Cooperative Spectrum Sensing With M-Ary Quantized Data in Cognitive Radio Networks Under SSDF Attacks

Huifang Chen, *Member, IEEE*, Ming Zhou, Lei Xie, *Member, IEEE*, and Jie Li, *Senior Member, IEEE*

***Abstract*— In this paper, we address the challenging and important cooperative spectrum sensing (CSS) problem with M-ary quantized data under spectrum sensing data falsification (SSDF) attacks. We introduce a probabilistic SSDF attack model to characterize the attacks by a malicious secondary user (SU). We analyze the attack behavior and derive the condition to nullify the detection capability of the fusion center (FC). To defend against the SSDF attacks, we propose a novel attack-proof CSS scheme with M-ary quantized data, mainly including a malicious SU identification method and an adaptive linear combination rule. By using the malicious SU identification approach, FC identifies malicious SUs and removes them from the data fusion process. The adaptive linear combination rule adjusts the weighted coefficients with the distribution parameter sets of identified normal SUs estimated using a maximum likelihood-based estimator. FC performs the spectrum sensing process with M-ary quantized data from the identified normal SUs. Comprehensive evaluation is conducted. Evaluation results show that the proposed malicious SU identification method can remove malicious SUs successfully and the proposed CSS scheme with M-ary quantized data is robust against the SSDF attacks.**

***Index Terms*— Cognitive radio networks, cooperative spectrum sensing, malicious SU identification method, quantization, spectrum sensing data falsification attack.**

I. Introduction

COGNITIVE radio (CR) has emerged as a solution to the spectrum scarcity, since it allows secondary users (SUs) to opportunistically access the under-utilized spectrum bands of primary users (PUs) on a non-interfering basis [1], [2].

Manuscript received June 28, 2016; revised January 5, 2017 and March 28, 2017; accepted May 8, 2017. Date of publication May 26, 2017; date of current version August 10, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61471318, Grant 61071127, and Grant 61571410, in part by the Science and Technology Department of Zhejiang Province under Grant 2012C01036-1 and Grant 2011R10035, and in part by the Grand-in-Aid for Scientific Research from Japan Society for Promotion of Science, and Research Collaboration Grant from NII. The associate editor coordinating the review of this paper and approving it for publication was X. Zhou. *(Corresponding authors: Jie Li; Huifang Chen.)*

H. Chen and L. Xie are with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China, and also with the Zhejiang Provincial Key Laboratory of Information Processing, Communication and Networking, Hangzhou 310027, China (e-mail: chenhf@zju.edu.cn; xiel@zju.edu.cn).

M. Zhou is with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: maven@zju.edu.cn).

J. Li is with the Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba 305-8573, Japan (e-mail: lijie@cs.tsukuba.ac.jp).

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.2017.2707407

One of the main challenges in a cognitive radio network (CRN) is using spectrum sensing with the aim of finding the vacant spectrum band [3]. In the spectrum sensing process, various effects of the listening channels (i.e., the wireless channels between the PU and the SUs), such as shadowing, multi-path fading, and hidden terminal problem, have crucial impacts on the system performance. Thus, the single-user spectrum sensing may not be reliable. To mitigate these effects, cooperative spectrum sensing (CSS) has been proposed and has attracted considerable attention in recent years [4], [5]–[10].

In the CSS schemes, data fusion and final decision making can be performed in a centralized [5]–[8] or decentralized mode [9], [10]. In the centralized mode, there is a fusion center (FC) undertaking the responsibility of coordinating the cooperation among SUs and generating the overall sensing result. The cooperation of SUs with the FC is generally carried out in a three-phase process. The first phase is the local spectrum sensing performed at SUs individually with their built-in sensing mechanisms [3]. In other words, SUs listen to their environment and generate local sensing results about the PU signal. The second phase is the local sensing reporting performed at both SUs and FC sides. SUs involving cooperation send their local sensing results to the FC through a dedicated [7], [8] or non-dedicated channel [9], [10], where the local sensing results are transmitted in a raw [7], [8], [11], [12] or quantization mode [13], [14]. The third phase is the data fusion performed at the FC. The FC fuses the received local sensing results to decide the status of the PU using a fusion rule, such as the linear combination [7], [8], [11]–[15], the likelihood ratio test [16], and so on. In the decentralized mode, since the FC does not exist, SUs exchange their local sensing results and make the final decision by themselves in the second and third phases [17]. Most CSS schemes are performed in a centralized mode. In this paper, we consider the CSS with M-ary quantized data in the centralized mode.

Most research on the CSS in the CRN mentioned above has been carried out under the assumption of conditionally independent observations at SUs. In practice, as sensors are observing the same phenomenon, it is likely to have spatially dependent observations. Owing to the dependence among observations, the design of the sensing scheme at local sensors and the fusion rule at the FC becomes highly complex. The effect of dependence on the performance of distributed detection has been investigated recently [18], [19].

In this paper, we consider the CSS with M-ary quantized data using conditionally independent observations at SUs.

On the other hand, the cooperation introduces new security threats to the CRN. The spectrum sensing data falsification (SSDF) attack [20], in which malicious SUs send falsified local sensing results to degrade the performance of the spectrum sensing, is a typical attack in the CSS. An SSDF attack may impair the cooperation process, which results in either the excessive interference on the PU network or the decrease of the spectrum utilization of the CRN. Therefore, having the ability to mitigate the SSDF attacks is a critical issue for the CSS system. The SSDF attack problem has been widely studied in the CSS with 1-bit quantized data or soft data, and some attack-proof CSS schemes have been proposed [20]–[32]. Due to the limited bandwidth in practice, the reporting channel is assumed as a digital communication link through which the quantized local sensing data are sent to the FC. However, the SSDF attack problem in the CSS with M-ary quantized data is still an open issue.

There is a number of research work related to the CSS schemes under SSDF attacks. In [33], the negative effect of the SSDF attacks on the detection performance of the CSS with M-ary quantized data was analyzed, where it is assumed that the attacker has complete knowledge about the status of the PU, and malicious SUs choose symbols using an optimal probability distribution based on the true hypothesis in order to degrade the detection performance maximally. The assumption in [33] may be too strong because malicious SUs should have an extra power of knowing the true hypothesis. In [34], the problem of distributed detection with M-ary quantized data under SSDF attacks was also studied, where it is assumed that malicious SUs do not have knowledge about the status of the PU and the attacker is ignorant about the quantization thresholds used at the SUs to generate M-ary symbols. The assumption used in [34] may be too weak since malicious SUs may have some knowledge about the quantization thresholds used and incomplete knowledge about the true hypothesis based on their local measurements. Moreover, the attack-proof approaches proposed in [33] and [34] are under the assumption that the attacker's strategy is known such that the *a posteriori* probabilities of malicious SUs can be computed. In [35], an abnormality detection approach to alleviate the challenge of the unknown attack strategy is proposed to detect malicious SUs. This abnormality detection algorithm is based on proximity, where it is assumed that the number of malicious SUs is far smaller than that of cooperative SUs. The essential technique for identifying a malicious user is to compare the behavior of this user behavior with that of other honest users. A malicious SU detection method using two conditional frequency check statistics proposed by He *et al.* [36] can deal with the case where malicious SUs dominate the network. However, this method needs the assistance of a trusted user.

In this paper, we investigate the problem of the CSS with M-ary quantized data under SSDF attacks from both perspectives of the attacker and the defender. The main contributions of this paper are summarized as follows.

(1) We introduce a probabilistic and independent SSDF attack model for the CSS with M-ary quantized data, where the malicious SU independently modifies its quantized data according to its attack probability, the local decision about the status of the PU, and the local sensing result about the PU signal. This model captures the characteristics of the SSDF attacks by malicious SUs well.

(2) We characterize the negative effect of the proposed probabilistic SSDF attack on the performance of the CSS with M-ary quantized data. By letting the modified deflection coefficient of the global statistic test be zero, we derive the condition of the proposed attack model to nullify the detection capability of the FC.

(3) We propose a malicious SU identification method, where only the report history of each SU and the knowledge about the quantization scheme adopted at SUs are used. The performance of malicious SU identification method, namely, the identification probability and the detectability, is analytically evaluated.

(4) Using a technique based on the maximum likelihood estimation to learn the distribution parameters of identified normal SUs, we present an adaptive linear combination rule for the fusion process of the CSS with M-ary quantized data under SSDF attacks.

The remainder of this paper is organized as follows. The system model and the problem of the CSS with M-ary quantized data under SSDF attacks are described in Section II. We also introduce a probabilistic SSDF attack model in this section. In Section III, the attack performance of the proposed SSDF attack is analyzed, and the blind condition is derived. To resolve the SSDF attack problem, an attack-proof CSS scheme with M-ary quantized data is presented in Section IV. Numerical results and conclusion are given in Sections V and VI, respectively.

For clarity, we explain the denotation of some notations used in this paper. H_0 and H_1 are the hypotheses of the absence and the presence of the PU, respectively. $\mathcal{H}_0$ and $\mathcal{H}_1$ denote the inferences of the absence and the presence of the PU, respectively. TY_i denotes the type of SU i, and $TY_i \in \{\mathrm{H}, \mathrm{M}\}$, where H and M correspond to "normal" and "malicious", respectively. $\mathcal{TY}_i$ denotes the type of SU i to be declared using the malicious SU identification method, and $\mathcal{TY}_i \in \{\mathrm{H}, \mathrm{M}\}$. Symbol M in italic denotes the number of the quantization levels. $\mathcal{CN}(\cdot,\cdot)$ and $\mathcal{N}(\cdot,\cdot)$ denote the circularly symmetric normal distribution and the normal distribution, respectively.

II. System Model and Problem Formulation

A. System Model

Consider an infrastructure-based network consisting of a PU network and a CRN under the IEEE 802.22 network standard model [37]. We focus on the CRN with one primary transmitter (regarded as PU in the CRN), one FC and N SUs, where K $(0 < K < N)$ SUs are assumed to be malicious. The PU is located at a place far away from all SUs. The PU network has a licensed spectrum band, and the CRN is located in the coverage area of the PU network. SUs can use the licensed spectrum band assigned to the PU network when the status of PU is inferred as absent [38].

Fig. 1 shows the basic configuration of the CSS system in a CRN, including listening and reporting channels,

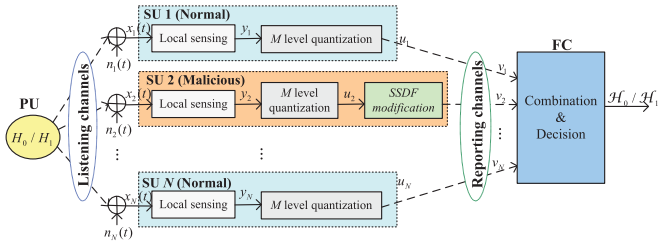


Fig. 1. The CSS system model under SSDF attacks.

PU, SUs (normal or malicious) and the FC. These N SUs cooperatively sense the radio spectrum to find spatial and/or temporal vacant bands for their communication in the CRN. It is assumed that the CSS is performed in the centralized mode. Specifically, SUs perform local spectrum sensing. Due to the constrained resource, SUs send an M-ary quantized version of their local sensing results to the FC via the reporting channel, which is assumed to be ideal [26]. However, malicious SUs may transmit falsified quantized data to the FC in order to deteriorate the CSS. Finally, the FC combines the quantized data from SUs and makes the final decision about the status of the PU.

B. Local Sensing and Quantization

To simplify the analysis, we assumed that N SUs are with the same sensing capability, where some SUs are malicious. Since the distance between SUs and the PU is much farther than that between SUs, it can also be assumed that the sensing channel between SUs and the PU is relatively static, and all SUs have similar average received signal-noise-ratio (SNR).

In the system model, the jth sample of the received PU signal at SU i, $x_i(j)$, is presented as

$$x_i(j) = \begin{cases} n_i(j), & H_0, \\ h_i s(j) + n_i(j), & H_1, \end{cases}$$

where H_0 and H_1 are the hypotheses of the absence and the presence of the PU, respectively. $s(j)$ denotes the PU signal; h_i is the block fading gain of the listening channel between the FC and SU i; and $n_i(j)$ denotes the jth sample of the circularly symmetric additive white Gaussian noise (AWGN) with zero-mean and variance σ_i^2 at SU i, i.e., $n_i(j) \sim \mathcal{CN}(0, \sigma_i^2)$.

SU i performs the spectrum sensing by using its built-in sensor to derive the local test statistic, y_i. The SU's built-in sensor can be of any common types, such as energy detection, cyclostationary detection, and so on. In this work, the energy detection mechanism is assumed to be used as the fundamental brick of local spectrum sensing because of its low complexity and needing no *a priori* knowledge about the PU [6]. Specifically,

$$y_i = \begin{cases} (1/J)\sum_{j=1}^{J} [n_i(j)]^2, & H_0, \\ (1/J)\sum_{j=1}^{J} [h_i s(j) + n_i(j)]^2, & H_1, \end{cases}$$

where J denotes the number of samples.

When J is large enough, according to the Central Limit Theorem (CLT) [39], y_i follows asymptotically normal distribution with mean and variance as

$$y_i \sim \begin{cases} \mathcal{N}(\sigma_i^2, 2\sigma_i^4/J), & H_0, \\ \mathcal{N}\left((1+\mu_i)\sigma_i^2, 2(1+2\mu_i)\sigma_i^4/J\right), & H_1, \end{cases}$$

where μ_i is the average SNR, and $\mu_i = E[|h_i s(j)|^2]/\sigma_i^2$.

Considering the constrained resource of the reporting channel, y_i is quantized using the following quantization rule as

$$\mu_i = \psi_i(y_i) = l, \text{ if } E_{i,l-1} < y_i \le E_{i,l}, \quad i = 1, 2, \ldots, N, \ l = 1, 2, \ldots, M, \tag{1}$$

where $\psi_i(\cdot)$ denotes the quantization process at SU i; M is the number of quantization levels; u_i denotes the quantized level of y_i; $E_{i,l-1}$ and $E_{i,l}$ denote the $(l-1)$th and lth quantization boundaries at SU i, respectively. There are several quantization methods that can be considered at SUs, such as uniform quantization, maximum output entropy (MOE) quantization and minimum average error (MAE) quantization [40]. It is shown in [40] that, for a signal that follows the normal distribution, the quantizers with MOE and MAE are approximately the same within a multiplicative constant. In this paper, we consider the MOE quantization method because of its low computational complexity.

In the MOE quantization incorporated at SU i, the range of y_i is divided into M levels, and each level has the probability mass function (PMF) of $1/M$. Hence, the PMF of u_i can be calculated as

$$\Pr(u_i = l) = \int_{E_{i,l-1}}^{E_{i,l}} f_{y_i}(x)\, \mathrm{d}x = 1/M, \quad i = 1, 2, \ldots, N, \ l = 1, 2, \ldots, M, \tag{2}$$

where $f_{y_i}(\cdot)$, the probability density function (PDF) of y_i, is given by

$$f_{y_i}(x) = p(H_0) f_{y_i}(x|H_0) + p(H_1) f_{y_i}(x|H_1), \quad i = 1, 2, \ldots, N, \tag{3}$$

where $p(H_0)$ and $p(H_1)$ are the prior probabilities of H_0 and H_1, respectively; $f_{y_i}(\cdot|H_0)$ and $f_{y_i}(\cdot|H_1)$ denote the PDFs of y_i conditioned H_0 and H_1, respectively.

The quantized data of the lth quantized level at SU i, $q_{i,l}$, lies in the centroid of $E_{i,l-1}$ and $E_{i,l}$, i.e.,

$$q_{i,l} = \frac{\int_{E_{i,l-1}}^{E_{i,l}} x f_{y_i}(x)\, \mathrm{d}x}{\int_{E_{i,l-1}}^{E_{i,l}} f_{y_i}(x)\, \mathrm{d}x} = M \int_{E_{i,l-1}}^{E_{i,l}} x f_{y_i}(x)\, \mathrm{d}x, \quad i = 1, 2, \ldots, N, \ l = 1, 2, \ldots, M. \tag{4}$$

For a CRN under SSDF attacks, note that a malicious SU may not transmit its real quantized level. Denote the transmitted quantized level as v_i for SU i. If SU i is honest, $v_i = u_i$; otherwise, we assume that SU i may modify u_i to v_i according to the SSDF attack model, and $v_i \neq u_i$.

C. Probabilistic SSDF Attack Model

The objective of the SSDF attacker is to deteriorate the detection performance of the CSS in the CRN. In this work,

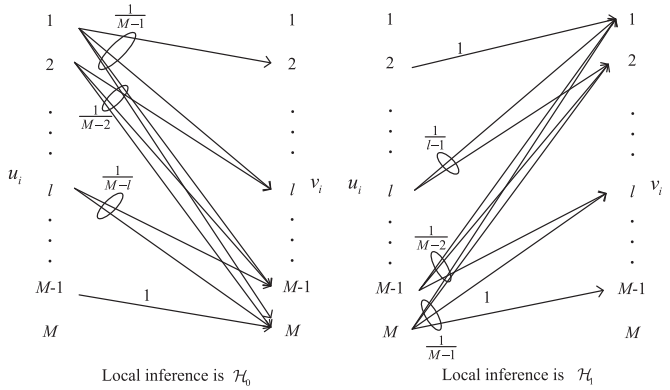


Fig. 2. Quantized level modification in the probabilistic SSDF attack model.

we introduce a probabilistic SSDF attack model, where a malicious SU can use its local information to launch an attack. Let β_i denote the attack probability of SU i. That is, SU i behaves maliciously with probability β_i, and behaves normally with probability $1-\beta_i$. If SU i is honest, $\beta_i = 0$.

At each sensing interval, malicious SU i utilizes a probability, β_i, to decide whether to launch an SSDF attack or not.

When a malicious SU decides to launch the attack, it prefers to make the attack successful. If SU i decides to launch the SSDF attack, it first makes its local decision according to $y_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \phi_i$, where ϕ_i is the local decision threshold, $\mathcal{H}_0$ and $\mathcal{H}_1$ denote the inferences of the absence and the presence of the PU, respectively. Based on the decision, SU i falsifies its quantized level according to the model as illustrated in Fig. 2. If the local inference is $\mathcal{H}_0$, SU i modifies its quantized level $u_i = l$ into $v_i = k$ with probability $\frac{1}{M-l}$, where k is one of the quantized levels larger than l. Similarly, if the local inference is $\mathcal{H}_1$, SU i modifies its quantized level $u_i = l$ into $v_i = k$ with probability $\frac{1}{l-1}$, where k is one of the quantized levels smaller than l. Here, SU i modifies the quantized level with a uniform distribution in order to prevent from being identified by the FC easily.

If malicious SU i decides not to launch the SSDF attack, it sends its true quantized level to the FC with probability $(1-\beta_i)$.

Let TY_i be the type of SU i, $TY_i \in \{\mathrm{H}, \mathrm{M}\}$ and $i = 1, 2, \ldots, N$. We say that if $TY_i = \mathrm{H}$, SU i is an honest user, while $TY_i = \mathrm{M}$ means that SU i is a malicious user.

Based on the probabilistic SSDF attack model introduced above, for a malicious SU i, the PMFs of v_i under H_0 and H_1 are presented as

$$\begin{aligned}&\Pr(v_i = l|H_0, TY_i = \mathrm{M})\\ &= (1-\beta_i)\Pr(u_i = l|H_0) + \beta_i(1-P_{\mathrm{f},i})\sum_{k=1}^{l-1}\frac{\Pr(u_i = k|H_0)}{M-k}\\ &\quad + \beta_i P_{\mathrm{f},i}\sum_{k=l+1}^{M}\frac{\Pr(u_i = k|H_0)}{k-1}, \quad l = 1, 2, \ldots, M \end{aligned} \tag{5}$$

and

$$\begin{aligned}&\Pr(v_i = l|H_1, TY_i = \mathrm{M})\\ &= (1-\beta_i)\Pr(u_i = l|H_1) + \beta_i(1-P_{\mathrm{d},i})\sum_{k=1}^{l-1}\frac{\Pr(u_i = k|H_1)}{M-k}\\ &\quad + \beta_i P_{\mathrm{d},i}\sum_{k=l+1}^{M}\frac{\Pr(u_i = k|H_1)}{k-1}, \quad l = 1, 2, \ldots, M, \end{aligned} \tag{6}$$

respectively. Here, $P_{\mathrm{f},i}$ is the local false-alarm probability at SU i, and $P_{\mathrm{d},i}$ is the local detection probability at SU i.

Hence, if SU i is malicious, the PMF of v_i is

$$\begin{aligned}&\Pr(v_i = l|TY_i = \mathrm{M})\\ &= p(H_0)\Pr(v_i = l|H_0, TY_i = M)\\ &\quad + p(H_1)\Pr(v_i = l|H_1, TY_i = M),\ l = 1, 2, \ldots, M. \end{aligned} \tag{7}$$

Obviously, if SU i is honest, the PMF of v_i is the same as that of u_i. That is,

$$\Pr(v_i = l|TY_i = \mathrm{H}) = 1/M, \quad l = 1, 2, \ldots, M. \tag{8}$$

D. Linear Combining and Decision Making

It is assumed that SUs transmit the quantized levels via an ideal reporting channel. Although the quantized levels may be corrupted by the noise and interference in the reporting channel, the influence can be avoided by using an efficient channel coding mechanism. Thus, we neglect the effect of the reporting channel errors in this paper. In other words, the quantized levels received by the FC are the transmitted quantized levels from SUs, $\{v_i\}_{i=1}^N$.

In this paper, we consider the CSS is carried out under the assumption of conditionally independent observations from SUs. However, dependence often occurs in practice as the SUs observing the same phenomenon are likely to have spatially dependent observations. The effect of dependence on the performance of distributed detection has been investigated recently [18], [19]. However, it is beyond the scope of this paper.

A linear combining is performed at the FC, which means that the global test statistic, Z_{c}, is constructed as a weighted sum of the received quantized data. That is,

$$Z_{\mathrm{c}} = \sum_{i=1}^{N} w_i \psi_i^{-1}(v_i), \tag{9}$$

where w_i is the weighted coefficient of the received quantized data from SU i, $\psi_i^{-1}(\cdot)$ denotes the inverse of the quantization process at SU i, and $\psi_i^{-1}(v_i)$ is the centroid of the quantization region of v_i. In most cases, it is a nonlinear inverse mapping.

Then Z_{c} is compared with a pre-defined global decision threshold, λ_{c}, to decide the status of PU, i.e.,

$$Z_{\mathrm{c}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda_{\mathrm{c}}. \tag{10}$$

The detector performance of the CSS with M-ary quantized data is commonly measured by two probabilities, namely, the global false-alarm probability $Q_{\mathrm{f}} = \Pr(Z_{\mathrm{c}} \geq \lambda_{\mathrm{c}}|H_0)$ and the global detection probability $Q_{\mathrm{d}} = \Pr(Z_{\mathrm{c}} \geq \lambda_{\mathrm{c}}|H_1)$.

The integrated performance of the CSS with M-ary quantized data in a CRN under SSDF attacks can be measured by the global error probability, which is defined as

$$Q_{\mathrm{e}} = p(H_0)Q_{\mathrm{f}} + p(H_1)(1 - Q_{\mathrm{d}}). \tag{11}$$

We consider the Neyman-Pearson formulation [41] at the FC, and the global decision threshold is determined such that the global false-alarm probability subjects to an upper bound, $\bar{Q}_{\mathrm{f}}$. Hence, λ_{c} can be written as

$$\lambda_{\mathrm{c}} = \arg\min_{x}\{x : \Pr(Z_{\mathrm{c}} \geq x|H_0) \leq \bar{Q}_{\mathrm{f}}\}. \tag{12}$$

To derive the closed-form expressions of the global false-alarm probability and the global detection probability of the CSS with M-ary quantized data, the PDFs of Z_{c} under H_0 and H_1 are needed. Since v_i in (9) follows multivariate Bernoulli distribution, the exact distribution of Z_{c} is in the form of generalized multivariate binomial. The distribution of Z_{c} has a very complicated form with many terms, and its computational complexity is $O(N^{M-1})$ [42]. Therefore, it is not feasible to obtain the exact distribution function of Z_{c}.

In order to reduce the computational complexity, we should consider an approximation of the distribution of Z_{c}. According to the CLT, if N is large enough, a Gaussian approximation can be made for the distribution of Z_{c}. Since $\{v_i\}_{i=1}^{N}$ are independently and identically distributed (iid), the mean and variance of $\psi_i^{-1}(v_i)$ conditioned H_j, $j = 0, 1$, are given as

$$\mu(\psi_i^{-1}(v_i)|H_j) = \sum_{l=1}^{M} q_{i,l} \Pr(v_i = l|H_j), \quad i = 1, 2, \ldots, N, \quad j = 0, 1, \tag{13}$$

and

$$\sigma^2(\psi_i^{-1}(v_i)|H_j) = \sum_{l=1}^{M} q_{i,l}^2 \Pr(v_i = l|H_j) - \mu(\psi_i^{-1}(v_i)|H_j)^2, \quad i = 1, 2, \ldots, N, \ \ j = 0, 1. \tag{14}$$

Hence, the closed-form expressions of the global false-alarm probability and the global detection probability of the CSS scheme with M-ary quantized data can be expressed as

$$Q_{\mathrm{f}} = Q\left(\frac{\lambda_c^{'} - \boldsymbol{\mu}_{H_0}^{\mathrm{T}}\mathbf{w}}{\sqrt{\mathbf{w}^{\mathrm{T}}\sum_{H_0}\mathbf{w}}}\right) \tag{15}$$

and

$$Q_{\mathrm{d}} = Q\left(\frac{\lambda_c^{'} - \boldsymbol{\mu}_{H_1}^{\mathrm{T}}\mathbf{w}}{\sqrt{\mathbf{w}^{\mathrm{T}}\sum_{H_1}\mathbf{w}}}\right), \tag{16}$$

respectively. Here, $\lambda_{\mathrm{c}}^{'}$ is the global decision threshold for the CSS with Gaussian approximation; $\mathbf{w}$ is the set of weight coefficients, and $\mathbf{w} = [w_1\, w_2 \ldots w_N]$, $\boldsymbol{\mu}_{H_j}$ is the set of mean conditioned H_j, and $\boldsymbol{\mu}_{H_j} = [\mu(\psi_1^{-1}(v_1)|H_j)\ \mu(\psi_2^{-1}(v_2)|H_j) \ldots \mu(\psi_N^{-1}(v_N)|H_j)]$, $j = 0, 1$, $\sum_{H_j}$ is the set of variance conditioned H_j, and $\sum_{H_j} = diag\left(\sigma^2(\psi_1^{-1}(v_1)|H_j)\ \sigma^2(\psi_2^{-1}(v_2)|H_j) \ldots \sigma^2(\psi_N^{-1}(v_N)|H_j)\right)$, $j = 0, 1$; $Q(x)$ is the Q-function, and $Q(x) = \int_x^{+\infty} \exp(-t^2/2)\, \mathrm{d}t/\sqrt{2\pi}$.

By considering a required global false-alarm probability, $\bar{Q}_{\mathrm{f}}$, $\lambda_{\mathrm{c}}^{'}$ can be calculated by

$$\lambda_{\mathrm{c}}^{'} = Q^{-1}(\bar{Q}_{\mathrm{f}})\sqrt{\mathbf{w}^{\mathrm{T}}\sum_{H_0}\mathbf{w}} + \boldsymbol{\mu}_{H_0}^{\mathrm{T}}\mathbf{w}, \tag{17}$$

where $Q^{-1}(\cdot)$ is the functional inverse of the Q-function.

From the perspective of the attacker, the aim of malicious SUs is to destroy the network such that the detection performance of the CSS is degraded. The most serious case is to make the FC blind (completely dysfunctional), in which the decisions made by the FC are no better than merely flipping a coin without using any received quantized data. Although incapable of making the FC blind, malicious SUs will try to degrade the performance of the CSS as far as possible. In this paper, we will analyze the maximal impact of the introduced SSDF attack on the detection performance of the CSS.

On the other hand, in the view of the network designer, the objective is to make the FC infer the status of the PU reliably, although there are malicious SUs in the network. In this paper, we present an attack-proof CSS scheme with M-ary quantized data in the CRN, where the malicious SU identification method and the linear combination rule at the FC are mainly studied.

III. Derivation of Blind Condition

In this section, we analyze the maximal impact of the probabilistic SSDF attack on the detection performance of the CSS with M-ary quantized data.

As described in Subsection II.D, the FC adopts the Neyman-Pearson detector to infer the status of the PU. It is proven in [43] that the performance of Neyman-Pearson detector can be evaluated by the deflection coefficient since it can measure the variance-normalized distance between the centers of two conditional PDFs.

According to (14), Z_{c} has a different variance under H_0 and H_1. Since the PDF of Z_{c} under H_1 has a heavier tail than that under H_0, the modified deflection coefficient is used to characterize the detection performance of the CSS with M-ary quantized data in this paper. The modified deflection coefficient of Z_{c} can be represented as

$$D(Z_{\mathrm{c}}) = \frac{(\boldsymbol{\mu}_{H_1}^{\mathrm{T}}\mathbf{w} - \boldsymbol{\mu}_{H_0}^{\mathrm{T}}\mathbf{w})^2}{\mathbf{w}^{\mathrm{T}}\sum_{H_1}\mathbf{w}}. \tag{18}$$

In the CSS with M-ary quantized data, malicious SUs aim to make the modified deflection coefficient as small as possible in order to maximally degrade the detection performance. Since the modified deflection coefficient is always non-negative, making $D(Z_{\mathrm{c}}) = 0$ means that malicious SUs disrupt the decision mechanism, and the FC is incapable of inferring the status of the PU using the received quantized data from SUs. Therefore, the condition making FC blind is summarized as Theorem 1.

Theorem 1: For the probabilistic SSDF attack model and the weighted linear data combination rule, the condition to

blind the CSS system with M-ary quantized data is

$$\sum_{i=1}^{K} w_i \beta_i \sum_{l=1}^{M} q_{i,l} \Bigg[\sum_{k=1}^{l-1} \frac{(1-P_{\mathrm{f},i})a_{i,k}^0 - (1-P_{\mathrm{d},i})a_{i,k}^1}{M-k} + \sum_{k=l+1}^{M} \frac{P_{\mathrm{f},i}a_{i,k}^0 - P_{\mathrm{d},i}a_{i,k}^1}{k-1} + (a_{i,l}^1 - a_{i,l}^0) \Bigg] = \sum_{i=1}^{N} w_i \sum_{l=1}^{M} q_{i,l}(a_{i,l}^1 - a_{i,l}^0), \tag{19}$$

where $a_{i,l}^1 = \Pr(u_i = l|H_1)$ and $a_{i,l}^0 = \Pr(u_i = l|H_0)$.

Proof: The variance of Z_{c} conditioned H_1 can be computed by (14). To make $D(Z_{\mathrm{c}}) = 0$, (18) becomes

$$\sum_{i=1}^{N} w_i \sum_{l=1}^{M} q_{i,l} \Pr(v_i = l|H_0) = \sum_{i=1}^{N} w_i \sum_{l=1}^{M} q_{i,l} \Pr(v_i = l|H_1). \tag{20}$$

For the probabilistic SSDF attack model defined in Subsection II.C and the weighted linear data combination rule described in Subsection II.D, the means of Z_{c} conditioned H_0 and H_1 can be computed by (13).

If SU i is an honest user, the PMFs of v_i under H_0 and H_1 are the same as those of u_i under H_0 and H_1. Since K out of N SUs are malicious, SUs labeled from 1 to K are malicious, and SUs labeled from $K+1$ to N are honest without loss of generality. Substituting (5), (6) for $i = 1, 2, \ldots, K$, $\{\Pr(v_i = l|H_0) = \Pr(u_i = l|H_0)\}_{i=K+1}^{N}$ and $\{\Pr(v_i = l|H_1) = \Pr(u_i = l|H_1)\}_{i=K+1}^{N}$ into (20), the condition to make $D(Z_{\mathrm{c}}) = 0$ becomes

$$\sum_{i=1}^{K} w_i \beta_i \sum_{l=1}^{M} q_{i,l} \Bigg[\sum_{k=1}^{l-1} \frac{(1-P_{\mathrm{f},i})a_{i,k}^0 - (1-P_{\mathrm{d},i})a_{i,k}^1}{M-k} + \sum_{k=l+1}^{M} \frac{P_{\mathrm{f},i}a_{i,k}^0 - P_{\mathrm{d},i}a_{i,k}^1}{k-1} + (a_{i,l}^1 - a_{i,l}^0) \Bigg] = \sum_{i=1}^{N} w_i \sum_{l=1}^{M} q_{i,l}(a_{i,l}^1 - a_{i,l}^0).$$

■

For a special case where all SUs have the same average received SNR since the distances between SUs and PU are much larger than those between any two SUs, the subscript i in $a_{i,l}^0$ and $a_{i,l}^1$ can be neglected and thus we have a_l^0 and a_l^1. In the case, all SUs adopt the same MOE quantization rule, $E_{i,l} = E_l$ and $q_{i,l} = q_l$, $i = 1, 2, \ldots, N$, $l = 1, 2, \ldots, M$. The FC uses the equal gain combination (EGC) rule, and $w_i = 1/N$, $i = 1, 2, \ldots, N$. It is reasonable to assume that the behaviors of malicious SUs are the same, that is, $\beta_i = \beta$, $P_{\mathrm{d},i} = P_{\mathrm{d}}$ and $P_{\mathrm{f},i} = P_{\mathrm{f}}$, $i = 1, 2, \ldots, K$. Hence, when the attack probability is given, the condition to make FC blind can be simplified as

$$\alpha_{\mathrm{blind}} = \frac{K}{N} = \frac{\sum_{l=1}^{M} q_l(a_l^1 - a_l^0)}{\beta \sum_{l=1}^{M} q_l[(a_l^1 - a_l^0) + \sum_{k=1}^{l-1} \frac{(1-P_{\mathrm{f}})a_k^0 - (1-P_{\mathrm{d}})a_k^1}{M-k} + \sum_{k=l+1}^{M} \frac{P_{\mathrm{f}}a_k^0 - P_{\mathrm{d}}a_k^1}{k-1}]}, \tag{21}$$

where α_{blind} is the minimum fraction of malicious SUs to nullify the detection capability of the FC.

IV. Proposed CSS Scheme With M-Ary Quantized Data Under SSDF Attacks

If the SSDF attacker cannot compromise enough SUs, the FC will not become completely blind. Hence, we consider the CSS scheme with M-ary quantized data against the SSDF attacks in this section.

A. Optimal Linear Combination

As the FC uses the weighted linear combination rule, the global test statistic is given in (9).

In order to characterize the performance of the FC, we also consider the modified deflection coefficient as the performance metric. Hence, the optimal linear combination problem for the CSS scheme with M-ary quantized data under SSDF attacks and its solution are given in Theorem 2.

Theorem 2: The optimal linear combination problem for the CSS scheme with M-ary quantized data under SSDF attacks is formulated as

$$\max_{\mathbf{w}} \frac{(\boldsymbol{\mu}_{H_1}^{\mathrm{T}}\mathbf{w} - \boldsymbol{\mu}_{H_0}^{\mathrm{T}}\mathbf{w})^2}{\mathbf{w}^{\mathrm{T}} \sum_{H_1} \mathbf{w}}, \quad \text{s.t.} \sum_{i=1}^{N} w_i = 1. \tag{P.1}$$

Solving (P.1), the optimal weighted coefficients are given as

$$w_i = \frac{\frac{\mu(\psi_i^{-1}(v_i)|H_1) - \mu(\psi_i^{-1}(v_i)|H_0)}{\sigma^2(\psi_i^{-1}(v_i)|H_1)}}{\sum_{k=1}^{N} \frac{\mu(\psi_k^{-1}(v_k)|H_1) - \mu(\psi_k^{-1}(v_k)|H_0)}{\sigma^2(\psi_k^{-1}(v_k)|H_1)}}, \quad i = 1, 2, \ldots, N. \tag{22}$$

Proof: On partially differentiating $\frac{(\boldsymbol{\mu}_{H_1}^{\mathrm{T}}\mathbf{w} - \boldsymbol{\mu}_{H_0}^{\mathrm{T}}\mathbf{w})^2}{\mathbf{w}^{\mathrm{T}} \sum_{H_1} \mathbf{w}}$ with respect to w_i, $i = 1, 2, \ldots, N$, we have $\frac{\mu(\psi_1^{-1}(v_1)|H_1) - \mu(\psi_1^{-1}(v_1)|H_0)}{w_1 \sigma^2(\psi_1^{-1}(v_1)|H_1)} = \frac{\mu(\psi_2^{-1}(v_2)|H_1) - \mu(\psi_2^{-1}(v_2)|H_0)}{w_2 \sigma^2(\psi_2^{-1}(v_2)|H_1)} = \ldots = \frac{\mu(\psi_N^{-1}(v_N)|H_1) - \mu(\psi_N^{-1}(v_N)|H_0)}{w_N \sigma^2(\psi_N^{-1}(v_N)|H_1)}$.

Since $\sum_{i=1}^{N} w_i = 1$, the optimal weighted coefficients of linear combination rule at the FC are $w_i = \frac{\frac{\mu(\psi_i^{-1}(v_i)|H_1) - \mu(\psi_i^{-1}(v_i)|H_0)}{\sigma^2(\psi_i^{-1}(v_i)|H_1)}}{\sum_{k=1}^{N} \frac{\mu(\psi_k^{-1}(v_k)|H_1) - \mu(\psi_k^{-1}(v_k)|H_0)}{\sigma^2(\psi_k^{-1}(v_k)|H_1)}}$, $i = 1, 2, \ldots, N$. ■

However, the optimal weighted linear combination at the FC is difficult to numerically evaluate since the optimal weighted coefficients, $\{w_i, i = 1, 2, \ldots, N\}$, involve many unknown distribution parameters of SUs. To deal with this problem, malicious SUs should be identified by observing the data over multiple iterations and excluded from the linear combination process at the FC. Moreover, the distribution parameters of identified normal SUs should be estimated by observing the data over multiple iterations.

B. Malicious SU Identification Method

In this section, we present a malicious SU identification method to distinguish between malicious and normal SUs.

1) Proposed Method: For detecting the malicious SUs, the FC observes the M-ary quantized data of each SU over a time window T, where T is the number of the sensing intervals that have been completed. The history of reports for SU i is denoted by $\mathbf{v}_i = (v_i(1), v_i(2), \ldots, v_i(T))$, where $v_i(t)$ is the reported quantized level for SU i at sensing interval t.

Let $\pi_{i,l}$ be the reporting frequency of quantized level l for SU i over a time window T, $l = 1, 2, \ldots, M$. Using $\mathbf{v}_i$, $\pi_{i,l}$ can be estimated as

$$\pi_{i,l} = \frac{1}{T}\sum_{t=1}^{T}\delta(v_i(t)-l), \quad i = 1, 2, \ldots, N, \ l = 1, 2, \ldots, M, \tag{23}$$

where $\delta(x - x_0)$ is the Kronecker-delta function, and $\delta(x - x_0) = \begin{cases} 1, & x = x_0. \\ 0, & x \neq x_0. \end{cases}$

The normalized deviation of the reporting frequency of quantized level l for SU i is defined as

$$\xi_{i,l} = \frac{e_{i,l}}{\sqrt{\mathrm{Var}(e_{i,l})}}, \tag{24}$$

where $e_{i,l}$ is the deviation of the reporting frequency of quantized level l for SU i, and

$$e_{i,l} = \pi_{i,l} - \frac{1}{M}. \tag{25}$$

$\mathrm{Var}(e_{i,l})$ is the variance of $e_{i,l}$, and

$$\mathrm{Var}(e_{i,l}) = \frac{\pi_{i,l}(1 - \pi_{i,l})}{T}. \tag{26}$$

Hence, the deviation of the SU i, Ξ_i, can be calculated as

$$\Xi_i = \sum_{l=1}^{M}(\xi_{i,l})^2, i = 1, 2, \ldots, N. \tag{27}$$

SU i can be declared as either normal or malicious using the rule as follows

$$\Xi_i \underset{\mathcal{TY}_i=\mathrm{H}}{\overset{\mathcal{TY}_i=\mathrm{M}}{\gtrless}} \iota_i, i = 1, 2, \ldots, N, \tag{28}$$

where ι_i is the malicious SU identification threshold at SU i; $\mathcal{TY}_i$ denotes the type of SU i to be declared using the malicious SU identification method, and $\mathcal{TY}_i \in \{\mathrm{H}, \mathrm{M}\}$.

Hence, the proposed malicious SU identification method only uses the report history of each SU and the knowledge about the quantization scheme adopted at SUs. The essential technique for identifying the malicious user is to compare the reporting frequency of certain quantized levels using the report history of each SU with normal PMF of quantized levels. The behavior of the malicious SU identification method for SU i is quantified by two conditional probabilities, namely, the identification probability $\Pi_{\mathrm{d},i} = \Pr\{\Xi_i \geq \iota_i | TY_i = \mathrm{M}\}$ and the false identification probability $\Pi_{\mathrm{f},i} = \Pr\{\Xi_i \geq \iota_i | TY_i = \mathrm{H}\}$. Specifically, $\Pi_{\mathrm{d},i}$ denotes the probability that a malicious SU is identified correctly, and $\Pi_{\mathrm{f},i}$ denotes the probability that a normal SU is falsely declared as malicious.

2) Threshold Selection: From (28), the behavior depends strongly on the choice of ι_i. The value of ι_i should be set in such a way that the identification probability is high enough, and the false identification probability is low. However, a trade-off between the identification probability and the false identification probability should be achieved.

Now, we discuss how to choose ι_i for the proposed malicious SU identification method.

In order to find the optimal choice of ι_i in (28), we adopt the Neyman-Pearson framework in the context of the malicious SU identification, where the goal is to maximize $\Pi_{\mathrm{d},i}$ subject to the condition that $\Pi_{\mathrm{f},i} \leq \zeta$. The optimal problem can be expressed as

$$\max_{\iota_i} \Pi_{\mathrm{d},i}, \quad \text{s.t. } \Pi_{\mathrm{f},i} \leq \zeta. \tag{P.2}$$

To obtain $\Pi_{\mathrm{d},i}$ and $\Pi_{\mathrm{f},i}$, we need the closed-form expressions of conditional distributions of Ξ_i, $P(\Xi_i | TY_i = \mathrm{M})$ and $P(\Xi_i | TY_i = \mathrm{H})$, respectively. In practice, as T is finite, it is intractable to determine the conditional distributions of Ξ_i. Therefore, we present an asymptotic choice of ι_i in (28) as $T \to \infty$ in this paper.

As $T \to \infty$, according to the strong law of large numbers, the reporting frequency of quantized level l for SU i converges. As SU i is normal, $\pi_{i,l} \to \Pr(v_i = l | TY_i = \mathrm{H}) = 1/M$; otherwise, $\pi_{i,l} \to \Pr(v_i = l | TY_i = \mathrm{M})$. Hence, as $T \to \infty$, $\xi_{i,l}$ follows the normal distribution with unit variance. That is,

$$\xi_{i,l} \sim \begin{cases} \mathcal{N}(0, 1), & TY_i = \mathrm{H}. \\ \mathcal{N}\left(\dfrac{\Pr(v_i = l | TY_i = \mathrm{M}) - \frac{1}{M}}{\sqrt{\frac{\Pr(v_i = l | TY_i = \mathrm{M})(1 - \Pr(v_i = l | TY_i = \mathrm{M}))}{T}}}, 1\right), & TY_i = \mathrm{M}. \end{cases} \tag{29}$$

From (27), it can be inferred that Ξ_i follows a central Chi-square distribution with M degrees of freedom if $TY_i = \mathrm{H}$; otherwise, it follows a non-central Chi-square distribution with M degrees of freedom and a non-centrality parameter κ_i if $TY_i = \mathrm{M}$. That is,

$$\Xi_i \sim \begin{cases} \chi^2_M, & TY_i = \mathrm{H}, \\ \chi^2_M(\kappa_i), & TY_i = \mathrm{M}, \end{cases} \tag{30}$$

where $\kappa_i = \sum_{l=1}^{M} \frac{T\left(\Pr(v_i=l|TY_i=\mathrm{M}) - \frac{1}{M}\right)^2}{\Pr(v_i=l|TY_i=\mathrm{M})(1-\Pr(v_i=l|TY_i=\mathrm{M}))}$.

According to (28) and (30), the false identification probability and the identification probability of the proposed malicious SU identification method for SU i can be calculated by

$$\Pi_{\mathrm{f},i} = \Pr\{\Xi_i \geq \iota_i | TY_i = \mathrm{H}\} = \frac{\Gamma(\frac{M}{2}, \frac{\iota_i}{2})}{\Gamma(\frac{M}{2})}, \tag{31}$$

$$\Pi_{\mathrm{d},i} = \Pr\{\Xi_i \geq \iota_i | TY_i = \mathrm{M}\} = Q_{\frac{M}{2}}\left(\sqrt{\kappa_i}, \sqrt{\iota_i}\right), \tag{32}$$

where $\Gamma(a,x)$ is the incomplete gamma function, and $\Gamma(a,x) = \int_x^\infty t^{a-1}e^{-t}\,\mathrm{d}t$. $\Gamma(x)$ is the gamma function, and $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}\,\mathrm{d}t$. $Q_c(a,x)$ is the c-order generalized Marcum Q-function, and $Q_c(a,x) = \frac{1}{a^{c-1}}\int_x^\infty t^c e^{-\frac{t^2+a^2}{2}} I_{c-1}(at)\,\mathrm{d}t$ with modified Bessel function $I_{c-1}(at)$ of order $c-1$.

By considering $\Pr(\Xi_i \geq \iota_i | TY_i = \mathrm{H}) = \zeta$, the optimal $\iota_{\mathrm{opt},i}$ is calculated using (31). Substituting $\iota_{\mathrm{opt},i}$ into (32), we obtain the identification probability, $\Pi_{\mathrm{d},i} = Q_{\frac{M}{2}}\left(\sqrt{\kappa_i}, \sqrt{\iota_{\mathrm{opt},i}}\right)$.

Therefore, the malicious SU identification method is given in Algorithm 1.

Algorithm 1 Malicious SU Identification Method

Input and Parameter Initialization

(1) Input M, $\{\mathbf{v}_i,\ i = 1,2,\ldots,N\}$, $\{\bar{\Pi}_{\mathrm{f},i},\ i = 1,2,\ldots,N\}$, T.

Malicious SU Identification Procedure

(2) **for** SU i **do**

(3) Using $\mathbf{v}_i$, compute $\pi_{i,l}$ with (23), $l = 1,2,\ldots,M$.

(4) Compute $e_{i,l}$ and $\mathrm{Var}(e_{i,l})$ with (25) and (26), $l = 1,2,\ldots,M$.

(5) Compute $\xi_{i,l}$ with (24), $l = 1,2,\ldots,M$.

(6) Compute the deviation, Ξ_i, with (27).

(7) Setting $\zeta = \bar{\Pi}_{\mathrm{f},i}$ in $\Pr(\Xi_i \geq \iota_i | TY_i = \mathrm{H}) = \frac{\Gamma(\frac{M}{2}, \frac{\iota_i}{2})}{\Gamma(\frac{M}{2})} = \zeta$, compute $\iota_{\mathrm{opt},i}$.

(8) If $\Xi_i > \iota_{\mathrm{opt},i}$, SU i is declared as malicious, $\mathcal{TY}_i = \mathrm{M}$; otherwise, SU i is declared as normal, $\mathcal{TY}_i = \mathrm{H}$.

(9) **end for**

Output

(10). Output $\{\mathcal{TY}_i,\ i = 1,2,\ldots,N\}$.

For a practical system, the FC estimates $\pi_{i,l}$ in a recursive form as

$$\pi_{i,l}(t+1) = \frac{t\pi_{i,l}(t) + \delta(v_i(t+1) - l)}{t+1}, \quad l = 1,2,\ldots,M. \tag{33}$$

Similarly, the mean and variance of $e_{i,l}$ are estimated as

$$E(e_{i,l})(t+1) = \frac{tE(e_{i,l})(t) + [\pi_{i,l}(t+1) - 1/M]}{t+1} \tag{34}$$

and

$$\begin{aligned}\mathrm{Var}(e_{i,l})(t+1) = {} & \frac{t-1}{t}\mathrm{Var}(e_{i,l})(t) + [\pi_{i,l}(t+1) - 1/M]^2 \\ & + t[E(e_{i,l})(t)]^2 - (t+1)[E(e_{i,l})(t+1)]^2.\end{aligned} \tag{35}$$

3) Performance Analysis: In this subsection, we analyze the performance of the proposed malicious SU identification method.

The identification performance, namely the false identification probability and the identification probability, are analyzed in the preceding subsection. The closed-form expressions of $\Pi_{\mathrm{f},i}$ and $\Pi_{\mathrm{d},i}$ are given in (31) and (32), respectively.

As mentioned above, when SU i is normal, $\pi_{i,l} \to \Pr(v_i = l | TY_i = \mathrm{H}) = 1/M$ almost surely when $T \to \infty$ according to the strong law of large numbers; otherwise, $\pi_{i,l} \to \Pr(v_i = l | TY_i = \mathrm{M})$. Obviously, as $\Pr(v_i = l | TY_i = \mathrm{M}) \neq 1/M, l = 1,2,\ldots,M$, the malicious SU can be detected with probability 1 when $T \to \infty$ if the threshold is properly chosen.

Theorem 3: The malicious SU is always detectable using the proposed malicious SU identification method.

Proof: The malicious SU is non-detectable when $\Pr(v_i = l | TY_i = \mathrm{M}) = 1/M, l = 1,2,\ldots,M$. That is, $\Pr(v_i = l | TY_i = \mathrm{M}) = p(H_0)\Pr(v_i = l | H_0, TY_i = \mathrm{M}) + p(H_1)\Pr(v_i = l | H_1, TY_i = \mathrm{M}) = 1/M$.

Substituting (5) and (6) into (7), we obtain

$$\begin{aligned}&\Pr(v_i = l | TY_i = \mathrm{M}) \\ &\quad = \frac{1}{M} \\ &\qquad + p(H_0)\beta_i\left[(1 - P_{\mathrm{f},i})\sum_{k=1}^{l-1}\frac{\Pr(u_i = k|H_0)}{M-k}\right. \\ &\qquad \left. + P_{\mathrm{f},i}\sum_{k=l+1}^{M}\frac{\Pr(u_i = k|H_0)}{k-1}\right] \\ &\qquad + p(H_1)\beta_i\left[(1 - P_{\mathrm{d},i})\sum_{k=1}^{l-1}\frac{\Pr(u_i = k|H_1)}{M-k}\right. \\ &\qquad \left. + P_{\mathrm{d},i}\sum_{k=l+1}^{M}\frac{\Pr(u_i = k|H_1)}{k-1}\right].\end{aligned} \tag{36}$$

From (36), to make $\Pr(v_i = l | TY_i = \mathrm{M}) = 1/M$, one option is to make $\beta_i = 0$, which means that SU i does not launch the SSDF attack at all. Obviously, this condition does not satisfy the definition of the malicious SU. Another selection is to make $p(H_0)\left[(1-P_{\mathrm{f},i})\sum_{k=1}^{l-1}\frac{\Pr(u_i=k|H_0)}{M-k} + P_{\mathrm{f},i}\sum_{k=l+1}^{M}\frac{\Pr(u_i=k|H_0)}{k-1}\right] + p(H_1)\left[(1 - P_{\mathrm{d},i})\sum_{k=1}^{l-1}\frac{\Pr(u_i=k|H_1)}{M-k} + P_{\mathrm{d},i}\sum_{k=l+1}^{M}\frac{\Pr(u_i=k|H_1)}{k-1}\right] = 0, \forall l \in \{1,2,\ldots,M\}$ as $\beta_i \neq 0$. That is, which means that $P_{\mathrm{d},i}$ changes with the value of l. However, by adopting Neyman-Pearson detector, SU i makes local decision as $y_i \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \phi_i$, where $\phi_i = \sigma_i^2(Q^{-1}(\overline{P_{\mathrm{f},i}})\sqrt{\frac{2}{J}} + 1)$ and $\overline{P_{\mathrm{f},i}}$ is the required local false-alarm probability at SU i. The local detection probability of SU i is $P_{\mathrm{d},i} = Q\left(\frac{(Q^{-1}(\overline{P_{\mathrm{f},i}})\sqrt{\frac{2}{J}}+1)-(1+\mu_i)}{\sqrt{\frac{2(1+\mu_i)}{J}}}\right)$. Obviously, it contradicts (37), as shown at the top of the next page. Hence, when $\beta_i \neq 0$, it is impossible to make $\Pr(v_i = l | TY_i = \mathrm{M}) = 1/M$, $\forall l \in \{1,2,\ldots,M\}$.

Therefore, the malicious SU is always detectable. ■

According to Glivenko-Cantelli Theorem, $\pi_{i,l} \to \Pr(v_i = l | TY_i = \mathrm{H}) = 1/M$ or $\pi_{i,l} \to \Pr(v_i = l | TY_i = \mathrm{M})$ as T is large enough. For a practical system, it is impossible for obtaining infinity samples to estimate $\pi_{i,l}$. In this paper, the required number of sensing intervals is computed using the confidence interval method.

It is assumed that the required number of the sensing intervals for estimating $\pi_{i,l}$ is $T_{i,l}$. According to

$$P_{\mathrm{d},i} = \frac{p(H_0)P_{\mathrm{f},i}\left[\sum_{k=l+1}^{M}\frac{\Pr(u_i=k|H_0)}{k-1} - \sum_{k=1}^{l-1}\frac{\Pr(u_i=k|H_0)}{M-k}\right] + \frac{l-1}{M}\sum_{k=1}^{l-1}\frac{1}{M-k}}{p(H_1)\left[\sum_{k=1}^{l-1}\frac{\Pr(u_i=k|H_1)}{M-k} - \sum_{k=l+1}^{M}\frac{\Pr(u_i=k|H_1)}{k-1}\right]}, \quad \forall l \in \{1,2,\ldots,M\}, \tag{37}$$

the CLT, $\pi_{i,l}$ follows asymptotically normal distribution with mean and variance $\Pr(v_i = l|TY_i = \mathrm{H})$ (or $\Pr(v_i = l|TY_i = \mathrm{M})$) and $\frac{\Pr(v_i=l|TY_i=\mathrm{H})[1-\Pr(v_i=l|TY_i=\mathrm{H})]}{T_{i,l}}$ (or $\frac{\Pr(v_i=l|TY_i=\mathrm{M})[1-\Pr(v_i=l|TY_i=\mathrm{M})]}{T_{i,l}}$) for a normal (or malicious) SU, $l = 1, 2, \ldots, M$.

Define I_0 and I_1 be two-sided test problems $\pi_{i,l} = \Pr(v_i = l|TY_i = \mathrm{H})$ (or $\pi_{i,l} = \Pr(v_i = l|TY_i = \mathrm{M})$) and $\pi_{i,l} \neq \Pr(v_i = l|TY_i = \mathrm{H})$ (or $\pi_{i,l} \neq \Pr(v_i = l|TY_i = \mathrm{M})$), respectively. By controlling the number of samples, we can make the error probability under I_1 below a certain limited value. For the two-sided test problem, the conditions $|\pi_{i,l} - \Pr(v_i = l|TY_i = \mathrm{H})| \geq \vartheta$ (or $|\pi_{i,l} - \Pr(v_i = l|TY_i = \mathrm{M})| \geq \vartheta$) and $1 - \Pr(\pi_{i,l} = \Pr(v_i = l|TY_i = \mathrm{H})) \leq \gamma$ (or $1 - \Pr(\pi_{i,l} = \Pr(v_i = l|TY_i = \mathrm{M})) \leq \gamma$) need to be satisfied under I_1, where $\Pr(\pi_{i,l} = \Pr(v_i = l)|TY_i = \mathrm{H})$ (or $\Pr(\pi_{i,l} = \Pr(v_i = l)|TY_i = \mathrm{M})$) denotes the probability of the event $\pi_{i,l} = \Pr(v_i = l|TY_i = \mathrm{H})$ (or $\pi_{i,l} = \Pr(v_i = l|TY_i = \mathrm{M})$).

According to sampling size formula of two-sided test problem, when the confidence interval is set as ν, the required number of sensing intervals for estimating $\pi_{i,l}$ needs to satisfy

$$T_{i,l} \geq (z_{\nu/2} + z_\gamma)^2 \frac{\pi_{i,l}(1-\pi_{i,l})}{\vartheta^2}, \tag{38}$$

where z_x is the quantiles, $z_x = \Phi^{-1}(x)$, and $\Phi(x) = \int_{-\infty}^{x}\exp(-t^2/2)\,\mathrm{d}t/\sqrt{2\pi}$. As ν and γ are given, $z_{\nu/2}$ and z_γ can be obtained by table lookup.

Since the FC needs to estimate all the PMFs of reported quantized levels of SU i, the required number of sensing intervals for SU i, T_i, can be set as $T_i = \max_l T_{i,l}$. For a CRN with N SUs, the observation time window for the proposed malicious SU identification method can be selected as

$$T = \max_i T_i. \tag{39}$$

C. Adaptive Linear Combination Rule

In the way mentioned in Subsection IV.B, it is possible to resolve the SSDF attack problem by excluding malicious SU(s) from the information fusion process at the FC. After identifying and isolating malicious SUs, the FC performs the spectrum sensing process with M-ary quantized data from identified normal SUs.

Let N_{H} denote the number of identified normal SUs. Furthermore, from (13), (14) and (22), the distribution parameters, $\mu_{i,0} = E(\psi^{-1}(v_i)|H_0)$, $\mu_{i,1} = E(\psi^{-1}(v_i)|H_1)$, $\sigma_{i,0}^2 = \sigma^2(\psi^{-1}(v_i)|H_0)$ and $\sigma_{i,0}^2 = \sigma^2(\psi^{-1}(v_i)|H_1)$, should be estimated for N_{H} identified normal SUs, $i = 1, 2, \ldots, N_{\mathrm{H}}$.

These parameters are estimated by observing the reporting data over multiple learning iterations. In each iteration t, FC observes the reporting quantized data from SUs for L detection intervals to learn the respective distribution parameters. Let $\mathbf{z}_i(t) = \left(z_i^0(1),\ z_i^0(2),\ \ldots, z_i^0(L_0(t)), z_i^1(L_0(t)+1), z_i^1(L_0(t)+2), \ldots, z_i^1(L)\right)$ be the buffered quantized data coming from the identified normal SU i, where $L_0(t)$ denotes the number of times $\mathcal{H}_0$ occurred in learning iteration t, z_i^0 and z_i^1 denote the reporting quantized data of SU i for $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, and $z_i^{0/1}(l) = \psi_i^{-1}(v_i(l))$.

To estimate the distribution parameter set of the identified normal SU i, $(\mu_{i,0},\ \mu_{i,1},\ \sigma_{i,0}^2,\ \sigma_{i,1}^2)$, a maximum likelihood-based estimator is used. Let $(\hat{\mu}_{i,0}(t),\ \hat{\mu}_{i,1}(t),\ \hat{\sigma}_{i,0}^2(t),\ \hat{\sigma}_{i,1}^2(t))$ denote the estimated distribution parameter set of the identified normal SU i at learning iteration t. Hence, the maximum likelihood estimates of $\mu_{i,0},\ \mu_{i,1},\ \sigma_{i,0}^2,\ \sigma_{i,1}^2$ can be expressed in a recursive form as follows:

$$\begin{aligned}\hat{\mu}_{i,0}(t+1) &= \frac{\sum_{m=1}^{t}L_0(m)}{\sum_{m=1}^{t+1}L_0(m)}\hat{\mu}_{i,0}(t) \\ &\quad + \frac{1}{\sum_{m=1}^{t+1}L_0(m)}\sum_{l=1}^{L_0(t+1)}z_i^0(l),\end{aligned} \tag{40}$$

$$\begin{aligned}\hat{\mu}_{i,1}(t+1) &= \frac{\sum_{m=1}^{t}[L-L_0(m)]}{\sum_{m=1}^{t+1}[L-L_0(m)]}\hat{\mu}_{i,1}(t) \\ &\quad + \frac{1}{\sum_{m=1}^{t+1}[L-L_0(m)]}\sum_{l=L_0(t+1)+1}^{L}z_i^1(l),\end{aligned} \tag{41}$$

$$\begin{aligned}\hat{\sigma}_{i,0}^2(t+1) &= \frac{\left(\sum_{m=1}^{t}L_0(m)\right)\{\hat{\sigma}_{i,0}^2(t) + [\hat{\mu}_{i,0}(t+1) - \hat{\mu}_{i,0}(t)]^2\}}{\sum_{m=1}^{t+1}L_0(m)} \\ &\quad + \frac{\sum_{l=1}^{L_0(t+1)}[z_i^0(l) - \hat{\mu}_{i,0}(t+1)]^2}{\sum_{m=1}^{t+1}L_0(m)},\end{aligned} \tag{42}$$

$$\begin{aligned}\hat{\sigma}_{i,1}^2(t+1) &= \frac{\left(\sum_{m=1}^{t}[L-L_0(m)]\right)\{\hat{\sigma}_{i,1}^2(t) + [\hat{\mu}_{i,1}(t+1) - \hat{\mu}_{i,1}(t)]^2\}}{\sum_{m=1}^{t+1}[L-L_0(m)]} \\ &\quad + \frac{\sum_{l=L_0(t+1)+1}^{L}[z_i^1(l) - \hat{\mu}_{i,1}(t+1)]^2}{\sum_{m=1}^{t+1}[L-L_0(m)]}.\end{aligned} \tag{43}$$

Substituting (40)-(43) into (22), the optimal weighted coefficients of the linear combination rule at the FC for those identified normal SUs after learning iteration t can be represented as

$$w_i(t) = \frac{\frac{\hat{\mu}_{i,1}(t)-\hat{\mu}_{i,0}(t)}{\hat{\sigma}_{i,1}^2(t)}}{\sum_{k=1}^{N_{\mathrm{H}}}\frac{\hat{\mu}_{k,1}(t)-\hat{\mu}_{k,0}(t)}{\hat{\sigma}_{k,1}^2(t)}}, \quad i = 1, 2, \ldots, N_{\mathrm{H}}. \tag{44}$$

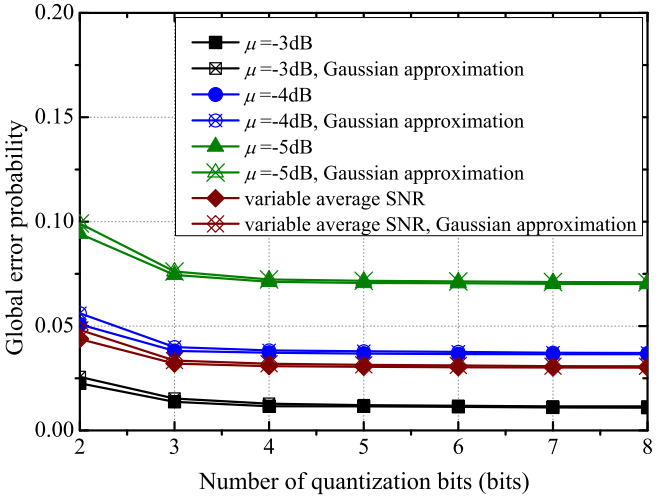


Fig. 3. The performance of the CSS scheme with M-ary quantized data without malicious SUs, where the MOE quantization method and its Gaussian approximation are considered.

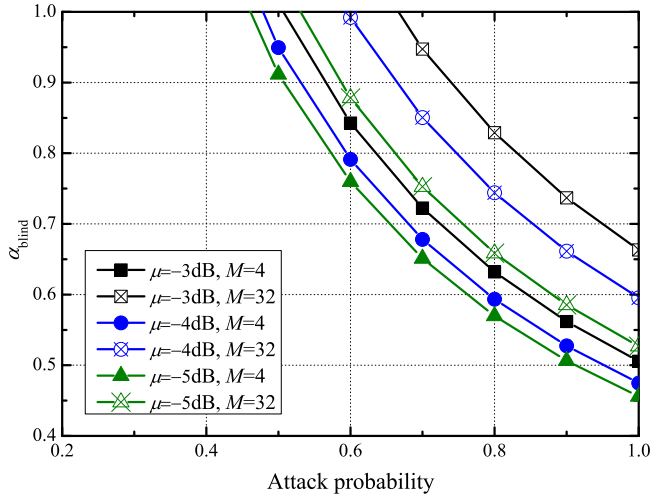


Fig. 4. Impact of the attack probability on the minimum fraction of malicious SUs to make the FC blind.

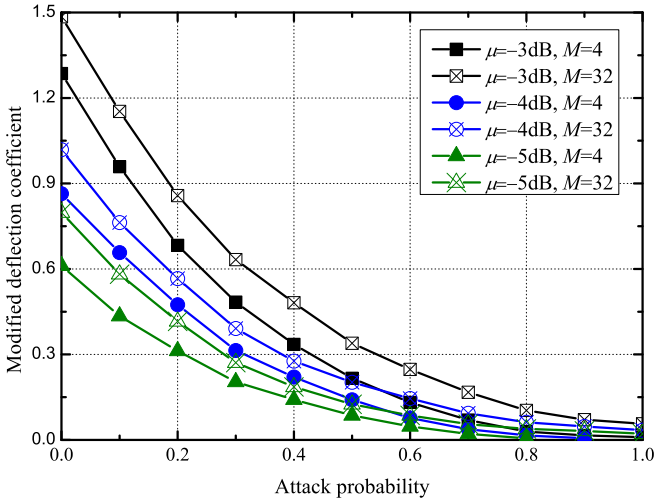


Fig. 5. Impact of the attack probability on the detection performance.

V. Performance Valuations

In this section, we perform a few experiments based on simulated data to validate our attack/defense analysis and demonstrate the performance of the proposed CSS scheme with M-ary quantized data.

We consider a CRN consisting of 1 PU, 1 FC and 12 SUs located far away from the PU. In each sensing interval, $J = 20$. We assume that $p(H_1) = p(H_0) = 0.5$, and $\bar{Q}_{\text{f}} = 0.1$.

A. Performance of the MOE Quantization Method

Fig. 3 shows the performance of the CSS with M-ary quantized data in terms of the global error probability using the MOE quantization method and its Gaussian approximation, where all SUs are normal, and $\sigma_i^2 = \sigma^2 = 1$ for all SUs. For the case of variable average SNR at SUs, $\{\mu_i\} = \{-4.0, -3.9, -3.0, -4.0, -3.8, -4.0, -3.9, -3.8, -3.9, -3.0, -3.8, -4.0\}$ in dB for 12 SUs, and $w_i = \mu_i / \sum_{i=1}^{N} \mu_i$ for SU i. For the case of similar average SNR at SUs, $\mu_i = \mu$, and $w_i = w = 1/12$ for all SUs. Here, we consider the CSS is carried out under the assumption of conditionally independent observations from SUs.

From Fig. 3, we observe that the performance of the CSS with M-ary quantized data using the MOE quantization method and its Gaussian approximation is nearly identical, which means that the Gaussian approximation can replace the MOE quantization method in the performance evaluation to reduce the computational complexity. Furthermore, we also observe that the performance of the CSS with M-ary quantized data improves as the number of quantization bits increases. Obviously, the performance improvement is in the price of the communication overhead. When the number of quantization bits is large enough, the global error probability does not degrade any more. Hence, to achieve a good trade-off between the communication overhead and the performance of the CSS with M-ary quantized data, it is reasonable to set $M = 32$.

B. Behavior of the Probabilistic SSDF Attack Model

Fig. 4 shows the impact of the attack probability on the minimum fraction of malicious SUs, α_{blind}, to make the FC blind for the proposed probabilistic SSDF attack model, where $\mu_i = \mu$, $\sigma_i^2 = \sigma^2 = 1$ and $w_i = w = 1/12$ for all SUs, $P_{\text{f},i} = P_{\text{f}} = 0.2$ and $\beta_i = \beta$ for all malicious SUs.

From Fig. 4, we observe that as the attack probability increases, the security performance of the CSS with M-ary quantized data under SSDF attacks degrades because the minimum fraction of SUs needed to be compromised by the attacker decreases. Furthermore, when the attack probability is smaller than a certain value, the SSDF attacker needs to compromise most SUs to blind the FC for the probabilistic SSDF attack in the CSS.

Fig. 5 shows the impact of the attack probability on the detection performance of the CSS with M-ary quantized data in terms of the modified deflection coefficient under the proposed probabilistic SSDF attack model, where $K = 6$, $\mu_i = \mu$, $\sigma_i^2 = \sigma^2 = 1$ and $w_i = w = 1/12$ for all SUs, $P_{\text{f},i} = P_{\text{f}} = 0.2$ and $\beta_i = \beta$ for all malicious SUs.

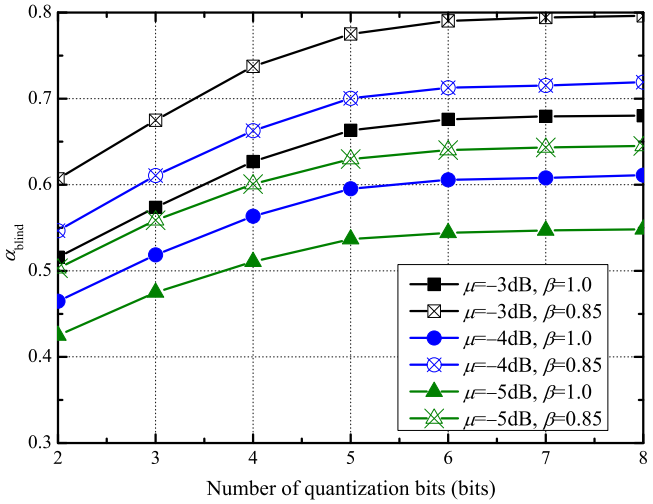


Fig. 6. Impact of the number of quantization bits on the minimum fraction of malicious SUs to blind the FC.

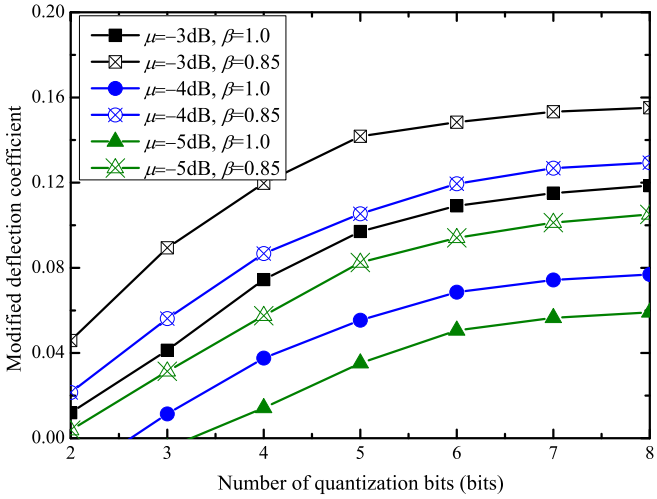


Fig. 7. Impact of the number of quantization bits on the detection performance.

From Fig. 5, we observe that the detection performance of the CSS with M-ary quantized data degrades rapidly as the attack probability increases. When the attack probability is large enough, the modified deflection coefficient of the CSS with M-ary quantized data approaches zero, which means that the FC cannot infer the status of PU correctly.

In practical, as the attack probability increases, the possibility of the malicious SUs being identified by the system increases. Therefore, a tradeoff between the performance damage and the hazard to be discovered needs to be settled by the attacker.

Fig. 6 shows the impact of the number of quantization bits on the minimum fraction of malicious SUs, α_{blind}, to make the FC blind for the proposed probabilistic SSDF attack model, where $\mu_i = \mu$, $\sigma_i^2 = \sigma^2 = 1$ and $w_i = w = 1/12$ for all SUs, $P_{\text{f},i} = P_{\text{f}} = 0.2$ and $\beta_i = \beta$ for all malicious SUs.

From Fig. 6, we observe that as the number of quantization bits increases, the security performance of the CSS with M-ary quantized data under SSDF attacks improves because the minimum fraction of SUs needed to be compromised by the attacker increases. However, the security performance does not keep improving as the number of quantization bits is large enough.

Fig. 7 shows the impact of the number of quantization bits on the detection performance of the CSS with M-ary quantized data in terms of the modified detection coefficient under the proposed probabilistic SSDF attack model, where $K = 6$, $\mu_i = \mu$, $\sigma_i^2 = \sigma^2 = 1$ and $w_i = w = 1/12$ for all SUs, $P_{\text{f},i} = P_{\text{f}} = 0.2$ and $\beta_i = \beta$ for all malicious SUs.

From Fig. 7, we observe that the detection performance of the CSS with M-ary quantized data improves as the number of quantization bits increases. However, the detection performance does not keep improving as the number of quantization bits is large enough.

In practical, as the number of quantization bits increases, the communication overhead of the quantized data transmission increases. Therefore, the defender should face with a tradeoff between the performance damage and the communication overhead.

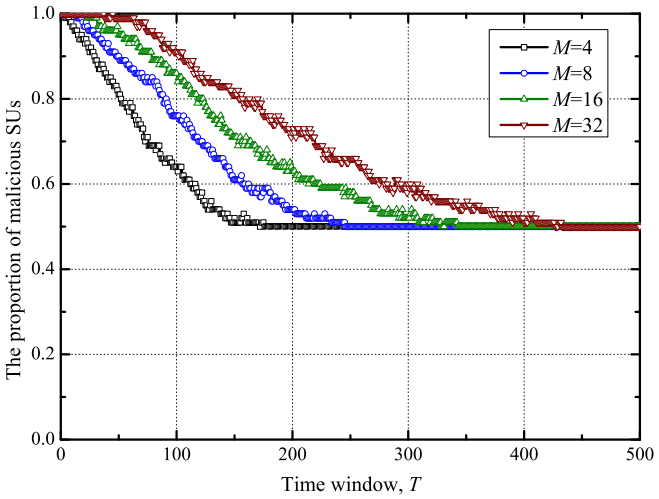
C. Performance of the Malicious SU Identification Method

Fig. 8 plots the performance of the proposed malicious SU identification method as a function of the time window T, in terms of the proportion of identified malicious SUs in Fig. 8(a) and the false identification probability in Fig. 8(b), where $K = 6$, $\mu_i = \mu$, $\sigma_i^2 = \sigma^2 = 1$ for all SUs, $P_{\text{f},i} = P_{\text{f}} = 0.2$ and $\beta_i = \beta = 1$ for all malicious SUs, and $\zeta = 0.01$.

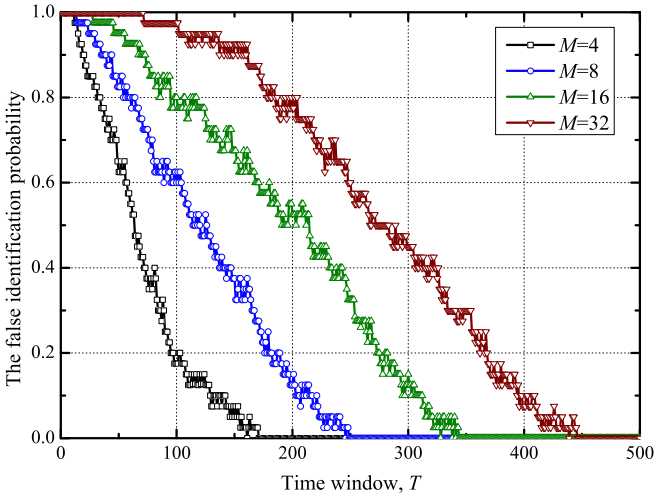
From Fig. 8, we observe that as the time window increases, the performance of the proposed malicious SU identification method improves. However, the performance degrades as the number of the quantization bits increases. Specifically, SUs are differentiated successfully as $T = 171,\ 249,\ 344$ and 452 for $M = 4,\ 8,\ 16$ and 32, respectively. The reason for this phenomenon is that for the M-ary quantization scheme, the required observation time window for estimating $\pi_{i,l}$ $(l = 1, 2, \ldots, M)$ precisely increases as the number of quantization bits increases. Furthermore, it can be seen in Figs. 8(a) and 8(b) that malicious SUs are always declared correctly, while the normal SUs are declared as malicious when the time window is not large enough. The reason for this phenomenon is that, for the M-ary quantization scheme, the required observation time window should be large enough for estimating $\pi_{i,l} (l = 1, 2, \ldots, M)$ precisely.

Fig. 9 shows the identification probability of the proposed malicious SU identification method, where $\mu_i = \mu$, and $\sigma_i^2 = \sigma^2 = 1$ for all SUs, $P_{\text{f},i} = P_{\text{f}} = 0.2$ and $\beta_i = \beta = 1$ for all malicious SUs, $\zeta = 0.01$, $T = 175$ and 455 for $M = 4$ and 32, respectively.

From Fig. 9, we observe that the identification probability of the proposed method increases as the attack probability increases. This is because when the attack probability increases, the behavior deviation between the malicious and normal SUs also increases, which makes malicious SUs easy to be identified. Furthermore, for a given attack probability, the identification probability decreases as the number of quantization bits increases. The reason for this phenomenon



(a) the proportion of identified malicious SUs



(b) the false identification probability

Fig. 8. Identification performance vs. time window T.

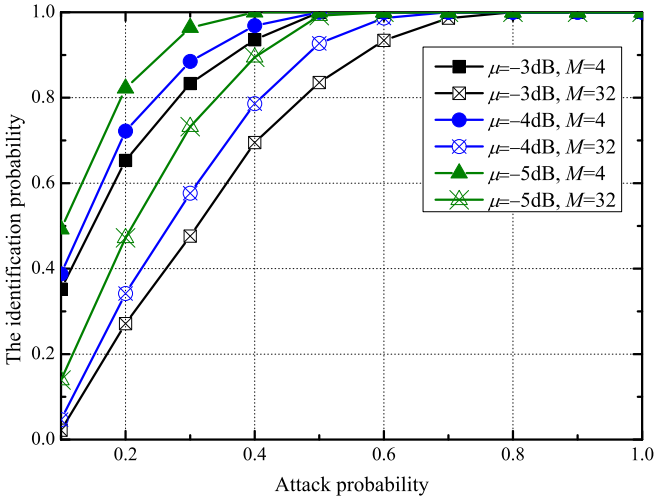


Fig. 9. The identification probability of the proposed malicious SU identification method.

is that the quantization region reduces as the number of quantization bits increases, which also makes the behavior deviation between the malicious and normal SUs reduce.

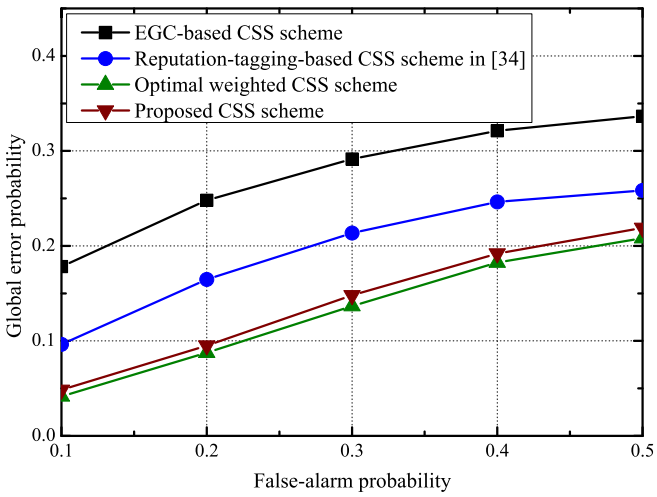


Fig. 10. The performance comparison of different CSS schemes with M-ary quantized data.

D. Performance of the CSS Scheme With M-ary Quantized Data Under SSDF Attacks

Fig. 10 shows the performance comparison of different CSS schemes with M-ary quantized data, where $M = 32$, $K = 3$, and $\sigma_i^2 = \sigma^2 = 1$ for all SUs, $\{\mu_i\} = \{-4.0, -3.9, -3.8, -4.0, -3.8, -4.0, -3.9, -3.8, -3.9\}$ in dB for 9 normal SUs, $P_{\mathrm{f},i} = P_{\mathrm{f}} = 0.2$ and $\beta_i = \beta = 1$ for all malicious SUs, $\{\mu_i\} = \{-3.8, -3.9, -4.0\}$ in dB for 3 malicious SUs, $\zeta = 0.01$ and $T = 455$ for the proposed malicious SU identification method, $L = 64$ and the number of iterations is 5 for the proposed adaptive linear combination rule.

It can be seen in Fig. 10 that the performance of the proposed CSS scheme with the proposed malicious SU identification method and adaptive linear combination rule is better than that of the EGC-based CSS scheme and reputation-tagging-based CSS scheme in [34], but a bit worse than that of the optimal weighted CSS scheme. However, the distribution parameter sets of all SUs are needed for the optimal weighted CSS scheme, while only distribution parameter sets of identified normal SUs need to be estimated for the proposed CSS scheme. Since the FC has no *a priori* information about the SSDF attack model, obtaining the distribution parameter sets of the malicious SUs is intractable. Since the malicious SU identification method does not depend on the global detection result in the proposed CSS scheme, the malicious identification performance is better than that of the malicious identification method in [34] when the SNR is low at SUs or/and the number of the malicious SUs is much large. Hence, the performance of the proposed CSS scheme is better than that of the reputation-tagging-based CSS scheme in [34].

Fig. 11 plots the performance of the proposed CSS scheme with M-ary quantized data as a function of the attack probability, where $\mu_i = \mu = -4$dB, $\sigma_i^2 = \sigma^2 = 1$, and $w_i = w = 1/N_{\mathrm{H}}$ for all identified SUs, $P_{\mathrm{f},i} = P_{\mathrm{f}} = 0.2$ and $\beta_i = \beta = 1$ for all malicious SUs. For the proposed malicious SU identification method, $\zeta = 0.01$, $T = 175$ and 455 for $M = 4$ and 32, respectively. For the proposed adaptive linear combination rule, $L = 64$ and the number of iterations is 5.

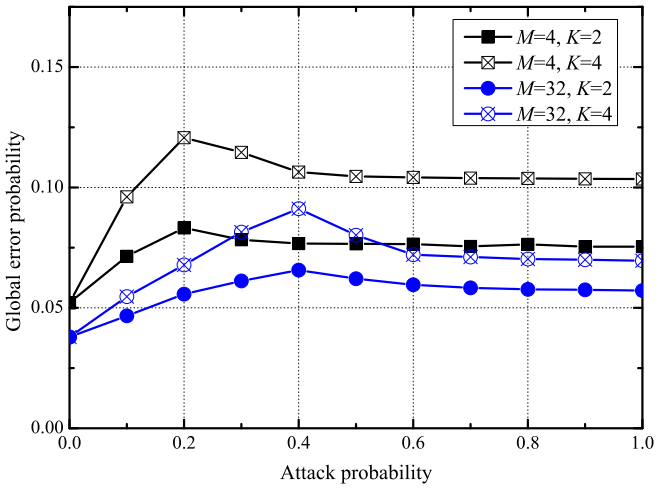


Fig. 11. Global error probability vs. attack probability.

It is shown in Fig. 11 that for the proposed CSS scheme, an optimal attack probability, which does not equal to 1, exists. Moreover, the value of the optimal attack probability is related to the number of quantization bits. Furthermore, the performance of the proposed CSS scheme degrades as the number of malicious SUs increases. The reason for this is that for the proposed CSS scheme, the malicious SUs are identified using the malicious SU identification method and removed from the combination process at the FC. The FC performs the spectrum sensing process with M-ary quantized data from the identified normal SUs.

VI. Conclusion

We have studied the challenging and important CSS problem with M-ary quantized data under SSDF attacks. We have significantly extended the research results obtained in [34] by considering a more realistic scenario in the distributed detection, where the malicious SUs have incomplete knowledge about the true hypothesis based on their local sensing results, and the knowledge about the quantization thresholds used have been considered. We introduce a probabilistic SSDF attack model for the CSS with M-ary quantized data. The negative effect of defined probabilistic SSDF attack for the CSS with M-ary quantized data has been characterized, and the condition of the proposed SSDF attack model to make the FC completely incapable of inferring the status of PU has been derived. Furthermore, we propose an efficient method to indentify malicious SUs and remove them from the data fusion process at the FC. The performance of the malicious SU identification method is analytically evaluated. Finally, using a maximum likelihood estimator to estimate the distribution parameter sets of identified normal SUs, we present an adaptive linear combination rule for the fusion process of the CSS with M-ary quantized data under SSDF attacks. The presented analytical expressions followed by simulation results demonstrate that the proposed malicious SU identification method can successfully remove the malicious SUs, and the proposed CSS scheme with M-ary quantized data is robust against SSDF attacks.

References

[1] J. Mitola and G. Q. Maguire, Jr., "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Apr. 1999.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[3] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, 1st Quart., 2009.

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

[5] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part I: Two user networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2204–2213, Jun. 2007.

[6] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part II: Multiuser networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2214–2222, Jun. 2007.

[7] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 28–40, Feb. 2008.

[8] J. Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4502–4507, Nov. 2008.

[9] Y. Zou, Y.-D. Yao, and B. Zheng, "A selective-relay based cooperative spectrum sensing scheme without dedicated reporting channels in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1188–1198, Apr. 2011.

[10] Q. Chen, M. Motani, W.-C. Wong, and A. Nallanathan, "Cooperative spectrum sensing strategies for cognitive radio mesh networks," *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 56–67, Feb. 2011.

[11] G. Taricco, "Optimization of linear cooperative spectrum sensing for cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 77–86, Feb. 2011.

[12] W. Han, J. Li, T. Li, J. Si, and Y. Zhang, "Efficient soft decision fusion rule in cooperative spectrum sensing," *IEEE Trans. Signal Process.*, vol. 61, no. 8, pp. 1931–1943, Apr. 2013.

[13] D.-C. Oh, H.-C. Lee, and H.-Y. Lee, "Linear hard decision combining for cooperative spectrum sensing in cognitive radio systems," in *Proc. IEEE VTCFall*, Sep. 2010, pp. 1–5.

[14] Y. Abdi and T. Ristaniemi, "Joint local quantization and linear cooperation in spectrum sensing for cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 62, no. 17, pp. 4349–4362, Sep. 2014.

[15] H. Chen, M. Zhou, L. Xie, and X. Jin, "Fault-tolerant cooperative spectrum sensing scheme for cognitive radio networks," *Wireless Pers. Commun.*, vol. 71, no. 4, pp. 2379–2397, Aug. 2013.

[16] B. Chen and P. K. Willett, "On the optimality of the likelihood-ratio test for local sensor decision rules in the presence of nonideal channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 693–699, Feb. 2005.

[17] V. Matta, P. Braca, S. Marano, and A. H. Sayed, "Distributed detection over adaptive networks: Refined asymptotics and the role of connectivity," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 2, no. 4, pp. 442–460, Dec. 2016.

[18] V. Aalo, "On distributed detection with correlated sensors: Two examples," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 25, no. 3, pp. 414–421, May 1989.

[19] H. He and P. K. Varshney, "Fusing censored dependent data for distributed detection," *IEEE Trans. Signal Process.*, vol. 63, no. 16, pp. 4385–4395, Aug. 2015.

[20] R. Chen, J.-M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.

[21] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, Aug. 2010.

[22] W. Wang, H. Li, Y. Sun, and Z. Han, "Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks," *EURASIP J. Adv. Signal Process.*, vol. 2010, no. 1, p. 695750, Jan. 2010.

[23] 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.

[24] S. Althunibat, B. J. Denise, and F. Granelli, "Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7308–7321, Sep. 2016.

[25] N. Nguyen-Thanh and I. Koo, "Evidence-theory-based cooperative spectrum sensing with efficient quantization method in cognitive radio," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 185–195, Jan. 2011.

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

[27] A. W. Min, K. G. Shin, and X. Hu, "Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation," *IEEE Trans. Mobile Comput.*, vol. 10, no. 10, pp. 1434–1447, Oct. 2011.

[28] J. Yao, Q. Wu, and J. Wang, "Attacker detection based on dissimilarity of local reports in collaborative spectrum sensing," *IEICE Trans. Commun.*, vol. E95-B, no. 9, pp. 3024–3027, Sep. 2012.

[29] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour, "Decentralized hypothesis testing in wireless sensor networks in the presence of misbehaving nodes," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 205–215, Jan. 2013.

[30] 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.

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

[32] B. Kailkhura, S. Brahma, B. Dulek, Y. S. Han, and P. K. Varshney, "Distributed detection in tree networks: Byzantines and mitigation techniques," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1499–1512, Jul. 2015.

[33] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16–29, Jan. 2009.

[34] V. Nadendla, Y. S. Han, and P. K. Varshney, "Distributed inference with M-ary quantized data in the presence of Byzantine attacks," *IEEE Trans. Signal Process.*, vol. 62, no. 10, pp. 2681–2695, May 2014.

[35] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.

[36] 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.

[37] C. Cordeiro, K. Challapali, D. Birru, and N. S. Shankar, "IEEE 802.22: The first worldwide wireless standard based on cognitive radios," in *Proc. IEEE Symp. New Froniters Dyn. Spectr. Access Netw.*, 2005, pp. 328–337.

[38] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[39] B. V. Gendenko and A. N. Kolmogorov, Eds., *Limit Distributions for Sums of Independent Random Variables*. New York, NY, USA: Addison-Wesley, 1954.

[40] D. Messerschmitt, "Quantizing for maximum output entropy," *IEEE Trans. Inf. Theory*, vol. 17, no. 5, p. 612, Sep. 1971.

[41] D. R. Cox, Ed., *Principles of Statistical Inference*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[42] D. L. Evans and L. M. Leemis, "Algorithms for computing the distributions of sums of discrete random variables," *Math. Comput. Model.*, vol. 40, no. 13, pp. 1429–1452, Dec. 2004.

[43] S. A. Aldosari and J. M. F. Moura, "Detection in sensor networks: The saddlepoint approximation," *IEEE Trans. Signal Process.*, vol. 55, no. 1, pp. 327–340, Jan. 2007.

Huifang Chen (M'99) received the B.S. degree in electronic engineering, and the M.S. and Ph.D. degrees in communications and information systems from Zhejiang University, Hangzhou, China, in 1994, 1997, and 2000, respectively.

Since 2000, she has been with Zhejiang University, where she is currently an Associate Professor with the College of Information Science and Electronic Engineering. She has co-authored one book and has authored over 150 papers. Her current research interests include wireless networks, underwater acoustic networks, adaptive networks, and network security.

She is a member of the ACM and a Senior Member of the China Institute of Communications.

Ming Zhou received the B.S. degree in electrical engineering from the Nanjing University, Nanjing, China, in 2010.

He is currently pursuing the Ph.D. degree with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China. His current research interests include cognitive radio networks, especially the security issues in cognitive radio networks.

Lei Xie (M'02) received the B.S. degree in electronic engineering, and the M.S. and Ph.D. degrees in communications and information systems from Zhejiang University, Hangzhou, China, in 1994, 1997, and 2002, respectively.

Since 1997, he has been with Zhejiang University, where he is currently an Associate Professor with the College of Information Science and Electronic Engineering. His current research interests include information theory and coding, network security, and multimedia streaming in heterogeneous wireless networks.

He is a senior member of the China Institute of Communications.

Jie Li (M'94–SM'04) received the B.E. degree in computer science from Zhejiang University, Hangzhou, China, in 1982, the M.E. degree in electronic engineering and communication systems from the China Academy of Posts and Telecommunications, Beijing, China, in 1985, and the Dr.Eng. degree from the University of Electro-Communications, Tokyo, Japan, in 1993. He is currently a Professor with the Faculty of Engineering, Information and Systems, University of Tsukuba, Japan. He has been a Visiting Professor with Yale University, New Haven, CT, USA, and Inria, France. His current research interests are in mobile distributed computing and networking, big data and cloud computing, IoT, information security, OS, and modeling and performance evaluation of information systems. He is a senior member of the ACM and a member of the Information Processing Society of Japan (IPSJ). He is the Chair of the Technical Committee on Big Data, IEEE Communications Society. He has served as Secretary of the Study Group on System Evaluation, IPSJ, and on several editorial boards for the international journals and steering committees of the SIG of System Evaluation of IPSJ, the SIG of DataBase System of IPSJ, and the SIG of Mobile Computing and Ubiquitous Communications of IPSJ. He has also served on the program committees for several international conferences such as the IEEE INFOCOM, the IEEE GLOBECOM, and the IEEE MASS.