This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

Partner Selection and Incentive Mechanism for Physical Layer Security

Ning Zhang, *Student Member, IEEE,* Nan Cheng, *Student Member, IEEE,* Ning Lu, *Student Member, IEEE,* Xiang Zhang, Jon W. Mark, *Life Fellow, IEEE,* Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—In this paper, we study user cooperation to enhance the physical layer security. Specifically, the source cooperates with friendly intermediate nodes to transmit message securely in the presence of multiple eavesdroppers. We propose a cooperative framework, whereby the source selects multiple partners and stimulates them by granting an amount of reward. First, multiple cooperative relays and jammers are selected by the source using greedy or cross-entropy based approaches. Then, the source and the partners negotiate for the payment and transmission power, which is modeled as a two-layer game. At the top layer, a buyer-seller game is utilized, where the source buys the service provided by the partners. At the bottom layer, all the partners share the reward by determining their transmission powers in a distributed way, which is formulated as a non-cooperative power selection game. By analyzing the game, the partners can determine the transmission powers for cooperation, while the source can select the best payment. To further improve the utility of the source, a set of reward allocation coefficients are introduced and optimized using particle swarm optimization approach. Simulation results are provided to demonstrate the performance of the proposed schemes.**

Index Terms **–Physical layer security, information-theoretic security, relay and jammer selection, incentive mechanism, particle swarm optimization.**

I. Introduction

It is well known that security is of paramount importance for wireless networks due to the inherent openness of the wireless medium, where anyone within the transmission range of the source can receive the message. To protect the transmitted message, encryption/decryption can be adopted, which is usually implemented at upper layers of the protocol stack [1]. However, encryption algorithms could be compromised as the capabilities of the adversaries expand, e.g., when quantum computing is available. Moreover, it is difficult to distribute and manage key materials in a network without infrastructure [2]. As a complement, physical (PHY) layer security, or information-theoretic security, can provide perfect security even though the adversary has unlimited computational power, by means of exploiting the properties of the wireless channel to protect the transmitted signal from being received or decoded by eavesdroppers [3]–[6]. By doing so, the the sequence of bits that are transmitted through physical layer can be guaranteed to be secure, i.e., the eavesdroppers cannot recover the correct bit sequence. Therefore, physical layer security can be leveraged to significantly strengthen the security of the communication system.

The theoretical basis for PHY layer security or information-theoretic security is the well known notion of the perfect secrecy from Shannon [7]. In the pioneer work [3], it is shown that the information with perfect secrecy can be exchanged at a nonzero rate between the source and the destination, while the eavesdropper cannot learn anything, if the channel of eavesdropper is worse than that of the destination. This rate is coined as the *secrecy rate*, and the maximal achievable secrecy rate is refereed to as the *secrecy capacity*. More specifically, suppose that X, Y, and Z are the input of the source, the outputs at the destination and the eavesdropper, respectively. The secrecy capacity can be given by $\max[I(X;Y) - I(X;Z)]$, where $I(\cdot,\cdot)$ is the mutual information. It holds that the secrecy capacity is positive when the channel of eavesdropper is worse than that of the destination. However, when the source-destination channel is worse than the source-eavesdropper channel, the source and destination cannot exchange any secure information since the secrecy capacity is equal to zero under such a scenario.

To address the above issue, user cooperation has been introduced to enhance the secrecy of communications [8]–[14]. In [8], cooperative relaying is leveraged to increase the secrecy rate, either in decode-and-forward (DF) mode or amplify-and-forward (AF) mode. In [9], friendly jammers are employed to jam the eavesdropper by broadcasting artificial noise. In [10], distributed beamforming is performed at relays, where each cooperative node forwards a weighted version of the source's message. By selecting suitable beamforming weights, the secrecy rate can be maximized. In [11], zero-forcing beamforming is employed, whereby the cooperative nodes can create noise to confound the eavesdroppers while protecting the destination from interference. In summary, to improve the secrecy of communication, individual nodes can act as relays or friendly jammers, or collaborate with each other to perform beamforming. However, the existing work relies on the assumption that the users are voluntary to cooperate. Considering that the nodes consume energy during cooperation and have no gain, the assumption might not be suitable in practice. The issue of how to stimulate users to cooperate for security enhancement needs to be studied [15], [16]. Moreover, most of the existing works focus on the power allocation

Manuscript received September 27, 2014; revised January 28, 2015.

N. Zhang, N. Cheng, N. Lu, Jon W. Mark and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, ON N2L 3G1, Canada (e-mail:{n35zhang, n5cheng, n7lu, jwmark, sshen}@uwaterloo.ca).

X. Zhang is with School of Information and Software Engineering, University of Electronic Science and Technology of China, China. Email: zhangx@uestc.edu.cn

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

or weight selection to maximize the secrecy rate and only a few works pay attention on partner selection [17], [18]. However, the work in [17], [18] only considers a single relay or jammer, or multiple relays without jammers, which may not fully exploit the benefits of cooperation. Although there has been a flurry of research activities in this area, the above fundamental issues still need to be further studied.

In this paper, we aim to facilitate cooperation for security, whereby a source selects multiple partners and stimulates them for cooperation by paying an amount of reward to exchange information securely with the destination in the presence of multiple eavesdroppers. To transmit the information securely, the source first selects a set of partners for cooperation, each of which can act as a relay or a jammer[1]. To select suitable partners, i.e., cooperative relays and jammers, two heuristic algorithms are proposed: greedy partner selection and cross-entropy based partner selection. Then, the source stimulates the selected partners for cooperation by paying them for their service, i.e., relaying or jamming. Considering that both the source and the participants are rational and selfish, they are only interested in maximizing their own utilities. Thus, to negotiate the parameters for cooperation, i.e., the payment of the source and the transmission power of the partners, the negotiation process is modeled by a two-layer game. At the top layer, based on the Stackelberg game framework, a buyer-seller game is utilized to model the process that the source pays an amount of reward to buy the service provided by the partners. At the bottom layer, all the partners determine their transmission powers to share the reward of the source in a distributed way, which is formulated as a non-cooperative power selection game. The utility functions of both players are first defined and each player selects the best strategy to maximize its own utility. Then, the existence and the uniqueness of Nash equilibrium (NE) is proved. By analyzing the game, the partners can determine their best transmission powers for cooperation, while the source can select the best payment. To further improve the utility of the source, a set of reward allocation coefficients are introduced. To find the optimal allocation coefficients, particle swarm optimization approach is adopted, where the particles are constructed and moves towards the best solution by iteratively adjusting the movement of particles. Simulation results are provided to validate and show the performance of the proposed algorithms and the incentive mechanism.

In a nutshell, the contributions of this paper are summarized as follows:

1) To the best of our knowledge, there is no existing work to stimulate cooperation for physical layer security enhancement. Based on game-theoretical approach, we propose an incentive mechanism to bridge this gap.
2) Two partner selection algorithms are devised, whereby the source selects multiple relays and jammers to maximize the secrecy rate.
3) The cooperative relays and jammers autonomously select the transmission power to maximize their utilities, which is modeled by a non-cooperative power allocation game. It is proved that there exists a unique pure NE in this game.
4) The source can select the total payment and a suitable allocation coefficient vector to provide incentive for the intermediate nodes such that its utility can be maximized.

[1]We only consider cooperating relays and jammers for simplicity, since collaborative beamforming requires perfect synchronization and information exchange among intermediate nodes

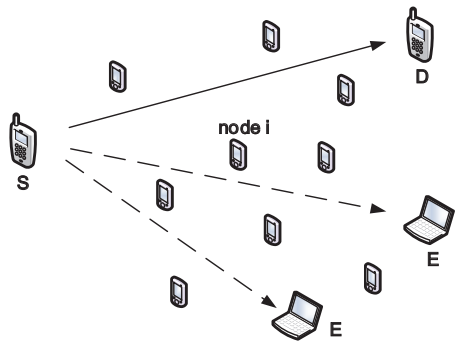


Figure 1. System model.

The remainder of this paper is organized as follows. The system model is presented in Section II. The partner selection and incentive mechanism are given in Section III and Section IV, respectively. The weighted payment allocation approach is presented in Section V. Simulation results are provided in Section VI, followed by the conclusion in Section VII.

II. System Model

As depicted in Fig. 1, the considered system consists of a source (S), a destination (D), M intermediate nodes ($i = 1, 2, ..., M$), and one or multiple eavesdroppers (E) who aim to decode the source's information. It is known that when the channel between S and D is worse than that between S and E, the secrecy rate is zero. To transfer information securely, S requests the intermediate nodes for cooperation, which are all considered friendly[2]. The intermediate node can act as a relay or a friendly jammer and cooperation can be performed in a two-phase fashion. In the first phase, S transmits message to the cooperating relays, which is also overheard by D and E. In the second phase, the cooperative relays employ Amplify-and Forward (AF) protocol to relay the source's message to D to increase the transmission rate at D, while the jammers simultaneously broadcast artificial noise to confound E[3]. To maximize the secrecy rate, the suitable cooperative relays and jammers should be carefully selected by the source.

A slow, flat, block Rayleigh fading environment is considered, where the channel remains static in one time slot and changes independently over different time slots. The channel

[2]The work in [19], [20] consider user cooperation with untrusted nodes.

[3]Please note that certain techniques can also be used to protect the transition in the first phase such as [21], [22]. Since the focus of this work is on partner selection and incentive mechanism design, interested readers can refer to those works.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

coefficients from S to D and S to a specific E are denoted by h_{sd} and h_{se}, respectively. The channel coefficient from S to intermediate node $i \in \mathcal{M}$ is denoted by h_s^i. Similarly, the channel coefficients from intermediate node $i \in \mathcal{M}$ to D and E are h_d^i and h_e^i, respectively. The global CSI is assumed available for the system, including D-related CSI (D-CSI) and E-related CSI (E-CSI), which is a common assumption in PHY layer security literature [8], [10], [12], [13], [23]. E-related CSI (E-CSI) can be obtained in the scenarios where the eavesdroppers are active [4] in the network and their transmission can be monitored [8]. In addition, additive white Gaussian noise is assumed with zero mean and the one-side power spectral density is N_0. Moreover, each node is equipped with a single antenna and communicates with each other in a half-duplex mode.

III. Partner Selection

We use secrecy rate as a measure for secure communication, which is defined as the difference between the transmission rate at D and that at E. In what follows, we will first analyze the secrecy rate through cooperation and then select the suitable partners.

At the destination D, the SNR γ_{sd} from the direct link (S to D) is given by

$$\gamma_{sd} = \frac{P_s \left|h_{sd}\right|^2}{N_0}, \tag{1}$$

where P_s is the transmission power of the source.

Suppose that node i is in the relay set $\mathbb{R}$, then the SNR from relay i using AF cooperative protocol can be given as follows [24]:

$$\gamma_d^i = \frac{1}{N_0} \frac{P_s \left|h_s^i\right|^2 P_i \left|h_d^i\right|^2}{P_s \left|h_s^i\right|^2 + P_i \left|h_d^i\right|^2 + N_0}, i \in \mathbb{R}, \tag{2}$$

where P_i is the transmission power of node i.

Suppose that node j is in the jammer set $\mathbb{J}$, the interference γ_d^j caused by jammer j can be given as follow:

$$\gamma_d^j = \frac{P_j \left|h_d^j\right|^2}{N_0}, j \in \mathbb{J}. \tag{3}$$

The achievable rate at D can be expressed as follows:

$$R_d = \frac{W}{2} \log_2(1 + \frac{\gamma_{sd} + \sum_{i\in\mathbb{R}} \gamma_d^i}{1 + \sum_{j\in\mathbb{J}} \gamma_d^j}). \tag{4}$$

At a generic eavesdropper, e.g., k-th E, the SNR γ_{se} from the source can be given as follows:

$$\gamma_{se} = \frac{P_s \left|h_{se}\right|^2}{N_0}. \tag{5}$$

The SNR γ_e^i from relay i, where $i \in \mathbb{R}$, can be given as follows:

$$\gamma_e^i = \frac{1}{N_0} \frac{P_s \left|h_s^i\right|^2 P_i \left|h_e^i\right|^2}{P_s \left|h_s^i\right|^2 + P_i \left|h_e^i\right|^2 + N_0}, i \in \mathbb{R}. \tag{6}$$

[4]When the eavesdroppers are passive, in order to avoid interfering with the destination, the jammers can create artificial noise which is transmitted in the null space of the channel from the source to destination [10], [11].

The interference γ_e^j caused by jammer j, where $j \in \mathbb{J}$, can be given as follow:

$$\gamma_e^j = \frac{P_j \left|h_e^j\right|^2}{N_0}, j \in \mathbb{J}. \tag{7}$$

Similarly, the achievable rate at the k-th E can be expressed as follows:

$$R_e^k = \frac{W}{2} \log_2(1 + \frac{\gamma_{se} + \sum_{i\in\mathbb{R}} \gamma_e^i}{1 + \sum_{j\in\mathbb{J}} \gamma_e^j}). \tag{8}$$

According to the definition of secrecy rate, the secrecy rate is given by

$$R_{sec}^k = R_d - R_e^k, \tag{9}$$

where R_d and R_e^k are given in (4) and (8), respectively.

Considering the presence of multiple eavesdroppers, the overall secrecy rate R_{sec} is given by

$$R_{sec} = \max\{0, \min_k\{R_d - R_e^k\}\}, \tag{10}$$

where R_e^k is the achievable rate at the k-th eavesdropper.

In the first step, the source selects the cooperative relays and jammers to maximize the secrecy rate, assuming that the transmission power of the potential participants is fixed. This problem can be formulated as follows:

$$\begin{aligned} &\max_{X_{i,j}, \forall i \in \{1,2,...,M\}} \quad R_{sec} \\ \text{s.t.} \quad &\sum_{j\in\{R,J,N_u\}} X_{i,j} = 1, \forall i \in \{1,2,...,M\} \\ &X_{i,j} \in \{0,1\}, \forall i \in \{1,2,...,M\} \text{ and } \forall j \in \{R,J,N_u\} \end{aligned}$$

Specifically, the binary variable $X_{i,j}$ indicates the role of node i, where j can be $\{R, J, N_u\}$, which correspond to act as a relay (R), a jammer (J), or keep silent (N_u). For example, when $X_{i,R} = 1$, node i acts as a relay. The secrecy rate $R_{sec} = \frac{W}{2} \log_2(1 + \frac{\gamma_{sd} + \sum_{i\in\mathbb{R}} \gamma_d^i}{1 + \sum_{j\in\mathbb{J}} \gamma_d^j}) - \frac{W}{2} \log_2(1 + \frac{\gamma_{se} + \sum_{i\in\mathbb{R}} \gamma_e^i}{1 + \sum_{j\in\mathbb{J}} \gamma_e^j})$, where the relay and jammer set can be determined by $\mathbb{R} = \{i, X_{i,R} = 1\}$ and $\mathbb{J} = \{i, X_{i,J} = 1\}$. Exclusive search can obtain the optimal solution. However, the complexity is very high since the search space is exponential to the number of intermediate nodes. Instead, two heuristical algorithms are proposed in the following.

A. Greedy Partner Selection Algorithm

Based on the above formula, a greedy partner selection algorithm is developed, as shown in Algorithm 1. The main idea is to select the best relaying node at each round until the overall secrecy rate cannot be improved.

B. Cross-Entropy based Partner Selection Algorithm

The partner selection problem can also be solved using the Cross-entropy (C-E) method, which is more efficient in searching the optimal solution [25]. In C-E method, "deterministic" optimization problem should be translated into a related "stochastic" optimization problem, where the rare event simulation techniques similar to [26] can be utilized. In other

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

Algorithm 1 Greedy Parter Selection Algorithm

Input: $\mathcal{M}$, $h_s^i, h_d^i, h_e^i, \forall i \in \mathcal{M}$.
Output: Partner selection results $\mathbb{R}$ and $\mathbb{J}$
(**Initialization**): Set $R_{sec} = 0$, $\forall i \in \mathcal{M}$.
for $i \leftarrow 1$ to M **do**
  for $j \in \{R, J, N_u\}$ **do**
    $X_{i,j} = 1$
    Calculate $R_{sec}^{'}$
  end for
  Find the maximum R'_{sec}
  if $R'_{sec} > R_{sec}$ **then**
    $R_{sec} = R'_{sec}$
    $X_{i,j} = arg\max R'_{sec}$
  end if
end for
return $\mathbb{R} = \{i, X_{i,R} = 1\}$ and $\mathbb{J} = \{i, X_{i,J} = 1\}$

Algorithm 2 C-E Partner Selection Algorithm

Input: $\mathcal{M}$, T, Z, ρ, $h_s^i, h_d^i, h_e^i, \forall i \in \mathcal{M}$.
Output: Partner selection results $\mathbb{R}$ and $\mathbb{J}$
(**Initialization**): Set $R_{sec} = 0$ and $p_{j,t}^i = 1/3, j \in \{R, J, N_u\}$, $\forall i \in \mathcal{M}$.
for $t \leftarrow 1$ to T **do**
  for $z \leftarrow 1$ to Z **do**
    for $i \leftarrow 1$ to M **do**
      Generate samples of the strategy vector.
    end for
  end for
  for $z \leftarrow 1$ to Z **do**
    Calculate the utilities $U(z)$ according to (9).
  end for
  Order the utilities $U(z)$ in a nonincreasing manner.
  for $i \leftarrow 1$ to M **do**
    for $j \leftarrow \{R, J, N_u\}$ **do**
      Update $\mathbb{P}_t^i$ using (14)
    end for
  end for
end for
return $\mathbb{R} = \{i, p_{R,T}^i = 1\}$ and $\mathbb{J} = \{i, p_{R,J}^i = 1\}$

words, the main idea behind the C-E method is to define for the original optimization problem an associated stochastic problem (ASP) and then efficiently solve the ASP by an adaptive scheme. It sequentially generates random solutions which converge stochastically to the optimal or near-optimal one.

Typically, the C-E method involves an iterative procedure where each iteration comprises of the following two phases: i) Generate a random data sample according to a specified stochastic policy; ii) Update the stochastic policy based on the outcome of the sample to produce a "better" sample in the next iteration.

C-E algorithm: Algorithm 2 represents the detailed procedure of channel selection, which consists of five main steps as follows.

Define the strategy space $\mathbb{S}$ for all the intermediate nodes as follows:

$$\mathbb{S} := \{R, J, N_u\}. \tag{11}$$

The probability vector associated with the strategy space is given as follows:

$$\mathbb{P}_t^i := \{p_{R,t}^i, p_{J,t}^i, p_{N_u,t}^i\}, \sum_{j \in \{R,J,N_u\}} p_{j,t}^i = 1, \tag{12}$$

where $\mathbb{P}_t^i$ denotes the stochastic policy of node i on the strategy space $\mathbb{S}$ at t-th iteration, and $p_{j,t}^i$ denotes the probability that node i chooses strategy j at t-th iteration.

1) (Initialization). Set the iteration counter $t := 1$. Set the initial stochastic policy $\mathbb{P}_0^i$ of all SUs to be the uniform distribution on the strategy space $\mathbb{S}$. In other words, for each intermediate node, it picks the strategy from the strategy space uniformly, with equal probability $1/3$.
2) (Generation samples). Based on the initial stochastic policy of all nodes, the Z samples of the strategy vector are generated, which can be given as follows:

$$\mathbb{S}^i(z) := \{I_R^i(z), I_J^i(z), I_{N_u}^i(z)\}, \tag{13}$$

where $\mathbb{S}^i(z)$ is the z-th strategy vector of node i with only one element to be "1" and the rest are "0". The probability for I_j^i to be "1" is $p_{j,t}^i$.
3) (Performance evaluation). Substitute the samples into (11) to calculate the utilities $U(z)$. Arrange the $U(z)$ in a nonincreasing order according to the values, i.e., $U^1 > U^2 > ... > U^Z$. Let υ be the $(1-\rho)$ sample quantile of the performances: $\upsilon = U_{\lceil (1-\rho)Z \rceil}$, where $\lceil \cdot \rceil$ is the ceiling function.
4) (Stochastic policy update). Based on the same sample, calculate $\mathbb{P}_t^i := \{p_{R,t}^i, p_{J,t}^i, p_{N_u,t}^i\}$, using the following equation:

$$p_{j,t}^i = \frac{\sum_{z=1}^{Z} X_{U^n \geq \upsilon} I_j^i(z) = 1}{\sum_{z=1}^{Z} X_{U^z \geq \upsilon}}, \tag{14}$$

where $X_{U^z \geq \upsilon}$ is defined as follows:

$$X_{U^z \geq \upsilon} = \begin{cases} 1 & U^z \geq \upsilon \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

5) If the stopping criterion is met (e.g., the maximum iteration number is reached), stop; otherwise increase the iteration counter t by 1, and reiterate from step 3.

Theorem 1: For the given number of intermediate nodes M, the time complexity of the proposed greedy and C-E algorithm is polynomial in M.

IV. Incentive Mechanism for Cooperative Secure Communications

To motivate the intermediate nodes to participate in cooperation for security enhancement, the source announces an amount of reward to all the participants. Then, given the announced reward, all the participants, which is competitive with each other, maximize their utilities by determining the transmission power for cooperation. This process is modeled as a two-layer game, which can be illustrated in Fig. 2. At the top layer, a buyer-seller game is utilized to model the payment selection process, based on the framework of two-stage Stackelberg game. At the bottom layer, all the partners share the reward by determining their transmission

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

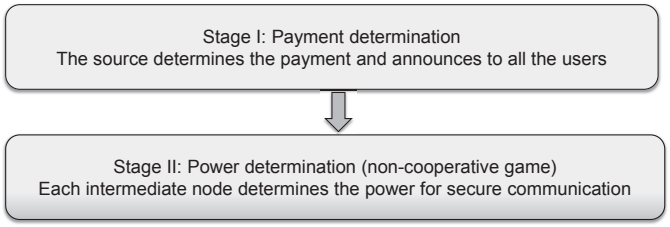


Figure 2. Two-layer game for the incentive mechanism.

powers in a distributed way, which is formulated as a non-cooperative power selection game. By analyzing the game, the best payment and transmission power can be determined. In the following, we first define the utilities of players and then analyze the game to find the best strategies for the players.

A. Utility Functions

The utility of the source node is given by

$$U_s = \lambda_1 R_{sec} - R_m \tag{16}$$

where λ_1 is the profit per secrecy rate, while $0 \leq R_m \leq R_{max}$ is the payment it grants to the cooperative relays and jammers.

The cooperative relays and jammers share the payment according to their contribution to the secrecy rate. In other words, the payment the cooperative participant can obtain is proportional to the contribution it makes in the cooperation. Since the relay is leveraged to increase the perfect secrecy of the relaying link compared with that of the eavesdropper link, the contribution for relay i can be approximately given by $\frac{P_i|h_d^i|}{|h_e^i|}$. While the jammer is leveraged to increase more artificial noise at eavesdropper than at the destination node, the contribution for the jammer j can be approximately given by $\frac{P_j|h_e^j|}{|h_d^j|}$.

The utility of the selected node i is given by

$$U_i = \frac{P_i r_i}{\sum_{j\subseteq\mathbb{C}} P_j r_j} R_m - \lambda_2 P_i. \tag{17}$$

where $\mathbb{C} := \mathbb{R} \uplus \mathbb{J}$ is the set of selected nodes with the size N, λ_2 is the cost rate for transmission power, and the contribution factor r_i is defined as follows:

$$r_i = \begin{cases} \frac{|h_d^i|}{|h_e^i|}, & i \in \mathbb{R} \\ \frac{|h_e^i|}{|h_d^i|}, & i \in \mathbb{J} \end{cases} \tag{18}$$

As a two-stage game, the buyer-seller game can be analyzed by the backward induction method. First, the optimal strategies (i.e., the transmission powers) of the partners are analyzed, assuming the strategy of the source node (i.e., the payment) is fixed. Second, based on the results of the first step, the source node decides the optimal strategy, being aware of the effects of its decision on the strategies selected by the partners. By doing so, the best strategies of both the source node and the partners are obtained such that the corresponding utilities can be maximized.

B. No-cooperative Power Selection game

In order to stimulate cooperation of the intermediate nodes, the source pays rewards for their service. Each intermediate node gets a certain amount of rewards according to its contribution in the service. For a given reward, each cooperative node tries to maximize its own utility by selecting a suitable transmission power, which is modeled as a non-cooperative power selection game. In the following, we will analyze this game to find the best power selection strategies, which constitute a Nash equilibrium (NE)

***Definition** 1:* Non-cooperative power selection game is defined by $G = \{\mathbb{C}, \{\mathbb{S}_i\}, \{U_i\}\}$, where $\mathbb{C}$ is the set of players, $\mathbb{S}_i$ is the strategy set of node i, and U_i is the utility function of node i.

Note that $\mathbb{S}_i$ is the transmission power that node i can choose and the utility function of node i is given by (17).

***Theorem** 2:* There exists an NE in the non-cooperative power selection game $G = \{\mathbb{C}, \mathbb{S}_i, \{U_i\}\}$.

***Proposition** 1:* An NE exists in the non-cooperative power selection game $G = \{\mathbb{C}, \{\mathbb{S}_i\}, \{U_i\}\}$, if for all node $i \in \mathbb{C}$: i) S_i is a nonempty, convex, and compact subset of some Euclidean space R^N; and ii) U_i is continuous in P and concave in P_i, where P is the set of $P_i, i \in \mathbb{C}$.

The strategy space $\mathbb{S}_i$ is defined as the transmission power $0 \leq P_i \leq P_{max}$. Therefore, the strategy space is a nonempty, convex, and compact subset of some Euclidean space R^n.

Since the utility U_i is given by

$$U_i = \frac{P_i r_i}{\sum_{j\subseteq\mathbb{C}} P_j r_j} R_m - \lambda_2 P_i. \tag{19}$$

which is continuous in P. Taking the first derivative of U_i with respect to P_i yields

$$\frac{\partial U_i}{\partial P_i} = \frac{r_i R_m \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} - \lambda_2 \tag{20}$$

Then, taking the second derivative of U_i with respect to P_i, we have

$$\frac{\partial^2 U_i}{\partial^2 P_i} = -2\frac{{r_i}^2 R_m \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^3} < 0 \tag{21}$$

The second derivative of U_i with respect to P_i is always negative, which means U_i is concave in P_i. Therefore, the non-cooperative power selection game G exists an NE.

***Theorem** 3:* The non-cooperative power selection game G has a unique NE.

***Definition** 2:* A weighted sum of $U_i(P)$ is given by $\sigma(P,\mu) = \sum_{i=1}^{N} \mu_i U_i(P)$, where $\mu = \{\mu_1, \mu_2, ..., \mu_N\}$ with $\mu_i \geq 0$ and $P = \{P_1, P_2, ...P_i, ...P_N\}$. The pseudogradient of $\sigma(P,\mu)$ is defined by $\varphi(P,\mu)$, which is given by

$$\varphi(P,\mu) = \begin{bmatrix} \mu_1 \nabla_1 U_1(P) \\ \mu_2 \nabla_2 U_2(P) \\ \vdots \\ \mu_N \nabla_N U_N(P) \end{bmatrix} \tag{22}$$

Define $\Psi(P,\mu)$ to be the Jacobian matrix of $\varphi(P,\mu)$ with respect to P.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

***Proposition** 2:* If $\sigma(P,\mu)$ is diagonally strict concave in P for some positive μ, the non-cooperative power selection game has a unique Nash equilibrium [27].

***Proposition** 3:* $\sigma(P,\mu)$ is diagonally strict concave if the symmetric matrix $[\Psi(P,\mu),\Psi'(P,\mu)]$ is negative definite for P [27].

***Proposition** 4:* The symmetric matrix $[\Psi(P,\mu),\Psi'(P,\mu)]$ is negative definite for P if the following conditions are satisfied: i) $U_i(P)$ is concave with respect to P_i; ii) $U_i(P)$ is convex with respect to P_i^-, where P_i^- is the transmission power of other nodes rather than node i; iii) $\sigma(P,\mu)$ is concave with respect to P for some positive μ [27].

According to above propositions 2, 3 and 4, we only need to prove the proposition 4 to have the theorem 2. For proposition 4, we have already proved that $U_i(P)$ is concave with respect to P_i. Next, we will prove that $U_i(P)$ is convex with respect to P_i^-. Taking the first derivative of $U_i(P)$ with respect to P_j, $j \neq i$, yields

$$\frac{\partial U_i}{\partial P_j} = -\frac{r_i R_m r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} \tag{23}$$

The second derivative of $U_i(P)$ with respect to P_j ($j \neq i$) is given by

$$\frac{\partial^2 U_i}{\partial^2 P_j} = \frac{2 r_i R_m r_j^2}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^3} > 0 \tag{24}$$

Therefore, $U_i(P)$ is convex with respect to P_i^-. According to the rule that $\frac{\partial \sum_i f(x)}{\partial x} = \sum_i \frac{\partial f(x)}{\partial x}$, based on (21) and (33), the second derivative of $\sigma(P,\mu)$ with respect to P_i is given by

$$\begin{aligned}\frac{\partial^2 \sigma(P,\mu)}{\partial^2 P_i} = \mu_i \frac{-2{r_i}^2 R_m \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^3} \\ + \sum_{j\neq i, j\subseteq\mathbb{C}} \mu_j \frac{2 r_j R_m r_i^2}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^3}\end{aligned} \tag{25}$$

It is obvious that for some positive μ, $\frac{\partial^2 \sigma(P,\mu)}{\partial^2 P_i} > 0$. Then, it applies that $\sigma(P,\mu)$ is concave with respect o P for some positive μ. Therefore, the non-cooperative power selection game has a unique NE.

Since U_i is concave with respect to P_i, the best response correspondence can be obtained by setting the first derivative of U_i with respect to P_i to 0, as follows:

$$\frac{\partial U_i}{\partial P_i} = -\frac{-r_i R_m A_i + \lambda_2 {A_i}^2 + 2\,\lambda_2 A_i P_i r_i + \lambda_2 {P_i}^2 {r_i}^2}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} = 0 \tag{26}$$

where $A_i = \sum_{j\neq i, j\subseteq\mathbb{C}} w_j P_j r_j$. By solving it, the solutions are given by (27).

The detailed procedure can be found in the Appendix-A.

By solving the equations set (26), we can find the unique equilibrium as follows:

$$P_i^* = [\min\{\frac{R_m r_i B_i}{\lambda_2 (r_i + B_i)^2}, P_{max}\}]^+ \tag{28}$$

where $B_i = \frac{(N-1) r_i}{\sum_{j=1}^{N} \frac{r_i}{r_j} - N + 1}$. The detailed procedure can be found in the Appendix-B.

C. Source Node Utility Maximization

Based on the analytical results of the power selection game, the source determines its strategy (the payment) to maximize its utility, aware of the effects of its strategy on the results of the power selection game. It can be formulated as the following problem:

$$\begin{aligned}\max_{R_m} \;\; & U_s = \lambda_1 R_{sec} - R_m \\ s.t. \;\; & 0 \leq R_m \leq R_{max}.\end{aligned} \tag{29}$$

where R_{sec} is obtained when the partners adopt the transmission power given by (28), which is a function of R_m. Therefore, the utility function of the source becomes a function of one single parameter R_m. To find the best R_m, the classical approach is to get the extremum by setting the first derivative of U_s with respect to R_m equal to 0 and then compare the extremum with the boundary to find the best payment R_m^*. Finally, we can obtain the best strategy of partners by substituting R_m^* into (28).

V. Weighted Payment Allocation Approach

In the previous section, the source can only determine the amount of payment to the cooperative partners. To further improve the utility of the source, it can actively affect the way how the partners share the payment by means of introducing a set of weights for the partners, which are relevant to the CSI of the partners. Specifically, the source introduces the weights $W := \{w_1, w_2, ..., w_i, ..., w_N\}$ as the allocation coefficients, associated with the selected nodes, where N is the total number of selected nodes for cooperation, $0 \leq w_i \leq 1$ is the allocation coefficient for node i and $\sum_i w_i = 1$. With the allocation coefficient posed by the source, the interaction between the source and intermediate nodes are modeled using a similar game as before.

A. Utility Functions

The utility function of the source node is the same as before, which is given as follows:

$$U_s = \lambda_1 R_{sec} - R_m. \tag{30}$$

Different from the previous case, the utility of the cooperative node i is given by

$$U_i = \frac{P_i w_i r_i}{\sum_{j\subseteq C} P_j w_j r_j} R_m - \lambda_2 P_i. \tag{31}$$

where w_i is the payment allocation coefficient for node i and r_i is the contribution factor defined in (18).

B. Non-cooperative Power Selection Game

Given the payment R_m and the allocation coefficients $W := \{w_1, w_2, ..., w_i, ..., w_N\}$, the selected nodes determine their own strategies, i.e., the transmission power, to maximize their utilities, given by (31).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

$$P_i^*(P_i^-) = \begin{cases} 0 & \text{if } \sum_{j\neq i, j\in\mathbb{C}} P_j r_j \geq \frac{R_m P_i r_i}{\lambda_2} \\ \frac{1}{r_i}(\sqrt{\frac{R_m P_i r_i A}{\lambda_2}} - A) & \text{if } \sum_{j\neq i, j\in\mathbb{C}} P_j r_j < \frac{R_m P_i r_i}{\lambda_2} \text{ and } \frac{1}{r_i}(\sqrt{\frac{R_m P_i r_i A}{\lambda_2}} - A) < P_{max} \\ P_{max} & \text{otherwise} \end{cases} \quad (27)$$

Taking the first derivative of U_i with respect to P_j, $j \neq i$, yields

$$\frac{\partial U_i}{\partial P_j} = -\frac{w_i r_i R_m w_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} w_j P_j r_j\right)^2} \quad (32)$$

The second derivative of U_i with respect to P_j ($j \neq i$) is given by

$$\frac{\partial^2 U_i}{\partial^2 P_j} = \frac{2 w_i r_i R_m (w_j r_j)^2}{\left(\sum_{j\subseteq\mathbb{C}} w_j P_j r_j\right)^3} > 0 \quad (33)$$

Similar to the proof for the existence of NE and the uniqueness in the previous case, the new power allocation game can be proved to have a unique NE.

Since U_i is concave with respect to P_i, the best response correspondence can be obtained by setting the first derivative of U_i with respect to P_i equal to 0, i.e., $\frac{\partial U_i}{\partial P_i} =$

$$-\frac{-w_i r_i R_m A_i + \lambda_2 {A_i}^2 + 2\,\lambda_2 A_i w_i P_i r_i + \lambda_2 {w_i}^2 {P_i}^2 {r_i}^2}{\left(\sum_{j\subseteq\mathbb{C}} w_j P_j r_j\right)^2} = 0$$

where $A_i = \sum_{j\neq i, j\subseteq\mathbb{C}} w_j P_j r_j$.

By solving the equations set (34), we can find the unique equilibrium as follows:

$$P_i^* = [\min\{\frac{R_m w_i r_i B_i}{\lambda_2 (w_i r_i + B_i)^2}, P_{max}\}]^+ \quad (34)$$

where $B_i = \frac{(N-1) w_i r_i}{\sum_{j=1}^{N} \frac{w_i r_i}{w_j r_j} - N + 1}$.

C. Source Node Utility Maximization

In the previous section, we present how the weight coefficient W affects the power allocation of the cooperative partners, as shown in (34). Different transmission power selection in turn changes the utility function of the source. Therefore, there exists an implicit relationship between the utility function U_s and the weight coefficient W. In this section, we aim to find the optimal W such that U_s can be maximized, which can be formulated as the following optimization problem:

$$\begin{aligned} &\max_{w_1, w_2, \ldots, w_N} U_s \\ s.t.\ \ &0 \leq w_i \leq 1, i = 1, 2, ..., N \\ &\sum_i w_i = 1 \end{aligned} \quad (35)$$

Since it is difficult to derive an explicit equation to express the relation between U_s and W, regular optimization methods may not be applicable. Bio-inspired and swarm intelligence optimal method, as an important branch of optimization theory, provides an effective way to address such complex problems. Genetic algorithm (GA) is the most successful one in this area and has been applied to solve many practical problems. However, due to the inherent encoding structure and iteration rule, GA is not appropriate for continuous variable optimization. In this section, we adopt a relatively new swarm intelligence method, named Particle Swarm Optimization (PSO) to solve the above problem [28], [29]. Compared with GA, PSO has better global searching ability, especially in the continuous space, and a local searching ability near the end of the run.

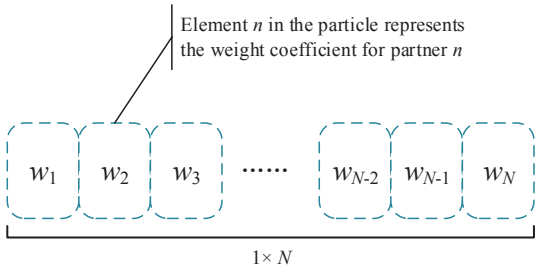


Figure 3. The structure of particle.

The standard PSO algorithm typically involves the following steps: 1) Construct particle structure to map the solution of interest problem; 2) Create initial topology for particle swarm and parameters; 3) Evaluate fitness value of each particle; 4) Update particle position; 5) Repeat step (2) to (4) until the solution satisfies the terminating condition.

Following this framework, we first construct a root particle $\textbf{particle}_{\text{root}}$, as shown in Fig. 3. The n-th element of $\textbf{particle}_{\text{root}}$ indicates the allocation coefficient for n-th partner (i.e., w_n). In other words, $\textbf{particle}_{\text{root}}$ implies an initial allocation, as well as a start point for the optima searching. In this paper, an equal weight distribution strategy are adopoted, i.e. $\textbf{particle}_{\text{root}}(n) = 1/N$.

Based on the given $\textbf{particle}_{\text{root}}$, we initialized the particle swarm with the size of N^{PSO}. The i-th particle can be expressed as an N-dimensional vector $\textbf{particle}_i$ and denote its n-th element by $\textbf{particle}_i(n)$, which is given as follows:

$$\textbf{particle}_i(n) = \textbf{particle}_{\text{root}}(n) + \omega, \quad (36)$$

where ω follows the uniform distribution in $[-\textbf{particle}_{\text{root}}(n), 1 - \textbf{particle}_{\text{root}}(n)]$.

$$\textbf{particle}_i(n) = \frac{\textbf{particle}_i(n)}{\sum_n \textbf{particle}_i(n)}, \forall i \in [1, N^{\text{PSO}}], n \in [1, N] \quad (37)$$

The fitness value of the i-th particle is denoted as $\textbf{Fitness}_i$, which actually is the utility of the source. In other words, $\textbf{Fitness}_i$ is the utility function U_s of the source that can be obtained by using (16). Fig. 4 illustrates the process for calculating the fitness for a given particle. In addition, denote by $\textbf{particle}^{\text{Gopt}}$ the global best particle of the swarm, i.e.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

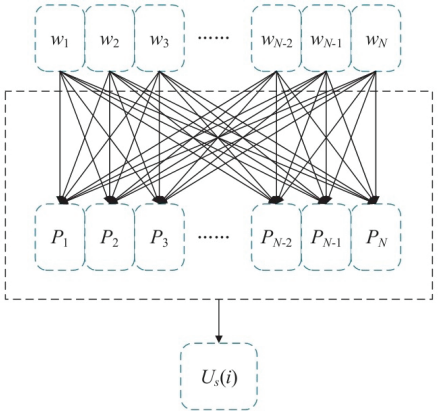


Figure 4. Illustration of calculating the fitness for a given particle.

the particle with the highest fitness value $Gopt$; denote by $\mathbf{particle}_i^{\text{Gopt}}$ the best historical position of i-th particle with the corresponding fitness value Popt_i. The position variation for i-th particle is denoted as $\mathbf{velocity}_i^t$. At the t-th iteration, the particle position can be updated by the following equations:

$$\mathbf{velocity}_i^{t+1} = \lambda(\mathbf{velocity}_i^t + c\gamma_1(\mathbf{Pparticle}_i^t - \mathbf{particle}_i^t) + c\gamma_2(\mathbf{Gparticle}^t - \mathbf{particle}_i^t)) \quad (38)$$

$$\mathbf{particle}_i^{t+1} = \mathbf{particle}_i^t + \mathbf{velocity}_i^t \quad (39)$$

where λ is the inertia coefficient in PSO algorithm and the random variables γ_1 and γ_2 are uniformly distributed within [0,1]. In this paper, these parameters are set as follows:

$$\lambda = \frac{1}{|1 - c - \sqrt{c^2 - 2c}|} \quad (40)$$

where $c = 2.05$ and $\lambda = 0.729$. Algorithm 3 represents the detailed procedure of the PSO based weight selection.

Algorithm 3 PSO based weight selection algorithm

Input: Number of partners, number of particle swarm N^{PSO}
Output: Weight Coefficient W
// **Step1: Initialization**
Generate root particle $\mathbf{particle}_{\text{root}}$ with equal weight distribution,
for $i \leftarrow 1$ to N^{PSO} **do**
  Generate searching particle $\mathbf{particle}_i$
end for
// **Step2: Find particle$^{\text{Gopt}}$,** $Gopt$
Calculate the $\mathbf{Fitness}_i$ of source node, $i = 1, 2, ..., N^{\text{PSO}}$
Find the global best $\mathbf{particle}^{\text{Gopt}}$ and $Gopt$
Find the local best $\mathbf{particle}_i^{\text{Gopt}}$ and Popt_i
// **Step3: Update**
for $i \leftarrow 1$ to N^{PSO} **do**
  Update $\mathbf{particle}_i$ using (38) and (39)
  Run Step 2
  if $\mathbf{particle}^{\text{Gopt}}$ and $\mathbf{particle}_i^{\text{Gopt}}$ stay unchanged **then**
    Stop
  else
    Continue
  end if
end for
Return $\mathbf{particle}^{\text{Gopt}}$

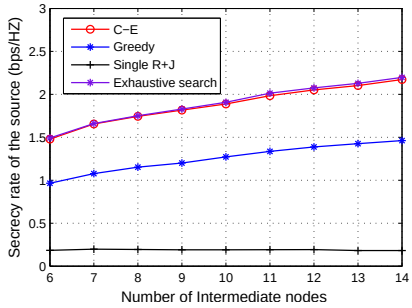


Figure 5. Comparison among different partner selection algorithms.

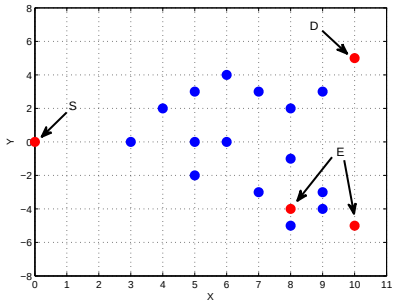


Figure 6. The network scenario for simulation.

VI. Simulation Results

In this section, simulation results are provided to evaluate the performance of the proposed scheme. The simulation is set up as follows. In a 1 km$\times$ 1 km area, the source, the destination, and two eavesdroppers are located at the origin, (1 km, 0.5 km), (1 km, -0.5 km), and (0.8 km, -0.4 km), respectively, while a set of nodes are located in between. The maximum transmission power of all nodes are set to 10 W, while the noise power is set to -70 dB. The average power gains between nodes is calculated by the path loss with exponent $\mu = 3.5$.

To evaluate the average performance of the proposed partner selection algorithms with respect to the number of intermediate nodes, Monte Carlo simulation is carried out, which consists of 500 trials. At each trial, a number of intermediate nodes are uniformly distributed in the area. Fig. 5 shows the average secrecy rate using the exhaustive search algorithm, the proposed greedy algorithm, C-E algorithm, and single relay and jammer selection algorithm in [17]. The exhaustive search algorithm has the best performance and it provides a performance benchmark. It can be seen that the C-E algorithm can achieve almost the same performance as the exhaustive search algorithm does. Moreover, it can be seen that the proposed algorithms can achieve higher secrecy rate, compared with the single relay and jammer selection algorithm. This is because they can fully exploit the benefits of cooperation by leveraging multiple relays and jammers.

In the following simulation, we validate the incentive mechanism in the network scenario, as shown in Fig. 6. The source, destination, eavesdroppers are fixed at the same location as before, while 15 intermediate nodes are distributed at the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

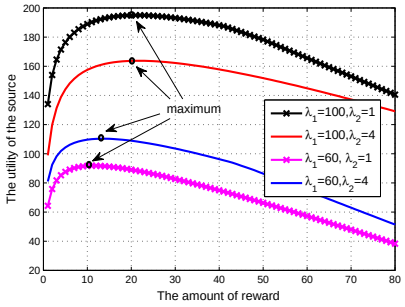


Figure 7. Utility of the source versus the amount of rewards.

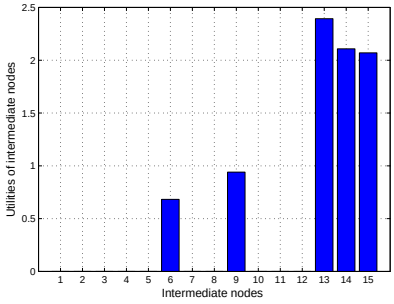


Figure 8. Utilities of intermediate nodes averaged over fading when $\lambda_1 = 60$ and $\lambda_2 = 1$.

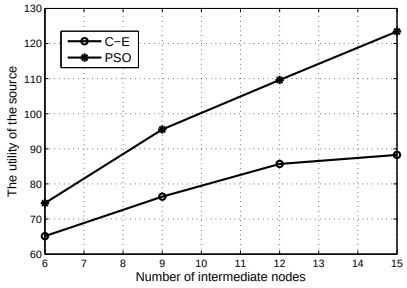


Figure 9. Utilities of the source with PSO when $\lambda_1 = 100$ and $\lambda_2 = 1$.

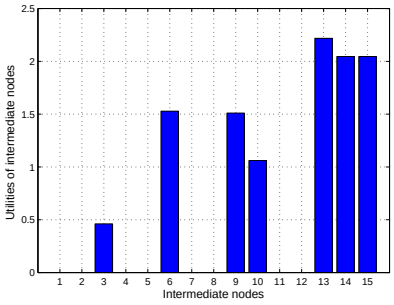


Figure 10. Utilities of intermediate nodes averaged over fading using PSO when $\lambda_1 = 60$ and $\lambda_2 = 1$.

locations marked in the figure. The source can choose the reward from the range between 0 and 100. Fig. 7 shows the utility of the source, averaged over fading distribution, versus the amount of reward, for different λ_1 and λ_2. It can be seen that the overall utility first increases and then decreases as the reward increases. The reason is that, at the beginning, with increasing reward, the partners are willing to devote more transmission power during cooperation, which leads to an increase in the secrecy rate. However, when the reward keeps rising, the cost also increases, which will lower the overall utility. It can also be seen that there exists an optimal value of the reward, with which the utility can be maximized. It can also be seen that a larger λ_1 leads to a greater utility and payment because the source node cares more about the secrecy rate and is willing to pay more reward to increase the secrecy rate. Moreover, a larger λ_2 leads to a lower utility, since the intermediate node cares more about their energy consumption and it will devote less power to cooperate given the same payment.

Fig. 8 shows the utilities of intermediate nodes, averaged over fading distribution. It can be seen that the partners, who contribute to increase the secrecy rate of the source, can receive a certain amount of reward through cooperation, which implies that all the partners have the incentive for cooperation. Moreover, the node located at (0.9 km, -0.4 km) act as a jammer (node 13), while other nodes receiving non-zero rewards act as relays.

Fig. 9 shows the average utility of the source using PSO with respect to the number of intermediate nodes, using Monte Carlo simulation. It can be seen that with PSO algorithm, the source can achieve higher utility than that using only C-E partner selection algorithm when the proposed incentive mechanism is applied. That is because the source can actively affect the power allocation of the intermediate nodes by introducing the reward allocation weights. Through adjusting the weights, the intermediate nodes can be better stimulated to further improve the secrecy rate.

Fig. 10 shows the utilities of intermediate nodes, averaged over fading distribution using the same network scenario in Fig. 6. Compared with Fig. 8, it can be seen that more intermediate nodes are encouraged/stimulated to contribute to increase the secrecy rate when PSO algorithm is applied.

VII. Conclusion

In this paper, we have proposed a cooperative framework to enhance security when multiple eavesdroppers exist. Two partner selection algorithms have been devised, which can select suitable relays or jammers to maximize the secrecy rate. A game-theoretic incentive mechanism has been proposed to stimulate the partners to participate into cooperation. With the proposed cooperative framework, security can be significantly enhanced by preventing eavesdroppers from decoding the message transmitted, which can be applied to a network without infrastructure for secure information transfer, or for secret key exchange. Moreover, the proposed cooperative framework can be combined with the upper layer cryptographic schemes to further enhance the security.

In the future, we will consider secure communications for scenario with the multiple source-destination pairs. In such a scenario, the source nodes will compete with each other to recruit from intermediate nodes for security enhancement while the intermediate nodes will have more options to gain reward from different source nodes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

APPENDIX

A. Derivation of (27)

The objective function can be rewritten as follows:

$$\frac{\partial U_i}{\partial P_i} = \frac{r_i P_m \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} - \lambda_2 = 0$$

$$\Longrightarrow \sum_{j\subseteq\mathbb{C}} P_j r_j = \sqrt{\frac{r_i \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\lambda_2}}$$

$$\Longrightarrow P_i = \frac{1}{r_i}\left(\sqrt{\frac{r_i P_m \sum_{j\neq i, j\subseteq C} P_j r_j}{\lambda_2}} - \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j\right)$$

Since the power cannot be negative and greater than the maximum power, we have (27).

B. Derivation of (28)

To solve the optimal transmission power of the selected partners, let

$$\frac{\partial U_i}{\partial P_i} = 0 \Longrightarrow \quad \frac{r_i P_m \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} = \lambda_2 \tag{41}$$

Then, we have

$$\begin{aligned} \frac{r_1 P_m \sum_{j\neq 1, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} &= \lambda_2 \\ &\vdots \\ \frac{r_i P_m \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} &= \lambda_2 \\ &\vdots \\ \frac{r_n P_m \sum_{j\neq n, j\subseteq\mathbb{C}} P_j r_j}{\left(\sum_{j\subseteq\mathbb{C}} P_j r_j\right)^2} &= \lambda_2 \end{aligned} \tag{42}$$

Therefore,

$$\begin{aligned} \sum_{j\neq 1, j\subseteq\mathbb{C}} P_j r_j &= \tfrac{r_i}{r_1} \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j \\ &\vdots \\ \sum_{j\neq n, j\subseteq\mathbb{C}} P_j r_j &= \tfrac{r_i}{r_n} \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j \end{aligned} \tag{43}$$

Since the summation of the left side equal to the summation of the right side, we have,

$$\left(\sum_{j=1}^{n} \frac{r_i}{r_j}\right) \cdot \sum_{j\neq i, j\in\mathbb{C}} P_j r_j = (n-1)\left(\sum_{j\neq i, j\in\mathbb{C}} P_j r_j + P_i r_i\right). \tag{44}$$

In addition,

$$P_i = \frac{1}{r_i}\left(\sqrt{\frac{r_i P_m \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j}{\lambda_2}} - \sum_{j\neq i, j\subseteq\mathbb{C}} P_j r_j\right) \tag{45}$$

Then, we can calculate P_i as follows:

$$P_i = \frac{P_m r_i B_i}{\lambda_2 (r_i + B_i)^2} \tag{46}$$

where $B_i = \frac{(n-1) r_i}{\sum_{j=1}^{n} \frac{r_i}{r_j} - n + 1}$.

Since P_i cannot be negative and greater than the maximum power, we have

$$P_i^* = [\min\{\frac{P_m r_i B_i}{\lambda_2 (r_i + B_i)^2}, P_{max}\}]^+ \tag{47}$$

REFERENCES

[1] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and privacy in mobile social networks: challenges and solutions," *IEEE Wireless Communications*, vol. 21, no. 1, pp. 33–41, 2014.

[2] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications*, vol. 19, no. 2, pp. 40–47, 2012.

[3] L. Ozarow and A. Wyner, "Wire-tap channel ii," in *Advances in Cryptology*. Springer, pp. 33–50, 1985.

[4] J. Huang and A. Swindlehurst, "Robust secure transmission in miso channels based on worst-case optimization," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, 2012.

[5] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 2067–2076, 2011.

[6] N. Anand, S. Lee, and E. Knightly, "Strobe: Actively securing wireless communications using zero-forcing beamforming," in *Proc. of IEEE INFOCOM'12*, 2012.

[7] C. E. Shannon, "Communication theory of secrecy systems*," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[8] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[9] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2840–2852, 2013.

[10] H. Wang, Q. Yin, and X. G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 60, pp. 3532–3545, 2012.

[11] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, "Cooperative spectrum access towards secure information transfer for crns," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, pp. 2453–2464, 2013.

[12] G. Zheng, L. Choo, and K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.

[13] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 99, pp. 4985–4997, 2011.

[14] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–11, 2009.

[15] M. Mahmoud and X. Shen, "Fescim: fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks," *IEEE Transactions on Mobile Computing*, vol. 11, pp. 753–766, 2012.

[16] M. Wen, K. Zhang, J. Lei, X. Liang, R. Deng, and X. Shen, "Cit: A credit-based incentive tariff scheme with fraud-traceability for smart grid," *Security and Communication Networks*, 2013.

[17] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, 2009.

[18] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 2099–2111, 2013.

[19] N. Zhang, N. Cheng, N. Lu, H. Zhou, J. W. Mark, and X. Shen, "Risk-aware cooperative spectrum access for multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 516–527, 2014.

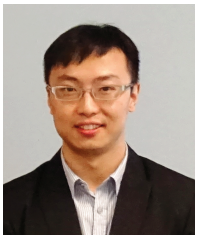
[20] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[21] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure af relay systems with individual power constraint and no eavesdropper's csi," *IEEE Signal Processing Letters*, vol. 20, pp. 39–42, 2013.

[22] H. Wang, M. Luo, Q. Yin, and X. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2007–2020, 2013.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2418316, IEEE Transactions on Wireless Communications

[23] N. Zhang, N. Cheng, X. Zhang, N. Lu, J. W. Mark, and X. Shen, "A cooperative scheme for secure communications with partner selection and incentive mechanism," *in Proc. of IEEE WCSP'14*, 2014.
[24] J. N. Laneman, D. N. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.
[25] M. G. Damavandi, A. Abbasfar, and D. G. Michelson, "Peak power reduction of ofdm systems through tone injection via parametric minimum cross-entropy method," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1838–1843, 2013.
[26] R. Y. Rubinstein, "Optimization of computer simulation models with rare events," *European Journal of Operational Research*, vol. 99, pp. 89–112, 1997.
[27] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Journal of the Econometric Society Econometrica*, pp. 520–534, 1965.
[28] Y. Wang, Q. Zhang, Y. Zhang, and P. Chen, "Adaptive resource allocation for cognitive radio networks with multiple primary networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–18, 2012.
[29] Q. Xu, X. Li, H. Ji, and X. Du, "Energy-efficient resource allocation for heterogeneous services in ofdma downlink networks: Systematic perspective," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2071–2082, 2014.



Ning Zhang (S'12) earned the Ph.D degree from University of Waterloo in 2015. He received his B.Sc. degree from Beijing Jiaotong University and the M.Sc. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2010, respectively. His current research interests include dynamic spectrum access, 5G, physical layer security, and vehicular networks.

Nan Cheng (S'13) is currently a Ph.D. candidate in the department of Electrical and Computer Engineering, the University of Waterloo, Waterloo, ON, Canada. He received his B.S. degree and M.S. degree from Tongji University, China, in 2009 and 2012, respectively. Since 2012, he has been a research assistant in the Broadband Communication Research group in ECE Department, the University of Waterloo. His research interests include vehicular communication networks, cognitive radio networks, and resource allocation in smart grid.

Ning Lu (S'12) earned the Ph.D degree from University of Waterloo in 2015. He received the B.Sc. and M.Sc. degrees from Tongji University, Shanghai, China, in 2007 and 2010, respectively. He is currently a Mitacs postdoctoral research fellow in BLiNQ, Ottawa, ON. His current research interests include capacity and delay analysis, media access control, and routing protocol design for vehicular networks.

Xiang Zhang received the B.Eng. degree in Information Engineering and the M.Sc. degree in Computer Application Technology from University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2003 and 2009, respectively. He is currently a Senior Engineer with the School of Information and Software Engineering, UESTC. Between 2013 and 2014, he was a Visiting Researcher with the University of Waterloo, Waterloo, ON, Canada. His research interests includes the areas of vehicular communication and networking, resources management, and multimedia streaming and services.

Jon W. Mark (M'62-SM'80-F'88-LF'03) received the Ph.D. degree in electrical engineering from McMaster University in 1970. In September 1970 he joined the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, where he is currently a Distinguished Professor Emeritus. He served as the Department Chairman during the period July 1984-June 1990. In 1996 he established the Center for Wireless Communications (CWC) at the University of Waterloo and is currently serving as its founding Director. Dr. Mark had been on sabbatical leave at the following places: IBM Thomas J. Watson Research Center, Yorktown Heights, NY, as a Visiting Research Scientist (1976-77); AT&T Bell Laboratories, Murray Hill, NJ, as a Resident Consultant (1982-83): Laboratoire MASI, universit pierre et marie curie, Paris France, as an Invited Professor (1990-91); and Department of Electrical Engineering, National University of Singapore, as a Visiting Professor (1994-95). He has previously worked in the areas of adaptive equalization, image and video coding, spread spectrum communications, computer communication networks, ATM switch design and traffic management. His current research interests are in broadband wireless communications, resource and mobility management, and cross domain interworking.

Dr. Mark is a Life Fellow of IEEE and a Fellow of the Canadian Academy of Engineering. He is the recipient of the 2000 Canadian Award for Telecommunications Research and the 2000 Award of Merit of the Education Foundation of the Federation of Chinese Canadian Professionals. He was an editor of IEEE TRANSACTIONS ON COMMUNICATIONS (1983-1990), a member of the Inter-Society Steering Committee of the IEEE/ACM TRANSACTIONS ON NETWORKING (1992-2003), a member of the IEEE Communications Society Awards Committee (1995-1998), an editor of Wireless Networks (1993-2004), and an associate editor of Telecommunication Systems (1994-2004).

Xuemin (Sherman) Shen (IEEE M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as the Technical Program Committee Chair/Co-Chair for IEEE Infocom'14, IEEE VTC'10 Fall, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications; an Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks, etc.; and the Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007 and 2010 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.