Computer Communications 105 (2017) 124–132

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

# An adaptive trust-Stackelberg game model for security and energy efficiency in dynamic cognitive radio networks

He Fang[a], Li Xu[a,*], Jie Li[b], Kim-Kwang Raymond Choo[c]

[a] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China
[b] Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba Science City, Ibaraki 305-8573, Japan
[c] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

ARTICLE INFO

*Article history:*
Received 22 February 2016
Revised 28 October 2016
Accepted 29 November 2016
Available online 30 November 2016

*Keywords:*
Dynamic cooperative cognitive radio networks
Secure Relay Selection
Power control
Stackelberg game
Reinforce learning

ABSTRACT

Due to the potential of cooperative cognitive radio networks (CCRNs) in addressing the spectrum scarcity problem in wireless communication networks, CCRN has become a subject of active research. For example, security and energy efficiency are two salient areas of research in CCRNs. In this paper, we propose a novel adaptive trust-Stackelberg game model designed to (a) improve the energy efficiency and (b) defend against insider attacks in CCRNs. More specifically, the distributed learning algorithm (DLA) for the relays in our model, inspired by the stochastic learning automata, allows the system to achieve Stackelberg equilibrium in the proposed game; and the trust evolution based on evolutionary stable strategy algorithm (TEEA) allows the primary user to defend against insider attacks efficiently and adaptively adjust the trust evolution in dynamic CCRNs. We demonstrate the utility of the proposed model comparing with other models using a numerical investigation. The numerical results show that the proposed model can improve the performance in energy efficiency and defending against insider attacks with an appropriate cooperation between primary users and relays.

## 1. Introduction

The capability to efficiently allocate the limited spectrum to an increasing wireless application and service user base is an ongoing challenge to both regulators and the industry, and is a challenge that is unlikely to go away anytime soon. Cooperative transmission has been identified as a viable option for both licensed users (primary users – PUs) and unlicensed users (secondary users – SUs) [1–3]. More specifically, in a cooperative cognitive radio network (CCRN), a PU selects one or more SUs as amplify-and-forward (AF) or decode-and-forward (DF) relays and the PU is also able to lease spectrum to one or more SUs when the spectrum is not fully utilized [4,5]. The ability of SUs to opportunistically access a larger spectrum band can result in better spatial and temporal reuse, but there is a need to ensure effective interference management particularly in a multiple PUs and multiple SUs setting. Despite the various advantages of CCRNs, there are known security threats which are not present in the traditional radio environment (e.g. insider attacks) [6].

While cryptography can be deployed to improve the communication security, cryptographic solutions are generally ineffective against insider attackers (e.g. malicious or corrupt SUs) who are legitimate CCRN users. One potential mitigation strategy for defending against insider attacks is using trust management to authorize and verify users (and in our context, SUs) in real-time [7]. However, the centralized cooperative communication schemes, which require the relays to know the instantaneous and perfect channel state information (CSI) between each other, are impractical for deployment in dynamic systems. Besides, security against insider attacks are generally not considered in existing schemes (see [8–10]). For example, a malicious SU may misbehave in order to abuse the network resources and services or attempt to attack one or more PUs in concert with other malicious SUs. In order to defend against insider attacks in dynamic CCRNs, an effective trust management system needs to be robust and objective. However, it is difficult to accurately calculate the trust value. Therefore, it is not surprising that most existing trust management models generally do not consider an entity's variational trust evolution required in a dynamic CCRN setting (see [11–14]).

In order to address security challenges posed by one or more untrustworthy SUs in CCRNs, we propose a trust-based approach to ensure secure communication. In our approach, whenever a SU

[*] Corresponding author.
*E-mail address:* xuli@fjnu.edu.cn (L. Xu).

http://dx.doi.org/10.1016/j.comcom.2016.11.012
0140-3664/© 2016 Elsevier B.V. All rights reserved.

wants to be the relay for a PU, we will first check the trustworthiness of the requesting SU in obeying the opportunistic access rules. For example, a SU known to drop packets, tamper with communication data or falsify sensing information in the network will not be approved. In addition, we model the interaction between the PU and SU in the cooperation architecture (referred to as ***S***ecure ***R***elay selection) as a trust-***S***tackelberg ***G***ame (***SRSG***). The trust-based cooperation in the CCRN is defined using power control and pricing. Then, a distributed learning algorithm inspired by the stochastic learning automata is proposed for the selected relay to achieve the Stackelberg equilibrium of the proposed game (i.e., optimal power allocation, price allocation, relay selection, and relay action). A learning algorithm, based on the evolutionary game theory, to adaptively adjust the trust evolution is also proposed for the PU.

The rest of this paper is organized as follows. Related work and the system model are presented in Sections 2 and 3, respectively. In Sections 4 and 5, we present the SRSG game model and our proposed distributed learning algorithm (DLA) to achieve the equilibrium of proposed game, respectively. A learning algorithm (TEEA) for trust evolution is formulated in Section 6. Simulation results are presented in Section 7. Finally, the last section concludes the paper.

## 2. Related work

Huang, Han and Ansari surveyed existing energy-efficient CR techniques and the optimization of green-energy-powered wireless networks in [3]. They also presented a new joint spectrum and power allocation scheme for a cooperative downlink multiuser system using the frequency division multiple access scheme in [15]. In [16], the authors presented an orthogonal frequency division multiplexing (OFDM) based cooperative relay system, where the relay node forwards the data to the destination node and is capable of transferring energy to the source node.

Game-theoretic approach has been applied extensively to study cooperative communications [8–10,17–20]. Cao et al. [21] studied the relay power allocation and pricing problems, and modeled the interaction between the users and the relay as a two-level Stackelberg game. A game-theoretic power control algorithm was proposed in [8] to minimize the total power consumption in a cooperative communication network, which transmits information from multiple sources to a destination via multiple relays to save energy and improve communication performance. In [17], the authors quantified PU's and SU's benefits from the channel sharing model by deriving the Stackelberg equilibrium. A two-level Stackelberg game was also employed in [10] to jointly consider the benefits of the source node and the relay nodes in which the source node was modeled as a buyer and the relay nodes were modeled as sellers, respectively. However, none of these models consider insider attacks; therefore, they are not suitable for the CCRN deployment.

Trust management has been shown to be a viable solution to address insider threats. For example, in [22], the authors proposed a novel secure and reliable multi-constrained quality of service (QoS) aware routing algorithm for vehicular ad-hoc networks. A computational dynamic trust model for user authorization in an open environment was proposed in [23], and more recently in 2015, a trust-based privacy-preserving friend recommendation scheme for online social networks was presented in [24]. A number of researchers have also attempted to expedite the authentication process, in order to increase the attractiveness of their solution. For example, Huang et al. proposed a secure generic multi-factor authentication protocol designed to speed up the whole authentication process [[25]].

Yang et al. [26] designed an integrated optimal relay assignment scheme for cooperative networks and a payment mechanism to avoid system performance degradation due to selfish relay selections by source nodes. However, the relay assignment scheme is centralized, which cannot be easily deployed in dynamic CCRNs. A secure trust-based authentication approach was proposed for CRNs in [6], where the trust is embedded in the certificate during the pre-deployment of trust relation and can be used to evaluate trust continuously based on behaviors. In another independent yet related work, a trust-aware model was proposed for spectrum sensing in CRNs [11]. However, the researchers did not evaluate the system and consequently, users cannot be assured of the security and soundness of the proposed solution. In [12], the authors proposed a theoretical framework for combining reputation-based systems, game theory and network selection mechanism in order to ensure that mobile users are “always best connected” anywhere and anytime. However, the proposed scheme fails to consider the entities' variational trust evolution in a dynamic CCRN setting. A number of trust updating schemes based on direct trust or recommendation [27,28] have also been presented in the literature, but most of these proposed schemes focused on analyzing the forgetting factor and other factors in trust evolution. Different from these schemes, we focus on the weight factor adjustment in this paper.

## 3. System model

In this paper, we focus on insider attacks where malicious insiders (e.g. unlicensed users) will drop or tamper with packets, falsify or fabricate sensing information, consume additional network resources in CCRNs, etc. We remark that in a typical system, licensed users (i.e., primary users, PUs) should have the priority to use the channels and reduce its energy consumption by using unlicensed users (i.e., secondary users, SUs) for relaying. In return, the relays obtain payment from the PUs as a reward and an incentive for cooperation. We assume that the SUs are rational and noncollude because they are competing with each other for resources from PUs. This is a reasonable assumption, since the SUs (which are unlicensed users in CCRNs) need to transmit the packets to each other if they wish to collude with each other, and it also costs time. The notations used in the paper are shown in Table 1.

A typical cognitive radio network comprises a primary network and a secondary network. The primary network consists of $n$ users with one primary base station (PBS), and multiple PUs, who communicate with the PBS over the licensed spectrum. The secondary network consists of $m$ SUs, and Fig. 1 illustrates the process of the cooperative transmission. When a PU wishes to send packets to PBS, the PU will first request a service to the SUs and select one of these SUs to be the relay. We assume the malicious nodes are in the secondary network, and all SUs require the PUs' authorization to be the relay. In the authorization process, the PU requests recommendations to the neighbor nodes of the selected SU (neighbor nodes are nodes in the transmission range of the SU). The PU will then decide whether to choose the SU to be the relay or not based on the trust management. We assume that the SUs transmit the PU's signals in the decode-and-forward (DF) protocol, where each relay node decodes its received signals and forwards its decoded outcomes to the PBS.

The primary transmission is divided into frames by $\gamma$, where the $\gamma$ is time allocation coefficient, and the frame duration is $T$. There are three possible situations as follow:

*Case 1:* When $\gamma = 0$, the channel is idle, and the SUs can lease the channel and transmit their own packets.

*Case 2:* When $\gamma = 1$, the PU transmits its packets to the PBS directly in the whole frame duration without the cooperation of relays.

*Case 3:* When $0 < \gamma < 1$, the PU broadcasts its packets to relays, then the relays cooperatively transmit the primary packets to PBS in the DF way.

**Table 1**
Summary of notations .

| Notation | Definition |
|---|---|
| $n$ | Number of the PUs |
| $m$ | Number of the SUs |
| $T$ | Frame duration of the primary transmission |
| $\gamma$ | Time allocation coefficient |
| $W$ | Bandwidth of channels in the network |
| $\varsigma$ | Noise power per bandwidth |
| $R_1$ | Achievable rate of the relay from PU |
| $R_2$ | Achievable rate of the cooperation from relay $r$ to PBS |
| $R_3$ | Achievable rate of cooperation from the PU to PBS |
| $d$ | Price of unit of power for relaying the packets |
| $P_u$ | Transmit power of the PU |
| $a$ | Gain per unit of the achievable rate |
| $b$ | Cost per unit transmission energy of the relays |
| $c$ | Gain per unit attack of the relays |
| $d$ | Price per unit of power which the PU pays for the SUs' relaying |
| $K$ | Highest level of attack |
| $\theta$ | Level of the attacks, $\theta \in \{0, 1, \dots, K\}$ |
| $Z$ | Highest level of the PU's transmitter power |
| $D$ | Set of SUs who can decode the PU's messages |
| $\Omega$ | Sample space of $D$, $\Omega = \{\emptyset,\ D_1,\ D_2, \dots, D_Z\}$ |
| $P_r$ | Transmit power of the relay $r$ |
| $\Im_r$ | Trust value of the relay $r$ |
| $\Im^*$ | Threshold of the trust value |
| $\Im_r^D$ | Direct trust of the relay $r$ |
| $\Im_r^R$ | Recommendation value of the relay $r$ |
| $\rho$ | Forgetting factor in the trust management |
| $\omega$ | Weight factor of direct trust in the trust management, while $1 - \omega$ denotes the weight factor of the recommendation |

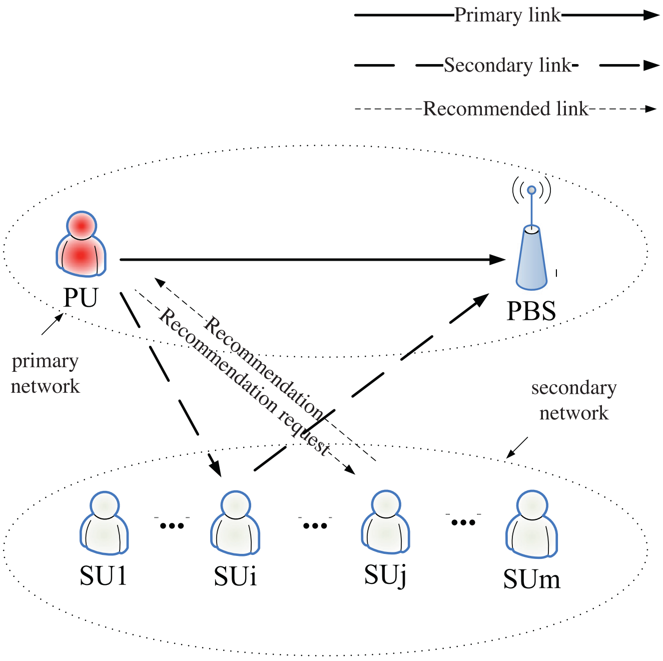


**Fig. 1.** The process of the cooperative transmission.

Let $D$ denotes the set of SUs who can decode PU's messages with a fixed power $P_u \in \{0, 1, \dots, Z\}$, where $Z$ represents the highest level of PU's transmitter power. There are $Z$ possible subsets $D$; thus, the sample space of $D$ is defined as:

$$\Omega = \{\emptyset,\ D_1,\ D_2, \dots,\ D_Z\}, \tag{1}$$

where $\emptyset$ represents the empty set. $D_i$ is the $i$th non-empty subset of the $m$ SUs, and $i$ corresponds to level-$i$ power of the PU, $i = 1, .., Z$. If the set $D_i$ is empty, this implies that all SUs remain silent in the route discovery process. Then, the PU has to improve the transmission power $P_u$ or the price of relaying.

*Step one:* With duration $\gamma T$, the primary packets are transmitted with a fixed power $P_u \in \{0, 1, \dots, Z\}$ to the relay $r$, $r \in D_{P_u}$. The achievable rate of broadcasting is shown as follows:

$$R_1(P_u) = W \log\left(1 + \frac{g_1 P_u}{W \varsigma}\right), \tag{2}$$

where $W$ is the bandwidth, $\varsigma$ denotes the channel noise power per bandwidth, and $g_1$ is the complex channel gain between PU and relay $r$.

*Step two:* With duration $(1 - \gamma)T$, relay $r$ cooperatively transmits the data to PBS with a fixed power $P_r$ in the DF protocol. The achievable rate of cooperation from $r$ to the PBS can be described as:

$$R_2(P_r) = W \log\left(1 + \frac{g_2 P_r}{W \varsigma}\right), \tag{3}$$

where $g_2$ is the complex channel gain between relay $r$ and PBS. Finally, the achievable rate from the PU to PBS in this case is as follows:

$$R_3 = T \min\{\gamma R_1, (1 - \gamma) R_2\}. \tag{4}$$

We remark that the main objective of this paper is to improve the PU's energy efficiency in the presence of a malicious insider in the CCRN. Therefore, the PU needs to allocate the power efficiently and select a best relay to maximize their achievable capacity. In this way, power control and relay selection strategy for the PU can be formulated as the optimization problem, as described below:

$$\max_{P_u, r} R_3,$$
$$s.t.\ P_u \in \{0, 1, \dots, Z\},\ \ r \in D_{P_u},\ \ R_3 \ge R^{req}. \tag{5}$$

where $R^{req}$ is the required data rate. The constraint represents PU's power allocation set, and guarantees the required transmission rate $R^{req}$. It is an QoS indicator that guarantees normal transmission (i.e., without outage).

**Remark.** The objective of this work is to develop a novel cooperative transmission framework that examines the interactions between the PUs and SUs to achieve the relay based cooperative communication for improving energy efficiency and transmission security in the presence of malicious insiders. It is clear that the optimization problem in (5) is a nonlinear and nonconvex optimization problem, external energy and additional computational costs are required, and is challenging to solve. More specifically, due to the existence of malicious users in the secondary network, it is difficult for the PU to choose a best relay to improve energy efficiency and guarantee secure transmission. In other words, the PU may choose a malicious SU to be the relay, resulting in the failure of cooperative transmission. Hence, the optimization problem in (5) is nonconvex and has multiple objectives. In such a setting, game theory provides an effective tool in modeling and analyzing the interactions among independent decision makers, and it is also a useful mathematical tool for solving nonconvex and multiple objectives problems. Thus, we are motived to model the interactions between the users to achieve the cooperative transmission and solve the optimization problem (5) by using game theory.

## 4. Secure Relay Selection based on Game (SRSG) model

In order to achieve the relay based cooperative communication for improving the energy efficiency and transmission security in the presence of insider attacks, and solve the nonconvex and multiple objectives optimization problem in (5), a novel game framework (hereafter referred to as the Secure Relay Selection based on Game (SRSG) model) is presented in this section. In this game framework, power control, relay selection, pricing scheme, and trust management are considered. Specifically, power control and relay selection are designed to facilitate PUs in improving the energy efficiency by controlling the transmit power and selecting a relay to forward the signals. Pricing scheme is used between the PUs and SUs to achieve the cooperative transmission, since the SUs will not forward the PUs' signals if they are unable to benefit from the cooperative transmission. We also design the trust management for the PUs as a foundation to select a best (i.e., secure) relay for defending against the insider attacks.

In this SRSG model, PU acts as the leader and decides its own transmission power $P_u$, the reward for SUs' relaying and the selection of relay. Meanwhile, the selected relay acts as the follower, and determines its relaying action. Then, we can decompose the optimization problem (5) into two sub-optimization problems according to the behaviors and utilities of PU and selected relay. In these sub-optimization problems, both the PU and SU's objectives are to maximize the their own total profits. Then, a distributed learning algorithm (i.e., DLA) inspired by the stochastic learning automata is proposed to facilitate the selected relay in achieving the Stackelberg equilibrium of the proposed game (i.e., optimal power allocation, price allocation, relay selection, and relay action). A learning algorithm (i.e., TEEA), based on the evolutionary game theory, to adaptively adjust the trust evolution is also proposed for the PU.

### 4.1. SRSG model formulation

Stackelberg game is a model of first-mover advantages, and all CCRN users can obtain such advantages in the competition. In a realistic scenario, the PU has priority to start the communications and use the resources in the cognitive radio network, and the SU's reactions are based on the PU's decisions. Therefore, the PU adopts its strategies first as leader, and the SUs obey as followers. Note that all the users are rational, and we formulate the problems as a two-stage Stackelberg game as follows:

*Stage 1*, the PU (i.e., the leader) decides its own transmission power $P_u$ to improve energy efficiency, reward for SUs' relaying to encourage SUs to join in the cooperative communication, and the selection of relay to defend against the insider attacks. The PU's objective is to maximize the total profit (i.e., secure and efficient communication) generated from the cooperative transmission for improving the security performance and energy efficiency.

*Stage 2*, the selected relay (i.e., the follower) decides its relaying action. The objective of the selected relay is to maximize its own profit by choosing an appropriate relaying action.

The SRSG model is defined as:

**Definition 1.** $G = \langle N,\ A,\ U\rangle$ is a SRSG model, where $N$ denotes the set of players, and consists of PUs and SUs. $A = A_1 \bigcup A_2$, where $A_1 = \{(P_u,\ d),\ P_u \in \{0, 1, \ldots, Z\},\ d \geq 0\}$ and $A_2 = \{\theta_r,\ r \in D_{P_u},\ \theta_r = 0, 1, 2, \ldots, K\}$ are the strategy sets of PU and relay $r$, respectively. $U = \{U_{PU}\} \bigcup \{U_r\}$, where $U_{PU}$ and $U_r$ denote the utility functions of PU and relay $r$, respectively.

In Definition 1, $d$ represents the price per unit of power which the PU pays for the SUs' relaying. $\theta$ corresponds to level-$\theta$ attack, and $\{0, 1, 2, \ldots, K\}$ is the action set of relaying. $\theta = 0$ represents the SU taking the action of relaying without attacks. Each SU is allocated a trust value, which is associated with the credibility of relaying data. In our work, $\Im_r$ denotes the trust value of $r$, only when $\Im_r \geq \Im^*$ can $r$ be trusted by PUs, where $\Im^*$ is the threshold value and $r \in D_{P_u}$.

In trust management, we take the direct trust, recommendations, and forgetting factor into account. More importantly, the information's timeliness is included in the calculation on relay's trust value. We denote the forgetting factor as $\rho[t]$. Then, the direct trust of relay $r$ with time decay factor can be computed using:

$$\Im_r^D[t] = \frac{\sum_{i=1}^{t}(K - \theta_r[i])\rho[i]}{K\sum_{i=1}^{t}\rho[i]}. \tag{6}$$

The value of recommendations is given as:

$$\Im_r^R[t] = \frac{\sum_{i=1}^{l}\tau_i[t]\eta_i[t]}{\sum_{i=1}^{l}\eta_i[t]}, \tag{7}$$

where $l$ is the number of recommended nodes, $\eta_i$ denotes node $i$'s influence degree of service for PU, and $\tau_i$ represents the $i$th node's recommendation, $i = 1, \ldots, l$.

Combining both direct trust and recommendation, we obtain the integrated trust degree of relay $r$ as follows:

$$\Im_r[t] = \omega[t]\Im_r^D[t] + (1 - \omega[t])\Im_r^R[t], \tag{8}$$

where $\omega[t]$ indicates the weight factor of the direct trust, while $1 - \omega[t]$ is the weight factor of the recommendation. Note that $\omega[t]$ is real-time, that is to say, the weight factor is changing all the time in the dynamic CCRN. The process of SRSG model can be formulated as:

*Stage I:* PU (i.e., the leader) chooses a best relay, and decides transmits power $P_u$ and price $d$ to maximize its utility function $U_{PU}$. Its utility is affected by the profit of transmission and its cost of transmit power, and the relaying price pay to the selected relay. So the instant utility function of PU is shown as follows:

$$\begin{aligned} &U_{PU}(P_u, d)[t] \\ &\quad = aR_3\frac{K - \theta_r[t]}{K} - bP_u\gamma T - dP_r(1 - \gamma)T, \end{aligned} \tag{9}$$

where $a$ represents the gain per unit of rate and $b$ denotes the cost per unit transmission energy. The first term of (9) represents the quality of selected relay's service, which considers the behaviors of selected relay. The second term and third term are the costs in transmitting the packets and purchasing the relay's service, respectively.

In this paper, we design the price $d$ as a decreasing function of $P_u$: $d(P_u) = e_1P_u + e_2$, where $e_1 < 0$ and $e_2 > 0$ satisfy $e_1P_u + e_2 > 0$. In other words, the PU can pay more for the relaying to improve the active of relays when it is on a low power. Therefore, there is an optimal price strategy $d$ for a PU to pay for the relaying based on its transmission power. In conclusion, an optimal power and price strategy for SRSG model can be formulated as the problem (*P-P*):

$$\begin{aligned} &\max_{P_u} U_{PU}, \\ &s.t.\ r \in D_{P_u},\ \Im_r \geq \Im^*,\ P_u \in \{0, 1, \ldots, Z\},\ R_3 \geq R^{req}. \end{aligned} \tag{10}$$

We can observe from the problem *P-P* that, for a given $P_u$, the $d$ can be calculated through $d(P_u) = e_1P_u + e_2$. Then the transmit power of selected relay $P_r$ can be obtained by satisfying the constraint $R_3 \geq R^{req}$. Now, given a $P_u$ with the relay set $D_{P_u}$, it is crucial to determine which relay should be selected as the best relay to assist PU's packets transmission. Ideally, the best relay selection should aim to minimize the probability of attack and maximize the utility of PU. Accordingly, the best relay selection criterion is designed as:

$$\text{Best Relay } r^* = \arg\max_{r \in D_{P_u}} \Im_r[t]. \tag{11}$$

*Stage II:* In response to the PU's decisions, the selected relay $r$ (i.e., the follower) decides its relaying action $\theta_r$, to maximize its utility. The instant utility of selected relay is designed based on the relaying action, which is as follows:

$$U_r(\theta_r)[t] = \Im_r[t]((d - b)P_r(1 - \gamma)T + c\theta_r[t]), \tag{12}$$

where $\Im_r[t]$ represents the probability of the node $r$ that will be chosen by the PU. $dP_r(1 - \gamma)T$ in (12) represents the income of relay $r$ in relaying the PU's packets, and $bP_r(1-\gamma)T$ is the relay's normalized cost in relaying PU's packets. $c\theta_r[t]$ is the income of relay through attacking the route, where $c$ is denoted as the income per unit attack of relays. Clearly, as a rational user, the relay will not attack constantly, since frequent attacks will reduce the trust value $\Im_r$ and decrease subsequent utility.

The utility function for relay node $r$ is a function of $\theta_r$; therefore, an optimal relaying strategy for SRSG can be formulated as the problem (*R-P*):

$$\max_{\theta_r} U_r,$$
$$s.t.\ \theta_r \in \{0, 1, 2, \ldots, K\}. \tag{13}$$

*4.2. Equilibrium analysis of SRSG model*

Based on the game formulation, we know that the strategy of each stage affects another stage's strategy. Therefore, we use backward induction method to analyze the proposed game since it can capture the sequential dependence of the decisions in the stages of the game. We first define the Stackelberg equilibrium of the proposed game as follows:

**Definition 2.** A strategy $(r^*, P_u^*, \theta_r^*)$ is a Stackelberg equilibrium of the proposed game, if the following conditions are satisfied:

1. $U_{PU}(r^*, P_u^*, \theta_{r^*}^*) \geq U_{PU}(r, P_u, \theta_r^*)$ for all $P_u \in \{0, 1, \ldots, Z\}$ and $r \in D_{P_u}$;
2. $U_r(P_u^*, \theta_r^*) \geq U_r(P_u^*, \theta_r)$ for all $\theta_r \in \{0, 1, 2, \ldots, K\}$.

*Analysis of the selected relay's strategies:* In order to maximize its own utility, the relay adjusts its individual action based on the decision of the PU. Assuming that the strategies of the PU are given, the selected relay's best response strategy can be computed by solving the optimization problem (*R-P*) in (13).

Then the first order partial derivative of $U_r$ with respective to $\theta_r$ is shown as:

$$\frac{\partial U_r[t]}{\partial \theta_r[t]} = ((d-b)P_r(1-\gamma)T + c\theta_r[t])\frac{\partial \Im_r[t]}{\partial \theta_r[t]} + c\Im_r[t]$$
$$= -\frac{\omega[t]\rho[t]}{K\Sigma_{i=1}^t \rho[i]}((d-b)P_r(1-\gamma)T + c\theta_r[t]) + c\Im_r[t], \tag{14}$$

and the second order partial derivatives of $U_r$ is:

$$\frac{\partial^2 U_r[t]}{\partial \theta_r[t]^2} = -\frac{2c\omega[t]\rho[t]}{K\Sigma_{i=1}^t \rho[i]}. \tag{15}$$

Therefore, the objective function (13) is strictly concave, and there exists a unique optimal relaying strategy of the selected relay. By setting $\partial U_r[t]/\partial\theta_r[t] = 0$, the selected relay's optimal action for its problem (13) at time $t$ can be expressed as (16) when $\Im_r \geq \Im^*$

$$\theta_r[t]' = X_1[t] + \frac{1}{2}\left(K - \frac{1}{c}(d-b)P_r(1-\gamma)T\right), \tag{16}$$

where

$$X_1[t] = \frac{\Sigma_{i=1}^t \rho[i] K(1-\omega[t])\Im_r^R[t]}{2\omega[t]\rho[t]} + \frac{\sum_{i=1}^{t-1}(K-\theta_r[i])\rho[i]}{2\rho[t]}.$$

Since $\theta_r \in \{0, 1, 2, \ldots, K\}$, the optimal action of relay $r$, $r \in D_{P_u}$, can be rewritten as follows:

$$\theta_r[t]^* = \begin{cases} [\theta_r[t]'] + 1 & 0 < t \leq \kappa T \\ [\theta_r[t]'] & \kappa T < t \leq T, \end{cases} \tag{17}$$

where $[\cdot]$ represents a rounding function.

Then two lemmas can be summarized as follows:

**Lemma 1.** *When $\Im_r \geq \Im^*$, PUs can prevent the insider attacks caused by relay $r$ by increasing the price of relaying $d$, which satisfies (18).*

$$d \geq \frac{cK(1-\omega[t])\Im_r^R[t]\Sigma_{i=1}^t \rho[i]}{\omega[t]\rho[t]P_r(1-\gamma)T} + \frac{c\sum_{i=1}^{t-1}(K-\theta_r[i])\rho[i]}{\rho[t]P_r(1-\gamma)T}$$
$$+ \frac{Kc}{P_r(1-\gamma)T} + b, \quad r \in D_{P_u}. \tag{18}$$

**Proof.** By letting $\theta_r[t]^* \leq 0$, it is straightforward to show that when $d$ satisfies (18), $r$ will always choose action $\theta_r[t]^* = 0$. Therefore, this concludes the proof. □

**Lemma 2.** *If $d \leq cK/(P_r(1-\gamma)T) + b$ holds, SUs in the secondary network will take only two actions: (1) not to be the relay, and (2) attack the route with probability 1.*

$$a\frac{K-\theta_r^*}{K}\frac{\partial R_3}{\partial P_u} - \frac{aR_3}{K}\frac{\partial \theta_r^*[t]}{\partial d} \cdot \frac{\partial d}{\partial P_u} - P_r(1-\gamma)T\frac{\partial d}{\partial P_u} - b\gamma T = 0. \tag{19}$$

**Proof.** From (16), it is clear that $X_1[t]$ is positive. By letting $K - \frac{1}{c}(d-b)P_r(1-\gamma)T \geq 0$, $\theta_r[t]^* > 0$ happens all the time, regardless of the strategies undertaken by the PU. Then, we can rewritten $K - \frac{1}{c}(d-b)P_r(1-\gamma)T \geq 0$ as $d \leq cK/(P_r(1-\gamma)T) + b$, which completes the proof of Lemma 2. □

*Analysis of the PU's strategies:* To maximize its utility, the PU first chooses a best relay according to the relay selection criterion (11) to cooperatively transmit the PU's packets, then adjusts its individual power allocation strategy $P_u$ and decides the reward of the SU's relaying $d$.

When the trust value of a SU $i$ satisfies $\Im_i < \Im^*$, $i \in \{1, 2, \ldots, m\}$, the PU will not choose SU $i$ to be relay. In this way, SU $i$'s instant utility equals to 0, which leads to failure in leasing the spectrum when it needs to access the spectrum. Based on the problem formulation and Lemmas 1 and 2, we can obtain the following theorem.

**Theorem 1.** *If condition (**C₁**): $\Im_r \geq \Im^*$ and $d \leq cK/(P_r(1-\gamma)T) + b$ holds, then there exists a unique Stackelberg equilibrium for the proposed game.*

**Proof.** We divide our proof in three steps. Firstly, since the utility function $U_r(\theta_r)$ is a strictly concave function on the set $\{0, 1, \ldots, K\}$, it can achieve its maximum value at some $\theta_r \in \{0, 1, \ldots, K\}$ [33]. So when $\Im_r \geq \Im^*$, relay $r$'s optimal action for its problem (13) is unique, which has been shown in (17).

Then by submitting (16) to the utility function $U_{PU}$ at time $t$ and letting $\partial U_{PU}[t]/\partial P_u = 0$, we can obtain (19).

The PU's optimal power allocation $P_u^*$ for its problem (10) at time $t$ is the root of function (20),

$$\frac{2ln2 \cdot g_1 c}{W\varsigma + g_1 P_u^*}(K - \theta^*[t]) + e_1 P_{r^*}(1-\gamma)T\log(1 + \frac{g_1 P_u^*}{W\varsigma})$$
$$= \frac{2cK(b\gamma + P_{r^*}(1-\gamma)e_1)}{a\gamma W}, \quad r^* \in D_{P_u^*}, \tag{20}$$

and satisfies:

$$\begin{cases} P_u^* \geq (2^{\frac{R^{req}}{W}} - 1)\frac{W\delta}{g_1} \\ P_{r^*} \geq (2^{\frac{R^{req}}{W}} - 1)\frac{W\delta}{g_2}. \end{cases} \tag{21}$$

Finally, for the given $P_u^*$, it is easy to affirm the set $D_{P_u^*}$, price $d^*$, and best relay's power allocation $P_{r^*}$, which satisfies (21).

In conclusion, there exists a Stackelberg equilibrium $(r^*, P_u^*, \theta_r^*)$ for the proposed game model under ***C₁***, where $\theta_r^*$, $P_u^*$ are shown in (17) and (20) respectively, and $d^* = e_1 P_u^* + e_2$. □

## 5. A distributed learning algorithm (DLA) for the proposed game to achieve the Stackelberg equilibrium

We now present a distributed learning algorithm (DLA) for SUs to achieve the Stackelberg equilibrium of the proposed game. Each relay $r$ chooses an action $\theta_r[t]$ from set $\{0, 1, \ldots, K\}$ based on its current action probability distribution

$\boldsymbol{q_r}[t] = (q_r^0[t], q_r^1[t], \ldots, q_r^K[t])$, where $q_r^i[t] = Prob[\theta_r[t] = i]$ denotes the probability of $r$ choosing action $i$, and $i$ represents the level of attack. Each SU updates its strategy according to the following rule:

$$\boldsymbol{q_r}[t+1] = \boldsymbol{q_r}[t] + cU_r(\boldsymbol{e}_{\theta_r[t]} - \boldsymbol{q_r}[t]), \tag{22}$$

where $0 < c < 1$ is a parameter, $\boldsymbol{e}_{\theta_r[t]}$ is a unit vector with $\theta_r[t]$ component unity and all others zero. The details of DLA are shown in Algorithm 1.

**Algorithm 1** A distributed learning algorithm (DLA) for SUs to achieve the Stackelberg equilibrium.

```
Given gain per unit of rate of PUs $a$, cost per unit transmission energy of relays $b$, utility per unit attack of relays $c$, coefficient $e_1$, and $e_2$.
1. Initialize : $t = 0$
  • for each relay $r$, select initialized strategy $\boldsymbol{q_r}[0] = [\frac{1}{2}, \frac{1}{2(K-1)}, \ldots, \frac{1}{2(K-1)}, \frac{1}{2(K-1)}]$;
  • calculate $r's$ trust value $\Im_r[0]$ according to (8);
  • calculate utility $U_r[0]$ according to (12);
2. Learn :
  • update $r's$ strategy $q_r[t]$ according to (22);
  • relay $r$ selected an action based on its strategy $q_r[t]$;
  • PU updates trust value $\Im_r[t]$ of $r$ according to the trust evolution in (6), (7), and (8);
  • relay $r$ gets feedback from PU, i.e., the probability of selection;
  • obtain the utility $U_r[t]$ according to (12);
  • loop until the optimal strategy of relayr occurs, which satisfies that $\lim_{t\to m} q_r^{\theta_r} \to 1$, where $m$ represent finitesteps.
```

It is trivial to observe from (22) that Algorithm 1 neither requires information exchange nor needs perfect information about the number of SUs and the actions of other SUs. Hence, Algorithm 1 is a distributed algorithm. Then, a theorem about the convergence of DLA is given as follows:

**Theorem 2.** *Consider the sequence of processes* $\{\boldsymbol{q_r}[t]\}$, $\{\boldsymbol{q_r}[t]\}$ *converges weakly, as* $c \to 0$.

**Proof.** From DLA and (22), we can see $\{\boldsymbol{q_r}[t], t \geq 0\}$ is a Markov process. Also note that $\{\boldsymbol{q_r}[t], \ t \in [t, t+1)\}$ is a piecewise-constant, which is right continuous and have left hand limits. First, we define a function $f$ that satisfies:

$$\boldsymbol{q_r}[t+1] = \boldsymbol{q_r}[t] + cf(\boldsymbol{q_r}[t], \theta_r[t]). \tag{23}$$

This function represents the updating specified by (22), and is bounded and continuous. The function does not depend on $c$. We then define another function $\phi$ using:

$$\phi(\boldsymbol{q_r}[t]) = E[f(\boldsymbol{q_r}[t], \theta_r[t])|\boldsymbol{q_r}[t] = \boldsymbol{q}]. \tag{24}$$

Consider the following ordinary differential equation:

$$\frac{d\boldsymbol{q}}{dt} = \phi(\boldsymbol{q}),$$
$$\boldsymbol{q_r}(0) = \left[\frac{1}{2}, \frac{1}{2(K-1)}, \ldots, \frac{1}{2(K-1)}, \frac{1}{2(K-1)}\right]. \tag{25}$$

Hence by [31] (Theorem 3.2), the ordinary differential Eq. (25) has a unique solution, and the sequence $\{\boldsymbol{q}[t], \ t \in [t, t+1)\}$ converges weakly as $c \to 0$ to the solution of (25). □

The convergence of functions implied by weak convergence ensured by Theorem 2, along with the knowledge of the nature of the solutions of the ordinary differential Eq. (25), enables us to understand the long term behavior of $\boldsymbol{q}$.

## 6. Trust evolution

In trust management, when the behavior of one relay is consistent with the global network behavior, its trust value will be increased. Otherwise, the trust value of the relay will decrease. In practice and from (8), we assume each PU will choose a factor $\omega$ from a set $\{\mu_1, \ldots, \mu_l\}$ satisfying $\mu_i \in [0, 1], \ i = 1, \ldots, l$, and $\mu_1 < \ldots < \mu_i < \mu_{i+1} < \ldots < \mu_l$ where $\mu_l$ represents the highest level of factor $\omega$. Formally, the population state $\boldsymbol{\upsilon}[t] = (\upsilon_1[t], \ldots, \upsilon_l[t])^T$ describes the proportion of reproduction process, where $\upsilon_i, \ i = 1, \ldots, l$, is the proportion of PUs in the network selecting action $\mu_i$ at time $t$. The replicator dynamics are designed as follows:

$$\dot{\upsilon}_i = (U(\mu_i, \boldsymbol{\upsilon}_{-i}) - \overline{U}(\boldsymbol{\upsilon}))\upsilon_i, \tag{26}$$

where $\overline{U}(\boldsymbol{\upsilon})$ is the average utility of all PUs, and $U(\mu_i, \boldsymbol{\upsilon}_{-i})$ denotes the average payoff of PUs choosing $\mu_i$. It means that the strategy which works better than the average will be promoted [29]. The $\overline{U}(\boldsymbol{\upsilon})$ is given by:

$$\overline{U}(\boldsymbol{\upsilon}) = \frac{1}{n}\sum_{j=1}^{n} U_{PU_j}, \ \ j = 1, \ldots, n. \tag{27}$$

Using the replicator dynamics, players can adapt their strategy and converge to the evolutionary stable strategy (ESS) [30]. We provide the definition of ESS for the SRSG model to be as follows:

**Definition 3.** A strategy $\boldsymbol{\upsilon}^{opt}$ is an ESS, if for all $\boldsymbol{\upsilon} \neq \boldsymbol{\upsilon}^{opt}$ in some vicinity of $\boldsymbol{\upsilon}^{opt}$, there is an expected payoff function $\pi(\boldsymbol{\upsilon}, \boldsymbol{\upsilon}^{opt})$ satisfying the following conditions:

1. $\pi(\boldsymbol{\upsilon}, \boldsymbol{\upsilon}^{opt}) \leq \pi(\boldsymbol{\upsilon}^{opt}, \boldsymbol{\upsilon}^{opt})$,
2. if $\pi(\boldsymbol{\upsilon}, \boldsymbol{\upsilon}^{opt}) = \pi(\boldsymbol{\upsilon}^{opt}, \boldsymbol{\upsilon}^{opt})$, $\pi(\boldsymbol{\upsilon}, \boldsymbol{\upsilon}) \leq \pi(\boldsymbol{\upsilon}^{opt}, \boldsymbol{\upsilon})$ is satisfied.

To be specific, in condition (1) $\boldsymbol{\upsilon}^{opt}$ is the best response strategy of the game; hence, it is a NE. We also remark that condition (2) is interpreted as a stability condition. An ESS ensures the stability such that the population is robust to perturbations by a small fraction of players. The mutant strategy cannot invade the population when the perturbation is adequately small, and the incumbent strategy is an ESS. Based on the evolutionary game theory and the concept of ESS above, we propose a learning process (see Algorithm 2) to dynamically adjust the trust evolution, which is based on the complete information.

**Theorem 3.** *The trust evolution based on ESS algorithm (TEEA) converges to an equilibrium* $\boldsymbol{\upsilon}^*$ *such that PUs with different relays achieve the same expected utility:*

$$U_j(\mu_j, \boldsymbol{\upsilon}^*) = U_{j'}(\mu_{j'}, \boldsymbol{\upsilon}^*),$$
$$s.t. \ \forall j, j' \in \{1, 2, \ldots n\}, \ and \ \mu_j, \mu_{j'} \in \{\mu_1, \ldots, \mu_l\}. \tag{28}$$

*More specially, this equilibrium is an ESS.*

**Proof.** Since $U_j(\mu_j, \boldsymbol{\upsilon}^*) = U_{j'}(\mu_{j'}, \boldsymbol{\upsilon}^*), \ for \ \forall j, j' = 1, 2, \ldots n$, it follows that $\overline{U}(\boldsymbol{\upsilon}) = \frac{1}{n}\sum_{j=1}^{n} U_{PU_j} = U_j(\mu_j, \boldsymbol{\upsilon}^*)$, so $\dot{\upsilon}_i = 0$. In other words, $\boldsymbol{\upsilon}^*$ in (26) is an equilibrium of the proposed game.

We now suppose a PU $k$, $k \in \{1, 2, \ldots n\}$ makes an unilateral deviation to another action $\mu_{k'} \neq \mu_k$, and the population state turns into:

$$\boldsymbol{\upsilon}' = \Big(\upsilon_1, \ldots, \upsilon_{\mu_k - 1}, \upsilon_{\mu_k} - \frac{1}{n}, \upsilon_{\mu_k + 1}, \ldots, \upsilon_{\mu_{k'} - 1},$$
$$\upsilon_{\mu_{k'}} + \frac{1}{n}, \upsilon_{\mu_{k'}+1}, \ldots, \upsilon_l\Big). \tag{29}$$

Hence, the utility of PU becomes:

$$\begin{aligned} U_i(\mu_i, \boldsymbol{\upsilon}') &= aR_3\Im_{r^*}(\mu_i) - bP_u^*\gamma T - d^*P_{r^*}(1-\gamma)T \\ &= aR_3(\mu_i\Im_r^D + (1-\mu_i)\Im_r^R) - bP_u^*\gamma T - d^*P_{r^*}(1-\gamma)T \\ &< U_j(\mu_{j'}, \boldsymbol{\upsilon}'), \ \ i = k' \ or \ k, \ \ j \neq k', k. \end{aligned} \tag{30}$$

**Algorithm 2** Trust evolution based on ESS algorithm (TEEA) for PUs.

```
Given the equilibrium of proposed game $(r^*, P_u^*, \theta_r^*)$.
1. Initialize : $t = 0$
  • for each PU wanting to send a packet to PBS, initialize the system with strategy $(\omega[0], 1-\omega[0]) = (0.5, 0.5)$, and direct trust $\Im_r^D[0] = 1$ of relay $r$, where $r = 1, 2, \dots, m$;
  • gather the recommendations $\Im_r^R[0]$ from the neighbors of $r$;
  • calculate the trust value of relay $r$ according to (8);
  • decide whether to choose relay $r$ or not according to (11);
  • estimate the expect utility $U_i[1]$ of PU $i$ and average utility $\overline{U}[1]$ according to (9) and (27), $i = 1, \dots, n$;
2. Learn :
  • update $\Im_r^D[t]$ of $r$ at time $t$ according to (6);
  • gather recommendations $\Im_r^R[t]$ from the neighbors of $r$;
  • calculate trust value $\Im_r[t]$ of relay $r$ according to (8);
  • if $\Im_r \geq \Im^*$, choose a relay according to (11);
  • otherwise, PU initiate a new route discovery to PBS;
  • broadcast the chosen strategy and its utility to other PUs;
  • receive the information from other PUs and calculate the average utility $\overline{U}[t]$ of the network at time $t$ according to (27);
  • for each PU, if $U_i[t] < \overline{U}[t]$, select another strategy$(\omega[t], 1-\omega[t])$ with the probability updating according to (26);
  • otherwise, choose the strategy $(\omega[t-1], 1-\omega[t-1])$;
```

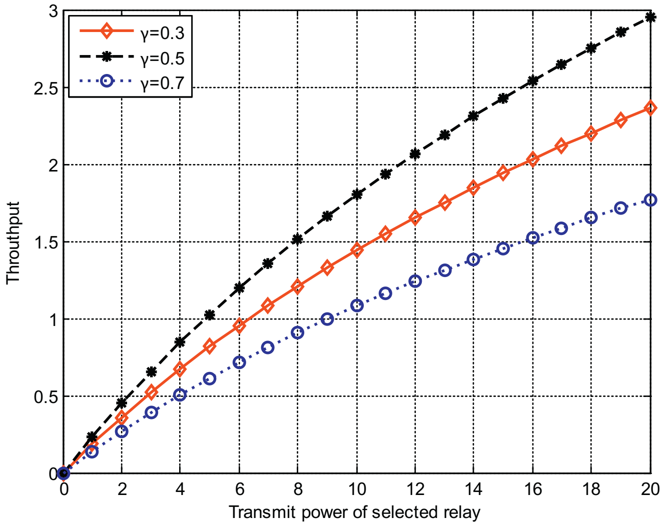


**Fig. 2.** Throughput versus transmission power of relay $P_r$.

For the equilibrium $\boldsymbol{\upsilon}^*$, we have $U_k(\mu_k, \boldsymbol{\upsilon}^*) = U_{k'}(\mu_{k'}, \boldsymbol{\upsilon}^*)$. Hence, $U_i(\mu_i, \boldsymbol{\upsilon}') < U_i(\mu_i, \boldsymbol{\upsilon}^*)$ is satisfied, for $i$ is one of $k$ and $k'$. Then, the stable of trust management is broken.

In conclusion, based on the definition of ESS in Definition 2, we know $\boldsymbol{\upsilon}^*$ is a strict NE, as well as an ESS. □

Note that in Algorithm 2, it is necessary for each PU to know the number of PUs, the average utility of primary network and the population state.

## 7. Simulation findings

In these simulations, we assume that the link bandwidth is 4.5 MHz, and the data-packet size is 1024 bytes. We set $g_1 = g_2 = 0.1$, $\varsigma = 0.1$, $e_1 = -1$, and $a = b = c = T = e_2 = 1$.

The expected throughput versus transmission power of relay $P_r$ in different cases with $P_u = 30$ are shown in Fig. 2. In case $\gamma = 0.7$, the network achieves a lower throughput than those of cases $\gamma = 0.3$ and $\gamma = 0.5$. This is due to the fact that SUs in case $\gamma = 0.7$ get less opportunities and time slots to access the spectrum than those in cases $\gamma = 0.3$ and $\gamma = 0.5$, and therefore, a lower enthusiasm relaying. We can also observe from Fig. 2 that the throughput value in the case $\gamma = 0.3$ is lower than those of cases $\gamma = 0.5$, as the number of PUs' packets decreases with the reducing of $\gamma$ (which are more efficient than the SUs). In other words, SRSG can achieve a higher throughput with an appropriate cooperation between PUs and relays.

We present the following scenarios as benchmark schemes:

(1) Nash equilibrium (NE) scheme [32]: Each PU decides the transmission power $P_u$ and relaying price $d$ without knowing the strategy of relay $r$. Thus, PU and relays set their strategies simultaneously; and

(2) Random power control (RAND) scheme: PU and relays randomly set their strategies, regardless of the existence of the others.

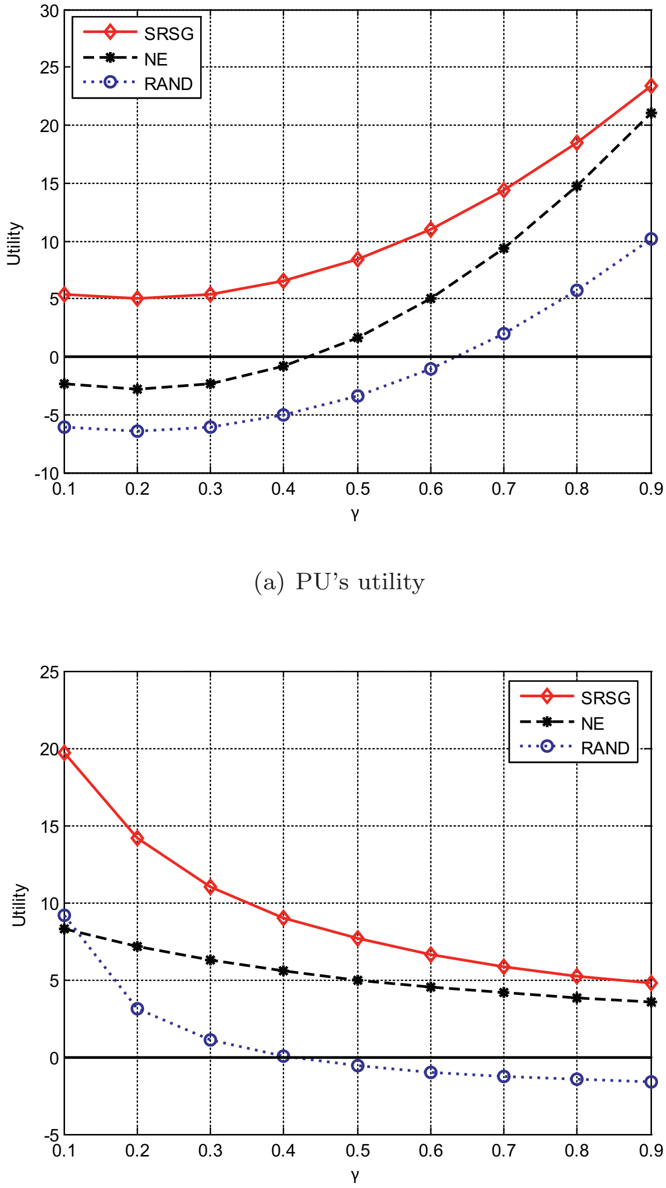
Fig. 3(a) and (b) shows the impact of time allocation coefficient $\gamma$ on the utility values of PU and SU, respectively. We can observe from Fig. 3 that the utility values of PU increases while SU's utility decreases. As $\gamma$ increases from $\gamma = 0.1$ and $\gamma = 0.9$, the proposed scheme leads to the highest utility values compared to NE and RAND schemes in both Fig. 3(a) and (b). It is because the selected relay in the proposed scheme chooses its own strategies based on the actions of PU. Therefore, the proposed game model performances better than NE model and RAND model in the energy efficiency and defending against the insider attackers. It also can observe from Fig. 3 that the utility value of RAND scheme is lowest. The reason is that the PU and relays randomly set their strategies without knowing each other's strategy and the existence of malicious SUs. Note that in Fig. 3(a) and (b), the utility values of the PU and the selected relay are all larger than 0 in the proposed scheme, which means that, in SRSG, the selected relay will always help the PU to transmit the packets, and the PU can get profit in the cooperative transmission.

In Fig. 4, we demonstrate the dynamics for the proposed game using the distributed learning algorithm (DLA) shown in Algorithm 1. As expected, starting from a high attack level $\theta$, which satisfies $\theta \in \{0, 1, 2, 3, 4, 5\}$, the SUs tend to reduce the attack level to zero after several steps. Consequently, the system tends to increase the utility value. Finally, the proposed game achieves a pure-strategy NE, which is shown in Fig. 4.

The converging process of the trust evolution based on ESS algorithm (TEEA) for achieving ESS is shown in Fig. 5. During the iterations, the strategies cause a lower utility value of each PU in (9). Strategies with a better influence in the utility value of PUs converge to 1. In other words, the converging process shows strategies which work better than the average utility will be promoted, and the population state soon achieves a unit vector. Finally, each PU will choose an optimal strategy, which is an ESS, for evolving the trust value.

Then, we compare the packet drop ratios of the proposed scheme whit HADOF [33], which focuses on detecting attackers without considering the cooperation between PUs and SUs, under random attacks with $\gamma = 0.5$. As shown in Fig. 6, the packet drop ratios of both schemes increase as the number of attackers increases. It can also be observed from Fig. 4 that the packet drop ratio of HADOF is higher than that of the proposed scheme. It is clear that the packet drop ratio of the proposed has a smaller packet drop ratio value, particularly as the number of attackers increases. Therefore, the proposed scheme performs better in defending the routing disruption attacks in a dynamic CCRN.

A comparative summary of outage probability of PUs under random attacks in different cases is shown in Fig. 5. As the number of attackers increases, the outage probability of PUs in SRSG and HADOF increases significantly. However, the higher $\gamma$ PUs take, the



(a) PU's utility

(b) SU's utility

**Fig. 3.** Impact of time allocation coefficient $\gamma$ on players' utility values.

higher outage probability they will get. Specially, the outage probabilities of PUs with $\gamma = 0.5$ and $\gamma = 0.3$ in SRSG are smaller than outage probability of PUs in HADOF. Therefore, as shown in Fig. 7, the proposed scheme performs better in defending against routing disruption attacks when the PUs take a relatively relative low $\gamma$. The reason is that the relays will perform better if there are enough idle slots which can be used by the relays in the CCRN. Therefore, the proposed model achieves a better performance in defending against attacks with an appropriate cooperation.

## 8. Conclusion

In this paper, we presented our proposed novel trust-Stackelberg game model with the aims of improving energy efficiency and defending against insider attacks in cooperative cognitive radio networks (CCRNs). In our approach, we also designed (1) a stochastic learning automata-inspired distributed learning al-

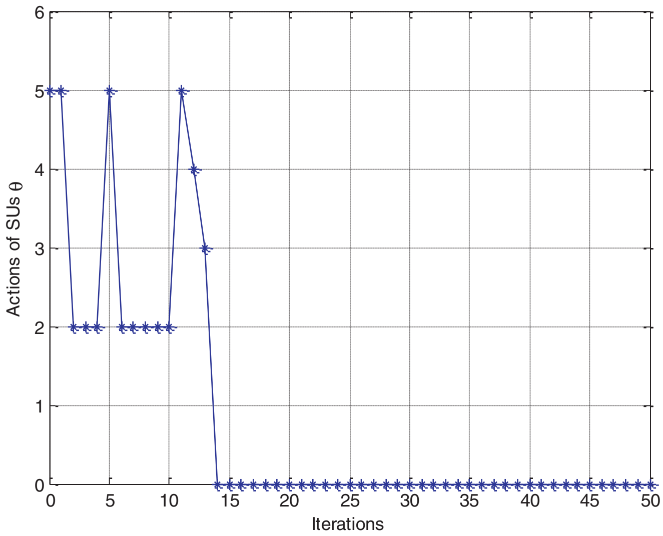


**Fig. 4.** Converging process of the distributed learning algorithm (DLA).

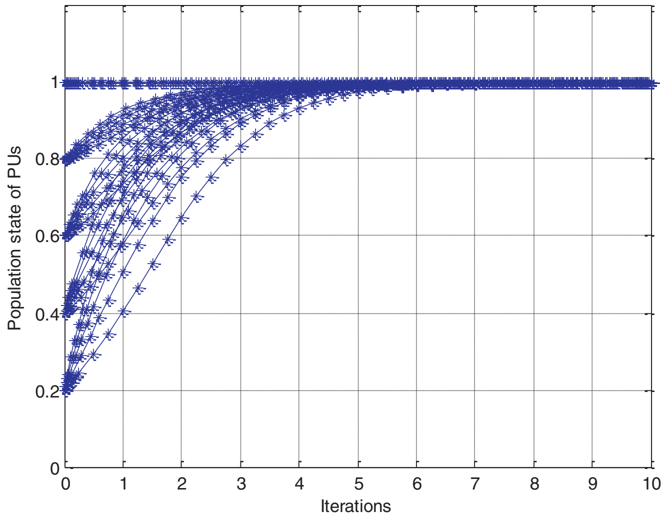


**Fig. 5.** Converging process of the trust evolution based on ESS algorithm (TEEA) for PUs.

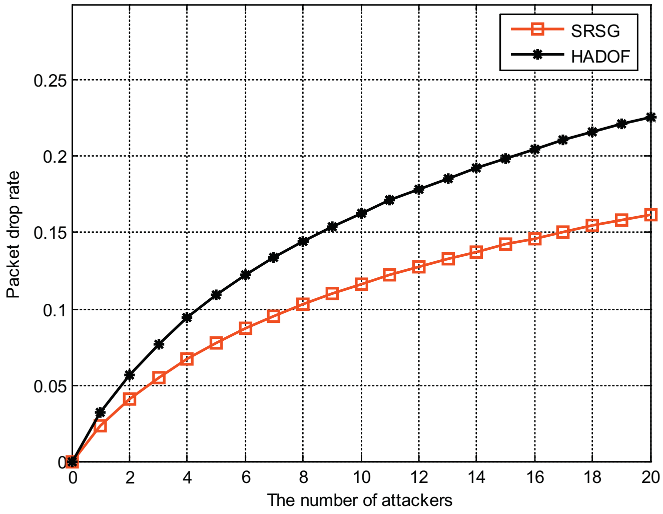


**Fig. 6.** Packet drop ratios versus the number of attackers.

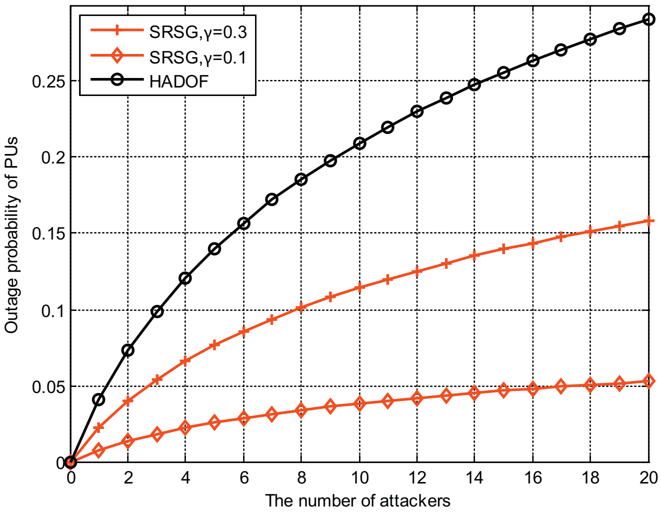


**Fig. 7.** Outage probability of PUs versus the number of attackers.

gorithm to achieve the equilibrium required in the game, and (2) a learning algorithm based on evolution game theory for PUs to self-adaptively adjust the trust evolution. The simulation findings confirmed that the proposed scheme performs better in defending against insider attacks and energy efficiency, in comparison to similar schemes.

We noted, however, that we only studied insider attacks relying on the assistance of relay selection in this paper. Therefore, a possible extension of this work will be to consider other security problems, such as eavesdropping or jamming attacks. For example, the eavesdropper and jammer can collaborate to undertake more damaging attacks. We speculate that a scheme based on physical-layer security and game theory will lead to a significant wireless security enhancement.

## Acknowledgment

The authors wish to thank National Natural Science Foundation of China (Nos. 61072080, U1405255), Fujian Normal University Innovative Research Team (No. IRTL1207) and Major Science and Technology Project in Fujian province (No. 2014H61010105).

## References

[1] J. Backens, C. Xin, M. Song, A novel protocol for transparent and simultaneous spectrum access between the secondary user and the primary user in cognitive radio networks, Comput. Commun. 69 (2015) 98–106.
[2] D. Li, Y. Xu, X. Wang, M. Guizani, Coalitional game theoretic approach for secondary spectrum access in cooperative cognitive radio networks, IEEE Trans. Wirel. Commun. 10 (2011) 844–856.
[3] X. Huang, T. Han, N. Ansari, On green-energy-powered cognitive radio networks, IEEE Commun. Surv. Tutor. 17 (2015) 827–842.
[4] S. Bhattacharjee, S. Sengupta, M. Chatterjee, Vulnerabilities in cognitive radio networks: a survey, Comput. Commun. 36 (2013) 1387–1398.
[5] Z. Zhang, H. Zhang, A variable-population evolutionary game model for resource allocation in cooperative cognitive relay networks, IEEE Commun. Lett. 17 (2013) 361–364.
[6] S. Parvin, F. Hussain, O. Hussain, Conjoint trust assessment for secure communication in cognitive radio networks, Math. Comput. Model 58 (2013) 1340–1350.
[7] G. Yin, Y. Wang, Y. Dong, H. Dong, Wright–Fisher multi-strategy trust evolution model with white noise for internetware, Expert Syst. Appl. 40 (2013) 7367–7380.
[8] H. Xiao, S. Ouyang, Power control game in multisource multirelay cooperative communication systems with a quality-of-service constraint, IEEE Trans. Intell. Transp. Syst. 16 (2015) 41–50.
[9] Y. Liu, L. Dong, Spectrum sharing in MIMO cognitive radio networks based on cooperative game theory, IEEE Trans. Wirel. Commun. 13 (2014) 4807–4820.
[10] B. Wang, Z. Han, K.J.R. Liu, Distributed relay selection and power control for multiuser cooperative communication networks using Stackelberg game, IEEE Trans. Mob. Comput. 8 (2009) 975–990.
[11] K. Zeng, P. Paweczak, D. Cabric, Reputation-based cooperative spectrum sensing with trusted nodes assistance, IEEE Commun. Lett. 14 (2010) 226–228.
[12] R. Trestian, O. Ormond, G.M. Muntean, Reputation-based network selection mechanism using game theory, Phys. Commun. 4 (2011) 156–171.
[13] L. Zhao, T. Hua, C. Lu, I. Chen, A topic-focused trust model for twitter, Comput. Commun. 76 (2016) 1–11.
[14] K. Hamouid, K. Adi, Efficient certificateless web-of-trust model for public-key authentication in MANET, Comput Commun 63 (2015) 24–39.
[15] X. Huang, N. Ansari, Joint spectrum and power allocation for multi-node cooperative wireless systems, IEEE Trans. Mob. Comput. 14 (2015) 2034–2044.
[16] X. Huang, N. Ansari, Data and energy cooperation in relay-enhanced OFDM systems, in: Proceedings of IEEE International Conference on Communications, 2016.
[17] Y. Wu, T. Zhang, D.H.K. Tsang, Joint pricing and power allocation for dynamic spectrum access networks with Stackelberg game model, IEEE Trans. Wirel. Commun. 10 (2011) 12–19.
[18] L. Xiao, Y. Chen, W. Lin, K.J.R. Liu, Indirect reciprocity security game for large-scale wireless networks, IEEE Trans. Inf. Forens. Secur. 7 (2012) 1368–1380.
[19] J. Chen, A.R. Kiremire, M.R. Brust, V.V. Phoha, Modeling online social network users' profile attribute disclosure behavior from a game theoretic perspective, Comput. Commun. 49 (2014) 18–32.
[20] N. Basilico, N. Gatti, M. Monga, S. Sicari, Security games for node localization through verifiable multilateration, IEEE Trans. Depend. Secure Comput. 11 (2014) 72–85.
[21] Q. Cao, H.V. Zhao, Y. Jing, Power allocation and pricing in multiuser relay network using Stackelberg and bargaining game, IEEE Trans. Veh. Technol. 61 (2012) 3177–3190.
[22] M.H. Eiza, T. Owens, Q. Ni, Secure and robust multi-constrained QoS aware routing algorithm for VANETs, IEEE Trans. Depend. Secure Comput. 13 (2016) 32–45.
[23] Y. Zhong, B. Bhargava, Y. Lu, P. Angin, A computational dynamic trust model for user authorization, IEEE Trans. Depend. Secure Comput. 12 (2015) 1–15.
[24] L. Guo, C. Zhang, Y. Fang, A trust-based privacy-preserving friend recommendation scheme for online social networks, IEEE Trans. Depend. Secure Comput. 12 (2015) 413–427.
[25] X. Huang, Y. Xiang, E. Bertino, J. Zhou, L. Xu, Robust multi-factor authentication for fragile communications, IEEE Trans. Depend. Secure Comput. 11 (2014) 568–581.
[26] D. Yang, X. Fang, G. Xue, HERA: an optimal relay assignment scheme for cooperative networks, IEEE J. Sel. Areas Commun. 30 (2012) 245–253.
[27] Y. Shen, Z. Yan, R. Kantola, Analysis on the acceptance of global trust management for unwanted traffic control based on game theory, Comput. Secur. 47 (2014) 3–25.
[28] H. Yahyaoui, A trust-based game theoretical model for web services collaboration, Knowl.-Based Syst. 27 (2012) 162–169.
[29] X. Chen, J. Huang, Evolutionary stable spectrum access, IEEE Trans. Mob. Comput. 12 (2013) 1281–1293.
[30] B. Wang, Y. Wu, K.J.R. Liu, Game theory for cognitive radio networks: an overview, Comput. Netw. 54 (2010) 2537–2561.
[31] P.S. Sastry, V.V. Phansalkar, M.A.L. Thathachar, Decentralized learning of Nash equilibria in multi-person stochastic games with incomplete information, IEEE Trans. Syst. Man Cybern. 24 (1994) 769–777.
[32] D. Yang, J. Zhang, X. Fang, G. Xue, A. Richa, Optimal transmission power control in the presence of a smart jammer, in: Proceedings of IEEE Global Communications Conference (GLOBECOM), 2012, pp. 5506–5511.
[33] W.R. Wade, An Introduction to Analysis, 4th edition, Pearson, 2010.