This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

Robust Reputation-Based Cooperative Spectrum Sensing via Imperfect Common Control Channel

Lichuan Ma, *Student Member, IEEE*, Yong Xiang, *Senior Member, IEEE*, Qingqi Pei, *Senior Member, IEEE*, Yang Xiang, *Senior Member, IEEE*, and Haojin Zhu, *Senior Member, IEEE*

***Abstract*—Due to the fast-growing usage of wireless devices, cognitive radio networks have been proposed to address the spectrum scarcity problem. As the foundation of their practical applications, designing robust and secure spectrum sensing mechanisms is of great significance. In most existing works, the common control channel (CCC) is assumed to be perfect. However, this assumption may not hold in practice and imperfect CCC makes the existing methods against independent or cooperative data falsification attacks less effective. In this paper, we first analyze the impact of an imperfect CCC on the identification of malicious secondary users under independent and cooperative attacks. To better differentiate honest users and malicious users, a reputation threshold is derived for each secondary user. Based on the obtained reputation threshold, we propose a new reputation-based cooperative spectrum sensing method, which is validated to be robust against attacks under imperfect CCC. Extensive numerical simulations demonstrate the effectiveness of the proposed method.**

***Index Terms*—Cognitive radio networks, cooperative spectrum sensing, reputation value threshold computation.**

I. Introduction

With the wide employment of wireless devices in various communication systems and networks, the current static frequency allocation schemes cannot, cope with the dramatically increasing data transmission demand [1]. However, a survey from the Federal Communications Commission states many spectra authorized to users are not efficiently utilized [2]. Under such a circumstance, the emerging concept of cognitive radio networks (CRNs) has been inspired, which is considered as a promising way to improve the utilization of scarce radio spectrum [3]. Moreover, the first cognitive radio based network standard has been proposed in IEEE 802.22. It defines a centralized, single hop, and one-point to multi-point communication standard for wireless regional area networks [4], in which there are three main entities: primary users (PUs), secondary users (SUs) and a fusion center (FC). The PUs have authorized spectra which are always available to them. The SUs are devices that are capable of sensing the surrounding spectra and sending the local sensing results to the FC. The FC makes a final spectrum sensing decision and broadcasts it to all SUs. After that, the SUs would perform data transmission according to the decision of the FC. A dedicated channel, named common control channel (CCC), is utilized to exchange control messages between the FC and the SUs. The kind of control messages can be cooperative spectrum sensing (CSS) data, spectrum-aware routing information and spectrum access coordination information. Thus, a reliable and "always on" CCC is indispensable [5]. Since the CCC is utilized by all SUs and its capacity is limited, the control messages should be carefully simplified. Otherwise, the CCC may become the bottleneck of the whole network.

In CRNs, it is essential that the SUs do not cause interference to the PUs. To ensure this, the SUs periodically sense the spectra to detect the presence of the PUs and vacate the spectra in time when the PUs come back. Therefore, spectrum sensing plays a key role in CRNs. However, some SUs may be malicious and can transmit false local sensing results to the FC or other SUs. As a result, the transmission of PUs can be interfered and the idle spectra can be only occupied by malicious SUs [6]. The presence of these malicious SUs (MSUs) can degrade the effectiveness of CSS dramatically. This kind of attack launched by MSUs is usually referred as spectrum sensing data falsification attack [7]. When the MSUs launches attacks independently, it is referred as independent attacks and otherwise, it is referred as cooperative attacks when MSUs act cooperatively [4], [8]. In order to prevent these two kinds of attacks from MSUs, it is essential to detect MSUs so that the FC only uses information from the honest SUs (HSUs) to make a correct spectrum sensing decision.

Existing works to defend against MSUs in CSS phase usually assume that the CCC is perfect (i.e., error-free) [4], [8]-[11]. However, this assumption cannot be satisfied in practice. Based on modeling the probability of reporting one-bit error via CCC introduced by [13], we find that the effectiveness of the above methods to detect MSUs and guarantee the correctness of the FC's spectrum sensing decisions can be degraded dramatically in this case. Thus, the impact of imperfect CCC on identifying of MSUs from HSUs should be analyzed at first under both independent and cooperative attacks.

Since different SUs have different probabilities of reporting one-bit error via CCC due to their different locations, it is improper to use just one unified reputation value threshold to filter out MSUs as in [4] and [8]. It also requires that

L. Ma and Q. Pei are with the State Key Laboratory of Integrated Services Network, Xidian University, Xi'an, 710071, China. (E-mail: malichuan@126.com, qqpei@mail.xidian.edu.cn). Q. Pei is the corresponding author.

Y. Xiang is with the School of Information Technology, Deakin University, Victoria 3125, Australia. (E-mail: yxiang@deakin.edu.au).

Y. Xiang is with the School of Software and Electrical Engineering, Swinburne University of Technology, VIC 3122, Australia. (E-mail: yxiang@swin.edu.au).

H. Zhu is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, 200240, China. (E-mail: zhuhj@cs.sjtu.edu.cn).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

the probability that an HSU is misjudged as a malicious one should be limited to a low level when designing such a reputation value threshold. Hence, it is necessary to set a personalized threshold for each SU to decide whether it is filtered out as an MSU.

After filtering out the SUs whose reputation value is lower than their own personalized thresholds, the FC should decide which remaining SUs should participate in CSS in the future and what fusion rules should be utilized to draw final spectrum sensing decisions.

Therefore in this paper, we develop a robust reputation-based cooperative spectrum sensing (R^2-CSS) method, which can tackle both independent and cooperative attacks under an imperfect CCC. The development of the R^2-CSS method involves three stages, which also form the three major contributions of the paper:

- Firstly, we analyze the impact of an imperfect CCC on the detection of MSUs under independent and cooperative attacks. It is shown that an imperfect CCC could make more HSUs be incorrectly recognized as MSUs, which would cause the FC to make incorrect final spectrum sensing decisions.
- Secondly, to better differentiate HSUs and MSUs in the scenario of imperfect CCC, we derive a novel reputation threshold for each SU, which can be used to judge whether an SU is malicious or not.
- At last, the R^2-CSS method is proposed, built upon the reputation threshold of each SU. Here, a number of HSUs are randomly chosen to perform CSS by a weighted majority rule. Theoretical analysis and extensive simulations justify the effectiveness of the proposed method.

The rest of the paper is organized as follows. Related work is summarized in Section II. The impact of imperfect CCC on the detection of MSUs is analyzed in Section III. The new reputation threshold for MSU detection is derived in Section IV. In Sections V, we present the R^2-CSS method and its performance defending against MSUs is analyzed in Section VI. Simulation results are provided in Section VII to show the superior performance of the proposed method and Section VIII concludes the paper.

II. Related Work

So far, a number of spectrum sensing methods have been reported in the literature, which can be classified into two categories: non-cooperative spectrum sensing (n-CSS) and CSS.

In n-CSS, each SU makes its decision without exchanging information with the others. On the basis that each SU has an embedded energy detector, the signals of PUs can be detected by comparing the output of the energy detector with a threshold which depends on the noise floor [14], [15]. When the waveform patterns of the PU signals are known, the SUs can compare the waveform patterns of the received signals with the known ones to find the presence and absence of PUs [16]. For example, the PUs can be detected by exploiting the cyclostationary features of PU signals [17]. The PUs can also be detected by radio identification based sensing [18] and matched-filter based sensing [19]. However, the effectiveness of the n-CSS methods degrades significantly in the situation of wireless channel uncertainty caused by noise, small-scale fading and shadowing, which is unavoidable in practical applications.

In contrast, the CSS methods are less sensitive to wireless channel uncertainty. A cluster-based CSS method is proposed in [20] to obtain a proper assignment policy in which all SUs in the same cluster cooperate in sensing the same set of PU spectra. In [21], the SUs to perform CSS would be selected with different rates aiming to satisfy the global detection and false alarm requirements. In [22], it is assumed that the energy detector of each SU has a different signal-to-noise ratio (SNR) and the SUs are chosen for CSS according to a derived optimal detection threshold. Taking practical spectrum conditions and link failures into consideration, a weighted soft measurement combining with an FC for CSS is developed in [23]. Dai *et al* put forward a sensor selection method for CSS in [24], with the purpose of minimizing the interference to PUs caused by the transmission behaviors of SUs. In [25], two scenarios, with and without sensor node location information respectively, are considered and the corresponding SU selection methods are derived satisfying the average global detection probability constraints.

Although the above CSS schemes can provide multiplexing gains and improve accuracy, they are vulnerable to attacks. A number of CSS methods that can tackle attacks have been reported in [4], [8]-[11], and [26]-[27]. In [10], Wang *et al* propose to thwart malicious behaviors by designing a protocol which makes the payoff of launching attacks smaller than zero. Whilst this may reduce the number of MSUs launching attacks, it cannot stop all MSUs from attacking. In [26], a fast searching algorithm is proposed to find a cluster of HSUs to perform CSS but many HSUs are not included in this cluster, which lowers the effectiveness of CSS. An iterative expectation maximization algorithm is proposed in [27] to detect MSUs but it requires some strong conditions, as to be shown later.

Differently, the reputation of SUs is exploited to design CSS methods in [4], [8], [9] and [11]. In a reputation based method, the reputation value of each SU is computed based on the similarity between its own sensing history and the final decisions made by the FC. In [9], the trust of an SU and its capability to sense the spectra are taken into account when computing the reputation value. In [11], Mousavifar and Leung design a reputation-based spectrum sensing protocol with less SU sensing reports and the accuracy of reputation values is proved. Yet, it cannot judge whether an SU is malicious or not. It should be noted that the reputation-based methods in [9] and [11], as well as the methods in [10], [26] and [27], assume that an MSU individually sends out the sensing result opposite to its own local sensing counterpart by a probability (referred as independent attack) and the FC always makes correct spectrum sensing decisions. However, they do not consider the case of cooperative attack [4], [8].

In order to detect the MSUs under both independent and cooperative attacks, a reputation factor is defined in [8] and a threshold to detect whether an SU is malicious is derived

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

under the assumption that the fraction of MSUs over all SUs is known to the FC. However, this fraction is seldom known in practice, which causes many HSUs being labeled as MSUs in [8]. On the contrary, the MSU selection method in [4] does not require any prior information about MSUs. In this method, the reputation value is determined by the structure of the clusters and an SU is deemed as a malicious one when its reputation value is under a threshold. Unfortunately, how to find such a threshold is not given in [4] because too much uncertainty is introduced by the structure of clusters. Instead, the reputation value threshold is fixed at 0.5. As a result, a portion of MSUs would not be detected. Furthermore, many CSS methods, including those above except [11], assume that the CCC is perfect. This assumption, however, hardly holds in practical applications, thanks to the presence of interference and noise. Although the CSS protocol in [11] considers imperfect channel but it cannot, as previously mentioned, be used to detect MSUs.

Note that there may exist some other attacks, like jamming attacks [28], primary user emulation attacks [29], location inference attacks [30], *etc*. Since these attacks are not unique in the cooperative spectrum phase and can be mitigated by spread-spectrum techniques [31] or existing countermeasures in wireless sensor networks [32], it is beyond the scope of this paper to deal with such attacks.

III. Imperfect CCC and Its Impact

In this section, we first introduce the CRN model considered, which has been widely used in other works. Given this CRN model, we then analyze how an imperfect CCC affects the detection of the MSUs, which consequently has an impact on the final spectrum sensing decision made by the FC.

A. CRN model

According to [4], [8]-[12], and [26]-[27], the system model we consider is as shown in Fig. 1. There are N SUs and one PU coexisting in the same area. An FC is in charge of spectrum management for all SUs. Among these SUs, there are M MSUs and the FC has no idea which SUs are malicious. Let $\mathcal{N}$ and $\mathcal{M}$ denote the collection of all the SUs and all the MSUs respectively. The distances between the FC and the SUs are assumed to be much shorter than the distance between the FC and the PU. The FC and the SUs are synchronized and a time slotting structure is utilized where each time slot is divided into two parts: spectrum sensing phase and data transmission phase.

To perform CSS, each SU first conducts individual spectrum sensing to decide on the spectrum state and then reports a one-bit decision to the FC via CCC. As for individual spectrum sensing, the energy detector based sensing is utilized here, thanks to its low computation and implementation complexities and its nonnecessity of any knowledge on the PU signal [1]. Let ld_i denote the local decision of the ith SU, labelled as SU_i. If SU_i detects the existence of the PU signal, we set $ld_i = 1$; otherwise, $ld_i = 0$. The detection probability P_d and the false alarm probability P_f are utilized to evaluate the accuracy of individual spectrum sensing. Here,

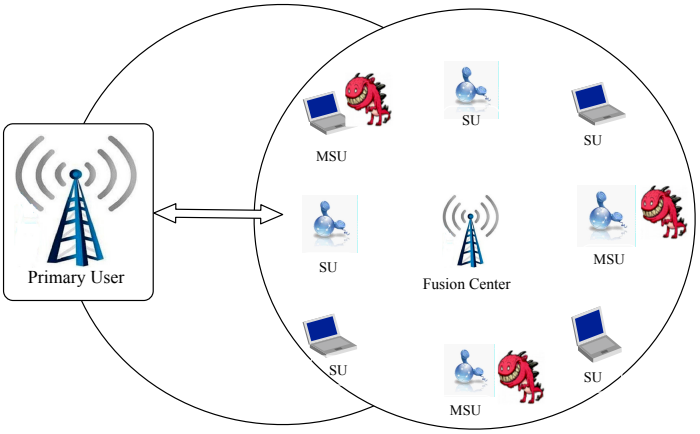


Fig. 1. The considered CRN model.

$P_d = P(ld_i = 1|H_1)$ and $P_f = P(ld_i = 1|H_0)$ with H_0 and H_1 being two hypotheses defined as

$$\begin{cases} H_0 & \text{the spectrum is idle} \\ H_1 & \text{the spectrum is occupied by the PU.} \end{cases}$$

In this scenario, all SUs have the same P_d, as well as the same P_f [4]. Specifically, P_d and P_f can be computed by the FC as follows [13], [14]:

$$\begin{aligned} P_d = e^{-\frac{\lambda}{2}} \sum_{n=0}^{w-2} \frac{1}{n!} \left(\frac{\lambda}{2}\right)^n + \left(\frac{1+\bar{\gamma}}{\bar{\gamma}}\right)^{w-1} \\ \times \left[e^{-\frac{\lambda}{2(1+\bar{\gamma})}} - e^{-\frac{\lambda}{2}} \sum_{n=0}^{w-2} \frac{1}{n!} \left(\frac{\lambda\bar{\gamma}}{2(1+\bar{\gamma})}\right)^n \right] \end{aligned} \tag{1}$$

and

$$P_f = \frac{\Gamma\left(w, \frac{\lambda}{2}\right)}{\Gamma(w)} \tag{2}$$

where w is the time bandwidth product, λ is the energy detection threshold, $\Gamma(.)$ is the gamma function, $\Gamma(.,.)$ is the incomplete gamma function, and $\bar{\gamma}$ is the average SNR of the received signal from the PU to the SUs. Here, $\bar{\gamma}$ is given by

$$\bar{\gamma} = \rho_{PU} h_{PU} / \sigma^2 \tag{3}$$

where ρ_{PU} is the transmit power of the PU, σ^2 is the Gaussian noise variance, and

$$h_{PU} = \kappa / d_P^{\mu} \tag{4}$$

is the path loss between the PU and the SUs with κ, μ and d_P being the path loss constant, the path loss exponent and the distance between the PU and the SUs, respectively.

After the FC receives the reports from all SUs, it will work out a final spectrum sensing decision and broadcast it to all SUs. Depending on the CSS methods used, the rules for the FC to get the final spectrum sensing decision would be different.

B. Impact of imperfect CCC on MSU detection

In most existing works about CSS, the CCC is assumed to be perfect. In this case, for any HSU, the probability of reporting a correct sensing result is [4], [8]:

$$p_H = P_B P_d + P_I (1 - P_f) \tag{5}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

where P_d and P_f are given in (1) and (2) respectively, P_B is the probability that the PU is transmitting on the authorized spectrum, and $P_I = 1 - P_B$. As indicated in Section III-A, all SUs have the same P_d and P_f, and thus all SUs have the same p_H.

However, as previously mentioned, the CCC cannot be perfect in practice. Consequently, errors could occur when SUs transmit messages to the FC. Moreover, as shown in [5], the CCC is usually capacity limited and thus it is impossible to use check codes to guarantee the successful transmission of local spectrum sensing results, especially when the number of SUs is large. Next, we discuss how this affects the FC to identify the MSUs and subsequently make the final spectrum sensing decision.

According to [13], given BPSK modulation in Rayleigh fading environment, the probability of reporting one-bit error between SU_i and the FC via an imperfect CCC is given by

$$P_{e,i} = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_i}{1+\bar{\gamma}_i}}\right) \tag{6}$$

with

$$\bar{\gamma}_i = \rho_i h_i / \sigma^2 \tag{7}$$

being the average SNR for the bit reporting between SU_i and the FC. Here, ρ_i is the transmit power of SU_i;

$$h_i = \kappa / d_i^{\mu} \tag{8}$$

and d_i are the path loss and the distance between SU_i and the FC, respectively. Based on p_H and $P_{e,i}$, the probability for any HSU SU_i to report a correct sensing result under an imperfect CCC is

$$\begin{aligned} P_{H,i} &= p_H(1-P_{e,i}) + (1-p_H)P_{e,i} \\ &= \mathcal{F}(p_H, P_{e,i}) \end{aligned} \tag{9}$$

where $\mathcal{F}$ is a function defined as $\mathcal{F}(x,y) = x(1-y)+(1-x)y$.

As stated in [4], the ability of the FC to distinguish MSUs from HSUs is determined by the probability of reporting different local sensing results for an HSU and an MSU. The larger such probability is, the more easily the FC can separate MSUs from HSUs. Let $p_{AH}^{i,j}$ be this probability for an HSU SU_i and an MSU SU_j under a perfect CCC, and $P_{AH}^{i,j}$ be the counterpart of $p_{AH}^{i,j}$ under an imperfect CCC. Then, $P_{AH}^{i,j} - p_{AH}^{i,j}$ can be used to analyze the influence of an imperfect CCC on the ability of the FC to identify MSUs. In order to calculate $P_{AH}^{i,j} - p_{AH}^{i,j}$, let us further denote $p_{M,j}$ and $P_{M,j}$ as the probabilities that the MSU SU_j reports a correct sensing result under perfect and imperfect CCCs, respectively. Similar to (9), it holds that

$$P_{M,j} = \mathcal{F}(p_{M,j}, P_{e,j}). \tag{10}$$

Then, based on p_H, $P_{H,i}$, $p_{M,j}$ and $P_{M,j}$, one can compute $p_{AH}^{i,j}$ and $P_{AH}^{i,j}$ as follows:

$$p_{AH}^{i,j} = p_H(1-p_{M,j}) + (1-p_H)p_{M,j} \tag{11}$$

and

$$P_{AH}^{i,j} = P_{H,i}(1-P_{M,j}) + (1-P_{H,i})P_{M,j}. \tag{12}$$

Considering (9)-(11), we can further write (12) as

$$\begin{aligned} P_{AH}^{i,j} &= \mathcal{F}(p_H, P_{e,i}) \cdot (1 - \mathcal{F}(p_{M,j}, P_{e,j})) \\ &\quad + (1 - \mathcal{F}(p_H, P_{e,i})) \cdot \mathcal{F}(p_{M,j}, P_{e,j}) \\ &= (1 - 2(P_{e,i} + P_{e,j}) + 4P_{e,i}P_{e,j}) \cdot (p_H(1-p_{M,j}) \\ &\quad + (1-p_H)p_{M,j}) + P_{e,i} + P_{e,j} - 2P_{e,i}P_{e,j} \\ &= (1 - 2(P_{e,i} + P_{e,j}) + 4P_{e,i}P_{e,j})\, p_{AH} \\ &\quad + P_{e,i} + P_{e,j} - 2P_{e,i}P_{e,j}. \end{aligned} \tag{13}$$

From (11) and (13), it results in

$$P_{AH}^{i,j} - p_{AH}^{i,j} = (1 - 2p_{AH}^{i,j})(P_{e,i} + P_{e,j} - 2P_{e,i}P_{e,j}). \tag{14}$$

In the context of CSS, there are two kinds of attacks: independent attack and cooperative attack [4], [8]. In the following two subsections, we will discuss how an imperfect CCC affects the ability of the FC to detect MSUs under these attacks. Note that in the presence of independent attack (resp. cooperative attack), $p_{M,j}$ in (10) and (11) will be denoted as $p_{MI,j}$ (resp. $p_{MC,j}$).

1) Impact under independent attack: In the case of independent attack, an MSU would report the sensing decision opposite to its own local sensing result with the probability of P_{mal}. For any MSU SU_j, the probability that it offers a correct sensing result via a perfect CCC is [4]:

$$p_{MI,j} = \mathcal{F}(p_H, P_{mal}). \tag{15}$$

Replacing $p_{M,j}$ in (11) with the above $p_{MI,j}$, one can get

$$\begin{aligned} p_{AH}^{i,j} &= p_H(1-p_{MI,j}) + (1-p_H)p_{MI,j} \\ &= p_H \cdot (1 - \mathcal{F}(p_H, P_{mal})) + (1-p_H) \cdot \mathcal{F}(p_H, P_{mal}) \\ &= 2p_H(1-p_H)(1-2P_{mal}) + P_{mal}. \end{aligned} \tag{16}$$

Considering the most harmful situation, i.e., $P_{mal} = 1$, it follows from (16) that $p_{AH}^{i,j} = -2p_H(1-p_H) + 1$. As stated in [4], p_H is close to 1. Thus one can verify that $p_{AH}^{i,j}$ is also close to 1, which leads to $1 - 2p_{AH}^{i,j} < 0$. Moreover, $P_{e,i} + P_{e,j} - 2P_{e,i}P_{e,j} \geq 0$ holds all the time. Hence, one can conclude from (14) that $P_{AH}^{i,j} - p_{AH}^{i,j} \leq 0$. This means that the difference of spectrum sensing histories between an HSU and an MSU under an imperfect CCC is smaller than that under a perfect CCC. Therefore, more MSUs may be considered as HSUs and thus escape from being detected. This would misguide the FC to make an incorrect final spectrum sensing decision.

2) Impact under cooperative attack: In the presence of cooperative attack, the MSUs exchange their sensing information to decide their response collaboratively and the collaboration strategy can be 'L out of M' [4], [8]. This strategy means that when L of the total M MSUs find that the spectrum is idle, all MSUs would report to the FC that the spectrum is occupied by the PU. Reversely, if the spectrum is found being occupied by the PU, the MSUs would report to the FC that the spectrum is available.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

According to [4] and [8], if all of the MSUs perform cooperative attack, the probability that any MSU $SU_j \in \mathcal{M}$ reports a correct sensing result through a perfect CCC is

$$p_{MC,j} = \mathcal{F}\left(\sum_{l=L}^{M}\binom{M}{l}p_H^l(1-p_H)^{M-l}, P_{mal}\right) \tag{17}$$

where

$$L = \min(M, \lceil M/(1+\nu)\rceil) \ \text{ with } \ \nu = \left(ln\frac{P_f}{P_d}\right)\left(\frac{1-P_d}{1-P_f}\right). \tag{18}$$

Using the above $p_{MC,j}$ to replace $p_{M,j}$ in (11), one can get

$$\begin{aligned} p_{AH}^{i,j} &= p_H(1-p_{MC,j}) + (1-p_H)p_{MC,j} \\ &= p_H \cdot \left(1 - \mathcal{F}\left(\sum_{l=L}^{M}\binom{M}{l}p_H^l(1-p_H)^{M-l}, P_{mal}\right)\right) \\ &\quad + (1-p_H)\cdot \mathcal{F}\left(\sum_{l=L}^{M}\binom{M}{l}p_H^l(1-p_H)^{M-l}, P_{mal}\right) \\ &= (p_H - 2p_H\sum_{l=L}^{M}\binom{M}{l}p_H^l(1-p_H)^{M-l} \\ &\quad + \sum_{l=L}^{M}\binom{M}{l}p_H^l(1-p_H)^{M-l})\cdot(1-2P_{mal}) + P_{mal}. \end{aligned} \tag{19}$$

Similar to the analysis under independent attack, in the most harmful case (i.e., $P_{mal} = 1$), p_H is close to 1. Thus, one can derive from (19) that $p_{AH}^{i,j}$ is also close to 1, giving $1-2p_{AH}^{i,j} < 0$. Also, since $P_{e,i} + P_{e,j} - 2P_{e,i}P_{e,j} \geq 0$, it can be concluded from (14) that $P_{AH}^{i,j} - p_{AH}^{i,j} \leq 0$. Due to this, more MSUs will be mistakenly identified as HSUs, which would cause the FC to make a wrong final spectrum sensing decision.

IV. Selection of Reputation Threshold

In the reputation-based methods for MSU detection, a reputation threshold is usually used for each SU. If the reputation value of an SU is not greater than the considered threshold, this SU is classified as an MSU; otherwise, it is categorized as an HSU. Obviously, the selection of a suitable reputation value threshold is crucial. In [8], a reputation value threshold is derived under the condition that the fraction of MSUs over all SUs is known. However, this condition is too restrictive to meet in practice. In [4], the reputation value threshold is set to 0.5. Since the reputation values obtained in [4] cannot be confined between 0 and 1, they can accumulate over time. Hence, setting the reputation threshold to 0.5 is not appropriate. Furthermore, when selecting the reputation threshold, the approaches in [4] and [8] only consider the case that the CCC is perfect. Next, we will derive a proper reputation threshold for each SU to facilitate the detection of MSUs under imperfect CCC and in the presence of attacks.

To proceed, let us consider the widely-used reputation value defined below.

Definition 1: [11], [33], [34]: The reputation value of SU_i, denoted by r_i, is the probability of reporting an accurate sensing result. It can be estimated by

$$r_i = \tau_i / T_w \tag{20}$$

where T_w is the recording time window and τ_i denotes the number of reports from SU_i which are identical to the final decisions of the FC during T_w.

It can be seen from Proposition 1, the calculation of r_i utilizes the local spectrum sensing decision history of SU_i. Further, let η_i be the reputation value threshold for SU_i and p_i denote the probability that SU_i reports a local sensing result identical to the final spectrum sensing decision. If SU_i is honest, $p_i = P_{H,i}$ where $P_{H,i}$ is given in (9). If SU_i is malicious, $p_i = P_{M,i}$ where $P_{M,i}$ is given in (10). As we previously mentioned, $p_{M,i}$ is denoted as $p_{MI,i}$ in the presence of independent attack, which leads to $P_{M,i} = \mathcal{F}(p_{MI,i}, P_{e,i})$. Similarly, $P_{M,i} = \mathcal{F}(p_{MC,i}, P_{e,i})$ under cooperative attack.

Let $z_i(t)$ denote the correctness of the local spectrum sensing results of SU_i at the tth time slot, and

$$z_i(t) = \begin{cases} 1 & SU_i \ \text{reports a correct sensing result} \\ 0 & \text{otherwise} \end{cases}.$$

Clearly, $P(z_i(t) = 1) = p_i$ and $P(z_i(t) = 0) = 1 - p_i$. Thus $z_i(t)$ follows the Bernoulli distribution. According to Definition 1, we have

$$r_i = \frac{\sum_{t=t_0}^{t_0+T_w-1} z_i(t)}{T_w} \tag{21}$$

where t_0 is the start time of the recording time window. Since $z_i(t)$ follows the Bernoulli distribution, it is shown in [35] that if T_w satisfies

$$T_w p_i \geq 10 \ \text{ and } \ T_w(1-p_i) \geq 10 \tag{22}$$

then r_i follows the normal distribution $N(p_i, p_i(1-p_i)/T_w)$. This property can be utilized to derive the reputation threshold.

Firstly, we need to find T_w satisfying (22). In this process, since the FC has no prior information of which SUs are malicious, it is reasonable for it to assume that all SUs are honest, which implies $p_i = P_{H,i}$. Based on (22), we can determine T_w as follows:

$$\begin{aligned} T_w = &min\{T_w : T_w P_{H,i} \geq 10 \text{ and } T_w(1-P_{H,i}) \geq 10 \\ &\text{for all } SU_i \in \mathcal{N}\}. \end{aligned} \tag{23}$$

Obviously, such T_w ensures $r_i \sim N(P_{H,i}, P_{H,i}(1-P_{H,i})/T_w)$.

Secondly, we derive the reputation threshold η_i for each SU_i, which will be discussed under two scenarios: SU_i is honest and SU_i is malicious. Let $erfc(x)$ denote the complementary error function defined as [35]

$$erfc(x) = \frac{2}{\sqrt{\pi}}\int_x^{+\infty} exp\left(-t^2\right) dt. \tag{24}$$

Then, under the first scenario, we have the following Proposition 1.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

Proposition 1: When SU_i is honest, if η_i satisfies

$$\frac{1}{2}\cdot erfc\left(\frac{\sqrt{T_w}(\eta_i - P_{H,i})}{\sqrt{2P_{H,i}(1-P_{H,i})}}\right) \geq 1-\epsilon \tag{25}$$

then the probability that SU_i is considered as an MSU is smaller than a predefined error rate ϵ.

Proof: See Appendix A.

Proposition 1 means that one can use a reputation threshold η_i satisfying (25) to detect an HSU and the detection error rate is ϵ, which is predefined. It is interesting to know that if this η_i is used to detect an MSU, what is the detection error probability? The following Proposition 2 answers this question.

Proposition 2: If η_i obtained from (25) is applied to an MSU, denoted by SU_i, the probability that SU_i is considered as an HSU is

$$P_{md} = \frac{1}{2}\cdot erfc\left(\frac{\sqrt{T_w}(\eta_i - P_{M,i})}{\sqrt{2P_{M,i}(1-P_{M,i})}}\right). \tag{26}$$

Proof: See Appendix B.

Clearly, the reputation threshold η_i should be properly selected to make P_{md} in (26) as small as possible. It can be seen from (24) that the complementary error function $erfc(x)$ is monotonic decreasing as x increases. In conjunction with (26), it is obvious that the larger η_i, the smaller P_{md}. Thus, based on Proposition 1 and Proposition 2, a proper value of η_i should be

$$\eta_i = max\left\{\eta_i^* : \frac{1}{2}\cdot erfc\left(\frac{\sqrt{T_w}(\eta_i^* - P_{H,i})}{\sqrt{2P_{H,i}(1-P_{H,i})}}\right) \geq 1-\epsilon\right\}. \tag{27}$$

As mentioned above, $erfc(x)$ is monotonic decreasing as x increases. Therefore, η_i should be the solution of the following equation:

$$\frac{1}{2}\cdot erfc\left(\frac{\sqrt{T_w}(\eta_i - P_{H,i})}{\sqrt{2P_{H,i}(1-P_{H,i})}}\right) = 1-\epsilon. \tag{28}$$

V. The R^2-CSS method

In this section, we present the R^2-CSS method. As is shown in Fig. 2, it consists of three processes: initialization, reputation threshold selection, and CSS.

A. Initialization

When the whole network begins to work, the FC knows the PU and the whole set of participating SUs, i.e., $\mathcal{N}$, in terms of their transmit powers (ρ_{PU} and ρ_is) and their distances to the FC (d_P and d_is). It also knows P_B, the probability that the PU is transmitting on the authorized spectrum, and $P_I = 1 - P_B$. Moreover, the FC can determine the path loss constant κ, the path loss exponent μ, the time bandwidth product w, the energy detection threshold λ and the Gaussian noise variance σ^2. Based on these initial parameters, some intermediate parameters can be obtained as follows:

- Compute P_d, P_f, $\bar{\gamma}_{FC}$, and $h_{PU,FC}$ by (1), (2), (3) and (4), respectively.
- Compute $P_{e,i}$, $\bar{\gamma}_i$, and h_i by (6), (7) and (8), respectively.
- Determine p_H and $P_{H,i}$ by (5) and (9), respectively.

Furthermore, the FC should initialize the error rate ϵ and the set of HSUs chosen to perform CSS, i.e., $\mathcal{N}_{ch}$. Here, $\mathcal{N}_{ch}$ is initialized as $\mathcal{N}_{ch} = \mathcal{N}$ because the FC does not know any reputation information about the SUs at this stage. When the reputation values of SUs are available, the FC would choose n_{ch} HSUs with the highest reputation values to construct $\mathcal{N}_{ch}$. The value of n_{ch} is determined by the FC according to practical situations.

B. Selecting Reputation Thresholds

In this process, the FC determines the reputation threshold for each SU_i. As shown in Section IV, this process involves two tasks:

- Determine the recording time window T_w according to (23).
- Use (28) to select the reputation threshold η_i for each SU_i.

While the first task is easy, the second task is not straightforward. Now, we explain the procedure in detail. From Proposition 1, it implies that solving (28) is equivalent to finding the reputation threshold η_i ensuring $Pr(r_i < \eta_i) = \epsilon$, where the reputation value r_i follows the normal distribution. Since the standard normal distribution of r_i is

$$\frac{r_i - P_{H,i}}{\sqrt{P_{H,i}(1-P_{H,i})/T_w}} \sim N(0,1) \tag{29}$$

then solving (28) is also equivalent to finding the reputation threshold η_i ensuring

$$Pr\left(\frac{r_i - P_{H,i}}{\sqrt{P_{H,i}(1-P_{H,i})/T_w}} < \frac{\eta_i - P_{H,i}}{\sqrt{P_{H,i}(1-P_{H,i})/T_w}}\right) = \epsilon. \tag{30}$$

Consequently, given ϵ, we can use the standard normal distribution chart to find the value of $\frac{\eta_i - P_{H,i}}{\sqrt{P_{H,i}(1-P_{H,i})/T_w}}$ such that (30) holds, from which the value of η_i can be determined. For example, assume $P_{H,i} = 0.7984$, $T_w = 50$ and $\epsilon = 0.025$. Then, (30) becomes $Pr\left(\frac{r_i - 0.7984}{0.057} < \frac{\eta_i - 0.7984}{0.057}\right) = 0.025$. According to the standard normal distribution chart, if $\epsilon = 0.025$, the value of $\frac{\eta_i - 0.7984}{0.057}$ should be -2, i.e., $Pr\left(\frac{r_i - 0.7984}{0.057} < -2\right) = 0.025$. Thus, from $\frac{\eta_i - 0.7984}{0.057} = -2$, it follows $\eta_i = 0.7984 - 2 \times 0.057 = 0.6844$.

C. CSS

When the network begins to work, no reputation values of the SUs are available. So, in the first round of CSS, all SUs are chosen to perform CSS, i.e., $\mathcal{N}_{ch} = \mathcal{N}$ as in Initialization. In this case, the FC collects the local spectrum sensing decisions from all SUs and then make a final spectrum sensing decision using the majority rule.

Starting from the second round of CSS, after collecting the local spectrum sensing decisions from all SUs, the FC exploits the local spectrum sensing decision history of each SU_i to compute its reputation value r_i by (20). If $r_i > \eta_i$, SU_i is considered as an HSU. Otherwise, SU_i is labeled as

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

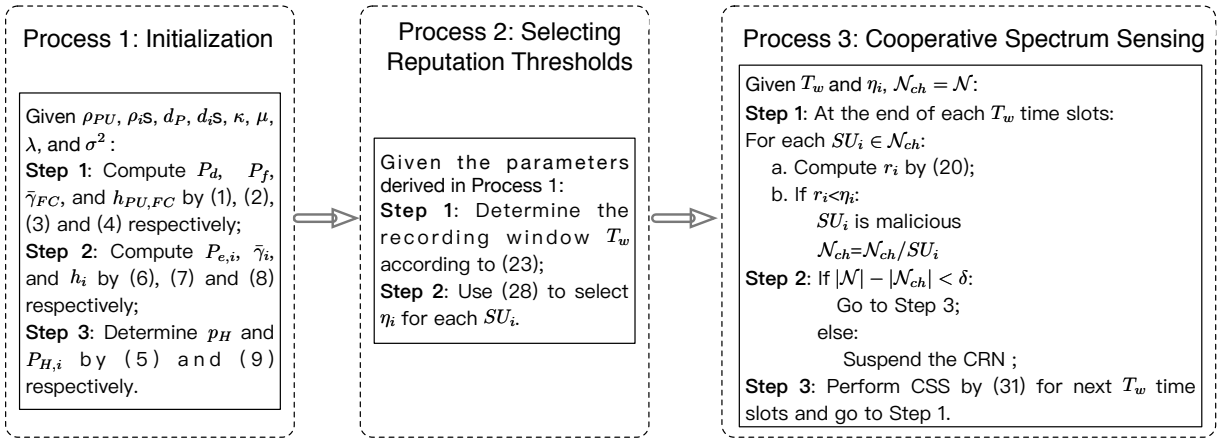


Fig. 2. The block diagram of R^2-CSS.

an MSU and will be removed from the network for next T_w time slots, followed by updating the SU set $\mathcal{N}$. Among the SUs in the updated set $\mathcal{N}$, the FC chooses n_{ch} of them at random to form the subset $\mathcal{N}_{ch}$ to perform CSS for next T_w time slots. This operation can prohibit the same collection of SUs from performing CSS all the time. Then, the FC makes a final spectrum sensing decision using the following weighted majority rule :

$$S = \sum_{SU_i \in \mathcal{N}_{ch}} r_i \cdot (0.5 - ld_i). \tag{31}$$

Here, ld_i denotes the local spectrum sensing decision of SU_i, which is either 0 or 1, as mentioned in Section III-A. If $S < 0$, the final spectrum sensing decision is 1; otherwise, the final spectrum sensing decision is 0. Note that after filtering out the SUs whose reputation values are lower than the related thresholds, the accuracy of the fusion results can be always achieved via the weighted majority rule when tuning n_{ch} carefully.

When the number of MSUs is large and thus the FC cannot always make correct spectrum sensing decisions, more HSUs would be judged as malicious ones because their reputation values computed by the FC would be decreased dramatically. Since HSUs form the majority of all the SUs, the total number of SUs judged as malicious ones could be very large. To alleviate the problem caused by a large number of MSUs, a parameter, denoted by δ is set. When the number of SUs judged as MSUs exceeds δ, the whole network should be suspended and a deeper check on each SU should be done by the owner of the network.

VI. Performance Analysis

In this section, we first analyze Scenario 1 where the number of MSUs and their P_{mal} values keep unchanged all the time, and derive the value of parameter δ. Then, we analyze Scenario 2 where HSUs can change to be malicious and explain how our method defend against attacks in this case.

A. Analysis for Scenario 1

As stated in Section V, all the SUs participate in CSS during the first T_w time slots after the whole network is set up since there is no prior reputation information about the SUs. After that, the SUs with lower reputation values than the related thresholds are filtered out as MSUs and n_{ch} SUs are randomly chosen from the remaining to perform CSS for next T_w time slots. Since the number of MSUs and their P_{mal} values keep unchanged all the time in this scenario, the only chance for MSUs to disrupt the whole network is to launch independent or cooperative attacks during the first T_w time slots so that the FC would always make wrong spectrum sensing decisions and filter out more HSUs as malicious ones.

Due to the fact that all the SUs participate in CSS and the FC derives final decisions by the majority rule during the first T_w time slots, the collection of MSUs, $\mathcal{M}$, can greatly influence the probability that the FC makes correct decisions. Let P_A denote such a probability. It can be computed as in (32):

$$\begin{aligned} &P_A(\mathcal{M}) \\ &= \sum_{i=\lfloor N/2 \rfloor+1}^{N} \Big(\sum_{j=0}^{M} \sum_{\substack{\mathcal{M}_c \in \mathcal{M} \\ |M_c|=j}} \prod_{k \in \mathcal{M}_c} P_{M,k} \prod_{u \in \mathcal{M}/\mathcal{M}_c} (1 - P_{M,u})\Big) \\ &\cdot \Big(\sum_{v=i-j}^{N-M} \sum_{\substack{\mathcal{N}_c \in \mathcal{N}/\mathcal{M} \\ |\mathcal{N}_c|=v}} \prod_{x \in \mathcal{N}_c} P_{H,x} \prod_{y \in \mathcal{N}/(\mathcal{M} \cup \mathcal{N}_c)} (1 - P_{H,y})\Big) \end{aligned} \tag{32}$$

where $P_{H,x}$ and $P_{H,y}$ are computed via (9). If under independent attack, $P_{M,k} = \mathcal{F}(p_{MI,k}, P_{e,k})$ where $p_{MI,k}$ is computed by (15). If under cooperative attack, $P_{M,k} = \mathcal{F}(p_{MC,k}, P_{e,k})$ where $p_{MC,k}$ is computed by (17). In both cases, $P_{e,k}$ is computed by (6).

When the probability that the FC makes correct spectrum sensing results is 0.5 under independent or cooperative attack, the ability of the FC to differentiate MSUs from HSUs is no better than guessing by flipping a coin. So, the whole network is considered as disrupted when such a probability (P_{IA} or P_{CA}) reaches 0.5. Let LDB_{IA} and LDB_{CA} be the lower bound of the number of MSUs to disrupt the whole network.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

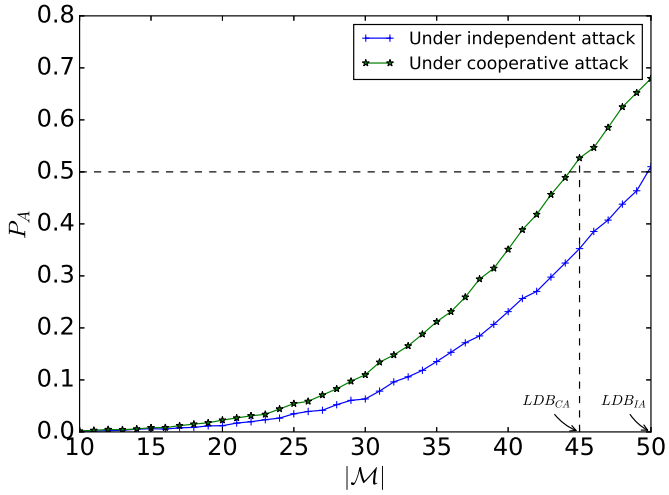


Fig. 3. P_A versus $|\mathcal{M}|$ ($N = 100$, $P_B = 0.6$, $P_I = 0.4$, $P_d = 0.9$, $P_f = 0.1$, $\rho_i = 10$ mW, $\sigma^2 = -90$dBm, $\mu = 3$ and $\kappa = 1$).

On the basis of (32), LDB_{IA} and LDB_{CA} can be computed as follow:

$$LDB_{IA} = min\{|\mathcal{M}| : P_A(\mathcal{M}, P_{M,k} = \mathcal{F}(p_{MI,k}, P_{e,k})) \geq 0.5\} \tag{33}$$

and

$$LDB_{CA} = min\{|\mathcal{M}| : P_A(\mathcal{M}, P_{M,k} = \mathcal{F}(p_{MC,k}, P_{e,k})) \geq 0.5\} \tag{34}$$

In practice, the FC has no idea about which SUs are honest or which are malicious. The FC can estimate LDB_{IA} and LDB_{CA} with the assumption that all the SUs are at the same place from which the distance to the FC is half of that from the FC to the farthest SU. Then, LDB_{IA} and LDB_{CA} can be estimated via numerical methods to satisfy (33) and (34) respectively. After that, the FC can set $\delta = min\{LDB_{IA}, LDB_{CA}\}$. Once the number of SUs judged as malicious ones exceeds δ, the whole network can be considered as disrupted and should be suspended to have a thorough check. For instance, Fig. 3 shows P_A versus $|\mathcal{M}|$ under both independent and cooperative attacks, where $N = 100$, $P_B = 0.6$, $P_I = 0.4$, $P_d = 0.9$, $P_f = 0.1$, $\rho_i = 10$ mW, $\sigma^2 = -90$dBm, $\mu = 3$ and $\kappa = 1$. According to Fig. 3, it is easy to obtain $LDB_{IA} = 50$ and $LDB_{CA} = 45$ via (33) and (34) respectively. Thus, $\delta = min\{50, 45\} = 45$.

B. Analysis for Scenario 2

In this scenario, the number of MSUs and their P_{mal} values can change over time. This may occur when some HSUs are compromised by attackers and then act as malicious ones. As stated in Section V, after filtering out the SUs whose reputation values are lower than their related thresholds, n_{ch} of the remaining SUs are chosen randomly to perform CSS for next T_w time slots via a weighted majority rule. If just a small proportion of HSUs become malicious suddenly, the probability that these SUs are chosen for CSS is small. Thus, the FC can always make correct spectrum sensing decisions and at the end of current round, the reputation values of these SUs can be very low and thus would be filtered out. In this scenario, attackers can disrupt the network by compromising at least half of the entire SUs. If so, no security countermeasures can deal with this problem. When the number of the compromised HSUs is not large but the probability that the FC makes correct decisions is influenced greatly by such behavior, many HSUs can be judged as MSUs and thus the total number of SUs judged as malicious ones would increase rapidly. Once this number exceeds δ, the network would be suspended to have a thorough check by the owner of the network. In this way, the harmful influence in this scenario can be alleviated.

VII. Simulation Results

In this section, simulation examples are provided to illustrate the performance of the proposed R^2-CSS method, in comparison with the reputation-based CSS methods in [4] and [8]. In our simulations, we consider a network scenario similar to [13], where 100 SUs (i.e., $N = 100$) are randomly distributed in an area of 5km $\times$ 5km, the FC is located at the center of this area, and the distance between the FC and the PU is 20km. Besides, we set the PU transmit power $\rho_{PU} = 100$mW, the SU transmit power $\rho_i = 10$ mW, $\forall i \in N$, the noise variance $\sigma^2 = -90$ dBm, the pair of path loss $\mu = 3$ and $\kappa = 1$, the energy detection threshold $\lambda = 0.01$. We also set $P_{mal} = 1$, i.e., in the case of independent attack, each MSU would report the sensing decision opposite to its own local sensing result.

Three performance metrics, Q_E, Q_D and Q_F, are used to evaluate the effectiveness of the proposed method, which are the probability that the FC makes a wrong final spectrum sensing decision, the probability that an MSU is detected correctly, and the probability that an HSU is misidentified as an MSU, respectively. These performance metrics can be calculated as follows:

$$Q_E = \frac{\text{Number of incorrect decisions}}{T_{win}} \tag{35}$$

$$Q_D = \frac{\text{Number of MSUs detected}}{\text{Total number of MSUs}} \tag{36}$$

$$Q_F = \frac{\text{Number of HSUs misidentified}}{\text{Total number of HSUs}}. \tag{37}$$

Clearly, the smaller Q_E and Q_F and larger Q_D, the better.

A. Impact of n_{ch} on CSS performance

In the proposed R^2-CSS method, n_{ch} SUs are randomly chosen by the FC to perform CSS after filtering out the SUs whose reputation values are lower than their related thresholds. In this simulation, we evaluate the influence of n_{ch} on CSS performance by varying the values of n_{ch} from 5 to 30, in the presence of different number of MSUs ($M = 10$, 20, 30 and 40, respectively). The MSUs could launch both independent and cooperative attacks. Figs. 4 and 5 show the CSS performance metrics Q_E, Q_D and Q_F versus n_{ch} under independent and cooperative attacks, respectively. It can be seen that in general, the larger n_{ch}, the better CSS performance (i.e. the smaller Q_E and Q_F, and the larger Q_D).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology

The advantage of using more SUs (i.e., larger n_{ch}) for CSS is more evident with the increase of attacks (i.e., with the increase of M). This is expected because when more SUs are employed in CSS, the R^2-CSS method can be more robust against attacks due to the weighted majority rule used to derive final spectrum sensing decisions. When n_{ch} exceeds 20, the performance improvement with respect to Q_E, Q_D and Q_F as n_{ch} increases is not as obvious as that when $n_{ch} < 20$. On the other hand, the R^2-CSS method resists both independent and cooperative attacks very well in the cases of $M = 10$ and 20. While further increasing M will deteriorate the CSS performance, the negative impact of cooperative attack on CSS is more severe than that caused by independent attack. In the following simulations, n_{ch} is set to 20.

B. The Effect of Different P_{mal}

One may wonder whether there exist some strategies for MSUs by tuning P_{mal} carefully to avoid being detected by the FC. In this subsection, we evaluate the influence of P_{mal} on CSS performance by varying the values of P_{mal} from 0.2 to 1.0 with a step size of 0.2, under both independent and cooperative attacks. Here, we set $\epsilon = 0.025$ to derive the reputation value thresholds.

Figs. 6 and 7 show the CSS performance metrics Q_E, Q_D and Q_F versus M, where M the number of MSUs, under these two kinds of attacks with different P_{mal} values. Generally, one can see that the larger P_{mal}, the larger Q_E (i.e., worse CSS performance). This is understandable as P_{mal} can reflect the frequency of MSUs launching attacks and thus the CSS performance would be obviously degraded when MSUs launch attacks persistently. In addition, from Fig. 6b and Fig. 7b, the smaller P_{mal}, the smaller Q_D (i.e., more MSUs escape from detection). This is because MSUs act more similarly to HSUs when P_{mal} decreases. However, when P_{mal} is not 1.0, R^2-CSS can always keep Q_E (Fig. 6a & Fig. 7a) and Q_F (Fig. 6c & Fig. 7c) in a low level under both independent and cooperative attacks. This indicates that when P_{mal} is not 1.0, the proposed method can guarantee the FC to always make correct spectrum sensing decisions and constrain the number of HSUs to be filtered out under an accepted rate. The only chance to disrupt the whole network is to set P_{mal} to 1.0 and make as many MSUs as possible to launch independent or cooperative attacks, i.e. in this case, dramatical CSS performance degration can be caused when the number of MSUs reaches 45 and 35 under independent and cooperative attacks respectively.

Note that when some MSUs perform independent attacks and the other MSUs perform cooperative attacks, Figs. 6 and 7 present the lower and upper bounds of the influence of P_{mal} values referring to the three CSS performance metrics. In the following two subsections, we set $P_{mal} = 1$ and compare the effectiveness of R^2-CSS with the methods proposed in [4] and [8] under independent and cooperative attacks separately.

C. Performance Comparison under Independent Attacks

In this subsection, the performance of the R^2-CSS method, in terms of Q_E, Q_D and Q_F, is compared with those of the methods in [4] and [8], under independent attacks. In the simulation, we set $\epsilon = 0.025$. Besides, both perfect and imperfect CCCs are considered.

Fig. 8 shows Q_E, Q_D and Q_F versus M under independent attacks, where the CCC is imperfect. One can see that the R^2-CSS method and the method in [4] significantly outperform the method in [8] according to the metrics Q_E and Q_F, so long as the number of MSUs is not too large. With respect to the metric Q_D, the R^2-CSS method and the method in [8] have similar performance, and both of them outperform the method in [4] by large margins. Importantly, the R^2-CSS method performs the best in all situations. These simulation results are not surprising. As we previously mentioned, the methods in [4] and [8] require perfect CCC but this assumption does not hold in this case, which leads to performance degradation. Furthermore, the method in [8] requires that the fraction of MSUs over all SUs is known to the FC. While this condition is not satisfied, many HSUs will be incorrectly classified as MSUs (see Fig. 3(c)). This will reduce the number of HSUs used to perform CSS, resulting in poor CSS performance (see Fig. 3(a)). Also, this will cause those HSUs incorrectly classified as MSUs being removed from the network. On the other hand, while performing MSU detection, the method in [4] fixes the reputation value threshold to 0.5, which is not appropriate as the reputation value obtained in [4] can accumulate over time. As a result, a portion of MSUs cannot be detected (see Fig. 3(b)). This implies that some of these MSUs might be used for CSS, which decreases the CSS performance (see Fig. 3(a)). In contrast, the R^2-CSS method does not have these problems. Consequently, its overall performance is much better than that of [4] and [8].

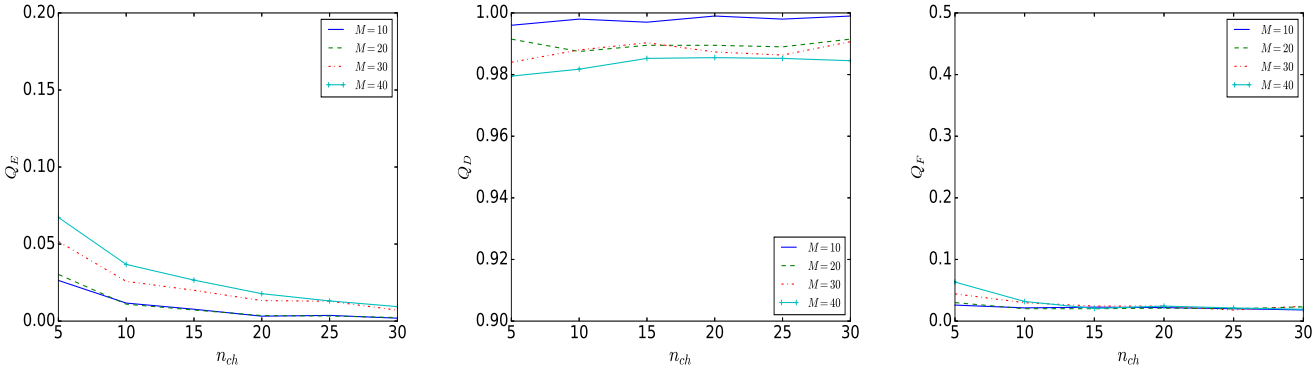
Fig. 9 shows the simulation results for the case that the CCC is perfect. Although the performance margins between the R^2-CSS method and the methods in [4] and [8] are narrowed, the overall performance of the R^2-CSS method is still much superior to that of the other two methods.

D. Performance Comparison under Cooperative Attacks

In this simulation, we evaluate the three methods under cooperative attacks, where $\epsilon = 0.025$. Fig. 10 shows their performance in the case of imperfect CCC. By comparing Fig. 10 with Fig. 8, it is obvious that the performance of all methods degrades under cooperative attacks. This is understandable as cooperative attacks are generally more severe than independent attacks. Nevertheless, one can see from Fig. 10 that when M is about 40 or smaller, the R^2-CSS method performs very well according to all three performance metrics Q_E, Q_D and Q_F, and significantly outperforms the methods in [4] and [8]. When M exceeds 40, all three methods fail to achieve satisfactory performance.

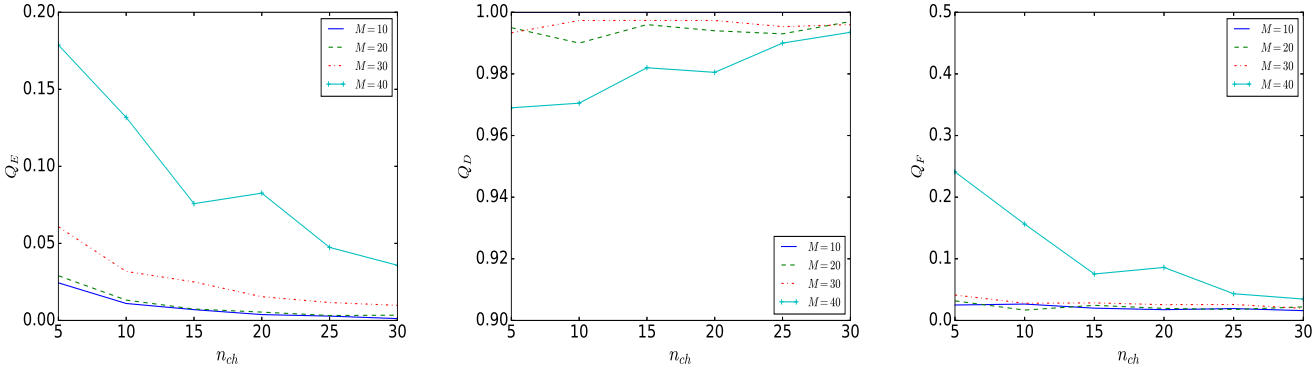
Fig. 11 shows the performance of the three methods in the case of perfect CCC. We can see that in terms of Q_E and Q_F, while the methods in [4] and [8] fail at $M = 33$ or smaller, the R^2-CSS method fails when M reaches the much greater value of 45. Regarding Q_D, the methods in [4] and [8] start to break down at M smaller than 35, but the R^2-CSS method performs perfectly for all M values considered.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology



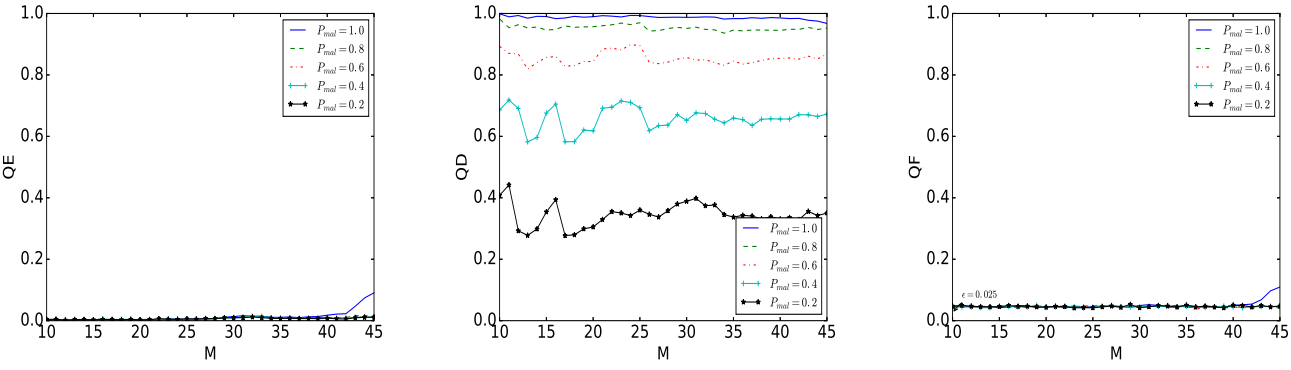
(a) (b) (c)

Fig. 4. Q_E, Q_D and Q_F versus n_{ch} under independent attacks, where four different M values are considered and $N = 100$.



(a) (b) (c)

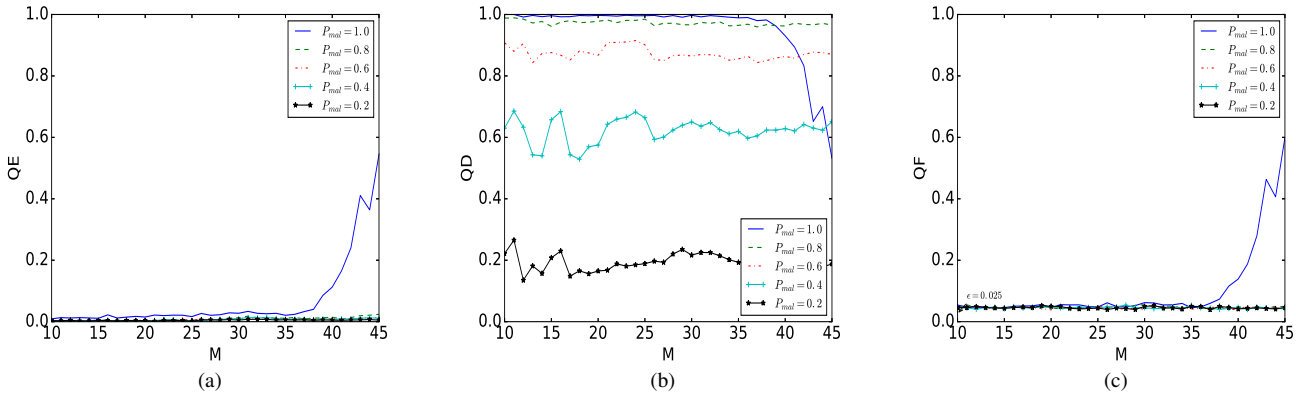
Fig. 5. Q_E, Q_D and Q_F versus n_{ch} under cooperative attacks, where four different M values are considered and $N = 100$.



(a) (b) (c)

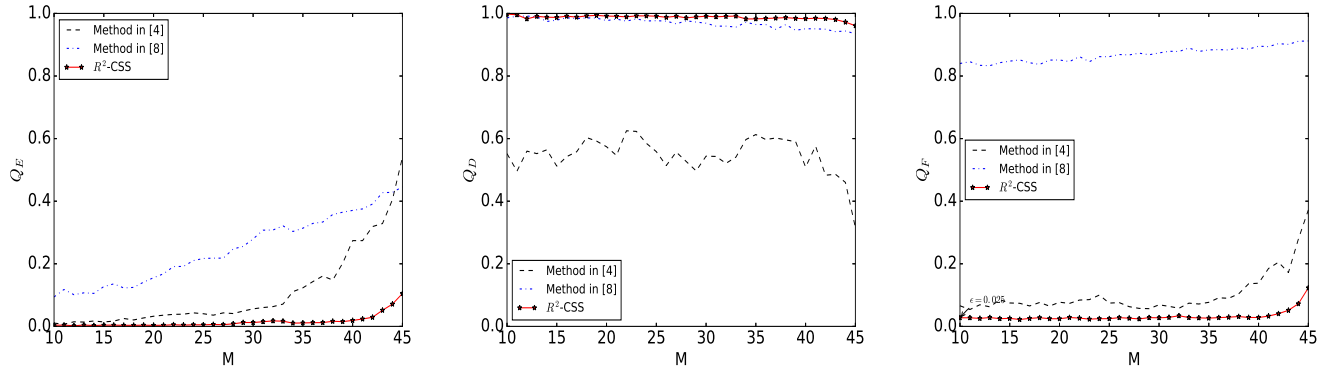
Fig. 6. Q_E, Q_D and Q_F versus M under independent attacks, where P_{mal} is from 0.2 to 1.0.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology



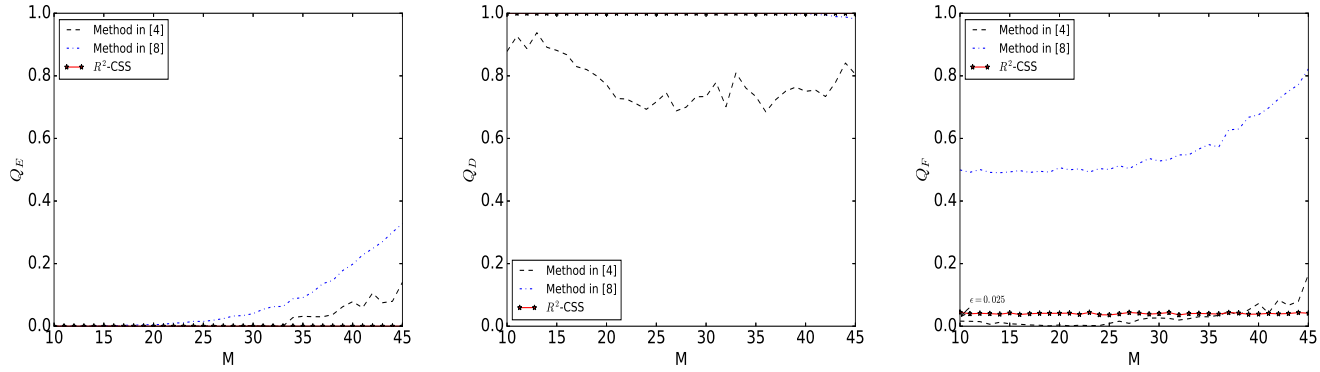
(a) (b) (c)

Fig. 7. Q_E, Q_D and Q_F versus M under cooperative attacks, where P_{mal} is from 0.2 to 1.0.



(a) (b) (c)

Fig. 8. Q_E, Q_D and Q_F versus M under independent attacks, where the CCC is imperfect.



(a) (b) (c)

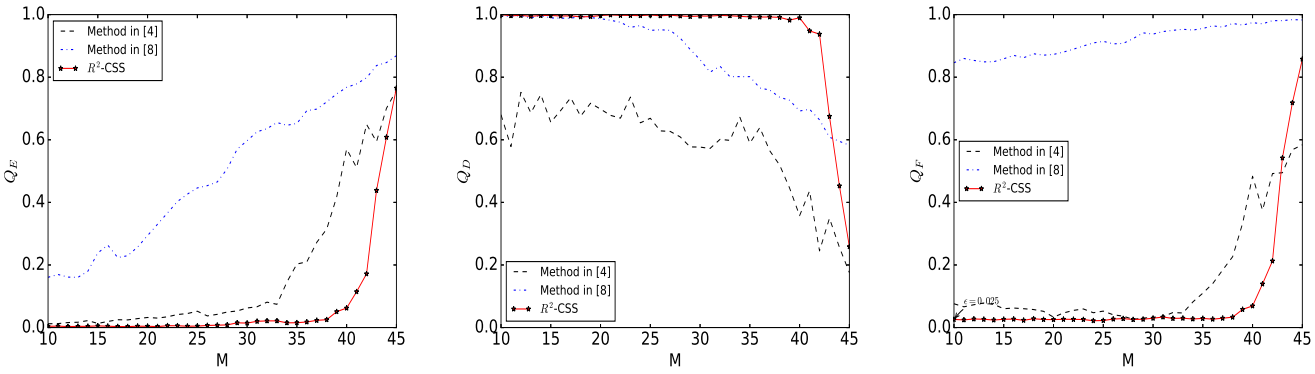
Fig. 9. Q_E, Q_D and Q_F versus M under independent attacks, where the CCC is perfect.

Besides, it is interesting to see from Fig. 11 that when the CCC is perfect, the influence of cooperative attacks on the three methods appears in a sharper manner, in terms of Q_E and Q_F. The reason is that under a perfect CCC, the effect of cooperative attacks will be reflected more accurately due to the lossless exchange of control messages between the FC and the SUs.

E. Performance Comparison under Mixed Attacks

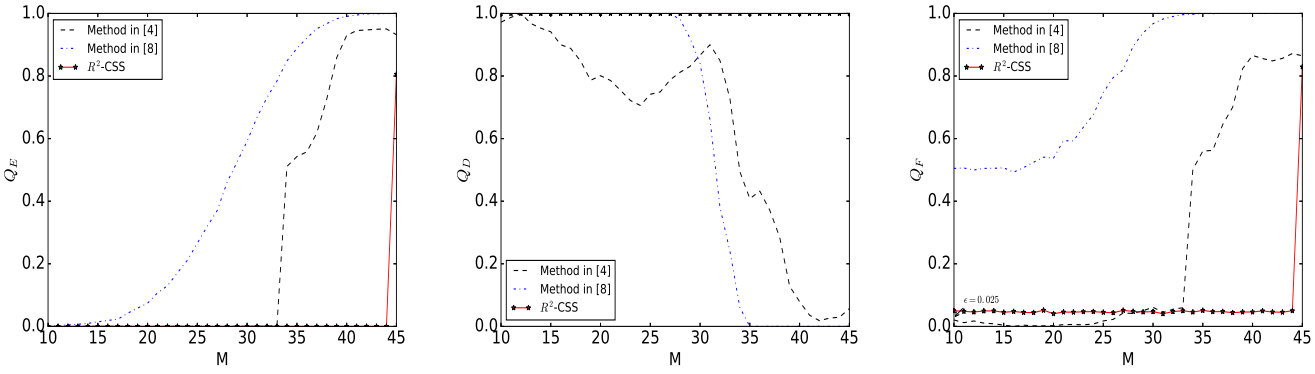
After verifying the effectiveness of the R^2-CSS method under both independent and cooperative attacks, one may wonder whether it is still effective under mixed attacks where some MSUs perform independent attacks and the remaining MSUs perform cooperative attacks. Let ζ denote the ratio of the number of MSUs performing cooperative attacks over the total number of MSUs. In this subsection, the performance of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology



(a) (b) (c)

Fig. 10. Q_E, Q_D and Q_F versus M under cooperative attacks, where the CCC is imperfect.



(a) (b) (c)

Fig. 11. Q_E, Q_D and Q_F versus M under cooperative attacks, where the CCC is perfect.

the proposed method is compared with that of the methods in [4] and [8] by varying ζ from 0.2 to 0.8 with a step size of 0.2. Since the influence of mixed attacks is not evident when the total number of MSUs is too small and all the methods may fail when this number is too large, we set the total number of MSUs $M = 30$. Besides, $\epsilon = 0.025$.

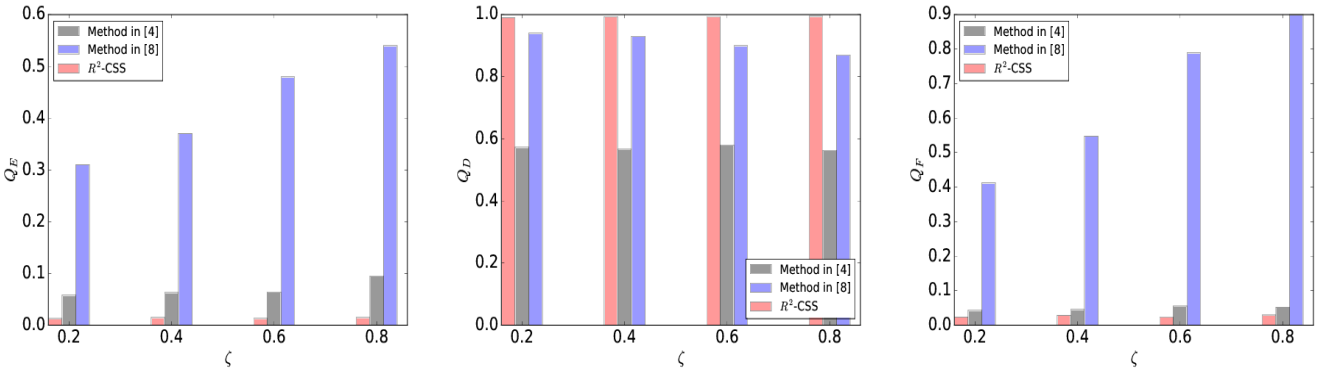
Fig. 12 shows Q_E, Q_D and Q_F versus ζ. It is obvious that the R^2-CSS method and the method in [4] outperform the method in [8] with respect to the metrics Q_E and Q_F with the R^2-CSS method performing the best (see Figs. 12a and 12c). In terms of the metric Q_D, the R^2-CSS method also outperforms the other two methods (see Fig. 12b). This is similar to the case under independent or cooperative attacks. We can also see that the effectiveness of the method in [8] degrades as ζ increases while that of the R^2-CSS method or the method in [4] keeps stable. This is because when the total number of MSUs is constant, the influence of MSUs becomes greater as ζ increases and the worst case is when under cooperative attacks. By a further checking, Q_Es, Q_Ds and Q_Fs of these three methods fall in the ranges determined under independent and cooperative attacks respectively. Since the performance of the R^2-CSS method or the method in [4] is very similar under both independent and cooperative attacks, it is not surprising to find that the effectiveness of these two methods keeps stable when ζ varies.

In summary, the R^2-CSS method has the best performance in all situations. In other words, no matter under independent, cooperative, or mixed attacks, the R^2-CSS method can be always superior to that of the other two methods.

VIII. Conclusion

In this paper, we first analyzed the impact of imperfect CCC on the identification of MSUs. Our analysis showed that under an imperfect CCC, more HSUs could be mistakenly identified as MSUs, causing the FC to make incorrect final spectrum sensing decisions. To solve this problem, we derived a novel reputation value threshold for each SU, which can help better differentiate HSUs and MSUs. Built upon the derived reputation threshold, we developed a new reputation-based CSS method, called R^2-CSS method, in which the SUs with higher reputation values are chosen to perform CSS. The R^2-CSS method is robust against independent and cooperative attacks under both imperfect and perfect CCCs. Extensive simulations were carried out to compare the performance of the proposed method and the reputation-based CSS methods in [4] and [8]. Simulation results demonstrated the superior performance of our method.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2763980, IEEE Transactions on Vehicular Technology



(a) (b) (c)

Fig. 12. Q_E, Q_D and Q_F versus ζ, where $M = 30$ and $\epsilon = 0.025$.

APPENDIX A
PROOF OF PROPOSITION 1

Proof: Given that the FC always makes correct decisions [4] and

$$r_i \sim N(P_{H,i}, P_{H,i}(1-P_{H,i})/T_w) \tag{38}$$

the probability density function of r_i, denoted by $f_{H,i}(x)$, can be expressed as

$$f_{H,i}(x) = \frac{\sqrt{T_w}}{\sqrt{2\pi P_{H,i}(1-P_{H,i})}} \cdot exp\left(-\frac{T_w(x-P_{H,i})^2}{2P_{H,i}(1-P_{H,i})}\right). \tag{39}$$

Thus, we have

$$\begin{aligned}
&\int_{-\infty}^{\eta_i} f_{H,i}(x)dx \\
&= \int_{-\infty}^{\eta_i} \frac{\sqrt{T_w}}{\sqrt{2\pi P_{H,i}(1-P_{H,i})}} \cdot exp\left(-\frac{T_w(x-P_{H,i})^2}{2P_{H,i}(1-P_{H,i})}\right) dx \\
&= 1 - \int_{\eta_i}^{+\infty} \frac{\sqrt{T_w}}{\sqrt{2\pi P_{H,i}(1-P_{H,i})}} \cdot exp\left(-\frac{T_w(x-P_{H,i})^2}{2P_{H,i}(1-P_{H,i})}\right) dx \\
&= 1 - \frac{1}{\sqrt{\pi}} \int_{\frac{\sqrt{T_w}(\eta_i - P_{H,i})}{\sqrt{2P_{H,i}(1-P_{H,i})}}}^{+\infty} exp\left(-y^2\right) dy \\
&= 1 - \frac{1}{2} \cdot erfc\left(\frac{\sqrt{T_w}(\eta_i - P_{H,i})}{\sqrt{2P_{H,i}(1-P_{H,i})}}\right).
\end{aligned} \tag{40}$$

From (25) and (40), it is easy to see that $\int_{-\infty}^{\eta_i} f_{H,i}(x)dx \leq \epsilon$, i.e., the probability of $r_i < \eta_i$ is at most ϵ. This ensures that the probability that SU_i is considered as an MSU is smaller than ϵ. This completes the proof. ■

APPENDIX B
PROOF OF PROPOSITION

Proof: Recall that when SU_i is malicious, we have $p_i = P_{M,i}$, where $P_{M,i} = \mathcal{F}(p_{MI,i}, P_{e,i})$ under independent attack and $P_{M,i} = \mathcal{F}(p_{MC,i}, P_{e,i})$ under cooperative attack. According to (23), T_w is derived assuming that all the SUs are honest. However, when the range the network is large enough and SUs are distributed randomly in this area, $T_w P_{M,i} \geq 10$ and $T_w(1-P_{M,i}) \geq 10$ can be considered as right since all the SUs are considered to derive T_w in (23). Thus, $r_i \sim N(P_{M,i}, P_{M,i}(1-P_{M,i})/T_w)$. The probability density function of r_i, denoted by $f_{M,i}(x)$, is

$$f_{M,i}(x) = \frac{\sqrt{T_w}}{\sqrt{2\pi P_{M,i}(1-P_{M,i})}} \cdot exp\left(-\frac{T_w(x-P_{M,i})^2}{2P_{M,i}(1-P_{M,i})}\right). \tag{41}$$

If SU_i is considered to be honest, this means that $r_i > \eta_i$. So, P_{md} can be computed by

$$P_{md} = \int_{\eta_i}^{+\infty} f_{M,i}(x)dx. \tag{42}$$

Similar to the proof of Proposition 1 and on the basis of (24), (41) and (42), one can obtain (26). This completes the proof. ■

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundations of China (No. U1636209, No. 61672350, No. 61373170) and in part by the National Key Research and Development Program of China under Grant 2016YFB0800601. Also, L. Ma is supported by China Scholarship Council (CSC).

REFERENCES

[1] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 116-130, Mar. 2009.

[2] F. S. P. T. Force, "Report of the spectrum efficiency working group," no. 03-237, Nov. 2002.

[3] L. Zhang, C. Fang, Y. Li, H. Zhu, and M. Dong, "Optimal strategies for defending location inference attack in database-driven CRNs," in *Proceedings of 2015 IEEE International Conference on Communications*, London, UK, Jun. 2015, pp. 7640-7645.

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

[5] B. F. Lo, "A survey of common control channel design in cognitive radio networks," *Physical Communication*, vol. 4, no. 1, pp. 26-39, Mar. 2011.

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

[7] S. Li, H. Zhu, Z. Gao, X. Guan and K. Xing, "YouSense: Mitigating entropy selfishness in distributed collaborative spectrum sensing," in *Proceedings of the 32nd IEEE International Conference on Computer Communications*, Turin, Italy, Apr. 2013, pp. 2535-2543.

[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 Transactions on Signal Processing*, vol. 59, no. 2, pp. 774-786, Feb. 2011.

[9] Y. Cai, L. Cui, K. Pelechrinis, P. Krishnamurthy, M. B. Weiss, and Y. Mo, "Decoupling trust and wireless channel induced effects on collaborative sensing attacks," in *Proceedings of 2014 IEEE International Symposium on Dynamic Spectrum Access Networks*, McLean, VA, USA, Apr. 2014, pp. 464-469.

[10] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Thwarting intelligent malicious behaviors in cooperative spectrum sensing," *IEEE Transactions on Mobile Computing*, vol. 14, no. 11, pp. 2392-2405, Nov. 2015.

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

[12] I. Konno, H. Nishiyama, and N. Kato, "An adaptive media access control mechanism for cognitive radio," *IEICE Transactions on Communications*, vol. J94-B, no. 2, pp. 253-263, Feb. 2011.

[13] W. Saad, Z. Han, T. Basar, M. Debbah, and A. Ørungnes, "Coalition formation games for collaborative spectrum sensing," *IIEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 276–297, Jan. 2011.

[14] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Transactions on Communications*, vol. 55, no. 1, pp. 21-24, Jan. 2007.

[15] T. Ngo, H. Nishiyama, N. Kato, T. Sakano, and A. Takahara, "A spectrum- and energy-efficient scheme for improving the utilization of MDRU-based disaster resilient networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2027-2037, Jun. 2014.

[16] H. Tang, "Some physical layer issues of wide-band cognitive radio systems," in *Proceedings of 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Baltimore, MD, USA, Nov. 2005, pp. 151-159.

[17] K. Kim, I. A. Akbar, K. K. Bae, J.-S. Um, C. M. Spooner, and J. H. Reed, "Cyclostationary approaches to signal detection and classification in cognitive radio," in *Proceedings of 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, Ireland, Apr. 2007, pp. 212-215.

[18] T. Yucek and H. Arslan, "Spectrum characterization for opportunistic cognitive radio systems," in *Proceedings of 25th IEEE Military Communications Conference*, Washington, DC, USA, Oct. 2006, pp. 1-6.

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

[20] W. Zhang, Y. Yang, and C. K. Yeo, "Cluster-based cooperative spectrum sensing assignment strategy for heterogeneous cognitive radio network," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2637-2647, Jul. 2015.

[21] S. Maleki, G. Leus, S. Chatzinotas, and B. Ottersten, "To AND or to OR: on energy-efficient distributed spectrum sensing with combined censoring and sleeping," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4508-4521, Aug. 2015.

[22] A. Ebrahimzadeh, M. Najimi, S. M. H. Andargoli, and A. Fallahi, "Sensor selection and optimal energy detection threshold for efficient cooperative spectrum sensing," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 4, pp. 1565-1577, Apr. 2015.

[23] W. Zhang, Y. Guo, H. Liu, Y. Chen, Z. Wang, and J. Mitola, "Distributed consensus-based weight design for cooperative spectrum sensing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 1, pp. 54-64, Jan. 2015.

[24] Z. Dai, J. Liu, and K. Long, "Selective-reporting-based cooperative spectrum sensing strategies for cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 7, pp. 3043-3055, Jul. 2015.

[25] M. Najimi, A. Ebrahimzadeh, S. M. Hosseini Andargoli, and A. Fallahi, "Energy-efficient sensor selection for cooperative spectrum sensing in the lack or partial information," *IEEE Sensors Journal*, vol. 15, no. 7, pp. 3807-3818, Jul. 2015.

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

[27] E. Soltanmohammadi and M. Naraghi-Pour, "Fast detection of malicious behavior in cooperative spectrum sensing," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 377-386, Mar. 2014.

[28] H. Zhu, C. Fang, Y. Liu, C. Chen, M. Li and X. S. Shen, "You can jam but you cannot hide: defending against jamming attacks for geo-location database driven spectrum sharing," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2723-2737, Sep. 2016.

[29] Z. M. Fadlullah, H. Nishiyama, N. Kato, and M. M. Fouda, "Intrusion detection system (IDS) for combating attacks against cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 51-56, Jun. 2013.

[30] Z. Gao, H. Zhu, Y. Liu, M. Li and Z. Cao, "Location privacy in database-driven cognitive radio networks: attacks and countermeasures," in *Proceedings of the 32nd IEEE International Conference on Computer Communications*, Turin, Italy, Apr. 2013, pp. 2751-2759.

[31] R. Zhang, J. Zhang, Y. Zhang and C. Zhang, "Secure crowdsourcing-based cooperative spectrum sensing," in *Proceedings of the 32nd IEEE International Conference on Computer Communications*, Turin, Italy, Apr. 2013, pp. 2526-2534.

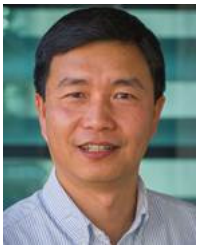
[32] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416-424, Jan. 2016.

[33] B. Sonja and L. B. Jean, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in *Proceedings of 2003 International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, INRIA Sophia-Antipolis, France, Mar. 2003, pp. 1-10.

[34] Y. L. Sun, H. Zhu, Y. Wei, and K. R. Liu, "Attacks on trust evaluation in distributed networks," in *Proceedings of the 40th Annual Conference on Information Sciences and Systems*, Princeton, NJ, USA, Mar. 2006, pp. 1461-1466.

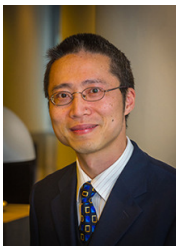
[35] D. R. Anderson, D. J. Sweeney, T. A. Williams, J. D. Camm, and J. J. Cochran, *Statistics for business and economics*, INelson Education, 2016.

Lichuan Ma received his B.S. degrees in Information Security from the School of Mathematics, Shandong University, in 2012. He is currently pursuing the Ph.D degree in information security at Xidian University. His research interests focus on wireless networks and security.



Yong Xiang (IEEE SM'12) received the Ph.D. degree in Electrical and Electronic Engineering from The University of Melbourne, Australia. He is a Professor and the Director of the Artificial Intelligence and Data Analytics Research Cluster, School of Information Technology, Deakin University, Australia. His research interests include information security and privacy, multimedia (speech/image/video) processing, wireless sensor networks and IoT, and biomedical signal processing. He has published 2 monographs, over 90 refereed journal articles, and numerous conference papers in these areas. He is an Associate Editor of IEEE Signal Processing Letters and IEEE Access. He has served as Program Chair, TPC Chair, Symposium Chair, and Session Chair for a number of international conferences.

Qingqi Pei received his B.S., M.S. and Ph.D. degrees in Computer Science and Cryptography from Xidian University, in 1998, 2005 and 2008, respectively. He is now a Professor and member of the State Key Laboratory of Integrated Services Networks, also a Professional Member of ACM and Senior Member of IEEE, Senior Member of Chinese Institute of Electronics and China Computer Federation. His research interests focus on digital contents protection and wireless networks and security.



Yang Xiang received his PhD in Computer Science from Deakin University, Australia. He is currently a full professor and the Dean of Digital Research & Innovation Capability Platform, Swinburne University of Technology, Australia. His research interests include cyber security, which covers network and system security, data analytics, distributed systems, and networking. In particular, he is currently leading his team developing active defense systems against large-scale distributed network attacks. He is the Chief Investigator of several projects in network and system security, funded by the Australian Research Council (ARC). He has published more than 200 research papers in many international journals and conferences. He served as the Associate Editor of IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, Security and Communication Networks (Wiley), and the Editor of Journal of Network and Computer Applications. He is the Coordinator, Asia for IEEE Computer Society Technical Committee on Distributed Processing (TCDP). He is a Senior Member of the IEEE.

Haojin Zhu (IEEE M'09-SM'16) received his B.Sc. degree (2002) from Wuhan University (China), his M.Sc.(2005) degree from Shanghai Jiao Tong University (China), both in computer science and the Ph.D. in Electrical and Computer Engineering from the University of Waterloo (Canada), in 2009. Since 2017, he has been a full professor with Computer Science department in Shanghai Jiao Tong University. His current research interests include network security and privacy enhancing technologies. He published 35 international journal papers, including JSAC, TDSC, TPDS, TMC, TWC, TVT, and 60 international conference papers, including ACM CCS, ACM MOBICOM, ACM MOBIHOC, IEEE INFOCOM, IEEE ICDCS. He received a number of awards including: IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award (2014), Top 100 Most Cited Chinese Papers Published in International Journals (2014), Supervisor of Shanghai Excellent Master Thesis Award (2014), Distinguished Member of the IEEE INFOCOM Technical Program Committee (2015), Outstanding Youth Post Expert Award for Shanghai Jiao Tong University (2014), SMC Young Research Award of Shanghai Jiao Tong University (2011). He was a co-recipient of best paper awards of IEEE ICC (2007) and Chinacom (2008) as well as IEEE GLOBECOM Best Paper Nomination (2014). He received Young Scholar Award of Changjiang Scholar Program by Ministry of Education of P.R. China in 2016.