Huang et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:270
https://doi.org/10.1186/s13638-018-1288-x

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Based on the Stackelberg game with decode and forward protocol for physical layer security in the heterogeneous wireless networks

Shuanglin Huang*, Qiongying Tan, Aixia Jing and Sanjun Liu

Abstract

Using wireless relay nodes to cooperate is a very important helpful way to improve the physical layer security performance. In this paper, in the presence of an eavesdropping node between the source and destination nodes, a decoded and forward technology is used to form a virtual beam through the relay nodes, which selectively enables the main lobe to point to the destination node to achieve the secure communication of the physical layer. However, this situation often requires the assumption that the relay nodes involved in collaborative help can unconditionally and unselfishly assist other nodes in secure communication. In the actual heterogeneous wireless network environment, each wireless node has selfishness, and their relationship is not only cooperative but also competitive. First, in order to encourage the active participation of the relay nodes, the relationship between the source nodes and the cooperative relay nodes is modeled as the Stackelberg game. Through this game, the dynamic compensation of the power consumed for the cooperative nodes is achieved. Then, in order to promote the virtuous competition among the relay nodes involved in the cooperation, the competition relationship among the participating cooperation nodes is constructed as a noncooperative game. The game will enable all cooperative relay nodes to dynamically and reasonably charge the consumed power. In the case of a certain security rate, this paper proves the power allocation of the source node and the cooperative relay node, as well as the existence and uniqueness of the equilibrium point of the power price. And the convergent search algorithm is given. The simulation results show that the distribution power of the source node and the cooperative relay node will be dynamically optimized with the dynamic change of channel characteristics. The power pricing of the relay nodes will also change with the dynamic changes of channel characteristics and node distribution. In addition, when the number of relay nodes participating in cooperation exceeds 6, the additional revenue to the source node is less.

Keywords: The heterogeneous wireless network, Physical layer security, Decode and forward, Stackelberg game, Power dynamic pricing

1 Introduction

With the rapid development of modern wireless communication technology and network, especially the global 4G, and even the 5G mobile network development, communication security is an important problem to be solved urgently. Because of the openness of the wireless communication media, the transmission of information is easily stolen, tampered, or attacked. In order to solve this problem, a new solution is proposed, which is the physical layer security technology. The physical layer security technology is not dependent on the encryption and encapsulation of data, but it has the characteristics of absolute security of information transmission [1, 2], which has the advantage that the encryption processing of the upper layer of the protocol stack can not be compared. In recent years, the physical layer security technology has become a hot topic in the field of information security.

In 1975, Wyner proved that in a discrete and memoryless channel, if the quality of the eavesdropping channel

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

is worse than the main channel, a channel coding can always be found so that the eavesdropper cannot get any information from the received signal to achieve a perfect state of secrecy in the case of the correct demodulation of the legitimate user. There is an upper limit on the way, which is called the security capacity [3]. Leung-Yan-Cheong and Hellman and Csiszar and Korner proved in 1978 that the secrecy capacity of the AWGN channel is actually the difference between the channel capacity of the legitimate channel and the eavesdropping channel, and it actually describes the upper bound of the channel in the secure transmission channel [4, 5]. Therefore, when the capacity of the main channel of the legitimate communication channel is greater than the capacity of the eavesdropping channel, it can transmit the secret information at a nonzero rate, without fear of the eavesdropper's illegal eavesdropping. Since the early wireless communication is a single-antenna system with point-to-point communication, it is difficult to meet the condition that the capacity of the main channel is greater than that of the eavesdropping channel under the presence of the eavesdropping nodes, which makes the actual physical layer security capacity zero.

In recent years, with the development of wireless communication technology, complex communication systems (such as multiple-input multiple-output (MIMO)) and cooperative relay technology have opened new windows for physical layer security communication. The rapid progress of physical layer technology in wireless communication has promoted the emergence of a new form of eavesdropper. The reference [6] presented a method of using space-time codes to approximate the capacity of secret channels in ultra-wideband (UWB) systems. In reference [7], the maximum achievable security rate of orthogonal frequency division multiplexing (OFDM) system through reasonable power allocation is studied. In reference [8], a scheme for transmitting artificial noise is proposed. Because artificial noise is in the zero space of the legitimate channel and does not affect the legitimate parties, it will deteriorate the performance of the eavesdropper. In reference [9], the method of maximizing the transmission rate of the system by dispatching the antenna to transmit power is studied when the number of multicast antennas is larger than the number of the antenna. In particular, many useful researches have been made on the third party trusted nodes.

The reference [10] first studied various models of eavesdropper relay channel. In reference [11], the rate region and random rate region of the eavesdropping relay channel are derived, and the coding problem of the eavesdropping relay channel was studied under the assumption that the transmission information is secret to the relay node. In reference [12], the authors studied the physical layer security problem of relay network models with multiple relay nodes. With the goal of maximizing the security rate, several different cooperative mechanisms are proposed, which are amplified and forward cooperative relays, decoded and forward cooperative relays, and cooperative jamming relays. The reference [13] further optimizes the collaborative scheme based on decode and forward (DF) technology proposed in reference [12] and obtains a more general global optimal solution. In reference [14], the DF and cooperative jamming (CJ) technologies are fused on the basis of the above scheme, and a collaboration scheme based on decode-and-forward plus cooperative jamming (DFCJ) is proposed, which can improve the security performance of the physical layer more effectively. In reference [15], a cooperative node sent a blocking signal to suppress information leakage to the eavesdropper. The current research focused on how to improve the second-stage security [16] of relay cooperation. In reference [17, 18], the authors also used a joint and blocking joint selection scheme to improve the physical layer security performance of the system for both the amplified and forward and decoding forward two-way relay networks. The physical layer security technology based on OFDM communication system was outlined in reference [19]. The robustness of beamforming in the presence of noise, interference and multipath fading was analyzed. It can be seen that the relay cooperation technology has further widened the application scope of the physical layer security and has broad application prospects.

However, due to the mobility of wireless nodes under heterogeneous wireless networks, the channel characteristics of nodes change dynamically. The effective physical layer security capacity is difficult to be effectively guaranteed. Considering the selfishness of cooperative nodes, people propose a game cooperative approach. The references [20, 21] not only study the physical layer security performance of the two cooperative nodes to assist the same source node, but also study the physical layer security performance of the single cooperative interference node in the multi source node competition, and model the relationship between them as a Stackelberg game. In reference [22], a noncooperative game was used to study the transmission of uplink in the future wireless network, and a behavior hypothesis based method is proposed to solve the problem of relay selection and response to malicious nodes. In [23], the static game between Alice and relay was studied by auction theory, which helps solve the problem of active utilization of interference. The reference [24] investigated the cooperation between source, legitimate relay and destination node, and formed a cooperative alliance. The alliance game was used to study the formation of the wireless node cooperation alliance and the impact on the security performance of the physical layer. Based on the OFDM

multicarrier allocation technology, the wireless nodes belonging to different subjects were formed into a cooperative alliance, and the Nash bargaining solution, which is satisfied by both parties, is obtained through the bargaining cooperation game in reference [25]. On the basis of the above, based on the cooperative jamming technology, the power allocation between the source nodes and the third party trusted nodes participating in the collaboration was further studied and modeled as a Stackelberg game in reference [26].

However, these studies mainly consider the simple cooperative strategy or the countermeasures, and still need to be further studied in the dynamic network environment. Unlike the reference [26], the cooperative jamming technique is used to interfere the acceptance of the eavesdropping node. This paper uses trusted cooperative relay nodes to forward the information from the source node. At the same time, the beamforming technology is used to avoid wiretap eavesdropping and enhance the signal strength to the legitimate destination node. Thus, a higher physical layer security capacity is obtained. In this paper, under the environment of heterogeneous wireless network, the information security transmission between source node and destination node is realized with the help of cooperative relay nodes. The power weight of cooperative relay nodes is optimized by the source node, so that the virtual beamforming is directed to the destination node, and at the same time, the effective power of the eavesdropper nodes is minimized. Thus it can not only help the information security transmission between the source nodes, but also against the malicious eavesdropping information of the eavesdropper nodes. For example, in heterogeneous network environments where wireless fidelity (WiFi) networks and cellular networks coexist, mobile terminals often need to transmit important information through WiFi networks. If the content or information of the mobile terminal is particularly important, It can use the help of other mobile terminal nodes that can be trusted to forward the key information to avoid malicious node eavesdropping. Similarly, in the heterogeneous environment where wireless sensor networks and WiFi coexist, there are similar issues of information security transmission and similar solutions.

In addition, the wireless nodes in the heterogeneous wireless communication network have mobility, the relationship between nodes changes and the channel characteristics between the wireless nodes are in dynamic change. Therefore, the relative relationship among the wireless nodes (neighborhood relationship, collaboration relationship, competition relationship) is also changing dynamically. At the same time, mobile wireless nodes generally belong to different subjects and have selfishness. Their participation in collaboration always chooses strategies that are more favorable to themselves. Therefore, in order to motivate the trustworthy relay nodes to actively participate in the cooperation, the source node with confidential information transmission requires a certain cost to compensate for the energy consumption which is used by the cooperation node to help it to complete the secure communication. On the other hand, the source node always wants to pay only less cost to the wireless nodes participating in cooperation, so that it can get satisfactory results. In this way, the source node will choose those third party trusted nodes with low power price and greater help to participate in collaboration. This requires the reasonable pricing of the potential wireless relay nodes, which can occupy the advantages that should be occupied in many alternative relay nodes and obtain the relative maximum income. For example, in the vegetable market, a single merchant raising the price will only make it difficult to sell their own goods, to their own losses. And if a merchant's product cost is lower, it can objectively sell the goods at a price lower than the market price, thus gaining more sales and profits. Based on this consideration, the relationship between the source node and the trusted relay nodes which participates in the cooperative secure transmission is modeled as the Stackelberg game, and the relationship between the competing trusted relay nodes is modeled as a noncooperative 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 experimental model design

In this paper, a wireless network system model is studied. It consists of a source node, a destination node, N trustworthy relay nodes and an eavesdropper node. As shown in Fig. 1, there is a source node and destination node pair, which communication is helped by N relay nodes in the presence of an eavesdropping node. The N relay nodes r_1,... r_N, execute the decoding and forwarding protocol. When the source and destination node channel

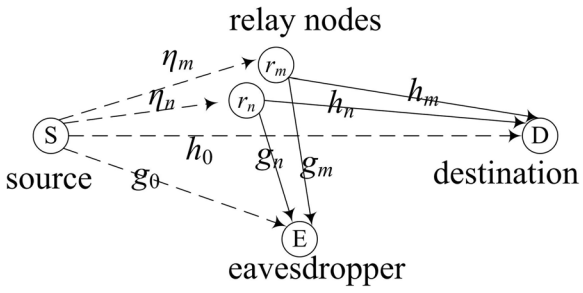

Fig. 1 The system model for cooperative transmission with terminals S_i transmitting information to destination D_i

capacity is weaker than the wiretap channel, in order to ensure the physical layer secure transmission of information, it is necessary to resort to the assistance of some cooperative relay nodes by sending a virtual beamforming signal, which can greatly improve the channel capacity between the source node and destination node, and create a secure communication environment. All wireless nodes are equipped with an omnidirectional single antenna to transmit and receive data, and work in a half-duplex mode.

In this paper, the variables are expressed in the following form. The bold body capitals represent the matrix, while the bold body lowercase letter represents the column vector. The conjugate, transposition and conjugate transposition of the matrix are expressed by three markers, $(\bullet)^*$, $(\bullet)^T$, and $(\bullet)^\dagger$ respectively. In addition, it is assumed that all communication channels are ergodic, flat fading and semi static. The whole communication process includes two parts for the cooperation scene of relay nodes. First, the source node sends the signal to the destination node and the relay nodes with power P_s. Meanwhile, the information will also be eavesdropped by the eavesdropping node. The channel gain of link $S \rightarrow D$ and $S \rightarrow E$ is $|h_0|^2$ and $|g_0|^2$, respectively. And $\boldsymbol{\eta}(N \times 1)$ represents the channel vector between the N relay nodes and the source node. Second, all cooperative relay nodes are combined to decode and forward the signal from the source node with power P_D, and P_{r_i} is used to express the relaying power of the relay node r_i for the important information transmission of the source node. The weight vector of all the cooperative relay nodes to forward signals is $\mathbf{w}_D(N \times 1)$, $\mathbf{h}(N \times 1)$ represents the channel vector between the N relay nodes and the destination node, and $\mathbf{g}(N \times 1)$ represents the channel vector between the N relay node and the eavesdropping node, defining $\mathbf{R}_h = \mathbf{h}\mathbf{h}^\dagger$ and $\mathbf{R}_g = \mathbf{g}\mathbf{g}^\dagger$. 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.

2.1 The direct transmission

This paper discusses the use of relay node cooperation to improve the physical layer security performance. But all cooperation is achieved on the premise that better results can be achieved than direct transmission (without cooperation). Therefore, the following signals are given at the time of direct transmission to facilitate comparison with the subsequent cooperative transmission.

For the direct transmission, in a transmission slot, the source node consumes all the power that can be obtained directly to transmit its coded signal to the destination node. When the transmission signal in a time unit is x, the signal received at the destination is given by the next type

$$y_d = \sqrt{P_s} h_0 x + n_d \tag{1}$$

and the receiving signal at the eavesdropping node is

$$y_e = \sqrt{P_s} g_0 x + n_e \tag{2}$$

where the n_d and n_e represent the complex Gauss noise at the destination node and the eavesdropping node (where the noise is assumed to be white noise in each time slot), respectively.

2.2 The decode and forward cooperative transmission

The DF collaboration scheme is divided into two phases. In the first stage, the source node occupies the first time slot to broadcast its n code symbols to transmit to the trusted relay node. When the source node is transmitting the symbol x, the signal received by its N trusted relay nodes is expressed in the form of a vector.

$$\mathbf{y}_r = \sqrt{P_s}\, \boldsymbol{\eta} x + \mathbf{n}_r, r = 1, 2, \ldots, N \tag{3}$$

where $\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_N)$ is the channel gain vector between the source node and its N trusted relay nodes. $\mathbf{n}_r$ is the noise vector that is received at the N trusted relay nodes. Then, in the first stage, the signal received at the relay node r_i can be expressed as

$$y_{r_i} = \sqrt{P_s} \eta_i x + n_{r_i} \tag{4}$$

As a result, the lowest rate between the source node and its N trusted relay nodes is shown as follows

$$R_r^{\min} = \frac{1}{2} \log\left(1 + \frac{P_s \min\left\{|\eta_1|^2, |\eta_2|^2, \ldots, |\eta_N|^2\right\}}{\sigma^2}\right) \tag{5}$$

And, it is known by Eq. (2), the rate that the eavesdropping node can obtain in the first phase, $R_e^{(1)}$, is shown in the following form

$$R_e^{(1)} = \frac{1}{2} \log\left(1 + \frac{P_s |g_0|^2}{\sigma^2}\right) \tag{6}$$

In this way, the minimum secrecy rate that can be obtained between the source node and its N trusted relay nodes in the first phase can be expressed as follows

$$R_s^{(1)} = \max\left\{0, R_r^{\min} - R_e^{(1)}\right\} \tag{7}$$

Considering the situation of $R_r^{\min} - R_e^{(1)} \le 0$ means that the selected cooperative relay nodes are not suitable and the effective secure transmission rate can not be obtained.

Therefore, this paper only examines the situation of $R_r^{\min} - R_e^{(1)} > 0$. So, the following expression can be obtained.

$$R_s^{(1)} = \frac{1}{2}\log\left(\frac{\sigma^2 + P_s \min\left\{|\eta_1|^2, |\eta_2|^2, ..., |\eta_N|^2\right\}}{\sigma^2 + P_s|g_0|^2}\right) \tag{8}$$

It is visible from the upper form that the rate of secrecy obtained in the first stage is determined by the power of the source node when the channel condition is certain.

In the second stage, we assume that all trusted relay nodes can successfully decode confidential information sent from the source node, re-encode the information, and transmit the recoded information to the destination node cooperatively by using the next second time slots. Specifically, each relay node transmits copies of the re-coding information separately according to weight.

All the cooperative relays transmit the replica symbols of the recoded information respectively according to their weights, which are expressed as vector $\tilde{x}$. In this way, the signal received at the destination can be expressed as follows in the second stage.

$$y_d = \mathbf{h}^{\dagger}\mathbf{w}_D\tilde{x} + n_d \tag{9}$$

And the receiving signal at the eavesdropping node is

$$y_e = \mathbf{g}^{\dagger}\mathbf{w}_D\tilde{x} + n_e \tag{10}$$

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

Further, the information rates at the destination node and the eavesdropping node are represented respectively as $R_d^{(2)}$ and $R_e^{(2)}$, which are expressed as follows.

$$R_d^{(2)} = \frac{1}{2}\log\left(1 + \frac{P_s|h_0|^2}{\sigma^2} + \frac{\mathbf{w}_D^{\dagger}\mathbf{R}_h\mathbf{w}_D}{\sigma^2}\right) \tag{11}$$

$$R_e^{(2)} = \frac{1}{2}\log\left(1 + \frac{P_s|g_0|^2}{\sigma^2} + \frac{\mathbf{w}_D^{\dagger}\mathbf{R}_g\mathbf{w}_D}{\sigma^2}\right) \tag{12}$$

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

$$R_s^{(2)} = \max\left\{0, R_d^{(2)} - R_e^{(2)}\right\} \tag{13}$$

The cooperative transmission is divided into two stages, so the final secrecy rate needs to be satisfied in every transmission stage, so as to ensure that it is finally satisfied. In this way, in the first stage, it must first be ensured that the secret rate between the source node and each relay node performing DF protocol is not less than the final secret rate achieved by the destination node.

In order to ensure that the secrecy rate of each link reaches the final secrecy rate $R_s^{(2)}$ that can be obtained at the destination node, the condition of $R_s^{(1)} \geq R_s^{(2)}$ must be satisfied. If this condition is not satisfied temporarily, the transmission power of the source node can be adjusted to meet it. Therefore, the final secrecy rate obtained by the proposed scheme is as follows

$$R_s = \max\left\{0, \min\left\{R_s^{(1)}, R_s^{(2)}\right\}\right\} \tag{14}$$

In the next analysis, this paper only considers the situation that the rate of secrecy is greater than zero in practice. As a result, the final secrecy rate obtained by the DF scheme can be further simplified to the following expression

$$R_s = \min\left\{R_s^{(1)}, R_s^{(2)}\right\} \tag{15}$$

The entire collaboration scheme is divided into two parts. In the first part, the source node broadcasts its transmission information to the destination node and the relay node that participates in the collaboration. In the proposed scheme, when the N trusted relay nodes based on the decoded and forwarding protocol transmit the secret information from the source nodes according to the weight, all the cooperative nodes are virtual beamforming, and the main lobe is directed to the destination node. This can help the secure communication between the source node and its destination node.

3 Problem description and game modeling

The wireless nodes in the heterogeneous wireless communication network have mobility. The channel characteristics are dynamic, and neighborhood relationships among wireless nodes, cooperative relationship and competitive relationship are also changing dynamically. The source node always wants to pay only the lowest cost of the wireless nodes participating in the cooperation, so that the secret communication rate satisfying its full requirement can be obtained. Assuming that the minimum security rate of the source node is R_s^0, then $R_s \geq R_s^0$ is needed.

It is obvious that the communication nodes in the wireless collaboration network belong to different individuals and are selfish. Therefore, the source node needs to take measures to motivate the possible relay nodes to help forward the transmission of data from the source nodes. Depending on the relationship between the source node and the cooperative relay nodes, the source

node is regarded as the buyer, and all relay nodes participating in the cooperation act as sellers in this paper.

For the source node, we must consider both the power expenditure of the source node itself and the cost of purchasing the power of the cooperative relay node. Suppose that U_s represents all the payment, and U_s is defined as a linear function of the transmission power of the source node and the cooperative nodes. Thus, it is expressed as follows

$$U_s = v_s P_s + \sum_{m=1}^{M} v_{r_m} P_{r_m} \tag{16}$$

where v_s and v_{r_m} respectively represent the power price of the source node S and the cooperative relay node r_m, and P_{r_m} represents the power purchased by the source node from the relay node r_m for relay transmission.

The source node also wants to pay as little as possible. In this way, the key to the problem is to minimize the total cost of the source nodes by selecting the appropriate trusted collaboration nodes to meet the minimum security rate requirements. As a result, the optimization problem for the source node can be expressed as the following formula.

$$\min_{R_s \geq R_s^0} U_s = v_s P_s + \sum_{m=1}^{M} v_{r_m} P_{r_m} \tag{17}$$

where $\mathbf{P} = \{P_s, P_{r_1}, P_{r_2}, \ldots\ldots P_{r_N}\}$ is a power vector, and

$$R_s^0(\mathbf{P}) = \frac{1}{2} \log\left(\frac{\sigma^2 + P_s|h_0|^2 + \mathbf{w}_D^{\dagger}\mathbf{R}_h\mathbf{w}_D}{\sigma^2 + P_s|g_0|^2 + \mathbf{w}_D^{\dagger}\mathbf{R}_g\mathbf{w}_D}\right) \tag{18}$$

The optimization objective of Eq. (17) is to minimize the total payment, and the smaller the overall rate of confidentiality, the smaller the total payment required. Therefore, the minimum rate of secrecy required to satisfy the requirement is $R_s = R_s^0$. From Eqs. (11) and (12), we can get the results in the upper form. Equation (17) reflects that the source node plays a leading role in the relationship with all cooperative relay nodes, and it is a Stackelberg game. Through the above game, the source node will choose those low power prices and cooperate with the third party trusted nodes. This requires the reasonable pricing of the potential wireless relay nodes to maintain the inherent advantage in many alternative relay nodes and obtain the relative maximum income.

For a trusted and potential cooperative relay node, it is necessary to make reasonable pricing of the power paid by its cooperative secure transmission so that it can maintain its advantage in the competition with other potential trustworthy cooperative nodes and gain as much profit as possible. Thus, the utility function of the cooperative relay node r_m can be defined as

$$U_{r_m} = (v_{r_m} - c_{r_m}) P_{r_m} \tag{19}$$

where c_{r_m} is the power cost of the cooperative relay node r_m. As a result, the optimization problem for the revenue of cooperative relay node r_m can be expressed as

$$\max_{0 < P_{r_m} \leq P_{\max}} U_{r_m}, m = 1, 2, \ldots, M \tag{20}$$

In the network model given in this paper, all potential cooperative relays need to win the favor of the source nodes through competition in order to be selected as the cooperative nodes by the source nodes. Therefore, every potential relay node needs to develop a competitive power price. At the same time, all relay nodes participating in cooperation hope to get maximum benefits. The source node plays a leading role in the game between the source node and the cooperative relay nodes. The source node will perform optimal power allocation according to its own power cost, the channel state between each other, and the power price of each cooperative relay node. If a cooperative relay node increases its power price, the source node will reduce its power share to buy it, and vice versa. At the same time, if a cooperative relay node changes its power price, it will also cause other relay nodes to adjust its power price. This creates an internal constraint that will facilitate each relay node to work out a reasonable power price. It can obtain considerable power quotas from the source node and can get the highest possible return at a high price. Based on this consideration, this paper models the relationship between the source node and the trusted relay nodes participating in cooperative secure transmission into Stackelberg games. And the relationship between the competing trusted relay nodes is modeled as a noncooperative game [27].

Lemma 1: Order $\mathbf{s}$ and $\mathbf{t}$ ($\mathbf{s}$ and $\mathbf{t}$ are known) represent linear unrelated column vectors, so the matrix $\mathbf{ss}^{\dagger} - \mathbf{tt}^{\dagger}$ has and has only two nonzero eigenvalues. For example, $\eta_1 > 0$ and $\eta_2 < 0$ can be expressed as [13]:

$$\eta_1 = \|\mathbf{s}\|^2 - c_1|\mathbf{s}^{\dagger}\mathbf{t}|, \eta_2 = \|\mathbf{s}\|^2 - c_2|\mathbf{s}^{\dagger}\mathbf{t}| \tag{21}$$

The corresponding eigenvectors are

$$e_1 = c_3\left(\mathbf{s} + c_1\mathbf{t}e^{i(\pi-\theta)}\right), e_2 = c_4\left(\mathbf{s} + c_2\mathbf{t}e^{i(\pi-\theta)}\right) \tag{22}$$

where $c_3 = 1/\sqrt{\|\mathbf{s}\|^2 + c_1\|\mathbf{t}\|^2 - 2c_1|\mathbf{s}^{\dagger}\mathbf{t}|}$, $c_4 = 1/\sqrt{\|\mathbf{s}\|^2 + c_2\|\mathbf{t}\|^2 - 2c_2|\mathbf{s}^{\dagger}\mathbf{t}|}$, $\mathrm{i} = \sqrt{-1}$, $2c_1|\mathbf{s}^{\dagger}\mathbf{t}| = \|\mathbf{s}\|^2 + \|\mathbf{t}\|^2 - \sqrt{\left(\|\mathbf{s}\|^2 + \|\mathbf{t}\|^2\right)^2 - 4|\mathbf{s}^{\dagger}\mathbf{t}|^2}$, $2c_2|\mathbf{s}^{\dagger}\mathbf{t}| = \|\mathbf{s}\|^2 + \|\mathbf{t}\|^2 + \sqrt{\left(\|\mathbf{s}\|^2 + \|\mathbf{t}\|^2\right)^2 - 4|\mathbf{s}^{\dagger}\mathbf{t}|^2}$, and θ is the angle of the vector $\mathbf{s}^{\dagger}\mathbf{t}$.

4 The power allocation and price selection method

In heterogeneous wireless networks, the source nodes that need to transmit important data will first choose trusted and appropriate relay nodes as cooperative relay partners. Then, according to the preciousness of the power of each relay node (which is reflected by the power price), the source node determines the amount of power consumed by each relay node, and the source node pays for it. On this basis, each relay node needs to dynamically select the best power price according to the dynamic changes of the network environment, so as to obtain the best benefits.

4.1 The power allocation method

We first fix P_s and find the relay power weights that minimize the payment to the relay nodes. Then, we find the value of P_s that minimizes the overall payment U_s of the source node.

Equation (17) can be expressed as

$$\begin{aligned} &\min_{R_s \geq R_s^0} U_s = \nu_s P_s + \sum_{m=1}^{M} \nu_{r_m} P_{r_m} \\ &st\left\{ 4^{R_s^0} = \frac{\sigma^2 + P_s|h_0|^2 + \mathbf{w}_D^{\dagger}\mathbf{R}_h\mathbf{w}_D}{\sigma^2 + P_s|g_0|^2 + \mathbf{w}_D^{\dagger}\mathbf{R}_g\mathbf{w}_D} \right. \end{aligned} \tag{23}$$

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

In order to solve the optimization problem of the above Eq. (23), the optimal power distribution value of the cooperative relay node is solved by assuming that P_s is a constant numerical value. Then, in order to simplify the expression, $\tilde{\mathbf{h}} = \{\frac{h_{r1}}{\sqrt{\nu_{r1}}}, \frac{h_{r2}}{\sqrt{\nu_{r2}}}, \ldots\ldots, \frac{h_{rN}}{\sqrt{\nu_{rN}}}\}$, $\tilde{\mathbf{R}}_h = \tilde{\mathbf{h}}^{\dagger}\tilde{\mathbf{h}}$, $\tilde{\mathbf{g}} = \{\frac{g_{r1}}{\sqrt{\nu_{r1}}}, \frac{g_{r2}}{\sqrt{\nu_{r2}}}, \ldots\ldots, \frac{g_{rN}}{\sqrt{\nu_{rN}}}\}$, $\tilde{\mathbf{R}}_g = \tilde{\mathbf{g}}^{\dagger}\tilde{\mathbf{g}}$, and $\tilde{\mathbf{w}}_D = (\sqrt{\nu_{r1}}w_{r2}, \sqrt{\nu_{r2}}w_{r2}, \ldots\ldots, \sqrt{\nu_{rN}}w_{rN})$. As a result, the optimization problem of Eq. (23) can be further transformed into

$$\begin{aligned} &\min_{R_s \geq R_s^0} U_s = \nu_s P_s + \tilde{\mathbf{w}}_D^{\dagger}\tilde{\mathbf{w}}_D \\ &st\left\{ \tilde{\mathbf{w}}_D^{\dagger}\left(\tilde{\mathbf{R}}_h - 4^{R_s^0}\tilde{\mathbf{R}}_g\right)\tilde{\mathbf{w}}_D = \xi \right. \end{aligned} \tag{24}$$

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

Without loss of generality, the $\xi > 0$ is assumed first, the matrix $\tilde{\mathbf{R}}$ is positive definite, and any eigenvalue of the matrix $\tilde{\mathbf{R}}$ is assumed to be λ. So, the following relational expression can be obtained.

$$\lambda\tilde{\mathbf{w}}_D = \tilde{\mathbf{R}}\tilde{\mathbf{w}}_D \tag{25}$$

By multiplying the left and right sides of the above equation by $\tilde{\mathbf{w}}_D/\lambda$, it can be further obtained

$$\tilde{\mathbf{w}}_D^{\dagger}\tilde{\mathbf{w}}_D = \tilde{\mathbf{w}}_D^{\dagger}\tilde{\mathbf{R}}\tilde{\mathbf{w}}_D/\lambda = \xi/\lambda \tag{26}$$

Since $\xi > 0$ and it is a constant, the optimization problem of minimizing $\tilde{\mathbf{w}}_D^{\dagger}\tilde{\mathbf{w}}_D$ is equivalent to finding the optimization problem of maximizing λ. The largest λ is the largest eigenvalue of the matrix $\tilde{\mathbf{R}}$.Therefore, by Eq. (24), it is possible to know that the optimal $\tilde{\mathbf{w}}_D$ is the eigenvector corresponding to the largest eigenvalue of the matrix $\tilde{\mathbf{R}}$.

On the other hand, if $\xi \leq 0$, that means $P_s \geq \frac{\sigma^2(4^{R_s^0}-1)}{|h_0|^2 - 4^{R_s^0}|g_0|^2}$. For $P_s \geq \frac{\sigma^2(4^{R_s^0}-1)}{|h_0|^2 - 4^{R_s^0}|g_0|^2}$, it means that the source node and destination node can directly achieve the required secrecy rate in the first stage, and it does not need to introduce other relay nodes into collaboration in the second stage. Therefore, this paper does not discuss the absence of cooperative node participation under the $\zeta \leq 0$ condition.

To simplify the representation, $u = \|\tilde{\mathbf{h}}\|^2$ $\nu = 4^{R_s^0}\|\tilde{\mathbf{g}}\|^2$ and $q = 4^{R_s^0}|\tilde{\mathbf{h}}^{\dagger}\tilde{\mathbf{g}}|^2$ are defined first. So it is clear that there is $u\nu - q > 0$. Because of $\tilde{\mathbf{R}}_h = \tilde{\mathbf{h}}\tilde{\mathbf{h}}^{\dagger}$ and $\tilde{\mathbf{R}}_g = \tilde{\mathbf{g}}\tilde{\mathbf{g}}^{\dagger}$, $\tilde{\mathbf{R}}$ can be represented as

$$\tilde{\mathbf{R}} = \tilde{\mathbf{R}}_h - 4^{R_s^0}\tilde{\mathbf{R}}_g \tag{27}$$

According to Lemma 1, $\tilde{\mathbf{R}}$ has only one positive and one negative nonzero eigenvalues. And the positive eigenvalues can be expressed as

$$\lambda = u/2 - \nu/2 + \frac{1}{2}\sqrt{(u+\nu)^2 - 4q} \tag{28}$$

So, $\tilde{\mathbf{w}}_D^{\dagger}\tilde{\mathbf{w}}_D$ can be expressed

$$\tilde{\mathbf{w}}_D^{\dagger}\tilde{\mathbf{w}}_D = \frac{2\xi}{u - \nu + \sqrt{(u+\nu)^2 - 4q}} \tag{29}$$

According to the results of Eqs. (24) and (29), Eq. (17) is converted into

$$\min_{R_s \geq R_s^0} U_s = v_s P_s + \frac{2\xi}{u - v + \sqrt{(u+v)^2 - 4q}} \tag{30}$$

The function $U_s(P_s)$ is a monotonically increasing function of P_s, so the optimization problem for the minimum value of the above equation requires that the value of the P_s is as small as possible. In addition, according to Eq. (8), it must be satisfied

$$R_s^0 = \frac{1}{2} \log\left(\frac{\sigma^2 + P_s \min\left\{ |\eta_1|^2, |\eta_2|^2, \ldots, |\eta_N|^2 \right\}}{\sigma^2 + P_s |g_0|^2} \right) \tag{31}$$

To solve the above equation, the minimum value of P_s is obtained (that is the optimal solution for P_s).

$$P_s^{\min} = \frac{\sigma^2 \left(4^{R_s^0} - 1\right)}{\min\left\{ |\eta_1|^2, |\eta_2|^2, \ldots, |\eta_N|^2 \right\} - 4^{R_s^0} |g_0|^2} \tag{32}$$

In the first stage, $P_s^{\min}$ is the lowest power consumed by the source node to achieve the lowest confidential rate of the selected relay nodes in the presence of eavesdropping nodes. The upper limit of $P_s^{\min}$ is $\frac{\sigma^2(4^{R_s^0}-1)}{|h_0|^2 - 4^{R_s^0}|g_0|^2}$, which corresponds to the situation of $\xi = 0$. This means that communication between the source node and the destination node can directly obtain the required secrecy rate without relying on the selected relay nodes. At this point, the source node needs to reselect other more appropriate relay nodes to participate in collaboration for the secrecy communication, or without the help of the selected cooperative relay nodes. The principle of relay node selection: First, the source node should select the relay nodes which are more favorable to receive the source node information than the eavesdropper node, so as to ensure reliable secrecy rate in the first stage. Secondly, the source node should select the relay nodes that are more conducive to receiving source node information than destination node, so that they can really help the secret communication between source node and destination node.

The above Eq. (29) only gives the optimal solution of $\tilde{\mathbf{w}}_D^{\dagger} \tilde{\mathbf{w}}_D$ and does not give a specific power allocation solution for each cooperative relay node. According to Lemma 1, the power weight of the cooperative relay node r_m can be obtained

$$w_{r_m} = c_3 \left(\frac{h_{r_m}}{v_{r_m}} + c_1 \frac{g_{r_m}}{v_{r_m}} e^{\mathrm{i}(\pi - \theta)} \right) \tag{33}$$

Because of $P_{r_m} = |w_{r_m}|^2$, the power allocation solution of the cooperative relay node r_m is

$$P_{r_m} = \frac{c_3}{v_{r_m}^2} \left| h_{r_m} + c_1 g_{r_m} e^{\mathrm{i}(\pi - \theta)} \right|^2 \tag{34}$$

From the above equation, it can be seen that P_{r_m} is a monotone subtraction function for v_{r_m}.

4.2 The power pricing method for relay

In this section, we will discuss the power price strategy of the relay nodes.

It is noted that Eq. (20) is a noncooperative game between the cooperative relay nodes, and there is a tradeoff between the utility U_{r_m} and the energy price v_{r_m} of the relay nodes. If the relay node r_m has good channel conditions and its energy price is relatively low, the source node will ask for more cooperative power from the relay node r_m, so that U_{r_m} will increase with v_{r_m} growth. When v_{r_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 r_m is dominant. In this way, r_m needs to reduce v_{r_m}, so that the source node will select it, and request more power to participate in collaboration for relaying. Therefore, every relay node r_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 relay nodes, the optimal price will also be influenced by other relay nodes. In addition, when the power cost of cooperative relay 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 nodes' cooperation and power price will rise.

The problem of how to choose the power price of the relay node is discussed in the following. Let $q = \frac{k_{m1}}{v_{r_m}} + l_{m1}$, $u + v = \frac{k_{m2}}{v_{r_m}} + l_{m2}$, and $v = \frac{k_{m3}}{v_{r_m}} + l_{m3}$ and replace them into Eq. (34); it can be obtained

$$P_{r_m} = \frac{\gamma}{v_{r_m}(k_{m1} + l_{m1} v_{r_m})} \tag{35}$$

where $\gamma > 0$ and

$$\gamma = \frac{\left\| 2k_{m1}h_{r_m} + k_{m2}g_{r_m}e^{i(\pi-\theta)} + \left(2l_{m1}h_{r_m} + l_{m2}g_{r_m}e^{i(\pi-\theta)}\right)v_{r_m} - g_{r_m}e^{i(\pi-\theta)}\sqrt{(k_{m2}+l_{m2}v_{r_m})^2 - 4(k_{m1}+l_{m1}v_{r_m})^2} \right\|^2}{2\left[(k_{m2}+l_{m2}v_{r_m})(k_{m3}+l_{m3}v_{r_m}) - 2(k_{m1}+l_{m1}v_{r_m})(k_{m3}+l_{m3}v_{r_m}) + (2k_{m1}-k_{m3}+(2l_{m1}-l_{m3})v_{r_m})\sqrt{(k_{m2}+l_{m2}v_{r_m})^2 - 4(k_{m1}+l_{m1}v_{r_m})^2}\right]} \tag{36}$$

In conjunction with the result of Eq. (35), the substitution of Eq. (20) can be obtained.

$$\max_{0<P_m \le P_{\max}} U_{r_m} = \frac{(v_{r_m} - c_{r_m})\gamma}{v_{r_m}(k_{m1} + l_{m1}v_{r_m})} \tag{37}$$

Because the above objective function is not a concave function, it is difficult to get the optimal solution directly. Therefore, this paper uses the traditional local random search algorithm [28] to obtain numerical solutions. The initial value of v_{r_m} can be obtained by solving Eq. (37) on the condition that γ is constant. That is, the initial value can be obtained for Eq. (37) about finding the first derivative and making it zero.

$$v_{r_m}^{(0)} = c_{r_m} + \sqrt{\frac{c_{r_m}k_{m1}}{l_{m1}} + {c_{r_m}}^2} \tag{38}$$

On the basis of this, the specific algorithm process is as follows: (1) Initialization: initial setting and calculation, such as computing $v_{r_m}^{(0)} = c_{r_m} + \sqrt{\frac{c_{r_m}k_{m1}}{l_{m1}} + {c_{r_m}}^2}$; (2) Recursive computation: first, we generate a random perturbation value ε_i (zero mean Gauss random variable) and then update its power price (if the secrecy rate under $v_{r_m}^{(i-1)} + \varepsilon_i$ is greater than the secrecy rate under $v_{r_m}^{(i-1)}$, $v_{r_m}^{(i)} = v_{r_m}^{(i-1)} + \varepsilon_i$. Otherwise, $v_{r_m}^{(i)} = v_{r_m}^{(i-1)}$); (3) Repeat the step (2) until the stop condition (the number of recursion is reached or the secrecy rate reaches the error requirement) is satisfied.

In addition, for the whole network, the dynamic power pricing and power allocation involve the source node, the destination node, and the numerous relay nodes. This process requires repeated consultations between them. 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 relay nodes. In this case, it requires the source node and all the cooperative relay nodes to negotiate repeatedly through the "the power pricing of each relay node → the power allocation → the power pricing of each relay node → the power allocation of source node" way. After several rounds, it converges to the optimal value while meeting the error requirement.

In the proposed algorithm in this paper, the power allocated by the source node to each cooperative relay node can be directly calculated by Eqs. (29) and (34). The cooperative relay node needs to recursively calculate the power price dynamically based on Eqs. (34), (37), and (38). From the following simulation results, we can see that the five recursive calculations can get very good convergence results. Therefore, the overall computational complexity is very low. From the point of view of the whole network, the changes of network environment, cooperative node center to change, and other factors will lead to the power distribution and power price changes among the cooperative nodes in the whole network. If the scale of the network is too large and the influence range between the cooperative nodes is too large, the whole network will carry out a lot of information exchange and calculation and adjustment. Therefore, the feasible method is to restrict the selection range and number of partners, which will be discussed in the simulation section later.

5 Simulation and result

Under the wireless distributed network scenario, this part simulated many simulations. It includes power allocation, selection of cooperative relay nodes, power pricing, and algorithm convergence in dynamic scenarios. The simulation network model in this paper includes a source node, a destination node, an eavesdropping node,

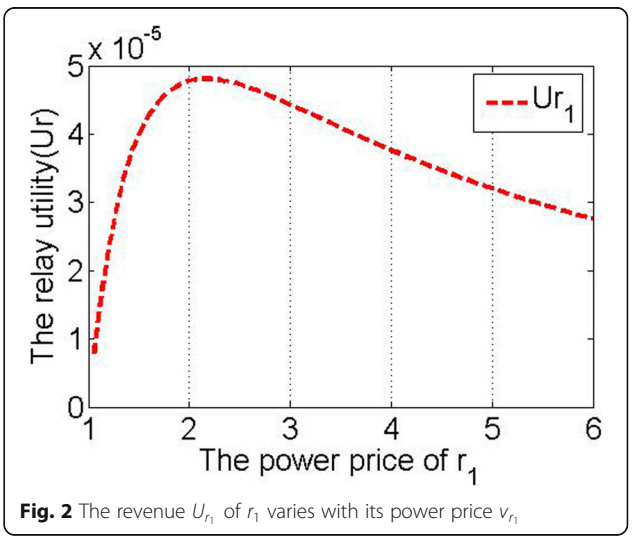

Fig. 2 The revenue U_{r_1} of r_1 varies with its power price v_{r_1}

and several trusted potential relay nodes. In addition, the variation of path loss is used to represent the dynamic characteristics of wireless channel. To illustrate the effect of distance (using the effect of distance to represent the change of the wireless channel information) and the channel model of any point to point is set as a sight line transmission model. The path gain can be expressed as $d^{-c/2}e^{i\theta}$, where d is the distance between any two wireless nodes (unit: meter), $c = 3.5$ is the path loss exponential factor, and θ is a random phase distributed evenly in $[0, 2\pi]$.

In the following simulation, it is assumed that the distance between the cooperative relay nodes is negligible relative to the distance from the source node, destination node, and eavesdropping node. The distance between the cooperative relay nodes to 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^{-10} W. The next simulation in this paper has carried out 1000 Monte Carlo independent experiments and then averages to get the average results.

The above Figure 2 shows that the benefit U_{r_1} of the cooperative relay node r_1 is changed with its power price v_{r_1}. It can be seen from the curve that the maximum value of U_{r_1} exists only.

In Figs. 3 and 4, the cooperative relay node utility function and power price with recursion times and the convergence of the situation are described (The cooperative relay nodes are at point (14, 5), and the eavesdropping node is at point (50, 0)). As it can be seen from the two figures, after four rounds of the dynamic power allocation and the dynamic power price adjustment, the utility function and the power price can quickly converge.

Figure 5 describes the curve of the total payment U_S of the source node that changes with the change of the location of the eavesdropping node (the location of the eavesdropping node moves from point (15, 0) to point (90, 0), and the relay node is fixed at the point (10, 5)). As it can be seen from Fig. 5, the farther the eavesdropping node is from the cooperative relay node, the less the total payment U_S of the source node is.

In Fig. 6, the total payment U_S of the source node changing along with the location of the cooperative relay nodes is described. The location of the cooperative relay nodes changes from point (− 20, 5) to point (32, 5) along a straight line, and the eavesdropping node is at point (50, 0). As it can be seen from Fig. 6, when the cooperative relay nodes are very close to the eavesdropping node, the closer the cooperative relay nodes are to the eavesdropping node, the greater the total U_S of the source node will be. When the relay node is nearest to the eavesdropping node, in order to prevent the eavesdropper from eavesdropping and obtain the same security rate, the power consumption and power price of the cooperative relay node will increase. When the cooperative relay node is far away from the eavesdropper node, the more the cooperative relay node is far away from the destination node, the greater the total U_S of the source node is. This is because the farther the cooperative relay nodes are from the destination node, in order to get the same security rate, the source node will inevitably need

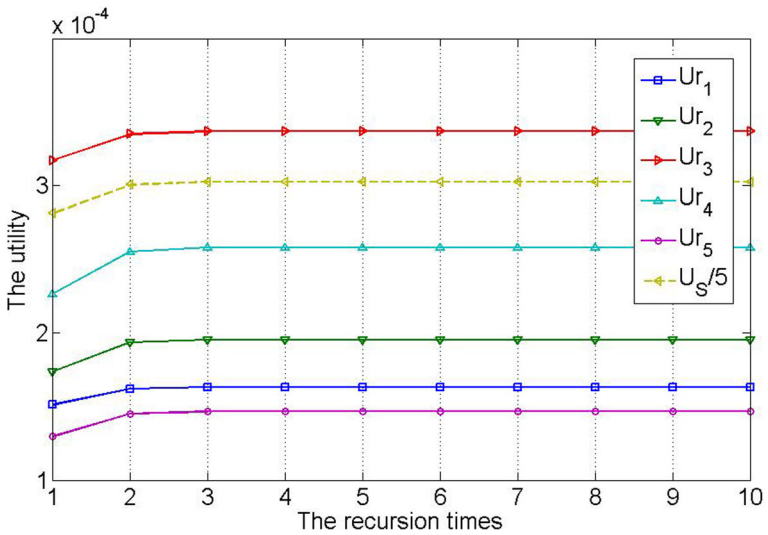

Fig. 3 The utility function gradually converge with the recursion

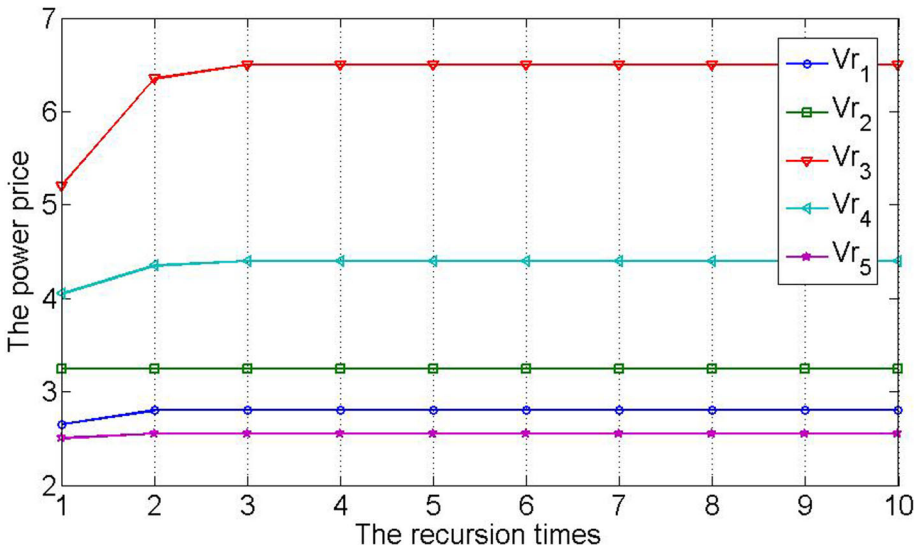

Fig. 4 The power price of the cooperative relay nodes gradually converge with the recursion

to purchase more power to participate in cooperative relay to relay node with higher power price.

The graph represents the source node's choice of cooperative relay nodes in Fig. 7. In the simulation shown in Fig. 7, three trustworthy relay nodes are located at points (10, 5), and the other three trustworthy relay nodes are located at points (30, 5), that is, a total of six relay nodes can be selected for the source node. An eavesdropping node moves along a straight line from point (18, 0) to point (90, 0). In this dynamic process, the source node selects the appropriate relay nodes to participate in cooperation based on the channel characteristics between different nodes (the path loss in this simulation), the power price, and the help of the cooperative transmission (determined by the relative position relationship with the destination node and the eavesdropper node). When the eavesdropping node is located on the left side of the curve turning point (the eavesdropper node is on the point (45, 0)) in Fig. 7, the source node chooses only three relay nodes at the point (10, 5) to participate in collaboration, giving up three relay nodes at point (30, 5). This is because three relay nodes at point (30, 5) are too close to the eavesdropping node. If source node chooses them to participate in cooperative relay transmission, it will not be able to get help. When the eavesdropping node is located on the right side of the curve inflection point (the eavesdropper node is on the point (45, 0)) in Fig. 7, the source node selects all six relay nodes to participate in cooperative transmission. The six relay nodes are far away from the

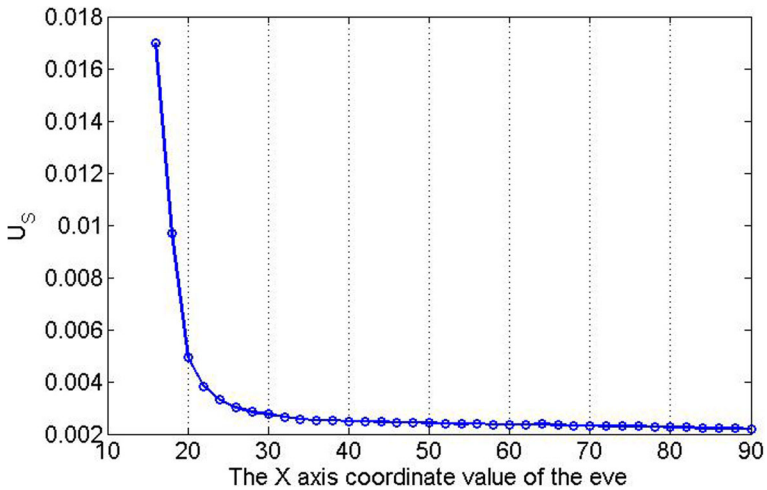

Fig. 5 The source node total payment U_S Vs the location change of eavesdropping node

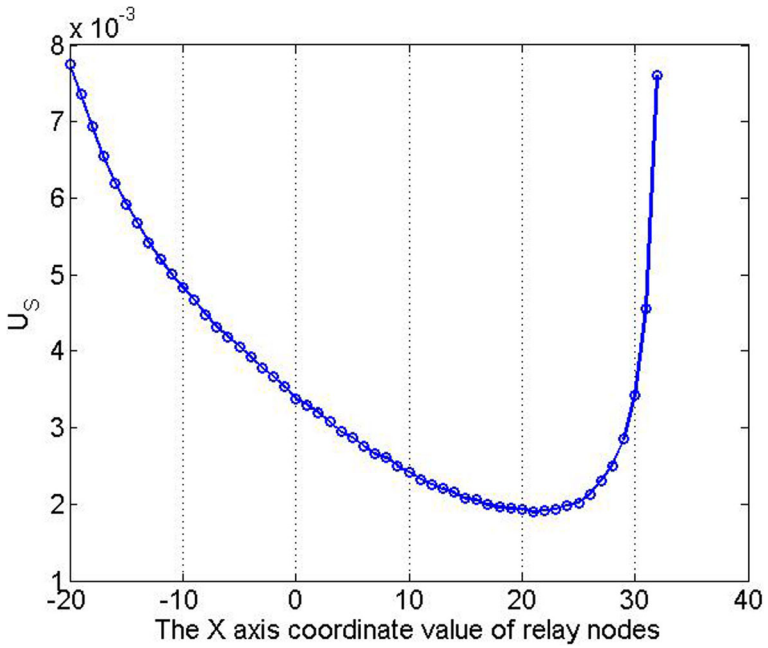

Fig. 6 The source node total payment U_S Vs the location change of cooperative relay nodes

eavesdropping nodes, and their participation in collaboration can help improve the physical layer security and secrecy rate.

Figure 8 describes the curve that the total payment U_S of the source node varies with the number of cooperative relay nodes. The eavesdropping node is fixed at point (50, 0), and the five simulation curves above correspond to the situation where the relay nodes are located at points (– 10, 5), (0, 5), (10, 5), (20, 5), and (30, 5), respectively. It is shown that the total source node payment U_S decreases with the increase of the number of the cooperative relay nodes. This is because the increase of the number of cooperation relay nodes will lead to more intense competition among them. As it is shown in Fig. 9, the increase of

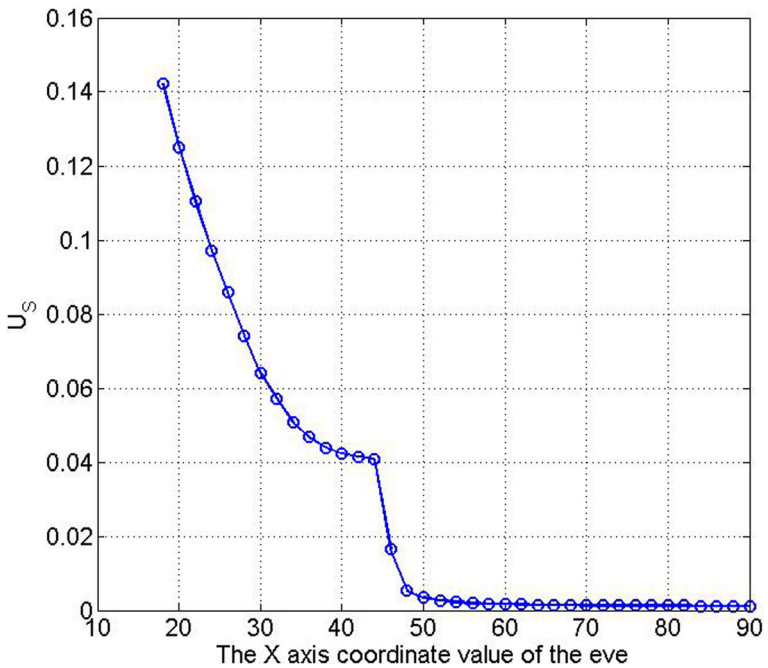

Fig. 7 The cooperative relay selection based on the total payment U_S Vs the location change of eavesdropping node

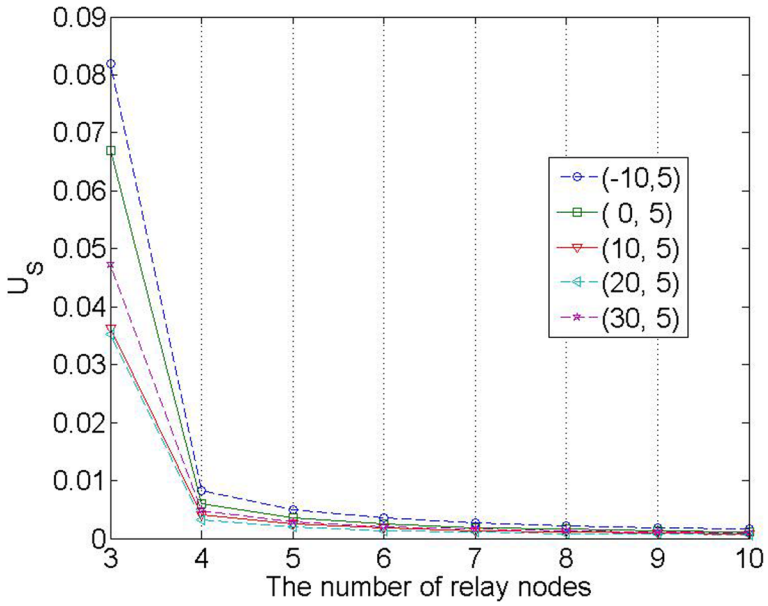

Fig. 8 The total payment U_S of the source node Vs the number of cooperative relay nodes

the number of cooperation relay nodes result in lower power price. Thus, the cost of the source node is inevitably reduced. Therefore, the source node always wants to seek more trustworthy relay nodes to participate in cooperation.

However, from Fig. 8, it can be seen that when the number of relay nodes involved in cooperative beamforming transmission reaches five, the total payment U_S will decrease slowly with the increase of the number of cooperative relay nodes. 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 relay nodes to participate in the cooperative transmission.

Competition among cooperative nodes is conducive to the promotion of each other's reasonable pricing of power, promotes more nodes to participate in the whole network, and promotes a more reasonable node selection and cooperation. This will help each node to find a

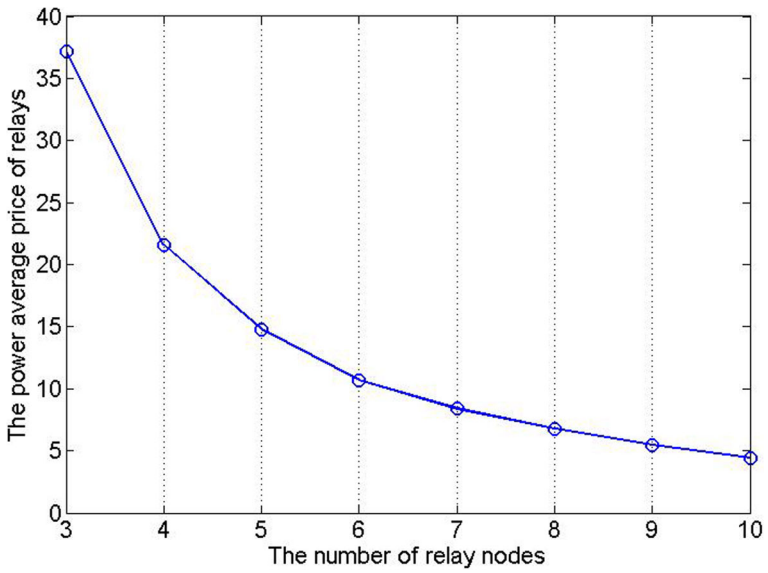

Fig. 9 The average power price of relay nodes Vs the number of cooperative relay nodes

more appropriate collaboration partner in a more appropriate way, in the appropriate scenario, thus improving the overall efficiency.

6 Conclusion

In this paper, third party trustworthy cooperative relay nodes were used to help forward the information of the resource nodes. At the same time, the eavesdropping was avoided by the beamforming technology. In order to reflect the dynamic characteristics of the channel in the wireless heterogeneous network and the dynamic characteristics of the relationship between the wireless nodes, and the dynamic time variation of the power allocation and the selection of the cooperative nodes, the cooperation relationship between the source nodes and the third party trustworthy cooperative relay nodes was modeled as the Stackelberg game. The relationship between relay nodes which are competing and working together was modeled as a noncooperative game. Through these two mutually progressive games, the power allocation between the source node and the cooperative relay nodes would be dynamically adjusted with the channel characteristics and the power price. It also realized the mutual restriction between the cooperative relay nodes for power pricing, and promoted the reasonable pricing of the power price. From the simulation results, it could be seen that the source node can dynamically select trusted cooperative nodes according to the channel characteristics and the power pricing of cooperative relay nodes. Due to the fact that too many cooperative nodes can cause complex channel state and other information interaction, it was suggested that there should be no more than six nodes participating in collaboration.

Acknowledgements

This work was supported by the National Science Foundation of China under Grant No. 61461018, and the Hubei Province colleges and universities in the outstanding youth science and technology innovation team plan (No: T201512).

Authors' contributions

SLH contributed to the conception and algorithm design of the study. QYT and AXJ contributed to the acquisition of simulation. SLH, QYT, AXJ, and SJL contributed to the analysis of simulation data. All authors read 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, high-speed communication, and Internet of Things.

Qiongying Tan received a B.S. degree from Science and Technology College of Hubei Minzu University, Enshi, China, in 2018. She is a master's graduate student in the School of Information Engineering, Hubei University for Nationalities, Enshi, Hubei, China. Her research interests lie in wireless sensor networks, wireless communication information security, Internet of Things, and high-speed communication.

Aixia Jing received a B.S. degree from Hubei University, Wuhan, China, in 2000. She is a librarian in the library of Hubei University for Nationalities, Enshi, Hubei, China. Her research interests lie in big data service mode, library and information retrieval, collaboration mode, and Internet of Things.

Sanjun Liu received M.S. and Ph.D. degrees from the University of 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.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 10 April 2018 Accepted: 7 November 2018
Published online: 27 November 2018

References

1. M. Bloch, M. Barros, M. Rodrigues, S.W. McLaughlin, 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. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975).
4. S.K. Leung-Yan-Cheong, M.E. Hellman, The Gaussian wire-tap channel. IEEE Trans. Inf. Theory **4**, 451–456 (1978).
5. I. Csiszar, J. Korner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**, 339–348 (1978).
6. Y.B. Zhang, H. Dai, A real orthogonal space-time coded UWB scheme for wireless secure communications. EURASIP J. Wirel. Commun. Netw. **2009**, 1–8 (2009). https://doi.org/10.1155/2009/571903.
7. X. Lin, X. Sun, 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.
8. A. Mukherjee, A.L. Swindlehurst, Robust beamforming for security in MIMO wiretap channels with imperfect CSI. IEEE Trans. Signal Process. **59**(1), 351–361 (2011). https://doi.org/10.1109/TSP.2010.2084574.
9. Q. Li, W. Ma, in *IEEE International Conference on Communications, Kyoto*. Multicast secrecy rate maximization for MISO channels with multiple multi-antenna eavesdroppers (2011), pp. 1–5. https://doi.org/10.1109/icc.2011.5963115.
10. Y. Oohama, in *IEEE International Symposium on Information Theory*. Capacity theorems for relay channels with confidential messages (IEEE, Nice, 2007), pp. 926–930. https://doi.org/10.1109/ISIT.2007.4557113.
11. X. He, A. Yener, Cooperation with an untrusted relay: a secrecy perspective. IEEE Trans. Inf. Theory **56**(8), 3807–3827 (2010). https://doi.org/10.1109/TIT.2010.2050958.
12. L. Dong, Z. Han, A.P. 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.
13. L. Jiangyuan, P. Petropulu Athina, W. Steven, On cooperative relaying schemes for wireless physical layer security. IEEE Trans. Signal Process. **59**(10), 4985–4997 (2011). https://doi.org/10.1109/TSP.2011.2159598.
14. S.L. Huang, J.L. Wei, Y. Cao, C. Liu, in *The 7th International Conference on Wireless Communications, Networking and Mobile Computing*. Joint decode-and-forward and cooperative jamming for secure wireless communications (2011). https://doi.org/10.1109/wicom.2011.6040145.
15. J. Huang, A.L. Swindlehurst, Cooperative jamming for seeure communieations in MIMO relay networks. IEEE Trans. Signal Process. **59**(10), 4871–4884 (2011). https://doi.org/10.1109/TSP.2011.2161295.
16. H.M. Wang, Q.Y. Yin, X.G. Xia, Distributed beamforming for physical-layer security of two-way relay networks. IEEE Trans. Signal Process. **60**(7), 3532–3545 (2012). https://doi.org/10.1109/TSP.2012.2191543.

17. J. Chen, R. Zhang, L. Song, et al., Joint relay and jammer selection for secure two-way relay networks. IEEE Trans. Inf. Theory **7**(1), 310–320 (2012). https://doi.org/10.1109/TIFS.2011.2166386.
18. J. Chen, L. Song, Z. Han, et al., in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Houston*. Joint relay and jammer selection for secure deeode-and-forward two-way relay communications (2011), pp. 1–5. https://doi.org/10.1109/GLOCOM.2011.6133875.
19. C. Shahriar, M. La Pan, M. Lichtman, T. Charles Clancy, R. McGwier, R. Tandon, S. Sodagari, J.H. 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.
20. Z. Han, N. Marina, M. Debbah, et al., in *International Conference on Game Theory for Networks*. Physical layer security game: how to date a girl with her boyfriend on the same table ([s. n.], Istanbul, 2009), pp. 287–294. https://doi.org/10.1109/GAMENETS.2009.5137412.
21. Z. Rongqing, S. Lingyang, H. Zhu, in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Improve physical layer security in cooperative wireless network using distributed auction game ([s. n.], Shanghai, 2011), pp. 18–23. https://doi.org/10.1109/INFCOMW.2011.5928805.
22. Q. Zhu, W. Saad, Z. Han, et al., in *Proceedings of the Military Communications Conference Track 1 Waveforms and Signal Processing*. Eavesdropping and jamming in next-generation wireless networks: a game-theoretic approach (2011), pp. 119–124. https://doi.org/10.1109/MILCOM.2011.6127463.
23. W. Saad, Z. Han, T. Basar, M. Debbah, A. Hjrungnes, Hedonic coalition formation for distributed task allocation among wireless agents. IEEE Trans. Mob. Comput. **10**(9), 1327–1344 (2011). https://doi.org/10.1109/TMC.2010.242.
24. R. Zhang, L. Song, H. Zhu, et al., Physical layer security for two-way untrusted relaying with friendly jammers. IEEE Trans. Veh. Technol. **61**(8), 3693–3704 (2012). https://doi.org/10.1109/TVT.2012.2209692.
25. S. Huang, A. Jing, J. Tan, J. Xu, Subcarrier allocation and cooperative partner selection based on nash bargaining game for physical layer security in OFDM wireless networks. Concurr. Comput. **29**(3), 1–15 (2017). https://doi.org/10.1002/cpe.3790.
26. S. Huang, L. Zhu, S. Liu, Based on virtual beamforming cooperative jamming with Stackelberg game for physical layer security in the heterogeneous wireless network. EURASIP J. Wirel. Commun. Netw. **69**, 1–11 (2018). https://doi.org/10.1186/s13638-018-1081-x.
27. G. Owen, *Game theory*, 3rd edn. (Academic, New York, 2001), pp. 120–200.
28. F.J. Solis, R.J.-B. Wets, Minimization by random search techniques. Math. Oper. Res. **6**, 19–30 (1981).