Huang et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:69
https://doi.org/10.1186/s13638-018-1081-x

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Based on virtual beamforming cooperative jamming with Stackelberg game for physical layer security in the heterogeneous wireless network

Shuanglin Huang*, Li Zhu and Sanjun Liu

Abstract

The physical layer security technology is a technical scheme developed in recent years to solve the problem of information security transmission in wireless communication networks. As one of the physical layer security technologies, cooperative jamming often requires collaborative nodes to actively cooperate with other nodes with secure communication requirements to transmit information. In the environment of heterogeneous wireless network, each wireless node is relatively independent, the relationship is both cooperative and competitive, and the nodes are selfish. In this paper, we study the information transmission between the source and destination nodes, and form a virtual beamforming through the cooperation of the jamming nodes to point to the malicious wiretap nodes, so as to achieve the physical layer secure communication. First, the interest distribution relationship between the source node and other cooperative interference nodes is modeled as the Stackelberg game. The source node pays the consumption of the power consumed by the cooperative jamming nodes and motivates the cooperative interference nodes to participate actively. Then, the competition relationship among all the cooperative nodes is built as a non-cooperative game, so as to promote the reasonable pricing of the consumed power when each node participates in collaboration. When the security rate between the source node and destination node is constant, the power allocation of source and cooperative nodes and the equilibrium point of power price exist and are unique. Through the combined optimization of the two games, the power pricing and power allocation can be dynamically optimized according to the change of the network environment. The simulation results show that the power dynamic allocation and power dynamic pricing have good convergence, and the source node provides a train of thought for the selection of cooperative nodes and their number.

Keywords: The heterogeneous wireless network, Physical layer security, Cooperative jamming, Stackelberg game, Power dynamic pricing

1 Introduction

With the rapid development of wireless communication technology, the problem of information security transmission in wireless networks is becoming more and more important. In recent years, physical layer security technology has become a research hotspot in the field of information security, because it does not rely on data encryption and encapsulation but has the absolute security of information transmission [1, 2]. For an additive noise-degraded wiretap channel, the security capacity C_S is $C_S = C_M - C_E$; the C_M and C_E are the main channel and wiretap channel capacity respectively. Wyner [3] has done an earlier research work in this area. His research shows that the source node and destination node can exchange secret information at a non-zero rate without stealing information from an eavesdropper. However, when the channel condition between the source node and its destination node is worse than that between the source node and the eavesdropper, the secrecy capacity of the source node and its destination node can be zero. Early wireless communication is mainly point-to-point

* Correspondence: huang-shuanglin@163.com
School of Information Engineering, Hubei University for Nationalities, Enshi 445000, China

communication. The wireless communication nodes are basically single-antenna configurations with a single function. These characteristics make the actual security capacity zero.

The physical layer security technology uses the characteristics of randomness, time variability, and reciprocity of wireless channels. It can make sure that both sides of legitimate communication cannot be wiretapped to any information in the presence of the eavesdropper [3]. Now, the rapid progress of wireless communication physical layer technology has promoted the emergence of a new form of eavesdropping channel. For example, the antenna array eavesdropper channel [4, 5], orthogonal frequency division multiplexing (OFDM) wiretap channel [6–8], and relay cooperative eavesdropping channel [9–11] can all get effective secrecy capacity. According to reference [4], when the degree of freedom of artificial noise is greater than that of the eavesdropper receiving signal, the eavesdropper cannot separate secret information and artificial noise from the received signal, and the artificial noise method can achieve a certain secrecy speed. Reference [5] has studied how to introduce the idea of frequency diversity array into an OFDM transmitter and to form effective physical layer secure communication capacity in free space. Reference [6] studied the maximum achievable secrecy rate of the OFDM system through reasonable power allocation. Reference [7] took the max-min fairness criterion of confidentiality rate as an optimization objective and studies how to allocate channels and power among multiple users in a cellular network downlink based on OFDM technology in the presence of an eavesdropper node. The literature in [8] studied the power allocation problem for the wireless users in the downlink of the OFDM system to consider the energy collection and the secret information decoding process. In reference [9], the author studied the physical layer security of the relay network model with multiple relay nodes. With the goal of maximizing the security rate, several different cooperative mechanisms were proposed. Reference [10] studied how to use cooperative nodes to send blocking signals to suppress information disclosure of an eavesdropper. Under the scenario of multiple relay nodes and multiple eavesdropping nodes, the relay adopts decode and forward technology; reference [11] first adopts the finite rate feedback scheme to study the resource allocation of the wireless source node.

When the channel quality between the legitimate users is inferior to the eavesdropping channel, the effective safe transmission rate cannot be obtained. Therefore, the cooperative interference mechanism is proposed, which reduces the quality of the eavesdropping channel by means of artificial interference and destroys the listening ability of the eavesdropping node. In reference [9], the cooperative jamming schemes for improving the physical layer security rate of wireless communication through cooperative nodes are studied. In reference [12], it studied how to use cooperative relay nodes to improve the physical layer security rate of wireless communication by combining decode and forward and cooperative jamming. The literature in [13] discussed the main technology and difficulties in the physical layer security of the OFDM communication system. In that paper, the OFDM beamforming was briefly introduced, and the robustness was also reviewed in the presence of noise and multipath fading. Then, the robustness of OFDM beamforming technology under various noise jamming attacks was discussed. Finally, the latest jamming attack techniques were explored and some potential anti-jamming attacks to improve the robustness and reliability were pointed out. On the basis of reference [14], in reference [15], the time domain artificial noise generation technology for the physical layer security in the multiple input and multiple output (MIMO) OFDM system was studied. It extends the limitation that the number of sender antennas must be less than the number of legitimate receiver antennas in application. In an OFDM technology access network where exist a source node, multiple untrusted nodes, and a friendly interference node, reference [16] studied how to interfere with friendly nodes or improve the sum of secrecy rates or improve the fairness of the whole system.

However, the wireless collaboration nodes in the heterogeneous wireless network are selfish and need an incentive mechanism to ensure their participation in collaboration. A game-based cooperative scheme can motivate the selfish relay nodes to participate in the cooperative [17–20]. Han and Zhang [17, 18] respectively analyze the system game performance of two cooperative interference nodes and the game performance of multi-user shared single cooperative interference node system. In view of the high requirement of communication quality among legitimate communication users and the limited energy of cooperative nodes, multiple collaboration nodes are required to interfere with the service. In order to allocate the compensation and improve the energy efficiency of the cooperative node, a scheme of energy efficiency optimal power allocation based on a Stackelberg game was proposed. The scheme used a two-tier game strategy, the first layer game determines the optimal payment compensation, and the second layer game is used for compensation allocation and power adjustment among the cooperative nodes. Reference [19] proposed a scheme for optimal energy efficiency compensation and power allocation based on a Stackelberg game theory. The two-level game model proved that there exists a global optimal energy efficiency only and gives a closed form solution of the

optimal power allocation scheme. Reference [20] studied sub-carrier allocation and cooperative partner selection based on the Nash bargaining game for physical layer security in OFDM wireless networks.

This paper studies the cooperation of multiple cooperative jamming nodes in a heterogeneous wireless network environment, forming virtual beamforming, which helps to secure information transmission between source node and destination nodes, and to prevent an eavesdropper node from eavesdropping on useful information. For example, in the heterogeneous network environment where wireless sensor network and wireless fidelity (WiFi) network coexist, the wireless sensor networks often need to communicate important information through WiFi network. The joint points connecting the wireless sensor network and the WiFi network are crucial. There are many trusted wireless sensor nodes around them, which can be used to collaborate and interfere in the process of important information interaction to prevent malicious nodes from eavesdropping. Similar situations will also occur in other wireless communication networks such as cellular networks.

In addition, in order to encourage potential trusted wireless nodes to participate in collaboration and optimize the allocation of overall energy consumption, on the one hand, the source node needs a paid use of the power consumed by the cooperative jamming node; on the other hand, the jamming nodes involved in cooperation can reasonably price the power cost and adjust the market price dynamically according to the importance of their own energy, which depends on the number of nodes involved in cooperation, the channel state information of the node itself, and the relative relationship between the node and the source node, the destination node, and the eavesdropper node. Therefore, the cooperation relationship between source node and cooperative nodes is modeled as a Stackelberg game, and the competition and cooperation relationship among all cooperative jamming nodes is modeled as a non-cooperative game.

The contents of this paper are organized as follows: the second part is the system model, the third part is the game modeling, the fourth part is the power allocation strategy and the power price dynamic adjustment program, the fifth part is the simulation, and the sixth part is the summary of this paper.

2 System model

In Fig. 1, there is a source node and destination node pair, which communication is helped by N jamming nodes (J_i, i∈N, $N = \{1,2,\ldots,N\}$) with the existence of an eavesdropper E. The eavesdropping node is always eavesdropping on the information sent by the source node. When the quality of the eavesdropping channel between the source node and the eavesdropping node is weaker than the quality of the main channel, the two parties of the legitimate communication can realize the physical layer security communication. When the main channel quality is weaker than the eavesdropper channel, in order to ensure the security of transmission information, it is necessary to request some cooperative jamming nodes to assist in sending artificial interference signals to destroy the quality of the eavesdropper channel, so as to create a secure communication environment. Here, N cooperative interference node $J_1,\ldots,J_N$ are equipped with a omnidirectional single antenna to transmit and receive data and jointly implement beamforming interference eavesdropping node.

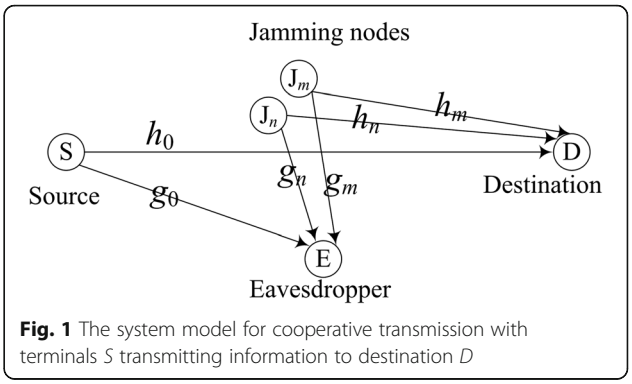

Fig. 1 The system model for cooperative transmission with terminals *S* transmitting information to destination *D*

The whole communication process includes two parts for the cooperation scene of jamming nodes. First, the source node sends the signal to the destination node with power P_s. Meanwhile, the information will also be eavesdropped by the eavesdropping node. The channel gain of link S → D and S → E is $|h_0|^2$ and $|g_0|^2$, respectively. The second is that all jamming nodes are combined to send an artificial interference signal with power P_J. The weight vector of all the cooperative nodes to transmit interference signals is $\mathbf{w}_J(N\times 1)$, $\mathbf{h}(N\times 1)$ represents the channel vector between the N jamming nodes and the destination node, and $\mathbf{g}(N\times 1)$ represents the channel vector between the N jamming nodes and the eavesdropping node, defining $\mathbf{R}_h = \mathbf{h}\mathbf{h}^\dagger$ and $\mathbf{R}_g = \mathbf{g}\mathbf{g}^\dagger$. In addition, it is assumed that all communication channels are ergodic, flat fading, and semi-static. It is assumed that the source node can obtain the instantaneous channel information of each communication channel and the noise power at the eavesdropping node and the destination node are σ^2. In this paper, the variables are expressed in the following form. The black body capitals represent the matrix, while the black body lowercase letter represents the column vector. The conjugate, transposition, and conjugate transposition

of the matrix are expressed by three markers, $(\cdot)*$, $(\cdot)^T$, and $(\cdot)^\dagger$ respectively.

In the recommended scheme, the N trusted relay nodes transmit the human interference signals completely independent of the source node, and the purpose is to confuse the eavesdropping nodes. This can help the secure communication between the source node and its destination node. The cooperative jamming nodes that participate in the cooperative transmission are transmitting to the human interference signal according to the weight, which are expressed as the vector z. In this way, the signal received at the destination can be expressed as follows

$$y_d = \sqrt{P_s} h_0 x + \mathbf{h}^\dagger \mathbf{w}_J z + n_d \tag{1}$$

And the signals received at the eavesdropping node can be

$$y_e = \sqrt{P_s} g_0 x + \mathbf{g}^\dagger \mathbf{w}_J z + n_e \tag{2}$$

where n_d and n_e represent the noise signals received at the destination node and the eavesdropping node, respectively.

Furthermore, the information rates that can be obtained at the destination node and the eavesdropping node are expressed as R_d and R_e respectively, which are expressed as follows

$$R_d = \frac{1}{2} \log\left(1 + \frac{P_s |h_0|^2}{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_h \mathbf{w}_J}\right) \tag{3}$$

$$R_e = \frac{1}{2} \log\left(1 + \frac{P_s |g_0|^2}{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_g \mathbf{w}_J}\right) \tag{4}$$

As a result, in the presence of an eavesdropping node, the secrecy rate that can be obtained at the destination node is shown as follows

$$R_s = \max\{0, R_d - R_e\} \tag{5}$$

In this paper, discussed only is $R_d > R_e$, so the above formula can be further expressed as

$$R_s = \frac{1}{2} \log\left(\frac{\sigma^2 + P_s |h_0|^2 + \mathbf{w}_J^\dagger \mathbf{R}_h \mathbf{w}_J}{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_h \mathbf{w}_J}\right) \times \left(\frac{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_g \mathbf{w}_J}{\sigma^2 + P_s |g_0|^2 + \mathbf{w}_J^\dagger \mathbf{R}_g \mathbf{w}_J}\right) \tag{6}$$

3 Problem description and game modeling

In practical applications, the demand for the secrecy rate of user link needs to be guaranteed. Assuming that the user's secrecy rate requirement is R_s^0, the user link secrecy rate demand will be satisfied when $R_s \geq R_s^0$ is satisfied. As a result, the key problem is to be built to minimize the payment of the source node under the constraints of $R_s \geq R_s^0$.

It is obvious that the nodes in the wireless collaboration network belong to different individuals and are selfish. As a result, the source nodes need to take measures to encourage possible collaboration nodes to participate in collaboration and interfere with eavesdropping in eavesdropping nodes. At the same time, the source node needs to select the most beneficial collaboration nodes for themselves. According to the behavior characteristics of the source node and the cooperative node, the distributed resource allocation scheme based on game theory is used to analyze.

For the source node, it can be regarded as a buyer whose purpose is to use as small as possible to achieve link secrecy rate requirements. Suppose that U_s represents the payment of the source node and U_s is defined as a linear function of the transmission power. It is expressed as follows:

$$U_s = v_s P_s + \sum_{m=1}^{M} v_{J_m} P_{J_m} \tag{7}$$

where v_s and v_{J_m} respectively represent the power price of the source node S and the cooperative jamming node J_m, and P_{J_m} represents the power purchased by the source node to the cooperative jamming node J_m to interfere with the eavesdropping node.

By combining the transmission power of the source node and the transmission power of the cooperative interference node, each source node always minimizes the payment of its own. As a result, the optimization problem for the source node can be expressed as the following formula:

$$\min_{R_s \geq R_s^0} U_s = v_s P_s + \sum_{m=1}^{N} v_{J_m} P_{J_m} \tag{8}$$

where $\mathbf{P} = \{P_s, P_{J_1}, P_{J_2}, \ldots\ldots P_{J_N}\}$ is a power vector, and

$$R_s(\mathbf{P}) = \frac{1}{2} \log\left(\frac{\sigma^2 + P_s |h_0|^2 + \mathbf{w}_J^\dagger \mathbf{R}_h \mathbf{w}_J}{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_h \mathbf{w}_J}\right) \times \left(\frac{\sigma^2 + \mathbf{w}_J^\dagger \mathbf{R}_g \mathbf{w}_J}{\sigma^2 + P_s |g_0|^2 + \mathbf{w}_J^\dagger \mathbf{R}_g \mathbf{w}_J}\right) \tag{9}$$

For cooperative jamming nodes, they can be considered as sellers. The goal is not only to satisfy the payment that the source nodes give them to participate in collaboration, but also to gain as much extra benefits as possible by competing with each other. Then, the utility function of the cooperative jamming node J_m can be defined as

$$U_{J_m} = (v_{J_m} - c_{J_m}) P_{J_m} \tag{10}$$

where c_{J_m} is the power cost of the cooperative jamming

node J_m. As a result, the optimization problem for the revenue of cooperative jamming nodes can be expressed as

$$\max_{0<P_{J_m}\le P_{\max}} U_{J_m}, m = 1, 2, ..., M \tag{11}$$

In the above network models, in order to maximize their profits, each cooperative jamming node needs not only to compete with other jamming nodes, but also to compete with the source node. For the source node, it will optimize the power allocation between the source node and the various jamming nodes based on the power price provided by the cooperative jamming node. For each of the jamming nodes, they must provide the optimal power price to maximize the utility. Between all the jamming nodes, they compete with each other by constantly adjusting their power prices. As a result, the source node can be regarded as the main party of the game, and the jamming node is regarded as a slave. Therefore, there is a Stackelberg game between the source node and the jamming nodes, while all the jamming nodes are non-cooperative games [21].

Lemma 1: Order $\mathbf{w}_J^\dagger \mathbf{g} = \mu$, and $\mathbf{w}_J^\dagger \mathbf{h} = 0$. The solution of the following problem [9]

$$\min \mathbf{w}_J^\dagger \mathbf{w}_J \tag{12}$$

can be expressed as

$$\mathbf{w}_J = \mu[\mathbf{g}\ \mathbf{h}] \begin{bmatrix} \mathbf{g}^\dagger \mathbf{g} & \mathbf{g}^\dagger \mathbf{h} \\ \mathbf{h}^\dagger \mathbf{g} & \mathbf{h}^\dagger \mathbf{h} \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{13}$$

4 The power and price selection method

4.1 Power allocation method

We first fix P_s and find the weights that minimize the payment of the source node to the jamming nodes. Then, we find the value of P_s that minimizes the overall payment. In practical applications, it is difficult to obtain the global information of malicious eavesdropping nodes. In addition, it is noted that the problem (8) is the product of two correlated generalized eigenvector problems, which is generally quite difficult. In order to simplify the analysis, we will add a constraint to completely eliminate the interference signals at the destination, i.e.,

$$\mathbf{w}_J^\dagger \mathbf{h} = 0 \tag{14}$$

Thus, the optimization problem of Eq. (8) can be expressed as

$$\begin{aligned} &\min_{R_s \ge R_s^0} U_s = v_s P_s + \sum_{m=1}^{M} v_{J_m} P_{J_m} \\ &st\{ \begin{array}{l} \mathbf{w}_J^\dagger \mathbf{h} = 0 \\ \mathbf{w}_J^\dagger \mathbf{g} = \mu \end{array} \end{aligned} \tag{15}$$

where $\mu = \sqrt{\frac{P_s |g_0|^2}{4^{-R_s^0}(1+P_s|h_0|^2/\sigma^2)-1} - \sigma^2}$.

Under the assumption that P_s is a constant value, the optimal power allocation of the jamming nodes involved in the cooperation is obtained. In order to solve the optimization problem of Eq. (15), let $\tilde{\mathbf{h}} = \{\frac{h_{J_1}}{\sqrt{v_{J_1}}}, \frac{h_{J_2}}{\sqrt{v_{J_2}}}, ..., \frac{h_{J_N}}{\sqrt{v_{J_N}}}\}$, $\tilde{\mathbf{g}} = \{\frac{g_{J_1}}{\sqrt{v_{J_1}}}, \frac{g_{J_2}}{\sqrt{v_{J_2}}}, ..., \frac{g_{J_N}}{\sqrt{v_{J_N}}}\}$ and $\tilde{\mathbf{w}}_J = (\sqrt{v_{J_1}} w_{J_1}, \sqrt{v_{J_2}} w_{J_2}, ..., \sqrt{v_{J_N}} w_{J_N})$. Then, the optimization problem of Eq. (15) can be further transformed into

$$\begin{aligned} &\min_{R_s \ge R_s^0} U_s = v_s P_s + \tilde{\mathbf{w}}_J^\dagger \tilde{\mathbf{w}}_J \\ &st\{ \begin{array}{l} \tilde{\mathbf{w}}_J^\dagger \tilde{\mathbf{h}} = 0 \\ \tilde{\mathbf{w}}_J^\dagger \tilde{\mathbf{g}} = \mu \end{array} \end{aligned} \tag{16}$$

From the above formula, it can be seen that $\tilde{\mathbf{w}}_J^\dagger \tilde{\mathbf{g}}$ is a positive real number.

According to Lemma 1, $\|\tilde{\mathbf{w}}_J\|^2$ can be first expressed as a function of μ^2:

$$\tilde{\mathbf{w}}_J = \frac{\mu\left(\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}} \tilde{\mathbf{g}} - \tilde{\mathbf{h}}^\dagger \tilde{\mathbf{g}} \tilde{\mathbf{h}}\right)}{\mathbf{g}^\dagger \mathbf{g}(\mathbf{h}^\dagger \mathbf{h}) - \mathbf{g}^\dagger \mathbf{h}(\mathbf{h}^\dagger \mathbf{g})} \tag{17}$$

Therefore, it can be further obtained

$$\|\tilde{\mathbf{w}}_J\|^2 = k_0 \mu^2 \tag{18}$$

$$P_{J_m} = \left\|w_{J_m}\right\|^2 = \frac{\mu^2 k_{m1}}{\left\|k_{m2} v_{J_m} + k_{m3}\right\|^2} \tag{19}$$

where the expressions of k_0, k_{m1}, k_{m2}, and k_{m3} are as follows

$$k_0 = \left\| \frac{\left(\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}} \tilde{\mathbf{g}} - \tilde{\mathbf{h}}^\dagger \tilde{\mathbf{g}} \tilde{\mathbf{h}}\right)}{\mathbf{g}^\dagger \mathbf{g}(\mathbf{h}^\dagger \mathbf{h}) - \mathbf{g}^\dagger \mathbf{h}(\mathbf{h}^\dagger \mathbf{g})} \right\|^2 \tag{20}$$

$$\begin{cases} k_{m1} = \mu^2 \left\| g_{J_m} \sum\limits_{i=1,i\neq m}^{N} \frac{h_{J_i}^{\dagger} h_{J_i}}{v_{J_i}} - h_{J_m} \sum\limits_{i=1,i\neq m}^{N} \frac{h_{J_i}^{\dagger} g_{J_i}}{v_{J_i}} \right\|^2 \\ k_{m2} = \sum\limits_{i=1,i\neq m}^{N} \frac{g_{J_i}^{\dagger} g_{J_i}}{v_{J_i}} \sum\limits_{i=1,i\neq m}^{N} \frac{h_{J_i}^{\dagger} h_{J_i}}{v_{J_i}} - \left(\sum\limits_{i=1,i\neq m}^{N} \frac{h_{J_i}^{\dagger} g_{J_i}}{v_{J_i}} \right)^2 \\ k_{m3} = \sum\limits_{i=1,i\neq m}^{N} \left(\frac{h_{J_m}^{\dagger} h_{J_m} g_{J_i}^{\dagger} g_{J_i}}{v_{J_i}} + \frac{g_{J_m}^{\dagger} g_{J_m} h_{J_i}^{\dagger} h_{J_i}}{v_{J_i}} - \frac{2 h_{J_m}^{\dagger} g_{J_m} h_{J_i}^{\dagger} g_{J_i}}{v_{J_i}} \right) \end{cases} \tag{21}$$

Therefore, Eq. (16) is further expressed as the following form with P_s as a variable

$$\min_{R_s \geq R_s^0} U_s = v_s P_s + \frac{k_0 P_s |g_0|^2}{4^{-R_s^0}\left(1 + P_s |h_0|^2/\sigma^2\right) - 1} - k_0 \sigma^2 \tag{22}$$

Equation (22) is the convex function of P_s, and there is a unique optimal solution. To obtain the first derivative of P_s and to make it zero, the optimal solution of P_s is obtained

$$P_s^* = \frac{\sqrt{\left(1 - 4^{-R_s^0}\right) k_0 |g_0|^2}}{4^{-R_s^0} |h_0|^2/\sigma^2} \frac{1}{\sqrt{v_s}} + \frac{1 - 4^{-R_s^0}}{4^{-R_s^0} |h_0|^2/\sigma^2} \tag{23}$$

It can be seen that the power of the source node decreases with the increase of the power cost v_s of the source node. However, the source node power value P_s will not be lower than the second half $\frac{1-4^{-R_s^0}}{4^{-R_s^0}|h_0|^2/\sigma^2}$ of the above formula on the right side. It is equivalent to the minimum power consumption of the source node in order to achieve the secret rate R_s^0 without the presence of the eavesdropping node.

4.2 Power price method for jamming nodes

In this section, we will discuss the power price strategy of the jamming nodes. To replace the P_{J_m} into Eq. (19), it can be obtained

$$\max_{0<P_m \leq P_{\max}} U_{J_m} = (v_{J_m} - c_{J_m}) P_{J_m}^*, m = 1, 2, \ldots, M \tag{24}$$

It is noted that Eq. (24) is a non-cooperative game between the cooperative jamming nodes, and there is a tradeoff between the utility U_{J_m} and the energy price v_{J_m} of the interference nodes. If the jamming node J_m has good channel conditions and its energy price is relatively low, the source node will ask for more cooperative power from the jamming node J_m, so that U_{J_m} will increase with v_{J_m} growth. When v_{J_m} grows to more than one value, it is no longer useful for the source node to select it to participate, even if the channel of J_m is dominant. In this way, J_m will reduce v_{J_m}, and U_{J_m} also decreases. Therefore, every jamming node J_m is required to dynamically give the optimal power price which changes with the channel condition. Because the source node will only choose the most favorable jamming nodes, the optimal price will also be influenced by other jamming nodes. In addition, when the power cost of cooperative jamming node is increased (for example, the energy of the node itself is reduced, the request of cooperation is increased, the maximum power limit value, and so on), the starting point of cooperative node's cooperation and power price will rise.

Property 1: When the power price of the source node and other cooperative jamming nodes are fixed, the equilibrium point of utility function U_{J_m} of every cooperative jamming node exists and unique.

Proof: from the above formula, Eq. (19) shows that

$$P_{J_m} = \frac{\mu^2 k_{m1}}{\left(k_{m2} v_{J_m} + k_{m3}\right)^2} \tag{25}$$

Then, substituting the above equation into the utility function of the interference node, it can be obtained.

$$\max_{0<P_m \leq P_{\max}} U_{J_m} = \frac{(v_{J_m} - c_{J_m}) k_{m1} \mu^2}{\left(k_{m2} v_{J_m} + k_{m3}\right)^2}, m = 1, 2, \ldots, M \tag{26}$$

Taking the first order derivative of U_{J_m} to v_{J_m}, it can be obtained.

$$\frac{\partial U_{J_m}}{\partial v_{J_m}} = \frac{\mu^2 k_{m1} \left(k_{m3} + 2 k_{m2} c_{J_m} - k_{m2} v_{J_m}\right)}{\left(k_{m2} v_{J_m} + k_{m3}\right)^3} \tag{27}$$

Then, taking the two order derivation of the objective function U_{J_m} to v_{J_m}, it can be further obtained.

$$\frac{\partial^2 U_{J_m}}{\partial v_{J_m}^2} = \frac{2 k_{m2} k_{m1} \mu^2 \left(k_{m2} v_{J_m} - 2 k_{m3} - 3 k_{m2} c_{J_m}\right)}{\left(k_{m2} v_{J_m} + k_{m3}\right)^4} \tag{28}$$

Through the first derivative $\partial U_{J_m}/\partial v_{J_m}$ and the two order derivations $\partial^2 U_{J_m}/\partial v_{J_m}^2$ of the above, we can analyze it piecewise.

(1) When $0 < v_{J_m} < 3c_{J_m} + 2k_{m3}/k_{m2}$, $\partial^2 U_{J_m}/\partial v_{J_m}^2$ is always less than zero. This shows that $U_{J_m}(0 < v_{J_m} < 3 c_{J_m} + 2k_{m3}/k_{m2})$ is a concave function, and there is a unique maximum value.

(2)When $v_{J_m} \geq 3c_{J_m} + 2k_{m3}/k_{m2}$, $\partial U_{J_m}/\partial v_{J_m}$ is always less than zero. This explanation decreases with the increase of $U_{J_m}(v_{J_m} \geq 3c_{J_m} + \frac{2k_{m3}}{k_{m2}})$.

Therefore, the maximum value of $U_{J_m}(v_{J_m} > c_{J_m})$ exists and is unique, and the Property 1 is proved.

According to the above analysis, we need to take the derivative of U_{J_m} to v_{J_m} and make it equal to zero, and it can be obtained.

$$\frac{\partial U_{J_m}}{\partial v_{J_m}} = P^*_{J_m} + (v_{J_m} - c_{J_m}) \frac{\partial P^*_{J_m}}{\partial v_{J_m}} = 0 \tag{29}$$

After solving all these equations about v_{J_m}, the optimal price of all the jamming nodes can be obtained in theory, which can be expressed as

$$v^*_{J_m} = v^*_{J_m}(\sigma^2, G_{sd}, G_{sJ_m}, G_{J_m d}, \{G_{sJ_n}\}, \{G_{J_n d}\}, \{v_{J_n}\}), n \neq m \tag{30}$$

Solving Eq. (29), it can be obtained

$$v_{J_m} = 2c_{J_m} + \frac{k_{m3}}{k_{m2}} \tag{31}$$

It is important to note that the value of v_{J_m} calculated by the upper type is obtained when the power of the source node and the power price of other relay nodes are given. So, the result of the upper calculation is not optimal. The value of the optimal v_{J_m} to meet the requirements of a certain precision can be recursively obtained by the gradient method. The steps are as follows: (1) The calculation of the initial price $v_{J_m}(0) = 2c_{J_m} + \frac{k_{m3}}{k_{m2}}$ by (31); (2) with Eq. (24) to calculate $U_{J_m}(v_{J_m}(n))$ and $U_{J_m}(v_{J_m}(n) + \Delta)$ (when the cost is $c_{J_m} = 1$, the step size Δ is generally 0.01); (3) the price update formula is $v_{J_m}(n+1) = v_{J_m}(n) + \lambda[U_{J_m}(v_{J_m}(n) + \Delta) - U_{J_m}(v_{J_m}(n))]$; (4) repeat (2) and (3) until $|v_{J_m}(n+1) - v_{J_m}(n)|$ is less than the stop value.

In heterogeneous wireless networks, each node is often able to obtain only local channel state information. Therefore, it is difficult to provide the optimal value directly, whether it is the power allocation by the source nodes or the pricing of the power price of the cooperative jamming nodes. In this case, it is necessary for the source node to cooperate with all the cooperative jamming nodes through "the power pricing of each jamming node → the power allocation → the power pricing of each jamming node → the power allocation of source node." After several rounds, it converges to the optimal value while meeting the error requirement.

5 Simulation and result

In this part, the dynamic power allocation, price dynamic pricing, cost price change, and convergence are simulated. The same system setting as reference [9] is used in this paper, where the source node, the destination node, and the eavesdropping node are placed in a straight line. In order to illustrate the effect of distance (the effect of distance is used to represent the change of wireless channel environment), the channel model between any two nodes is set as a line-of-sight transmission channel model. The path gain is expressed as $d^{-c/2}e^{i\theta}$, where d represents the distance between any two nodes (unit: meter), $c = 3.5$ represents the exponential factor of the path loss, and θ is a random phase that is evenly distributed between $[0, 2\pi]$.

In the following simulation, it is assumed that the distance between the cooperative jamming nodes is negligible relative to the distance from source node, destination node, and eavesdropping node. The distance between the cooperative jamming nodes and the source node, the destination node, and the eavesdropping node can be approximately regarded as the same. The source node and the destination node are fixed in the two-dimensional coordinate system at the point S (0, 0) and point D (100, 0),respectively(unit: meter). The noise in the channel is additive Gauss white noise, and the noise power is 10^{-9} W. The next simulation in this paper has carried out 1000 Monte Carlo independent experiments and then averages to get the average results.

Figure 2 describes that the benefit U_{J_1} of the cooperative jamming node J_1 is a curve with the change of its power price v_{J_1}. It can be seen from the diagram that the maximum value of the revenue U_{J_1} exists only.

In Figs. 3 and 4, the cooperative jamming node power price and utility function with recursion times and the convergence of the situation are described (The cooperative interference is at coordinate (30, 5), and the eavesdropping node is at coordinate (50, 0)). As it can be seen from the chart after five rounds of the dynamic adjustment of pricing power and power allocation, the power price and the utility function of each node can quickly converge.

Figure 5 describes a curve that the power price v_{J_1} of a cooperative jamming node J_1 changes dynamically as its position changes, and Fig. 6 describes a curve of dynamic changes in the revenue U_{J_1} of a cooperative jamming node J_1 with its location (The location of the cooperative jamming node moves along the straight line from the coordinate point (10, 5) to the coordinate point

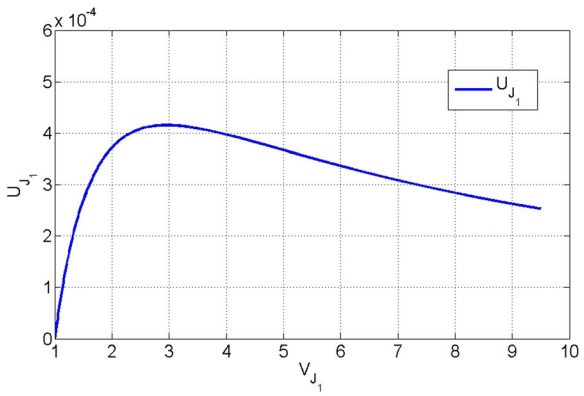

Fig. 2 The revenue U_{J_1} of J_1 varies with its power price v_{J_1} (There are 5 cooperative jamming nodes)

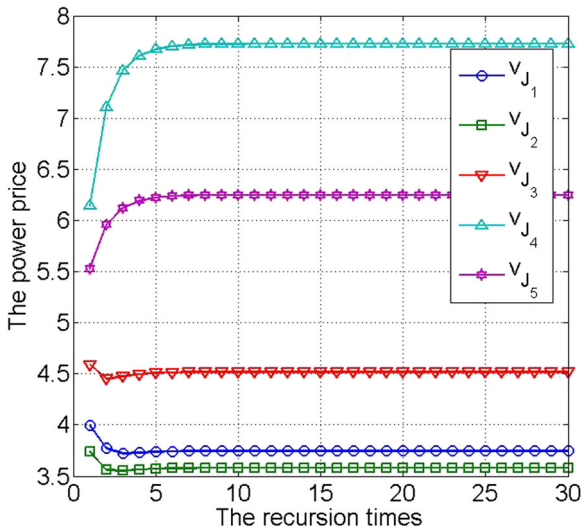

Fig. 3 The power price of the cooperative jamming nodes vs the recursion times

(90, 5), and the eavesdropping node is fixed at the coordinate point (50, 0)). When the jamming nodes are in different positions and their channel conditions are different, the optimal power price will be adjusted dynamically. As it can be seen from the above two figures, the highest power price does not deserve the highest income. The income of the jamming node is determined by its power price and the power consumed by it. Only the power price of the jamming node is appropriate, and the source node is willing to assign it more power to participate in the collaboration. The jamming nodes also gain the most benefit because of their reasonable choice.

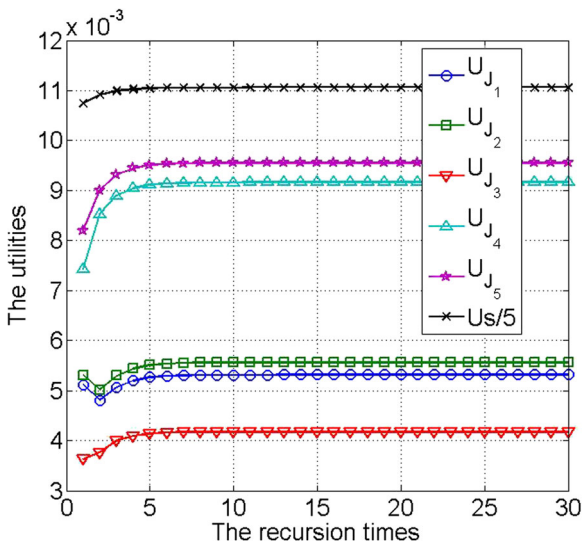

Fig. 4 The utility function vs the recursion times

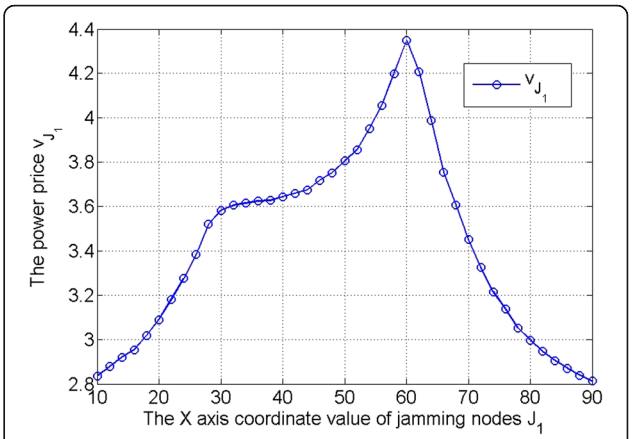

Fig. 5 The power price v_{J_1} of cooperative jamming node vs its position change

Figure 7 describes the total payment U_S of the source node changing along with the location of the cooperative jamming node (the cooperative jamming node moves along the straight line from the coordinate point (10, 5) to the coordinate point (90, 5), and the eavesdropping node is fixed at the coordinate point (50, 0)). As you can see from Fig. 7, the total payment of the source node is the lowest when the cooperative jamming node is nearest to the eavesdropper node. This is because the cooperative jamming node has the best effect on the eavesdropping node when the distance from the eavesdropping node is nearest and the power consumption is the lowest.

Figure 8 describes the total payment U_S of the source node changing along with the location of the eavesdropping node (the eavesdropping node moves along the straight line from the coordinate point (20, 0) to the coordinate point (90, 0)). The five simulation curves above correspond to the situation where the cooperative jamming nodes are located at the coordinate points (30, 5),

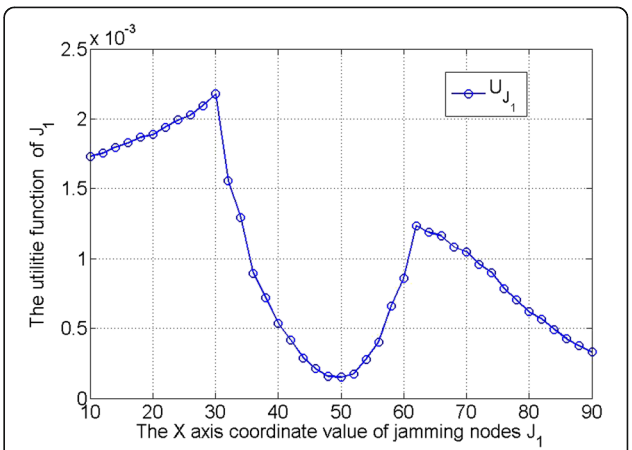

Fig. 6 The revenue U_{J_1} of cooperative jamming node vs its position change

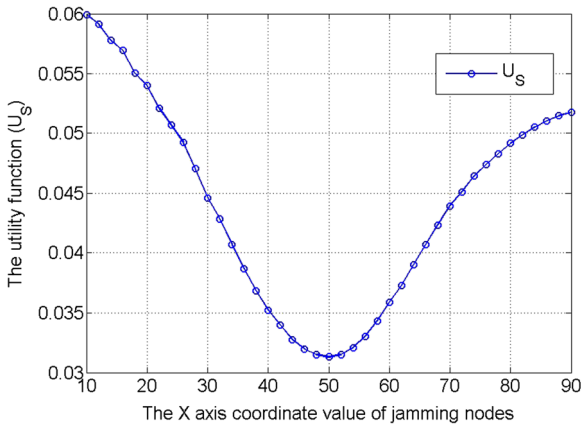

Fig. 7 The source node total payment U_S vs the location change of cooperative jamming nodes

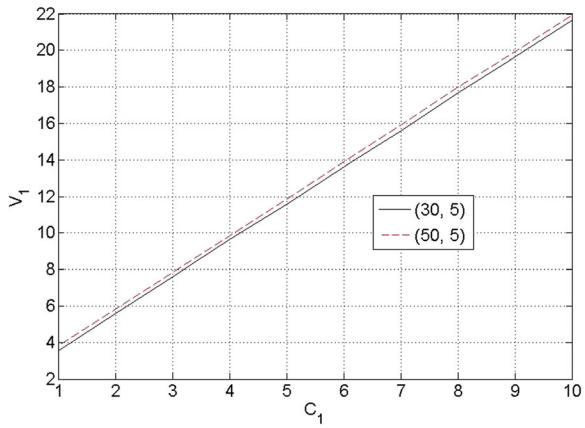

Fig. 9 The curve of the change in the price of power with the cost price

(40, 5), (50, 5), (60, 5), and (70, 5), respectively. It can be seen from the figure that the total payment of the source node is the lowest when the eavesdropping node is nearest to the cooperative jamming node. And the closer the distance from the source node to the cooperative jamming node, the lower the maximum value of each curve (the source node total payment U_S).

Combining with the previous analysis, when the information of the channel state of the eavesdropping node is known, it is most favorable to select the cooperative jamming node closest to the eavesdropping node; when the channel state information of the eavesdropping node is unknown, it is necessary to consider the worst case, that is, the best choice is to choose the cooperative jamming node closest to the source node.

Figure 9 is a curve that increases the power price V_1 of a cooperative jamming node J_1 as its cost price c_1 increases. This is due to the higher cost price of the cooperative jamming node, and it is bound to increase the power price in order to obtain the same income. From the simulation results, the curve approximated linearly.

Figure 10 describes the curve that the total payment U_S of the source node varies with the number of cooperative jamming nodes. The eavesdropping node is fixed at the coordinate point (50, 0), and the three simulation curves above correspond to the situation where the jamming nodes are located at the coordinate points (30, 5), (50, 5), and (70, 5) respectively. It can be seen that the total payment U_S of the source node decreases with the increase of the number of the cooperative jamming nodes. This is due to the increase of the number of cooperation nodes, which will lead to more intense competition among the cooperative nodes, resulting in lower power price of the cooperative jamming node. This inevitably reduces the cost that the source node seeks for collaboration. Therefore, the source nodes always want more cooperative

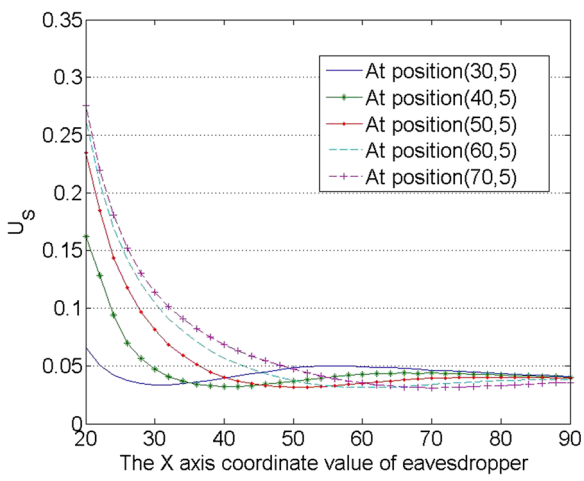

Fig. 8 The source node total payment U_S vs the location change of the eavesdropping node

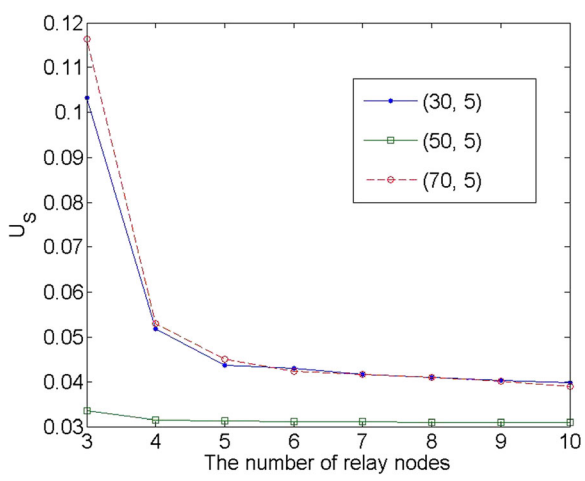

Fig. 10 The total payment U_S of the source node vs the number of cooperative jamming nodes

jamming nodes to participate in cooperative jamming in order to reduce the total cost of payment. However, from Fig. 9, it can be seen that when the number of jamming nodes involved in cooperative jamming transmission reaches five, the total payment U_S of the source node will decrease slowly with the increase of the number of nodes involved in cooperative jamming. In practice, the participation of more nodes in collaboration will bring more complex communication overhead of channel state information. Therefore, it is not necessary for source nodes to seek more than six interference nodes to participate in the cooperative jamming transmission.

In a word, the following conclusions can be obtained from the above simulations. The cooperative jamming nodes are competitive and cooperative. They dynamically optimize their own power price independently according to the network environment change (including channel characteristics, competition intensity, and energy status). Correspondingly, the source node can also optimize the power allocation according to the power pricing of the cooperative node, channel characteristics and its energy status, so as to improve the dynamic adaptability of the physical layer security rate.

6 Conclusions

In a heterogeneous wireless network environment, this paper studied, in the presence of an eavesdropping node, the source node and destination node cooperating to intercept the eavesdropping nodes through trusted jamming nodes, so as to achieve the physical layer secure communication. In order to encourage the potential nodes to participate in cooperation and interfere with the eavesdropping of malicious nodes, the relationship between the source node and the cooperative interference node was modeled as a Stackelberg game in this paper. The jamming power consumed by the cooperative jamming nodes was paid according to the market price, and the power allocation solution under the market price was given. At the same time, the competition relationship among the jamming nodes involved in cooperative jamming was modeled as a non-cooperative game. Each jamming node dynamically adjusts the power cost price and market price independently based on its own channel characteristics, surplus energy, and consumed power. In a word, through the joint optimization of these two games, the power pricing and power allocation can be dynamically optimized according to the change of channel characteristics and competition intensity.

In this paper, the following several cases were simulated. First, the simulation of the dynamic power allocation and the dynamic power pricing of each cooperative jamming node shows that the power allocation and the market price would soon reach the optimum value after more than five rounds of dynamic adjustment. And it had good convergence. Secondly, the dynamic changes of the location of the cooperative jamming node and the eavesdropping node were simulated respectively, and the results illustrated the cooperative node selection idea under different circumstances. Finally, it could be seen that the total payment U_S of the source node decreases with the increase in the number of participating cooperative jamming nodes. However, when the number of nodes involved in cooperative jamming transmission reaches five, the total payment U_S of the source node will decrease slowly as the number of cooperative jamming nodes increases, which is of guiding significance for the selection of the number of cooperative jamming nodes.

Acknowledgements

This work was supported by the National Science Foundation of China under grant no. 61461018, the Hubei Province and the colleges and universities in the Outstanding Youth Science and Technology Innovation team plan (no: T201512), and the Science and Technology Program Project of Enshi Autonomous Prefecture in 2016 (XYJ2016000155).

Authors' contributions

SLH contributed to the conception and algorithm design of the study. SJL and LZ contributed to the acquisition of simulation. SLH, SJL, and LZ contributed to the analysis of simulation data and approved the final manuscript.

Authors' information

Shuanglin Huang received M.S. and Ph.D. degrees from the Taiyuan University of Technology and Huazhong University of Science and Technology, in 2008 and 2012, respectively. He is an assistant professor in the School of Information Engineering, Hubei University for Nationalities, Enshi, Hubei, China. His research interests lie in wireless sensor networks, wireless communications and networks, game theory, parallel computing, and Internet of things. (E-mail:huang-shuanglin@163.com)

Li Zhu received a M.S. degree from the China University of Geosciences in 2009. She is a lecturer in the School of Information Engineering, Hubei University for Nationalities, Enshi, Hubei, China. Her research interests lie in wireless sensor networks, parallel computing, and Internet of things. (E-mail:lier_zhu@163.com)

Sanjun Lin received M.S. and Ph.D. degrees from the Chinese Academy of Sciences and Peking University, Beijing, China in 2007 and 2017, respectively. He is a lecturer in the School of Information Engineering, Hubei University for Nationalities, Enshi, Hubei, China. His research interests lie in wireless communication, embedded system, co-frequency co-time full-duplex and information theory, wireless sensor networks, parallel computing, and Internet of things. (E-mail: liusanjunbox1@126.com)

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 26 January 2018 Accepted: 15 March 2018
Published online: 27 March 2018

References

1. M Bloch, M Barros, M Rodrigues, ML SW, Wireless information-theoretic security. IEEE Trans. Inf. Theory **54**, 2515–2534 (2008). https://doi.org/10.1109/TIT.2008.921908
2. L Lai, H El Gamal, The relay-eavesdropper channel: cooperation for secrecy. IEEE Trans. Inf. Theory **4**, 4005–4019 (2008). https://doi.org/10.1109/TIT.2008.928272
3. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)

4. XY Zhou, MR Mckay, Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. IEEE Trans. Veh. Technol. **59**, 3831–3842 (2010). https://doi.org/10.1109/TVT.2010.2059057
5. Y Ding, J Zhang, V Fusco, Frequency diverse array OFDM transmitter for secure wireless communication. Electron. Lett. **51**(17), 1374–1376 (2015). https://doi.org/10.1049/el.2015.1491
6. X Lin, S Xiaoting, X Wang, et al., TSVC: timed efficient and secure vehicular communications with privacy preserving. IEEE Trans. Wirel. Commun. **7**(12), 4987–4998 (2008). https://doi.org/10.1109/T-WC.2008.070773
7. Sotiris Karachontzitis, Member, Stelios Timotheou. Security-aware max–min resource allocation in multiuser OFDMA downlink. IEEE Trans. Inf. Forensics Secur. 10(3): 529–542, 2015. https://doi.org/10.1109/TIFS.2014.2384392.
8. M Zhang, Y Liu, Energy harvesting for physical-layer security in OFDMA networks. IEEE Trans. Inf. Forensics Secur. **11**(1), 154–162 (2016. Digital Object Identifier 10.1109/TIFS.2015.2481797). https://doi.org/10.1109/TIFS.2015.2481797
9. L Dong, Z Han, AP Petropulu, et al., Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010). https://doi.org/10.1109/TSP.2009.2038412
10. J Huang, AL Swindlehurst, Cooperative jamming for secure communications in MIMO relay networks. IEEE Trans. Signal Process. **59**, 4871–4884 (2011). https://doi.org/10.1109/TSP.2011.2161295
11. MR Abedi, N Mokari, MR Javan, H Yanikomeroglu, Limited rate feedback scheme for resource allocation in secure relay-assisted OFDMA networks. IEEE Trans. Wirel. Commun. **15**(4), 2604–2618 (2016). https://doi.org/10.1109/TWC.2015.2505728
12. S Huang, J Wei, C Yang, C Liu, Joint decode-and-forward and cooperative jamming for secure wireless communications. Int. Conf. Wirel. Commun. Netw. Mob. Comput. IEEE, Wuhan **2011**, 1–4 (2011). https://doi.org/10.1109/wicom.2011.6040145
13. C Shahriar, M La Pan, M Lichtman, T Charles Clancy, R McGwier, R Tandon, S Sodagari, JH Reed, PHY-layer resiliency in OFDM communications: a tutorial. IEEE Commun. Surv. Tutorials. **17**(1), 292–314 (2015). https://doi.org/10.1109/COMST.2014.2349883
14. H Qin, Y Sun, TH Chang, X Chen, CY Chi, M Zhao, J Wang, Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs. IEEE Trans. Wirel. Commun. **12**(6), 2717–2729 (2013). https://doi.org/10.1109/TCOMM.2013.050713.120730
15. Tomoki Akitaya, Shunta Asano, Takahiko Saba. Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems. ©2014 IEEE ICC'14 - W1: Workshop on Wireless Physical Layer Security, 807–812, 2014. https://doi.org/10.1109/ICCW.2014.6881299.
16. R Saini, A Jindal, S De, Jammer-assisted resource allocation in secure OFDMA with untrusted users. IEEE Trans. Inf. Forensics Secur. **11**(5), 1055–1070 (2016). https://doi.org/10.1109/TIFS.2016.2516912
17. Han Z, Marina N, Debbah M, et al. Physical layer security game: how to date a girl with her boyfriend on the same table. International Conference on Game Theory for Networks. Istanbul: [s. n.]: 287–294, 2009. https://doi.org/10.1109/GAMENETS.2009.5137412.
18. Zhang Rongqing, Song Lingyang, Han Zhu. Improve physical layer security in cooperative wireless network using distributed auction game. 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Shanghai: [s. n.]: 18–23, 2011. https://doi.org/10.1109/INFCOMW.2011.5928805.
19. D Chen-hui, S Mei, W Li, M Yue, Improved physical layer security with cooperative jamming based on Stackelberg game. J. Beijing Univ. Posts. Telecommun. **37**(5), 11–15 (2014). https://doi.org/10.13190/j.jbupt.2014.05.003
20. S Huang, A Jing, J Tan, X Jian, Subcarrier allocation and cooperative partner selection based on nash bargaining game for physical layer security in OFDM wireless networks. Concurr. Comput. Prac. Exp. **29**(3), 1–15 (2017). https://doi.org/10.1002/cpe.3790
21. G Owen, *Game Theory*, 3rd edn. (New York, Academic, 2001), pp. 120–200