IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 9, 2016, accepted July 15, 2016, date of publication August 8, 2016, date of current version August 26, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2593952

Defending Against Byzantine Attack in Cooperative Spectrum Sensing: Defense Reference and Performance Analysis

LINYUAN ZHANG[1], GUORU DING[1,2], (Senior Member, IEEE), QIHUI WU[3], (Senior Member, IEEE), AND FEI SONG[1]

[1]College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China
[2]National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
[3]College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China

Corresponding author: G. Ding (dr.guoru.ding@ieee.org)

This work was supported in part by the National Natural Science Foundation of China under Grant 61501510 and Grant 61301160, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20150717, in part by the China Postdoctoral Science Foundation Funded Project, and in part by the Jiangsu Planned Projects for Postdoctoral Research Funds.

ABSTRACT Cooperative spectrum sensing (CSS) has been well recognized as an effective method to improve spectrum sensing accuracy and decrease sensing devices' complexity. However, spectrum sensing data falsification attack, also known as Byzantine attack, poses critical threats on the reliability of CSS. Due to lack of the ground-truth spectrum state, a reliable defense reference is vital to identify malicious behaviors and perform effective data fusion. However, the existing defense references have strong assumptions such as the attackers are in minority and/or a trusted node exists for data fusion. This observation motivates this paper to propose a novel defense reference, which jointly exploits the cognitive process of spectrum sensing and spectrum access in a closed-loop manner, to provide the defense scheme a solid basis without requiring any prior knowledge. Moreover, this paper analyzes the proposed reference's favorable reliability and high robustness over the state-of-the-art references, from two perspectives of spectrum sensing performance and the capability of identifying malicious sensors, respectively. Next, we design an optimal cooperative spectrum sensing scheme based on the proposed defense reference. Remarkably, from an information theoretic perspective, it is observed that based on the proposed reference, the information value of falsified reports is also exploited to further improve the global sensing performance. Furthermore, numerical simulations verify the proposed scheme's favorable performance, even in critical cases when malicious sensors are in majority.

INDEX TERMS Cognitive radio network, spectrum sensing, Byzantine attack, reliable reference.

I. INTRODUCTION

In cognitive radio networks, spectrum sensing enables secondary users to effectively explore spectrum holes while avoiding harmful interference to primary users [1]. However, the performance of spectrum sensing is susceptible to the integrated effects of noise, path loss, shadowing, and multipath fading [2]. To improve spectrum sensing performance, cooperative spectrum sensing (CSS) is needed to call upon a crowd of spectrum sensors to reap the spatial diversity [3]. Due to the openness of wireless channels [4], CSS is vulnerable to threats from abnormal reports incurred by various factors, such as equipment failure and malicious falsification [5], [6]. Specifically, the case of malicious falsification is well known as spectrum sensing data falsification attack, also named as Byzantine attack [7]. Our previous work has presented a comprehensive survey on this topic in [8]. Briefly, Byzantine attackers report falsified sensing results to mislead a fusion center to make a wrong decision, which seriously deteriorates the global spectrum sensing performance.

To eliminate the damage of Byzantine attack in CSS, several studies about Byzantine defense have been done (see [5], [9]–[18], [20]). Generally, a Byzantine defense scheme consists of three sequential procedures: i) designing a defense reference,[1] ii) evaluating sensors' trustiness or reputations, and iii) making final decisions based on

[1]In the paper, we use the phrase "reference" to represent a reliable standard, telling the SU whose report is right and whose report is wrong.

TABLE 1. Notations and symbols used in this paper.

Symbol	Definition
$\mathcal{H}$	The channel's real states
N_u	The number of sensors
N_m	The number of malicious sensors, i.e., attack population
p_a	The probability of a malicious sensor conducting attacks
$\mathcal{U}$	Sensor's reports
P_f^H	The false-alarm probability of an honest sensor
p_d^H	The detection probability of an honest sensor
P_f^B	The false-alarm probability of a Byzantine sensor
p_d^B	The detection probability of a Byzantine sensor
$\mathcal{F}$	Global decisions
Q_F^G	The global false-alarm probability
Q_M^G	The global miss-detect probability
$\mathcal{A}$	The results of the proposed reference
Q_F^R	The false-alarm probability of the proposed reference
Q_D^R	The detection probability of the proposed reference
Q_M^R	The miss-detect probability of the proposed reference
P_f^{EX}	The false-alarm probability of extended sensing over the whole slot
P_m^{EX}	The miss-detect probability of extended sensing over the whole slot
P_{fn}	The probability of an honest sensor mistaken as a malicious one
P_{fp}	The probability of a malicious sensor mistaken as an honest one
φ_f	The general denotation of certain reference's false-alarm probability
φ_d	The general denotation of certain reference's detection probability

evaluation results. Due to lack of the ground-truth spectrum state, a reliable defense reference is the cornerstone to identify malicious behaviors and perform effective data fusion.

Generally, the existing defense references in the literature can be grouped into three classes: global decision based reference (see [13], [14], [19]), mean-based reference (see [21], [22]), and trusted node(s) assisted reference (see [15], [23]). The first two references are built on fusion results from all reports and have an assumption that malicious sensors are in minority. In the third reference, it is assumed that there is one or several trusted sensors known by the fusion center and the trusted nodes' reports are used as the basis of evaluating other sensors. In practice, the prior knowledge of trusted nodes may be hard to obtain and, in some cases, trusted node(s) may suffer from serious shadowing and have inferior spectrum sensing performance.

Motivated by the fact that the existing references have strong assumptions such as the attackers are in minority or trusted node(s) exist for data fusion, this paper firstly focuses on the issue of designing a general and reliable reference for CSS. Instead of being limited to the sensing phase which makes it hard to avoid negative effects of falsified reports, the proposed reference jointly exploits the cognitive process of spectrum sensing and spectrum access in a closed-loop manner, to provide the defense scheme with a solid basis. Then, we analyze and prove the proposed reference's favorable reliability and high robustness over the state-of-the-art references, from two perspectives: the performance of spectrum sensing and the capability of identifying malicious sensors, respectively. Next, we design an optimal cooperative spectrum sensing scheme with the proposed defense reference. Remarkably, from an information theoretic perspective, it is observed that based on the proposed reference, the value of falsified reports is also exploited to further improve the global sensing performance. Furthermore, numerical simulations verify the proposed scheme's favorable performance, even in critical cases when malicious sensors are in majority.

Interestingly, due to the weak assumption and high feasibility, the proposed reference and defense scheme can be easily extended to the distributed networks in which no dedicated fusion center exists. In the distributed networks, the global view is hard to obtain and thus every honest user has to rely on its own results to more extent, which highlights the special role of the proposed reference and defense scheme.

The rest of this paper is organized as follows. Section II presents the system model. Section III introduces the proposed defense reference. Further, the proposed reference's performance is analyzed and compared with other references' in Section IV. Then, in Section V, an optimal cooperative spectrum sensing method and the proposed algorithm are described. Furthermore, we evaluate the performance of the proposed algorithm in Sections VI, followed by the conclusion in Sections VII. The key notations and symbols used in this paper are given in Table 1. A preliminary conference version of this paper has been presented in [24].

II. SYSTEM MODEL

As illustrated in Fig. 1, in this paper we consider the case that a secondary user (SU) has unfavorable sensing performance, possibly due to shadowing. Hence, the assistance from N_u neighboring spectrum sensors is introduced to improve the reliability of spectrum sensing. Specifically, each individual sensor firstly implements energy detection to obtain a local decision and then reports the corresponding results to the SU. The reports are fused in the SU and a global decision $\mathcal{F}$ is made on the state of the targeted channel.

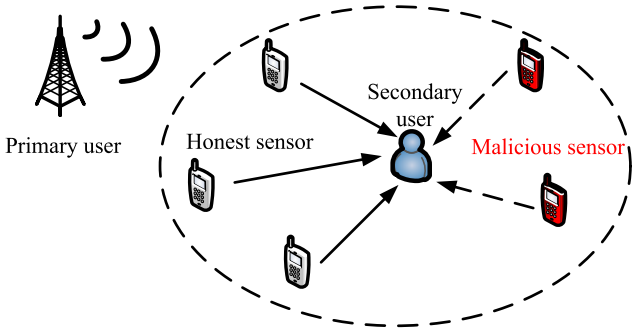


FIGURE 1. System model.

For each sensor, the spectrum sensing is generally formulated as a binary hypotheses test problem as follows [25]:

$$\begin{aligned} &\mathcal{H}_0 : r(t) = n(t) \\ &\mathcal{H}_1 : r(t) = h \cdot s(t) + n(t), \end{aligned} \tag{1}$$

where $\mathcal{H}_0$ denotes the case that PU is absent, $\mathcal{H}_1$ denotes the case that PU is present, $r(t)$ is the SU's received signal at that sensor in time t, $s(t)$ is the PU's transmit signal, h is the channel gain, and $n(t)$ denotes the additive white Gaussian noise.

With an energy detector, the collected energy observation can be given as $x_E = \sum_{t=1}^{2U} |r(t)|^2$, where $U = TW$ is the time-bandwidth product. According to the central limit theorem, when U is large enough (e.g., $U \gg 10$), x_E can be well approximated as a Gaussian random variable under both hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ as follows [26]:

$$\begin{cases} \mathcal{H}_0 : x_E \sim N(\mu_0, \sigma_0^2) \\ \mathcal{H}_1 : x_E \sim N(\mu_1, \sigma_1^2), \end{cases} \tag{2}$$

where $\mu_0 = 2U$, $\sigma_0^2 = 4U$, $\mu_1 = 2U(\gamma + 1)$, $\sigma_1^2 = 4U(2\gamma + 1)$ and γ is the received SNR of the SU.

The binary decision d of the SU can be obtained by comparing its energy observation with a local threshold λ,

$$x_E \underset{d=0}{\overset{d=1}{\gtrless}} \lambda. \tag{3}$$

Here, two metrics, the probability of false alarm p_f and the probability of detection p_d, are used to characterize the performance of spectrum sensing and formulated as follows:

$$\begin{cases} P_f^H \triangleq P(d = 1|\mathcal{H}_0) = Q\big(\dfrac{\lambda - \mu_0}{\sigma_0}\big) \\ P_d^H \triangleq P(d = 1|\mathcal{H}_1) = Q\big(\dfrac{\lambda - \mu_1}{\sigma_1}\big), \end{cases} \tag{4}$$

where $Q(x)$ is the Gaussian Q-function and the missed-detection probability $P_m^H = 1 - P_d^H$.

An honest sensor will report its original local decision d to the SU for data fusion, however, a Byzantine attacker or malicious sensor may send a falsified local decision u to mislead the SU to make a wrong decision, i.e., $u \neq d$. Different from the state-of-the-art studies, in this paper, we consider a general case that *the number of attackers can be either in minority and majority, and no trusted node is known as a prior*. Moreover, we consider a generalized attack model that a malicious sensor launches attack with a probability p_a [11], that is to say, it flips its reports with the probability p_a. This model is general since the attack probability p_a can range from 0 to 1, with 0 and 1 denoting two extreme cases of never-attack and always-attack, respectively.

Consequently, the corresponding sensing performance of a malicious sensor is formulated as follows:

$$\begin{cases} P_f^B = P_f^H \cdot (1 - p_a) + (1 - P_f^H) \cdot p_a \\ P_d^B = P_d^H \cdot (1 - p_a) + (1 - P_d^H) \cdot p_a. \end{cases} \tag{5}$$

Based on the sensing reports from all spectrum sensors, the SU performs data fusion to obtain a global decision $\mathcal{F}$ on the state of the targeted channel. The commonly used fusion rules include k-out-of N rule (with OR, AND, and Majority as three special cases) [32] and likelihood ratio test (LRT)-based rule [27]. According to [27], LRT-based rule is the optimal data fusion rule which jointly utilizes the sensing reports and the average sensing performance of each sensors. Relatively, k-out-of N rule is simple to implement and suitable for the case that all sensors have the same sensing performance.

The presence of Byzantine attackers makes the traditional fusion rule inefficient and misleads the SU to obtain a wrong decision on the spectrum state. Therefore, Byzantine defense schemes are needed to recognize sensor behaviors and make robust global detection. However, *due to lack of cooperation from the PU, the SU cannot have the ground-truth spectrum state and thus don't have a ground-truth defense reference to distinguish honest sensors and attackers.* Consequently, the first vital thing of a Byzantine defense scheme is to design a reliable reference based on the available information. In the following section, we will first present a brief review of the existing defense references and analyze the advantages and disadvantages, which motivates us to further propose a new reference.

III. BYZANTINE DEFENSE REFERENCES

A. BRIEF REVIEW OF EXISTING REFERENCES

To eliminate the damage of Byzantine attack and perform effective data fusion in CSS, a reliable defense reference generally serves as the cornerstone to identify malicious behaviors. In general, the existing defense references in the literature can be grouped into the following three classes:

- Global decisions as a reference (GDaR) (see [14]): The rationale of this reference is that although malicious sensors report falsified data, global decisions based on

all reports are reliable at most time when honest sensors are in the majority;
- Soft fusion results as a reference (SFRaR) (see [21], [22]): The combined results, obtained through data fusion before making a global decision, often carry more information than global decisions, such as different trustiness on the two hypothesis;
- Trusted sensor's reports as a reference (TRaR) (see [18], [23]): This reference assumes that certain honest sensor is known to the SU and its report is approximated as the ground-truth of the spectrum state and is used to evaluate other sensors' reports.

These references focus on the processing of reports and try to abstract reliable information to reflect the ground truth. However, they are always subject to the quality of data which is threatened by falsified data. For example, the reference GDaR is built on all reports but the real sensing performance of each sensor is always unknown, thus the reference's reliability is hard to guarantee. Seriously, when attackers are in the majority, the reference is of high inefficiency [14]. The same point also applies to the reference SFRaR. In the reference TRaR, the prior knowledge of trusted nodes in some cases may be hard to obtain and, although trusted node(s) do not provide falsified reports, they may suffer from serious shadowing and have inferior spectrum sensing performance, which will also make the reference TRaR unreliable.

B. THE PROPOSED REFERENCE

Considering the limitations of the state-of-the-art defense references, this subsection proposes a general and reliable reference for CSS.

1) DESIGN RATIONALE

The key idea is to build a reference by jointly exploiting the cognitive process of spectrum sensing and spectrum access in a closed-loop manner. Specifically, the idea of the proposed reference comes mainly from the following observations:

- Traditionally, the cognitive process of each frame consists of a spectrum sensing phase and a spectrum access phase. In the spectrum access phase, whether the SU to access the PU channel depends on the output of the global decision in the sensing phase. That is, if the global decision is PU absent, the SU will access; otherwise, the SU will wait for the next frame. This is indeed an open-loop cognitive manner.
- Once the SU decides to access the PU channel, one of two things can happen: i) success to transmit its data; ii) failure due to collisions with the PU's transmission. Generally, success corresponds to the case that the ground truth is PU absent and the global decision is right, while failure corresponds to the case that the ground truth is PU present and the global decision is a missed detection. This can be used as a feedback to facilitate the design of a reliable defense reference.
- Once the SU decides to wait for the next frame, one of two things also can happen: i) the PU channel is busy; ii) the PU channel is idle and an access opportunity is missed due to a false alarm of the global decision. Considering the fact that the local sensing performance of the SU improves with the increasing sensing time, during the waiting phase, the SU itself can continue to perform spectrum sensing that can enhance the SU's local sensing results significantly (see Fig. 2). The output of the extended sensing can also be used as a useful feedback.

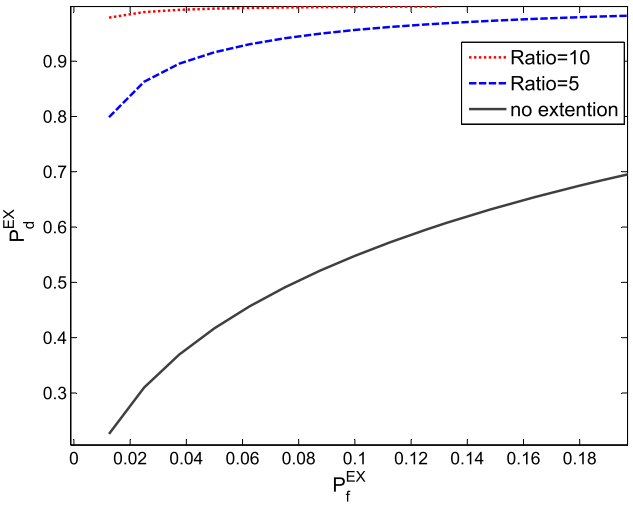


FIGURE 2. Performance with the extended sensing denoted as a false-alarm probability P_f^{EX} and a detection probability P_d^{EX}, where the local SNR is −10dB and the ratio is that of the extended sensing time to the original sensing time. It is observed that the extended sensing can enhance the SU's local sensing performance significantly.

Remark 1: In the proposed scheme, the SU itself performs the extended sensing. Considering the fact that the SU itself cannot obtain reliable spectrum sensing in wireless fading environment, it has to rely on the neighboring sensors to collaboratively obtain accurate spectrum sensing results. However, considering the existence of malicious sensors or collaborators, reliable defense are needed. Moreover, the introduction of spectrum access into the design of defense reference will not harm the primary users, since the proposed reference makes no modification on spectrum access and it just exploits the results of spectrum access. More exactly, in the proposed reference, we combine the output in the spectrum access phase with spectrum sensing output to build a reliable defense scheme, which in turn decreases the miss-detection and protects the primary users' normal communication (See Section IV for details).

Remark 2: There are some related work jointly considering spectrum sensing and access in defending against SSDF attack [20], [28]. In [20], the results of transmission is considered as a reference for defending against SSDF attack, but the transmission results are available only when the PU is declared as idle, which limits its performance. In [28], a joint

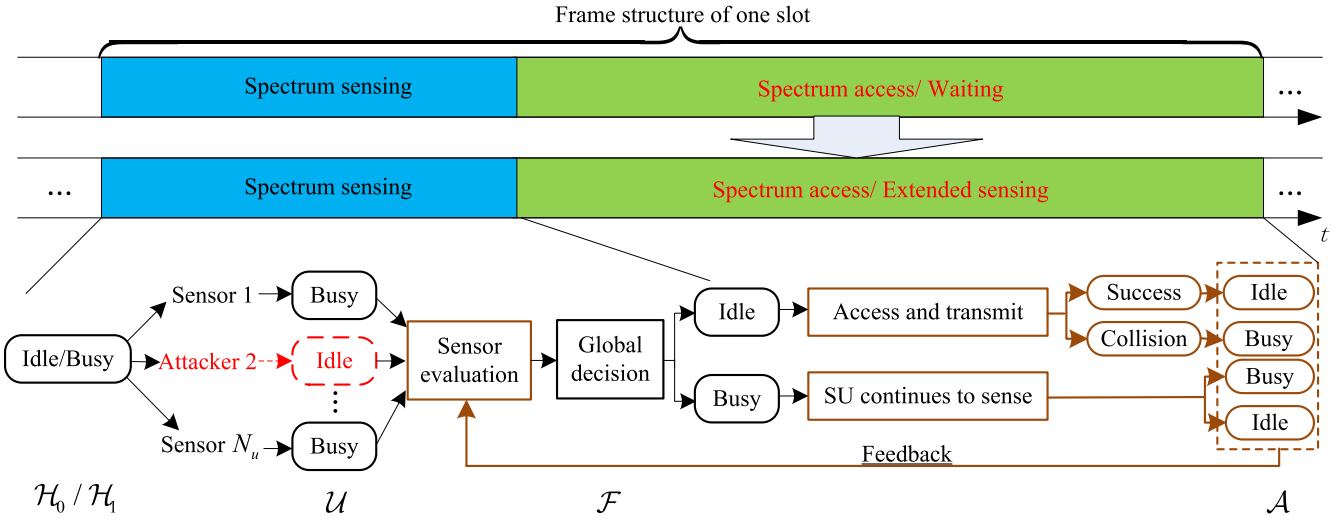


FIGURE 3. The proposed reference, where $\mathcal{H}_0/\mathcal{H}_1$ denotes the real channel state, $\mathcal{U}$ is the reports of sensors, $\mathcal{F}$ is the global decision, and $\mathcal{A}$ denotes the proposed reference's outputs.

spectrum sensing and access mechanism is proposed to thwart the malicious behaviors of rational and irrational intelligent malicious users through incentive compatibility. However, it needs to be noted that the work's defense schemes are built on an assumption that the attackers are selfish and intellect and can adjust their behaviors based on the gains and losses, which is ideal so that the application is limited.

2) REFERENCE DESIGN

Based on the observations above, here we design a novel closed-loop reference for defense, as illustrated in Fig. 3. Specifically, the cognitive process of the proposed scheme is as follows: Firstly, each sensor performs local sensing and reports the original (for an honest sensor) or falsified (for a Byzantine attacker) local decision $\mathcal{U}$ to the SU. Secondly, the SU evaluates the local sensing performance of each sensor, performs the data fusion and makes a global decision $\mathcal{F}$. If the global decision is PU absent (idle), the SU accesses the PU channel; otherwise, if the global decision is PU present (busy), the SU continues to perform extended spectrum sensing during the rest time of the current frame. Furthermore, the access results (success or collision) or the extended sensing results, accompanying the proposed reference $\mathcal{A}$ together, are feedbacked to assist the SU to re-evaluate the local sensing performance of each sensor.

Specifically, in the proposed reference, the probability of false alarms is formulated as,

$$\begin{aligned} Q_F^R &\triangleq P(\mathcal{A}=1|\mathcal{H}_0) \\ &= P(\mathcal{A}=1|\mathcal{H}_0,\mathcal{F}=0)\cdot P(\mathcal{F}=0|\mathcal{H}_0) \\ &\quad + P(\mathcal{A}=1|\mathcal{F}=1,\mathcal{H}_0)\cdot P(\mathcal{F}=1|\mathcal{H}_0) \\ &= 0 + P_f^{EX}\cdot Q_F^G, \end{aligned} \tag{6}$$

where $\mathcal{A} \in \{0(\text{idle}), 1(\text{busy})\}$ represents the results of the proposed reference, $\mathcal{F} \in \{0(\text{idle}), 1(\text{busy})\}$ is the global decision with a false-alarm probability $Q_F^G \triangleq P(\mathcal{F}=1|\mathcal{H}_0)$ and a missed-detection probability $Q_M^G \triangleq P(\mathcal{F}=0|\mathcal{H}_1)$. The SU's extended local spectrum sensing performance is measured with the false alarm probability p_f^{EX} and the miss detection probability p_m^{EX}. The second equation holds via the conditional total probability formula. The third equation holds for the following observations: In the proposed reference shown in Fig. 3, if the global decision is $\mathcal{F}=0$, the SU will access the channel, in this case we can obtain the real channel states from the feedback of the access results. Formally, we have $P(\mathcal{A}=\mathcal{H}_i|\mathcal{F}=0)=1$. Otherwise, if the global decision is $\mathcal{F}=1$, the SU will perform extended spectrum sensing, we can obtain the results of sensing over the whole slot and $P(\mathcal{A}=1|\mathcal{F}=1,\mathcal{H}_0)=P_f^{EX}$.

Similarly, the probability of missed detection in the proposed reference can be obtained as follows:

$$\begin{aligned} Q_M^R &\triangleq P(\mathcal{A}=0|\mathcal{H}_1) \\ &= P(\mathcal{A}=0|\mathcal{H}_1,\mathcal{F}=0)\cdot P(\mathcal{F}=0|\mathcal{H}_1) \\ &\quad + P(\mathcal{A}=0|\mathcal{F}=1,\mathcal{H}_1)\cdot P(\mathcal{F}=1|\mathcal{H}_1) \\ &= 0 + P_m^{EX}\cdot(1-Q_M^G). \end{aligned} \tag{7}$$

Remark 3: The proposed reference has many merits. First of all, the proposed reference follows a closed-loop design that can jointly exploits the cognitive process of spectrum sensing and spectrum access. Secondly, the proposed reference is general since it do not rely on assumptions such as attackers are in minority or trusted nodes are available (see Section IV for details). Thirdly, the proposed scheme can even mine the value of Byzantine attackers' reports (see Section V for details).

IV. PERFORMANCE ANALYSIS AND COMPARISONS

In this section, we perform theoretically and numerical analysis to verify the reliability of the proposed reference by

comparing with the state-of-the-art references. To make fair comparisons, the closeness of various references to the ground-truth is a fundamentally critical factor determining the Byzantine defense performance, which will be evaluated in the first part. Moreover, from the perspective of distinguishing malicious sensors from honest ones, we further verify the reliability of the proposed reference in defending against the Byzantine attack.

A. CLOSENESS OF VARIOUS REFERENCES TO THE GROUND-TRUTH

Due to lack of the ground-truth spectrum state at the SU, the closeness of various references to the ground-truth ($\mathcal{H}_0$(idle) or $\mathcal{H}_1$(busy)) can be measured in terms of spectrum sensing performance, that is, the probabilities of false alarm and missed detection.

To facilitate the analysis and combine the probabilities of false alarm and missed detection into one performance metric, the error probability is a popular choice in the literature [33]. Specifically, for the propose reference given in (7), the error probability Q_e can be given as

$$\begin{aligned} Q_e &\triangleq P(\mathcal{H}_0)Q_F^R + P(\mathcal{H}_1)Q_M^R \\ &= P(\mathcal{H}_0)Q_F^G \cdot P_f^{EX} + P(\mathcal{H}_1)(1-Q_M^G)\cdot P_m^{EX} \\ &= P(\mathcal{H}_0)Q_F^G \cdot Q\Big(\frac{\lambda-\dot{\mu}_0}{\dot{\sigma}_0}\Big) \\ &\quad + P(\mathcal{H}_1)(1-Q_M^G)\cdot Q\Big(\frac{\lambda-\dot{\mu}_1}{\dot{\sigma}_1}\Big), \end{aligned} \tag{8}$$

where $P(\mathcal{H}_0)$ and $P(\mathcal{H}_1)$ are the idle and busy probabilities of the ground-truth channel state, respectively, and due to the extended spectrum sensing, $\dot{\mu}_0$, $\dot{\mu}_1$, $\dot{\sigma}_0$, $\dot{\sigma}_1$ are r times of μ_0, μ_1, σ_0, σ_1 in (2), respectively, where r is the ratio of the whole sensing slot to the original sensing slot.

The threshold λ is a key optimization parameter to determine the detection performance. Specifically, we have obtained the following theorem.

Theorem 1: For the proposed reference, there is an optimal threshold λ_p for the SU to minimize the error probability Q_e as follows

$$\begin{aligned} \lambda_p &= \min_{\lambda} Q_e(\lambda) \\ &= \begin{cases} x, & c \leqslant 0 \\ \arg\min\limits_{\lambda\in\{0,x\}} Q_e(\lambda), & b^2-4ac>0,\ c>0 \\ 0, & b^2-4ac<0, \end{cases} \end{aligned} \tag{9}$$

where $x = \frac{-b+\sqrt{b^2-4ac}}{2a}$, $a = \frac{1}{\dot{\sigma}_0^2} - \frac{1}{\dot{\sigma}_1^2}$, $b = 2(\frac{\dot{\mu}_1}{\dot{\sigma}_1^2} - \frac{\dot{\mu}_0}{\dot{\sigma}_0^2})$, and $c = \frac{\dot{\mu}_0^2}{\dot{\sigma}_0^2} - \frac{\dot{\mu}_1^2}{\dot{\sigma}_1^2} + 2\ln(\frac{P(\mathcal{H}_1)(1-Q_M^G)\dot{\sigma}_0}{P(\mathcal{H}_0)Q_F^G\dot{\sigma}_1})$.

Proof: See Appendix A.

Now, we compare the proposed reference with the existing defense references reviewed in Section III-A. Firstly, the proposed reference outperforms the two references GDaR and SFRaR for the following reasons: The detection performance of both GDaR and SFRaR are determined by the original global decision's, i.e., Q_F^G and Q_M^G. Hence, in contrast with these two references, we consider the case that $\lambda = 0$ for the proposed reference, where $P_f^{EX} = 1, P_d^{EX} = 1$. In this case, $Q_M^R = 0$, $Q_F^R = Q_F^G$. Whenever we give the decision threshold a small incremental, we will have $Q_F^R < Q_F^G$, $Q_M^R < Q_M^G$. Secondly, the proposed reference also outperforms the reference TRaR for the following considerations: The detection performance of the reference TRaR is determined by a trust (i.e., honest) node, denoted as P_f^H and P_m^H. In the proposed reference, due to the extended sensing time, we have $P_f^{EX} < P_f^H$, $P_m^{EX} < P_m^H$. Considering the fact that $Q_F^G < 1$, $Q_M^G < 1$, we have $Q_F^R < P_f^H$, $Q_M^R < P_m^H$.

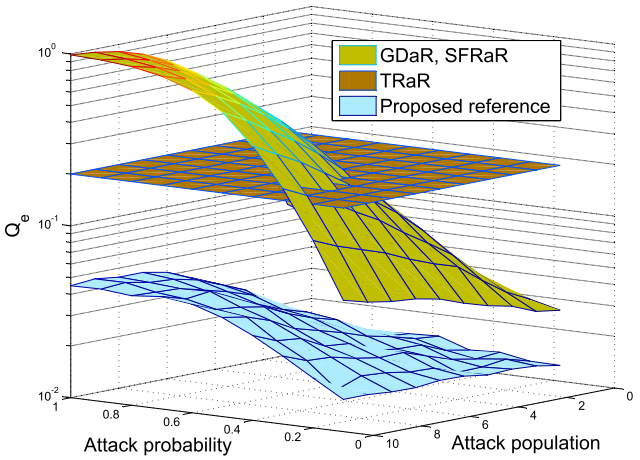


FIGURE 4. References' comparison on the error probability Q_e under different attack populations and attack probabilities where $N_u = 10$.

To present an illustrative comparison, Fig. 4 shows the detection performance of the proposed reference with that of the three existing references under varying attack population N_m and attack probability p_a. In the simulation, the global decisions are made using the majority rule, which represents the performance of the references GDaR and SFRaR. The detection performance of an honest sensor is chosen as the reference TRaR. As shown in Fig. 4, the detection performance of the references GDaR and SFRaR deteriorate dramatically as the attack population and/or attack probability increase, while the reference TRaR is robust to the varying attack behaviors, it is lack of flexibility and unfavorable even in cases that the attack behaviors are rare. Remarkably, the proposed reference's performance changes slightly with the attack population and attack probability, showing high robustness and reliability to attacks.

B. THE CAPABILITY OF DISTINGUISHING BYZANTINE ATTACKERS FROM HONEST SENSORS

Generally, the process of distinguishing malicious sensors from honest ones is as follows: Through comparing the sensors' reports with the reference, reputation of each sensor are generated and updated over time slots; after several time slots, sensors with low reputation are identified as malicious sensors (see [14], [20], [22] and literature therein).

As a general denotation, let Ω denote a reference with a false-alarm probability φ_f and a miss-detection probability φ_m. Let $x \in \{H, B\}$ denote the attribute of the sensors with H corresponding to an honest sensor and B corresponding to a Byzantine attacker, respectively. Let u^x denote the reports of a sensor with the attribute x whose detection performance is formulated as (P_m^x, P_f^x). When the number of sensors are large enough, the reports of one sensor and the final decision can be approximately independent. Thus, the probability of $u^x \neq \Omega$ is formulated as

$$\begin{aligned}\psi^x &= P(u^x \neq \Omega)\\ &= P(\mathcal{H}_1)P(u^x \neq \Omega|\mathcal{H}_1) + P(\mathcal{H}_0)P(u^x \neq \Omega|\mathcal{H}_0)\\ &\approx P(\mathcal{H}_1)[P_m^x(1-\varphi_m) + (1-P_m^x)\varphi_m]\\ &\quad + P(\mathcal{H}_0)[P_f^x(1-\varphi_f) + (1-P_f^x)\varphi_f]\\ &= P(\mathcal{H}_1)[P_m^x + (1-2P_m^x)\varphi_m]\\ &\quad + P(\mathcal{H}_0)[P_f^x + (1-2P_f^x)\varphi_f]. \end{aligned} \tag{10}$$

As shown in (10), ψ^x reflects the sensor's real performance, i.e., its attribute x. Based on this point, a manner of reputation generation below is widely adopted in the literature, e.g., the reference GDaR in [14] and the reference TRaR in [23]. Specifically, a sensor's reputation value Φ^x at the t-th slot is updated as [14]

$$\Phi^x(t) = \Phi^x(t-1) + \kappa, \tag{11}$$

where $\kappa = 0$ for the case $u^x(t) \neq \Omega(t)$ and $\kappa = 1$ for the case $u^x(t) = \Omega(t)$.

The reputation values follow the binomial distribution. Moreover, for the case that the number of time slots N_t is large enough, the Binomial distribution can be replaced by employing a Gaussian approximation as follows [14],

$$\Phi^H \sim \mathcal{N}(\mu_B, \sigma_B^2), \tag{12}$$

$$\Phi^B \sim \mathcal{N}(\mu_H, \sigma_H^2), \tag{13}$$

where $\mu_B = N_t\psi^B$, $\sigma_B^2 = N_t\psi^B(1-\psi^B)$, $\mu_H = N_t\psi^H$, and $\sigma_H^2 = N_t\psi^H(1-\psi^H)$.

Based on the reputation value, the sensor's attribute is determined as

$$\Phi^x \underset{x=H}{\overset{x=B}{\gtrless}} \theta, \tag{14}$$

where θ is the decision threshold. Then, two metrics are used to evaluate the identification performance. One is the false-negative probability P_{fn} that is the probability that an honest sensor is falsely identified as a malicious one. The other is the false-positive probability P_{fp} that is the probability that a malicious sensor is identified as an honest one, which are respectively formulated as,

$$P_{fn} \triangleq P(\Phi^H \geqslant \theta) = \int_{\theta}^{+\infty} f(\frac{x-\mu_H}{\sigma_H^2})dx, \tag{15}$$

$$P_{fp} \triangleq P(\Phi^B < \theta) = \int_{-\infty}^{\theta} f(\frac{x-\mu_B}{\sigma_B^2})dx. \tag{16}$$

Let π^H and π^B respectively denote the percentages of honest sensors and Byzantine attackers, we have $\pi^H + \pi^B = 1$ and, the probability of mistakenly identifying sensors' attributes P_{error} can be formulated as

$$P_{\text{error}} = \pi^B P_{fp}(\theta) + \pi^H P_{fn}(\theta). \tag{17}$$

Based on the analysis above, we find an interesting relation between a reference's sensing performance and the capability of identifying sensors' attributes, which can be formally characterized as the following Theorem.

Theorem 2: For any defense reference relying on formula (14) to identify honest sensors and malicious ones, we have

$$P_{\text{error}}(\varphi_m + \Delta_m, \varphi_f + \Delta_f) - P_{\text{error}}(\varphi_m, \varphi_f) \geq 0, \quad \forall \Delta_m, \Delta_f \geq 0. \tag{18}$$

Proof: See Appendix B.

It is observed in Theorem 18 that when the spectrum sensing performance of a reference becomes better, its capability of identifying sensors' attributes is enhanced. Based on this observation and the analysis in Section IV-A, we can also obtain the following corollary.

Corollary 1: The proposed reference is more reliable than the two references, GDaR and TRaR, in terms of distinguishing malicious sensors from honest sensors.

Notably, due to soft results of the reference SFRaR, it adapts another method to generate reputation values. Specifically, SFRaR uses the distance between sensors' reports and fused results to update reputation values [21]. It can be formulated as $\Phi_s(t) = \Phi_s(t-1) + \kappa_s$, where $\kappa_s = \frac{1}{2}|(-1)^{u_j(t)+1} - \frac{1}{N}\sum_{i=1}^{N}(-1)^{u_i(t)+1}|$, $u_i(t) \in \{0, 1\}$.

As shown in (17), there is a tradeoff between protection of honest sensors and identification of malicious sensors in choosing the threshold θ. Therefore, the problem of identifying malicious sensors can be regarded as a hypothesis test problem, as shown in Fig. 5. Here, the period is set as 10 slots to test the speed of identifying malicious sensors. Fig. 5 shows the probability distribution function (pdf) of sensors' reputation values of various defense references. Intuitively, from the perspective of hypothesis test, the smaller the overlapping region of the two PDFs is, the better the performance of identifying malicious sensors is. By comparing the four subfigures, it is observed that the proposed reference has the smallest overlapping region and thus the best performance in distinguishing Byzantine attackers from honest sensors.

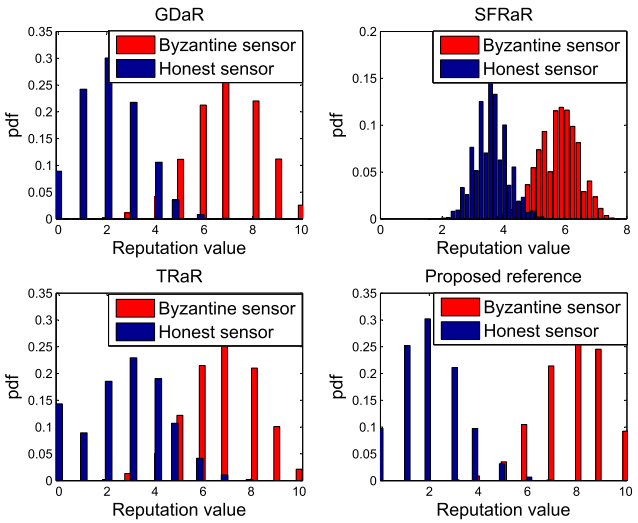


FIGURE 5. An illustration of a hypothesis test problem in identifying malicious sensors, where $N_u = 10$, $N_m = 2$, $p_a = 1$.

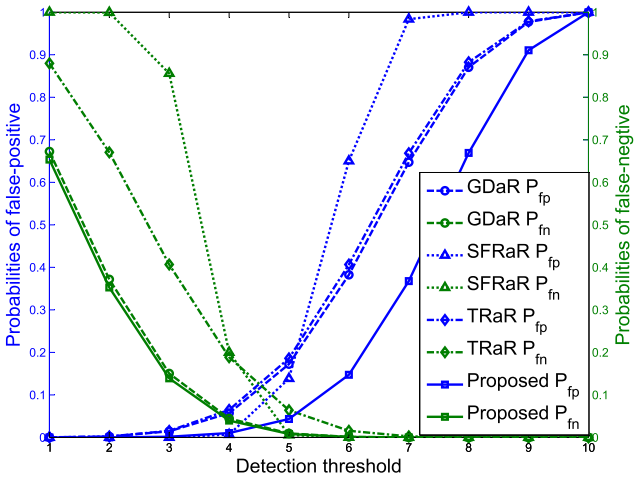


FIGURE 6. Performance comparison on identifying sensors' attributes, where $N_u = 10$, $N_m = 2$, $p_a = 1$.

Furthermore, Fig. 6 compares the false-negative probabilities and false-positive probabilities of various references under different identify threshold θ. The left (right) y-axis shows the false-negative (false-positive) probabilities. It can also be observed that under a given threshold, the proposed reference has the smallest false-negative probabilities and false-positive probabilities, indicating that it has the best performance in distinguishing Byzantine attackers from honest sensors, which is consistent with the theoretical analysis results above.

V. OPTIMAL COOPERATIVE SPECTRUM SENSING WITH THE PROPOSED REFERENCE

In the previous section, we have proposed a reliable defense reference. In this section, we will use the proposed reference to perform Byzantine defense and design an optimal cooperative spectrum sensing scheme.

Generally, the aim of cooperative spectrum sensing (CSS) is to improve the accuracy of spectrum sensing, which is closely related to the way of tackling with malicious sensors' reports. When malicious sensors are identified, their reports are generally filtered out [14], [31] or assigned with lower weights [13], [21], [23] in the process of global fusion. The former one has to endure the risks of mistaking an honest (malicious) sensor as a malicious (honest) one and may suffer from the diversity loss [5]. The latter one generally implies better CSS when the weights for all sensors are properly designed.

Traditionally, majority of the existing methods consider that the reports from malicious users are with negative impacts on CSS. Actually, *even fake reports reflect the real state of the target channel to some extent*, as the Byzantine attackers always falsified results based on the real sensing results to ensure attack accuracy. Motivated by this observation, in the following, we firstly introduce the Kullback-Leibler divergence (KLD) to measure the value of Byzantine attackers for CSS, which will help to illustrate the necessity and design rationale of making the optimal fusion. Then, based on the evaluation results, an optimal data fusion rule is developed to appropriately exploit the value of both honest sensors and Byzantine attackers. Considering the need of related parameters both in the KLD evaluation and the optimal fusion, we estimate the prior probability of the channel occupied and performance parameters of sensors relying on the proposed reference.

A. MOTIVATION

Here we use the relative entropy, called as the Kullback-Leibler divergence (KLD), to measure the distance of the two distributions of a sensor's reports under the two hypothesis [14]. Intuitively, as the distance increases, the reports show more definite inclination, which directly reflects the information value for hypothesis testing. Here the KLD is formulated as:

$$D\big(P(u_i|\mathcal{H}_1) \parallel P(u_i|\mathcal{H}_0)\big) = \sum_{u_i\in\{0,1\}} P(u_i|\mathcal{H}_1)\log\frac{P(u_i|\mathcal{H}_1)}{P(u_i|\mathcal{H}_0)}, \tag{19}$$

where $D\big(P(u_i|\mathcal{H}_1) \parallel P(u_i|\mathcal{H}_0)\big) \geq 0$, and the equation holds if and only if $P(u_i|\mathcal{H}_1) = P(u_i|\mathcal{H}_0)$. For the Byzantine attackers, the two distributions $P(u_i|\mathcal{H}_0)$ and $P(u_i|\mathcal{H}_1)$ are closely related to the attack probability p_a, which can be formulated as follows:

$$P(u_i = c|\mathcal{H}_j) = P(d_i = c|\mathcal{H}_j)\cdot(1-p_a) + P(d_i \neq c|\mathcal{H}_j)\cdot p_a, \quad j\in\{0,1\}, c\in\{0,1\}. \tag{20}$$

To illustrate the relation between the relative entropy and the attack probability, we give Theorem 3 below.

Theorem 3: The KLD $F \triangleq D\big(P(u_i|\mathcal{H}_1) \parallel P(u_i|\mathcal{H}_0)\big)$ is *convex* with respect to the attack probability p_a.

Proof: See Appendix C.

Remark: If and only if $p_a = 0.5$, $P(u_i|\mathcal{H}_1) = P(u_i|\mathcal{H}_0) = 0.5$ so that $D(P(u_i|\mathcal{H}_1) \parallel P(u_i|\mathcal{H}_0))$ obtain the minimum, i.e., zero. Based on Theorem 3, if $p_a \in (0, 0.5)$, the KLD decreases with p_a; else if $p_a \in (0.5, 1)$, the KLD increases with p_a. In the reputation-based schemes [13], [21], [23], the former case is considered through assigning low weight values, but the former case is ignored. In particular, when the attack probability is 1, $D\big(P(u_i|\mathcal{H}_1) \parallel P(u_i|\mathcal{H}_0)\big)$ remain unchanged. At this time, if the reports are reversed, then the Byzantine attacker will act as an honest sensor for spectrum sensing. It means that *the reports from the Byzantine attackers can help the fusion center to make spectrum sensing through appropriate adjustment*.

B. OPTIMAL COOPERATIVE SPECTRUM SENSING

The optimal data fusion scheme can be developed, according to the classical results by Varshney in [27], as follows:

$$\mathcal{F} = \begin{cases} 1, & \text{if } b_0 + \sum_{i=1}^{N_u} b_i(2u_i - 1)/2 > \eta_f \\ 0, & \text{otherwise,} \end{cases} \tag{21}$$

with

$$b_0 = \log \frac{P(\mathcal{H}_1)}{P(\mathcal{H}_0)},$$
$$b_i = \begin{cases} \log \dfrac{1 - P_m^x}{P_f^x}, & u_i = 1 \\ \log \dfrac{1 - P_f^x}{P_m^x}, & u_i = 0, \end{cases} \tag{22}$$

where P_f^x and P_m^x are the false alarm probability and the missed detection probability of a sensor's reports, which are estimated by comparing the sensor's reports and the proposed reference (see Section V-D for details). Notably, the developed fusion rule in formula (21) exploits the sensing reports of all sensors, including both honest sensors and malicious sensors, however, assigns different weights via $\{b_i, i = 1, ..., N_u\}$ to sensors.

However, in practice the parameters $P(\mathcal{H}_0)$, $P(\mathcal{H}_1)$, P_f^x, and P_m^x are unknown by the SU. Nevertheless, considering high reliability of the proposed reference, the parameters can be accurately estimated through the following Section V-C and Section V-D.

C. ESTIMATION OF THE PROBABILITY OF THE CHANNEL BEING OCCUPIED

For consecutive N_t time slots, the idleness and occupance probabilities of a given frequency band can be obtained approximately as follows:

$$\begin{cases} \hat{P}(\mathcal{H}_0) \triangleq [N(\mathcal{H}_0|\mathcal{F} = 1) + N(\mathcal{H}_0|\mathcal{F} = 0)]/N_t, \\ \hat{P}(\mathcal{H}_1) \triangleq [N(\mathcal{H}_1|\mathcal{F} = 1) + N(\mathcal{H}_1|\mathcal{F} = 0)]/N_t, \end{cases} \tag{23}$$

where $N(X)$ denotes the number of slots that the event X happens. Specifically, $N(\mathcal{H}_i|\mathcal{F} = j)$ is the number of slots that the channel is $\mathcal{H}_i$ when it is globally decided as j. Based on the proposed reference, $N(\mathcal{H}_0|\mathcal{F} = 0)$ and $N(\mathcal{H}_1|\mathcal{F} = 0)$ can be directly obtained by counting the number of access success and access failure/collusion, respectively. For the rest of the unknown parameters, we have

$$N(\mathcal{A} = 0|\mathcal{F} = 1) = N(\mathcal{H}_0|\mathcal{F} = 1) \cdot (1 - P_f^{EX}) + N(\mathcal{H}_1|\mathcal{F} = 1) \cdot (1 - P_d^{EX}), \tag{24}$$
$$N(\mathcal{A} = 1|\mathcal{F} = 1) = N(\mathcal{H}_0|\mathcal{F} = 1) \cdot P_f^{EX} + N(\mathcal{H}_1|\mathcal{F} = 1) \cdot P_d^{EX}. \tag{25}$$

Then, we have

$$N(\mathcal{H}_0|\mathcal{F} = 1) = \frac{N(\mathcal{A} = 0|\mathcal{F} = 1) \cdot P_d^{EX} - N(\mathcal{A} = 1|\mathcal{F} = 1) \cdot (1 - P_d^{EX})}{P_d^{EX} - P_f^{EX}}, \tag{26}$$

$$N(\mathcal{H}_1|\mathcal{F} = 1) = \frac{N(\mathcal{A} = 1|\mathcal{F} = 1) \cdot (1 - P_f^{EX}) - N(\mathcal{A} = 0|\mathcal{F} = 1) \cdot P_f^{EX}}{P_d^{EX} - P_f^{EX}}. \tag{27}$$

Theorem 4: As the accuracy of the extended sensing increases, the estimation accuracy of the prior probabilities of the channel state increases, that is,

$$\frac{\partial \hat{P}(\mathcal{H}_i)}{\partial P_d^{EX}} < 0, \tag{28}$$
$$\frac{\partial \hat{P}(\mathcal{H}_i)}{\partial P_f^{EX}} > 0. \tag{29}$$

Proof: See Appendix D.

Theorem 4 implies that the extended spectrum sensing in the proposed reference can improve the accuracy of parameter estimation, which further in turn improves the performance of the developed defense scheme in (21).

D. ESTIMATION OF SENSORS' REAL SENSING PERFORMANCE

The objective of this subsection is to estimate the real sensing performance of all sensors relying on their sensing reports, i.e., $\hat{P}_f^x$ and $\hat{P}_d^x$, $x \in \{H, B\}$. Intuitively, we have

$$\hat{P}_f^x = \frac{N(u = 1|\mathcal{H}_0)}{N(\mathcal{H}_0)}, \tag{30}$$
$$\hat{P}_d^x = \frac{N(u = 1|\mathcal{H}_1)}{N(\mathcal{H}_1)}, \tag{31}$$

where $N(\mathcal{H}_0)$ and $N(\mathcal{H}_1)$ can be obtained by multiplying N_t and the estimated $\hat{P}(\mathcal{H}_0)$ and $\hat{P}(\mathcal{H}_1)$ in section V-C, respectively. For $N(u = 1|\mathcal{H}_0)$ and $N(u = 1|\mathcal{H}_1)$, taking the former one as an example, we have

$$N(u=1|\mathcal{H}_0)=N(u=1|\mathcal{H}_0, \mathcal{F} = 0)+N(u = 1|\mathcal{H}_0, \mathcal{F}=1), \tag{32}$$

where the first part in the right of the equation can be directly obtained from the feedback of the transmitting results, however, it is hard to obtain an unbiased estimation of the second part. The reason is as follows: Due to the weights in the data

fusion varying with time slots, the dependence between local results u and global decisions $\mathcal{F}$ is dynamically changing, which makes it hard to estimate the second part in a probabilistic manner.

To address this issue, we propose another method to estimate the parameters by exploiting the characteristics of the proposed reference. The key rationale is as follows: It is observed that when the PU is globally declared as absent, we can obtain the real state of the licensed channel through the spectrum access results. Here, though the sensing over the whole slot is not done at this time, we can consider it is virtually done and obtain corresponding sensing results based on the real states and its performance parameters. Consequently, we can avoid tackling with the relation between local results u and global decisions $\mathcal{F}$ and design a simple but unbiased scheme of estimating parameters. Specifically, the estimation problem can be solved through the maximum likelihood estimation, which is formulated as follows:

$$\max\ L(\hat{P}_f^x, \hat{P}_d^x) = \max \prod_{j=1}^{N_t} p(y_i(j); \hat{P}_f^x, \hat{P}_d^x), \tag{33}$$

where $y_i(j) = (u(j), \mathcal{A}^{'}(j)) \in \{(0,0),(0,1),(1,0),(1,1)\}$. $\mathcal{A}^{'}(j)$ denotes the sensing result of the SU in the j-th slot, corresponding to the performance parameters, P_f^{EX} and P_d^{EX}, and $u(j)$ denotes the sensing report of the sensor in the j-th slot.

Further, we have

$$\begin{aligned}\ln L(\hat{P}_f^x, \hat{P}_d^x) = {} & a_{00} \cdot \ln P_{00} + a_{01} \cdot \ln P_{01} \\ & + a_{10} \cdot \ln P_{10} + a_{11} \cdot \ln P_{11},\end{aligned} \tag{34}$$

where a_{nm} denotes the frequency of $(u_i, \mathcal{A}^{'}) = (n, m)$, and P_{nm} denotes the corresponding probabilities, $n, m \in \{0, 1\}$. Here, P_{nm} is formulated as follows:

$$\begin{aligned}\begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} \triangleq {} & \begin{pmatrix} \hat{P}(\mathcal{H}_0)\cdot(1-\hat{P}_f^x) & \hat{P}(\mathcal{H}_1)\cdot(1-\hat{P}_d^x) \\ \hat{P}(\mathcal{H}_0)\cdot\hat{P}_f^x & \hat{P}(\mathcal{H}_1)\cdot\hat{P}_d^x \end{pmatrix} \\ & \times \begin{pmatrix} 1-P_f^{EX} & P_f^{EX} \\ 1-P_d^{EX} & P_d^{EX} \end{pmatrix}.\end{aligned} \tag{35}$$

Substitute Eq. (35) into Eq. (34), and take a derivative with respect to $\hat{P}_f^x$ and $\hat{P}_d^x$ respectively,

$$\begin{aligned}\frac{\partial \ln L}{\partial \hat{P}_f^x} = {} & a_{00}\frac{-\hat{P}(\mathcal{H}_0)\cdot(1-P_f^{EX})}{P_{00}} + a_{01}\frac{-\hat{P}(\mathcal{H}_0)\cdot P_f^{EX}}{P_{01}} \\ & + a_{10}\frac{\hat{P}(\mathcal{H}_0)\cdot(1-P_f^{EX})}{P_{10}} + a_{11}\frac{\hat{P}(\mathcal{H}_0)\cdot P_f^{EX}}{P_{11}} \\ = {} & 0,\end{aligned} \tag{38}$$

$$\begin{aligned}\frac{\partial \ln L}{\partial \hat{P}_d^x} = {} & a_{00}\frac{-\hat{P}(\mathcal{H}_1)\cdot(1-P_d^{EX})}{P_{00}} + a_{01}\frac{-\hat{P}(\mathcal{H}_1)\cdot P_d^{EX}}{P_{01}} \\ & + a_{10}\frac{\hat{P}(\mathcal{H}_1)\cdot(1-P_d^{EX})}{P_{10}} + a_{11}\frac{\hat{P}(\mathcal{H}_1)\cdot P_d^{EX}}{P_{11}} \\ = {} & 0.\end{aligned} \tag{39}$$

Then, we can obtain the following results:

$$\begin{cases} \dfrac{a_{00}}{P_{00}} = \dfrac{a_{10}}{P_{10}} \\ \dfrac{a_{01}}{P_{01}} = \dfrac{a_{11}}{P_{11}}. \end{cases} \tag{40}$$

Substitute Eq. (35) into Eq. (40), we can obtain the closed-form solutions of the sensor's detection probability and false-alarm probability as Eq. (36) and Eq. (37), as shown at the bottom of this page.

VI. PERFORMANCE EVALUATION AND DISCUSSIONS

In this section, the proposed method is compared with state-of-the-art methods in term of defense performance.

A. BASIC SIMULATION SETUP

Without further specifications, we consider that a SU is under severe shadowing with the local signal-to-noise ratio (SNR) as -10dB. The probability of the PU channel being busy is 0.2. Without loss of generality, honest sensors' local performances are set as $p_f^H = 0.2, p_d^H = 0.8$. The attack probability p_a of malicious sensors varies from 0 to 1. Considering the extended sensing time, the time-bandwidth product increases from 100 to 500 and the local decision threshold is set so that the false-alarm probability is 0.06. The results in the following figures are obtained by averaging 100000 time slots.

To show the effectiveness of the proposed method, we perform comparison among the follow seven schemes:

- A scheme named *no defense*, in which the SU fuses all reports normally without any preprocessing. In this case, the SU suffers all negative effects of attack behaviors, which is viewed as the lower-bound of various defense schemes.
- An ideal scheme with abandoning all malicious sensors, named *ideal abandoning*. All malicious sensors are correctly identified and discarded. Only honest sensors are left to participate in cooperative spectrum sensing. It is regarded as an upper-bound performance of methods filtering out malicious sensors.
- An ideal scheme with perfect knowledge of sensors' performance metrics and adapting the optimal fusion

$$\hat{P}_d^x = \frac{(\frac{a_{01}}{a_{11}}+1)P_f^{EX} - (\hat{P}(\mathcal{H}_0)P_f^{EX} + \hat{P}(\mathcal{H}_1)P_d^{EX})[\frac{a_{00}}{a_{10}} + 1 + (\frac{a_{01}}{a_{11}} - \frac{a_{00}}{a_{10}})P_f^{EX}]}{(\frac{a_{00}}{a_{10}}+1)(\frac{a_{01}}{a_{11}}+1)\hat{P}(\mathcal{H}_1)(P_f^{EX} - P_d^{EX})}, \tag{36}$$

$$\hat{P}_f^x = \frac{(\frac{a_{01}}{a_{11}}+1)P_d^{EX} - (\hat{P}(\mathcal{H}_0)P_f^{EX} + \hat{P}(\mathcal{H}_1)P_d^{EX})[\frac{a_{00}}{a_{10}} + 1 + (\frac{a_{01}}{a_{11}} - \frac{a_{00}}{a_{10}})P_d^{EX}]}{(\frac{a_{00}}{a_{10}}+1)(\frac{a_{01}}{a_{11}}+1)\hat{P}(\mathcal{H}_0)(P_d^{EX} - P_f^{EX})}. \tag{37}$$

method, named *optimal fusion*, which serves as the upper-bound performance of the proposed method.

- A scheme based on the reference GDaR, named *global filtering*, in which global decisions are regarded as the defense reference. Sensors identified as malicious are filtered and sensors left are allowed to participate into CSS [14].
- A scheme based on the reference SFRaR, named *soft fusion*, in which all reports are fused based on assigned reputation values [21].
- A scheme based on the reference TRaR, named *trusted-node assisting*, in which an honest sensor is prior known by the SU and sensors tested as honest are allowed to participate into CSS [23].
- The proposed method based on the proposed reference, named *proposed method*.

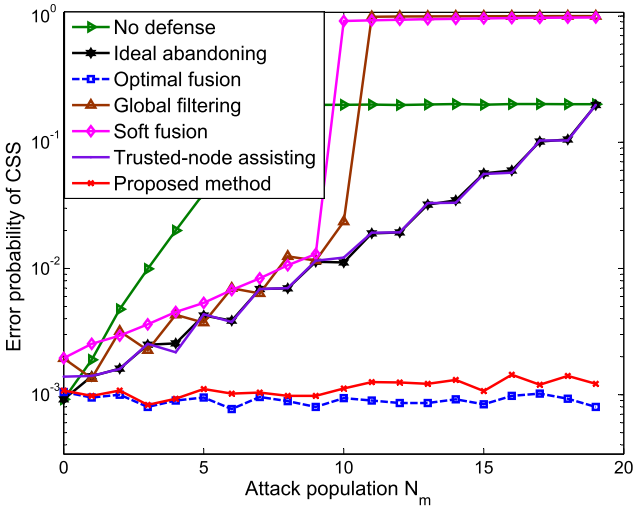


FIGURE 7. Defense performance with different attack populations.

B. PERFORMANCE EVALUATION

Fig. 7 compares the CSS performance of various defense schemes under different attack populations, where $N_u = 20$, $p_a = 1$. We observe that as the attack population N_m increases, the following schemes, *no defense, global filtering*, and *soft fusion* deteriorate dramatically and collapse when malicious sensors stand in majority, while the proposed method keeps favorable performance, which is consistent with Fig. 4. On one hand, the increasing attack population destroys the reliability of global fusion and decisions, which means that the references of the two schemes *no defense* and *global filtering* makes little sense in identifying sensors' attributes. On the other hand, as the attack population increases, more malicious sensors will be filtered out, which leads to a loss of spatial diversity. However, in the proposed scheme, the reference is nearly immune to the deterioration of global decisions (seen in Fig. 4) and can dig out useful information from malicious sensors' reports to avoid declined performance.

The relation between the defense performance and the attack probability is shown in Fig. 8, where $N_u = 10$, $N_m = 4$.

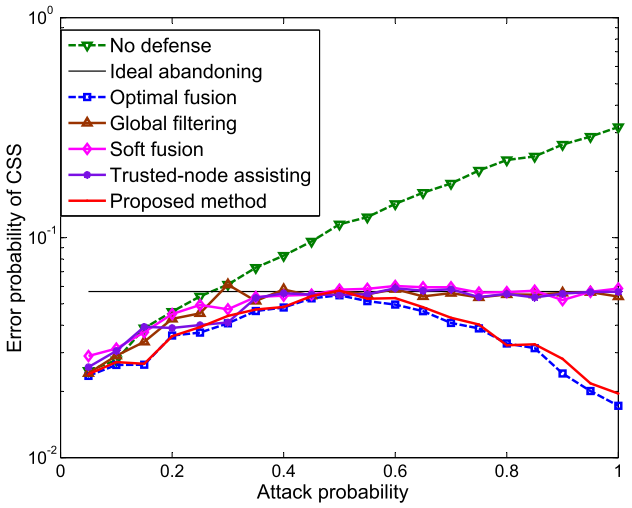


FIGURE 8. Defense performance with different attack probabilities.

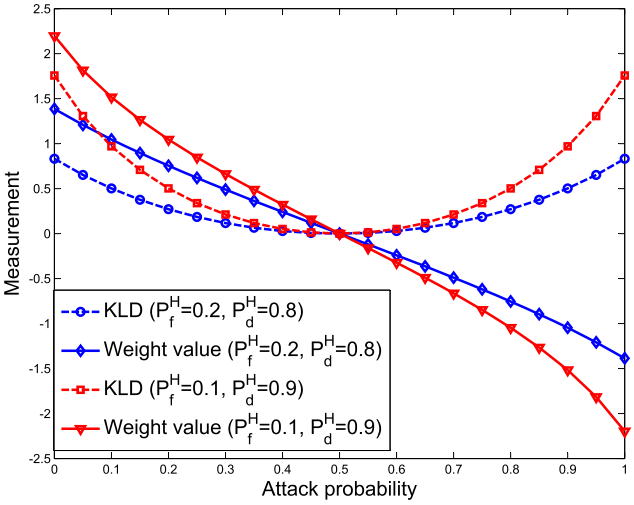


FIGURE 9. Kullback-Leibler divergence and weight values of malicious sensors vary with the attack probability.

As the attack probability increases, attack behaviors become more intense and consequently, malicious sensors are gradually identified and filtered out or assigned relatively low weights in the schemes *global filtering*, *trusted-node assisting*, and *soft fusion*. In particular, when the attack probability is large enough (see, e.g., around 0.5 in Fig. 8), almost all malicious sensors are not allowed to participate in data fusion and the performance of these schemes are almost the same as that of the scheme *ideal abandoning*. However, due to the decreased number of sensors participating in the data fusion, the performance of those schemes is limited. Differently, it is observed in Fig. 8 that for the *optimal fusion* scheme and the *proposed method*, the error probabilities firstly increases and then decreases with the attack probability, however, always better than other conventional schemes. The key insight is that the *optimal fusion* scheme and the *proposed method* can even dig out useful information from the reports of malicious sensors. More specifically, as shown in Fig. 9, the

Kullback-Leibler divergence (KLD) has relatively high value under low and high attack probabilities, which indicates high capability in identifying the channel's states; when the attack probability is 0.5, KLD obtains the minimum, corresponding to the lowest capability in identifying the channel's states. Moreover, as shown in Fig. 9, the weights for a malicious sensor in the *optimal fusion* scheme and the *proposed method* are appropriately assigned with the attack probability, enabling reports from both honest sensors and malicious sensors are properly exploited.

VII. CONCLUSIONS

This paper studied the issue of robust cooperative spectrum sensing against Byzantine attack. The first contribution was to propose a novel and reliable Byzantine defense reference for robust cooperative spectrum sensing against Byzantine attack. The proposed defense reference jointly exploited the cognitive process of spectrum sensing and spectrum access in a closed-loop manner, to provide the defense scheme a solid basis. The second contribution was to analyze and prove the proposed reference's favorable reliability and high robustness over the state-of-the-art references. The third contribution is to design an optimal cooperative spectrum sensing scheme with the proposed defense reference. Numerical simulations verify the proposed scheme's favorable performance, even in critical cases that malicious sensors are in majority.

APPENDIX A
PROOF OF THEOREM 1

For Eq. (8), taking a derivative with respect to λ, we have

$$\frac{\partial Q_e}{\partial \lambda} = P(\mathcal{H}_0)Q_F^G \frac{\partial P_f^{EX}}{\partial \lambda} + P(\mathcal{H}_1)(1-Q_M^G)\frac{\partial P_m^{EX}}{\partial \lambda}. \tag{41}$$

Let Eq. (41) be zero, we have

$$2\ln[\frac{P(\mathcal{H}_1)(1-Q_M^G)\dot{\sigma}_0}{P(\mathcal{H}_0)Q_F^G\dot{\sigma}_1}] = \frac{1}{\dot{\sigma}_1^2}(\lambda-\dot{\mu}_1)^2 - \frac{1}{\dot{\sigma}_0^2}(\lambda-\dot{\mu}_0)^2 \tag{42}$$

Here,

$$\begin{aligned}\hbar(\lambda) &= \frac{1}{\dot{\sigma}_0^2}(\lambda-\dot{\mu}_0)^2 - \frac{1}{\dot{\sigma}_1^2}(\lambda-\dot{\mu}_1)^2 + 2\ln[\frac{P(\mathcal{H}_1)(1-Q_M^G)\dot{\sigma}_0}{P(\mathcal{H}_0)Q_F^G\dot{\sigma}_1}] \\ &= (\frac{1}{\dot{\sigma}_0^2}-\frac{1}{\dot{\sigma}_1^2})\lambda^2 + 2(\frac{\dot{\mu}_1}{\dot{\sigma}_1^2}-\frac{\dot{\mu}_0}{\dot{\sigma}_0^2})\lambda + \frac{\dot{\mu}_0^2}{\dot{\sigma}_0^2}-\frac{\dot{\mu}_1^2}{\dot{\sigma}_1^2} \\ &\quad + 2\ln(\frac{P(\mathcal{H}_1)(1-Q_M^G)\dot{\sigma}_0}{P(\mathcal{H}_0)Q_F^G\dot{\sigma}_1}) \\ &\triangleq a\lambda^2 + b\lambda + c,\end{aligned} \tag{43}$$

where $a = \frac{1}{\dot{\sigma}_0^2}-\frac{1}{\dot{\sigma}_1^2}$, $b = 2(\frac{\dot{\mu}_1}{\dot{\sigma}_1^2}-\frac{\dot{\mu}_0}{\dot{\sigma}_0^2})$, and $c = \frac{\dot{\mu}_0^2}{\dot{\sigma}_0^2}-\frac{\dot{\mu}_1^2}{\dot{\sigma}_1^2} + 2\ln(\frac{P(\mathcal{H}_1)(1-Q_M^G)\dot{\sigma}_0}{P(\mathcal{H}_0)Q_F^G\dot{\sigma}_1})$.

$\because \dot{\sigma}_1 > \dot{\sigma}_0, \therefore a > 0.$

Simultaneously,

$\because \frac{\dot{\mu}_1}{\dot{\sigma}_1^2} = \frac{\gamma+1}{2(2\gamma+1)}, \frac{\dot{\mu}_0}{\dot{\sigma}_0^2} = 1/2, \therefore b < 0.$

Case 1: $c \leqslant 0$, then we have $b^2 - 4ac > 0$, and the larger solution is the optimal value λ_p.

Case 2: $c > 0$, then if $b^2 - 4ac \geqslant 0$, λ_p is one of zero and the larger solution to $\hbar(\lambda)$, which makes $Q_e(\lambda)$ obtain a smaller value; if $b^2 - 4ac < 0$, then $\lambda_p = 0$.

APPENDIX B
PROOF OF THEOREM 2

For an honest sensor, generally we have $P_f^H < 0.5$, $P_m^H < 0.5$.

Therefore, $\frac{\partial \psi^H}{\partial \varphi_f} > 0$, $\frac{\partial \psi^H}{\partial \varphi_m} > 0$

For a Byzantine sensor, there are two cases as follows.

Case 1: The attack probability $p_a < 0.5$. Here, $P_f^H < P_f^B < 0.5$, $P_m^H < P_m^B < 0.5$.

$\therefore \psi^H < \psi^B < 0.5$, $\frac{\partial \psi^H}{\partial \varphi_f} > \frac{\partial \psi^B}{\partial \varphi_f} > 0$, $\frac{\partial \psi^H}{\partial \varphi_m} > \frac{\partial \psi^B}{\partial \varphi_m} > 0$.

Case 2: The attack probability $p_a \geq 0.5$. Here, $P_f^H < 0.5 \leq P_f^B$, $P_m^H < 0.5 \leq P_m^B$.

$\therefore \psi^H < 0.5 \leq \psi^B$, $\frac{\partial \psi^H}{\partial \varphi_f} > 0 > \frac{\partial \psi^B}{\partial \varphi_f}$, $\frac{\partial \psi^H}{\partial \varphi_m} > 0 > \frac{\partial \psi^B}{\partial \varphi_m}$.

Let φ_f be $(\varphi_f + \Delta)$, where $\Delta < 0$. Then the mean value and variance value of Φ^H become $(\mu_H + \Delta_1^H)$ and $(\sigma_H^2 + \Delta_2^H)$, and these metrics of Φ^B become $(\mu_B + \Delta_1^B)$ and $(\sigma_B^2 + \Delta_2^B)$. Based on the analysis results, it can be simply proved that in both two cases, $\Delta_1^H < \Delta_1^B$, $\Delta_2^B < 0$, and $\Delta_1^B < 0$.

Therefore, the probability of mistakenly identifying sensors' attributes is formulated as

$$\begin{aligned}&P_{\text{error}}(\varphi_f, \varphi_m) \\ &= \int_{-\infty}^{\theta} \pi^B f(\frac{x-\mu_B}{\sigma_B^2})dx + \int_{\theta}^{+\infty} \pi^H f(\frac{x-\mu_H}{\sigma_H^2})dx \\ &= \int_{-\infty}^{\theta+\Delta_1^B} \pi^B f(\frac{t-(\mu_B+\Delta_1^B)}{\sigma_B^2})dt \\ &\quad + \int_{\theta+\Delta_1^H}^{+\infty} \pi^H f(\frac{y-(\mu_H+\Delta_1^H)}{\sigma_H^2})dy \\ &\overset{\Delta<0}{>} \int_{-\infty}^{\theta+\Delta_1^B} \pi^B f(\frac{t-(\mu_B+\Delta_1^B)}{\sigma_B^2+\Delta_2^B})dt \\ &\quad + \int_{\theta+\Delta_1^H}^{+\infty} \pi^H f(\frac{y-(\mu_H+\Delta_1^H)}{\sigma_H^2+\Delta_2^H})dy \\ &> \int_{-\infty}^{\theta+\Delta_1^H} \pi^B f(\frac{t-(\mu_B+\Delta_1^B)}{\sigma_B^2+\Delta_2^B})dt \\ &\quad + \int_{\theta+\Delta_1^H}^{+\infty} \pi^H f(\frac{y-(\mu_H+\Delta_1^H)}{\sigma_H^2+\Delta_2^H})dy \\ &= P_{\text{error}}(\varphi_f+\Delta, \varphi_m).\end{aligned} \tag{44}$$

Similarly, we can obtain $P_{\text{error}}(\varphi_f, \varphi_m) > P_{\text{error}}(\varphi_f, \varphi_m + \Delta)$, where $\Delta < 0$. Therefore, when the sensing performance of the reference becomes better, i.e., $\Delta < 0$, the performance of identifying sensors' attributes, malicious or honest, is improved.

$$E(N(\mathcal{H}_0)) = N(\mathcal{H}_0|\mathcal{F}=0) + N(\mathcal{F}=1)\cdot P_0, \tag{49}$$

$$\begin{aligned} D(N(\mathcal{H}_0)) &= D[N(\mathcal{H}_0|\mathcal{F}=0) \\ &\quad + \frac{N(\mathcal{A}=0|\mathcal{F}=1)\cdot P_d^{EX} - N(\mathcal{A}=1|\mathcal{F}=1)\cdot(1-P_d^{EX})}{P_d^{EX}-P_f^{EX}}] \\ &= \frac{D(N(\mathcal{A}=0|\mathcal{F}=1))}{(P_d^{EX}-P_f^{EX})^2} \\ &= N(\mathcal{F}=1) \\ &\quad \cdot \frac{P_d^{EX} - {P_d^{EX}}^2 + (P_d^{EX}-P_f^{EX})(2P_d^{EX}-P_{a0}) - (P_d^{EX}-P_f^{EX})^2 {P_{a0}}^2}{(P_d^{EX}-P_f^{EX})^2}. \end{aligned} \tag{50}$$

APPENDIX C
PROOF OF THEOREM 3

Denote $P(u_i|\mathcal{H}_j)$ as α_{ij}. As shown in (5), α_{ij} is linear with the attack probability p_a and then we have $\alpha_{ij}(\lambda p_a^{'} + (1-\lambda)p_a^{''}) = \lambda\alpha_{ij}(p_a^{'}) + (1-\lambda)\alpha_{ij}(p_a^{''})$. Based on the log-sum inequality, we have

$$\begin{aligned} &\alpha_{i1}(\lambda p_a^{'} + (1-\lambda)p_a^{''}) \log \frac{\alpha_{i1}(\lambda p_a^{'} + (1-\lambda)p_a^{''})}{\alpha_{i0}(\lambda p_a^{'} + (1-\lambda)p_a^{''})} \\ &= (\lambda\alpha_{i1}(p_a^{'}) + (1-\lambda)\alpha_{i1}(p_a^{''})) \log \frac{\lambda\alpha_{i1}(p_a^{'}) + (1-\lambda)\alpha_{i1}(p_a^{''})}{\lambda\alpha_{i0}(p_a^{'}) + (1-\lambda)\alpha_{i0}(p_a^{''})} \\ &\le \lambda\alpha_{i1}(p_a^{'}) \log \frac{\lambda\alpha_{i1}(p_a^{'})}{\lambda\alpha_{i0}(p_a^{'})} + (1-\lambda)\alpha_{i1}(p_a^{''}) \log \frac{\lambda\alpha_{i1}(p_a^{''})}{\lambda\alpha_{i0}(p_a^{''})}. \end{aligned} \tag{45}$$

Sum over all i, we have

$$\begin{aligned} &D(\alpha_{i1}(\lambda p_a^{'} + (1-\lambda)p_a^{''}) \parallel \alpha_{i0}(\lambda p_a^{'} + (1-\lambda)p_a^{''})) \\ &\quad \le \lambda D(\alpha_{i1}(p_a^{'}) \parallel \alpha_{i0}(p_a^{'})) + (1-\lambda) D(\alpha_{i1}(p_a^{''} \parallel \alpha_{i0}(p_a^{''})). \end{aligned} \tag{46}$$

Hence, $D(P(u_j|\mathcal{H}_1) \parallel P(u_j|\mathcal{H}_0))$ is convex with the attack probability.

APPENDIX D
PROOF OF THEOREM 4

Apparently, the estimation is un-biased and the smaller its variance is, the more accurate the estimation is. We assume that during the past N_t slots, P_0 and P_1 denote the frequencies of the channel' absence and presence when the channel is globally declared as occupied respectively. Then,

$$P(\mathcal{A}=0|\mathcal{F}=1) = P_0\cdot(1-P_f^{EX}) + P_1\cdot P_d^{EX}, \tag{47}$$

which is denoted as P_{a0}.

Then, the corresponding expected value and variance are

$$\begin{cases} E\,(N\,(\mathcal{A}=0|\mathcal{F}=1)) = N(\mathcal{F}=1)\cdot P_{a0} \\ D(N(\mathcal{A}=0|\mathcal{F}=1)) = N(\mathcal{F}=1)\cdot P_{a0}\cdot(1-P_{a0}). \end{cases} \tag{48}$$

In sequence, we have (49) and (50), as shown at the top of this page.

It can be easily obtained that

$$\frac{\partial D(N(\mathcal{H}_0))}{\partial P_d^{EX}} < 0, \quad \frac{\partial D(N(\mathcal{H}_0))}{\partial P_f^{EX}} > 0. \tag{51}$$

Then, we have

$$\frac{\partial \hat{P}(\mathcal{H}_i)}{\partial P_d^{EX}} < 0, \quad \frac{\partial \hat{P}(\mathcal{H}_i)}{\partial P_f^{EX}} > 0. \tag{52}$$

Hence, the more accurate the sensing performance is, the smaller the estimation's variance is and the more accurate the estimation is.

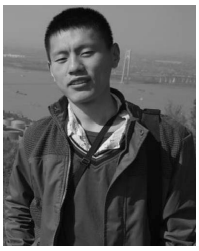
ACKNOWLEDGMENT

Part of this work has been accepted to be presented at the IEEE/CIC International Conference on Communications in China (ICCC) 2016, Chengdu, China.

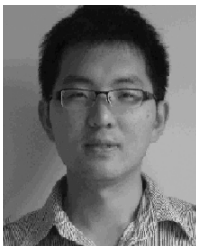
REFERENCES

[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] X. L. Huang, F. Hu, J. Wu, H. H. Chen, G. Wang, and T. Jiang, "Intelligent cooperative spectrum sensing via hierarchical Dirichlet process in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 5, pp. 771–787, May 2015.
[3] 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.
[4] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. PP, no. 99, pp. 1–39, May 2016, doi: 10.1109/JPROC.2016.2558521.
[5] G. Ding *et al.*, "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014.
[6] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: Current state and future challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 32–39, Nov. 2011.
[7] A. Vempaty, L. Tong, and P. K. Varshney, "Distributed inference with Byzantine data: State-of-the-art review on data falsification attacks," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 65–75, Sep. 2013.
[8] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342–1363, 3rd Quart., 2015.
[9] 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.
[10] Z. Qin, Q. Li, and G. Hsieh, "Defending against cooperative attacks in cooperative spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2680–2687, Jun. 2013.

[11] L. Zhang, Q. Wu, G. Ding, S. Feng, and J. Wang, "Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing," *EURASIP J. Adv. Signal Process.*, vol. 2014, no. 1, pp. 1–9, May 2014.
[12] X. He, H. Dai, and P. Ning, "HMM-based malicious user detection for robust collaborative spectrum sensing," *IEEE J. Sel. Areas. Commun.*, vol. 31, no. 11, pp. 2196–2208, Nov. 2013.
[13] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 31–35.
[14] 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.
[15] 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.
[16] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Distributed detection in tree topologies with Byzantines," *IEEE Trans. Signal Process.*, vol. 62, no. 12, pp. 3208–3219, Jun. 2014.
[17] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Distributed Bayesian detection in the presence of Byzantine data," *IEEE Trans. Signal Process*, vol. 63, no. 19, pp. 5250–5263, Oct. 2015.
[18] B. Kailkhura, B. Dulek, S. Brahma, 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.
[19] M. Jo, L. Han, D. Kim, and H. P. In, "Selfish attacks and detection in cognitive radio ad-hoc networks," *IEEE Netw.*, vol. 27, no. 3, pp. 46–50, May/Jun. 2013.
[20] S. Althunibat, B. Denise, and F. Granelli, "Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–20, Nov. 2015.
[21] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in *Proc. ICC*, Dresden, Germany, Jun. 2009, pp. 1–5.
[22] 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.
[23] K. Zeng, P. Paweczak, and D. Čabrić, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 226–228, Mar. 2010.
[24] L. Zhang, G. Ding, F. Song, and Q. Su, "Defending against Byzantine attack in cooperative spectrum sensing relying on a reliable reference," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Chengdu, China, Jul. 2016, pp. 1–6.
[25] Q. Wu, G. Ding, J. Wang, and Y.-D. Yao, "Spatial-temporal opportunity detection for spectrum-heterogeneous cognitive radio networks: Two-dimensional sensing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 516–526, Feb. 2013.
[26] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.
[27] Z. Chair and P. K. Varshney, "Optimal data fusion in multiple sensor detection systems," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-22, no. 1, pp. 98–101, Jan. 1986.
[28] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Secure cooperative spectrum sensing and access against intelligent malicious behaviors," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 1267–1275.
[29] L. Duan, A. W. Min, J. Huang, and K. G. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," *IEEE J. Sel. Areas. Commun.*, vol. 30, no. 9, pp. 1658–1665, Oct. 2012.
[30] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.
[31] G. Ding, Q. Wu, Y.-D. Yao, J. Wang, and Y. Chen, "Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions," *IEEE Signal Process. Mag.*, vol. 30, no. 4, pp. 126–136, Jul. 2013.
[32] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5761–5766, Dec. 2009.
[33] Y. Zhao, M. Song, and C. Xin, "A weighted cooperative spectrum sensing framework for infrastructure-based cognitive radio networks," *Comput. Commun.*, vol. 2011, no. 34, pp. 1510–1517, Feb. 2011.



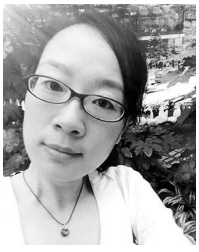
LINYUAN ZHANG received the B.S. degree (Hons.) in electronics engineering from Inner Mongolia University, Hohhot, China, in 2012, and the M.S. degree in communications and information system from the College of Communications Engineering, PLA University of Science and Technology, in 2015, where he is currently pursuing the Ph.D. degree. His research interests are wireless communications and cognitive radio networks.



GUORU DING (S'10–M'14–SM'16) received the B.S. degree in electrical engineering from Xidian University, Xi'an, China, in 2008, and the Ph.D. degree from the College of Communications Engineering, PLA University of Science and Technology (CCE, PLA UST), Nanjing, China, in 2014. Since 2014, he has been an Assistant Professor with CCE, PLA UST. Since 2015, he has been a Post-Doctoral Research Associate with the National Mobile Communications Research Laboratory, Southeast University, Nanjing. His current research interests include massive MIMO, cognitive radio networks, wireless security, and big spectrum data analytics for future wireless networks. He currently serves as a Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and an Associate Editor of *KSII Transactions on Internet and Information Systems*. He was a recipient of Best Paper Awards from the IEEE VTC2014-Fall and the IEEE WCSP 2009. He is a Voting Member of the IEEE 1900.6 Standard Association Working Group.

QIHUI WU received the B.S. degree in communications engineering, and the M.S. and Ph.D. degrees in communications and information systems from the Institute of Communications Engineering, Nanjing, China, in 1994, 1997, and 2000, respectively. From 2003 to 2005, he was a Post-Doctoral Research Associate with Southeast University, Nanjing. From 2005 to 2007, he was an Associate Professor with the College of Communications Engineering, PLA University of Science and Technology, Nanjing, where he served as a Full Professor from 2008 to 2016. Since 2016, he has been a Full Professor with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing. In 2011, he was an Advanced Visiting Scholar with the Stevens Institute of Technology, Hoboken, USA.

His current research interests span the areas of wireless communications and statistical signal processing, with emphasis on system design of software defined radio, cognitive radio, and smart radio.



FEI SONG received the B.S. degree in communications engineering and the Ph.D. degree in communications and information system from the Institute of Communications Engineering, PLA University of Science and Technology (PLA UST), Nanjing, China, in 2002 and 2007, respectively. She is currently an Associate Professor with the College of Communications Engineering, PLA UST. Her current research interests are cognitive radio networks, MIMO, and statistical signal processing.