Exploiting Secure and Energy-Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks

Ju Ren, *Student Member, IEEE*, Yaoxue Zhang, Qiang Ye, *Student Member, IEEE*, Kan Yang, *Member, IEEE*, Kuan Zhang, *Student Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*— Cognitive radio sensor network (CRSN) has emerged as a promising solution to address the spectrum scarcity problem in traditional sensor networks, by enabling sensor nodes to opportunistically access licensed spectrum. To protect the transmission of primary users and enhance spectrum utilization, collaborative spectrum sensing is generally adopted for improving spectrum sensing accuracy. However, as sensor nodes may be compromised by adversaries, these nodes can send false sensing reports to mislead the spectrum sensing decision, making CRSNs vulnerable to spectrum sensing data falsification (SSDF) attacks. Meanwhile, since the energy consumption of spectrum sensing is considerable for energy-limited sensor nodes, SSDF attack countermeasures should be carefully devised with the consideration of energy efficiency. To this end, we propose a secure and energy-efficient collaborative spectrum sensing scheme to resist SSDF attacks and enhance the energy efficiency in CRSNs. Specifically, we theoretically analyze the impacts of two types of attacks, i.e., independent and collaborative SSDF attacks, on the accuracy of collaborative spectrum sensing in a probabilistic way. To maximize the energy efficiency of spectrum sensing, we calculate the minimum number of sensor nodes needed for spectrum sensing to guarantee the desired accuracy of sensing results. Moreover, a trust evaluation scheme, named FastDtec, is developed to evaluate the spectrum sensing behaviors and fast identify compromised nodes. Finally, a secure and energy-efficient collaborative spectrum sensing scheme is proposed to further improve the energy efficiency of collaborative spectrum sensing, by adaptively isolating the identified compromised nodes from spectrum sensing. Extensive simulation results demonstrate that our proposed scheme can resist SSDF attacks and significantly improve the energy efficiency of collaborative spectrum sensing.**

Manuscript received March 1, 2016; revised May 25, 2016; accepted June 26, 2016. Date of publication July 13, 2016; date of current version October 7, 2016. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada, in part by the China Hunan Provincial Science and Technology Program under Grant 2012GK4106, in part by the International Science and Technology Cooperation Program of China under Grant 2013DFB10070. The associate editor coordinating the review of this paper and approving it for publication was S. Wang. *(Corresponding author: K. Zhang.)*

J. Ren and Y. Zhang are with the School of Information Science and Engineering, Central South University, Changsha 410083, China (e-mail: renju@csu.edu.cn; zyx@csu.edu.cn).

Q. Ye, K. Yang, K. Zhang, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: q6ye@uwaterloo.ca; kan.yang@uwaterloo.ca; k52zhang@uwaterloo.ca; sshen@uwaterloo.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2016.2591006

***Index Terms*— Spectrum sensing data falsification (SSDF) attack, Byzantine attacks, collaborative spectrum sensing, energy efficiency, security, trust evaluation.**

I. Introduction

As THE explosion of wireless devices and services make the unlicensed spectrum increasingly crowded, traditional sensor networks operating on the unlicensed spectrum may suffer from severe interference caused by the nearby applications working on the same spectrum band. This situation is getting worse with our proceeding to the Internet-of-Things era. An example could be a monitoring sensor network application in a crowded area, e.g., shopping mall, where battery-powered sensor nodes are deployed to sense temperature or human traffic data and send it to the control center through wireless systems, e.g., ZigBee. Since many overlapping wireless applications exist in the mall, such as WiFi, ad hoc networks, operating over the same 2.4 GHz ISM band as ZigBee, they can cause significant and uncontrollable interference to sensor nodes, which may greatly impact the performance of data collection. By applying cognitive radio technology into sensor network, cognitive radio sensor network (CRSN) has emerged as a promising solution to address the interference problem caused by spectrum-scarcity [1]. Sensor nodes in a CRSN can sense the availability of licensed channels and access the idle channels for data transmission. However, due to channel fading and shadowing, spectrum sensing by individual sensor node has inevitable sensing errors, which adversely impact the performance of both the CRSN and the primary users (PUs) of the licensed channels.

To overcome the limitation of individual spectrum sensing, collaborative spectrum sensing is generally employed in CRSNs to improve the spectrum sensing accuracy [2]. However, since sensor nodes may be compromised by adversaries, these nodes can send false sensing results, making CRSNs vulnerable to spectrum sensing data falsification (SSDF) attack [3], [4]. In SSDF attacks, compromised nodes may operate independently or collaboratively to mislead the channel availability decision, which can significantly reduce spectrum utilization and degrade overall network performance [5]. To resist SSDF attacks, a number of countermeasures,

including trust/reputation based approaches [6]–[9], abnormal statistical-behavior detection based approaches [10]–[14] and clustering based approaches [15], [16], have been proposed in cognitive radio networks (CRNs), which could be applied into CRSNs. However, few related works consider energy efficiency in SSDF attack countermeasure design [17], [18].

The energy consumption in spectrum sensing is considerable for energy-sensitive sensor nodes [19], [20], comparing to that for mobile devices in CRNs. Particularly, in a poor radio environment, sensor nodes have to use a long sensing duration to detect the availability of licensed channels (i.e., PU signals) [21], which consequently increases the energy consumption in spectrum sensing. When collaborative spectrum sensing is adopted, the energy consumption would linearly increase with the number of sensor nodes participating in spectrum sensing [22]. If the number of spectrum sensing nodes can be reduced, the energy efficiency of collaborative spectrum sensing could be greatly improved. On the other hand, the number of spectrum sensing nodes and associated decision rule have significant impacts on the security of collaborative spectrum sensing [8]. Therefore, it is critical to study the minimum number of sensor nodes and optimal decision rule to optimize the energy efficiency under a desired security requirement.

In addition, in the presence of compromised nodes, how to design an evaluation/detection scheme that can quickly identify the compromised nodes with high accuracy becomes another key issue for securing collaborative spectrum sensing. Generally, compromised nodes can be identified with a higher accuracy during a longer evaluation period, since the historical records can provide more evidence for identification. Thus, a trade-off could be achieved between the speed and accuracy of the compromised nodes identification. Meanwhile, by isolating the identified compromised nodes from spectrum sensing, the evaluation scheme can be further exploited to adaptively reduce the number of spectrum sensing nodes, and hence to improve the energy efficiency of collaborative spectrum sensing.

In this paper, we propose a secure and energy-efficient collaborative spectrum sensing scheme to resist SSDF attacks and enhance the energy efficiency in CRSNs. Specifically, we focus on two types of SSDF attacks, i.e., independent and collaborative SSDF attacks, and analyze their impacts on the accuracy of collaborative spectrum sensing in a probabilistic way. Under both types of SSDF attacks, we derive the relationships between energy efficiency and security, respectively. Moreover, we develop a trust evaluation scheme with asymmetric rewarding and punishing mechanism to distinguish the compromised nodes and honest nodes. With the trust evaluation, compromised nodes can be accurately identified and isolated from collaborative spectrum sensing. As a consequence, the required number of spectrum sensing nodes can be adaptively reduced to meet the desired security requirement, leading to a further improvement of the energy efficiency. In summary, the main contributions of this paper are three-fold.

- We theoretically analyze the trade-off between energy efficiency and security, and determine the minimum number of spectrum sensing nodes and associated decision rule for collaborative spectrum sensing to guarantee a certain level of spectrum sensing accuracy under two types of SSDF attacks.
- We develop a trust evaluation scheme, FastDtec, to evaluate the spectrum sensing behaviors and identify the compromised nodes. Furthermore, we determine the optimal detection threshold for FastDtec, which can accelerate the identification of compromised nodes and maintain the probability of identifying a honest node as compromised below a certain probability.
- By isolating the identified compromised nodes from spectrum sensing, a secure and energy-efficient collaborative spectrum sensing scheme is further proposed to adaptively reduce the required number of spectrum sensing nodes, and hence to improve the energy efficiency of collaborative spectrum sensing.

The remainder of this paper is organized as follows. Section II reviews related works and Section III introduces the system model and design goals. We analyze the attack impacts and the trade-off between security and energy efficiency in Section IV, and then propose the FastDtec scheme in Section V. The secure and energy-efficient collaborative spectrum sensing scheme is detailed in Section VI. Simulation results are provided in Section VII to evaluate the performance of the proposed schemes. Finally, Section VIII concludes the paper and outlines our future work.

II. Related Works

With the rapid development of cognitive radio technology, increasing attention has been paid to securing spectrum sensing against SSDF attacks [2]. Most of the countermeasures in CRNs can be effectively applied to CRSNs which are special types of CRNs. Therefore, we briefly review some existing countermeasures in CRNs by dividing them into three main categories: trust/reputation based approaches, abnormal statistical-behavior detection based approaches, and clustering based approaches.

Trust and reputation based approaches are the most widely studied techniques in the literature [6]–[9]. The main idea of these approaches is to update the trust values of spectrum sensing nodes according to their historical sensing behaviors, and design weighted decision making strategies to resist SSDF attacks based on the evaluated trust values. Qin et al. [6] propose a trust-based model and design a weighted sensing result aggregation scheme to remove attackers from the decision making process. In [8], Rawat et al. analyze the performance limits of collaborative spectrum sensing under independent and collaborative SSDF attacks, respectively, and then propose a simple reputation-based scheme to resist SSDF attacks. They prove that, by employing the theory of Kullback-Leibler divergence metric, a certain fraction of attackers can make collaborative spectrum sensing no better than random guess. Another category of promising countermeasures is to identify SSDF attackers by detecting their abnormal statistical spectrum sensing behaviors [10]–[14]. From this perspective, two hidden Markov models (HMMs), with respect to honest and malicious users, are adopted in [10] to characterize

their different sensing behaviors. Attackers are identified by the difference in the corresponding HMM parameters. He et al. [12] use two conditional frequency check statistics to identify SSDF attackers based on the Markovian model of spectrum state. In addition, several recent research works focus on securing the collaborative spectrum sensing based on clustering the cooperating sensors [15], [16], [23]. Hyder et al. [16] develop a reputation-based clustering algorithm to divide nodes into a number of virtual clusters based on their evaluated reputation values. A bi-level voting strategy, consisting of intra-cluster and inter-cluster decision voting, is then proposed to make the final decision. There are also some works resisting SSDF attacks by using consensus-based approaches [24]–[26], radio propagation characteristics [27], data cleansing approaches [28], and incentive-based mechanisms [29].

Despite of their effectiveness in resisting SSDF attacks, most of existing works do not consider the energy efficiency of SSDF attack countermeasures [17], [18]. In a CRSN, sensor nodes have to consume considerable energy for collaborative spectrum sensing, which may degrade the energy efficiency of the network. However, if the unlicensed channel is facing significant interference when a CRSN starts to collect data, the performance of data collection would be hardly guaranteed by keeping working on the channel. It makes sensing and accessing a licensed channel as a necessary way to guarantee the network performance. Meanwhile, it also motivates us to carefully consider the energy efficiency in spectrum sensing and SSDF countermeasure design. Several recent works pay attention to the significance of energy efficiency in resisting SSDF attacks for CRNs. In [20], a low-overhead scheme is proposed for CRNs to address the always-1 SSDF attack under a trade-off between security and the energy efficiency of sensing report transmission. Recently, Mousavifar and Leung [18] develop a collaborative spectrum sensing scheme based on trust management to resist independent SSDF attacks in a CRN with a fixed number of compromised nodes and honest nodes. It is verified as effective to reduce the required sensing reports to achieve a targeted accuracy requirement. However, as more powerful SSDF attacks than independent SSDF attacks, collaborative SSDF attacks, where compromised nodes can collaboratively launch SSDF attacks, are not studied in both of the aforementioned works.

III. System Model and Design Goals

A. Network Model

Consider a CRSN application in a crowded area, where S cognitive sensor nodes are deployed to periodically transmit the sensed data, e.g., temperature or traffic information, to a sink node (or access point). The network operation can be divided into a sequence of time periods. There are also a number of overlapping wireless systems in this area, such as, WiFi and ad hoc networks, causing significant and uncontrollable interference over the unlicensed channel. To guarantee the performance of data transmission, the sink node coordinates sensor nodes to perform spectrum sensing over licensed channels and opportunistically access the idle ones for data transmission, when the unlicensed channel is suffering from significant interference. Since we aim to study the performance of spectrum sensing, we only focus on the time periods wherein spectrum sensing is required for licensed channel access. There are a number of orthogonal licensed channels owned by PUs in the primary network coexisting with the CRSN. At the beginning of each time period, a number of sensor nodes are randomly selected to sense the licensed channels and report their local binary decisions to the sink. Then, the sink makes global decisions based on the local reports and schedule sensor nodes to access the idle channels for data transmission.

We consider the radio environment in this area is poor, which causes that sensor nodes have to use a relatively long sensing duration to detect the availability of licensed channels (i.e., PU signals) within a required accuracy [21], [30]. It consequently increases the energy consumption for spectrum sensing. As all the sensor nodes are battery-powered, the energy-hungry spectrum sensing makes energy efficiency critical for the CRSN. Meanwhile, due to the lack of physical protection, sensor nodes may be compromised and manipulated by attackers to send false sensing results, with the purpose of misleading the global decisions. Wrong decisions can lead to interference with PUs or missing transmission opportunities, both of which may significantly degrade the performance of the CRSN. We consider the attacks to each channel sensing are homogeneous and independent [16], [17]. Such that, we can focus on securing the spectrum sensing over a specific licensed channel. To ease the presentation, the key notations are listed in Table I.

B. Channel Sensing Model and Decision Rule

Sensor nodes adopt a threshold-based energy detection approach for spectrum sensing [21], [31]. Due to channel fading and shadowing, there are unavoidable errors in individual channel sensing. We define *conditional false alarm probability* as the probability of an idle channel being detected as occupied, and *conditional missed detection probability* as the probability of an occupied channel being detected as idle. The two probabilities are predetermined and can be controlled by adjusting spectrum sensing parameters (e.g., sensing duration and energy detection threshold). For analysis simplification, we assume that all the sensor nodes have the same conditional false alarm probability P_{cf} and conditional missed detection probability P_{cm} [8], [16], which can be expressed as $P_{cf} = P(s_i = 1|\mathcal{H}_0)$, $P_{cm} = P(s_i = 0|\mathcal{H}_1)$, where s_i is the local sensing result of node i; $\mathcal{H}_0$ and $\mathcal{H}_1$ represent the hypotheses that the licensed channel is idle and occupied, respectively. According to the PU's temporal channel usage statistics, the probability of the channel being idle (i.e., $P(\mathcal{H}_0)$) and the probability of the channel being occupied (i.e., $P(\mathcal{H}_1)$) are P_0 and P_1.

To enhance the accuracy of sensing results, collaborative spectrum sensing is recommended to detect the availability of the licensed channel. Let $\mathcal{N} = \{1, \ldots, N\}$ be the set of spectrum sensing nodes that are selected to sense the licensed channel. At the beginning of each time period, each node $i \in \mathcal{N}$

TABLE I
THE KEY NOTATIONS

Notation	Definition
S, N, K	Number of sensor nodes, spectrum sensing nodes and compromised spectrum sensing nodes
$\mathcal{H}_1$, $\mathcal{H}_0$	Hypotheses of licensed channel busy and idle
s_i, r_i	Local sensing and reporting results of node i
P_1, P_0	Probabilities of channel busy and idle
P_{cf}, P_{cm}	Conditional FAP and MDP of a sensor node
L, $\mathcal{D}$	Decision rule, global decision
α, α'	Percentage of compromised nodes, updated α after identification
$P_{a,0}$, $P_{a,1}$	attacking probabilities of I-SSDF attackers
$P_{a,c}$, R	attacking probability of C-SSDF attackers, consistent decision of C-SSDF attackers
P_{cf}^I, P_{cm}^I	Conditional FAP and MDP of I-SSDF attacker
P_{cf}^C, P_{cm}^C	Conditional FAP and MDP of C-SSDF attacker
P_F^I, P_M^I	FAP and MDP under I-SSDF attack
P_F^C, P_M^C	FAP and MDP under C-SSDF attack
δ_F, δ_M	Desired FAP and MDP requirements
N_{min}^I, N_{min}^C	Minimum number of required spectrum sensing nodes under I-SSDF and C-SSDF attacks
L^I, L^C	Decision rules associated with N_{min}^I and N_{min}^C
P_e^H, P_e^I, P_e^C	Reporting error probabilities of honest nodes, I-SSDF attackers and C-SSDF attackers
v_i, V_i	Trust score and trust value of node i
V_{min}, V_{max}	Minimum and maximum trust value of FastDtec
V_0, σ	Initial trust value of FastDtec, actual channel availability information
T, ξ	Number of evaluation periods, identification threshold of FastDtec
T_{min}, T_{max}	Minimum and maximum evaluation periods
$\xi^*(T)$, φ	Optimal ξ for T-th evaluation period, desired false identification probability of FastDtec

detects the PU presence independently and reports its binary decision to the sink. The sink adopts a general "L out of N" rule to determine the global decision based on the received N reports. If we use r_i as the binary decision report of $i \in \mathcal{N}$, the global decision $\mathcal{D}$ can be calculated as

$$\mathcal{D} = \begin{cases} \mathcal{H}_1, & \text{if } \sum_{i=1}^{N} r_i \geq L; \\ \mathcal{H}_0, & \text{otherwise.} \end{cases} \quad (1)$$

Apparently, the decision rule dpends on L. For example, when $L = 1$, the decision rule is *OR* rule; when $L = N$, it refers to the *AND* rule; when $L = \lfloor N/2 \rfloor + 1$, it represents the *Majority Voting* rule. Since the decision rule directly impacts the accuracy of the global decision, the general rule is flexible to different system requirements. Note that, since compromised nodes may report false sensing results to the sink, s_i and r_i could be different when node i is a compromised node. In addition, the CRSN (or the sink) can obtain the actual availability information of the licensed channel during a time period at the end of this time period [16], [18] (e.g., by communicating with the PU base station or monitoring the signal/interference over the licensed channel during the whole time period).

C. Attack Model

A portion of sensor nodes may be compromised and manipulated to launch spectrum sensing data falsification (SSDF) attacks in the CRSN. In such attacks, these compromised nodes can independently or collaboratively send false spectrum sensing results to mislead the global decision of collaborative spectrum sensing. Let α be the percentage of compromised sensor nodes in the CRSN. Here, we do not consider the case with $\alpha > 50\%$, because it is costly to maintain a network with a majority of nodes being attackers [16]. Let K be the number of compromised nodes chosen for spectrum sensing, then we have $K \leq N$. For each honest node i, it reports the actual sensing result to the sink, i.e., $r_i = s_i$. Comparatively, the compromised sensor nodes can launch SSDF attacks to change their reports independently or collaboratively. Specifically, we present two types of SSDF attacks as follows.

1) Independent SSDF (I-SSDF) Attack: Independent SSDF attack refers to that each compromised node independently changes its sensing result with specific probabilities. For each compromised node i, we can define two attacking probabilities, $P_{a,0}$ and $P_{a,1}$, as

$$\begin{cases} P(r_i = 1|s_i = 0) = P_{a,0}, & P(r_i = 0|s_i = 0) = 1 - P_{a,0}, \\ P(r_i = 0|s_i = 1) = P_{a,1}, & P(r_i = 1|s_i = 1) = 1 - P_{a,1}. \end{cases}$$

We assume that each compromised node has the same attacking probabilities $P_{a,0}$ and $P_{a,1}$ [8], [16]. However, our analytical results can be extended to the case where compromised nodes have different probabilities. Given $P_{a,0}$ and $P_{a,1}$, for each compromised node i, the conditional false alarm probability P_{cf}^I and missed detection probability P_{cm}^I are

$$\begin{aligned} P_{cf}^I &= P(r_i = 1|s_i = 1)P(s_i = 1|\mathcal{H}_0) \\ &\quad + P(r_i = 1|s_i = 0)P(s_i = 0|\mathcal{H}_0) \\ &= (1 - P_{a,1})P_{cf} + P_{a,0}(1 - P_{cf}) \\ P_{cm}^I &= P(r_i = 0|s_i = 0)P(s_i = 0|\mathcal{H}_1) \\ &\quad + P(r_i = 0|s_i = 1)P(s_i = 1|\mathcal{H}_1) \\ &= (1 - P_{a,0})P_{cm} + P_{a,1}(1 - P_{cm}) \end{aligned} \quad (2)$$

2) Collaborative SSDF (C-SSDF) Attack: In C-SSDF attack, compromised nodes can collaboratively send false sensing results to mislead the global decision, when they are selected for spectrum sensing. In specific, they can first exchange their sensing results and collaboratively make a consistent decision about the availability of the licensed channel. Then, the compromised nodes send reports opposite to the consistent decision to the sink. The consistent decision of compromised nodes is made by the majority voting rule [8], [16]. Let R be the consistent decision and $P_{a,c}$ be the probability that compromised nodes collaboratively launch attacks. Once the compromised nodes decide to attack, they collaboratively decide R and report $r_i = \bar{R}$ to the

sink. Otherwise, the compromised nodes will report the original sensing results $r_i = s_i$ to the sink. Here, $\bar{R}$ is the opposite of R. Therefore, for each compromised node i, the conditional false alarm probability P_{cf}^C consists of two parts. The first is the conditional false alarm probability of node i, when the compromised nodes do not launch C-SSDF attacks. That is $P_{cf}(1 - P_{a,c})$. The second part is the conditional false alarm probability of node i, when the compromised nodes launch C-SSDF attacks. In such case, we have $R = 0$, which means that there are at least $M = \lfloor K/2 \rfloor + 1$ compromised nodes with $s_i = 0$. Since local sensing is independent among all the nodes, we have the probability of M compromised nodes with $s_i = 0$ is $\binom{K}{M}(1 - P_{cf})^M (P_{cf})^{K-M}$. Thus, we can calculate the second part as $\sum_{i=M}^{K} (1 - P_{cf})^M (P_{cf})^{K-M} \cdot P_{a,c}$. Similarly, we can calculate the conditional missed detection probability P_{cm}^C. In summary, for each compromised node i under C-SSDF attacks, we have

$$\begin{cases} P_{cf}^C = P_{cf}(1 - P_{a,c}) + \sum_{i=M}^{K} Q\Big(K, i, 1 - P_{cf}\Big) P_{a,c} \\ P_{cm}^C = P_{cm}(1 - P_{a,c}) + \sum_{i=M}^{K} Q\Big(K, i, 1 - P_{cm}\Big) P_{a,c} \end{cases} \tag{3}$$

where $Q(K, i, p) = \binom{K}{i} p^i \ (1 - p)^{K-i}$ and $M = \lfloor K/2 \rfloor + 1$.

The sink, which is highly protected, is assumed not to be compromised by attackers. Moreover, we consider that cryptographic techniques are applied into the communication of the CRSN, such that the compromised nodes cannot obtain the reported sensing results of honest sensor nodes and decide their attack plans (i.e., sensing report r_i) accordingly [16].

D. Energy Consumption Model

In CRSNs, sensor nodes consume energy in data transmission and reception, spectrum sensing and idle listening. However, since we focus on investigating the energy efficiency of spectrum sensing, the discussion of the energy consumption in data transmission and reception, as well as idle listening, is out of the scope of this paper. The energy consumption of spectrum sensing consists of two parts, energy consumption in sensing the spectrum and sensing results transmission. Since we use a binary local decision result in our spectrum sensing, the energy consumption of transmitting the sensing results is very small and can be ignored, compared to the energy consumption of spectrum sensing [22]. When collaborative spectrum sensing is adopted, the energy consumption of spectrum sensing becomes considerable for the CRSN [20]. According to [22], the total energy consumption of spectrum sensing can be simply calculated as

$$E = \sum_{i \in \mathcal{N}} e_i \cdot t_i, \tag{4}$$

where $\mathcal{N}$ is the set of spectrum sensing nodes; for each node i, e_i is the energy consumption rate of spectrum sensing and t_i is the sensing duration. To guarantee the required local sensing accuracy, i.e., P_{cf} and P_{cm}, e_i and t_i may be slightly different for each $i \in \mathcal{N}$, due to the spatially varied radio environment. However, the total energy consumption of spectrum sensing would still linearly increase with the number of spectrum sensing nodes, which indicates the energy efficiency can be significantly enhanced by reducing N [20], [32].

E. Design Goals

The first objective is to defend collaborative spectrum sensing against SSDF attacks. Since SSDF attacks aim to mislead the global decision $\mathcal{D}$ made by the sink, the security level of resisting SSDF attacks can be measured by the accuracy of $\mathcal{D}$. Specifically, we define the *false alarm probability* (FAP) $P_F = P(\mathcal{D} = 1|\mathcal{H}_0) \cdot P(\mathcal{H}_0)$ and the *missed detection probability* (MDP) $P_M = P(\mathcal{D} = 0|\mathcal{H}_1) \cdot P(\mathcal{H}_1)$ as security level indicators. Let δ_F and δ_M be the required security levels, then we should guarantee

$$\begin{cases} P_F = P(\mathcal{D} = 1|\mathcal{H}_0) \cdot P_0 \le \delta_F \\ P_M = P(\mathcal{D} = 0|\mathcal{H}_1) \cdot P_1 \le \delta_M \end{cases} \tag{5}$$

The second objective is to optimize the energy efficiency of collaborative spectrum sensing under the security requirements. According to the decision rule, the number of spectrum sensing nodes N and the value of L can remarkably impact the global decision accuracy, i.e., P_F and P_M. On the other hand, the energy consumption model indicates that the energy efficiency can be improved by reducing the number of spectrum sensing nodes. Therefore, for a given α, we aim to determine N_{min}^I and N_{min}^C, which denote the minimum number of spectrum sensor nodes to resist I-SSDF and C-SSDF attacks respectively, as well as appropriate L^I and L^C denoting the corresponding decision rules, to satisfy the security requirement, i.e., Eq. (5).

Moreover, we aim to evaluate the spectrum sensing behaviors and identify the compromised nodes by developing a trust evaluation scheme. The trust evaluation scheme should be able to identify the compromised nodes with a high speed and accuracy. In addition, how to utilize the trust evaluation scheme to further reduce the number of required spectrum sensing nodes should be investigated for improving the energy efficiency of collaborative spectrum sensing.

IV. Analysis on Attack Impact and Trade-Off Between Security and Energy Efficiency

In this section, we study the impact of SSDF attacks on the global decision accuracy and propose an algorithm to determine the minimum N_{min}^I, N_{min}^C, and appropriate L^I, L^C, to satisfy the desired security requirements.

A. Detection Accuracy Analysis Under SSDF Attacks

We first analyze the global detection accuracy under the two types of SSDF attacks, respectively. The analysis and corresponding results are presented by the following lemmas and propositions.

Lemma 1: Given K, N and L, the FAP $P^I_{F,K}$ and MDP $P^I_{M,K}$ under I-SSDF attacks are

$$\begin{cases} P^I_{F,K} = \left(\sum_{i=0}^{N-K} \left[Q(N-K,i,P_{cf}) \sum_{j=L-i}^{K} Q(K,j,P^I_{cf}) \right] \right) P_0, \\ P^I_{M,K} = \left(\sum_{i=0}^{N-K} \left[Q(N-K,i,P_{cm}) \times \sum_{j=N-L-i+1}^{K} Q(K,j,P^I_{cm}) \right] \right) P_1, \end{cases} \tag{6}$$

where we define that $\sum_{i=a}^{b} Q(b,i,p) = 1$, if $a \le 0$; and $\sum_{i=a}^{b} Q(b,i,p) = 0$, if $a > b$.

Proof: We first calculate the false alarm probability. Let X be the number of honest nodes reporting channel being occupied (i.e., $r_i = 1$), and Y be the number of compromised nodes reporting channel being occupied. Therefore, we have $P^I_{F,K} = P(X+Y \ge L|\mathcal{H}_0) \cdot P(\mathcal{H}_0)$. Since all the honest nodes and the compromised nodes are independent, X should follow a binomial distribution $X \sim B(N-K, P_{cf})$, while Y follows a binomial distribution $Y \sim B(K, P^I_{cf})$. Then, we have

$$\begin{aligned} & P^I_{F,K} \\ &= P(X+Y \ge L|\mathcal{H}_0) \cdot P(\mathcal{H}_0) \\ &= \left(\sum_{i=0}^{N-K} \left[P(X=i|\mathcal{H}_0) \sum_{j=L-i}^{K} P(Y=j|\mathcal{H}_0) \right] \right) P_0 \\ &= \left(\sum_{i=0}^{N-K} \left[Q(N-K,i,P_{cf}) \sum_{j=N-L-i+1}^{K} Q(K,j,P^I_{cf}) \right] \right) P_0. \end{aligned}$$

To ensure the equation suitable for different K and L, we define that $\sum_{i=a}^{b} Q(b,i,p) = 1$, if $a \le 0$; and $\sum_{i=a}^{b} Q(b,i,p) = 0$, if $a > b$. Similarly, we can calculate $P^I_{M,K}$ as shown in Eq. (6), which completes the proof. ∎

Lemma 2: Given K, N and L, the FAP $P^C_{F,K}$ and MDP $P^C_{M,K}$ under C-SSDF attacks are

$$\begin{cases} P^C_{F,K} = \left(\sum_{i=0}^{N-K} \left[Q(N-K,i,P_{cf}) \sum_{j=L-i}^{K} P(Y=j|\mathcal{H}_0) \right] \right) P_0, \\ P^C_{M,K} = \left(\sum_{i=0}^{N-K} \left[Q(N-K,i,P_{cm}) \times \sum_{j=N-L-i+1}^{K} P(Z=j|\mathcal{H}_1) \right] \right) P_1, \end{cases} \tag{7}$$

where $P(Y=j|\mathcal{H}_0)$ can be obtained by Eq. (8) and $P(Z=j|\mathcal{H}_1)$ can be obtained by the equation replacing P_{cf} in Eq. (8) with P_{cm}.

Proof: We prove this lemma with the procedures similar to Lemma 1. Denote X and Y as the number of honest nodes and compromised nodes that report channel being occupied, respectively. Under C-SSDF attacks, X still follows a binomial distribution $X \sim B(N-K, P_{cf})$ but the distribution of Y changes. If compromised nodes do not launch attacks, Y follows a binomial distribution $Y \sim B(K, P_{cf})$, where $0 \le Y \le K$; otherwise, Y can only be 0 (i.e., when $R=1$) or K (i.e., when $R=0$). Therefore, we discuss the probability distribution of Y under $\mathcal{H}_0$ from the following three cases.

(1) $Y = 0$. This case can be further divided into two cases. One is when no C-SSDF attack happens in spectrum sensing, we have $P(Y=0|\mathcal{H}_0) = Q(K,0,P_{cf})$. The other is when C-SSDF attack happens, there should be at least M compromised nodes with $s_i = 1$. In such case, we have $P(Y=0|\mathcal{H}_0) = \sum_{z=M}^{K} Q(K,z,P_{cf})$. Thus, according to the law of total probability, we have $P(Y=0|\mathcal{H}_0) = (1-P_{a,c})\, Q(K,0,P_{cf}) + \sum_{z=M}^{K} Q(K,z,P_{cf}) P_{a,c}$.

(2) $1 \le Y \le K$. It only happens under the condition of no C-SSDF attack in spectrum sensing. We can calculate the probability distribution as $P(Y=j|\mathcal{H}_0) = Q(K,0,P_{cf})$, $\forall 1 \le j < K$.

(3) $Y = K$. This case can also be further divided into two cases. According to the analysis in (1), we have $P(Y=K|\mathcal{H}_0) = (1-P_{a,c}) Q(K,K,P_{cf}) + \sum_{z=M}^{K} Q(K,z,1-P_{cf}) P_{a,c}$.

In summary, we can write the probability distribution of Y under $\mathcal{H}_0$ as

$$\begin{aligned} & P(Y=j|\mathcal{H}_0) \\ &= \begin{cases} (1-P_{a,c}) Q\Big(K,0,P_{cf}\Big) + \sum_{z=M}^{K} Q\Big(K,z,P_{cf}\Big) P_{a,c}, & \text{if } j=0; \\ (1-P_{a,c}) Q\Big(K,j,P_{cf}\Big), & \text{if } 1 \le j < K; \\ (1-P_{a,c}) Q\Big(K,K,P_{cf}\Big) + \sum_{z=M}^{K} Q\Big(K,z,1-P_{cf}\Big) P_{a,c}, & \text{if } j=K. \end{cases} \end{aligned} \tag{8}$$

Since X and Y are two independent variables, $P^C_{F,K}$ can be calculated as

$$\begin{aligned} P^C_{F,K} &= P(X+Y \ge L|\mathcal{H}_0) \cdot P(\mathcal{H}_0) \\ &= \Big[P(X=0, Y \ge L|\mathcal{H}_0) + \ldots \\ &\quad + P(X=N-K, Y \ge L-N+K|\mathcal{H}_0) \Big] \cdot P(\mathcal{H}_0) \\ &= \Big[P(X=0|\mathcal{H}_0) P(Y \ge L|\mathcal{H}_0) + \ldots \\ &\quad + P(X=N-K|\mathcal{H}_0) P(Y \ge L-N+K|\mathcal{H}_0) \Big] \\ &\quad \cdot P(\mathcal{H}_0) \\ &= \sum_{i=0}^{N-K} \left(Q(N-K,i,P_{cf}) \sum_{j=L-i}^{K} P(Y=j|\mathcal{H}_0) \right) P_0, \end{aligned}$$

where $P(Y=j|\mathcal{H}_0)$ can be obtained by Eq. (8). Accordingly, $P^C_{M,K}$ can be calculated in the same way, which completes the proof. ∎

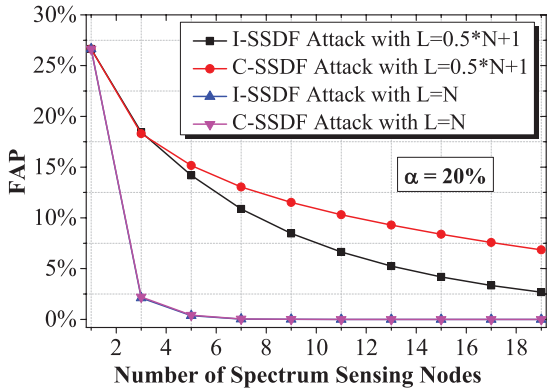


Fig. 1. FAP comparison under different N and L.

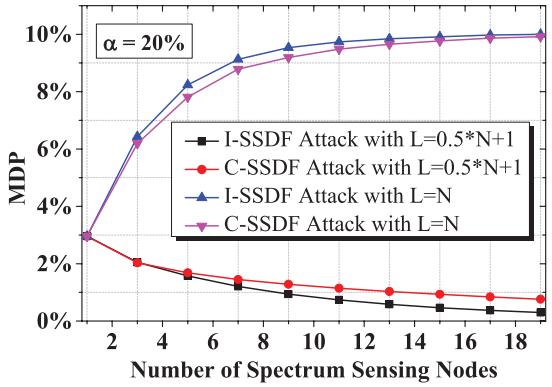


Fig. 2. MDP comparison under different N and L.

With Lemma 1 and 2, we can calculate the security levels under two types of SSDF attacks with given K, N and L. However, K is a random variable following a binomial distribution $K \sim (N, \alpha)$. The following proposition analyzes the FAP and MDP under given α.

Proposition 1: Given α, if N sensor nodes are randomly selected for spectrum sensing, the FAP P_F^I and MDP P_M^I under I-SSDF attacks are

$$P_F^I = \sum_{K'=0}^{N} Q\Big(N, K', \alpha\Big) P_{F,K'}^I,$$
$$P_M^I = \sum_{K'=0}^{N} Q\Big(N, K', \alpha\Big) P_{M,K'}^I, \tag{9}$$

while the FAP P_F^C and MDP P_M^C under C-SSDF attacks are

$$P_F^C = \sum_{K'=0}^{N} Q\Big(N, K', \alpha\Big) P_{F,K'}^C,$$
$$P_M^C = \sum_{K'=0}^{N} Q\Big(N, K', \alpha\Big) P_{M,K'}^C. \tag{10}$$

Proof: Since N sensor nodes are randomly selected for spectrum sensing, the probability that K' out of N sensor nodes are compromised is $Q(N, K', \alpha)$. As a result, the FAP P_F^I and MDP P_M^I under I-SSDF attacks are $P_F^I = \sum_{K'=0}^{N} Q(N, K', \alpha) P_{F,K'}^I$ and $P_M^I = \sum_{K'=0}^{N} Q(N, K', \alpha) P_{M,K'}^I$. Similarly, the FAP P_F^C and MDP P_M^C under C-SSDF attacks can be derived as Eq. (10). ■

B. Trade-Off Between Security and Energy Efficiency

Based on the analysis in the previous subsection, we can see that N and L directly determine the security level, and the corresponding relationship is presented by Eq. (9) and (10).

Fig. 1 and 2 show the FAPs and MDPs under different N and L, where the percentage of compromised nodes is $\alpha = 20\%$, $P_0 = 90\%$, $P_1 = 10\%$, $P_{cf} = P_{cm} = 20\%$, $P_{a,0} = P_{a,1} = P_{a,c} = 80\%$ and $S = 20$. From these figures, it can be seen that the number of spectrum sensing nodes N and the decision rule L can significantly impact the security levels, under both types of attacks. When $L = \lfloor N/2 \rfloor + 1$, the increasing N leads to decreasing FAP and MDP under both types of SSDF attacks. However, MDP increases with the increasing N when $L = N$. This is because MDPs can be calculated as $P_M^I = (1 - (1 - P_{cm}^I)^N) \cdot P_1$, $P_M^C = (1 - (1 - P_{cm}^C)^N) \cdot P_1$ when $L = N$. Both of P_M^I and P_M^C are monotone increasing functions with N. Moreover, for a fixed N, different decision rules (i.e., different values of L) can bring different security levels. Specifically, a larger L produces lower FAPs but higher MDPs under both types of SSDF attacks.

Since we aim to optimize the energy efficiency under a fixed security level, the problem can be formulated as an integer programming problem. Given α, δ_F and δ_M, to resist I-SSDF attacks, we aim to determine the minimum N_{min}^I and L^I to satisfy

$$P_F^I \le \delta_F, \ P_M^I \le \delta_M, \quad 1 \le N_{min}^I \le S, \ 1 \le L^I \le N, \tag{11}$$

while to resist C-SSDF attacks, it changes to determine the minimum N_{min}^C and L^C to satisfy

$$P_F^C \le \delta_F, \ P_M^C \le \delta_M, \quad 1 \le N_{min}^C \le S, \ 1 \le L^C \le N. \tag{12}$$

Obviously, the searching space of the above integer programming problems is $(1 + S)S/2$. It means that brute-force algorithm can be adopted to find the optimal solutions with computation complexity $O(S^2)$. The main idea is to search each pair of N and L to find the minimum N_{min}^I and N_{min}^C, as well as the corresponding L^I and L^C, for satisfy Eq. (11) and (12), respectively.

V. FastDtec: Trust Evaluation for Fast Compromised Node Detection

In this section, we develop a trust evaluation scheme, named FastDtec, to evaluate the periodical spectrum sensing behaviors and fast identify the compromised nodes.

A. Trust Evaluation Design

According to the system model, the CRSN can obtain the actual availability of the licensed channel during each time period. As a result, the actual information, denoted by a binary variable σ, can be used to evaluate the behaviors of spectrum

sensing nodes at the end of this time period. To this end, we propose FastDtec to evaluate the reported sensing results of spectrum sensing nodes by dynamically updating their trust values. Specifically, in FastDtec, the sink maintains a trust table to record the trust values of sensor nodes, and updates the trust table at the end of each time period according to the reported sensing results. For each spectrum sensing node $i \in \mathcal{N}$, if $r_i = \sigma$, node i should be rewarded a trust increment; otherwise, it should face a trust punishment. When the trust value of a sensor node decreases below a certain threshold, this node would be identified as a compromised node by FastDtec.

In order to reduce the trust values of compromised nodes and identify them in a small number of evaluation periods, the punishment should be defined heavy enough. However, since honest nodes may be punished with a certain probability due to the imperfect spectrum sensing, a large punishment could make the trust values of honest nodes drop quickly. Therefore, the evaluated trust score should be carefully determined to protect the honest nodes and punish the compromised nodes. Let P_e be the sensing error probability of node i in spectrum sensing. Then,

$$\begin{cases} P_e = P_e^H = P_{cf} P_0 + P_{cm} P_1, & \text{if } i \text{ is honest;} \\ P_e = P_e^I = P_{cf}^I P_0 + P_{cm}^I P_1, & \text{if } i \text{ is I-SSDF attacker.} \end{cases} \tag{13}$$

When node i is a C-SSDF attacker,

$$P_e = P_e^C = \sum_{k=0}^{N} Q\Big(N, k, \alpha\Big) \cdot \Big(P_{cf}^C P_0 + P_{cm}^C P_1\Big). \tag{14}$$

Based on Eq. (13) and (14), FastDtec evaluates a trust score v_i for a spectrum sensing node i, which is defined as

$$v_i = \begin{cases} 1, & \text{if } r_i = \sigma; \\ -(1 - P_e^H)/P_e^H, & \text{if } r_i \neq \sigma. \end{cases} \tag{15}$$

Here, we use a unit score as the reward and a well-chosen punishment for a correct and a wrong spectrum sensing result, respectively. The asymmetrical trust evaluation can keep the trust value of a honest node stable but efficiently reduce the trust value of a compromised node [18], which can be proved by the following Lemma 3. Meanwhile, FastDtec updates the trust table based on the evaluated trust score as follows

$$V_i = \min\{\max\{V_i + v_i, V_{min}\}, V_{max}\}, \tag{16}$$

where V_{min} and V_{max} are the minimum and maximum trust values in FastDtec, respectively.

Let V_0 be the initial trust value of sensor nodes. The expected trust values of a honest node and a compromised node can be obtained according to Lemma 3.

Lemma 3: In FastDtec, if node i is selected for spectrum sensing T times, its expected trust value $\mathbb{E}(V_i)$ is

$$\mathbb{E}(V_i) = \begin{cases} V_0, & \textit{if } i \textit{ is honest}; \\ V_0 - \dfrac{P_e^I - P_e^H}{P_e^H} \cdot T, & \textit{if } i \textit{ is I-SSDF attacker}; \\ V_0 - \dfrac{P_e^C - P_e^H}{P_e^H} \cdot T, & \textit{if } i \textit{ is C-SSDF attacker}. \end{cases} \tag{17}$$

Proof: Let X be the number of the wrong sensing reports of node i. Since each spectrum sensing is independent for node i, X is a random variable following a binomial distribution as $X \sim B(T, P_e)$, where P_e is the sensing error probability of node i shown in Eq. (13) and (14). Therefore, the expected trust value of node i after T times of trust evaluation is

$$\begin{aligned} \mathbb{E}(V_i) &= V_0 + T - \mathbb{E}(X) - \mathbb{E}(X) \cdot \frac{1 - P_e^H}{P_e^H} \\ &= V_0 + \frac{P_e - P_e^H}{P_e^H} \cdot T. \end{aligned} \tag{18}$$

By substituting P_e according to Eq. (13) and (14), the lemma can be proved. ■

Note that, to reduce the decision accuracy of collaborative spectrum sensing, a compromised node should have a larger sensing error probability than a honest node, i.e., $P_e^I > P_e^H$ and $P_e^C > P_e^H$. It also indicates that FastDtec can keep the trust values of honest nodes stable but decrease the trust values of compromised nodes linearly with the spectrum sensing times.

B. Optimal Detection Threshold for Compromised Node Identification

To identify the compromised nodes, FastDtec defines a detection threshold for the trust values of sensor nodes. Once the trust value of a sensor node is below the detection threshold, the node is identified as compromised. Intuitively, if the threshold is defined as a large value (close to V_0), the compromised nodes can be identified quickly. However, a large threshold may increase the probability of detecting a honest node as compromised at the same time. Therefore, there exists a trade-off between the detection speed and accuracy in compromised node identification. In this subsection, we determine the optimal detection threshold for FastDtec to accelerate the identification of compromised nodes while keeping the detection accuracy at a controllable level.

Let ξ be the detection threshold of FastDtec. Lemma 4 provides the probability of a honest node being identified as compromised based on ξ.

Lemma 4: Given ξ, if node i is honest and chosen for spectrum sensing T times, the probability that node i is identified as compromised by FastDtec is

$$FP(\xi, T) = \sum_{k=\lceil f(\xi,T) \rceil}^{T} Q(T, k, P_e^H), \tag{19}$$

where $f(\xi, T)$ is

$$f(\xi, T) = P_e^H \cdot (V_0 + T - \xi). \tag{20}$$

Proof: Let X be the number of the wrong sensing reports of node i, then we have $X \sim B(T, P_e^H)$. After T times of spectrum sensing, node i's trust value is $V_i = V_0 + (T - X) - X \cdot \dfrac{1 - P_e^H}{P_e^H}$. If node i is identified as compromised, it means $V_i \leq \xi$. Substituting V_i, we have $X \geq P_e^H \cdot (V_0 + T - \xi)$. Since $X \sim B(T, P_e^H)$, the probability that

node i is identified as compromised is $FP(\xi, T) = P\{X \geq f(\xi, T)\} = \sum_{k=\lceil f(\xi,T)\rceil}^{T} Q(T, k, P_e^H)$, where $f(\xi, T) = P_e^H \cdot (V_0 + T - \xi)$. ■

To guarantee the detection accuracy of FastDtec, we introduce an accuracy requirement φ $(0 < \varphi < 1)$, which requires $FP(\xi, T) \leq \varphi$. Therefore, the optimal detection threshold ξ^* that can be used to identify compromised nodes quickly should be the maximum value satisfying $FP(\xi^*, T) \leq \varphi$ for each $T \in \{1, \ldots, +\infty\}$. It also indicates that the optimal threshold ξ^* varies with the value of T. We use $\xi^*(T)$ to denote the optimal threshold for given T, then $\xi^*(T)$ should adaptively change with the increment of T. Unfortunately, according to Eq. (19), there is no closed-form expression that can describe the relationship between $\xi^*(T)$ and T.

To determine $\xi^*(T)$, we first introduce a numerical procedure, which can be applied to the case when T is bounded as a relatively small value. Let X be a binomial random variable to denote the number of wrong sensing reports, then $X \sim B(T, P_e^H)$. To meet the detection accuracy requirement, we have $P(X \geq f(\xi^*(T), T)) \leq \varphi$, where $f(\xi^*(T), T)$ is shown in Eq. (20). For given T, $f(\xi, T)$ is a linearly decreasing function with respect to ξ, which means the minimum $f(\xi, T)$ corresponding to the optimal $\xi^*(T)$. Actually, the minimum $f(\xi, T)$ to satisfy $P(X \leq f(\xi, T)) \geq 1 - \varphi$ is known as the upper tolerance limit for the binomial distribution $B(T, P_e^H)$ with tolerance requirement $1 - \varphi$ [33], [34]. The upper tolerance limit can be derived as follows. We first compute right-tail probabilities $P(X = T)$, $P(X = T - 1)$, …, until the sum of these probabilities is greater than or equal to φ. If this happens at $X = T - l$, that is, $\sum_{k=T-l}^{T} P(X = k) \geq \varphi$ and $\sum_{k=T-l+1}^{T} P(X = k) < \varphi$, then $T - l$ is the required upper tolerance limit. Let $f(\xi^*(T), T) = T - l$ and substitute $f(\xi^*(T), T)$ according to Eq. (20), we have $\xi^*(T) = V_0 + T - \dfrac{T - l}{P_e^H}$. On the other hand, if there is no such upper tolerance limit that can make $P(X \leq f(\xi, T)) \geq 1 - \varphi$, it can be claimed that T is not large enough for compromised node identification. We use T_{min} to denote the minimum T that can make $P(X = T) = (P_e^H)^T \leq \varphi$. Due to $P_e^H < 1$, we have $T \geq \log_{P_e^H} \varphi$. Thus,

$$T_{min} = \log_{P_e^H} \varphi = \log_2 \varphi / \log_2 P_e^H. \tag{21}$$

Only if $T \geq T_{min}$, we could find an upper tolerance limit and the optimal $\xi^*(T)$, which can be derived by the numerical procedure.

The above numerical procedure can determine $\xi^*(T)$ for given T, however, it is not applicable and efficient when T is large enough, due to the high computation complexity of combinatorial number. We use T_{sw} to denote the value of T which makes a sensor node unable to afford the computation burden of the numerical procedure. To determine $\xi^*(T)$ for $T > T_{sw}$, Proposition 2 provides an approximation solution.

Proposition 2: To guarantee that the probability of a honest node being identified as compromised by FastDtec is no larger than φ, the approximate optimal detection threshold $\xi^*(T)$, when $T_{sw} < T \leq T_{max}$, , is

$$\begin{cases} \xi^*(T) \approx V_0 - \dfrac{z_{1-\varphi}\sqrt{T P_e^H (1 - P_e^H)}}{P_e^H}, \\ T_{max} = \left\lfloor \dfrac{(V_0 - V_{min})^2 \cdot P_e^H}{1 - P_e^H} \right\rfloor. \end{cases} \tag{22}$$

where $z_{1-\varphi}$ is $1 - \varphi$ quantile of standard normal distribution, V_{min} is the minimum trust value.

Proof: Let X be the number of wrong sensing reports with $X \sim B(T, P_e^H)$. When $T \geq 20$, the binomial distribution $B(T, P_e^H)$ can be approximated as a normal distribution [33], [34], i.e., $X \sim N(T P_e^H, T P_e^H (1 - P_e^H))$. On the basis of the normal approximation to the quantity $\dfrac{X - T P_e^H}{\sqrt{T P_e^H (1 - P_e^H)}}$, the $1 - \varphi$ quantile of $B(T, P_e^H)$, denoted by $L(T, P_e^H, 1 - \varphi)$, is given as

$$L(T, P_e^H, 1 - \varphi) \approx T P_e^H + z_{1-\varphi}\sqrt{T P_e^H (1 - P_e^H)}, \tag{23}$$

where $z_{1-\varphi}$ is the $1 - \varphi$ quantile of the standard normal distribution. To guarantee $P(X \geq f(\xi, T)) \leq \varphi$, we have $f(\xi, T) \geq L(T, P_e^H, 1 - \varphi)$. Thus, $f(\xi^*(T), T) = L(T, P_e^H, 1 - \varphi)$. By substituting $f(\xi^*(T), T)$ according to Eq. (20), we have the optimal $\xi^*(T)$ for given T is

$$\xi^*(T) \approx V_0 - \frac{z_{1-\varphi}\sqrt{T P_e^H (1 - P_e^H)}}{P_e^H}.$$

Noting that, since φ is usually a small value, such as 5%, $z_{1-\varphi}$ is a positive value. Therefore, $\xi^*(T)$ is a decreasing function with respect to T, which indicates that the optimal threshold $\xi^*(T)$ decrease with the increasing T. Since V_{min} is the minimum trust value, we can calculate the maximum T, denoted by T_{max}, which can makes $\xi^*(T)$ below V_{min}. Let $\xi^*(T) \leq V_{min}$, we have $T_{max} = \left\lfloor \dfrac{(V_0 - V_{min})^2 \cdot P_e^H}{1 - P_e^H} \right\rfloor$. ■

According to Proposition2, we can adaptively determine the optimal detection threshold $\xi^*(T)$ for FastDtec when $T_{sw} < T \leq T_{max}$. We define T_{max} as a trust evaluation cycle of FastDtec. When node i is selected for spectrum sensing $T_{max} + 1$ times, we consider it is the first evaluation period of a new evaluation cycle, and reset its trust value to V_0. It indicates that a compromised node would be missed by FastDtec if it can keep its trust value large than V_{min} after T_{max} times of spectrum sensing. Lemma 5 analyzes the probability that a compromised node is not identified by FastDtec within a trust evaluation cycle.

Lemma 5: Given the required false identification probability φ, the missed identification probability of FastDtec is $MD(\varphi) = \min\{MD(\varphi, T_{min}), \ldots, MD(\varphi, T_{max})\}$, where $MD(\varphi, T)$ is given as $MD(\varphi, T) = \sum_{k=\lfloor f(\xi^*(T),T)\rfloor}^{T} Q(T, k, P_e)$; T_{min} and T_{max} are in Eq. (21) and (22), and $P_e = P_e^I$ or P_e^C according to Eq. (13) and (14) under I-SSDF or C-SSDF attacks, respectively.

Proof: We first focus on calculating the missed identification probability of FastDtec for given T. Let X be the number of wrong sensing reports with $X \sim B(T, P_e)$.

Algorithm 1 The Procedures of FastDtec

Input: The parameters related to FastDtec, such as V_0, V_{min}, V_{max} and φ.

$T_i \leftarrow 0$ for each node $i \in \mathcal{S}$, $\mathcal{CM} \leftarrow \emptyset$;
for each spectrum sensing node $i \in \mathcal{N}$ **do**
  $T_i \leftarrow T_i + 1$;
  Evaluate a trust score and update its trust value table according to Eq. (15) and (16), respectively;
  if $T_{min} \leq T_i \leq T_{sw}$ **then**
    Determine the optimal detection threshold $\xi^*(T)$ according to the numerical procedure;
  else if $T_{sw} < T_i \leq T_{max}$ **then**
    Determine the optimal detection threshold $\xi^*(T)$ according to Proposition 2;
  end if
  if $V_i \leq \xi^*(T)$ **then**
    $\mathcal{CM} \leftarrow \mathcal{CM} + \{i\}$;
  end if
  if $T_i \geq T_{max}$ && $i \notin \mathcal{CM}$ **then**
    $T_i = 0$, $V_i = 0$;
  end if
end for

If a compromised node is missed by FastDtec, it means $V_0 + (T - X) - X(1 - \frac{1 - P_e^H}{P_e^H}) \geq \xi^*(T)$. Thus, we have that $X \leq f(\xi^*(T), T)$ and the corresponding probability is $MD(\varphi, T) = P(X \leq f(\xi^*(T), T)) = \sum_{k=\lfloor f(\xi^*(T),T) \rfloor}^{T} Q(T, k, P_e)$.

If a compromised node is missed by FastDtec, it means that the node is not identified by FastDtec at any $T \in \{T_{min}, \ldots, T_{max}\}$. Thus, we have that the missed identification probability of FastDtec is $MD(\varphi) = \min\{MD(T_{min}), \ldots, MD(T), \ldots, MD(T_{max})\}$. ■

C. The Proposed FastDtec Scheme

Based on the preceding analysis, FastDtec can utilize asymmetric evaluation to stabilize the trust values of honest nodes and linearly reduce the trust values of compromised nodes. Moreover, an adaptive detection threshold is dynamically derived for FastDtec to accelerate the identification of compromised nodes while keeping the false identification probability below a specific requirement. We summarize the main ideas of FastDtec in Algorithm 1.

VI. Secure and Energy-Efficient Collaborative Spectrum Sensing for CRSNs

In this section, we propose a secure and energy-efficient collaborative spectrum sensing scheme for CRSNs, which can utilize FastDtec to accurately identify the compromised nodes and adaptively reduce the number of spectrum sensing nodes for further enhancing energy efficiency.

A. The Proposed Scheme

Based on our analysis, FastDtec can fast and accurately identify the compromised nodes launching SSDF attacks in CRSNs. If we isolate the identified compromised nodes from collaborative spectrum sensing, we can adaptively reduce the number of spectrum sensing nodes, i.e., N, to further improve the energy efficiency of collaborative spectrum sensing in CRSNs.

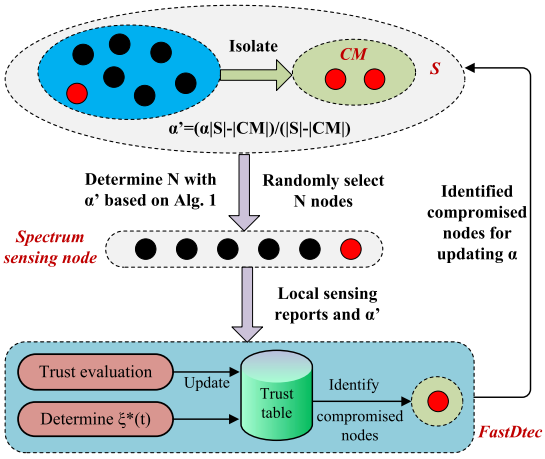


Fig. 3. Illustration of the proposed secure and energy-efficient collaborative spectrum sensing scheme.

For example, after M sensor nodes are identified as compromised nodes, the probability of selecting a compromised node into spectrum sensing changes to $\alpha' = \frac{\alpha S - M}{S - M}$. Obviously, we have $\alpha' < \alpha$. According to Proposition 1, the reduced α' means the decreased false alarm probabilities P_F^I, P_F^C and missed detection probabilities P_M^I, P_M^C under fixed L and N, which also indicates that reduced N_{min}^I and N_{min}^C could be derived to guarantee the required δ_F and δ_M. Therefore, once there is a sensor node identified as compromised by FastDtec, we can redetermine the optimal number of spectrum sensing nodes. The main idea of the proposed secure and energy-efficient collaborative spectrum sensing scheme is illustrated in Fig. 3, and the detailed procedures are summarized in Algorithm 2.

B. Further Discussion

In the proposed scheme, all the spectrum sensing nodes are randomly selected from the sensor nodes without being blacklisted. Meanwhile, the reports from the spectrum sensing nodes have the same weights for the global decision making. A number of existing works have done in-depth investigation to leverage the evaluated trust values in spectrum sensing node selection and global decision making. It can also be applied into the proposed scheme to improve the accuracy of global decision making. For example, we can allocate higher priority to the sensor nodes with higher trust values when selecting the spectrum sensing nodes. However, the energy consumption balancing issue should be further studied to keep the sensor nodes with high trust values from exhausting their energy quickly. Moreover, when the sink fuses local decisions to make a global decision, the reports from the sensor nodes with higher trust values can be allocated with higher weights for decision making. The related techniques

Algorithm 2 The Proposed Secure and Energy-Efficient Collaborative Spectrum Sensing Scheme

Input: The percentage of compromised nodes α, the required security levels δ_F and δ_M, the set of sensor nodes $\mathcal{S}$, V_0, V_{min}, V_{max} and other parameters.

1: $\mathcal{SN} \leftarrow \mathcal{S}$, $\alpha' \leftarrow \alpha$, $\mathcal{CM} \leftarrow \emptyset$;
2: $V_i \leftarrow V_0$ for each $i \in \mathcal{S}$;
3: **for** each time period t from 1 to $+\infty$ **do**
4: ***At the beginning of time period*** t :
5: Determine N^I_{min}, L^I, N^C_{min} and L^C with α', δ_F and δ_M by addressing Eq. (11) and (12);
6: Under I-SSDF and C-SSDF attack scenarios, randomly select N^I_{min} and N^C_{min} sensor nodes from $\mathcal{SN}$ with L^I and L^C for spectrum sensing, respectively;
7: ***At the end of time period*** t :
8: Update the trust values of spectrum sensing nodes according to Algorithm 1;
9: **if** There exists node $i \in \mathcal{SN}$ with $V_i \leq \xi^*$ **then**
10: $\mathcal{SN} \leftarrow \mathcal{SN} - \{i\}$, $\mathcal{CM} \leftarrow \mathcal{CM} + \{i\}$;
11: $\alpha' \leftarrow \dfrac{\alpha S - |\mathcal{CM}|}{|\mathcal{SN}|}$;
12: **end if**
13: **end for**

and analysis can be referred to [7], [16], and [18]. In [18], it is proved that the weighted decision making based on evaluated trust values has positive impacts on reducing the number of sensing reports. However, when weighted decision making is adopted, the designed SSDF countermeasure should be capable of resisting promotion attacks, where compromised nodes can collaboratively promote the trust values of several compromised nodes to mislead the decision making. In this work, we provide a probabilistic analysis for securing collaborative spectrum sensing, from the energy efficiency perspective. The proposed secure and energy-efficient collaborative spectrum sensing scheme can guarantee a desired security requirement and maximize the energy efficiency simultaneously. To the best of our knowledge, this is the first work to investigate the energy efficiency optimization for collaborative spectrum sensing under a desired security requirement in a probabilistic way.

VII. Performance Evaluation

In this section, we validate our theoretical analysis and evaluate the performance of our proposed schemes by OMNET++ [35], [36]. We setup a CRSN with $|\mathcal{S}| = 200$ sensor nodes and a sink node. The network process is divided into a sequence of time periods. At the beginning of each time period, the sink randomly chooses a number of sensor nodes to sense a licensed channel. The idle and busy probabilities of the licensed channel are $P_0 = 90\%$ and $P_1 = 10\%$, respectively. The parameters for individual spectrum sensing are set as $P_{cf} = 20\%$ and $P_{cm} = 20\%$. The percentage of compromised nodes in the CRSN is $\alpha = 20\%$, if it is not specified in the simulation figures. The desired missed detection probability and false alarm probability of collaborative spectrum sensing are set as $\delta_M = 1\%$ and $\delta_F = 5\%$, respectively. For the settings of FastDtec, we have $V_0 = 200$, $V_{min} = 0$ and $V_{max} = 255$. The requirement of the false identification probability of FastDtec is $\varphi = 2.5\%$, and $T_{sw} = 20$.

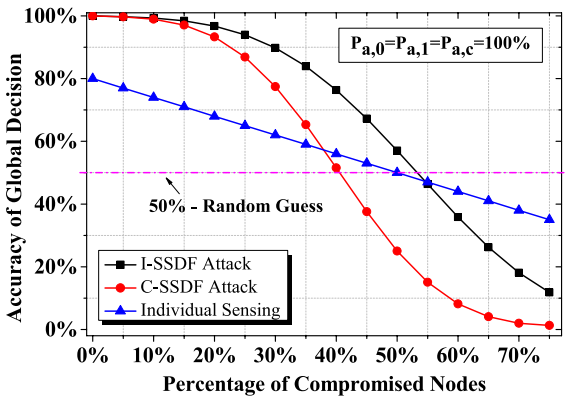


Fig. 4. The impacts of I-SSDF and C-SSDF attacks on the accuracy of collaborative spectrum sensing.

A. Attack Impacts on Collaborative Spectrum Sensing

In this subsection, we first evaluate the impacts of I-SSDF and C-SSDF attacks on the accuracy of collaborative spectrum sensing. Then, we show the trade-off between security and energy efficiency determined by addressing Eq. (11) and (12).

Fig. 4 shows the accuracy of global decision by collaborative spectrum sensing under different percentages of SSDF attackers (i.e., compromised nodes). The accuracy of global decision is defined as $P(\mathcal{D} = 1|\mathcal{H}_1) + P(\mathcal{D} = 0|\mathcal{H}_0)$. 20 sensor nodes are involved in the collaborative spectrum sensing and the decision rule is "majority" rule, which mean $N = 20$ and $L = 11$. The individual sensing refers to that only one sensor node is selected for sensing the licensed channel. It can be seen from the figure that the accuracy of global decision is significantly reduced with the increasing percentage of compromised nodes. The collaborative spectrum sensing under C-SSDF attacks has a lower accuracy than that under I-SSDF attacks. Moreover, when the percentage of compromised nodes exceeds 39%, the global decision accuracy of collaborative spectrum sensing under C-SSDF attacks is below 50%. It means that collaborative spectrum sensing is no better than random guess for a network with more than 39% compromised nodes to launch C-SSDF attacks. A similar conclusion can be found in [8] and [16]. In addition, under C-SSDF attacks, individual sensing is more accurate than collaborative spectrum sensing when the percentage of compromised nodes is larger than 37%. Fig. 5 compares the required number of spectrum sensing nodes to guarantee desired security levels (i.e., δ_F and δ_M) under different percentages of compromised nodes. It is shown that the required number of specturm sensing nodes increases sharply with increasing compromised nodes, especially for resisting C-SSDF attacks.

B. Trust Evaluation and Compromised Node Identification by FastDtec

In this subsection, we evaluate the performance of the proposed FastDtec scheme, in terms of the speed and accuracy of compromised node identification.

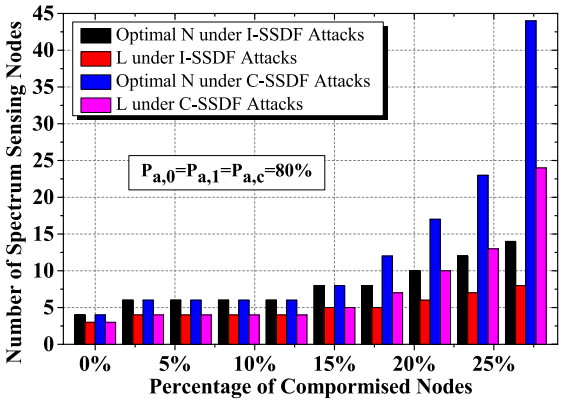


Fig. 5. Required number of spectrum sensing nodes to guarantee a desired security level.

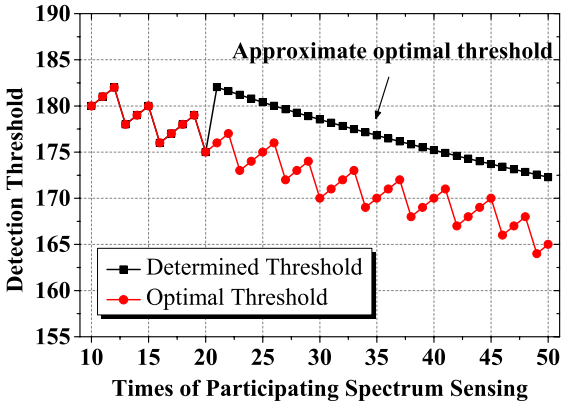


Fig. 7. Comparison of determined detection threshold and optimal detection threshold.

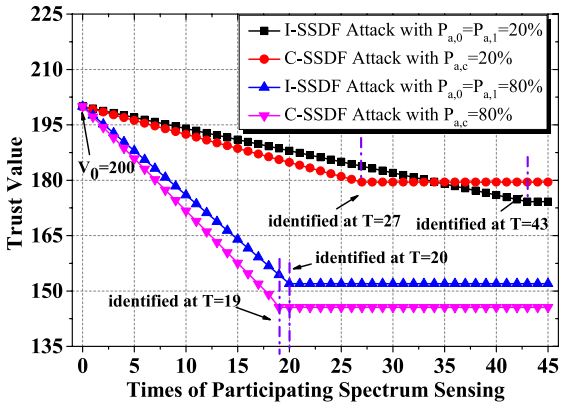
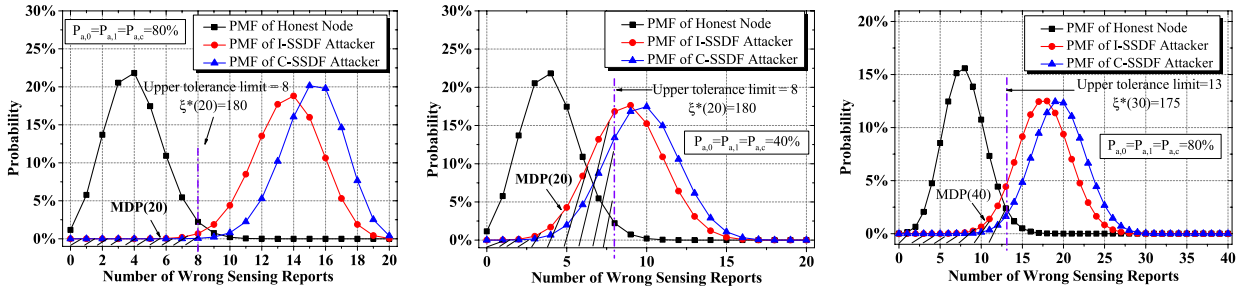


Fig. 6. Expected trust values of compromised nodes under different attacking probabilities.

Fig. 6 compares the expected trust values of compromised nodes with different attacking probabilities. It can be seen that the expected trust values of compromised nodes with a higher attacking probability drop more quickly as the times of participating spectrum sensing increases. Consequently, it leads to that the compromised nodes with higher attacking probability are identified by FastDtec faster than those with lower attacking probability. Moreover, with the same attacking probability, the compromised node launching C-SSDF attacks has a lower expected trust value and is identified by FastDtec faster than the one launching I-SSDF attacks.

Fig. 7 compares the determined threshold $\xi^*(T)$ and the optimal threshold under different T. It shows that the approximate optimal threshold determined by Proposition 2 is very close to the optimal threshold. Fig. 8 shows the determined optimal detection thresholds of FastDtec under different attacking probabilities and T. We use X to denote the wrong sensing reports of a sensor node. These three figures show the probability mass functions (PMF, i.e., $P(X = k)$ where $0 \leq k \leq T$), of different sensor nodes, under different T and attacking probabilities. It can be seen from the figures that the overlap of the PMFs of a honest node and a compromised node becomes larger when the attacking probability is low. It indicates that the missed identification probability of FastDtec $MD(\varphi, T)$ would be larger under a lower attacking probability when T is fixed. Meanwhile, as the number of times of participating spectrum sensing increases, the missed identification probability of FastDtec reduces significantly. Fig. 9 shows the percentage of the compromised nodes that are not identified by FastDtec. It can be seen that the compromised nodes under C-SSDF attack scenarios are identified faster than those under I-SSDF attack scenarios. Furthermore, the percentage of the compromised nodes without being identified quickly plummets to 0 after a compromised node is identified by the proposed scheme. It also demonstrates that FastDtec can fast identify the compromised nodes in a small number of time periods.

To show the superiority of FastDtec in compromised node identification, we compare FastDtec with an existing scheme [37], named CatchIt, in terms of the accuracy and speed of compromised node identification. Fig. 10 shows the comparison of the identification accuracy of FastDtec and CatchIt under different attacking probabilities. The identification accuracy is evaluated by the sum of two probabilities. One is false identification probability (FIP), which means the probability that the trust system falsely identifies a honest node as a compromised node. And the other is missed identification probability (MIP), which means the probability that a compromised node is missed by the trust scheme within a certain number of periods. It can be seen from the figure that the identification accuracy increases with the attacking probability of compromised nodes and both of FastDtec and CatchIt can achieve a high identification accuracy under different attacking probabilities. However, FastDtec can still outperform CatchIt, i.e., having lower FIP+MIP, especially when the attacking probability is low. Fig. 11 compares the identification speed of FastDtec and CatchIt under different attacking probabilities. We evaluate the identification speed by the number of evaluation periods that is required to identify a compromised node. It can be seen that, under both of FastDtec and CatchIt, C-SSDF attackers can be identified faster than I-SSDF attackers at the same attacking probability. Meanwhile, FastDtec has a faster identification speed than CatchIt. The comparison results of the two figures also demonstrate that by guaranteeing the identification accuracy and optimizing the identification speed, FastDtec can significantly improve the performance of



(a) $T = 20$, $P_{a,0} = P_{a,1} = P_{a,c} = 80\%$ (b) $T = 20$, $P_{a,0} = P_{a,1} = P_{a,c} = 40\%$ (c) $T = 40$, $P_{a,0} = P_{a,1} = P_{a,c} = 40\%$

Fig. 8. Determined detection thresholds of FastDtec under different attacking probabilities and T.

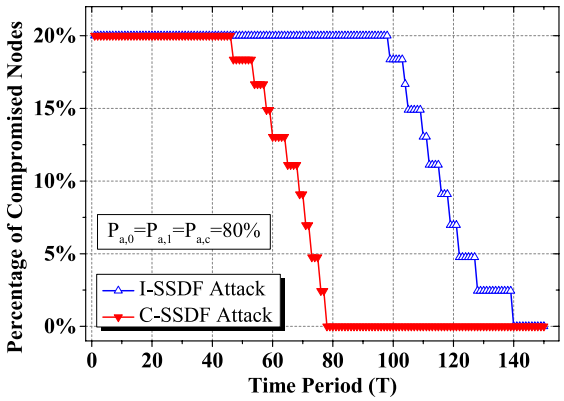


Fig. 9. The speed of compromised node identification under I-SSDF and C-SSDF attacks.

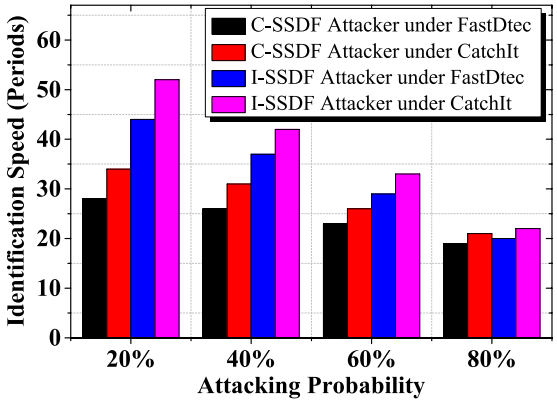


Fig. 11. Compromised node identification speed comparison under different attacking probabilities.

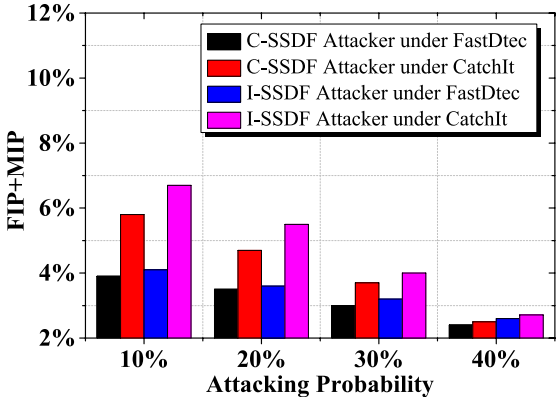


Fig. 10. Compromised node identification accuracy comparison under different attacking probabilities.

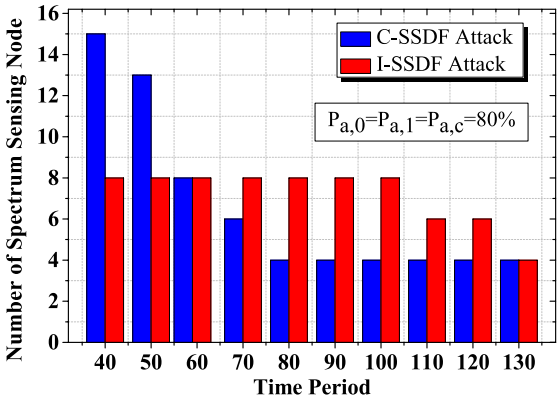


Fig. 12. Required number of spectrum sensing nodes under different time periods.

compromised node identification for collaborative spectrum sensing.

C. Performance of Secure and Energy Efficient Collaborative Spectrum Sensing Scheme

In this subsection, we evaluate the performance of the proposed secure and energy-efficient collaborative spectrum sensing scheme. Since the proposed collaborative spectrum sensing scheme can guarantee the desired accuracy requirements by Eq. (11) and (12), we mainly focus on evaluating the energy efficiency enhancement. As the energy consumption of collaborative spectrum sensing is high and increases linearly with the number of spectrum sensing nodes, we use the required number of sensor nodes that can guarantee the accuracy requirements to evaluate the energy efficiency. Fig. 12 shows the required numbers of spectrum sensing nodes during different time periods. It can be seen that the number of required spectrum sensing nodes is significantly reduced with the increasing time period, under both types of SSDF attacks. And the number of spectrum sensing nodes decreases earlier

and faster under C-SSDF attacks, as the compromised nodes with C-SSDF attacks are identified faster by the proposed scheme.

VIII. Conclusion

In this paper, we have investigated the secure collaborative spectrum sensing for CRSNs, from the energy efficiency perspective. We theoretically analyze the impacts of independent and collaborative SSDF attacks on the accuracy of collaborative spectrum sensing. Our analysis and simulations show that the number of spectrum sensing nodes and associated global decision rule have significant impacts on the accuracy of collaborative sensing results. To achieve the tradeoff between security and energy efficiency, we determine the minimum number of spectrum sensing nodes to guarantee desired security requirements. Moreover, we have developed a trust evaluation scheme, named FastDtec, to evaluate the spectrum sensing behaviors and identify the compromised nodes. By determining an adaptive and optimal detection threshold, FastDtec can fast and accurately identify compromised nodes. In addition, taking advantage of FastDtec to isolate the identified compromised nodes from spectrum sensing, we have proposed a secure and energy-efficient collaborative spectrum sensing scheme to further enhance the energy efficiency of collaborative spectrum sensing. Extensive simulation results demonstrate that the proposed collaborative spectrum sensing scheme can effectively resist SSDF attacks, and fast and accurately identify compromised nodes, as well as improving energy efficiency. For our future work, we will extend our research to a more general network scenario, where the CRSN has no prior knowledge about the compromising probability of the network and the percentage of compromised node may increase time to time. Thus, we will design a scheme that can estimate the compromising probability based on historical records and adaptively adjust its defending strategy with the belief to the estimated results.

References

[1] Z. Liang, S. Feng, D. Zhao, and X. Shen, "Delay performance analysis for supporting real-time traffic in a cognitive radio sensor network," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 325–335, Jan. 2011.

[2] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart., 2015.

[3] Y. Cai, Y. Mo, K. Ota, C. Luo, M. Dong, and L. T. Yang, "Optimal data fusion of collaborative spectrum sensing under attack in cognitive radio networks," *IEEE Netw.*, vol. 28, no. 1, pp. 17–23, Jan./Feb. 2014.

[4] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Commun.*, vol. 19, no. 6, pp. 106–112, Dec. 2012.

[5] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Gödor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 355–379, 2nd Quart., 2012.

[6] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 13, no. 2, pp. 86–95, 2009.

[7] K. Zeng, P. Pawełczak, and D. Čabrić, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 226–228, Mar. 2010.

[8] 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.

[9] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 31–35.

[10] X. He, H. Dai, and P. Ning, "HMM-based malicious user detection for robust collaborative spectrum sensing," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2196–2208, Nov. 2013.

[11] J. Wang, J. Yao, and Q. Wu, "Stealthy-attacker detection with a multidimensional feature vector for collaborative spectrum sensing," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 3996–4009, Oct. 2013.

[12] X. He, H. Dai, and P. Ning, "A Byzantine attack defender in cognitive radio networks: The conditional frequency check," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2512–2523, May 2013.

[13] F. Penna, Y. Sun, L. Dolecek, and D. Čabrić, "Detecting and counteracting statistical attacks in cooperative spectrum sensing," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1806–1822, Apr. 2012.

[14] Z. Qin, Q. Li, and G. Hsieh, "Defending against cooperative attacks in cooperative spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2680–2687, Jun. 2013.

[15] M. Ghaznavi and A. Jamshidi, "A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network," *IEEE Sensors J.*, vol. 15, no. 3, pp. 1810–1816, Mar. 2015.

[16] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1707–1719, Aug. 2014.

[17] S. Althunibat, V. Sucasas, H. Marques, J. Rodriguez, R. Tafazolli, and F. Granelli, "On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1564–1567, Aug. 2013.

[18] 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.

[19] J. Ren, Y. Zhang, N. Zhang, D. Zhang, and X. Shen, "Dynamic channel access to improve energy efficiency in cognitive radio sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3143–3156, May 2016.

[20] S. Althunibat, R. Palacios, and F. Granelli, "Energy-efficient spectrum sensing in cognitive radio networks by coordinated reduction of the sensing users," in *Proc. IEEE ICC*, Jun. 2012, pp. 1399–1404.

[21] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[22] M. Timmers, S. Pollin, A. Dejonghe, L. Van der Perre, and F. Catthoor, "A distributed multichannel MAC protocol for multihop cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 446–459, Jan. 2010.

[23] G. Ding, Q. Wu, Y.-D. Yao, J. Wang, and Y. Chen, "Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions," *IEEE Signal Process. Mag.*, vol. 30, no. 4, pp. 126–136, Jul. 2013.

[24] S. Liu, H. Zhu, S. Li, X. Li, C. Chen, and X. Guan, "An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing," in *Proc. IEEE GLOBECOM*, Dec. 2012, pp. 603–608.

[25] 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. IEEE INFOCOM*, Mar. 2012, pp. 900–908.

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

[27] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An anomaly detection framework for dynamic spectrum access networks," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 675–683.

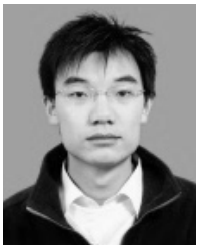
[28] G. Ding *et al.*, "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014.

[29] S. Sodagari, A. Attar, V. C. M. Leung, and S. G. Bilén, "Denial of service attacks in cognitive radio networks through channel eviction triggering," in *Proc. IEEE GLOBECOM*, Dec. 2010, pp. 1–5.

[30] D. Zhang *et al.*, "Energy harvesting-aided spectrum sensing and data transmission in heterogeneous cognitive radio sensor network," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2016.2551721.

[31] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5761–5766, Dec. 2009.

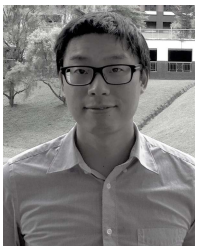
[32] S. Althunibat, "Towards energy efficient cooperative spectrum sensing in cognitive radio networks," Ph.D. dissertation, Inf. Commun. Technol. School, Univ. Trento, Trento, Italy, 2014.
[33] T. T. Cai and H. Wang, "Tolerance intervals for discrete distributions in exponential families," *Statist. Sinica*, vol. 19, no. 3, pp. 905–923, 2009.
[34] K. Krishnamoorthy, Y. Xia, and F. Xie, "A simple approximate procedure for constructing binomial and Poisson tolerance intervals," *Commun. Statist.-Theory Methods*, vol. 40, no. 12, pp. 2243–2258, 2011.
[35] J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, and X. S. Shen, "Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 788–800, Apr. 2016.
[36] Q. Ye, W. Zhuang, L. Li, and P. Vigneron, "Traffic load adaptive medium access control for fully-connected mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2016.2516910.
[37] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE GLOBECOM*, Nov./Dec. 2009, pp. 1–6.



Ju Ren (S'13) received the B.Sc., M.Sc., and Ph.D. degrees from Central South University, China, in 2009, 2012, and 2016, respectively, all in computer science. From 2013 to 2015, he was a Visiting Ph.D. Student with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a Distinguished Professor with the School of Information Science and Engineering with Central South University, China. He has authored over 20 peer-reviewed papers on some pretigious international journals and conferences, including the IEEE TWC, TII, TVT, TETC, and ComMag. His research interests include wireless sensor network, mobile sensing/computing, transparent computing, and cloud computing.

Yaoxue Zhang received the B.Sc. degree from the Northwest Institute of Telecommunication Engineering, China, in 1982, and the Ph.D. degree in computer networking from Tohoku University, Japan, in 1989. He is currently a Professor with the Department of Computer Science, Central South University, China, and also a Professor with the Department of Computer Science and Technology, Tsinghua University, China. He has authored over 200 technical papers in international journals and conferences, and nine monographs and textbooks. His research interests include computer networking, operating systems, ubiquitous/pervasive computing, transparent computing, and big data. He is a fellow of the Chinese Academy of Engineering and the President of Central South University.

Qiang Ye (S'16) received the B.Sc. and M.Sc. degrees from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2009 and 2012, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research interests include medium access control and performance optimization in mobile ad hoc networks, and Internet of Things.



Kan Yang (M'13) received the B.Eng. degree in information security from the University of Science and Technology of China in 2008, and the Ph.D. degree in computer science from the City University of Hong Kong in 2013. From 2013 to 2014, he was a Post-Doctoral Fellow with the Department of Computer Science, City University of Hong Kong. From 2014 to 2016, he was a Post-Doctoral Fellow and the Co-Ordinator of Security Group with the Broadband Communications Research Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He will join the Department of Computer Science with the University of Memphis. His research interests include cloud security, big data security, mobile security, applied cryptography, and distributed systems.

Kuan Zhang (S'13) received the B.Sc. degree in electrical and computer engineering, and the M.Sc. degree in computer science from Northeastern University, China, in 2009 and 2011, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2016. He is currently a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include security and privacy for mobile social networks, and e-healthcare.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, China, in 1982, and the M.Sc. and Ph.D. degrees from Rutgers University, NJ, USA, in 1987 and 1990, respectively, all in electrical engineering. He is currently a Professor and the University Research Chair with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is also the Associate Chair for graduate studies. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He is an elected member of IEEE ComSoc Board of Governors, and the Chair of Distinguished Lecturers Selection Committee. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award from the University of Waterloo in 2004, 2007, 2010, and 2014, respectively, the Premier's Research Excellence Award from the Province of Ontario, Canada, in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, in 2002 and 2007, respectively. He served as the Technical Program Committee Chair/Co-Chair for the IEEE Globecom'16, Infocom'14, the IEEE VTC'10 Fall, and the Globecom'07, the Symposia Chair for the IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring and the IEEE ICC'08, the General Co-Chair of the ACM Mobihoc'15, the Chinacom'07 and the QShine'06, the Chair of the IEEE Communications Society Technical Committee on Wireless Communications, and the P2P Communications and Networking. He also serves/served as the Editor-in-Chief of the IEEE NETWORK, the *Peer-to-Peer Networking and Application*, and the *IET Communications*, a Founding Area Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Networks*, and the ACM/*Wireless Networks*, and the Guest Editor of the IEEE JSAC, the IEEE WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS MAGAZINE, and the ACM *Mobile Networks and Applications*. He is also a Registered Professional Engineer in Ontario, Canada, an the Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society.