Secure Cooperative Spectrum Sensing and Allocation in Distributed Cognitive Radio Networks

Hui Lin, Jia Hu, Chuan Huang, Li Xu, and Bin Wu

1Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China
2College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX4 4QF, UK
3State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Correspondence should be addressed to Jia Hu; jiahu9@gmail.com

Received 10 May 2015; Revised 15 September 2015; Accepted 21 September 2015

1. Introduction

Cognitive radio networks (CRNs) are promising wireless communications systems that can resolve the spectrum scarcity problem arising from the escalating demand of wireless radio frequency and spectrum underutilization by license holders [1]. The architecture of CRNs is depicted in Figure 1, which consists of base stations and cognitive terminals. The base stations (i.e., primary users) constitute a primary network using the licensed spectrum and the cognitive terminals (i.e., secondary users) form a secondary network that makes use of the licensed spectrum when it is not occupied by the primary users [2]. To avoid the potential interference with the primary users, secondary users firstly sense whether the spectrum of interest is being used by the primary users. If the spectrum is unoccupied, the secondary users apply certain spectrum allocation scheme to decide which of them may access the available spectrum [3].

CRN can improve the efficiency of spectrum usage, but it also introduces new security threats including internal attacks during the spectrum sensing and allocation process, which can degrade the effectiveness of spectrum sensing and allocation dramatically. For example, an adversary may launch data or information falsification attacks during spectrum sensing and allocation process, where the adversary corrupts a subset of secondary users as illustrated in Figure 2 to report falsified data or information, aiming to affect the final group decision [2].

Cooperation in spectrum sensing and allocation can be achieved in two models: centralized or distributed. The former uses a common receiver (i.e., fusion center) to collect sensing results from all SUs and to make final spectrum sensing and allocation decisions [1, 4]. In contrast, a distributed approach allows SUs to share individual sensing results with their neighbors and to make their own sensing and allocation decisions [3, 5]. Despite the many benefits cooperative spectrum sensing and allocation process entitles, it is vulnerable to many potential attacks. A distributed scheme is even more vulnerable to such attacks due to its distributed and cooperative natures.
A number of papers [4–9] propose various methods to improve the security in spectrum sensing and allocation. These solutions are usually based on a centralized infrastructure, where a central authority plays an essential role in coordinating the attack defending. However, the centralized schemes will incur heavy communication overheads, and the malicious nodes can compromise the central authority to paralyze the entire system. Different distributed sensing schemes have also been proposed [10–14], using game theory [10], incentive design [11], consensus algorithm [3, 12], outlier detection, computation verification [14], and so forth. Most of the existing works ignore the internal attacks launched by an inside attacker that has the legal identity. To overcome the above-mentioned problems, in this paper, we firstly design a distributed secure sensing strategy based on a dynamic reputation model.

The strategy establishes a distributed reputation database for nodes as a basis for the channel search sequence in spectrum sensing. Next, we design a novel Vickrey-Clarke-Groves (VCG) mechanism [3, 15] based on the reputation generated from exchanged sensing results and propose a novel cheat-proof spectrum resource allocation strategy to restrict the impact of the malicious behaviours. As an important mechanism design, the VCG mechanism studies how to design mechanisms to incent the players (i.e., users or nodes) to provide truthful information about their preferences over different outcomes [3, 15]. A VCG mechanism is a dominant strategy mechanism, which can achieve ex-post incentive compatibility (truth-telling is a dominant strategy for every player in the game) [3, 15].

This paper makes the following main contributions.

(1) The reputation model and Vickrey-Clarke-Groves (VCG) mechanism are introduced into the cooperative sensing and spectrum allocation strategies. This combination can better reflect the real world nature of communication networks and defend against spectrum sensing data falsification (SSDF) attacks from internal malicious nodes.

(2) A distributed algorithm is designed to help secondary users compute the sensing result and allocate the spectrum. Secondary users iteratively update their local values to arrive at consensus, without help from any central authority.

(3) Simulation results demonstrate that the proposed strategies can provide an effective countermeasure against the internal SSDF attacks without relying on a central authority or a common control channel and are therefore applicable in distributed CRNs.

In the rest of the paper, Section 2 reviews related work. Section 3 introduces the network and adversary models. Section 4 presents the distributed secure cooperative sensing strategy. Section 5 presents the VCG based distributed cheat-proof spectrum allocation strategy. Section 6 presents the simulation results and performance analysis. Section 7 concludes the paper.

2. Related Work

2.1. Distributed Spectrum Sensing. Distributed spectrum sensing in CRNs has been widely studied, using game theory [10], incentive design [11], consensus algorithm [3, 12], outlier detection, computation verification [14], and so forth. For instance, Mukherjee [10] discussed cooperative sensing problem in distributed CRNs with the game-theoretic models. Mukherjee considered the utility function for secondary users as improved sensing accuracy and examined the impact of various sensing parameters. Li et al. [11] first identified a new selfishness model named entropy selfishness in distributed CRNs. They further proposed YouSense, a one-time pad based incentive design in which sensing reports were encrypted before sharing, to prevent the entropy selfish users from learning the sensing reports. And yet, the honest user can recover this plaintext by spectrum sensing. Li et al. [3, 12] proposed a distributed and scalable cooperative spectrum sensing scheme based on recent advances in consensus algorithms. In the proposed scheme, the secondary users can maintain coordination based on only local information exchange without a centralized common receiver and the proposed scheme used the consensus of secondary users to make the final decision. Zhang et al. [2, 13] designed a fully distributed security scheme RediSen to counter attacks in cooperative sensing. RediSen applied the reputation generated from exchanged sensing results as an aid to restrict the impact of the malicious behaviours. Yan et al. [14] proposed a robust distributed outlier detection scheme with adaptive local threshold to counter covert adaptive attacks by exploiting the state convergence property. In addition, they also presented a hash-based computation verification scheme to effectively defend against colluding attackers.
2.2. Spectrum Allocation. There are a number of works focused on spectrum allocation [16–21] in CRNs. For example, Xie et al. [16] formulated the energy-efficient resource allocation problem in heterogeneous CRNs with femtocells as a Stackelberg game and a gradient based iteration algorithm is proposed to obtain the Stackelberg equilibrium solution to the energy-efficient resource allocation problem. Jiang et al. [17] proposed a novel channel allocation scheme for the QoE-driven multimedia transmission over the CRNs. Moreover, a new analytical Markov model combining the ON/OFF model of PCs and the service queuing model is derived to evaluate the system performance. Xie et al. [18] studied the problem of resource allocation in CRNs supporting heterogeneous services with imperfect channel sensing. To reduce the computation complexity in the formulation with the imperfect channel information, Xie et al. formulated the problem of resource allocation as a mixed integer programming problem and proposed an aggressive discrete stochastic approximate algorithm based joint power and channel allocation. Tan and Le [19] first presented an optimal brute-force search algorithm to resolve the spectrum resource allocation problem for CRNs. And then, Tan and Le further proposed two channel assignment algorithms to resolve the high complexity of the optimal search. Wang et al. [20] proposed a mechanism to resolve the complex mixed integer programming problem faced in the resource allocation process in CRNs. The proposed mechanism developed a fast barrier-based method which can achieve the optimal solution with an almost linear complexity and also proposed a method which can achieve nearly optimal solution with a constant complexity. Tachwali et al. [21] developed a new resource allocation optimization framework for single-cell multiuser multicarrier CRNs in the presence of multiple primary networks. The framework aims to minimize the spectral footprint of the CRN through the bandwidth-power product metric. The protection of PU from harmful interference is incorporated in the framework through PU activity index.

2.3. Joint Design of Spectrum Sensing and Spectrum Allocation. The joint design of spectrum sensing and spectrum allocation in CRNs has attracted much attention from both industry and academia. El-Sherif and Liu [22] proposed a novel joint design of the spectrum sensing and channel access mechanisms based on the observation that the value of the test statistics could be used as a confidence measure for the test outcome. Therefore, this value can be used to define different channel access probabilities for secondary users. Zhang et al. [3] designed a distributed scheme to incentivize participation of nodes in cooperative sensing, by connecting sensing and spectrum allocation, and offering incentive from the latter to the former. In the proposed scheme, reputation is used as a pricing factor to incentivize cooperative sensing and a reputation-based pricing method is proposed to offer strong incentive for secondary users to pursue a lower price in the spectrum allocation process.

Existing spectrum sensing and allocation methods and security mechanisms are usually based on a centralized infrastructure, where a central authority plays an essential role in coordinating the defense against attacks and thus brings heavy communication overheads and the issue that central authority may be compromised by attackers. Moreover, few works took into account the joint design of spectrum sensing and spectrum allocation, but they only considered individual spectrum sensing or allocation. In particular, they did not consider the internal attacks launched by an inside attacker that has the legal identity. Consequently, it is still an open problem and a challenging task to design secure and distributed spectrum sensing and allocation schemes in CRNs to resist the internal attacks. The main notations and symbols used in this paper are summarized in Notations and Symbols.

3. Network and Adversary Models

3.1. Network Model. We consider a distributed CRN consisting of a primary user network and a secondary user network [3, 13]. There are $N$ secondary users and $K$ orthogonal frequency channels. Let $\Omega_N = \{1, 2, \ldots, N\}$ and $\Omega_K = \{1, 2, \ldots, K\}$ denote the sets of secondary users and channels, respectively. We suppose that each secondary user is equipped with a cognitive radio and they utilize omni-directional antennas to communicate with each other. Meanwhile, secondary users are located within the transmission range of the primary users and can individually sense the environment to detect the existence of the primary users [3, 13]. In the cooperative sensing process, we use the energy sensing method for a secondary user to detect primary users’ presence. We also assume that an adversary can compromise a subset of honest secondary users. A secondary user may provide incorrect information (including attacking malicious users and honest users that sense channels incorrectly due to severe fading or system failure) or correct information (including honest users that sense channels correctly and nonattacking malicious users). An honest user has no a priori information on which of its neighbors are malicious. If the final sensing results indicate that the primary users are not transmitting on certain channels, the secondary users use the spectrum allocation scheme to allocate spectrum and transmit on these channels.

3.2. Adversary Model. In distributed CRNs, the secondary user network is vulnerable to both external and internal attacks. External attacks can be effectively solved by using the traditional cryptography theory and authentication method. The internal attacks are launched by an inside attacker that has the legal identity, which makes the traditional encryption and authentication techniques no longer effective. In the internal attacks, the attackers may or may not participate in the cooperative sensing process and may report falsified values when participating.

We assume that, in spectrum sensing, malicious secondary users strategically report falsified sensing results, aiming at incurring interference between the primary users and legitimate secondary users. In spectrum allocation, malicious secondary users may launch collision attacks or bad mouthing attacks to report falsified reputation values, aiming to keep the legitimate secondary users away from using the spectrum resource.
4. Distributed Secure Cooperative Sensing Strategy (DSCS)

Distributed cooperative sensing strategy implements spectrum sensing through the distributed secondary users in a wide area. In distributed cooperative sensing, each secondary user obtains a local measurement in a time interval $T$. After a sensing session, a series of value update sessions are executed by the secondary users. All secondary users exchange their local spectrum sensing results with their neighbors within its communication range and update their own values based on the received values.

Since distributed cooperative sensing can enhance sensing accuracy, while reducing the need for sensitive and expensive sensing technology, it is proposed to enhance the sensing performance [3, 13]. However, it is vulnerable to the internal attacks threats. The internal adversary may control some nodes to report false sensing results to degrade the final sensing decision, which will make the performance of cooperative sensing degrade significantly.

Reputation systems are widely used to cope with liars holding false positive/negative opinions [23]. The concept of reputation has been widely used in economics, ecology, anthropology, and other social sciences. A rich body of literature has been devoted to the investigation of different reputation systems for computer networks [24–26]. Recently, derived from the Dempster-Shafer theory [27] and with the ability to explicitly represent and manage a node’s uncertainty, subjective logic and uncertainty based reputation mechanism has emerged as an attractive tool for handling trust relationships and has attracted much attention in distributed CRNs.

In this section, we propose DSCS, a reputation-based sensing strategy that is a distributed cooperative strategy using subject logic based reputation mechanism to defend against internal malicious secondary users’ attacks.

Subjective logic [28, 29] represents a specific belief calculus that uses a belief metric called opinion to express subjective reputation. Since it is necessary to develop mechanisms to detect and manage malicious users in distributed CRNs, subjective logic with the ability to explicitly represent and manage a user’s uncertainty has emerged as an attractive tool for handling trust relationships in distributed CRNs.

In subjective logic each opinion is denoted by a 4-tuple $\omega_{x:y} = (b_{x:y}, d_{x:y}, a_{x:y}, u_{x:y})$, where $b_{x:y}$, $d_{x:y}$, and $u_{x:y}$ designate node x’s belief, disbelief, and uncertainty towards y, respectively. The base rate $a_{x:y}$ designates x’s willingness to believe y which determines how uncertainty is viewed as belief when the reputation is used. The uncertainty reflects the confidence in node x’s knowledge of y; an uncertainty of 1.0 represents that a node has no basis for any conclusion. They satisfy the following conditions:

$$b_{x:y} + d_{x:y} + u_{x:y} = 1.0,$$

$$b_{x:y}, d_{x:y}, a_{x:y}, u_{x:y} \in [0.0, 1.0].$$

When an opinion is used in a decision, it is projected onto the belief/disbelief axis through its expectation, $E(\omega_{x:y})$,

which is used to identify malicious nodes and can be computed as

$$E(\omega_{x:y}) = b_{x:y} + a_{x:y}u_{x:y}.$$

However, for the case that the belief, disbelief, uncertainty, and base rate change over time, the secondary users’ reputation evaluation and the trust relationship between the secondary users also changes over time. Therefore, the reputation evaluation and the trust relationship at present time depends not only on the values of the underlying parameters but also on the decayed values of the previous trust.

Let $\omega_{h,n}^{direct}(b_n, d_n, u_n, a_n)$ be the direct opinion of user x to user y at time $t_n$, which is stored in x’s local reputation table and can be computed at x as follows:

$$b_n = \frac{1}{|C|} \sum_{c \in C} N^s_{(n, x:y)}^f (n, x:y),$$

$$d_n = \frac{1}{|C|} \sum_{c \in C} (1 - p^{uncertain}_c) N^f_{(n, x:y)} (n, x:y),$$

$$u_n = \frac{1}{|C|} \sum_{c \in C} P_c^{uncertain} N^f_{(n, x:y)} (n, x:y),$$

$$a_n = 0.5,$$

where $N^f_{n, x:y}$ is the total number of the sensing results that x received from the user y. $N^s_{n, x:y}$ is the number of the correct results and $N^f_{n, x:y}$ is the number of the wrong results from y, respectively. $a_n = 0.5$ stands for the case that x’s willingness to believe y is 50%.

$P_c^{uncertain}$ denotes the degree of uncertainty whether y is trustworthy. $P_c^{uncertain}$ can be computed as

$$p^{uncertain} = p_c \cdot d_c \cdot (1 - p_f),$$

$$p_d = 1 - p_m,$$

where we assume that the channel is AWGN, $p_c$ denotes the transition probability of the channel state from 1 to 0 after y has sent some sensing results. $p_f$ is the detection probability of the secondary user, $p_f$ is the false alarm rate, and $p_m$ is the false negatives rate. $p_f$ and $p_d$ are defined as

$$p_f = \Pr \{ Y > \tau \mid H_0 \} = 1 - \Gamma \left( \frac{L}{2}, \frac{\tau}{2\sigma_0^2} \right),$$

$$p_d = \Pr \{ Y > \tau \mid H_1 \} = 1 - \Gamma \left( \frac{L}{2}, \eta \frac{\sigma_0^2}{\sigma_1^2} \right),$$

where $H_0$ is the zero hypothesis, indicating that the sensed channel is idle, while $H_1$ is the alternative hypothesis, indicating that the channel is busy. $Y$ is the output and $\tau$ denotes the threshold. The signal/noise ratio (SNR) is $(\sigma_1^2 - \sigma_0^2)/\sigma_0^2$. $L$ is the number of testing samples, $\eta$ satisfies $\Gamma(L/2, \eta) = 1 - p_f$, and $\Gamma(\cdot, \cdot)$ denotes the incomplete Gamma function.
Algorithm 1: Distributed secure cooperative sensing strategy (DSCS).

Considering the influence of time on opinion, the time-dependent value of a trust relationship from time $t_i$, computed at the present time $t_n$, is given by

$$
\begin{align*}
    b_n &= b_i \times e^{-(b_i)^{-1}\Delta t}^k, \\
    d_n &= d_i \times e^{-(d_i)^{-1}\Delta t}^k, \\
    u_n &= 1 - b_n - d_n, \\
    a_n &= a_i \times e^{-(a_i)^{-1}\Delta t}^k, \\
    \Delta t &= t_n - t_i,
\end{align*}
$$

where $k$ ($k \geq 1$) is the decay rate determining the rate of change over time of the opinion. $\Delta t$ ($\Delta t > 1$) is the interval between $t_i$ and $t_n$. When $\Delta t \to \infty$, $e^{-(b_i)^{-1}\Delta t}^k \to 0$ and hence $b_n \to 0$. This corroborates that the past opinion value has less influence on the present opinion evaluation as the time interval between them increases.

The dynamic final reputation considering the trust decay at the time $t_n$ can be given by

$$
\alpha_{\text{final}}^{x:y} = \eta_1 \times (b_i, d_i, u_i, a_i) + \eta_2 \times (b_n, d_n, u_n, a_n),
$$

where $\eta_1$ and $\eta_2$ are the weight factors ($\eta_1 + \eta_2 = 1, (\eta_1, \eta_2 \in [0, 1])$) used to determine how much the reputation evaluation results at times $t_i$ and $t_n$ affect the dynamic final reputation. When $E(\alpha_{\text{final}}^{x:y})$ is less than the threshold, the secondary user will start the recommendation reputation and final reputation evaluation [25, 26].

Based on the abovementioned dynamic reputation model and combining with the characteristics of CRN, a reputation-based distributed secure cooperative sensing strategy (DSCS) is proposed. In DSCS, a secondary user combines its sensing results with the results of cooperative group members to evaluate the true state of the channel to improve the accuracy of sensing. Moreover, DSCS can also punish the untrustworthy user to reduce the influence of the false information to the network. The details of the DSCS are described in Algorithm 1. It is worth noting that $DB_{\text{local}}^{X}$ is $x$'s local reputation table. The size of the table is 1 Mb–10 Mb depending on the number of cycles in the simulation, so the memory overhead is not much considering the memory size of modern devices.

5. Distributed Cheat-Proof Spectrum Allocation Strategy (DCSA)

After spectrum sensing, how to ensure the rationality and reliability of spectrum resource allocation is a new challenge for distributed CRNs. In this section, a novel cheat-proof spectrum allocation strategy based on Vickrey-Clarke-Groves (VCG) mechanism is proposed. With the mechanism, we formulate the utility function of system and malicious users and then analyze and prove the efficiency of the strategy through the utility function.
In DCSA, we denote the channel set that can be controlled as \( C = \{c_1, c_2, \ldots, c_m \mid m > 1 \} \) and define the relevant bandwidth set as \( B = \{b_1, b_2, \ldots, b_n\} \), where \( m \) represents the number of channels. We model the spectrum allocation processes as a VCG based auctions process and define the user’s profit model, system’s profit model, and VCG based distributed cheat-proof mechanism as follows.

### 5.1. User's Profit Model

Suppose user \( i \) has got the permission to access the channel \( c \) \((c \in C)\) and its throughput requirement is \( q_i \), which is often private information known only to the user itself. Here, we adopt classical transmission model \([30]\) as

\[
q = \log_2 (1 + Q \cdot y),
\]

\[
Q = \frac{1.5}{\ln (0.2/\text{BER}^{\text{tar}})},
\]

where \( Q \) is the transfer efficiency and \( y \) is the signal-to-noise ratio of the receiver.

The profit of the user \( i \), \( u_i(q_i, c) \), can be expressed as

\[
u_i(q_i, c) = \begin{cases} V(q_i) - P(q_i, c), & \text{purchase} \\ 0, & \text{do not purchase}, \end{cases}
\]

where \( V(q_i) \) is the profit function that the profits user \( i \) will gain when it gets the access permission. \( V(q) \) can be computed as

\[
V(q) = aq^2 + bq
\]

s.t. \( q_i = 0 \),

\[
V(0) = 0
\]

\[
V'(q_i) > 0,
\]

\[
V''(q_i) < 0
\]

in which \( a \) and \( b \) are the weight factors. \( P(q_i, c) \) is the cost of user \( i \) and can be computed as

\[
P(q_i, c) = p_c q_i
\]

where \( p_c \) is the cost of channel \( c \). \( p_c \) is relevant to the reputation; the higher the reputation the lower the cost.

Hence, when \( q_i > 0 \), the profit of the user \( i \), \( u_i(q_i, c) \), can be computed as

\[
u_i(q_i, c) = aq_i^2 + (b - p_c)q_i.
\]

### 5.2. System’s Profit Model

We consider distributed CRNs consisting of \( n \) \((n = n_1 + n_2, n_1 \geq 1, n_2 \geq 1)\) users, where \( n_1 \) and \( n_2 \) represent the number of the primary users and secondary users, respectively. In the round of channel allocation, let \( o = (c_{ij} \mid i = 1, 2, \ldots, m; j = 1, 2, \ldots, n) \) denote the set of channel allocation, where \( c_{ij} \) indicates that the channel \( i \) is assigned to the user \( j \). The system’s best profit \( \pi^* \) can be expressed as

\[
\pi^* = \sum_{i=1}^{n} u_i(q_i, o^*) = \max_{o_c \in O} \sum_{i=1}^{n} u_i(q_i, o_k),
\]

in which \( o^* \) is the best allocation results and can be computed as

\[
o^* = \arg \max_{o_c \in O} \sum_{i=1}^{n} u_i(q_i, o_k).
\]

### 5.3. VCG Based Distributed Cheat-Proof Mechanism

In the distributed spectrum allocation process, some secondary users behave maliciously to maximize their own performance by providing the false resource demand. To offer stronger incentives for secondary users to honestly participate in the spectrum allocation process, we connect spectrum allocation to the reputation through a VCG based distributed cheat-proof mechanism.

Based on the abovementioned analysis in Sections 5.1 and 5.2, we first propose a distributed cheating-proof mechanism detailed description as follows.

In the proposed mechanism, the secondary user must pay taxes \( T(q_i, o) \) > 0 in addition to the cost of channel to gain the spectrum resource. The taxes for a user \( i \) denoted by \( T_i(q_i, o^*) \) can be expressed as

\[
T_i(q_i, o^*) = \sum_{j \neq i} u_j(q_j, o^-) - \sum_{j \neq i} u_j(q_j, o^*),
\]

in which \( \sum_{j \neq i} u_j(q_j, o^-) \) is the total utility of all the other applicants when \( i \) participates in the mechanism. As opposed to \( \sum_{j \neq i} u_j(q_j, o^*) \), \( \sum_{j \neq i} u_j(q_j, o^-) \) is the total utility of all the other applicants when \( i \) withdraws from the mechanism. Then, the best utility of user \( i \) can be expressed as

\[
u_i^*(q_i, o^*) = u_i(q_i, o^*)
\]

\[
- \left[ \sum_{j \neq i} u_j(q_j, o^-) - \sum_{j \neq i} u_j(q_j, o^*) \right].
\]

A mechanism is the VCG mechanism if it can satisfy the following conditions \([15, 31, 32]\):

1. The mechanism is incentive compatible.
2. The mechanism is individual rational.

Next, we will prove that the proposed distributed cheating-proof mechanism is a VCG mechanism.

**Theorem 1** (the mechanism is incentive compatible (IC)). A mechanism is incentive compatible (IC) if truth-telling is the best strategy for the users, which means that the users have no incentive to reveal false information.

**Proof.** Suppose user \( i \) needs \( q_i \) unit resource, but it applies for \( q_j \) and declares that \( u_i(q_j) \) > \( u_i(q_i) \), which gets the outcome \( \tilde{o} \). According to the above description, user \( i \) needs to pay the taxes as

\[
T_i(q_i, \tilde{o}) = \sum_{j \neq i} u_j(q_j, o^-) - \sum_{j \neq i} u_j(q_j, \tilde{o}).
\]
individual rational (IR). In our simulations, the number of secondary users is 5 (secondary user is denoted by $x$ in the simulations) and the number of detectable channels of each secondary user is 4. The initial reputation of $x$ is 5 (secondary user is denoted by $x$ in the simulations).

In conclusion, according to the definition of VCG, the proposed mechanism is a VCG mechanism.

The details of the DCSA are described in Algorithm 2. In DCSA, the application and allocation of channels are done in competing slots, which have two stages. At the first stage, the base station calculates the best allocation results and then allocates the channels based on the demands from primary users. Primary users can apply for consecutive slots to complete its transmission. At the second stage, base station allocates the remaining vacant channels to secondary users, who can only apply for one slot in order to avoid the interference with primary users. After the allocation, base station waits for the users to complete transmission and then reallocate channels in the next competing slot.

\[\text{Algorithm 2: Distributed cheating-proof spectrum allocation strategy (DCSA).}\]

\begin{algorithm}
\begin{algorithmic}
\State \textbf{Input:} Channel set $C$, bandwidth set $B$, number of user $n$ and iterations loop
\State \textbf{Output:} The resource allocation results, the total profit of the PU and SU secondary users $\pi_{PU}^*$, $\pi_{SU}^*$
\Procedure{\textbf{loop}}{1}
\While{\text{loop} > 0}
\State Receive (user's resource request);
\State Allocate the channel to the PU according to the $\alpha_{PU}^*$;
\State Compute the total profit of the PU $\pi_{PU}^*$ according to the $\alpha_{PU}^*$;
\State If there are the idle channel then
\State Compute the $\alpha_{SU}^* = KM(q_{SU})$ according to the SU's resource requirement $q_{SU}$;
\State Allocate the channel to the SU according to the $\alpha_{SU}^*$;
\State Compute the total profit of the SU $\pi_{SU}^*$ according to the $\alpha_{SU}^*$;
\EndIf
\State End if
\State loop--;
\EndWhile
\State \textbf{End}
\EndProcedure
\end{algorithmic}
\end{algorithm}

\begin{equation}
\tilde{u}_i(q_i, \tilde{\sigma}) = u_i(q_i, \tilde{\sigma}) - \left[ \sum_{j \neq i} u_j(q_j, o, \sigma) - \sum_{j \neq i} u_j(q_j, \tilde{\sigma}) \right] \\
= u_i(q_i, \tilde{\sigma}) + \sum_{j \neq i} u_j(q_j, \tilde{\sigma}) - \sum_{j \neq i} u_j(q_j, o, \sigma) \\
= \pi(\tilde{\sigma}) - \sum_{j \neq i} u_j(q_j, o, \sigma).
\end{equation}

For $\pi(\tilde{\sigma}) \leq \pi^*$, we can get $\tilde{u}_i(q_i, \tilde{\sigma}) \leq u_i^*(q_i, o^*)$, which incents user $i$ to give true application resources and truth-telling is the best strategy for user $i$. \hfill \Box

\textbf{Theorem 2} (the mechanism is individual rational (IR)). In an individual rational (IR) mechanism, rational users are expected to gain a higher utility from actively participating in the mechanism than from avoiding it.

\textbf{Proof.} In the proposed mechanism, we consider the following two malicious behaviors:

1. The user does not have the requirement, but it still applies for resources.
2. The user does not have enough to pay the cost and taxes for the resource, but it still applies for resources.

The utility of the user with these malicious behaviors, $\tilde{u}_i(q_i, \tilde{\sigma})$, can be computed as

\begin{equation}
\tilde{u}_i(q_i, \tilde{\sigma}) = u_i(q_i, \tilde{\sigma}) - T_i(q_i, \tilde{\sigma}).
\end{equation}

It is easy to show that in both cases the $\tilde{u}_i(q_i, \tilde{\sigma}) < 0$ when the incentive compatible is achieved. Therefore, for each user $i$, utility $> 0$ and participation into the recommendation is an optimal choice, which means that the mechanism is individual rational.

\section{Performance Evaluation}

In this section, we implement our strategies and conduct extensive simulation experiments using MATLAB to verify the efficacy of the proposed strategies. We assume that the malicious nodes can launch SSDF attacks in the sensing and allocation process by reporting falsified values. They can also implement the Random Attack strategy or the Intermittent Attack strategy which means that the attacks are launched intermittently in a random way. For the Intermittent Attack strategy, we simulate the scenario where the malicious nodes attack with a 50\% intensity. The intensity stands for the probability that the malicious node launches an attack during an interaction.

\subsection{Performance of the DSCS}

In this subsection, the performance of the proposed DSCS is compared to the distributed Random [33] and EDSO [34] schemes in terms of the sensing accuracy rate denoted by ACC.

In our simulations, the number of secondary users is 5 (secondary user is denoted by $x$ in the simulations) and the number of detectable channels of each secondary user is 4. The initial reputation of $x$ toward $y$ is
\( \omega_{xy} = (0.5, 0.25, 0.25, 0.5) \); the threshold of the reputation expectation, \( E_{\text{threshold}} \) is 0.5. The parameters \( \eta_1, \eta_2 \) are 0.5 and 0.5, which are empirical values obtained from multiple experiments. The time slot is 1s and the simulation results are the average values obtained from 1000 runs of simulation experiments.

First, we compare the ACC of the three strategies without SSDF attacks (i.e., without dishonest recommendations). Suppose that there are 6 available channels and each secondary user can detect up to 4 channels. The ACC can be computed as

\[
\text{ACC} = \frac{N_{\text{success}}}{N_{\text{select}}},
\]

where \( N_{\text{success}} \) is the number of successful channel accesses and \( N_{\text{select}} \) is the number of channel accesses.

We can observe in Figure 3 that all the three strategies can detect the channels from 1–4. But, since both the Random and EDSO strategies do not adopt the cooperative sensing scheme, they cannot detect channels 5 and 6. The proposed DSCS adopts the cooperative sensing scheme, which makes it possible to receive the sensing results recommended by the other cooperative users, so it can gain the status of channels 5 and 6 and use them to improve the channel utilization rate. Moreover, it is seen that the sensing accuracy performance of the DSCS is better than that of the Random and EDSO scheme. In the Random and EDSO scheme, the channel status information is computed and obtained only from the local sensing results, while in DSCS, the secondary users gather channel status information from the cooperative users and compute the final sensing results through combining the local sensing result with these cooperative sensing results.

Next, we compare the sensing accuracy performance of DSCS to that of the Random and EDSO scheme under the random SSDF and Intermittent SSDF attacks. The results are shown in Figures 4–6.

In Figure 4, we analyze the ACC performance of DSCS when malicious users exist. The results indicate that the sensing results are affected by the malicious users, and the ACC of DSCS decreases from 0.6 to less than 0.4 as the number of malicious users increases from 20 to 30. In DSCS, the proposed reputation mechanism will identify the malicious users and then punish them by isolating them from the network. The punishment will decrease the number of cooperative users and the cooperative sensing information; as a result, the accuracy of the DSCS drops.

As shown in Figure 5, the ACC of all the three strategies decreases when the number of the channels increases. Since the SSDF is randomly launched and cannot be detected effectively, the ACC of the Random and EDSO scheme decreases at a percentage up to 70% and 73%, respectively. However, for the DSCS, because the cooperative users can provide additional sensing information combined with the local sensing information to compute the final sensing result, its ACC only decreases by 35%.

In Figure 6, we compare the ACC of all the three strategies when the Intermittent SSDF attacks are present. In the simulation, we consider the scenario where the malicious nodes attack with a 50% intensity. The results in Figure 6 are similar to those in Figure 5; the ACC of Random and EDSO scheme decreases at a percentage up to 80% and 83% (in Figure 5, they are 70% and 73%), respectively. For the DSCS, its ACC only decreases by 40% (in Figure 5, it is 35%), which is much lower than that of the Random and EDSO scheme.

6.2. Performance of the DCSA. In this subsection, the performance of the proposed DCSA is verified in terms of the spectrum allocation accuracy rate denoted by ACR. We consider that there are 10 primary users and 10 secondary users. We set \( \text{BER}_{\text{tar}} = 10^{-4} \) and \( \gamma \in [5 \text{ dB}, 20 \text{ dB}] \). The values of parameters \( a \) and \( b \) in (13) are –10, 40.
In Figure 7, we set the deception rate $\lambda = 0.2$ and compare the ACR of the spectrum allocation process without DCSA under SSDF attacks to that with no SSDF attacks. The results in Figure 7 indicate that the ACR of both scenarios increases when the time increases. As expected, the ACR under no SSDF attacks is better than that under SSDF attacks, since the spectrum allocation will be affected by the SSDF attacks. Then, we investigate the impact of deception rates $\lambda$ on the ACR. The simulation results are shown in Figure 8. It can be seen that the average ACR when $\lambda = 0.2$ is higher than that when $\lambda = 2$. The simulation results demonstrate that the deception rate has a big impact on the ACR: the higher is the deception rate, the lower is the ACR.

The above analysis shows that it is necessary to build a SSDF-proof spectrum allocation strategy. In the following, we will compare the ACR performance of the strategy with DCSA to that of the strategy without DCSA.

As shown in Figures 9 and 10, under the SSDF attack, the ACR of both strategies (with or without DCSA) decreases when the time or the percentage of the malicious users increases, while the ACR of strategy with DCSA decreases slower than that without DCSA. In this simulation, the malicious users are assumed to be rational, so the proposed DCSA can effectively incentivize secondary users to honestly participate in the spectrum allocation process by reducing its reputation when it provides dishonest information. Since the reputation of a secondary user will be the reference for the next round of spectrum allocation and cooperative user
selection, the reduction of reputation will keep the malicious users away from lying because they cannot get utility from lying. As a result, the ACR of the strategy with DCSA is better than that without DCSA.

7. Conclusions

In this paper, we have investigated the challenging problems of secure spectrum sensing and spectrum allocation in CRNs and have proposed a distributed cooperative sensing strategy (DSCS) and a cheat-proof spectrum allocation strategy (DCSA). Based on the combination of the proposed dynamic reputation model and VCG mechanism, the DSCS and DCSA can effectively defend against the internal SSDF attacks. Moreover, the DSCS and DCSA do not rely on a central authority or a common control channel and are therefore applicable in distributed CRNs. Nevertheless, the proposed algorithm imposes some communications and computing overhead caused by nodes interactions which is not calculated in this work, as we focus on the security and effectiveness of the cooperative spectrum sensing and allocation scheme in CRNs. We intend to investigate and analyze the overhead issue in our future work. The elaborated simulation tests and performance analysis have verified that the DSCS and DCSA are secure and efficient. More specifically, in the presence of SSDF attacks, the sensing accuracy rate and the spectrum allocation accuracy rate of the proposed DSCS and DCSA are much better than those of the existing strategies.

**Notations and Symbols**

- \( \omega_{x,y}, \omega_{n,x,y}^{\text{direct}}, \omega_{n,x,y}^{\text{final}} \): \( x \)'s reputation, direct and final reputation towards \( y \) at time \( t_n \)
- \( b_{n,x,y}, d_{n,x,y}, u_{n,x,y}, a_{n,x,y} \): \( x \)'s belief, disbelief, and uncertainty towards \( y \) and \( x \)'s willingness to believe \( y \) at time \( t_n \)
- \( N_{n,x,y}, N_{n,x,y}^{s}, N_{n,x,y}^{f} \): The total number of the sensing results that \( x \) received from the user \( y \), the number of the correct results, and the number of the wrong results from \( y \)
- \( p_{c}^{\text{uncertain}} \): The degree of uncertainty whether \( y \) is trustworthy
- \( \beta_{c} \): The transition probability of the channel state from 1 to 0 after \( y \) has sent some sensing results
- \( P_{d}, P_{f}, P_{m} \): The detection probability of the secondary user, the false alarm rate, and the false negatives rate
- \( \Gamma(\cdot, \cdot) \): The incomplete Gamma function
- \( H_0, H_1 \): The zero hypothesis and the alternative hypothesis
- \( \eta_1, \eta_2 \): The weight factors used to determine how much the reputation evaluation results at times \( t_i \) and \( t_n \) affect the dynamic final reputation
- \( C = \{c_1, c_2, \ldots, c_m \mid m > 1\} \): The channel set that can be controlled
- \( B = \{b_1, b_2, \ldots, b_m\} \): The relevant bandwidth set with the \( m \) channels
- \( Q, \gamma \): The transfer efficiency and the signal-to-noise ratio of the receiver
- \( u_i(q_i, c) \): The profit of the user \( i \)
- \( V(q_i) \): The profit function that the profits user \( i \) will gain when it gets the access permission
- \( P(q_i, c) \): The cost of user \( i \)
\( P_c, q \): The cost of channel \( c \) and the throughput requirement to access the channel

\( \pi^*, o^* \): The system’s best profit and the best allocation results

\( T_i(q_i, o^*) \): The taxes for a user \( i \)

\( \sum_{j \neq i} T_j(q_j, o^*) \): The total utility of all the other applicants when \( i \) participates in the mechanism and the total utility of all the other applicants when \( i \) withdraws from the mechanism

\( u_i^*(q_i, o^*) \): The best utility of user \( i \).

**Conflict of Interests**

The authors declare that there is no conflict of interests regarding the publication of this paper.

**Acknowledgments**

This work is supported by National Natural Science Foundation of China (61202390, 61363068, 61472083, and 61402110), the Foundation of Fujian Provincial Educational Department of China (J15121), Fujian Normal University Innovative Research Team (IRT1207), and Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund (Fujian Normal University).

**References**

[1] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, “Cooperative spectrum sensing in cognitive radio networks: a survey,” Physical Communication, vol. 4, no. 1, pp. 40–62, 2011.

[2] T. Zhang, “Security issues in cognitive radio networks,” in Cognitive Networks: Towards Self-Aware Networks, pp. 271–291, John Wiley & Sons, 2014.

[3] T. Zhang, Z. Li, and R. Safavi-Naini, “Incentivize cooperative sensing in distributed cognitive radio networks with reputation-based pricing,” in Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM ’14), pp. 2490–2498, Toronto, Canada, May 2014.

[4] C.-Y. Chen, Y.-H. Chou, H.-C. Chao, and C.-H. Lo, “Secure centralized spectrum sensing for cognitive radio networks,” Wireless Networks, vol. 18, no. 6, pp. 667–677, 2012.

[5] R. Chen, J.-M. J. Park, and K. Bian, “Robustness against Byzantine failures in distributed spectrum sensing,” Computer Communications, vol. 35, no. 17, pp. 2115–2124, 2012.

[6] Y. Han, Q. Chen, and J.-X. Wang, “An enhanced D-S theory cooperative spectrum sensing algorithm against SDDF attack,” in Proceedings of the 75th Vehicular Technology Conference (VTC ’12), Yokohama, Japan, June 2012.

[7] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, “Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks,” IEEE Transactions on Signal Processing, vol. 59, no. 2, pp. 774–786, 2011.

[8] S. Yadav and M. J. Nene, “RSS based detection and expulsion of malicious users from cooperative sensing in cognitive radios,” in Proceedings of the 3rd IEEE International Advance Computing Conference (IACCESS ’13), pp. 181–184, Ghaziabad, India, February 2013.

[9] M. Zhou, J. Shen, H. Chen, and L. Xie, “A cooperative spectrum sensing scheme based on the Bayesian reputation model in cognitive radio networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’13), pp. 614–619, IEEE, Shanghai, China, April 2013.

[10] A. Mukherjee, “Diffusion of cooperative behavior in decentralized cognitive radio networks with selfish spectrum sensors,” IEEE Journal on Selected Topics in Signal Processing, vol. 7, no. 2, pp. 175–183, 2013.

[11] S. Li, H. Zhu, Z. Gao, X. Guan, and K. Xing, “YouSense: mitigating entropy selfishness in distributed collaborative spectrum sensing,” in Proceedings of the 32nd IEEE Conference on Computer Communications (INFOCOM ’13), pp. 2535–2543, Turin, Italy, April 2013.

[12] Z. Li, F. R. Yu, and M. Huang, “A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios,” IEEE Transactions on Vehicular Technology, vol. 59, no. 1, pp. 383–393, 2010.

[13] T. Zhang, R. Safavi-Naini, and Z. Li, “ReDiSen: reputation-based secure cooperative sensing in distributed cognitive radio networks,” in Proceedings of the IEEE International Conference on Communications (ICC ’13), pp. 2601–2605, IEEE, Budapest, Hungary, June 2013.

[14] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. T. Hou, “Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks,” in Proceedings of the 31st Annual IEEE International Conference on Computer Communications (INFOCOM’12), pp. 900–908, Orlando, Fl, USA, March 2012.

[15] J. Deng, R. Q. Zhang, L. Y. Song, Z. Han, and B. L. Jiao, “Truthful mechanisms for secure communication in wireless cooperative system,” IEEE Transactions on Wireless Communications, vol. 12, no. 9, pp. 4236–4245, 2013.

[16] R. Xie, F. R. Yu, H. Ji, and Y. Li, “Energy-efficient resource allocation for heterogeneous cognitive radio networks with femtocells,” IEEE Transactions on Wireless Communications, vol. 11, no. 11, pp. 3910–3920, 2012.

[17] T. Jiang, H. Wang, and A. V. Vasilakos, “QoE-driven channel allocation schemes for multimedia transmission of priority-based secondary users over cognitive radio networks,” IEEE Journal on Selected Areas in Communications, vol. 30, no. 7, pp. 1215–1224, 2012.

[18] R. Xie, F. R. Yu, and H. Ji, “Dynamic resource allocation for heterogeneous services in cognitive radio networks with imperfect channel sensing,” IEEE Transactions on Vehicular Technology, vol. 61, no. 2, pp. 770–780, 2012.

[19] L. T. Tan and L. B. Le, “Channel assignment with access contention resolution for cognitive radio networks,” IEEE Transactions on Vehicular Technology, vol. 61, no. 6, pp. 2808–2823, 2012.

[20] S. Wang, Z.-H. Zhou, M. Ge, and C. Wang, “Resource allocation for heterogeneous cognitive radio networks with imperfect spectrum sensing,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 3, pp. 464–475, 2013.

[21] Y. Tachwali, B. F. Lo, I. F. Akyildiz, and R. Agusti, “Multiuser resource allocation optimization using bandwidth-power product in cognitive radio networks,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 3, pp. 451–463, 2013.

[22] A. A. El-Sherif and K. J. R. Liu, “Joint design of spectrum sensing and channel access in cognitive radio networks,” IEEE
Transactions on Wireless Communications, vol. 10, no. 6, pp. 1743–1753, 2011.

[23] S. Buchegger and J.-Y. Le Boudec, "Self-policing mobile ad hoc networks by reputation systems," IEEE Communications Magazine, vol. 43, no. 7, pp. 101–107, 2005.

[24] J. Mundinger and J.-Y. Le Boudec, "Analysis of a reputation system for Mobile Ad-Hoc Networks with liars," Performance Evaluation, vol. 65, no. 3–4, pp. 212–226, 2008.

[25] H. Lin, J. f. Ma, J. Hu, and K. Yang, "PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks," EURASIP Journal on Wireless Communications and Networking, vol. 2012, no. 1, article 69, 16 pages, 2012.

[26] H. Lin, J. F. Hu, J. Ma, L. Xu, and A. Nagar, "A role based privacy-aware secure routing protocol for wireless mesh networks," Wireless Personal Communications, vol. 75, no. 3, pp. 1611–1633, 2014.

[27] G. Shafer, A Mathematical Theory of Evidence, Princeton, Nanjing, China, 1976.

[28] M. S. Islam, M. A. Hamid, and C. S. Hong, "SHWMP: a secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks," in Transactions on Computational Science VI, vol. 5730 of Lecture Notes in Computer Science, pp. 95–114, Springer, Berlin, Germany, 2009.

[29] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 2, pp. 203–215, 2010.

[30] A. J. Goldsmith and S. G. Chua, "Variable-rate variable-power MQAM for fading channels," IEEE Transactions on Communications, vol. 45, no. 10, pp. 1218–1230, 1997.

[31] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism design-based secure leader election model for intrusion detection in MANET," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 1, pp. 89–103, 2011.

[32] Z. Wei, W. Zhou, M. Kang, M. Collins, and P. Nixon, "A strategy-proof trust mechanism for pervasive computing environments," in Proceedings of the IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS ’09), pp. 728–733, Macau, China, October 2009.

[33] L. Luo and S. Roy, "Analysis of search schemes in cognitive radio," in Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON ’07), pp. 647–654, IEEE, San Diego, Calif, USA, June 2007.

[34] H. Kim and K. G. Shin, "Efficient discovery of spectrum opportunities with MAC-layer sensing in cognitive radio networks," IEEE Transactions on Mobile Computing, vol. 7, no. 5, pp. 533–545, 2008.