Long, W. Xiang, J. Wang, et al., "Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems," in Proc. IEEE Wireless Communications and Networking Conference (WCNC) 2013, Shanghai, China, pp. 4216-4220, Apr. 2013.

6. H. Long, W. Xiang, J. Wang, et al., "Cooperative jamming and power allocation in two-way relaying system with eavesdropper," in Proc. IEEE Vehicular Technology Conference (VTC) 2013 fall, Las Vegas, Nevada, USA, Sep. 2013, pp. 1-5.

9. R. Zhang, L. Song, Z. Han, et al., "Physical layer security for two way relay communications with friendly jammers," in Proc. IEEE Globecom 2010, Miami, Florida, Dec. 2010, pp. 1-6.