International Journal of Future Generation Communication and Networking
Vol. 9, No. 12 (2016), pp. 87-96
http://dx.doi.org/10.14257/ijfgcn.2016.9.12.08

Three-phase Cooperative Jamming Based Improving PHY Security for Multicast Network with an Untrusted Relay

Xingqun Fu[1], An Li[1,*], Panagiotis G Sarigiannidis[2]

[1]*Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China*
[2]*Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani 50100, Greece*

Abstract

In this paper, a multicast network in the presence of an untrusted relay is investigated. A three-phase AF-based cooperative jamming with power allocation is proposed to enhance the system secrecy rate. Based on time division based cooperative multicast (TDCM) protocol, the source uses part of its available power to broadcast pre-defined jamming signals in order to create interference at the untrusted relay, while the relay amplifies the linearly combined two received signals and then re-transmits it to the destination. Optimum power allocation policy involving the allocation between the information and jamming signals at the source and between two combined signal factors at the relay to maximize the achievable worse secrecy rate or sum-rate are derived and analyzed. Numerical results are provided to demonstrate our analytical results and reveal that compared with the two benchmarks schemes, the proposed scheme can obtain significantly higher positive secrecy rate for the same transmit power budget, especially in the case of maximizing secrecy sum-rate.

Keywords*: physical-layer security, multicast network, cooperative jamming, TDCM, power allocation*

1. Introduction

In recent years, with the rapid development of wireless communication technology and the coexistence of various networks, users have an increasing requirement not only for the transmission performance of wireless communication systems, but also for the security of wireless communication. Traditional communication security is achieved mainly by the authentication of the upper communication protocol stack and encryption algorithms such as AES, DES, and NTRUE [1] which are highly complex mathematical calculations. Meanwhile, since the next-generation communications networks such as cognitive radio networks, sensor networks use a lot of miniature nodes with power constraints and decentralized nature, the traditional encryption algorithms are not applicable to these networks [2]. Pioneered by Wyner's work [3], which introduced the wire-tap channel and shows that almost perfectly secure communication can take place without relying on private keys only if Alice-Bob channel is better than Alice-Eve channel, physical (PHY) layer security has been identified as a promising approach to provide secure communication by exploiting the imperfections of wireless channel.

Unfortunately, there is no guarantee that Alice will have better channel than the Eve in the practical communication scenario, therefore, the key of physical layer security is to create channel advantage for Alice. Cooperative jamming is a popular PHY layer security transmission technique by introducing the artificial jamming signals to confuse the

* Corresponding author (lian@ncu.edu.cn)

ISSN: 2233-7857 IJFGCN

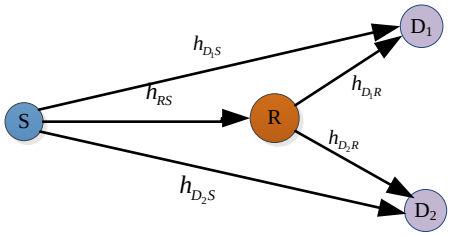
eavesdropper [4-8]. Common to [4-8] is that all of them assume the relays are trusted while being eavesdropped by an external entity. However, one may also need to prevent the confident signal from the relay itself when forwarded to the destination, which means the relay acts as an eavesdropper even if it helps to forward the useful signals. He firstly presented a destination-aided jamming strategy by using an untrusted compress-and-forward relay node to retransmit information to achieve the non-zero secrecy rate [9]. Later a few attempts have been made very recently to study untrusted relay channels [10-14]. Specifically, [10] and [11] investigated the secrecy outage probability performance with the help of an untrusted relay by using friendly noise as jamming signal for the relay. The authors in [12] studied joint the relay selection and transmit design problem for an untrusted relay network with the help of cooperative jamming from the destination. In [13], the achievable secrecy rate region for *K*-user multiple access channel with untrusted relay without source-destination link. An alternate jamming and security-enhanced relay selection policy is studied to prevent the confidential message from being eavesdropped by the untrusted relays in [14].

The aforementioned works have focuses on the secure communication for the unicast network, multicast has been an elementary service in many group communications such as information gathering in wireless sensor network, event notification systems, resource discovery, one-to many content deliveries in P2P network, and cellular phone-based teleconference, etc. A few attempts have been made very recently to study secret communication in multicast networks [15-17]. The authors in [15] considered SIMO multicast systems with external multiple eavesdroppers and developed closed-form expressions for positive secrecy. The outage performance of SIMO multicast scenarios was analyzed in [16]. A cooperative transmission which divided the multicast scenario into two cooperative unicast transmissions at two phases by enlisting the help of two destinations each other to jam the eavesdropper in turn was proposed in [17].

From these existing literature, one can find that secure communication problem in single-antenna multicast system with the untrusted relay has not been considered yet. In this paper, we investigate physical layer security in single-antenna multicast relay system, where the source broadcasts confidential message to two destinations through an untrusted relay. The relay acts as both a friendly helper and a potential passive eavesdropper. Based on time division, a three-phase AF joint power allocation and cooperative jamming scheme is presented. Without employing external jamming nodes, the source also transmits jamming signals as well information to interfere the untrusted relay, and the relay combines the received signals at two phases to broadcast the two destinations. In particular, we formulate and analyze the optimal power allocation problems to maximize the achievable worse secrecy rate or secrecy sum-rate subject to the source and relay power constraints. Furthermore, two benchmark schemes for the purpose of performance comparison are discussed.

2. System Model and Protocol Design

Consider a wireless multicast scenario with a source (S), an untrusted relay (R) and two destinations (D_1 and D_2), as shown in Figure 1. We assume that each node is equipped with only one antenna and operates in half-duplex mode. The three-phase time division based cooperative multicast (TDCM) protocol is employed as depicted in Figure 2. For a time period *T*, the first two *T*/3 parts are assigned for S to broadcast information-bearing signal X_1 and X_2 with power P_i, both the destination D_1, D_2 and R can hear the signal. The remaining *T*/3 duration is used for R to broadcast the combination of two signals it received.



1st Phase $T/3$	2nd Phase $T/3$	3rd Phase $T/3$
S Broadcast X_1	S Broadcast X_2	R Broadcast X_R

Figure 1. Illustration of System Model Figure 2. Three-phase TDCM Protocol

Let h_{D_1S}, h_{D_2S}, h_{RS}, h_{D_1R}, h_{D_2R} denote the complex channel coefficient of the channel from D_1 to S, D_2 to S, R to S, D_1 to R, and D_2 to R respectively. Assuming that all the channels are subject to Rayleigh fading and modeled as follows: $h_{D_1S} \sim \mathcal{CN}(0, \Omega_{D_1S})$, $h_{D_2S} \sim \mathcal{CN}(0, \Omega_{D_2S})$, $h_{D_1R} \sim \mathcal{CN}(0, \Omega_{D_1R})$, $h_{D_2R} \sim \mathcal{CN}(0, \Omega_{D_2R})$ and $h_{RS} \sim \mathcal{CN}(0, \Omega_{RS})$, where $\Omega_{D_1S} = d_{D_1S}^{-m}$, $\Omega_{D_2S} = d_{D_2S}^{-m}$, $\Omega_{RS} = d_{RS}^{-m}$, $\Omega_{D_1R} = d_{D_1R}^{-m}$ and $\Omega_{D_2R} = d_{D_2R}^{-m}$, d_{ij} is the Euclidean distance between node i ($i \in D_1, D_2, R$) and j ($j \in S, R, i \neq j$), and m is the path loss exponent.

To prevent the untrusted relay from eavesdropping the transmitted information, based on the TDCM protocol illustrated in Figure 2, we propose a three-phase AF joint power allocation and cooperative jamming scheme by employing the space diversity and artificial noise to maximize the achievable worse secrecy rate or the secrecy sum-rate. Note that the global channel state information is assumed to be available. Let $0 \leq \alpha_i \leq 1$ denote the power allocation factor, so that $\alpha_i P_i$ part is assigned for S to transmit the information while the remaining part $(1-\alpha_i)P_i$ is used for the pre-defined artificial jamming signal $\mathcal{Z}_i$, which is a priori known at D_1 and D_2 but are unknown at R. The jamming signal can be completely eliminated at each destination with a SIC receiver, therefore, cooperative jamming just reduces the eavesdropper's SNR but doesn't causes any harm to destinations' performance.

Phase 1: S broadcasts the signal X_{S1} as follows

$$X_{S1} = \sqrt{\alpha_1 P_1} X_1 + \sqrt{(1-\alpha_1)P_1}\mathcal{Z}_1 \quad (1)$$

Then the received signals Y_i at R, D_1 and D_2 are given as follows, respectively

$$Y_{R1} = X_{S1} h_{RS} + n_{R1} = \left(\sqrt{\alpha_1 P_1} X_1 + \sqrt{(1-\alpha_1)P_1}\mathcal{Z}_1\right) h_{RS} + n_{R1} \quad (2)$$

$$Y_{D1} = X_{S1} h_{D_1S} + n_{D1} = \sqrt{\alpha_1 P_1} X_1 h_{D_1S} + n_{D1} \quad (3)$$

$$Y_{D2} = X_{S1} h_{D_2S} + n_{D2} = \sqrt{\alpha_1 P_1} X_1 h_{D_2S} + n_{D2} \quad (4)$$

Phase 2: Similar to Phase 1, S transmits the information X_2 for D_2 and the jamming signal $\mathcal{Z}_2$ with the power allocation of $\alpha_2 P_2$ and $(1-\alpha_2)P_2$ respectively to R and D_i ($i \in 1, 2$). Thus the received signals at the untrusted relay, the destination D_1 and D_2 are

$$Y_{R2} = \left(\sqrt{\alpha_2 P_2} X_2 + \sqrt{(1-\alpha_2)P_2}\mathcal{Z}\right) h_{RS} + n_{R2} \quad (5)$$

$$Y'_{D1} = \sqrt{\alpha_2 P_2} X_2 h_{D_1S} + n'_{D1} \quad (6)$$

$$Y'_{D2} = \sqrt{\alpha_2 P_2} X_2 h_{D_2S} + n'_{D2} \quad (7)$$

Phase 3: R firstly combines the received signals Y_{R1} and Y_{R2} as X_R, and then uses the power P_R to broadcast to D_1 and D_2 as follows.

$$X_R = \xi_1 Y_{R1} + \xi_2 Y_{R2} \quad (8)$$

where $\xi_i (i = 1, 2)$ is a normalization factor to satisfy the power constraint, i.e.

$$\xi_i = \sqrt{\frac{\theta_i}{P_i |h_{RS}|^2 + 1}} \quad (9)$$

where $0 < \theta_i < 1$, and $\theta_1 + \theta_2 = 1$. When signal to noise ratio (SNR) $P_i |h_{RS}|^2$ is high,

$\xi_i \approx \sqrt{\frac{\theta_i}{P_i|h_{\mathrm{RS}}|^2}}$. Therefore, the received signals at D_1 and D_2 are

$$Y''_{\mathrm{D}1} = \sqrt{P_{\mathrm{R}}}h_{\mathrm{D}_1\mathrm{R}}\mathrm{X}_R + n''_{\mathrm{D}1}$$
$$= \sqrt{P_{\mathrm{R}}}h_{\mathrm{D}_1\mathrm{R}}\xi_1\sqrt{\alpha_1 P_1}X_1 h_{\mathrm{RS}} + \sqrt{P_{\mathrm{R}}}h_{\mathrm{D}_1\mathrm{R}}\xi_1 n_{\mathrm{R}1} + \sqrt{P_{\mathrm{R}}}h_{\mathrm{D}_1\mathrm{R}}\xi_2 n_{\mathrm{R}2} + n''_{\mathrm{D}1} \quad (10)$$
$$Y''_{\mathrm{D}2} = \sqrt{P_{\mathrm{R}}}h_{\mathrm{D}_2\mathrm{R}}\xi_2 h_{\mathrm{RS}}\sqrt{\alpha_2 P_2}X_2 + \sqrt{P_{\mathrm{R}}}h_{\mathrm{D}_2\mathrm{R}}\left(\xi_1 n_{\mathrm{R}1} + \xi_2 n_{\mathrm{R}2}\right) + n''_{\mathrm{D}2} \quad (11)$$

Note that since D_1 receives X_2 at Phase 2 and has an apriori knowledge of the jamming signal Z_1, all the interference signals have been cancelled off in (10), so is the same in (11). In (1) –(11), n_i are AWGN at R, D_1 and D_2 with $n_{\mathrm{R}}\sim\mathcal{CN}(0,\ 1)$, $n_{\mathrm{D}1}\sim\mathcal{CN}(0,\ 1)$, $n_{\mathrm{D}2}\sim\mathcal{CN}(0,\ 1)$, $n_{\mathrm{R}2}\sim\mathcal{CN}(0,\ 1)$, $n'_{\mathrm{D}1}\sim\mathcal{CN}(0,\ 1$, $n'_{\mathrm{D}2}\sim\mathcal{CN}(0,\ 1)$, $n''_{\mathrm{D}1}\sim\mathcal{CN}(0,\ 1)$ and $n''_{\mathrm{D}2}\sim\mathcal{CN}(0,\ 1)$.

3. Power Allocation for Achievable Secrecy Rate Maximization

In this section, the secrecy rate is derived and the optimal power allocation policy to maximize the achievable worse secrecy rate or secrecy sum-rate is discussed.

Since D_1 and D_2 receive the intended signals during two phases, Maximal Ratio Combining (MRC) is considered as the combining method, the information rate at D_1 and D_2 can be written as, respectively

$$I_{\mathrm{D}1} = \frac{2}{3}\log_2\left(1 + \alpha_1 P_1\left|h_{\mathrm{D}_1\mathrm{S}}\right|^2 + \frac{P_{\mathrm{R}}\left|h_{\mathrm{D}_1\mathrm{R}}\right|^2\xi_1^2\alpha_1 P_1|h_{\mathrm{RS}}|^2}{P_{\mathrm{R}}\left|h_{\mathrm{D}_1\mathrm{R}}\right|^2(\xi_1^2+\xi_2^2)+1}\right) \quad (12)$$

$$I_{\mathrm{D}2} = \frac{2}{3}\log_2\left(1 + \alpha_2 P_2\left|h_{\mathrm{D}_2\mathrm{S}}\right|^2 + \frac{P_{\mathrm{R}}\left|h_{\mathrm{D}_2\mathrm{R}}\right|^2\xi_2^2\alpha_2 P_2|h_{\mathrm{RS}}|^2}{P_{\mathrm{R}}\left|h_{\mathrm{D}_2\mathrm{R}}\right|^2(\xi_1^2+\xi_2^2)+1}\right) \quad (13)$$

The rates leaked to the untrusted relay R with respect to X_1 and X_2 are given as follows, respectively

$$I_R^1 = \frac{1}{3}\log_2(1 + \frac{\alpha_1 P_1|h_{\mathrm{RS}}|^2}{(1-\alpha_1)\ P_1|h_{\mathrm{RS}}|^2+1}) \quad (14)$$

$$I_R^2 = \frac{1}{3}\log_2(1 + \frac{\alpha_2 P_2|h_{\mathrm{RS}}|^2}{(1-\alpha_2)\ P_2|h_{\mathrm{RS}}|^2+1}) \quad (15)$$

Thus the achievable secrecy rate from S to D_1 can be easily calculated as

$$R_{\mathrm{D}_1\mathrm{S}}^{\mathrm{sec}} = [\frac{2}{3}\log_2(1+\alpha_1 P_1 |\, h_{\mathrm{D}_1\mathrm{S}}\,|^2 + \frac{P_{\mathrm{R}}\,|\,h_{\mathrm{D}_1\mathrm{R}}\,|^2|\,h_{\mathrm{RS}}\,|^2\,\alpha_1\theta_1 P_1}{P_{\mathrm{R}}\left|h_{\mathrm{D}_1\mathrm{R}}\right|^2 + P_1\,|\,h_{\mathrm{RS}}\,|^2}) - \frac{1}{3}\log_2(1+\frac{\alpha_1 P_1\left|h_{\mathrm{RS}}\right|^2}{(1-\alpha_1)\ P_1\left|h_{\mathrm{RS}}\right|^2+1})]^+ \quad (16)$$

Likewise, the achievable secrecy rate from S to D_2, denoted as $R_{\mathrm{D}_2\mathrm{S}}^{\mathrm{sec}}$ can be obtained as

$$R_{\mathrm{D}_1\mathrm{S}}^{\mathrm{sec}} = [\frac{2}{3}\log_2(1+\alpha_2 P_2 |\, h_{\mathrm{D}_2\mathrm{S}}\,|^2 + \frac{P_{\mathrm{R}}\,|\,h_{\mathrm{D}_2\mathrm{R}}\,|^2|\,h_{\mathrm{RS}}\,|^2\,\alpha_2\theta_2 P_2}{P_{\mathrm{R}}\left|h_{\mathrm{D}_2\mathrm{R}}\right|^2 + P_2\,|\,h_{\mathrm{RS}}\,|^2}) - \frac{1}{3}\log_2(1+\frac{\alpha_2 P_2\left|h_{\mathrm{RS}}\right|^2}{(1-\alpha_2)\ P_2\left|h_{\mathrm{RS}}\right|^2+1})]^+ \quad (17)$$

where $[x]^+$ denotes $\max(x,0)$.

The optimization problem of maximizing the achievable secrecy rate can be formulated as

$$\begin{aligned} &\arg\ max_{\alpha_1,\theta_1,\alpha_2,\theta_2}\ R_{\mathrm{sec}} \\ &\text{s.t.}\ \ 0 \le \alpha_1,\theta_1,\alpha_2,\theta_2 \le 1 \\ &\qquad \theta_1 + \theta_2 = 1 \end{aligned} \quad (18)$$

where for the multi-user network, the secrecy rate R_{sec} is characterized from two different aspects, one goal is to maximize the worse secrecy rate, and another is to maximize the secrecy sum-rate.

a) In the case of maximizing the worse secrecy rate, R_{sec} can be represented as

$$R_{\mathrm{sec}} = \min(R_{\mathrm{D}_1\mathrm{S}}^{\mathrm{sec}}, R_{\mathrm{D}_2\mathrm{S}}^{\mathrm{sec}}) \quad (19)$$

Then the optimal power allocation factor to maximize R_{sec} is given in the following lemma.

Lemma 1: Assuming $P_1 = P_2$ and the system model is symmetric, then $|\mathrm{h}_{\mathrm{D}_1\mathrm{S}}|^2 =$

$|h_{D_2S}|^2$, $\left|h_{D_1R}\right|^2 = \left|h_{D_2R}\right|^2$. From (16) and (17), it can be easily seen that $R_{D_1S}^{sec}$ and $R_{D_2S}^{sec}$ are monotonically increasing with respect to the value of θ_1 and θ_2 respectively. It is not difficult to prove using proof by contradiction that when $\alpha_1 = \alpha_2$ and $\theta_1 = \theta_2 = 0.5$, i.e. $R_{D_1S}^{sec} = R_{D_2S}^{sec}$, the corresponding R_{sec} is the maximum achievable secrecy rate.

Proof: Suppose $R_{sec} = R_{D_2S}^{sec}$, then $R_{D_1S}^{sec} \geq R_{D_2S}^{sec}$. Let $\alpha_1 = \alpha^*$, $\alpha_2 = \alpha'$ and $\theta_1 = \theta$, $\theta_2 = 1 - \theta$ denote the corresponding optimal power factor, then $\theta_1 \geq \theta_2$. If $\theta_1 \leq \theta_2$, and setting $\alpha_2 = \alpha_1 = \alpha^*$, it can be obtained $R_{D_1S}^{sec} \leq R_{D_2S}^{sec}$ which contradicts the hypothesis. Let $\theta_1' = \theta_1 - \varepsilon > \theta_2$, where ε is a minimum value greater than zero, then there exist θ_2' larger than θ_2 for which the corresponding $R_{sec}' > R_{sec}$. This contradicts the supposition that R_{sec} is the maximum. Thus, it can be seen that when θ_2 is increased to meet $\theta_2 = \theta_1$, the maximum worse secrecy rate can be achieved, and the corresponding optimal power allocation factor meets $\alpha_2 = \alpha_1$. This completes the proof.

Using Lemma 1, the optimization problem in (18) can be rewritten as

$$\begin{aligned} &\arg\ max_{\alpha_1} R_{D_1S}^{sec} \\ &\text{s.t. } 0 \leq \alpha_1 \leq 1 \end{aligned} \tag{20}$$

Substituting (16) into (20), the problem can be transformed to maximize $8^{R_{sec}}(\alpha)$ as

$$8^{R_{sec}} = A_1\alpha^3 + B_1\alpha^2 + C_1\alpha + 1 \qquad \alpha \in (0,1) \tag{21}$$

where $A_1 = -(AB+C)^2 E / B^2 D$, $B_1 = (AB+C)(ABD+CD-2BE)/B^2 D$, $C_1 = [2BD(AB+C) - B^2 E]/B^2 E$, and $A = P_1|h_{D_1S}|^2$, $B = P_R|h_{D_1R}|^2 + P_1|h_{RS}|^2$, $C = P_R|h_{D_1R}|^2|h_{RS}|^2\theta_1 P_1$, $D = P_1|h_{RS}|^2 + 1$, $E = P_1|h_{RS}|^2$

When $P_i|h_{ij}|^2 \gg 1$, it yields $A_1 < 0$, $B_1 > 0$, $C_1 > 0$. To take the derivative of $8^{R_{sec}}(\alpha)$ with respect to α, this yields

$$\frac{\partial f}{\partial \alpha} = 3A_1\alpha^2 + 2B_1\alpha + C_1 \tag{22}$$

As $B_1^2 - 3A_1C_1 > 0$, let $\frac{\partial f}{\partial \alpha} = 0$ and it can be obtained

$$\alpha^* = (-B_1 - \sqrt{B_1^2 - 3A_1C_1})/3A_1 > 0,\ \alpha' = (-B_1 + \sqrt{B_1^2 - 3A_1C_1})/3A_1 < 0 \tag{23}$$

When $\alpha^* \in (0,1)$, the optimal power allocation factor shall be selected as $\alpha_1 = \alpha^*$, and the corresponding R_{sec} is the maximum achievable worse secrecy rate. Otherwise α_1 shall be selected as $\alpha_1 = 1$ representing a non-jamming scenario or $\alpha_1 = 0$ indicating that the secrecy rate outage will arise.

b) In the case of maximizing the secrecy sum-rate, R_{sec} can be expressed as

$$R_{sec} = R_{D_1S}^{sec} + R_{D_2S}^{sec} \tag{24}$$

To substitute (9) into (24), the optimization problem in (18) becomes

$$\begin{aligned} \arg\max_{\alpha_1,\alpha_2,\theta_1}\ & \frac{2}{3}\log_2\left(1+\alpha_1 P_1 |h_{D_1S}|^2 + \frac{P_R |h_{D_1R}|^2 |h_{RS}|^2 \alpha_1\theta_1 P_1}{P_R\left|h_{D_1R}\right|^2 + P_1 |h_{RS}|^2}\right) + \\ & \frac{2}{3}\log_2\left(1+\alpha_2 P_2 |h_{D_2S}|^2 + \frac{P_R |h_{D_2R}|^2 |h_{RS}|^2 \alpha_2\theta_2 P_2}{P_R\left|h_{D_2R}\right|^2 + P_2 |h_{RS}|^2}\right) - \\ & \frac{1}{3}\log_2\left(1+\frac{\alpha_1 P_1 |h_{RS}|^2}{(1-\alpha_1) P_1 |h_{RS}|^2 + 1}\right) - \frac{1}{3}\log_2\left(1+\frac{\alpha_2 P_2 |h_{RS}|^2}{(1-\alpha_2) P_2 |h_{RS}|^2 + 1}\right) \\ \textit{s.t.}\quad & 0 \leq \alpha_1 \leq 1 \qquad 0 \leq \theta_1 \leq 1 \qquad 0 \leq \alpha_2 \leq 1 \end{aligned} \tag{25}$$

Clearly, (25) is a nonlinear programming (NLP) problem with a constraint set. A

solution of the NLP problem generally requires an iterative procedure to establish a search direction for each major iteration. Here, the Sequential Quadratic Programming (SQP) method is exploited. It usually outperforms other NLP methods in terms of efficiency and accuracy to determine the optimal power allocation factor $(\alpha_1, \alpha_2, \theta_1)$ since the objective function in (25) is twice continuously differentiable, and the corresponding R_{sec} is the maximum achievable secrecy rate.

Next for the purpose of performance comparisons used in Section 4, two benchmark schemes are analyzed.

A. AF-based untrusted relay without jamming (AFU)

For the first benchmark, a conventional AF-based untrusted relay without jamming (AFU) scheme is considered. In fact, AFU scheme can be viewed as a special case of the proposed three-phase AF joint cooperative jamming and power allocation (CJP) scheme, that is, $\alpha_1 = \alpha_2 = 1$, where both S and R transmit their information signals with all available power. Substituting $\alpha_1 = \alpha_2 = 1$ into (16), the achievable secrecy rate at D_1 becomes

$$\mathrm{R}_{\text{sec}}^{\text{AFU}} = [\frac{2}{3}\log_2(1+P_1\left|h_{\mathrm{D_1S}}\right|^2 + \frac{P_{\mathrm{R}}\,|\,h_{\mathrm{D_1R}}\,|^2|\,h_{\mathrm{RS}}\,|^2\,\theta_1 P_1}{P_{\mathrm{R}}\left|h_{\mathrm{D_1R}}\right|^2 + P_1\,|\,h_{\mathrm{RS}}\,|^2}) - \frac{1}{3}\log_2(1+P_1\left|h_{\mathrm{RS}}\right|^2)]^+ \tag{26}$$

From (26), it can be easily seen that when there exist $|h_{\mathrm{RS}}|^2 \gg |\mathrm{h_{D_1S}}|^2, |\mathrm{h_{D_1R}}|^2$, i.e. the eavesdropper's channel is much better than the main channel, so it cannot guarantee that the value of the secrecy rate is greater than zero.

Similarly, to maximize the worse secrecy rate in AFU scheme, using proof by contradiction, it can be obtained that the optimal value θ_1 shall be selected as $\theta_1^* = 0.5$, and the corresponding R_{sec} is the maximum achievable secrecy rate. To maximize the secrecy sum-rate, substituting $\alpha_1 = \alpha_2 = 1$ into (24), it yields

$$\begin{aligned} R_{\text{sec}}^{\text{AFU'}} = {} & \frac{2}{3}\log_2(1+P_1\left|h_{\mathrm{D_1S}}\right|^2 + \frac{P_{\mathrm{R}}\,|\,h_{D_1R}\,|^2|\,h_{RS}\,|^2\,\theta_1 P_1}{P_{\mathrm{R}}\left|h_{D_1R}\right|^2 + P_1\,|\,h_{RS}\,|^2}) - \frac{1}{3}\log_2(1+P_1\left|h_{\mathrm{RS}}\right|^2) + \\ & \frac{2}{3}\log_2(1+P_2\,|\,h_{D_2S}\,|^2 + \frac{P_{\mathrm{R}}\,|\,h_{D_2R}\,|^2|\,h_{RS}\,|^2\,\theta_2 P_2}{P_{\mathrm{R}}\left|h_{D_2R}\right|^2 + P_2\,|\,h_{RS}\,|^2}) - \frac{1}{3}\log_2(1+P_2\,|\,h_{RS}\,|^2) \end{aligned} \tag{27}$$

In (27), the maximum secrecy sum-rate R_{sec} will be achieved when θ_1, θ_2 get the maximum value, thus the maximum R_{sec} can be achieved when $\theta_1 = \theta_2 = 0.5$.

B. Direct transmission based on artificial noise jamming signal (DTJ)

This benchmark involves a jamming process while just treating the untrusted relay as an eavesdropper. S directly transmits its signals to D_i one by one to avoid collisions with part power $\alpha_i P_i$. Due to the symmetry of the system model, the secrecy rate at D_i relative to X_i is equal, thus from (12)-(15), the achievable secrecy rate at D_1 can be easily drawn as

$$\mathrm{R}_{\text{sec}}^{\text{DTJ}} = [\tfrac{1}{2}\log_2(1+\alpha_1 P_1\left|h_{\mathrm{D_1S}}\right|^2) - \tfrac{1}{2}\log_2\left(1+\tfrac{\alpha_1 P_1|h_{\mathrm{RS}}|^2}{(1-\alpha_1)P_1|h_{\mathrm{RS}}|^2+1}\right)]^+ \tag{28}$$

From (17), one can easily see that $4^{\mathrm{R}_{\text{sec}}^{\text{DTJ}}}$ with respect to α_1 is a quadratic function as follows

$$4^{\mathrm{R}_{\text{sec}}^{\text{DTJ}}} = A\alpha_1^2 + B\alpha_1 + 1 \tag{29}$$

where $A = -\frac{P_1^2\left|h_{\mathrm{D_1S}}\right|^2|h_{\mathrm{RS}}|^2}{(1+P_1|h_{\mathrm{RS}}|^2)} < 0$, $B = P_1^2\left|h_{\mathrm{D_1S}}\right|^2|h_{\mathrm{RS}}|^2 + P_1\left|h_{\mathrm{D_1S}}\right|^2 - P_1|h_{\mathrm{RS}}|^2 > 0$. Since $B^2 \geq 4A$, when the vertex of the quadratic curve $r_1 = -B/2A$ is located in the range [0, 1], the optimal value α_1 shall be selected as $\alpha_1^* = r_1$ and the corresponding $\mathrm{R}_{\text{sec}}^{\text{DTJ}}$ is the maximum achievable secrecy rate. Otherwise, α_1 shall be selected as $\alpha_1^* = 1$ representing a non-jamming scenario or $\alpha_1^* = 0$ indicating that the secrecy rate

outage will arise.

4. Numerical Results

In this section, numerical results are provided to verify our theoretical analysis on the system secrecy rate of the proposed CJP scheme for multicast network with an untrusted relay. Moreover, the effects of the relay position on the system secrecy rate will be discussed based on the optimal power factor pair (α_1, θ_1) numerically obtained. Let set $P_1 = P_2 = 16\text{dB}$, $P_R = 10\text{dB}$, m=3. The distance between D_1 and D_2 is normalized to 1, and the untrusted relay is located on the height of the triangle consisting of S, D_1 and D_2 as shown in Figure 1.

Figure 3 first depicts the effect of the relay positions on the values of the optimal power factor $(\alpha_1, \alpha_2, \theta_1)$ in the case of maximizing the worse secrecy rate for the proposed CJP scheme. It can be found from the figure that to maximize the worse secrecy rate, the optimal α_1 shall locate in the range [0.5, 0.6], and $\alpha_2 \in$ [0.3,0.5] while θ_1 is equal to about 0.6.

Figure 4 shows the optimal power allocation factor α_1 with θ_1=0.5 versus the relay positions for the proposed CJP scheme and two benchmarks. As expected, when the untrusted relay moves close to the source, for the CJP and DTJ schemes the source is allowed to allocate a larger proportion of power to transmit artificial jamming signal in order to prevent the untrusted relay from listening. With the increase of α_1, the worse secrecy rate decreases. The corresponding maximum worse secrecy rate results are depicted in Figure 5. It can be observed from the figure that the proposed scheme can achieve a significantly higher secrecy rate than the two benchmarks. Moreover, when the untrusted relay is close to the source, the secrecy rate drops sharply for the AFU scheme.

Figure 6 compares the secrecy sum-rate of the proposed CJP scheme with that of the AFU and DTJ schemes versus the untrusted relay location. The achievable maximum worse secrecy rate of the CJP scheme is also shown in Figure 6 denoted by CJP1. As expected, because the proposed CJP scheme combines the artificial noise jamming and cooperative diversity together, it can effectively improve the system security performance. Compared with CJP1, the performance of CJP2 is slightly improved. This is because for the CJP2 scheme, the goal is to maximize secrecy sum-rate of the whole system without regard to the fair of individual security rates. As the optimal θ_1 for CJP2 is greater than that for CJP1, while $R_{D_1S}^{sec}$ increases with the increase of θ_1, therefore for CJP2 $R_{D_1S}^{sec}$ can be improved by optimizing θ_1 but this will lead to the decrease of $R_{D_2S}^{sec}$. But the secrecy sum-rate will still be greater than the maximum achievable worse secrecy rate under CJP1. Therefore, for the wireless communication system if there is no limit on the transmission rate of each node, CJP2 is preferred. But if there are the certain requirements for the individual secrecy rate, CJP1 is the first choice. In particular, for the CJP2 scheme, since $R_{D_2S}^{sec}$ may be lower than the limit of the system secrecy rate, the information transmission at D_2 may fail, which causes the data congestion, and even greatly increases the outage probability of some data link in multi-user cooperative relay network. This will further do harm to the overall system performance. Therefore, how to choose the optimal CJP scheme should be decided according to the requirement of the system and the user on the secrecy rate.

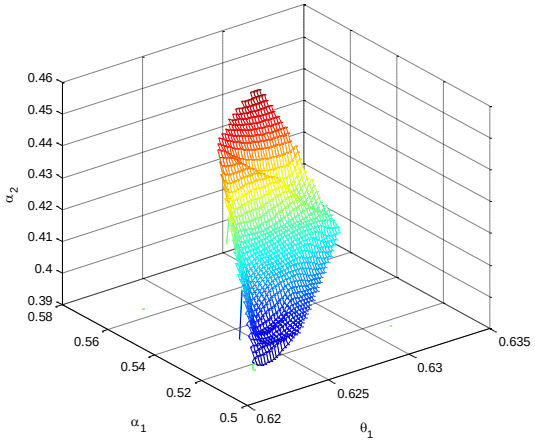


Figure 3. Optimal Power Pair $(\alpha_1, \alpha_2, \theta_1)$

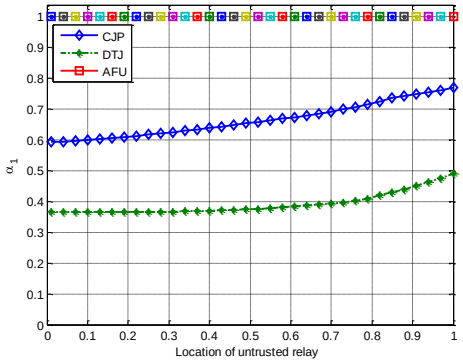


Figure 4. Optimal α_1 with $\theta_1 = 0.5$

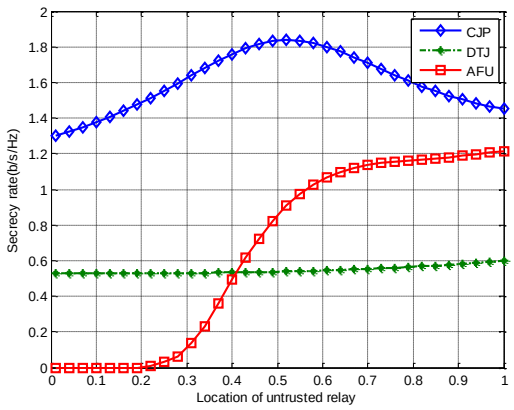


Figure 5. Worse Secrecy Rate

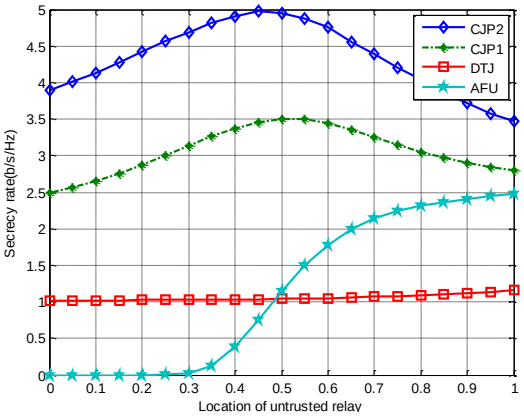


Figure 6.Secrecy Rate Comparison

5. Conclusions

This paper investigated a three-phase AF-based wireless multicasting network with an untrusted relay. By employing time division and artificial jamming signals, a three-phase AF joint cooperative jamming and power allocation scheme (CJP) to improve physical layer security is proposed. The source is allowed to allocate part of the power to transmit jamming signals, meanwhile the relay adopts a signal combining strategy when transmitting the signals from different nodes. Optimal power allocation problem aiming at maximizing the achievable worse secrecy rate or the secrecy sum-rate was derived and analyzed, and performance comparison with two benchmark schemes is also discussed. Numerical results further show that CJP scheme, especially CJP2 provides better achievable secrecy rate compared to DTJ and AFU scheme. Besides, the system resource allocation is more appropriate for the proposed CJP scheme and the achievable secrecy capacity is greater under the joint optimization of power factor pair.

Acknowledgements

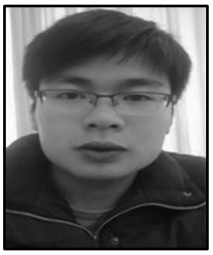
This work was supported by National Natural Science Foundation of China Grant 61362009,41504026, Natural Science Foundation of Jiangxi Province Grant 20152ACB21003, Foreign Science and Technology Cooperation Program of Jiangxi Province Grant 20133BDH80026, Jiangxi Provincial Key Technology R&D Program Grant 20142BBE50044, Science and Technology Project of Jiangxi Provincial Education Department Grant GJJ13056, Young and Middle-aged Teachers Development Program of

Jiangxi and the Innovation Fund Designated for Graduate Students of Jiangxi Grant YC2015-S075.

References

[1] Y. Liang, H. V. Poor and S. Shamai, "Information Theoretic Security", Now Publishers, Delft, The Netherlands, **(2009)**.
[2] V. M. Rohokale, N. R. Prasad and R. Prasad, "Cooperative Wireless Communications and Physical Layer Security: State of the Art", Journal of Cyber Security and Mobility, vol. 1, no. 2, **(2012)**, pp. 227–249.
[3] A. Wyner, "The Wire-tap Channel", Bell Syst. Tech. Journal, vol. 54, no. 8, **(1975)**, pp. 1355–1387.
[4] R. Bassily, E. Ekrem, X. He, E Tekin, J Xie, M Bloch, S Ulukus and A. Yener, "Cooperative Security at the Physical Layer: A Summary of Recent Advances", IEEE Signal Processing Magazine, vol. 30, no. 5, **(2013)**, pp. 16-28.
[5] L. Lai and H. El Gamal, "The Relay-eavesdropper Channel: Cooperation for Secrecy", IEEE Trans. Inform. Theory, vol. 54, no. 9, **(2008)**, pp. 4005–4019.
[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays", IEEE Trans. Signal Process, vol. 58, no. 3, **(2010)**, pp. 1875–1888.
[7] Z. Ding, K. Leung, D.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.
[8] A. Li, Y. Xu, Y. Wang and L. Sun, "Amplify-and-forward-based Cooperative Jamming Strategy with Power Allocation for Secure Communication", International Journal of Communication Systems, vol. 28, no. 10, **(2015)**, pp. 1621-1627.
[9] X. He and A. Yener, "Cooperation with an Untrusted Relay: A secrecy Perspective", IEEE Trans. Inf. Theory, vol. 56, no. 8, **(2010)**, pp. 3807–3827.
[10] P. Aggarwal and A Trivedi, "Secure Wireless Communication Using Friendly Noise through an Untrusted Relay", Wireless Personal Communication, **(2015)**, Article in Press.
[11] J. Huang, A. Mukherjee and A. L. Swindlehurst, "Secure Communication via an Untrusted Non-Regenerative Relay in Fading Channels", IEEE Trans. on Signal Processing, vol. 61, no. 10, **(2013)**, pp. 2536-2550.
[12] J. Huang and A. L. Swindlehurst, "Joint Transmit and Node Selection for One-way and Two-way Untrusted Relay Channels", Proceeding of Conference Record of the 47th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, United States, **(2013)**, pp. 1555-1559.
[13] A. Zewail and A. Yener, "The Multiple Access Channel with an Untursted Relay", Proceeding of Information Theory Workshop, Hobart, Tasmania, Australia, **(2014)**, pp. 25-29.
[14] L. Sun, P. Ren, and Q. Du, Y. Wang and Z. Gao, "Security-aware Relaying Scheme for Cooperative Networks with Untrusted Relay Nodes", IEEE Communications Letters, vol. 19, no. 3, **(2015)**, pp. 463-466.
[15] A. P. Shrestha, J. Jung, and K. S. Kwak, "Secure Wireless Multicasting in Presence of Multiple Eavesdroppers", Proceeding of the 13th Int. Symp. Commun. And Information Technologies (ISCIT), Surat Thani, Thailand, **(2013)**, pp. 814–817.
[16] J. Zhu, Y. Chen and Y. Nakamura, "Outage Performance of Secure Multicasting in the Presence of Multiple Eavesdroppers", Proceeding of the 8th International Conference on Mobile Computing and Ubiquitous Networking, Hakodate, Japan, **(2015)**, pp. 138-142.
[17] P. Xu and X. Xu, "A Cooperative Transmission Scheme for the Secure Wireless Multicasting", Wireless Personal Communications, vol. 77, no. 2, **(2014)**, pp. 1239-1248.

Authors



Xingqun Fu, he received the B.S. degree in communication engineering from Nanchang University, Nanchang, China, in 2014. Currently, He is pursuing his master degree in communication and information system at Nanchang University. His research interests include cooperation based physical-layer security.

An Li, she received the B.S. degree in electronics and communication engineering from the China University of Geosciences, Beijing, China, in 2001, and the M.S. and Ph.D. degrees in communication and information system from the Huazhong University of Science and Technology, Wuhan, China, in 2004 and in 2011, respectively. She was a Research Scholar with the Complex Networks and Security Research Laboratory, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA in 2013. She is currently an Associate Professor with the Department of Electronics Information Engineering at Nanchang University, Nanchang, China. Her current research interests include signal detection and processing, cooperative communication, and physical layer security.

Panagiotis G. Sarigiannidis, he received the B.Sc. and Ph.D. degrees in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and 2007, respectively. He is currently an assistant professor with the University of Western Macedonia, Kozani, Greece. He has published over 70 papers in international journals, conferences, and book chapters. His research interests include medium access protocols in optical networks, dynamic bandwidth allocation schemes in passive optical networks, scheduling policies in IEEE 802.16 wireless networks, wireless push systems design and optimization, quality of service provisioning in optical and wireless networks, traffic estimation and prediction via numerical analysis, and design of burst allocation for optical burst switching networks.

