Trust-based Cooperative Spectrum Sensing Against SSDF Attacks in Distributed Cognitive Radio Networks

Ji Wang
Dept. of Electrical and Computer Engineering
Virginia Tech
Blacksburg, VA 24060
Email: traceyw@vt.edu

Ing-Ray Chen
Dept. of Computer Science
Virginia Tech
Falls Church, VA 22043
Email: irchen@vt.edu

Jeffrey J.P. Tsai
Dept. of Bioinformatics and Biomedical Engineering
Asia University
Taichung, Taiwan
Email: jjptsai@gmail.com

Ding-Chau Wang
Dept. of Information Management
Southern Taiwan University of Science and Technology
Tainan, Taiwan
Email: dcwang@mail.stust.edu.tw

***Abstract*—We propose and analyze a trust-based data fusion scheme against spectrum sensing data falsification attacks in a distributed cognitive radio network. Our trust-based data fusion scheme is based on *mechanism design theory* to motivate users to report authentic sensing data so as to improve the success rate. Further, we decouple erroneous sensing reports due to low sensing capabilities from false reports due to attacks, thus avoiding unnecessary punishments to benign users. We conduct a theoretical analysis validated with extensive simulation and identify optimal parameter settings under which our trust-based data fusion scheme outperforms existing non-trust based data fusion schemes.**

***Index Terms*—Distributed cognitive radio networks, cooperative spectrum sensing, SSDF, trust, mechanism design.**

I. Introduction

The main idea of cognitive radio is to let the secondary users (SUs) opportunistically access the channels that are temporarily not occupied by the primary users (PUs). Cooperative spectrum sensing significantly improves the probability of detecting the transmission of PUs and provides a way to increase channel sensing accuracy in cognitive radio networks [1]. The idea behind cooperative spectrum sensing is to adopt data fusion rules to aggregate sensing reports from SUs within the network.

Cooperative spectrum sensing can be conducted in both centralized and distributed cognitive radio networks. In a centralized system, SUs report sensing outcomes to a data fusion center (DFC) and receive instructions from the DFC. In a distributed system, SUs do not rely on a DFC for channel access decision making but autonomously decide the channel availability by aggregating outcomes reported by other SUs. Cooperative spectrum sensing is confronted by spectrum sensing data falsification (SSDF) attacks by which malicious SUs intentionally report fake sensing results to mislead decision making. Most existing anti-attack fusion rules in cooperative spectrum sensing are for the centralized infrastructure [2]–[4]. To date, there are only a handful of works on fusion rule design against SSDF attacks in distributed cognitive radio networks [5]–[7]. This paper is concerned with effective data fusion rules against SSDF attacks in a distributed cognitive radio system.

One common drawback of existing works is that they fail to decouple erroneous sensing reports due to low sensing capabilities from false reports due to attacks. The consequence is that benign SUs can be misidentified as attackers, which can cause severe performance degradation. Recently, [4] proposed a fusion rule to discern erroneous sensing reports due to low sensing capabilities from false reports due to attacks. In particular, the data fusion rule requires each SU to report a binary sensing outcome together with its sensing power to the DFC in a centralized cooperative spectrum sensing system. However, their approach may fail when malicious SUs intentionally report higher sensing capabilities to impact more on the final data fusion outcome. To solve this problem, [3] proposed a data fusion rule to discourage malicious nodes from reporting fake sensing capabilities. The above two cited works are for centralized cooperative spectrum sensing only. In this work, we extend [3] to distributed cooperative spectrum sensing against SSDF in distributed cognitive networks.

A unique contribution of our work is that we develop a trust-based data fusion scheme based on *mechanism design theory* [8] to provide incentives for all SUs within the system to report their actual sensing capabilities and outcomes, despite the fact that some of the SUs are self-interested with malicious intent. Our trust-based data fusion scheme employs a trust system [9] to identify malicious SUs in the long run.

The primary contributions of this paper are as follows:

- We are the first to design trust-based data fusion rules

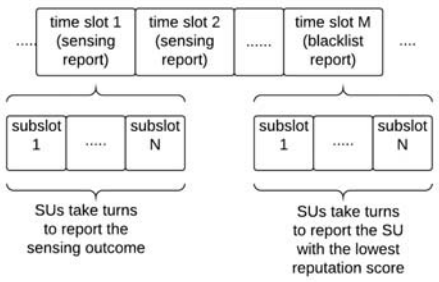

Figure 1: Time Schedule on the Common Control Channel.

which decouple erroneous reports due to low sensing capabilities from false reports due to attacks in distributed cooperative spectrum sensing systems.

- Our scheme based on *mechanism design* guarantees that a benign SU will be awarded with trust gain if it reports its true sensing capability and sensing outcome faithfully, while a malicious SU's trust will be penalized with trust loss if it falsely reports a high sensing capability and performs SSDF attacks.
- We identify the best parameter settings under which the performance of our proposed scheme is optimized and outperforms existing schemes.

We begin with introducing the system model in Section II. Our proposed scheme is described in III. Section IV conducts a theoretical analysis. Section V presents simulation results to validate theoretical results. We summarize the paper and outline directions for future work in Section VI.

II. System Model

We consider a distributed cognitive radio network with N SUs adopting the cooperative spectrum sensing technique to learn the PU's activity on one channel. We assume that all SUs are aware of the existence of each other and are within the communication range. In particular, each SU has a unique identity $i \in \{1, ..., N\}$ which is publicly known by other SUs. To control the overhead communication messages, SUs are not allowed to communicate directly with each other. Instead, the SUs share their sensing outcomes on a common control channel (CCC) in a broadcast manner. To avoid communication interference on the CCC, time is slotted and each time slot is further divided into N subslots, one for each SU. An SU with identity i will only broadcast its report in the ith designated subslot while listening to other SUs' reports in other subslots. Since each SU has a unique identity and it can broadcast only in its designated subslot, there is no identity attack possibility. There are altogether M time slots in a reporting cycle. The first $M-1$ slots (each called a sensing report slot) are used for reporting sensing outcomes and sensing capabilities, while the last time slot (called a blacklist report slot) is used for reporting malicious nodes for the purpose of building a blacklist. M is a system parameter and should be sufficiently large to allow each individual SU to assess trust scores of other SUs and report malicious SUs in the blacklist report slot. Figure 1 shows a time schedule on the common control channel.

In a sensing report slot, SUs take turns to broadcast their sensing outcomes in their respective subslots. Specifically, SU i broadcasts its outcome O_i^t together with its capability $C_{i,real}^t$ on the CCC. SU i's outcome O_i^t is a binary variable with $O_i^t = 1$ indicating that SU i sensed PU existence and $O_i^t = 0$ indicating that SU i sensed no PU activity. i's sensing capability denoted by $C_{i,real}^t$ is a continuous value $\in [0, 1]$ representing the probability of SU i being able to correctly sense the channel occupancy status. Hence, the closer $C_{i,real}^t$ is to 1, the more confident SU i is about its reported sensing outcome at time t. An SU's sensing capability is characterized by the probabilities of false alarm and missed detection. We follow [5] for estimating the missed detection rate P_{md} and the false alarm rate P_{fa}, as follows:

$$P_{md} = P(p_i^t < \gamma | H_1) \tag{1}$$

$$P_{fa} = P(p_i^t > \gamma | H_0) \tag{2}$$

where H_1 and H_0 denote the hypotheses corresponding to the presence and the absence of PU, respectively, and p_i^t represents the received signal power by SU i at time t which can be estimated by an energy detection sensing method [10]. The sensing capability $C_{i,real}^t$ of SU i can be estimated based on its false alarm rate P_{fa} and missed detection rate P_{md}. Specifically, when SU i senses the existence of PU, its sensing capability can be calculated as $C_{i,real}^t = 1 - P_{md}$. When SU i senses the absence of PU, its sensing capability can be calculated as $C_{i,real}^t = 1 - P_{fa}$.

Let $C_{i,report}^t$ be the sensing capability reported by SU i at time t. A benign SU i reports its real sensing capability, i.e., $C_{i,report}^t = C_{i,real}^t$, while a malicious SU i intentionally reports a higher sensing capability $C_{i,report}^t > C_{i,real}^t$ to impact other SUs' decision making.

In a blacklist report time slot, each SU reports an SU with the lowest trust score among all SUs it keeps in its database. SU i then updates its blacklist binary vector b_j^i for $j \in \{1, 2, ..., N\}$ based on the blacklist reports gathered in the blacklist report slot. We assume that a malicious node can perform *bad-mouthing* attacks to frame a good node as a bad node.

The goal of our distributed cooperative spectrum sensing design is for SU i to effectively aggregate self and received sensing information, i.e., (O_i^t,$C_{i,report}^t$) for $i \in \{1, ..., N\}$ such that it can achieve high accuracy in sensing PU occupancy and detect malicious SUs in the long run.

III. Trust-Based Data Fusion Rule Design

In this section, we describe our trust-based data fusion rule design consisting of a data fusion process and a blacklist generation process. An SU makes channel availability decisions using sensing reports gathered in a sensing report slot. An SU updates its blacklist in the blacklist generation process using blacklist reports gathered in a blacklist report time slot.

A. Data Fusion Process

In a sensing report slot, SU i makes a channel occupancy decision based on its own and received sensing outcomes from other SUs. Due to a lack of ground truth in decision making, SU i first decides whether to trust its own sensing outcome by comparing its own sensing outcome $C^t_{i,real}$ with a minimum sensing capability threshold T^t_i. There are two cases:

1) If $C^t_{i,real} > T^t_i$, SU i has high confidence about its own sensing outcome and will simply adopt its sensing outcome as the final decision, i.e., $O^t_{i,final} = O^t_i$. Meanwhile, i adjusts other SUs' trust scores by comparing the received sensing outcomes with its own sensing outcome. Initially all SUs start with the same trust score of 1 which represents ignorance. SU i updates the trust score of SU j, denoted by $R^t_{i,j}$, only if SU $j's$ reported sensing capability is over SU i's minimum trust threshold, i.e., $C^t_{j,report} > F^t_i$, where F^t_i is SU i's minimum trust threshold in the range of [0, 1]. In this case if j's reported outcome matches i's outcome, SU i increases SU j's trust score by:

$$R^t_{i,j} = R^t_{i,j}(1 + C^t_{j,report}) \tag{3}$$

If j's reported outcome O^t_j does not match i's sensing outcome, SU i decreases SU j's trust score by:

$$R^t_{i,j} = R^t_{i,j}(1 - (C^t_{j,report})^2) \tag{4}$$

2) If $C^t_{i,real} \leq T^t_i$, SU i does not have confidence in its own sensing outcome and will rely on the received sensing information reported by other SUs to decide the final outcome. In this case, given that SU i does not have any basis to judge the trustworthiness of sensing results reported by other SUs, SU i does not update the trust scores of other SUs. SU i first filters out sensing reports from receivers with low sensing capabilities, i.e., $C^t_{j,report} < F^t_i$, or on the blacklist, i.e., $b^i_j = 1$ for $j \in \{1, 2, ..., N\}$. After the minimum capability step, the remaining reports are separated into two groups based on if the sensing outcome is 0 or 1. For each group, a group trust score is calculated by a capability-weighted trust sum. SU i then chooses the group with a higher group trust score, and adopts the sensing outcome of the group (either 0 or 1) as the final outcome. If the group scores are of the same value, SU i randomly decides the channel occupancy status for that time slot.

B. Blacklist Generation Process

In a blacklist report slot t, SU i reports the identity of the lowest trust node $B^t_i \in \{1, ..., N\}$. If more than one node are of the same lowest trust score, SU i randomly chooses one to broadcast. Meanwhile, SU i updates a blacklist binary vector $[b^i_1, ..., b^i_N]$ based on the received node identities broadcast by other SUs. Since a malicious SU may perform bad-mouthing attacks and intentionally report a good node as a malicious node, SU i considers B^t_j (reported by SU j) as malicious only if i trusts j as well as i does not trust B^t_j itself. Specifically, SU i considers that B^t_j should be put on the blacklist if the following two conditions are met:

1) j's trust score is above the average trust score of all nodes maintained by i;
2) B^t_j's trust score is below the average trust score of all nodes maintained by i.

After i decides j as a malicious node, i sets b^i_j to 1 and will exclude j's reports in future decision making.

IV. Analysis

In this section, we theoretically analyze our data fusion rule design. We denote by G and L the trust gain and loss, respectively. The theorem below provides the design of G and L to make sure that a benign SU will be awarded with trust gain if it reports its true sensing capability and sensing outcome faithfully.

Theorem 1. *For a trust-based data fusion rule design to award SU j who reports its authentic sensing outcome and capability, the trust gain (G) and the trust loss (L) must satisfy:*

$$1 - C^t_{i,real} + C^t_{j,real} - 2C^t_{i,real}C^t_{j,real} \geq \frac{G}{G - L}$$

Proof: The reported sensing capability of node j, $C^t_{j,real}$, is the probability of j being able to sense PU existence status on the channel. According to our designed scheme (described in Section III) the conditions to award j's trust by SU i are: i trusts its own sensing outcome, i.e., $C^t_{i,real} > T^t_i$, j's sensing capability is above i's minimum trust threshold, i.e., $C^t_{j,real} > F^t_i$, and j's reported sensing outcome matches that of i, i.e., both i and j sense PU existence the same way either 0 or 1. Therefore, the probability for j being rewarded by SU i with sensing capability $C^t_{i,real}$, denoted by P_{award}, is given by:

$$\begin{aligned} P_{award} =& p(C^t_{i,real} > T^t_i)p(C^t_{j,real} > F^t_i) \\ & (C^t_{i,real}C^t_{j,real} + (1 - C^t_{i,real})(1 - C^t_{j,real})) \end{aligned} \tag{5}$$

On the other hand, the conditions to penalize j's trust by SU i are: i trusts its own sensing outcome, i.e., $C^t_{i,real} > T^t_i$, j's sensing capability is above i's minimum trust threshold, i.e., $C^t_{j,real} > F^t_i$, and j's reported sensing outcome conflicts with that of i, which happens if only one of the two SUs correctly senses PU existence. Therefore, the probability of j being punished by i with sensing capability $C^t_{i,real}$, denoted by P_{punish}, is given by:

$$P_{punish} = p(C^t_{i,real} > T^t_i)p(C^t_{j,real} > F^t_i) \\ (C^t_{i,real}(1 - C^t_{j,real}) + C^t_{j,real}(1 - C^t_{i,real})) \quad (6)$$

To guarantee j's trust is not penalized when it reports its real sensing outcome and capability, we need:

$$GP_{award} \geq LP_{punish} \quad (7)$$

By plugging in Equation 5 and Equation 6 into Equation 7 we can obtain the expression shown in the theorem. ■

We denote by $\triangle G$ and $\triangle L$ the gap of trust gain and loss between reporting higher sensing capability and real sensing capability. The theorem below provides the design of $\triangle G$ and $\triangle L$ to prevent a malicious SU from gaining trust if it reports high sensing capability and performs SSDF attacks.

Theorem 2. *To prevent a malicious SU j from reporting higher sensing capability to gain trust increase to SU i, $\triangle G$ and $\triangle L$ must satisfy:*

$$C^t_{i,real}\triangle L \geq (1 - C^t_{i,real})\triangle G$$

Proof: For a malicious SU j who reports a fake sensing outcome and a higher capability s.t. $C^t_{j,report} > C^t_{j,real}$, the conditions for j to be caught and punished by SU i are: i trusts its own sensing outcome, i.e., $C^t_{i,real} > T^t_i$, j's sensing capability is above i's minimum trust threshold, i.e., $C^t_{j,report} > F^t_i$, and j's reported sensing outcome disagrees with that of i, which requires i's sensing outcome to be true. SU i uses a higher sensing capability than the minimum trust threshold, i.e., $C^t_{j,report} > F^t_i$, to mislead the data fusion process. Therefore, the probability of j being caught by i with sensing capability $C^t_{i,real}$, denoted by P_{caught}, is given by:

$$P_{caught} = p(C^t_{i,real} > T^t_i)C^t_{i,real} \quad (8)$$

Similarly, the probability of a malicious node j not being punished by SU i, denoted by P_{miss}, is given by:

$$P_{miss} = p(C^t_{i,real} > T^t_i)(1 - C^t_{i,real}) \quad (9)$$

To guarantee j's trust is decreased when it reports a fake sensing outcome and a higher calculated capability, we need:

$$\triangle LP_{caught} \geq \triangle GP_{miss} \quad (10)$$

By plugging in Equation 8 and Equation 9 into Equation 10 we prove the theorem. ■

Corollary 3. *Our trust-based data fusion rule design guarantees that a benign SU's trust is increased when it reports authentic sensing outcome and capability, and a malicious SU's trust is decreased when it reports a false sensing outcome and a higher sensing capability.*

Proof: We prove this corollary by showing that our trust-based data fusion rule design satisfies the above two theorems. According to Equations 3 and 4, a benign SU (j) who reports true sensing outcome O^t_{real} and capability $C^t_{j,real}$ and will get a trust increase of $G = R^{t-1}_{i,j} \times C^t_{j,real}$ and get a trust loss of $L = R^{t-1}_{i,j} \times (C^t_{j,real})^2$.

On the other hand, a malicious SU (j) who reports a fake sensing outcome and a higher capability $C^t_{j,report} > C^t_{j,real}$ will get an extra trust increase of $\triangle G = R^{t-1}_{i,j} \times (C^t_{j,report} - C^t_{j,real})$ and an extra loss of $\triangle L = R^{t-1}_{i,j} \times ((C^t_{j,report})^2 - (C^t_{j,real})^2)$.

We can easily confirm that G, L, $\triangle G$ and $\triangle L$ satisfy Theorems 1 and 2. ■

Therefore, our trust-based data fusion rule design guarantees a trust gain to normal SUs and discourages malicious SUs from reporting false sensing outcomes and capabilities.

V. Simulation Results

In this section, we conduct a performance analysis of our data fusion rule design using Matlab and compare its performance with three baseline schemes: individual, majority voting, and capability-weighted majority voting. Under individual data fusion, an SU directly accepts its sensing outcome as the final outcome without considering reported information from other SUs. Therefore, it can be viewed as a non-cooperative scheme. Majority voting counts the number of 0's and 1's and takes the majority as the final outcome. Capability-weighted majority voting is the same as majority voting except that every count is weighted by the SU's reported capability. The performance metric is the individual success rate, or the probability of successfully detecting the actual status of the channel.

The simulation setup is based on $N = 20$ SUs. As in [5], we assume that the SU sensing capability follows the Gaussian distribution. That is, each SU's true sensing capability is modeled by a Gaussian distribution with mean $\mu = 0.6$ and variance $\sigma^2 = 0.2$. The reported sensing capability for a malicious SU is set to a high value at 0.95. The initial trust score for all nodes is set to 1 representing ignorance. The report cycle M is set to a high value at 20 to allow each individual SU to assess trust scores of other SUs and report malicious SUs in the blacklist report slot. So in every 20 time slots, SUs update their individual

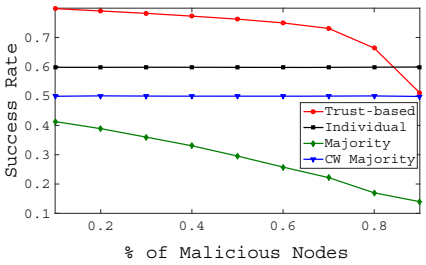

Figure 2: Impact of Malicious Node Population.

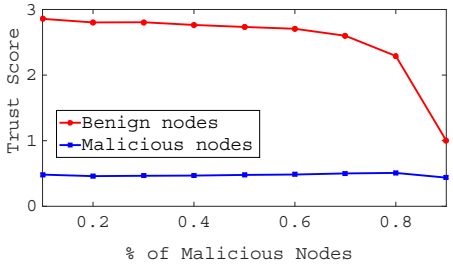

Figure 3: Comparison of Trust Scores.

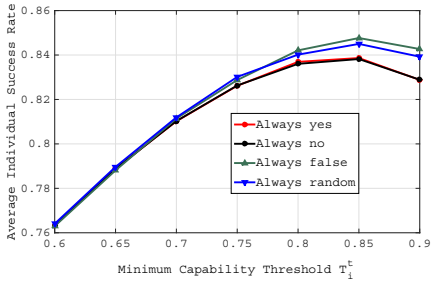

Figure 4: Impact of T_i^t.

blacklists based on blacklist reports from other SUs. Each experiment covers 200 time slots. The result is based on 1000 independent repeated experiments.

A. *Effect of Malicious Node Population*

We first investigate the effect of malicious node percentage on the individual success rate (i.e., the probability of successfully detecting the actual status of the channel). Figure 2 shows the individual success rate of our trust-based data fusion scheme (labeled by trust-based) against the three baseline schemes (labeled by individual, majority, and CW majority, respectively) in the presence of SSDF attacks. It is clear from Figure 2 that our data fusion rule design outperforms all baseline schemes. The gap between trust-based data fusion and individual data fusion can be viewed as the gain of adopting distributed cooperative spectrum sensing over non-cooperative spectrum sensing. The only exception happens when the percentage of malicious nodes is 90% in which case the number of benign nodes is only 2 (10% of N=20) and only one of which has capability higher than the minimum capability threshold, so there is no chance for them to update the trust scores of each other. As a result, the trust score remains at 1 and the success rate remains at 0.5.

We observe that the success rate under individual data fusion stays at 0.6. The reason is that each SU's true sensing capability is modeled by a Gaussian distribution with mean $\mu = 0.6$ and variance $\sigma^2 = 0.2$. We also observe that individual data fusion scheme performs better than majority voting which in turn performs better than capability-weighted majority voting, especially as the percentage of malicious nodes increases. This is because malicious SUs report a higher capability which has an adverse effect on capability-weighted majority voting. Our trust-based data fusion scheme on the other hand takes both trust and capability into consideration and can achieve a much higher accuracy in data fusion.

B. *Trust Scores of Benign and Malicious SUs*

We compare the average trust scores of benign and malicious nodes in our designed scheme. Figure 3 shows the average trust scores of benign and malicious SUs at the end of the 50^{th} time slot as recorded by benign SUs under SSDF attacks. The results support the claim that our trust-based data fusion scheme can effectively distinguish malicious SUs by their low trust scores. Figure 3 validates the theoretical analysis results that a benign SU will be awarded with trust gain if it reports its true sensing capability and sensing outcome faithfully, while a malicious SU's trust will be penalized with trust loss if it falsely reports a high sensing capability and a false sensing outcome. Our trust-based data fusion scheme can efficiently distinguish benign nodes from malicious nodes in the long run when the percentage of malicious nodes is below 80%.

C. *Impact of Threshold Parameters*

We analyze the impact of the minimum capability threshold T_i^t and the minimum trust threshold F_i^t on protocol performance. We consider 4 variants of SSDF attacks: always yes (always saying the channel is free), always no (always saying the channel is not free), always false (always saying

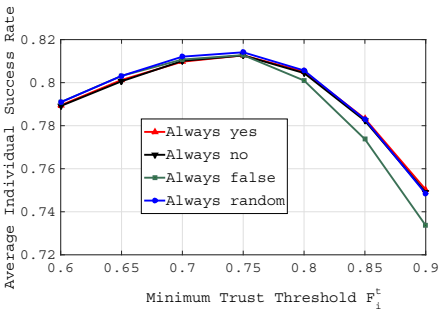

Figure 5: Impact of F_i^t.

the channel is free/not free opposite to what it senses), and always random (always saying the channel is free/not free randomly). Note that the analysis performed so far is for the case of "always false" SSDF attacks, which is the worst case among all.

Figure 4 shows the average individual success rate vs. T_i^t, with F_i^t=0.8 to isolate its effect. The figure is based on 20% malicious nodes. We observe that there exists an optimal T_i^t value under which the success rate is maximized. This is due to our data fusion rule design. Specifically, as the minimum capability threshold T_i^t increases, if SU i's true sensing capability is still above the increasing threshold, then its own sensing outcome is likely to be accurate, so the success decision rate will also increase. However, when T_i^t continues to increase, SU i's true sensing capability will more likely fall below the threshold. In this case, SU i cannot update the trust scores of other SUs effectively and must aggregate sensing outcomes from other SUs with inaccurate trust scores. As a result, the success decision rate decreases. This tradeoff results in the T_i^t optimal point.

Figure 5 shows the average individual success rate vs. F_i^t, with T_i^t=0.8. We observe that there exist an optimal F_i^t value under which the success rate is maximized. This is because as the minimum trust threshold F_i^t increases, there will be fewer sensing reports passing the threshold but the quality of information is better. This tradeoff results in the F_i^t optimal point.

The optimal T_i^t and F_i^t settings are sensitive to the percentage of malicious nodes (not reported here due to page limit). This result suggests adaptive control based on the percentage of malicious nodes sensed at runtime to maximize protocol performance.

VI. Conclusion

In this paper we proposed and analyzed a trust-based data fusion scheme for cooperative spectrum sensing in distributive cognitive radio networks to cope with data falsification attacks. We designed data fusion rules to distinguish erroneous reports due to low sensing capability from those due to malicious attacks. Our design effectively forces malicious nodes to report true sensing capability and outcome to prevent trust loss, thus allowing a high success rate to be achieved. We also identified optimal trust protocol settings under which the success rate is maximized. The simulation results validated the theoretical analysis and demonstrated that our trust-based data fusion scheme outperforms traditional data fusion rules and can distinguish malicious nodes performing data falsification attacks through their low trust scores in the long run.

In the future we plan to explore modeling techniques such as Stochastic Petri Nets [11]–[14] to model behaviors of benign and malicious SUs in order to study the interaction and exploit the design tradeoffs that exist in the game structure. We also plan to further test the resiliency of our trust-based data fusion scheme against more complicated environmental and operational scenarios such as different received signals at each node because of the geography effect of the SUs, as well as more sophisticated attack behaviors such as opportunistic, collusion, and insidious attacks [15], [16].

Acknowledgment

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

References

[1] L. Li, F.W. Li, and J. Zhu. "A method to defense against cooperative SSDF attacks in Cognitive Radio Networks." *IEEE Int. Conf. on Signal Processing, Commun. and Computing*, pp. 1-6, 2013.

[2] W. Wang, H. Li, Y. Sun, Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *43rd Annual Conference on Information Sciences and Systems,* 2009.

[3] J. Wang and I.R. Chen, "Trust-based Data Fusion Mechanism Design in Cognitive Radio Networks," *IEEE CNS Workshop on Cognitive Radio and Electromagnetic Spectrum Security*, 2014

[4] 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 Int. Symposium on Dynamic Spectrum Access Networks*, 2014.

[5] Q.B. Yan, M. Li, T. Jiang, W.J. Lou, and T. Hou. "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks." *IEEE INFOCOM*, pp. 900-908, 2012.

[6] C.L. Chen, M. Song, and C.S. Xin. "A density based scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks." *IEEE GLOBECOM*, pp.623-628, 2013.

[7] H. Tang, F.R. Yu, M. Huang, and Z. Li. "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks." *IET communications* vol. 6, no. 8, pp.974-983, 2012.

[8] 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.

[9] I.R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing*, 2016, in press.

[10] A. Goldsmith, Wireless Communications. *Cambridge University Press*, 2005.

[11] 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.

[12] I.R. Chen, T.M. Chen, and C. Lee, "Performance evaluation of forwarding strategies for location management in mobile networks," *The Computer Journal,* vol. 41, no. 4, 1998, pp. 243-253.

[13] I.R. Chen, O. Yilmaz, and I.L. Yen, "Admission control algorithms for revenue optimization with QoS guarantees in mobile wireless networks," *Wireless Personal Communications,* vol. 38, no. 3, pp. 357-376, 2006.

[14] S.T. Cheng, C.M. Chen, and I.R. Chen, "Performance evaluation of an admission control algorithm: dynamic threshold with negotiations," *Performance Evaluation*, vol. 52, no. 1, pp. 1-13, 2003.

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

[16] I.R. Chen, R. Mitchell, and J.H. Cho, "On Modeling of Adversary Behavior and Defense for Survivability of Military MANET Applications," *34th IEEE MILCOM*, 2015.