Trust-based Data Fusion Mechanism Design in Cognitive Radio Networks

Ji Wang†, Ing-Ray Chen*
†Department of Electrical and Computer Engineering, Virginia Tech
*Department of Computer Science, Virginia Tech
Email: traceyw@vt.edu, irchen@cs.vt.edu

***Abstract*—Cognitive radio is a promising solution for spectrum scarcities in the future. Secondary users (SUs) adopt cooperative sensing to learn the primary user's (PU's) occupancy activity. This paper develops a trust-based data aggregation scheme to cope with malicious SU attack in cooperative spectrum sensing in cognitive radio networks. The proposed scheme combines the first-hand and second-hand sensing evidence to guarantee the overall performance and adopts a static game model to discourage malicious SUs from reporting fake detection parameters. Both theoretical and simulation results show that the proposed scheme outperforms the traditional majority aggregation scheme despite a high percentage of malicious node population and can effectively distinguish malicious nodes from normal nodes by their reputation scores.**

***Index Terms*—Cognitive radio networks, cooperative spectrum sensing, trust, reputation, security, mechanism design.**

I. Introduction

Cognitive radio has aroused a lot of interest as a solution to spectrum scarcity in the next generation of wireless communication. The main idea of cognitive radio is to let the secondary users (SUs) opportunistically access the channels that are temporarily not occupied by the preassigned primary users (PUs). In a cognitive radio system, the access priorities of PUs have to be guaranteed, i.e., SUs need to learn the PUs' activities to avoid interfering with the PUs on the band. Therefore, SUs need to sense the PU activity on a particular spectrum before transmitting data on that spectrum. Due to limited sensing capabilities of individual SUs, cooperative spectrum sensing is provided as a way to gather SUs' sensing information in order to increase the accuracy of PU occupancy detection. However, cooperative spectrum sensing can be attacked by malicious SUs, who can intentionally report fake sensing results to mislead the final aggregated result. Therefore, how to design a secure data fusion scheme for cooperative spectrum sensing is a big challenge in security management of cognitive radio networks.

This paper proposes and analyzes a trust-based data fusion scheme based on *mechanism design theory* (also called reverse game theory) to aggregate the SUs' reported outcomes in such a way that the correctness of aggregated outcome is stable in the presence of a high percentage of malicious SUs. Mechanism design is a sub-field of microeconomics and game theory that considers how to construct and implement a mechanism that provides incentives for the users to communicate and act in such a way as to further the interest of the designer, despite the fact that the users are strategic and self-interested, and possess private information [1]. We apply mechanism design to implement a scheme providing incentives for all SUs within the system to report their actual sensing capabilities and sensing results, despite the fact that some of the SUs are self-interested with malicious intention. The basic idea is that the data fusion center (DFC) would like to know the true channel availability but the DFC cannot completely trust sensing reports from the SUs because it is in malicious SU's interest to distort the truth. With mechanism design, the DFC can design a static game whose rules can influence the SUs to act the way it would like. It is a static game in the sense that all SUs make decisions (or select a strategy) simultaneously, without knowledge of the strategies that are being chosen by the DFC.

Our trust-based data fusion scheme derived from the static game also employs a reputation system [2]–[4] to identify malicious SUs in the long run. During data fusion, a SU reports its sensing capability and the sensed channel availability to the DFC who makes a decision on the channel availability based on majority voting of trusted SUs. The SU sensing capability is taken into consideration in the static game in order to differentiate a fake outcome reported by a malicious SU from an erroneous outcome reported by a good SU with poor sensing capability. Moreover, the DFC can elect to check the channel availability in order to compare this first-hand evidence with a sensing outcome reported by a SU to detect if the SU lies about the channel availability.

The objectives of our trust-based data aggregation scheme are threefold: (1) under the designed scheme, malicious SUs have no incentive to report fake sensing capabilities; (2) considering the cost endured by the DFC, the proposed scheme should minimize the DFC checking probability in each time slot; and (3) the success decision rate for the data fusion outcome matching the ground truth channel availability should be maximized.

In order to identify erroneous sensing results due to SUs' poor sensing abilities, our scheme requires SUs to report the sensing capability. A threshold is set to filter out the SUs with low sensing capabilities. On the other hand, to avoid malicious SUs from reporting fake sensing abilities, the DFC can check the PU activity based on our static game model design. When checking the spectrum, the DFC punishes the SUs whose report outcomes are different by decreasing their reputation

scores based on their reported sensing capabilities. Otherwise, if the DFC does not sense the spectrum in a particular time slot, it aggregates the reported sensing outcomes from those SUs whose sensing capability is over a predefined threshold, weighed by their reputation scores.

In this paper we consider malicious attackers with intention to disrupt cooperative spectrum sensing. We consider four types of malicious SU attacks to test the resiliency of the proposed data aggregation scheme: "always yes," "always no," "always false," and "always random." Under the always yes attack scenario, the malicious SUs always report the presence of PUs ignoring their real sensing results. Under the always no attack scenario, the malicious SUs always report the absence of PUs on the channel ignoring the real detection results. Under the always false attack scenario, the malicious SUs always report the opposite of their sensed outcomes. Under the always random attack scenario, the malicious SUs randomly generate a sensing result to report to the DFC. We test the resiliency of our trust-based data fusion scheme against these four different attacks. We use simulation to demonstrate that our proposed scheme outperforms a traditional approach using a majority fusion rule under all attacking scenarios despite increasing malicious node population. Also, the malicious nodes can be identified through reputation scores in our scheme.

The research presented in this paper can be situated within the broader class of opportunistic channel selection strategy design in cognitive radio networks. The primary contributions of this paper are as follows:

- We design a trust-based scheme for cooperative spectrum sensing to enhance the detection accuracy of PU channel occupancy.
- We develop a static game based on mechanism design to discourage malicious SUs from reporting fake sensing capability.
- We analyze the impact of SUs' sensing capability regarding channel occupancy on their ability to dynamically exploit the band.

We begin with a brief discussion of the state of the art on opportunistic channel selection strategy design in Section II. Section III introduces the system model and notation used. Our proposed scheme is described and analyzed in Section IV. Section V presents the simulation results. We summarize our conclusions and outline directions for future work in Section VI.

II. Related work

In this section we summarize the state of art in trust and security mechanisms in cognitive radio networks.

A. Security in Cognitive Radio Networks

The security of cognitive radio networks was first discussed in [5], focusing on two security threats, i.e., incumbent emulation and spectrum sensing data falsification, that may wreak havoc on distributed spectrum sensing. After that, the security in cognitive radio networks has attracted a lot of interest. See [6] as a survey. [7] and [8] discussed the security and privacy requirements, and proposed a framework for security using a fast authentication and authorization architecture. [9] advocated trusted computing by which a co-process regulates SU reporting and prevents false reporting, or prevents a malicious SU from transmitting when the PU activity is detected.

The use of trust to enhance security of cognitive radio networks can be either centralized or distributed. [10] proposes a system-level trust model, in which trust is used as social capital to gain resources, based on a centralized cognitive radio network. [11] combines certificate-based trust with behavior-based trust in a distributed manner to establish direct and indirect communications among the SUs.

B. Cooperative Spectrum Sensing Related Attacks

Cooperative spectrum sensing is a promising technique to increase PU activity sensing accuracy in cognitive radio networks by aggregating sensing reports from different SUs. In cooperative spectrum sensing, malicious SUs may report false sensing data to the DFC to degrade the final aggregated sensing outcome.

In the literature, a number of research works have been conducted for effectively aggregating the reported outcomes from SUs. In [12], the sensing information of SUs is weighted to maximize the detection probability of available channels under the constraint of a required false alarm probability. However, the scheme only considers sensing errors from the SUs without considering the malicious behavior of SUs. [13] proposes a modified combinatorial optimization identification (COI) algorithm to defend against malicious attacks. [14] proposes an HMM-based malicious SU detection algorithm to simultaneously estimate two HMMs without requiring separated training sequences. [15] provides an algorithm based on the non-parametric Kruskal-Wallis test to detect malicious users without having a priori knowledge. [16] proposes a decentralized scheme utilizing spatial correlation of received signal strengths and aggregating decisions based on a neighborhood majority voting approach for the secondary users to decide malicious users. However, a common problem related to the works cited above [12]–[16] is that they cannot distinguish a fake sensing outcome reported by a malicious SU from an erroneous outcome reported by a good SU with poor sensing capability.

Recently, [17] discusses an innovative idea of decoupling the detection ability of each SU from the reported detection result. According to their model, each SU reports a binary detection result, i.e., whether the targeted frequency is used by PUs or not, together with its detection sensing power to the DFC. The DFC considers the detection ability and trust it has toward each SU, and applies a threshold below which the SU's reported result is filtered out. Therefore, the DFC's final decision is based on trusted SUs' reported outcomes only. However, their scheme may fail when there is a high percentage of malicious SUs in the system. In particular, as each SU reports

its own sensing capability, a malicious SU may intentionally report a higher sensing capability to get a higher impact on the final aggregated outcome. Moreover, if malicious SUs collude to report fake sensing capabilities, with a high percentage of malicious SUs within the system, their reported results will finally dominate the DFC's decision making, which will lead to a repeated wrong aggregated decision of the system. Our proposed scheme, on the other hand, can deal with the fake report problem despite the presence of a high percentage of malicious SUs. More specifically, our designed scheme allows the DFC to optionally sense the spectrum, then use the result to assess trustworthiness of SUs, and finally aggregate sensing outcomes from trusted SUs.

III. System Model and Notation

In this section, we discuss the system model for cooperative sensing in cognitive radio networks. The DFC architecture is shown in Figure 1. The notation used in the paper is summarized in Table I. We focus on the design principle and propose a general and flexible utility function design that applies to many scenarios. For example, the cost and utility functions considered in this paper (C, G and L in Table I) can be related to power, money, and/or risk in real scenarios.

We consider a cognitive radio network with N SUs and one DFC adopting the cooperative spectrum sensing technique to learn the PU activities on the channel. Time is slotted in fixed interval length. At the end of each time slot t, SU i reports its local sensing result in the current time slot O_i^t together with its sensing capability S_i^t to the DFC. More specifically, O_i^t is a binary value with $O_i^t = 1$ indicating SU i sensed PU existence in time slot t and $O_i^t = 0$ indicating SU i sensed no PU activity in time slot t. During the sensing process, SU i also knows its signal and noise level in time slot t, which can be translated into a continuous value $S_i^t \in [0, 1]$. This value indicates SU i's certainty for its reported sensing result, i.e., the closer S_i^t is to 1, the more certain SU i is about its reported sensing outcome in time slot t. Therefore, the closer S_i^t is to 1, the larger $i's$ reported result should be weighted in the final aggregated outcome. However, a malicious SU i may take advantage of this scheme by intentionally reporting a fake and high sensing capability $S_i^{'t}$ at time slot t to impact more on the final aggregated outcome. Apparently, a malicious SU does not want to report a low sensing capability because its sensing report will likely be filtered out by the DFC, and would not be able to affect the final accumulated sensing result. Therefore, we assume $S_i^{'t} > S_i^t$.

After gathering the reported information from SUs, the DFC applies data fusion rules for decision making. The data fusion rules can be categorized into hard decision and soft decision. Under hard decision rules, the DFC applies decision-based rules to combine the results from SUs. Three simple decision-based rules are "or," "and," and "majority" rules. Under soft decision rules, the DFC often makes decisions based on the reported energy from each SU. The soft decision rules usually have a higher communication overhead and require a complicated aggregation algorithm compared to hard decision rules. Therefore,

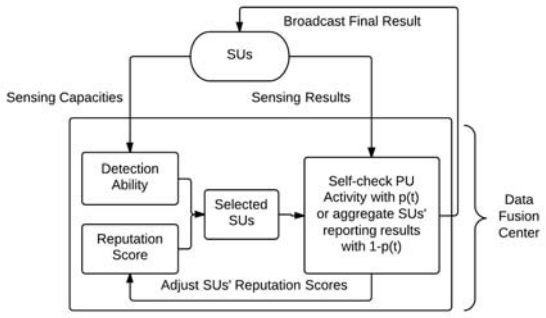


Figure 1: DFC Architecture.

we adopt hard decision rules in our fusion rule design. Let G denote the aggregation function adopted by DFC to generate the final outcome at time t, denoted by $O_{DFC}^t \in \{0, 1\}$.

Besides passively receiving reported results from SUs, the DFC can actively sense the spectrum so as to check if a SU lies about the sensing outcome. More specifically, the DFC checks the PU activity on the channel with probability p^t, with $p^t \in [0, 1]$, in each time slot t. After checking the spectrum availability, the DFC uses its "first-hand" evidence, denoted by O_{true}^t, to punish the SUs whose reported results are different from O_{true}^t based on the punishment function L. Note that malicious nodes will not know whether the DFC will check the PU activity on the channel in a particular slot because the DFC checks the PU activity probabilistically with probability p^t. The punishment to SU i in time slot t is in the form of decreasing SU i's reputation score R_i^t with $R_i^t \in Z$ for $i \in \{1, 2, ..., N\}$. We assume all SUs have the same initial reputation scores assigned by the DFC, i.e., $R_i^0 = R_j^0$ for $i \neq j$ and $i, j \in \{1, 2, ..., N\}$. Also, the punishment level to i is related to its reported sensing capability $S_i^{'t}$ because SU $i's$ erroneous sensing outcome is maybe due to its poor sensing capability. The reason that the DFC does not check the spectrum availability in every time slot is that the DFC spectrum sensing is often at a high cost of equipment, technology and energy. Moreover, when the coverage of spectrum is larger than the sensing range of the DFC (multiple channels), the DFC may not be able to check PU activities on all channels at the same time. Therefore, in our scheme, we represent this sensing cost by C which is a fixed value irrelevant of time. If in a particular time slot t the DFC checks the PU existence, it applies the punishment function L to decrease the reputation scores of those SUs with a different sensing result from O_{true}^t; if the DFC does not check the spectrum availability in t, it applies the aggregation function G to aggregate the opinions from SUs and generate the final outcome O_{DFC}^t.

Next, we introduce the type of malicious attacks considered in this paper. The attackers we consider are not just self-interested but also malicious with the intention to disrupt cooperative spectrum sensing. In cooperative spectrum sensing, the main attack is Spectrum Sensing Data Falsification (SSDF) by which a malicious SU attacks by sending a false sensing

Table I: Notation.

Symbol	Definition
N	the number of SUs.
O_i^t	The sensing result reported by SU i in time slot t. $i \in \{1, 2, ..N\}$ and $O_i^t \in \{0, 1\}$.
O_{DFC}^t	The accumulated outcome of the DFC in time slot t. $O_{DFC}^t \in \{0, 1\}$.
O_{true}^t	The true PU activity outcome sensed by DFC in time slot t. $O_{true}^t \in \{0, 1\}$.
S_i^t	The real sensing capability of SU i in time slot t. $i \in \{1, 2, ..N\}$ and $S_i^t \in [0, 1]$.
$S_i^{'t}$	The reported sensing capability of SU i in time slot t. $i \in \{1, 2, ...N\}$, $S_i^{'t} \in [0, 1]$ and $S_i^t \leq S_i^{'t}$
R_i^t	The reputation score of SU i in time slot t.$i \in \{1, 2, ..., N\}$ and $R_i^t \in Z$.
p^t	The probability for the DFC to check the PU activity on the spectrum in time slot t. $p^t \in [0, 1]$.
C	The cost of the DFC for sensing the spectrum in each time slot. $C > 0$.
G	Aggregation function adopted by DFC in each time slot.
L	Punishment function adopted by DFC in each time slot

report to the DFC. The SSDF attack can be further categorized into four types:

1) "Always yes" attack: malicious SUs always report the PU being active on the channels.
2) "Always no" attack: malicious SUs always report the channels being idle from PUs.
3) "Always false" attack: malicious SUs always report the opposite of their sensed channel occupancy.
4) "Always random" attack: malicious SUs report true/false channel occupancy randomly.

Our trust-based data fusion scheme derived from mechanism design thus has two design objectives:

- Design G and L to force malicious SUs to report the real sensing ability, i.e. $S_i^{'t} = S_i^t$ for $i \in \{1, ..., N\}$, $t > 0$.
- Design a scheme to allow the DFC to perform minimum checking with the smallest probability p^t.

IV. Mechanism Design for Cooperative Sensing and Its Analysis

In this section, we formulate a static game based on mechanism design to model decision making between the DFC and malicious SUs and then present a theoretical analysis.

We use a static game to model the relationship between the DFC and a malicious SU i in each single time slot. From a malicious SU i's perspective, in time slot t, it has two options on reporting its sensing capability: honestly reporting its sensing capability S_i^t or intentionally reporting a higher fake sensing capability $S_i^{'t} > S_i^t$. On the other side, from the DFC's perspective, in time slot t, it decides to sense the PU activity with probability p^t or not to with probability $1-p^t$. The payoff matrix for the DFC and a malicious SU i in the game model is shown in Table II. The table entry is in the format of (DFC payoff, malicious SU i payoff). For example, if the DFC checks the PU activity while SU i dishonestly reports a higher fake sensing capability $S_i^{'t} > S_i^t$, the payoff to the DFC is $L(S_i^{'t}, R_i^t) - C$ and the payoff to malicious SU i is $-L(S_i^{'t}, R_i^t)$.

We explain the payoff matrix Table II below. According to the described static game model of our scheme, in slot t, each malicious SU i reports both its detected result O_i^t and its sensing capability S_i^t to the DFC, who aggregates the reported results to the final outcome based on the aggregation function G. Therefore, the "impact" of i's reported result to the DFC's aggregation result O_{DFC}^t can be denoted as $G(S_i^{'t}, O_i^t, R_i^t)$, which can be viewed as the gain to the malicious SU if not caught by DFC. On the other side, in time slot t, the DFC decides to check the spectrum with probability p^t at a fixed cost C. If the DFC decides to check the spectrum, it can detect the true occupancy and then punish the nodes who reported a different outcome from the detected channel occupancy signal. Denoted by $L(S_i^t, R_i^t)$ the loss to SU i being punished due to the reported result different from that by the DFC. A malicious SU i who reports a fake value $S_i^{'t}$ will get a punishment $L(S_i^{'t}, R_i^t)$. Therefore, the payoff matrix between a malicious SU and the DFC can be defined as in Table II.

In this game, both the malicious SUs and the DFC want to maximize their own utility function. In particular, the malicious SUs aim at manipulating the DFC's aggregated outcome by reporting higher sensing capabilities. Meanwhile, the DFC aims to minimize the checking probability p^t and leave malicious SUs no motivation to report fake sensing capabilities.

Theorem 1 below conducts a theoretical analysis of the aggregation function G and the punishment function L.

Theorem 1. *To discourage malicious SU i from reporting a higher sensing capability than its actual sensing capability, i.e., $S_i^{'t} > S_i^t$, the DFC's checking probability p^t, aggregation function G and punishment function L should satisfy:* $p^t[L(S_i^{'t}) - L(S_i^t)] \geq (1 - p^t)[G(S_i^{'t}) - G(S_i^t)]$.

Proof: According to the described static game model and the payoff matrix shown in Table II, a malicious SU i's payoff of reporting S_i^t, i.e., $u_i(S_i^t, R_i^t)$, can be expressed as:

$$u_i(S_i^t, R_i^t) = \quad -p^t L(S_i^t, R_i^t) + (1 - p^t) G(S_i^t, O_i^t, R_i^t) \quad (1)$$

On the other side, if SU i reports a higher fake sensing capability $S_i^{'t}$, the payoff to SU, i.e., i $u_i(S_i^{'t}, R_i^t)$, is:

$$u_i(S_i^{'t}, R_i^t) = -p^t L(S_i^{'t}, R_i^t) + (1 - p^t) G(S_i^{'t}, O_i^t, R_i^t) \quad (2)$$

To guarantee that SU i has no incentive to report a higher fake sensing capability, we need $u_i(S_i^t, R_i^t) \geq u_i(S_i^{'t}, R_i^t)$. From Equations 1 and 2, we have:

Table II: The Payoff Matrix for the DFC and a Malicious SU.

	SU i reports S_i^t	SU i reports $S_i'^t$
DFC checks	$L(S_i^t, R_i^t) - C,\ -L(S_i^t, R_i^t)$	$L(S_i'^t, R_i^t) - C,\ -L(S_i'^t, R_i^t)$
DFC does not check	$-G(S_i^t, O_i^t, R_i^t), G(S_i^t, O_i^t, R_i^t)$	$-G(S_i'^t, O_i^t, R_i^t), G(S_i'^t, O_i^t, R_i^t)$

$$p^t(L(S_i'^t, R_i^t) - L(S_i^t, R_i^t)) \geq (1-p^t)(G(S_i'^t, O_i^t, R_i^t) - G(S_i^t, O_i^t, R_i^t)) \quad (3)$$

■

Theorem 1 provides a general rule for the design of the aggregation function G and the punishment function L. Let $\triangle G = G(S_i'^t, O_i^t, R_i^t) - G(S_i^t, O_i^t, R_i^t)$ and $\triangle L = L(S_i'^t, R_i^t) - L(S_i^t, R_i^t)$ denote the gain and loss of malicious SU i, respectively. Then, we can rewrite Equation 3 as $p^t \triangle L \geq (1-p^t)\triangle G$. That is, as long as the DFC checks the spectrum with probability no less than $\frac{\triangle G}{\triangle G + \triangle L}$, a malicious SU has no motivation to report a fake sensing capability.

Next, we analyze the checking probability p^t from the DFC's utility perspective. In time slot t, if DFC checks the spectrum availability, it observes the true PU activity result O_{true}^t. Let N_1 denote the set of malicious SUs within the system.

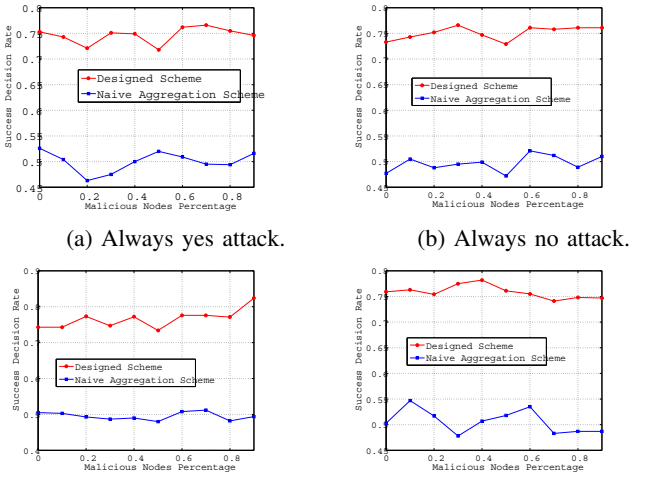
The DFC's payoff for checking the spectrum in a particular time slot can be expressed as $\sum_{i \in N_1} L(S_i^t, R_i^t) - C$; the DFC's payoff for not checking the spectrum is $-\sum_{i \in N_1} G(S_i^t, O_i^t, R_i^t)$. Therefore, the DFC's utility function under checking probability p^t is:

$$u_{DFC} = p^t(\sum_{i \in N_1} L(S_i^t, R_i^t) - C) - (1-p^t)\sum_{i \in N_1} G(S_i^t, O_i^t, R_i^t) \quad (4)$$

By taking the derivative of Equation 4 with respect to p^t, we get:

$$\frac{\partial u_{DFC}}{\partial p^t} = \sum_{i \in N_1} L(S_i^t, R_i^t) + \sum_{i \in N_1} G(S_i^t, O_i^t, R_i^t) - C \quad (5)$$

Equation 5 indicates that the optimized checking probability p^t depends on $\sum_{i \in N_1} L(S_i^t, R_i^t) + \sum_{i \in N_1} G(S_i^t, O_i^t, R_i^t) - C$. In particular, if $\sum_{i \in N_1} L(S_i^t, R_i^t) + \sum_{i \in N_1} G(S_i^t, O_i^t, R_i^t) - C > 0$, the optimal p^t value is 1. That is, the DFC should check the spectrum in every time slot to maximize its payoff. On the other side, if $\sum_{i \in N_1} L(S_i^t, R_i^t) + \sum_{i \in N_1} G(S_i^t, O_i^t, R_i^t) - C < 0$, the optimal p^t value is 0. Under this scenario, the DFC should not check spectrum to maximize its payoff. However, this analysis needs to be combined with the result generated in Theorem 1, which requires the check probability p^t to be at least $max_i \frac{\triangle G_i}{\triangle G_i + \triangle L_i}$



(a) Always yes attack. (b) Always no attack.

(c) Always false attack. (d) Always random attack.

Figure 2: Comparison of Success Decision Rate between Our Scheme and a Traditional Aggregation Scheme with varying Malicious Node Percentage.

V. Simulation Results

In this section, we analyze the performance of our trust-based data aggregation design by simulation. The performance of our trust-based data aggregation scheme will be compared with a traditional aggregation scheme where the DFC accumulates the reported results from all SUs and makes the final decision based on majority voting. In contrast, our scheme is designed based on Theorem 1 to discourage malicious nodes from reporting fake sensing capabilities.

We consider a cognitive radio system consisting 100 SUs and one DFC. We run a simulation experiment with 1000 repeated time slots. The ground truth of the channel occupancy is randomly simulated (either 0 or 1) in these 1000 runs. In each time slot, all SUs report the detected outcome (either 0 or 1) together with their sensing capabilities (within $[0, 1]$) to the DFC. We assume that malicious SUs report the highest sensing capability ($S_i'^t$=1) to maximize its impact, while good SUs report its true sensing capability (S_i^t following uniform distribution U[0, 1]) to the DFC. Also we assume that malicious SUs report the channel occupancy based on their attack strategies, while good SUs report the channel occupancy they sense.

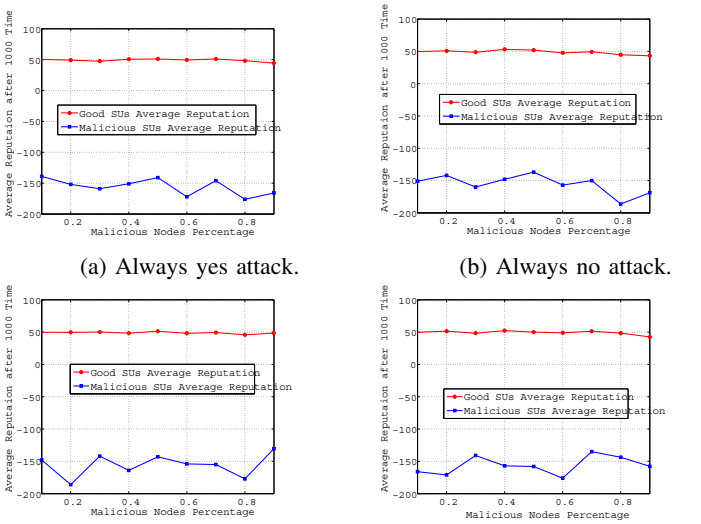
The data aggregation function G used by the DFC to aggregate SU sensing reports is based on trust-weighted majority voting. In particular, the DFC first filters out SUs whose reported sensing capabilities below a threshold (0.8). The DFC then categorizes the SUs into two groups S_0 and S_1: S_0

contains the SUs who reported no PU activity on the channel and S_1 contains the SUs who reported PU existence on the channel. Finally, the DFC decides the aggregated outcome as 0 if $\sum_{i\in S_0} R_i^t > \sum_{i\in S_1} R_i^t$, and as 1 otherwise. If the DFC does not check the spectrum, it applies the aggregation function G based on trust-based majority voting discussed above. If the DFC checks the spectrum in a particular time slot t, it senses true channel occupancy O_{true}^t, and uses it to punish the SUs who reported a different outcome. In particular, for a SU i with reported sensing capability S_i^t and reputation R_i^t at time slot t, the punishment function L on its reputation is $R_i^t = R_i^t - S_i^t$. The initial reputation score for each SU is 100, i.e., $R_i^0 = 100$ for $i \in \{1, ..., N\}$. Finally we note that with the G and L functions defined above, the DFC will check the spectrum in each time slot with probability $p^t = \frac{1}{2}$ based on Theorem 1 with the design of the aggregation function G and the punishment function L satisfying $\triangle G = \triangle L$. Notice here, we assume the cost for the DFC to check the channel is relatively large, i.e., $\sum_{i\in N_1} L(S_i^t, R_i^t) + \sum_{i\in N_1} G(S_i^t, O_i^t, R_i^t) - C < 0$. Therefore, from the DFC's perspective, it is always reluctant to check the channel availability by itself. However, to guarantee the malicious SUs do not have the incentive to fake sensing capabilities, the DFC still needs to sense the PU occupancy with the minimum checking probability given by Theorem 1.

A. Success Decision Rate

We analyze the success rate of the DFC's decision with respect to the percentage of malicious SUs under the four different malicious attacks considered in the paper. We vary the percentage of malicious SUs from 10% to 90% and calculate the success decision rate. We also output the success decision rate of the traditional data aggregation scheme as a comparison. The result is shown in Figure 2. Specifically, we analyze the performance under four types of malicious attacks: the "always yes" attack, shown in Figure 2a, where the malicious SUs always report the existence of PU activity; the "always no" attack, shown in Figure 2b, where the malicious SUs always report the absence of PU activity; the "always false" attack, shown in Figure 2c, where the malicious SUs always report the opposite of the sensed PU activity; the "always random" attack, shown in Figure 2d, where the malicious SUs randomly report a binary result as the PU activity.

From Figure 2 we see that our trust-based data aggregation scheme derived from the static game always performs better than the traditional approach. It especially outperforms the traditional approach under the "always false" attack behavior because the attackers will be caught whenever the DFC decides to check the channel availability with probability p^t. We conclude two observations. First, the performance of our designed scheme (around 75%) is significantly better than that of the traditional aggregation scheme (around 50%) over all four types of malicious SU attacks. Secondly, under all malicious attack scenarios, the performance of our designed scheme is stable over a wide range of malicious node percentage.



(a) Always yes attack. (b) Always no attack.

(c) Always false attack. (d) Always random attack.

Figure 3: Comparison of Good Node and Malicious Node Reputation Scores.

B. Reputation Scores

We compare the average reputation scores of the normal and malicious nodes under each attack scenario for our scheme. The results are shown in Figure 3 which demonstrates that our trust scheme can effectively distinguish malicious SUs by reputation scores. In particular, after 1000 time slots, the average reputation score of the normal nodes is around 50 while that of the malicious nodes is around -150. It means that when our trust-based fusion scheme is in place the malicious node reputation scores will drop dramatically with respect to time. Finally we also note that this reputation gap is stable with respect to the malicious node percentage.

VI. Conclusion

In this paper we proposed a trust-based data fusion scheme for cooperative spectrum sensing in cognitive radio networks to cope with malicious SU attacks. We formulated a static game to model decision making between the DFC and malicious nodes and identified design conditions that could force malicious nodes to report true sensing capabilities. We also combined the first-hand sensing information from the DFC with the reported sensing outcome from SUs to achieve a high success decision rate for the data fusion outcome, despite the presence a high percentage of malicious nodes. The simulation results demonstrated that our scheme outperforms a traditional data aggregation scheme when dealing with four different malicious nodes attack behaviors regardless of the percentage of malicious nodes. Moreover, our trust-based scheme is efficient in distinguishing malicious nodes with low reputation scores.

There are several future research areas. First, we plan to extend the static game model by considering new game rules and parameters including the minimum sensing capability threshold, and the malicious node attack probability to further improve the

success decision rate. Secondly, we plan to explore modeling techniques such as Stochastic Petri Nets [18]–[21] to model behaviors of the DFC and the SUs to study the interaction and exploit the design tradeoffs that exist in the game structure. Lastly, we plan to further test the resiliency of our trust-based data aggregation scheme derived from the static game model against more complicated environmental scenarios and more sophisticated attacks such as opportunistic and collusional attacks [22], [23]. The emphasis will be to relate the game theoretical model to actual systems and adversarial scenarios.

ACKNOWLEDGMENT

This work is supported in part by the U. S. Army Research Laboratory and the U. S. Army Research Office under contract number W911NF-12-1-0445.

REFERENCES

[1] L. Canzian, Y. Xiao, W. Zame, M. Zorzi, and M. van der Schaar, "Intervention with private information, imperfect monitoring and costly communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3192–3205, 2013.

[2] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[3] J.-H. Cho, A. Swami, and I.-R. Chen, "Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks," in *International Conference on Computational Science and Engineering*, August 2009, pp. 641–650.

[4] J.-H. Cho, A. Swami, and I.-R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1001–1012, 2012.

[5] R. Chen, J.-M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 50–55, April 2008.

[6] J. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, May 2008, pp. 1–7.

[7] N. Prasad, "Secure cognitive networks," in *Wireless Technology, 2008. EuWiT 2008. European Conference on*, Oct 2008, pp. 107–110.

[8] A. Sumathi and R. Vidhyapriya, "Security in cognitive radio networks - a survey," in *Intelligent Systems Design and Applications (ISDA), 2012 12th International Conference on*, Nov 2012, pp. 114–118.

[9] Y. Zhang, A. Baliga, and W. Trappe, "Reactive On-board Regulation of Cognitive Radios," in *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, Montreal, Canada, June 2010, pp. 1–6.

[10] T. Qin, C. Leung, C. Miao, and Y. Chen, "Trust-aware resource allocation in a cognitive radio system," in *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on*, vol. 3, May 2012, pp. 797–801.

[11] S. Parvin, S. Han, F. Hussain, and B. Tian, "A combinational approach for trust establishment in cognitive radio networks," in *International Conference on Complex, Intelligent, and Software Intensive Systems*, 2011, pp. 227–232.

[12] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 7, pp. 2135–2141, July 2011.

[13] Z. Qin, Q. Li, and G. Hsieh, "Defending against cooperative attacks in cooperative spectrum sensing," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 6, pp. 2680–2687, June 2013.

[14] X. He, H. Dai, and P. Ning, "Hmm-based malicious user detection for robust collaborative spectrum sensing," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 11, pp. 2196–2208, November 2013.

[15] F. Adelantado and C. Verikoukis, "A non-parametric statistical approach for malicious users detection in cognitive wireless ad-hoc networks," in *Communications (ICC), 2011 IEEE International Conference on*, June 2011, pp. 1–5.

[16] C. Chen, M. Song, C. Xin, and M. Alam, "A robust malicious user detection scheme in cooperative spectrum sensing," in *Global Communications Conference (GLOBECOM), 2012 IEEE*, Dec 2012, pp. 4856–4861.

[17] Y. Cai, L. Cui, K. Pelechrinis, P. Krishnamurthy, M. B. Weiss, and Y. Mo, "Decoupling trust and wireless chanel induced effects on collaborative sensing attacks," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, 2014.

[18] J.-H. Cho, I.-R. Chen, and P.-G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," *IEEE Transactions on Reliability*, vol. 59, no. 1, pp. 231–241, 2010.

[19] I.-R. Chen and D.-C. Wang, "Analyzing Dynamic Voting using Petri Nets," in *15th IEEE Symposium on Reliable Distributed Systems*, Niagara Falls, Canada, October 1996, pp. 44–53.

[20] I.-R. Chen and D.-C. Wang, "Analysis of replicated data with repair dependency," *The Computer Journal*, vol. 39, no. 9, pp. 767–779, 1996.

[21] Y. Li and I.-R. Chen, "Design and performance analysis of mobility management schemes based on pointer forwarding for wireless mesh networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 3, pp. 349–361, 2011.

[22] R. Mitchell and I. R. Chen, "Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems," *IEEE Transactions on Reliability*, vol. 62, no. 1, pp. 199–210, March 2013.

[23] R. Mitchell and I. R. Chen, "A Survey of Intrusion Detection in Wireless Network Applications," *Computer Communications*, vol. 42, pp. 1–23, March 2014.