IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 31, 2017, accepted September 28, 2017. Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.2767701

A Secure Collaborative Spectrum Sensing Strategy in Cyber-Physical Systems

HUI LIN[1], JIA HU[2], JIANFENG MA[3], (Member, IEEE), LI XU[1], (Member, IEEE), AND ZHENGXIN YU[2]
[1]College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117002C China
[2]College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX44QF, U.K.
[3]School of Cyber Engineering, Xidian University, Xi'an 710071, China

Corresponding author: Jia Hu (j.hu@exeter.ac.uk)

This work was supported in part by the National Natural Science Foundation of China under Grant 61363068, Grant 61472083, and Grant 61402110, in part by the Pilot Project of Fujian Province (formal industry key project) under Grant 2016Y0031, and in part by the Foundation of Science and Technology on Information Assurance Laboratory under Grant KJ-14-109.

ABSTRACT Cyber-physical systems (CPS) have the great potential to transform people's lives. Smart cities, smart homes, robot assisted living, and intelligent transportation systems are examples of popular CPS systems and applications. It is an essential but challenging requirement to offer secure and trustworthy real-time feedback to CPS users using spectrum sharing wireless networks. This requirement can be satisfied using collaborative spectrum sensing technology of cognitive radio networks. Despite its promising benefits, collaborative spectrum sensing introduces new security threats especially internal attacks (i.e., attacks launched by internal nodes) that can degrade the efficiency of spectrum sensing. To tackle this challenge, we propose a new transferring reputation mechanism and dynamic game model-based secure collaborative spectrum sensing strategy (TRDG). More specifically, a location-aware transferring reputation mechanism is proposed to resolve the reputation loss problem caused by user mobility. Furthermore, a dynamic game-based recommendation incentive strategy is built to incentivize secondary users to provide honest information. The simulation experiments show that the TRDG enhances the accuracy of spectrum sensing and defends against the internal attacks effectively without relying on a central authority.

INDEX TERMS Cyber-physical systems, cognitive radio networks, dynamic game theory, reputation mechanism, spectrum sensing.

I. INTRODUCTION

Due to the rapid proliferation of mobile devices such as smart phones and various things equipped with built-in sensors and processors, Cyber-Physical Systems (CPS) have been attracting wide attention in both academia and industry [1]. CPS is a system featuring a combination of computational and physical elements, all of which are capable of interacting, reflecting and influencing each other [2]. The emergence of the CPS will significantly change the way we see the world. In the meantime, the convergence of the physical and cyber spaces will exhibit a variety of complicated characteristics, which brings more open issues and challenges for research communities. Especially, how to provide secure and trustworthy real-time feedback relied on the existing wireless communication networks with limited spectrum resource is an essential and challenging requirement in CPS [2]. To tackle this challenge, as an efficient emerging technology, Cognitive radio network (CRN) based collabrative spectrum sensing (CSS) is introduced into the CPS to solve the spectrum scarcity problem and provide reliable and secure real-time communication [3], [4], where unlicensed users access idle channels opportunistically based on the dynamic channels' sensing information, without creating any harmful interference to primary users (PU) [4]. This method will also help to incorporate billions of wireless devices for different applications such as Internet-of-Things (IoT), CPS, smart grids, etc. These channels could be highly congested and may not be able to provide secure and reliable communications in urban areas [5].

CSS can improve the efficiency of spectrum usage, but it also introduces new security threats including internal attacks during the spectrum sensing process, which can degrade the effectiveness of spectrum sensing dramatically. For example, an adversary may launch spectrum sensing data falsification (SSDF) attacks, where the adversary corrupts a subset of secondary users (SUs) as illustrated in the Fig. 1 to report

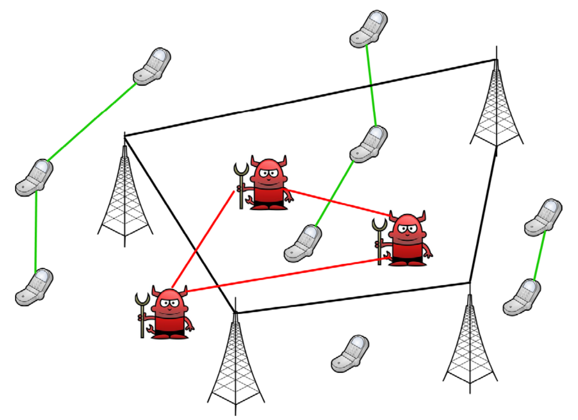


FIGURE 1. SSDF attacks model.

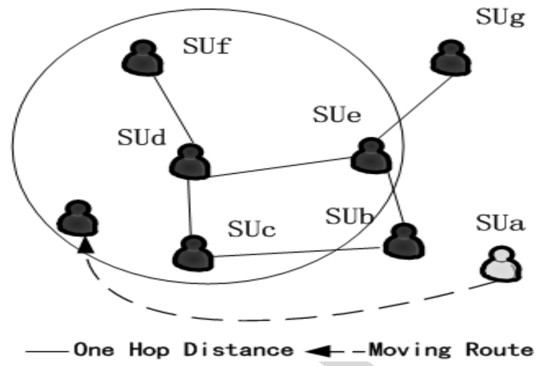


FIGURE 2. Mobile attacks model.

falsified information, aiming to affect the final group decision [6]. Moreover, an adversary may also launch internal Mobile attacks by moving position as shown in the Fig.2 to implement a new round interaction with the other secondary users as an initial secondary user.

Many papers [7]–[12] propose various methods to improve the security in spectrum sensing. 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 [13]–[17], using game theory [13], incentive design [14], consensus algorithm [15], [18], outlier detection and computation verification [17], etc. Most of the existing works ignore the internal SSDF attacks and Mobile attacks launched by an inside attacker that has the legal identity.

In CPS, most client users are mobile and they access the CPS opportunistically. Therefore, there is an urgent need for a new secure and reliable CSS strategy to address above-mentioned limitations of existing methods by taking in account the characteristics of CPS. To design a new secure and reliable CSS strategy, it is necessary to analyze the trustworthiness of the users. Thus, reputation based CSS has been introduced into CPS to implement secure spectrum sensing [9], [12], [16], [18]–[24].

Although some reputation based CSS strategies have been proposed in the literatures, most of them were based on the trusted third party and traditional cryptographic encryption and authentication techniques, thus ignoring internal attacks launched by an inside attacker that has the legal identity and dishonest recommendations used to frame up good parties and/or boost trust values of malicious peers. Moreover, they did not consider Mobile attacks and information leak.

To overcome the above-mentioned problems, a transferring reputation mechanism and dynamic game model based secure collaborative spectrum sensing strategy (TRDG) is proposed in this paper. In TRDG, a transferring reputation mechanism is firstly proposed. Then, a dynamic game based recommendation incentive strategy (DGRIS) is built. Finally, a secure collaborative spectrum sensing strategy TRDG is proposed based on the transferring reputation mechanism and the DGRIS. The major contributions of this work include:

(1) A location aware transferring reputation mechanism is proposed to resolve the reputation loss problem during the moving process of the SU. The proposed mechanism makes it possible to transfer the SUs' reputation to the new interaction area, which can better reflect the real-world nature of CPS, and defend against the internal Mobile attacks.

(2) A dynamic game based recommendation incentive strategy (DGRIS) is built to incentive the SUs to provide honest information. The DGRIS makes the attacks' utility below cost, which decreases the motivations of the rational malicious adversaries and thus can defend against the internal SSDF attacks.

(3) A transferring reputation mechanism and dynamic game model based secure collaborative spectrum sensing strategy (TRDG) is designed to help secondary users (SUs) sense the spectrum state and decide. SUs iteratively update their local values to arrive at consensus, without help from any central authority.

(4) Simulation experiments demonstrate that the TRDG can provide an effective, secure and trustworthy spectrum sensing countermeasure against the internal SSDF attacks and Mobile attacks without relying on a central authority.

The remainder of this paper is organized as follows. Section II presents a brief review of the related work; Section III describes the network and adversary models; Section IV introduces the implementation details of the TRDG strategy; Section V presents the performance evaluation of the TRDG; Finally, Section VI concludes the paper and discusses some future work.

II. RELATED WORK

In this section, we provide a literature review on the concepts of collaborative spectrum sensing. Spectrum sensing in CRN have been widely studied, using game theory [13], incentive design [14], consensus algorithm [18], outlier detection and computation verification [17], and etc.

For instance, Mukherjee [13] discussed cooperative sensing problem in distributed CRN 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. [14] first identified a new selfishness model named entropy selfishness in distributed CRN. 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, but the honest user can recover this plaintext by spectrum sensing. Zhang et al. [18] 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. [6], [16] 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. [17] 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.

Amjad et al. [21] proposed a framework for trustworthy collaboration in spectrum sensing for ad hoc CRNs. The framework incorporates a semi-supervised spatio-spectral anomaly/outlier detection system and a reputation system, both designed to detect byzantine attacks in the form of SSDF from malicious nodes within the CRN. Sun et al. [25] proposed hard and soft fusion collaborative spectrum sensing schemes based on online hidden bivariate Markov chain modeling of the signals received by secondary users. The proposed schemes do not rely on precomputed thresholds or weights, and provide predictive information that can be used to improve the performance of dynamic spectrum access. Sharifi et.al proposed attack-aware CSS (ACSS) scheme to against SSDF attack in literatures [26] and [27], respectively. The ACSS proposed in [26] estimates attack strength and applies it in the k-out-N rule to obtain the optimum value of k that minimizes the Bayes risk. And, the ACSS proposed in [27] estimates the credit value of each cognitive radio user and identifies the malicious attackers along with their attack strategies by allocating an appropriate collaborative weight for each user, which improves the CSS performance effectively. Hsieh et.al [28] proposed a coalition-based model for the Interference-aware spectrum sensing to maximize the utility sum of all secondary users while observing the protection requirement of the primary user. The proposed model first formulates a joint threshold detection and coalition formation problem under the target cooperative model, and then explore important properties of the target problem.

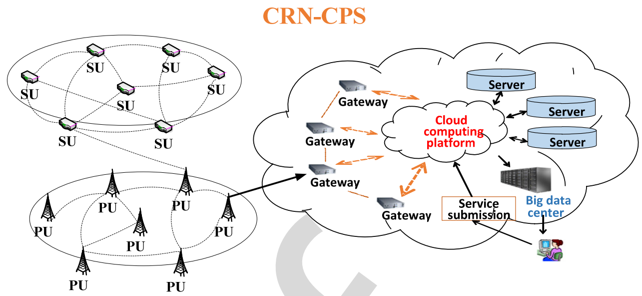


FIGURE 3. Architecture of CRN-CPS.

Overall, existing collaborative spectrum sensing methods are usually based on a centralized infrastructure in which a central entity coordinates the operations of the spectrum sensing and sensing information collection, thus brings heavy communication overheads and the issue that central authority may be compromised by attackers. On the one hand, they overlook the internal attacks launched by an inside attacker that has the legal identity whose presence is likely in the CRN and CPS environment. Consequently, it is still an open problem and a challenging task to design secure and distributed spectrum sensing allocation schemes in CRN to resist the internal attacks and provide sensing information security protection.

III. SYSTEM AND ADVERSARY MODEL

A. SYSTEM MODEL

In this paper, we focus on the network environment of CRN based CPS (CRN-CPS), which is a viable solution to implement fast and large-scale CPS applications [2], [4]. The typical CRN-CPS architecture is depicted in Fig. 3, which adopts the CRN as the access network. As shown in fig.3, the CRN in the CRN-CPS is consist of a PU network and a SU network. We suppose that each SU is equipped with a cognitive radio and they utilize omnidirectional antennas to communicate with each other. Meanwhile, SUs are located within the transmission range of the PUs, and can individually sense the environment to detect the existence of the Pus [16], [18]. In the CSS process, we use the energy sensing method for a SU to detect PUs' presence. We also assume that an adversary can compromise a subset of honest SUs. A SU may provide incorrect information (including attacking malicious SUs and honest SUs that sense incorrectly due to severe fading or system failure) or correct information (including honest SUs that sense correctly and non-attacking malicious SUs). An honest SU has no a priori information on which of its neighbors are malicious. If the final sensing results indicate that the PUs are not transmitting on certain channels, the SUs use the spectrum allocation scheme to allocate and transmit on these channels.

B. ADVERSARY MODEL

In this paper, we focus on the internal attacks launched by an inside legal and certificated user, which makes the

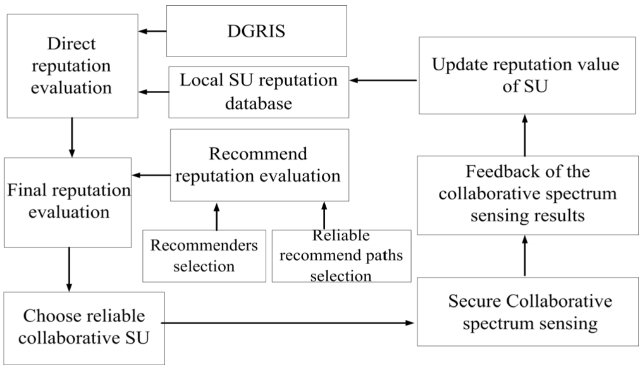


FIGURE 4. The TRDG system structure.

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. Furthermore, we assume, in spectrum sensing, the following internal attacks will be launched by the inside malicious SU:

- SSDF attacks: attackers corrupt a subset of SUs and strategically report falsified sensing results, aiming at incurring interference between the PUs and legitimate SUs and affect the final group decision.
- Mobile attacks: attackers move to other position and disguised as an initial or normal SU to implement a new round interaction with the other SUs.

IV. TRANSFERRING REPUTATION MECHANISM AND DYNAMIC GAME MODEL BASED SECURE COLLABORATIVE SPECTRUM SENSING STRATEGY (TRDG)

In this section, a novel transferring reputation mechanism and dynamic game model based secure collaborative spectrum sensing strategy (TRDG) is extended from our previous work [23], [24]. The TRDG integrates the collaborative spectrum sensing with multi-level security, reputation mechanism and dynamic game theory to defend against the insider threat and enhance the securityand efficiency of spectrum sensing in distributed CRN based CPS. The system structure of TRDG is shown in figure 4, and the details of the TRDG are described as follows.

A. DYNAMIC GAME BASED RECOMMENDATION INCENTIVE STRATEGY (DGRIS)

Traditional reputation mechanisms improve the trustworthiness of recommendations through weighted summation of recommendations from different recommenders. However, in the open network environment such as CPS, these mechanisms must face the significant problems caused by the selfish and malicious users who refuse to render the recommendations in order to avoid consuming limited resources or provide dishonest recommendations so as to launch attacks. To overcome the above shortcomings, in this subsection, we first propose a dynamic game based recommendation incentive strategy (DGRIS). Then the DGRIS is incorporated into the recommend reputation evaluation to motivate users to provide honest recommendations.

In DGRIS, the principal agent theory [29], [30] is used to incent recommenders to provide the honest information during the recommend reputation evaluation process. In this paper, we assume that the agent could take an action like S = {honest response (h), fake response (f)} after principal sends the request of cooperative spectrum sensing. Based on the dynamic game theory that is proposed in this paper, for example, if the neighbour secondary user replies with false information, its reputation will be reduced as punishment. When the value of reputation is lower than a threshold, no one would be provided cooperative to this user. If the secondary user SU_a replies honestly, the payoff is U_a. The formula for calculation is as follows:

$$U_a = 2 * A * P_d * R \tag{1}$$

A is the reward for secondary user of cooperative sensing from requesting cooperative sensing secondary user. R is a comprehensive value, according to the reputation value which passed by multipath and the requester's reputation value from local database. The more incentivize involvement of cooperative sensing, the greater value would be. P is the detection rate of spectrum sensing that is the probability of principal exist with correct judgment, $P_d = 1 - P_f$, P will provide a relative accurate sensing response.

The secondary user is rational. If the secondary user who offer collaboration provides an honest response, its own giving a fake response to other secondary users. The payoff is 3A and the other's is –A; Both secondary users provide an honest response, then the payoff is 2A for each; They will receive 0 if two sides all offer fake response.

As for the i-way interaction process of cooperative spectrum sensing, it can be divided into the following situations.

(a) All secondary user provides honest response, so the total payoff is as follows:

$$\begin{aligned} U_x &= 2 * A + (\sum_{i=2}^{\infty} U_a) * R \\ &= 2 * A + 2 * A * [R/(1 - P_d * R)] \end{aligned} \tag{2}$$

(b) The first round offers a fake response, then other rounds give honest responses, the total payoff is as follows:

$$U_y = 3 * A - A * R + \sum_{i=3}^{\infty} 0 = 3 * A - A * R \tag{3}$$

(c) The secondary user provides fake response continuously. The first cooperation is likely to succeed, but from the second-round other secondary users will not offer honest response any more. The total payoff is as follow:

$$U_z = 3 * A + \sum_{i=2}^{\infty} 0 = 3 * A \tag{4}$$

(d) Providing an honest response first, then giving the fake response. The total payoff is:

$$U_\pi = 2*A + 3*A*R + \sum_{i=3}^{\infty} 0 = 2*A + 3*A*R \quad (5)$$

In the situation of repeated games, the two situations compared:

Situation (a) with situation (b), if $U_x > U_y$, then $2*A + 2*A*\frac{R}{1-P_d*R} > 3*A - A*R$ and $0 \le R \le 1$, so $R \ge \frac{3+P_d-\sqrt{(3+P_d)^2-4P_d}}{2P_d}$ and R is monotonically increasing with the value of P_d changes. Since $0 \le P_d \le 1$, then $R \ge 2-\sqrt{3}$. Therefore, if $R \ge 2-\sqrt{3}$, the total payoff of the strategy with honest response is greater than the payoff from deceive strategy (situation b). To summarize: if $R \ge 2-\sqrt{3}$, honest response strategy is a dominant strategy. Otherwise, secondary user will provide fake response.

The next two situations compared: situation (a) with situation (c), if the payoff of honest response is greater than the fake response's payoff, then $U_x - U_z \ge 0$, that $(\sum_{i=2}^{\infty} U_a)*R - A = (2*A*R)/(1-P_d*R) - A \ge 0$. So $R \ge \frac{1}{2+P_d}$ and $P_d \ge 0$, in other words, $R \ge 1/2$. Considering it may be collaborated again, the dominant strategy is choosing to response honestly. If $R \ge 1/2$. Otherwise, a fake response would be provided by the secondary user.

Compared situation (a) with situation (d), if $U_x > U_\pi$, since $2*A + 2*A*\frac{R}{1-P_d*R} > 2*A + 3*A*R$, so $R > \frac{1}{3P_d}$ and $0 \le P_d \le 1$ that $R > \frac{1}{3}$. Therefore, honest response is a dominant strategy, if $R > \frac{1}{3}$. Otherwise, the secondary user will provide a fake response.

To summarize what has been mentioned above, considering the long-term benefit, all secondary users expect to get cooperative spectrum sensing. If $R \ge 1/2$, both sides provide honest response is Nash Equilibrium.

After the secondary user moved, if the secondary user SU_b doesn't receive the collaborative report by its neighbor secondary user SU_a, SU_b will broadcast the reputation value of SU_a to all other neighbor secondary users, in order to generate the corresponding reputation history information for SU_a in the network. The safety of cooperative spectrum sensing in the network would be improved if keeping the value of reputation $R \ge 1/2$. Using (2) to pass the value of reputation, it can effectively accelerate convergence for reputation value of SU_a, which will provide incentive participant for moved secondary users in cooperation and reduce the selfish behavior which only receive other's cooperation and not voluntarily contribute to desired cooperative sensing.

B. TRANSFERRING REPUTATION MECHANISM

In distributed CRN based CPS, the proposed transferring reputation mechanism is run at each SU who stores its historical opinion towards the others in the relevant local database. And it consists of three components: direct reputation evaluation, recommend reputation evaluation and final reputation evaluation.

When a SU wants to request (or provide) a service from (or to) another SU (including unknown SUs), it will send a request message to all neighboring SUs. Each neighboring SU receiving the request will first verify whether the requestor's security level (*sl*) satisfies the security requirement. If it is, the neighboring SU will execute the direct reputation evaluation to judge whether the requestor is a malicious SU. Otherwise, the neighboring SU will ignore the request. The security level computation and assignment please refer to our previous work [31], [32].

If the direct reputation evaluation cannot lead to a decision, the neighboring *SU* will further execute the recommended reputation query using Algorithm 2 to query requestor's reputation from its neighbors. Afterwards, the neighboring *SU* will evaluate the integrated recommended reputation combining the received replies of recommended reputations to the query. Finally, it will evaluate the final reputation and decide whether the requestor is a malicious SU or not.

Suppose SU_x and SU_y represent the requester and service provider respectively. The final reputation of SU_x and SU_y, denoted as R^{Final}, includes two components: One is the direct reputation R^{Direct} and the other is the recommendation reputation R^{Rec}. The final evaluation results will be stored in the local database of final reputation.

1) EVALUATION OF DIRECT REPUTATION

The direct reputation of SU_x toward SU_y is evaluated as follows.

(1) If SU_x is an unknown user, SU_y will start the DGRIS in 4.1 to ask for SU_x's reputation from its neighbors.

(2) Otherwise, the direct reputation evaluation between SU_x and SU_y depends on the historical interaction and dynamic real-time sensing information of the network, and can be computed as (6).

$$R_{T_n}^{Direct} = (IA_s/IA_{total})^* \varphi_{T_n}{}^*(1-\varphi_{location}) \quad (6)$$

where IA_s and IA_{total} denote the successful interaction number of times and the total interaction number of times during T time periods, respectively. φ_{T_n} is the weight factor, which determines how much the distribution of the interactions affects the direct reputation evaluation at time *Tn*, which is given by

$$\varphi_{T_n} = \left[1 - e \wedge (-NIA_{T_n}/(m^* n))\right]^* \sum_{l=1}^{n} \left(\frac{NIA_l}{m} * \frac{l}{n}\right) \quad (7)$$

where m is the number of cycles in a time period, and n is the number of time period. NIA_{T_n} is the number of the cycles that the interaction happens between SU_x and SU_y. NIA_l is the number of interaction in the l-st time period. $\varphi_{location}$ denotes how the real-time position change between SU_x and SU_y affects the direct reputation evaluation at time Tn. The larger the distance, the more untrusted the SU_x.

$$\varphi_{location} = e^{-E_{location}*\beta_{location}} * (1 - e^{-|L-L'|*\beta_{location}}) \quad (8)$$

In (8), the real-time position and the most recent position is denoted as L and L', respectively. We define |L-L'| as the distance between them. We also define Elocation as the error of location sensing and $\beta_{location}$ is the parameter that controls the weight of the location factor's influence on the reputation.

The details of the unidirectional direct reputation evaluation are shown in Algorithm 1.

Algorithm 1 Direct Reputation Evaluation

Input: Requester $SU_x's$ information
Output: Whether SU_x is a malicious node or not
1. Begin
2. Requester SU_x sends a *Request* message;
3. $SU_x's$ neighbor SU such as SU_y receives the *Request* message;
4. If $\left(SU_x'sl > Securitylevelrequirement\right)$ then
5. SU_y executes the Direct Reputation Evaluation and returns the result as:
6. R^{Direct}=Direct_reputation (SU_x);
7. Else
8. SU_y drops the *Request* message;
9. End if
10. If ($R^{Direct} > TH_{direct}^{upper}$) then
11. $R^{Final} = R^{Direct}$;
12. Else if ($TH_{direct}^{down} < R^{Direct} < TH_{direct}^{upper}$) then
13. SU_y executes the Recommendation Reputation Query;
14. SU_y executes the Recommendation Reputation Evaluation;
15. SU_y executes the Final Reputation Evaluation and gets the R^{Final};
16. Else
17. $R^{Final} = -1$;
18. End if
19. If ($R^{Final} < TH_{final}^{down}$) then
20. SU_x is considered as a malicious node and will be isolated;
21. Else if ($TH_{final}^{down} < R^{Final} < TH_{final}^{upper}$) then
22. SU_x will be punished by decreasing its reputation value;
23. Else
24. SU_x is considered as a trustworthy node;
25. SU_y sends *Accept* message to SU_x;
26. End if
27. End

2) EVALUATION OF RECOMMENDATION REPUTATION

If the direct reputation computation cannot lead to a decision, SU_y will first execute the recommended reputation query using Algorithm 2 to query SU_x's reputation and security level from its neighbors. Afterwards, SU_y will compute the integrated recommended reputation combining the received replies of recommended reputations to the query, which will be described in the following.

Suppose SU_y receives n (n>1) direct recommendation opinions and m (m>1) transferring path based recommendation opinions, then the integrated recommendation reputation,

Algorithm 2 Recommendation Opinion Query

Input: Requester $SU_x's$ mac address, ID
Output: $SU_x's$ reputation and security level
1. Begin
2. SU_y broadcasts a *query* message;
3. Wait (3-5*seconds*);
4. $SU_y's$ neighbor SU_k receives the *query* message;
5. If $\left(SU_y'sl > Securitylevelrequirement\right)$ then
6. {
7. If (there has the direct reputation and security level opinions about SU_x) then
8. SU_k evaluates the direct recommend reputation $R_{T_n}^{Dir\text{-}Rec}$;
9. Else
10. {
11. SU_k ask neighbor *s* to provide the reputation and security level
12. opinions about SU_x;
13. SU_k evaluates the transferring path based recommendation
14. reputation $R_{T_n}^{Path\text{-}Rec}$;
15. }
16. SU_k evaluates the integrated recommendation reputation $R_{T_n}^{Rec}$;
17. SU_k executes the DGRIS and returns the $R_{T_n}^{Rec}$ and security level
18. opinions to SU_y;
19. }
20. Else
21. SU_k drops the *query* message;
22. End

$R_{T_n}^{Rec}$, can be computed as follows.

$$\begin{cases} R_{T_n}^{Rec} = \eta_1 * R_{T_n}^{Dir\text{-}Rec} + \eta_2 * R_{T_n}^{Path\text{-}Rec} \\ \eta_1 + \eta_2 = 1, \quad \eta_1, \eta_2 \in [0, 1] \end{cases} \tag{9}$$

where η_1, η_2 are the weight factors, which determine how much the direct recommendation opinions $R_{T_n}^{Dir\text{-}Rec}$ and transferring path based recommendation opinions $R_{T_n}^{Path\text{-}Rec}$ affect the final recommendation reputation evaluation, respectively. The $R_{T_n}^{Dir\text{-}Rec}$ is from the direct recommenders who has the reputation opinion about the SU_x on its local reputation database, and the $R_{T_n}^{Path\text{-}Rec}$ is provided by the transferring recommenders who provide the reputation opinion about the SU_x with the opinion from their neighbors.

Let DirR $= \{dir - rec_i \,|i = 1 \ldots n\}$ and PathR $= \left\{path - rec_j \,|j = 1 \ldots m\right\}$ be the direct recommenders set and the transferring recommenders set, respectively. The $R_{T_n}^{Dir\text{-}Rec}$ can be given by

$$R_{T_n}^{Dir\text{-}Rec} = \frac{1}{n} * \sum_{j=1, j \in DirR}^{n} \left(\frac{sl_j}{sl_{max}} * R_{j:x}^{\mathrm{Direct}} \right) \tag{10}$$

where sl_{max} is the maximal security level. $R^{\text{Direct}}_{j:x}$ is the direct recommend opinion about SU_x provided by SU_j.

For a transferring recommender SU_k, $SU_k \in PathR$, if there are many recommend opinion about SU_x coming from different paths, the most reliable path denoted as $R_{k:path}$ is chosen based on the rules below. Here, we assume $L_{(i)}$, $(i = 1, \ldots, n)$ is the set of the recommend paths and each path includes j SUs.

$$
\begin{aligned}
R_{k:path} &= Max\ (\zeta_1 * R_{L(i)} + \zeta_2 * SL_{L(i)}), \quad i = 1..n \\
&\quad s.t.\ \zeta_1 + \zeta_2 = 1 \\
&\qquad Th_1 < E_{L(i)} < Th_2
\end{aligned} \tag{11}
$$

where ζ_1 and ζ_2 are the weight factors corresponding to the opinion and security level of path $L_{(i)}$ respectively. Th_1 and Th_2 are the thresholds of $E_{L(i)}$. $R_{L(i)}$ and $SL_{L(i)}$ are the opinion and security level of path $L_{(i)}$ respectively. $E_{L(i)}$ is the energy consumption of path $L_{(i)}$. $R_{L(i)}$, $SL_{L(i)}$ and $E_{L(i)}$ can be computed as:

$$
\begin{cases}
R_{L(i)} = Min(\sum_{j=1}^{m} R^i_j/m, \min(R^i_j)) \\
SL_{L(i)} = Min(SL^i_j) \\
E_{L(i)} = m * Max(\sum_{j=1}^{m} E^i_j/m, \max(E^i_j))
\end{cases} \tag{12}
$$

where R^i_j and SL^i_j are the opinion and security level of SU_i in the j-th path, respectively. E^i_j is the energy consumption of SU_i in the j-th path. SL^i_j is the security level assigned to the SU_i in the j-th path according to the SU's reputation value.

And then, the $R^{Path\text{-}Rec}_{T_n}$ can be computed as

$$
R^{Path\text{-}Rec}_{T_n} = \frac{1}{m} * \sum_{k=1, k\in PathR}^{m} \times \left[R_{k:path} * R^{\text{Direct}}_{k:x} * (1 - \varphi_{y:k,location}) \right] \tag{13}
$$

where $\varphi_{y:k,location} \in [0, 1]$ is the influence factor of the location between the SU_y and the recommender SU_k. Algorithm 3 gives the details of the integrated recommended reputation computation.

Algorithm 3 Integrated Recommended Reputation Evaluation

```
Input: N direct recommendation information and M transferring recommendation information
Output: Integrated recommended reputation value
Begin
  SU_y receives n + m Reply messages with the direct
  and transferring recommendation information about
  SU_x;
  SU_y executes the recommenders selection process;
  For (i = 1; i <= n + m; i + +)
  {
    If (SU'_i sl > Securitylevelrequirement) then
    {
      If (SU_i is a direct recommender) then
        Put SU_i into the recommenders set DirR;
      Else
        Put SU_i into the recommenders set PathR;
    }
    Else
      SU_y drops the Reply message;
    End if
  }
  SU_y computes the R^{Dir-Rec}_{T_n}, R_{k:path} and R^{Path-Rec}_{T_n} with
  DirR and PathR;
  SU_y executes the integrated recommendation
  reputation evaluation and returns the result as R^{Rec}_{T_n};
End
```

3) EVALUATION OF FINAL REPUTATION

After getting the direct and recommended reputation, the final reputation can be computed as:

$$
\begin{cases}
R^{Final}_{y:x} = \alpha_1 * R^{Direc}_{T_n} + \alpha_2 * R^{Rec}_{T_n} \\
\alpha_1 + \alpha_2 = 1, \quad \alpha_1, \alpha_2 \in [0, 1]
\end{cases} \tag{14}
$$

where α_1, α_2 are the weight factors for the direct reputation and integrated recommended reputation, respectively.

C. SECURE COLLABORATIVE SPECTRUM SENSING STRATEGY (TRDG)

CSS implements spectrum sensing through the SUs in a wide area. In CSS, each SU obtains a local measurement in a time interval. After a sensing session, a series of value update sessions are executed by the secondary users. All SUs exchange their local spectrum sensing results with their neighbors within its communication range, and update their own values based on the received values. Since CSS can enhance sensing accuracy, while reducing the need for sensitive and expensive sensing technology, it is proposed to enhance the sensing performance [16], [18]. However, it is vulnerable to the internal attacks threats, which will make the performance of CSS degrade significantly.

To solve the above-mentioned problems, based on transferring reputation mechanism, dynamic game based recommendation incentive strategy (DGRIS) and combining with the characteristics of CRN, a secure collaborative spectrum sensing strategy TRDG is proposed to improve the accuracy and reliability of the sensing results, and defend against the internal SSDF and Mobile attacks. In TRDG, a secondary user combines its sensing results with the results of collaborative group members to evaluate the true state of the channel to improve the accuracy of sensing. Moreover, TRDG can also punish the untrustworthy user to reduce the influence of the false information to the network.

During the sensing data fusion and decision process, the final reputation is put into (15) to compute the sensing data fusion result.

$$\Phi_d^s = \left(\sum_{i=1, i\neq d}^{\gamma} R_{d:i}^{Final} \times \Psi_i\right) / \sum_{i=1, i\neq d}^{\gamma} R_{d:i}^{Final} \tag{15}$$

where Φ_d^s is the sensing data fusion result when SU_d requests the channel s. γ is the total number of the sensing result fed back by the other SUs. Ψ_i is the state of the channel s sensed by the SU_i, which is defined as

$$\Psi_i = \begin{cases} 0, & s \text{ is busy} \\ 1, & s \text{ is idle} \end{cases} \tag{16}$$

Then, the decision O_d^s can be made by

$$O_d^s = \begin{cases} 1 \ s \text{ is idle}, & \Phi_d^s \geq \lambda \\ 0 \ s \text{ is busy}, & otherwise \end{cases} \tag{17}$$

where λ is the threshold of the channel being idle.

The details of the TRDG are described in Algorithm 4. It is worth noting that DB_X^{local} is SU's local reputation table. The size of the table is 1Mb-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.

Algorithm 4 Secure Collaborative Spectrum Sensing Strategy (TRDG)

Input: Wireless channel set C, detectable channel set C_X,
Output: Most trustworthy secondary users set, TSU untrustworthy secondary users set UTSU and the sensing data fusion result

1. Begin
2. The SU_s wanting to transfer data setups the spectrum collaborative detection secondary users set Ω_N by broadcasts the $REQ_{establish}$ message on the common control channel (CCC);
3. Any SU who receives the message and wants to collaboration feeds back a $RESP_{establish}$ and joins the Ω_N;
4. SU_s and all members in the Ω_N initialize the parameters of reputation mechanism, DGRIS, TRDG, the reputation threshold ($E_{threshold}$), and detection period of (T);
5. SU_s broadcasts the collaborative request to the members in Ω_N;
6. The member in Ω_N receiving the request executes the DGRIS and makes a decision whether to participate in the collaboration and provide the honest sensing results;
7. SU_s monitors the CCC during $[t_{start}, t_{start} + T]$;
8. After receives the feedback messages, SU_s executes the following steps:
9. SU_s selects the collaborative SUs whose security level satisfies the security requirement and setup a new collaborative SUs set Ω'_N;
10. SU_s executes transferring reputation mechanism to evaluate the reputation of the members in Ω'_N;
11. SU_s sets up the most trustworthy secondary users set TSU;
12. SU_s sets up the untrustworthy secondary users set UTSU;
13. SU_s executes the TRDG to compute the sensing data fusion result;
14. SU_s executes the channel search scheme(CSS): CSS(TSU);
15. SU_s update the reputation of the member in TSU and UTSU and broadcasts it on the CCC;
16. SU_s punishes(UTSU);
17. SU_s transfers the reputation of those members in Ω_N that do not feedback any sensing information to the neighbors within one-hop communication distance;
18. End

V. PERFORMANCE EVALUATION

In this section, we implement our strategy and conduct simulation experiments using MATLAB and compare TRDG with RCSS in [21], JSSRA in [22], and ICS in [33].

For evaluating our proposed framework for defending against aforementioned SSDF attacks and Mobile attacks, we have considered an CRN of size 1000 m x 1000 m and the PU and the SUs whether honest or malicious, are mobile with their speed varying between 0 and 4 m/s which represents a CRN user moving around on foot. The maximum transmission range s for both the PU and the SUs is 200 m. We have carried out simulations for both dense (100 secondary users) network configurations and the number of detectable channels of each secondary user is 6. The parameters η_1, η_2, α_1, α_2, ζ_1, ζ_2, $E_{threshold}$, are 0.4, 0.6, 0.3, 0.7, 0.5, 0.5, 0.5, which are empirical values obtained from multiple experiments. The number of time period is 6, the number of cycle in a time period is 10, and the time period is 1s. All the graphs represent results that are averaged over 100 simulation runs.

Because the Attack Ratio (AR) and Malicious SU Detection Accuracy (MDA) are the common metrics to evaluate the performance of the reputation mechanism and incentive strategy, while the Spectrum Decision Accuracy Ratio (SDA) and False Spectrum Decision Ratio (FSDR) are the important and frequently used metrics to evaluate the feasibility and availability of the spectrum sensing strategy, they are chosen as the metrics in the performance evaluation when internal SSDF attacks and Mobile attacks are present. These performance metrics are defined as follows.

- ➢ **Attack Ratio (AR)**: The rate of the number of malicious users who launch attacks to the total number of malicious users.
- ➢ **Malicious SU Detection Accuracy (MDA)**: The percent of malicious SUs that is correctly identified by the reputation management system.

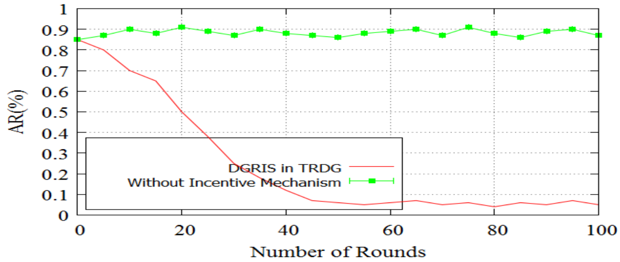


FIGURE 5. Attack ratio of TRDG with DGRIS and TRDG without DGRIS.

- ➢ **Spectrum Decision Accuracy Ratio (SDA)**: The percent of decision made by the proposed spectrum sensing strategy is the same as the actual state of the channel.
- ➢ **False Spectrum Decision Ratio (FSDR)**: Percent of state of the channel misidentified by the proposed spectrum sensing strategy.

1) ATTACK RATIO (AR)

First, we compare the AR of TRDG with DGRIS with the TRDG without DGRIS and the AR performance of the TRDG with that of the ICS to investigate the influence of the incentive mechanism on the attacks defense. In the simulation, we set a hostile network environment with 50 percent of the malicious SUs, and the estimated value is converged to constant values after applying almost 100 rounds of sensing.

In Fig. 5, the simulation results show that the AR of the TRDG without DGRIS is higher than the TRDG with DGRIS. For the TRDG with DGRIS, the incentive mechanism DGRIS makes the attacks utility below cost, which effectively decreases the attack wishes of the malicious SUs and leads to the AR of TRDG with DGRIS decreases with the simulation rounds increases. But for the TRDG without DGRIS, there has no incentive mechanism to incentive SUs to provide true information and punish the SUs who provide the false information, so the malicious SUs will continue launching attacks and its AR maintains a stable state.

The AR comparison results between TRDG and ICS considering the SSDF and Mobile attacks are shown in Fig. 6(a) and (b), respectively. In Fig. 6(a), we consider the SSDF attacks, as expected, the AR of both ICS and TRDG decreases with the simulation round increases, which demonstrate that both the ICS and TRDG can effectively defend against the SSDF attacks. Because both ICS and TRDG adopt reputation mechanism to judge whether a SU is a malicious user according to its reputation, and also adopt incentive mechanism to decreases the attack wishes of the rational malicious adversaries, so the rational malicious attackers will give up attacks to avoid being punished and costing more, and leading to the AR decrease.

In Fig. 6(b), we consider the Mobile attacks, from the results we can find that different from the SSDF attacks, the AR of TRDG is lower than that of the ICS, which means that the Mobile attacks affects the ICS more than for the TRDG. In ICS, it connects sensing participation to the reputation

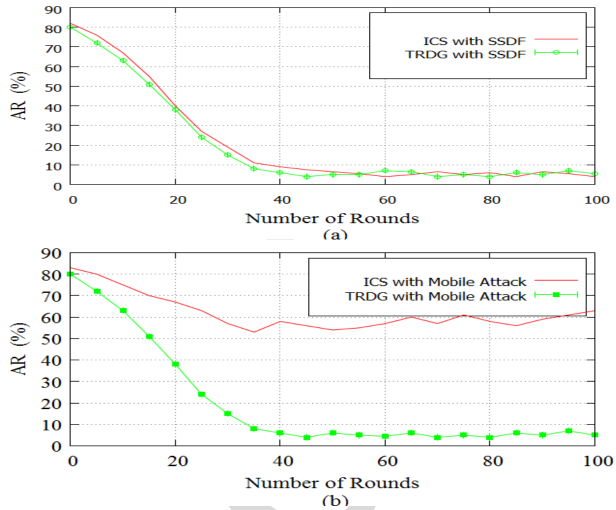


FIGURE 6. Attack ratio (a) with SSDF attacks (b) with mobile attacks.

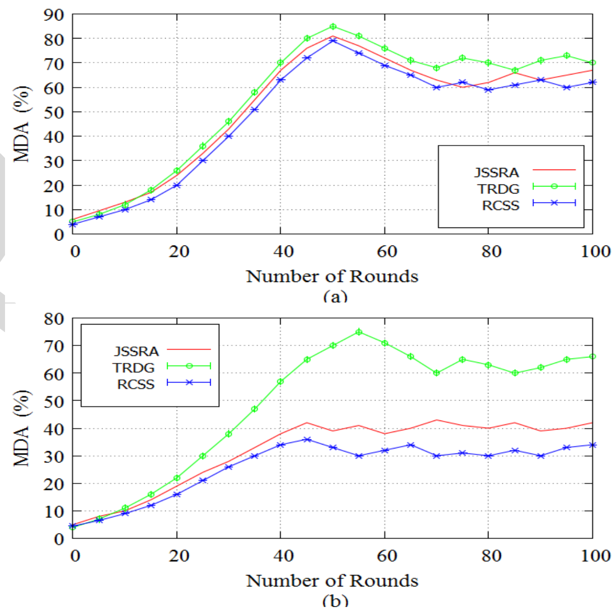


FIGURE 7. Malicious SU detection accuracy (a) with SSDF attacks (b) with mobile attacks.

through a user-dependent pricing function to offer stronger incentives for honest SUs to participate in the CSS. However, it ignores the Mobile attacks, and cannot transfer the reputation of the mobile malicious SUs to the new interaction area, which makes it cannot avoid the reputation loss problem during the moving process of the SU. And then, the malicious SUs in the new interaction area will be disguised as an initial or normal SU and been design an initial reputation to execute a new round interaction with the new neighbors. So, although the AR of the ICS decreases with the simulation round increases, it will finally maintain a relatively stable state and it is much higher than the AR of the TRDG. In TRDG, a transferring reputation mechanism is proposed to make the reputation transmission possible, which makes the mobile malicious SUs cannot veil its previous malicious behaviors, and defend against the internal Mobile attacks effectively. Thus, the AR performance of the TRDG is better than the ICS.

2) MALICIOUS SU DETECTION ACCURACY (MDA)

Next, we will evaluate the effectiveness and reliability of the three strategies by comparing their MDA performance to each other in the presence of SSDF and Mobile attacks.

The results in Fig. 7(a) and (b) show the MDA of the three strategies increase with the simulation rounds increase in the presence of the SSDF and Mobile attacks. This is because that all of the three strategies adopt the reputation model to evaluate the trustworthiness of a SU according to its reputation value. When a malicious SU launches attacks, its reputation value will be reduced, and if the reputation value of a SU is below a threshold, it will be identified as a malicious user. Since the more attacks the malicious SU launches, the lower its reputation value, which makes it more likely to be identified, so the MDA of the three strategies increase with more malicious users launch attacks.

Moreover, it is also observed that the MDA of the TRDG is the highest among all the three strategies in the presence of the SSDF and Mobile attacks.

The reason lies in that the integrated combination of the analysis of the distribution of interaction, real-time position information collection and multi-security scheme improves the accuracy, efficiency, and reliability of both the direct and recommendation reputation evaluation, and thus enhances the MDA of TRDG. Although the other strategies also adopt related technologies to improve the accuracy and reliability of reputation evaluation, they do not take all the above-mentioned influence factors into account. Meanwhile, they either consider only the improvement of the direct reputation evaluation, or just the improvement of the recommended reputation evaluation. Therefore, their MDA is lower than that of the TRDG. Moreover, both RCCS and JSSRA do not consider the mobile attacks and cannot transfer malicious attackers' reputation value, which influence the MDA performance of them. Thus, the MDA performance of the TRDG is much better than of the RCCS and JSSRA.

3) SPECTRUM DECISION ACCURACY RATIO (SDA)

We also evaluate the effectiveness and reliability of the three spectrum sensing strategies by comparing their SDA performance to each other in the presence of SSDF and Mobile attacks.

The results in Fig. 8(a) show that the SDA of the three strategies keep a relative stable high value in the presence of the SSDF attacks. This is because that all of the three strategies use the reputation and incentive mechanisms to incentive the user to provide true sensing information, and thus reduce the probability of the attack and increase the SDA of all the three strategies. For TRDG, the higher accuracy, efficiency, and reliability of the reputation mechanism leads to a better MDA performance than of the RCCS and JSSRA,

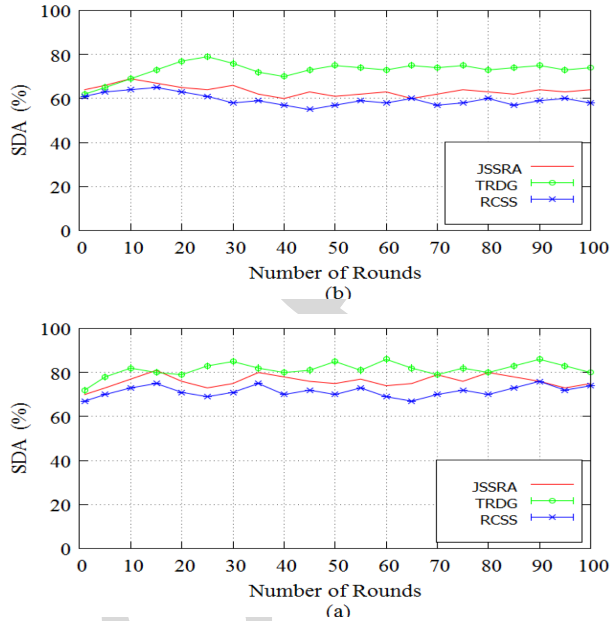


FIGURE 8. Spectrum decision accuracy (a) with SSDF attacks (b) with mobile attacks.

which makes the sensing information more accuracy and improve the SDA of the TRDG. So, the SDA of the TRDG is the highest among all the three strategies.

Comparing to the results in Fig. 8(a), in Fig. 8(b) where the Mobile attacks are present, the SDAs of TRDG, JSSRA and RCCS decrease by 6%, 10% and 12%, respectively. The comparison results show that the Mobile attacks have a big impact on the effectiveness and reliability of the SDAs of JSSRA and RCCS. The much less decline rate of TRDG makes TRDG keeping the highest SDA among all the three strategies in the presence of the Mobile attacks. The reason is that the JSSRA and RCCS lack of effective Mobile attack defense scheme, so the trustworthiness and reliability of the sensing information they collected are less than that of the TRDG, which makes their SDAs are worse than that of the TRDG.

4) FALSE SPECTRUM DECISION RATIO (FSDR)

Finally, we analyze the false spectrum decision ratio of the three spectrum sensing strategies in the presence of SSDF and Mobile attacks.

The results in Fig. 9(a) show that the FSDR of all the three strategies are less than 40%, which demonstrates that all of them have a good FSDR performance in the presence of SSDF attacks. This is because the proposed reputation and incentive mechanisms in all the three strategies improve the accuracy and reliability of the collected spectrum sensing information, enhance the ability of resistance to SSDF attacks, and then reduce the false ratio of the spectrum decision. For TRDG, the proposed reputation mechanism has greater accuracy and reliability than those of the other strategies, and the proposed incentive mechanism is dynamic and tightly coupled with reputation, all of these leads to a

IEEE Access

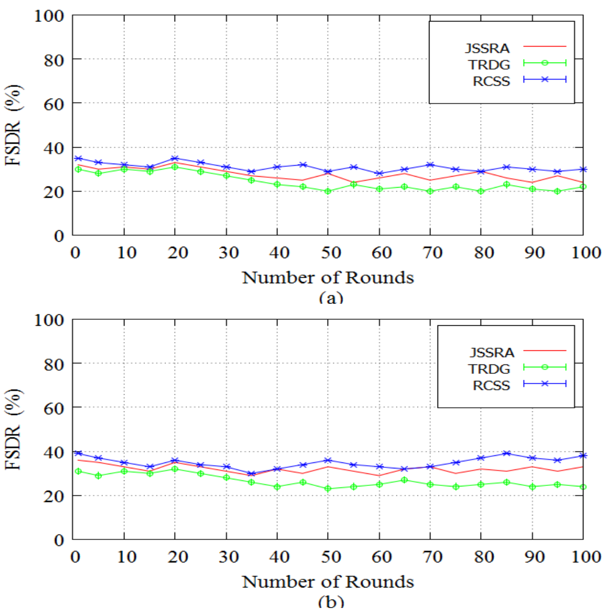


FIGURE 9. **False spectrum decision ratio (a) with SSDF attacks (b) with mobile attacks.**

better FSDR performance than of the RCCS and JSSRA. So, the FSDR of the TRDG is the lowest among all the three strategies.

Comparing to the results in Fig. 9(a), in Fig. 9(b) where the Mobile attacks are present, the FSDR of TRDG, JSSRA and RCCS increase by 2%, 5% and 6%, respectively. The comparison results show that the Mobile attacks have a big impact on accuracy of spectrum decision. However, the TRDG still have a best FSDR performance among all the three strategies. The reason is that the JSSRA and RCCS lack of effective Mobile attack defense scheme, so the accuracy, trustworthiness and reliability of the sensing information they collected are less than that of the TRDG, which makes their FSDRs are worse than that of the TRDG.

VI. CONCLUSIONS

In this paper, we investigated the challenging problem of protecting against internal SSDF and Mobile attacks for enhancing the security and accuracy of the collaborative spectrum sensing (CSS) in CRN based CPS (CRN-CPS). A new transferring reputation mechanism and dynamic game model based secure collaborative spectrum sensing strategy (TRDG) has been proposed, which incorporates innovative technologies in terms of the reputation value transferring, recommendation incentive and location sensing. The simulation experiments and performance analysis have verified that the TRDG is effective and efficient. More specifically, in the presence of SSDF attacks and Mobile attacks, the attack ratio, the malicious SU detection accuracy, the spectrum decision accuracy ratio, and the false spectrum decision ratio of the proposed TRDG are better than those of the existing ICS, JSSRA and RCSS strategies. For the future work, we plan to introduce the encryption or signature based privacy preserving technology into the reputation mechanism and spectrum collaborative sensing process to improve the performance of privacy preserving.

REFERENCES

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

[2] S. Y. Lien, S. M. Cheng, S. Y. Shih, and K. C. Chen, "Radio resource management for QoS guarantees in cyber-physical systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1752–1761, Sep. 2012.

[3] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, Mar. 2011.

[4] D. B. Rawat, S. Reddy, N. Sharma, B. B. Bista, and S. Shetty, "Cloud-assisted GPS-driven dynamic spectrum access in cognitive radio vehicular networks for transportation cyber physical systems," in *Proc. WCNC*, Mar. 2015, pp. 1942–1947.

[5] S. R. Reddy, "Heterogeneous dynamic spectrum access in cognitive radio enabled vehicular networks using network softwarization," Ph.D. dissertation, Dept. Electron., Georgia Southern Univ., Statesboro, GA, USA, 2016, p. 1392.

[6] T. Zhang, *Security Issues in Cognitive Radio Networks*. Springer, 2014, pp. 88–113.

[7] C.-Y. Chen, Y.-H. Chou, H.-C. Chao, and C.-H. Lo, "Secure centralized spectrum sensing for cognitive radio networks," *Wireless Netw.*, vol. 18, no. 6, pp. 667–677, Aug. 2012.

[8] R. Chen, J.-M. J. Park, and K. Bian, "Robustness against Byzantine failures in distributed spectrum sensing," *Comput. Commun.*, vol. 35, no. 17, pp. 2115–2124, Oct. 2012.

[9] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 360–368, Aug. 2014.

[10] 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 Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb. 2011.

[11] S. Yadav and M. J. Nene, "RSS based detection and expulsion of malicious users from cooperative sensing in cognitive radios," in *Proc. IACC*, Feb. 2013, pp. 181–184.

[12] 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 *Proc. WCNC*, Apr. 2013, pp. 614–619.

[13] A. Mukherjee, "Diffusion of cooperative behavior in decentralized cognitive radio networks with selfish spectrum sensors," *IEEE J. Sel. Topics Signal Process.*, vol. 7, no. 2, pp. 175–183, Apr. 2013.

[14] S. Li, H. Zhu, Z. Gao, X. Guan, and K. Xing, "YouSense: Mitigating entropy selfishness in distributed collaborative spectrum sensing," in *Proc. INFOCOM*, Apr. 2013, pp. 2635–2643.

[15] Z. Li, F. R. Yu, and M. Huang, "A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 383–393, Jan. 2010.

[16] T. Zhang, N. R. Safavi-Naini, and Z. Li, "ReDiSen: Reputation-based secure cooperative sensing in distributed cognitive radio networks," in *Proc. ICC*, Jun. 2013, pp. 1194–1198.

[17] 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 *Proc. INFOCOM*, Mar. 2012, pp. 900–908.

[18] T. Zhang, Z. Li, and R. Safavi-Naini, "Incentivize cooperative sensing in distributed cognitive radio networks with reputation-based pricing," in *Proc. INFOCOM*, Apr./May 2014, pp. 2490–2498.

[19] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.

[20] S. A. Mousavifar and C. Leung, "Energy efficient collaborative spectrum sensing based on trust management in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 1927–1939, Apr. 2015.

[21] M. F. Amjad, B. Aslam, A. Attiah, C. C. Zou, "Towards trustworthy collaboration in spectrum sensing for ad hoc cognitive radio networks," *Wireless Netw.*, vol. 22, no. 3, pp. 781–797, Apr. 2016.

[22] H. Chen, M. Zhou, L. Xie, K. Wang, J. Li, "Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9181–9191, Nov. 2016.

[23] H. Lin, J. Hu, C. Huang, L. Xu, and B. Wu, "Secure cooperative spectrum sensing and allocation in distributed cognitive radio networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 10, pp. 1–12, Jan. 2015.

[24] H. Lin, J. Hu, J. Ma, L. Xu, and L. Yang, "CRM: A new dynamic cross-layer reputation computation model in wireless networks," *Comput. J.*, vol. 58, no. 4, pp. 656–667, Apr. 2015.

[25] Y. Sun, B. L. Mark, and Y. Ephraim, "Collaborative spectrum sensing via online estimation of hidden bivariate Markov models," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5430–5439, Aug. 2016.

[26] A. A. Sharifi and M. J. M. Niya, "Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 93–96, Jan. 2016.

[27] A. Sharifi and J. M. Niya, "Securing collaborative spectrum sensing against malicious attackers in cognitive radio networks," *Wireless Pers. Commun.*, vol. 90, no. 1, pp. 75–91, Sep. 2016.

[28] H.-Y. Hsieh, Y.-E. Lin, and M.-J. Yang, "Weakest-link coalition: Further investigation on cooperative interference-aware spectrum sensing and access," *IEEE Trans. Mobile Comput.*, vol. 15, no. 3, pp. 774–788, Mar. 2016.

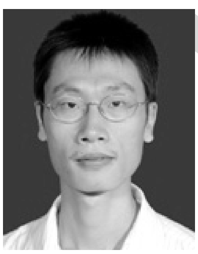
[29] S. Chen, H. A. Love, and C.-C. Liu, "Optimal opt-in residential time-of-use contract based on principal-agent theory," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4415–4426, Nov. 2016.

[30] Z. Zhu and B. Yu, "A modified homotopy method for solving the principal-agent bilevel programming problem," in *Computational and Applied Mathematics*. 2016, pp. 1–26.

[31] H. Lin, L. Xu, X. Huang, W. Wu, and Y. Huang, "A trustworthy access control model for mobile cloud computing based on reputation and mechanism design," *Ad Hoc Netw.*, vol. 35, pp. 51–64, Dec. 2015.

[32] H. Lin, L. Xu, Y. Mu, and W. Wu, "A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing," *Future Generat. Comput. Syst.*, vol. 52, pp. 125–136, Nov. 2015.

[33] B. Gao *et al.*, "Incentivizing spectrum sensing in database-driven dynamic spectrum sharing," in *Proc. INFOCOM*, Apr. 2016, pp. 1–9.



HUI LIN received the B.S. degree in computing science from Fujian Normal University, China, in 1999, and the M.E. degree in communication and information engineering from the Chongqing University of Posts and Telecommunications, China, in 2007. He is pursuing the PH.D. degree with the College of Computer Science, Xidian University. He is currently an Associate Professor with the College of Mathematics and Computer Science, Fujian Normal University, China. His research interests include wireless and mobile computing systems, computer networks, and information and network security.

JIA HU received the B.E. and M.E. degrees in communication engineering and physical electronics from the Huazhong University of Science and Technology, Wuhan, China, in 2004 and 2006, respectively, and the Ph.D. degree in computing from the University of Bradford, U.K., in 2010. He is currently a Lecturer with the Department of Computer Science, University of Exeter, U.K. His research interests include performance modeling and analysis, network protocols and algorithms, next generation networks, cross-layer optimization, network security, and resource management.

JIANFENG MA (M'–) received the B.S. degree in mathematics from Shanxi Normal University, China, in 1985, the M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University, China, in 1988 and 1995, respectively. From 1999 to 2001, he was with the Nanyang Technological University of Singapore as a Research Fellow. He is currently a Professor and a Ph.D. supervisor with the School of Computer Science, Xidian University, Xi'an, China. His current research interests include distributed systems, wireless and mobile computing systems, computer networks, and information and network security. He has authored over 150 refereed articles and co-authored ten books. He is a Senior Member of Chinese Institute of Electronics.

LI XU (M'–) received the B.S. and M.S. degrees from Fujian Normal University in 1992 and 2001, respectively, and the Ph.D. degree from the Nanjing University of Posts and Telecommunications in 2004. He is currently a Professor and a Ph.D. Supervisor with the School of Mathematics and Computer Science, Fujian Normal University. He is also the Vice Dean of the School of Mathematics and Computer Science and the Director of the Key Laboratory of Network Security and Cryptography in Fujian Province. He has authored over 100 papers in refereed journals and conferences. His interests include wireless networks and communication, network and information security, complex networks and systems, and intelligent information in communication networks. He has been invited to act as the PC chair or member at over 30 international conferences. He is a member of the ACM and a Senior Member of CCF and CIE in China.

ZHENGXIN YU is currently pursuing the Ph.D. degree with the Department of Computer Science, University of Exeter. Her research interests include machine learning, wireless networks, and performance evaluation.

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

PLEASE NOTE: We cannot accept new source files as corrections for your paper. If possible, please annotate the PDF proof we have sent you with your corrections and upload it via the Author Gateway. Alternatively, you may send us your corrections in list format. You may also upload revised graphics via the Author Gateway.

AQ:1 = Please note that there were discrepancies between the accepted pdf [AcceptedPdfQuery_Access-submit-0831] and the [Access-submit-FINAL.doc] in the sentence on lines 251–253, 551–556 and 733–737. We have followed [Access-submit-FINAL.doc].

AQ:2 = The subpart labels in “Figs. 6–9” have been hidden. As the images are non-editable, they not able to be processed further to set them right. Please provide updated images or advice as to how to proceed further.

AQ:3 = Please provide the publisher location for ref. [6].

AQ:4 = Please provide the pubisher name and publisher location for ref. [30].

AQ:5 = Please provide the missing IEEE membership years for the authors “Jianfeng Ma and Li Xu.”