IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 20, 2018, accepted August 16, 2018, date of publication August 23, 2018, date of current version October 17, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2866485

Generalized Byzantine Attack and Defense in Cooperative Spectrum Sensing for Cognitive Radio Networks

JUN WU[1], (Student Member, IEEE), TIECHENG SONG[2], (Member, IEEE), YUE YU[1], CONG WANG[1], (Student Member, IEEE), AND JING HU[2], (Member, IEEE)

[1]National Mobile Commutation Research Lab, Southeast University, Nanjing 210096, China
[2]School of Information Science and Engineering, Southeast University, Nanjing 211189, China

Corresponding author: Jun Wu (wojames2011@163.com)

This work was supported by the National Natural Science Foundation of China (No. 61771126).

ABSTRACT Cognitive radio (CR) is a revolutionary paradigm to solve the spectrum scarcity problem in wireless networks. In cognitive radio networks, cooperative spectrum sensing is regarded as a promising approach method to significantly improve the performance of spectrum sensing, but it can be threatened by Byzantine attack. The existing defense references have focused on how to mitigate the negative effect of Byzantine attack, but with some strong assumptions, such as the attackers are in minority and/or a trusted node exists for data fusion. This observation motivates us to comprehensively analyze the strategies of Byzantine attack and the fusion center (FC) in the absence of these restrictions. To be specific, we consider a generic Byzantine attack model by analyzing sophisticated malicious behaviors, which goes beyond the existing models for its generalization. Under this generalized attack model, we derive the condition which makes the FC blind from malicious perspective. On this basis, the optimal attack strategy to maximize Bayes risk is analyzed, respectively, in the case of the unknown and known fusion rule. Furthermore, we extend our analysis to the scenario where the FC has the knowledge of the attack strategy by an estimation algorithm and adopts the optimal fusion rule. Thus, we also give the closed form expression, in terms of the optimal attack strategy under different scenarios, sequentially. At last, the extensive numerical results are provided to verify our theoretical analyses and proposed estimation algorithm.

INDEX TERMS Cognitive radio networks, cooperative spectrum sensing, Byzantine attack, Bayes risk, attack strategy.

I. INTRODUCTION

With wireless devices and applications booming, the problem of inefficient utilization of the precious radio spectrum has arisen. Recent studies have shown that a considerable amount of licensed spectrum is rarely occupied. Cognitive radio (CR) is a key technology to improve spectrum utilization and solve the problem of spectrum shortage. There are three main CR systems: underlay, overlay, and interweave [1]. The interweave system based on the idea of opportunistic communication is the original motivation for CR and adopted in this paper. CR can be categorized as spectrum sensing based way and database-driven based way to determine channel availability. In the former, a secondary user (SU) finds an available channel by listening and analyzing the primary user's (PU's) signal in the channel, namely spectrum sensing, while in the latter, an SU queries a database to get spectrum availability information at its location [2]. In database-driven CR, the SU is required to query the database with its physical location, so that the database can inform it about spectrum availability in its vicinity. This explicit exposure of SUs' location information to third (commercial) parties raises serious privacy concerns [3]. Therefore, spectrum sensing is still the direction of our efforts.

Spectrum sensing unit as part of CR technology deals with detecting the licensed spectrum that is not used by the PUs. Under the help of spectrum sensing, SUs can opportunistically access the licensed spectrum without changing the operations of PUs. Some spectrum sensing methods include matched filter, energy detection, cyclostationary detection, and wavelet detection [4]. However, these single-user

spectrum sensing methods are extremely difficult to fulfill the detection accuracy due to noise uncertainty, multipath fading, and shadowing. Once the PU signal experiences deep fading or blocked by obstacles, the power of the received PU signal at the SU may be too weak to be detected. To overcome these impacts, cooperative spectrum sensing is proposed to enhance the detection accuracy by exploiting spatial diversity via the observations of spatially located SUs. In cooperative spectrum sensing, there exist two groups of strategies for combining individual reports, e.g., soft-combining and hard-combining. Soft-combining technique combines raw signal power measurements from SUs, whereas in hard-combining technique a 0/1 decision from each SU is considered [5]. Finally, the FC is responsible for making a global decision on the presence or absence of the primary signal based on its received information.

However, security vulnerabilities can be exploited by different types of attacks that can be launched in CRNs, for example, jamming, spoofing, wiretap disruption attacks, etc [6]. Apart from these well-known traditional security threats, several recent studies consider the spectrum sensing data falsification attack (SSDF) attack (known as a Byzantine attack) and primary user emulation (PUE) attack. Fortunately the effects of PUE attack are transient, once the attacker vacates the frequency, the SUs notice the spectrum being once again idle, and can resume using it. In contrast, Byzantine attack is considered to be a hazardous attack [7], because the nature of aggregating data makes cooperative spectrum sensing offer opportunities for malicious users (MUs) to sneak into cooperative SUs. Those MUs send falsified local spectrum inference in order to confuse the FC, resulting in that the FC falsely concludes that there is or not an ongoing incumbent transmission [8]. This mode of operation is a typical Byzantine attack, and their aims are to prevent reliable SUs from using the idle channel or to allure them to access the channels in use and cause excessive interference to PUs, thereby undermining the premise of CR technology [9].

A. RELATED WORK

Byzantine attack has been widely studied as a serious threat to cooperative spectrum sensing in CRNs, and extensive malicious detection and suppression algorithms have been proposed to defend against it. Zeng *et al.* [10] present a trusted node assistance scheme to secure cooperative spectrum sensing based on reputation accumulation for combating the adverse effects of MUs. [11] learns about the CR potential malicious behaviors over time by estimating their probabilities of false alarm and detection and thereby identifies Byzantine attack. The proposed algorithm of [12] combines with [10], [11] to identify and weed out both of independent and balanced collaborative attackers. Reference [13] studies the problem of distributed sensing in the presence of Byzantine attack when the number of sensor nodes is finite and propose a likelihood-based algorithm to identify Byzantine nodes. Chaitanya and Chari [14] propose a reputation-based clustering algorithm to mitigate SSDF attack in a centralized cooperative spectrum sensing CRN. Althunibat *et al.* [15] consider symmetric cryptographic mechanism, which can produce a message authentication code (MAC) to verify the spectrum sensing data reports, but using MAC requires extra energy consumption to provide some additional bits and they also ignore the influence of SUs' report error rate. S. Althunibat also present a robust algorithm against two types of SSDF attack in [16], including greedy attack and malicious attack.

Zhang *et al.* [17] propose a probabilistic soft SSDF attack model and discover a trade-off between destructiveness and stealthiness. By dividing the entire area of interest into cells, removing MUs based on their updated reputation scores and then providing larger weighting coefficients for detected results from cells with better channel conditions, the proposed reputation-based cooperative spectrum sensing algorithm in [18] is able to accurately remove MUs in a mobile CRN. Ye *et al.* [19] propose a faithworthy cooperative spectrum sensing scheme based on the Dempster-Shafer theory of evidence and holistic credibility to effectively defend against SSDF attack from MUs. In [20], a novel method of using clustering techniques for detecting and isolating SSDF attackers in a CRN is investigated by K. Rina *et al.* Pei *et al.* [21] propose a neighbor detection based spectrum sensing algorithm to solve the problem of wrong or inconsistent decision due to attackers or connectivity failure. Reference [22] proposes an easy, efficient and fast collaborative spectrum sensing scheme in CRNs to counter Byzantine attack by counting mismatches between their local decisions and the global decision at the FC over a time window, and removes attackers from the data fusion process. Reference [23] and [24] provide a comprehensive overview of the studies on Byzantine attack and defense for cooperative spectrum sensing in CRNs.

In the field of Byzantine attack mitigation, the above approaches are nothing more than reputation-based, evidence theory, clustering-based, consensus theory, etc. They often involve unrealistic assumptions such as MUs are in minority or trusted node(s) exist for data fusion. Most of them assume a somehow simplified attack strategy, i.e., the essence of two types of SSDF attack in [16] is a simple "always attack". It is noteworthy that this static attack strategy can be easily identified, especially when the malicious percentage is relatively small. Thereupon, there are different attack strategies that is adopted by the FC being compromised and controlled by the intelligent MUs, which are spread in the following research.

Marano *et al.* [25] consider distributed detection in the presence of Byzantine sensors created by an intruder and characterize the power of attack analytically. But they assume very strong Byzantine sensors that actually know the true hypothesis. This model is overly conservative. Rawat *et al.* [26] significantly extend the results of [25] in the context of wireless sensor networks to the context of CRNs. There are still many questions that remain to be explored such as an analysis of the dynamic interaction among the Byzantines and the FC to find the optimal strategy which can

maximize their performance. Kailkhura *et al.* [27] consider the problem of distributed Bayesian detection with Byzantine data, and obtain the closed form expression for the optimal attack strategy that most increase the error probability. The knowledge regarding the optimal attack strategy can be further used to implement the optimal detector at the FC. The non-asymptotic case is further presented in [28]. Unfortunately, Kailkhura *et al.* [27], [28] only focus on a distributed network and their researches are carried out under the assumption of the known proportion of Byzantine attack, but fail in considering an effective method to estimate or determine attack parameters. Not only that, but the performance criterion they choose are also questionable.

B. OUR CONTRIBUTIONS

Such limitations fuel the motivation in providing a broader and a more complete view on Byzantine attack and defense strategy of cooperative spectrum sensing. In this paper, there is continuing effort to comprehensively analyze various dynamic scenarios where both the FC and Byzantine attacker act in a strategic manner, but without any limitations on Byzantine attack and unrealistic assumptions. This paper makes three major contributions as follows.

- Starting with an objective to consider a generic Byzantine attack model, we analyze the negative effects of Byzantine attack on the network and derive the condition which makes the FC blind from the malicious perspective.
- When MUs are unaware of the fusion rule adopted by the FC, we analyze the optimal attack strategy how to maximize the local Bayes risk. Besides, in a known fusion rule (i.e., the majority rule), the optimal attack strategy is also deduced for maximizing the global Bayes risk.
- Another interesting extension to the scenario where both the FC and MUs know opponent's strategies. The FC employs an estimation algorithm to estimate the fraction of MUs and attack parameters, aiming to minimize the global Bayes risk while MUs take advantage of the optimal attack strategy to maximize the global Bayes risk.

Additionally, in order to comprehensively characterize strategies from MUs and the FC, we provide numerical results to verify our theoretical analyses and estimation algorithm. The rest of the paper is structured as follows: Section II formulates system mode including network model and Byzantine attack model; The preliminary analysis is provided in Section III, including the condition to make the FC blind and the performance criterion; Section IV discusses the attack strategy of scenario where MUs know or do not know the FC's strategy; Section VI further analyzes the attack strategy of scenario where both the FC and MUs act in a tragic manner to optimize their own utilities; Next in Section V, extensive simulations corroborate the correctness of theoretical analyses and effectiveness of the proposed algorithm; Finally, Section VII concludes this paper.

II. SYSTEM MODEL

A. NETWORK MODEL

Considering Byzantine attack has more impact in a centralized CRN wherein the false information can propagate quickly [29]. We assume a centralized CRN consisting of a FC, a PU and N collaborative SUs, a fraction ρ of N SUs is malicious.

In order to opportunistically access available spectrums, various spectrum sensing methods can be applied in CRNs, among which the most common is energy detector as it can be facilely implemented in hardware and without knowing any prior information about the PU signal. The PU signal detection can be formulated as a binary hypothesis test in the energy detection, and the spectrum sensing model at the i-th SU can be described as follows

$$\begin{aligned} y_i(n) &= u_i(n), \quad H_0 \\ y_i(n) &= h_i(k)s(n) + u_i(n), \quad H_1 \end{aligned} \tag{1}$$

where H_0 and H_1 represent the hypothesis on the presence or absence of the PU signal, prior probabilities of which are denoted by $P(H_0)$ and $P(H_1)$, respectively. The SU's received signal $s(n)$ transmitted by the PU is distorted by the channel gain $h_i(k)$ at the k-th sensing interval, $u_i(n)$ denotes the additive white Gaussian noise (AWGN) with mean zero and variance σ_0^2. Without loss of generality, $s(n)$ and $u_i(n)$ are assumed to be independent. The test statistic of the i-th SU for energy detector is calculated as

$$E_i(k) = \sum_{n=1}^{N_s} |y(n)|^2 = \begin{cases} \sum_{n=1}^{N_s} |u_i(n)|^2, H_0 \\ \sum_{n=1}^{N_s} |h_i(k)s(n) + u_i(n)|^2, H_1 \end{cases} \tag{2}$$

where N_s is the number of samples over a sensing interval. For a large N_s (i.e. $N_s > 10$), using central limit theorem, the probability density function (PDF) of $E_i(k)$ can be approximated by a Gaussian distribution as follows

$$E_i(k) \sim \begin{cases} \mathcal{N}(\mu_0, \sigma_0^2), H_0 \\ \mathcal{N}(\mu_1, \sigma_1^2), H_1 \end{cases} \tag{3}$$

where $\mu_0 = N_s\sigma_0^2$, $\sigma_0^2 = 2N_s\sigma_0^4$, $\mu_1 = N_s(\gamma_i(k)+1)\sigma_0^2$, $\sigma_1^2 = 2N_s(\gamma_i(k)+1)^2\sigma_0^4$, $\gamma_i(k) = |h_i(k)|^2\sigma_1^2/\sigma_0^2$ is the average SNR of the PU measured at the i-th secondary receiver of interest.

Then, the local sensing performance (i.e., the false alarm and miss detection probability) can be calculated by comparing the local measured energy with a predefined threshold. Each SU individually submits raw signal power measurement or a bit decision to the FC according to soft-combining or hard-combining technology. Several recent methods of quantifying sensing data have also been proposed in [30] [31]; however, this study is beyond the scope of our work. Due to space consideration, we only present the binary hard-combining case with a relatively low communication overhead but similar results are also obtained in the case of soft-combining.

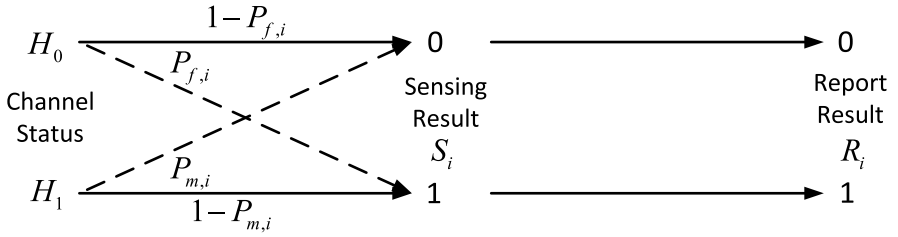

FIGURE 1. Local spectrum Sensing.

After each SU independently performs local spectrum sensing via energy detection and make a bit decision 0 or 1 regarding the presence of the phenomenon. The false alarm and miss detection probability for the i-th reliable SU can be further represented as

$$P_{f,i} = P(S_i = 1|H_0) \tag{4}$$

and

$$P_{m,i} = P(S_i = 0|H_1) \tag{5}$$

Under a prior channel status, the reliable SU truly submits the sensing result S_i to the FC, the report result R_i received by the FC is consistent with the sensing result from the reliable SU (i.e., $R_i = S_i$), as depicted in Figure 1.

B. BYZANTINE ATTACK MODEL

To avoid interference to the primary network, strict requirements on the detection accuracy are set, but the local sensing performance is limited by the fundamental characteristics of dynamically changed wireless channel. Therefore, cooperative spectrum sensing has been proposed to overcome this problem, the cooperative sensing performance can be improved by exploiting independent fading and multiple-user diversity.

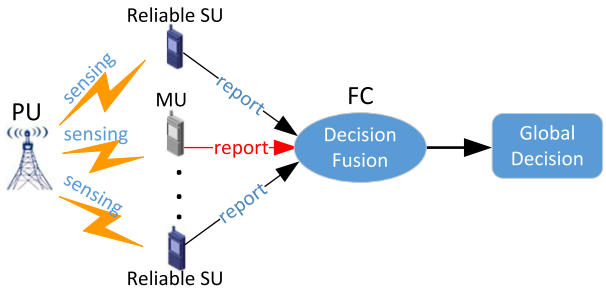

FIGURE 2. Cooperative spectrum sensing model.

In the process of cooperative spectrum sensing, as shown in Figure 2, after the local spectrum sensing is completed, each SU submits individual sensing report to the FC via a common control channel (the common control channels between SUs and the FC are assumed to be error-free). The FC uses data fusion technology to make a global decision regarding the PU activity. Although the participation of multiple SUs contributes to the improvement of detection accuracy, the global decision may be misguided when MUs flip individual sensing results via Byzantine attack and send these sensing results falsified to the FC, which further degrades the global performance.

Existing Byzantine attacks toward cooperative spectrum sensing generally fall into three categories based on the way they send false sensing reports [32]. The first type of attack is the one who always declares that the PU is active (i.e., the MU always submits a bit decision 1 to the FC), called Always-Yes (AY) attack. Always-No (AN) attack which always reports the absence of primary signal (i.e., the MU always submits a bit decision 0 to the FC) is the second type. The third type is Always-False (AF) attack which always reports the information opposite to the sensing result. In details, it submits 0 to the FC when the MU has sensed the PU's presence, while submits 1 when the PU is absence.

Apparently, "always attack" is an unadvisable strategy when MUs encounter drastic countermeasures or hostile environments. If the attack probability is appropriately set, such as, misleading the network occasionally but behaving correctly during the rest of the time [23], the MU exploits the opportunity of collaboration to sneak into a reliable SU and to launch stealth attack without being identified. On this account, a dynamic attack probability will be a reasonable choice in consideration of dynamic environment and countermeasures.

To gain a better understanding about malicious behaviors from Byzantine attack, let us present two phenomena in the decision-making. The first one is that a MU flips own sensing result 0 into 1 and submits it to the FC, its ultimate aim is to mislead the FC declaring that the channel is busy, resulting in the false alarm. The second one is that a MU flips own sensing result 1 into 0 and submits it to the FC announcing the channel as idle, with the intention of the miss detection. Combining these two phenomena, we show a generic Byzantine attack model in the process of cooperative spectrum sensing, one such example is the j-th MU, as illustrated in Figure 3. This generalized attack model can be mathematically represented as

$$\begin{cases} P(R_j = 1|S_j = 0) = \alpha \\ P(R_j = 0|S_j = 1) = \beta \end{cases} \tag{6}$$

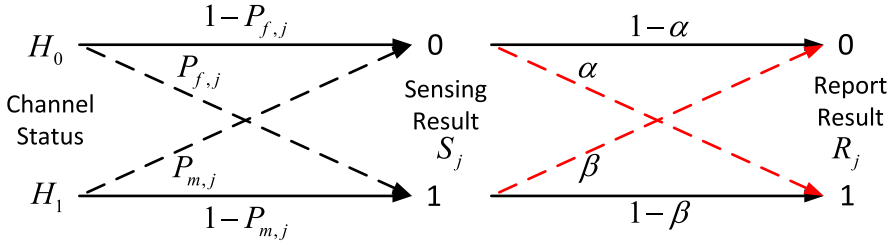

FIGURE 3. Generic Byzantine attack model.

where S_j is the sensing result and R_j is the report result. To be specific, on the one hand, when the j-th MU's sensing result S_j is 0, but the result R_j it actually reports to the FC is 1, this is false alarm attack, and α is the probability of false alarm attack which varies from 0 to 1. On the other hand, when the j-th MU's sensing result S_j is 1, but the result R_j it actually reports to the FC is 0, this is miss detection attack, and β is the probability of miss detection attack which varies from 0 to 1.

In this paper, each MU decides to launch Byzantine attack independently relying on its own observation and decision, the local performance is assumed to be the same among all SUs irrespective of whether they are honest or malicious, i.e., $P_{f,1} = P_{f,2} = \cdots = P_{f,N} = P_f$, $P_{m,1} = P_{m,2} = \cdots = P_{m,N} = P_m$. Using the local spectrum sensing and attack model, the false alarm probability and miss detection probability of the j-th MU can be represented as

$$\begin{aligned} P^m_{f,j} &= P((R_j = 1|S_j = 0)|H_0) + P((R_j = 1|S_j = 1)|H_0) \\ &= (1 - P_f)\alpha + P_f(1 - \beta) \end{aligned} \tag{7}$$

and

$$\begin{aligned} P^m_{m,j} &= P((R_j = 0|S_j = 0)|H_1) + P((R_j = 0|S_j = 1)|H_1) \\ &= P_m(1 - \alpha) + (1 - P_m)\beta \end{aligned} \tag{8}$$

where $P^m_{f,1} = P^m_{f,2} \cdots = P^m_{f,\rho N} = P^m_f$ and $P^m_{m,1} = P^m_{m,2} \cdots = P^m_{m,\rho N} = P^m_m$.

The generic Byzantine attack model is more consistent with malicious behaviors, and it can evolve different attack strategies because both of α and β can independently vary from 0 to 1, including "always attack". The traditional "always attack" is a special case of the generic attack model, such as, that is AN attack when $\alpha = 1$, $\beta = 0$; that is AY attack when $\alpha = 0$, $\beta = 1$; that is AF attack when $\alpha = 1$, $\beta = 1$.

Similar to our proposed Byzantine attack model, some researches assume an identical false alarm attack probability and miss detection attack probability, i.e., $\alpha = \beta$ [33] [34], even some of them arbitrarily regard the malicious percentage ρ as attack strength, such as [35]. Obviously, they fail to take the independence between the false alarm attack and the miss detection attack into consideration, and even confuse the difference between the attack probability and the malicious percentage. Besides, Li and Han [36] also propose a similar generic attack model, but one main limitation is that they only consider a MU in CRNs. In contrast, there is no special or a priori assumption in our proposed generic Byzantine attack model.

C. BYZANTINE FRAMEWORK

Now, we focus on a Bayesian detection framework for the PU signal detection. After the FC receives the report vector $\mathbf{R} = [R_1, R_2, \cdots, R_N]$ from SUs, the global decision is made by considering the maximum a posteriori probability rule which is expressed by $\frac{P(\mathbf{R}|H_1)}{P(\mathbf{R}|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \frac{P(H_0)}{P(H_1)}$ [37].

Given the independence of report results, the maximum a posteriori probability rule simplifies to the K-out-of-N rule. Therefore, the global false alarm and detection probability under this rule for data fusion are given by [28]

$$Q_f = \sum_{n=K}^{N} \binom{N}{n} P^n_{fa}(1 - P_{fa})^{N-n} \tag{9}$$

and

$$Q_d = \sum_{n=K}^{N} \binom{N}{n} P^n_{da}(1 - P_{da})^{N-n} \tag{10}$$

where P_{fa} is the conditional probability of the report result 1 given H_0 and P_{da} is the conditional probability of the report result 1 given H_1 over a sensing interval. By incorporating Byzantine attack into cooperative spectrum sensing, P_{fa} and P_{ma} can be represented as

$$P_{fa} = \rho P^m_f + (1-\rho)P_f = P_f + \rho((1-P_f)\alpha - P_f\beta) \tag{11}$$

and

$$P_{ma} = \rho P^m_m + (1-\rho)P_m = P_m + \rho((1-P_m)\beta - P_m\alpha) \tag{12}$$

where $P_{da} = 1 - P_{ma}$.

III. PRELIMINARY ANALYSIS

In this section, how a group of MUs make the FC blind in cooperative spectrum sensing is of our concern. We first formulate the blind problem of decision-making and then provide a closed form expression of the blind condition. Subsequently, we adopt Bayes risk instead of the error probability and Kullback-Leibler divergence (KLD) as the performance criterion and give the expression of overall Bayes risk.

A. BLIND CONDITION

Through Byzantine attack, MUs try to undermine the network operability, that is, the FC's ability of making the correct decision regarding the PU's presence or absence [26]. If possible, they would want to make the FC completely unable to decide on a particular decision, i.e., to make the cooperative sensing performance no better than a random guess of the channel status [38].

Numerous efforts have been paid to combat Byzantine attack threat and have shown the satisfactory performance in some setting, but little attention to the blind problem. This motivates us to address the question: what is the condition which makes the FC blind? In the Bayesian framework, we say that the FC is blind, if the received data does not provide any information about the hypotheses to the FC [28]. In other words, the report result received by the FC is completely independent of the hypothesis test. That is, the condition to make the FC blind can be stated as

$$P(\mathbf{R}|H_0) = P(\mathbf{R}|H_1) \tag{13}$$

Given the hypothesis, assume that each SU's sensing obseravtion is subject to conditional independent and identically distribution, the condition (13) becomes $P_{fa} = P_{da}$. Accordingly, we have

$$P_f+\rho((1-P_f)\alpha-P_f\beta)=1-P_m+\alpha(P_m\alpha-(1-P_m)\beta) \tag{14}$$

By some simple algebraic manipulations, (14) can be simplified as

$$\rho = \frac{1}{\alpha+\beta} \tag{15}$$

From (15), a critical value of 50% of MUs can completely blind the FC when $\alpha = \beta = 1$, it is also the minimum malicious percentage that makes the FC blind. Obviously, the assumptions about a low malicious percentage or especial ''always attack'' strategy enable the previous works to escape the blind problem.

B. BAYES RISK

The false alarm and detection probability or the error probability are the commonly used performance metric to characterize the system performance. In addition, KLD is also employed as the performance metric to measure the difference between two probability distributions, i.e., [25] [26], but the probability distribution of R is less affected by Byzantine attack when there only exist a few MUs or the attack probability is small. The more importance lies in that the different impacts of false alarm attack and miss detection attack are ignorant. For the network administrator, there may be a tradeoff between the waste of spectrum resources and the harmful interference to the primary network respectively caused by false alarm attack and miss detection attack, because they impose different risks on the secondary and primary network. It therefore makes sense to ask, ''what is the risk (loss)?''

In the Bayes theory, the criterion is minimum Bayes risk, where Bayes risk is defined as the average of a risk function with respect to the joint distribution of R and hypotheses [39]. In this regard, we elect Bayes risk as a performance metric instead of the error probability and KLD, which is represented as

$$\begin{aligned} L &= \sum_{u=0}^{1}\sum_{v=0}^{1} L_{u,v}P(H_v)P(H_u|H_v) \\ &= L_{0,1}P(H_1)P(H_0|H_1) + L_{1,0}P(H_0)P(H_1|H_0) \\ &= L_{0,1}P(H_1)(1-Q_d) + L_{1,0}P(H_0)Q_f \end{aligned} \tag{16}$$

where $P(H_u|H_v)$ is the conditional probability of declaring H_u when H_v is true ($u = 0, 1$; $v = 0, 1$), and $L_{u,v}$ is the corresponding risk, where $L_{0,0} = L_{1,1} = 0$. Specifically, Bayes risk simplifies to the error probability when $L_{0,1} = L_{1,0} = 1$. In practice, our research could be also applied for KLD.

IV. BYZANTINE ATTACK V. S. UNKNOWN OR KNOWN FUSION RULE

In this section, we derive the optimal attack strategy under various parameters to achieve the maximal local Bayes risk when MUs are unware of the fusion rule. Furthermore, a series of analyses will be provided on how MUs achieve the maximal global Bayes risk by the optimal Byzantine attack (α^*, β^*) under the majority fusion rule.

A. SCENARIO I: UNKNOWN FUSION RULE

Starting with the scenario where MUs have no knowledge of the FC's strategy, that is to say, the K-out-of-N rule used by the FC for MUs is unknown. The lack of knowledge of the fusion rule makes MUs only consider how to maximize the local Bayes risk. Since the local Bayes risk is independent of the fusion rule, we can formulate the local Bayes risk as

$$\begin{aligned} L_l &= L_{0,1}P(H_1)P_{ma} + L_{1,0}P(H_0)P_{fa} \\ &= L_{0,1}P_m + P(H_0)(L_{1,0}P_f - L_{0,1}P_m) + h_1\rho\alpha + h_2\rho\beta \end{aligned} \tag{17}$$

where $h_1 = L_{1,0}P(H_0)(1-P_f) - L_{0,1}P(H_1)P_m$, $h_2 = L_{0,1}P(H_1)(1-P_m) - L_{1,0}P(H_0)P_f$.

The local Bayes risk L_l is a linear function of α and β, respectively. It can be seen from (17) that the signs of h_1 and h_2 determine the optimal attack strategy (α^*, β^*). According to the relation of $\frac{L_{1,0}}{L_{0,1}}$, $\frac{P(H_1)P_m}{P(H_0)(1-P_f)}$ and $\frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, (α^*, β^*) can be summarized below.

(a) If $\frac{L_{1,0}}{L_{0,1}} < \frac{P(H_1)P_m}{P(H_0)(1-P_f)}$ and $\frac{L_{1,0}}{L_{0,1}} < \frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, then $h_1 < 0$ and $h_2 > 0$, $(\alpha^*, \beta^*) = (0, 1)$.

(b) If $\frac{L_{1,0}}{L_{0,1}} > \frac{P(H_1)P_m}{P(H_0)(1-P_f)}$ and $\frac{L_{1,0}}{L_{0,1}} > \frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, then $h_1 > 0$ and $h_2 < 0$, $(\alpha^*, \beta^*) = (1, 0)$.

(c) If $\frac{P(H_1)P_m}{P(H_0)(1-P_f)} < \frac{L_{1,0}}{L_{0,1}} < \frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, then $h_1 > 0$ and $h_2 > 0$, $(\alpha^*, \beta^*) = (1, 0)$.

(d) If $\frac{P(H_1)P_m}{P(H_0)(1-P_f)} > \frac{L_{1,0}}{L_{0,1}} > \frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, then $h_1 < 0$ and $h_2 < 0$, $(\alpha^*, \beta^*) = (1, 0)$.

(e) If $\frac{L_{1,0}}{L_{0,1}} = \frac{P(H_1)P_m}{P(H_0)(1-P_f)} = \frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, then $h_1 = 0$ and $h_2 = 0$, the local Bayes risk is a constant value, regardless of the attack strategy.

B. SCENARIO II: MAJORITY FUSION RULE

When the majority rule is adopted by the FC, $K = \lceil (N+1)/2 \rceil$, the attack strategy is considered. Although the FC has control of the fusion rule, it is not strategic. Hence, MUs make use of the known majority rule to maximize the global Bayes risk, while the FC cannot take effective action against Byzantine attack due to unknown information about attack strategy. Under the majority rule, the global Bayes risk can be stated as

$$L_g = L_{0,1}P(H_1)(1 - \sum_{n=\lceil (N+1)/2 \rceil}^{N} \binom{N}{n} P_{da}^n (1-P_{da})^{N-n}) + L_{1,0}P(H_0) \sum_{n=\lceil (N+1)/2 \rceil}^{N} \binom{N}{n} P_{fa}^n (1-P_{fa})^{N-n} \quad (18)$$

In contrast to the local Bayes risk, the global Bayes risk L_g is a non-linear function. Therefore, before going into deep analysis of the optimal attack strategy, we declare the property of L_g separately regarding α and β. For this aim, assuming that $\rho < \min\{0.5 - P_f, 1 - \frac{N}{(2N-2)(1-P_m)}\}$, which implies that it is not sufficient to blind the FC. Under this assumption and (11) (12), the following result can be obtained as

$$\begin{aligned} P_d a &= (1-P_m)(1-\rho\beta) + \rho P_m \alpha \\ &= (1-P_m)(1-\rho\beta) + \rho P_m \alpha \geq (1-P_m)(1-\rho) \\ &> N/(2N-2) \end{aligned} \quad (19)$$

Otherwise,

$$\begin{aligned} P_{fa} &= P_f + \rho((1-P_f)\alpha - P_f\beta) \\ &\leq P_f + \rho(1-P_f)\alpha \leq P_f + \rho < 0.5 \end{aligned} \quad (20)$$

Depending on (19) and (20), a comprehensive analysis on the relation between the global Bayes risk L_g and attack strategy (α, β) is presented as below.

1) GLOBAL BAYES RISK W. R. T. α

First, for a fixed β, the partial derivative of L_g to α is obtained as follows:

$$\frac{\partial L_g(\alpha,\beta)}{\partial \alpha} = -L_{0,1}P(H_1)\frac{\partial Q_d}{\partial \alpha} + L_{1,0}P(H_0)\frac{\partial Q_f}{\partial \alpha} \quad (21)$$

where $\frac{\partial Q_f}{\partial \alpha} = N\binom{N-1}{K-1}\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}(1-P_{fa})^{N-K}$ and $\frac{\partial Q_d}{\partial \alpha} = N\binom{N-1}{K-1}\frac{\partial P_{da}}{\partial \alpha}P_{da}^{K-1}(1-P_{da})^{N-K}$. See Appendix for details. The derivation can be given as:

$$\begin{aligned} \frac{\partial L_g(\alpha,\beta)}{\partial \alpha} &= N\rho L_{0,1}\binom{N-1}{K-1}P(H_1)P_m(1-P_{da})^{N-K} \\ &\cdot P_{da}^{K-1}[\frac{L_{1,0}}{L_{0,1}}\frac{P(H_0)}{P(H_1)}\frac{(1-P_f)P_{fa}^{K-1}(1-P_{fa})^{N-K}}{P_m P_{da}^{K-1}(1-P_{da})^{N-K}} - 1] \end{aligned} \quad (22)$$

It is expedient to reformulate (22) as:

$$\frac{\partial L_g(\alpha,\beta)}{\partial \alpha} = f_\alpha(\alpha,\beta)[e^{g_\alpha(\alpha,\beta)} - 1] \quad (23)$$

where $f_\alpha(\alpha,\beta) = N\rho L_{0,1}\binom{N-1}{K-1}P(H_1)P_m P_{da}^{K-1}(1-P_{da})^{N-K}$ and $g_\alpha(\alpha,\beta) = ln(\frac{L_{1,0}}{L_{0,1}}\frac{P(H_0)}{P(H_1)}\frac{1-P_f}{P_m}) + (K-1)ln(\frac{P_{fa}}{P_{da}}) + (N-K)ln(\frac{1-P_{fa}}{1-P_{da}})$.

Observing (23), it is easily recognized that $f_\alpha(\alpha,\beta) > 0$, while the sign of $g_\alpha(\alpha,\beta)$ should be further confirmed. Taking the partial derivative of $g_\alpha(\alpha,\beta)$ with respect to α as follows:

$$\begin{aligned} \frac{\partial g_\alpha(\alpha,\beta)}{\partial \alpha} &= \rho(K-1)(\frac{1-P_f}{P_{fa}} - \frac{P_m}{P_{da}}) \\ &\quad - \rho(N-K)(\frac{1-P_f}{1-P_{fa}} - \frac{P_m}{1-P_{da}}) \end{aligned} \quad (24)$$

In order to further confirm the sign of (24), we start from $\frac{1-P_m}{P_m} > \frac{P_f}{1-P_f}$ to obtain

$$\begin{aligned} \rho\alpha + (1-\beta\rho)\frac{1-P_m}{P_m} &> \rho\alpha + (1-\beta\rho)\frac{P_f}{1-P_f} \\ \Leftrightarrow \frac{P_{da}}{P_m} &> \frac{P_{fa}}{1-P_f} \\ \Leftrightarrow \frac{1-P_f}{P_{fa}} &> \frac{P_m}{P_{da}} \end{aligned} \quad (25)$$

Similarly, it can be shown that

$$\frac{1-P_f}{1-P_{fa}} > \frac{P_m}{1-P_{da}} \quad (26)$$

According to our assumption, an inequity can be formulated as

$$\begin{aligned} \frac{(1-P_{fa})(1-P_{da})}{P_{fa}P_{da}} &> -1 \\ \Leftrightarrow \frac{1}{P_{fa}} - \frac{1}{1-P_{fa}} &> \frac{1}{P_{da}} - \frac{1}{1-P_{da}} \end{aligned} \quad (27)$$

Since $P_{fa} < 0.5$ and $\frac{1-P_f}{P_m} > 1$, (27) is equivalent to

$$\begin{aligned} \frac{1-P_f}{P_m}(\frac{1}{P_{fa}} - \frac{1}{1-P_{fa}}) &> \frac{1}{P_{da}} - \frac{1}{1-P_{da}} \\ \Leftrightarrow \frac{1-P_f}{P_{fa}} - \frac{P_m}{P_{da}} &> \frac{1-P_f}{1-P_{fa}} - \frac{P_m}{1-P_{da}} \end{aligned} \quad (28)$$

Using the above facts, we will prove that (24) is the non-decreasing function according to the parity of N respectively.

When the number of SUs N is odd, $K = (N+1)/2$, an inequity can be derived as

$$\begin{aligned} (\frac{N+1}{2} - 1)(\frac{1-P_f}{P_{fa}} - \frac{P_m}{P_{da}}) \\ > (N - \frac{N+1}{2})(\frac{1-P_f}{1-P_{fa}} - \frac{P_m}{1-P_{da}}) \end{aligned} \quad (29)$$

When the number of SUs N is even, $K = N/2 + 1$, combining (26) (28), an inequity can be obtained as

$$\begin{aligned} \frac{N}{2}(\frac{1-P_f}{P_{fa}} - \frac{P_m}{P_{da}}) &> \frac{N}{2}(\frac{1-P_f}{1-P_{fa}} - \frac{P_m}{1-P_{da}}) \\ &\quad - (\frac{1-P_f}{1-P_{fa}} - \frac{P_m}{1-P_{da}}) \end{aligned} \quad (30)$$

(29) and (30) are sufficient to show that $\frac{\partial L_g(\alpha,\beta)}{\partial \alpha} > 0$, then, L_g is a quasi-convex function of α under a fixed β when $\rho < \min\left\{0.5 - P_f, 1 - \frac{N}{(2N-2)(1-P_m)}\right\}$.

2) GLOBAL BAYES RISK W. R. T. β

Next, we continue to analyze the property of L_g with respect to β for a fixed α. Observing that the partial derivative of L_g to β,

$$\begin{aligned}
&\frac{\partial L_g(\alpha,\beta)}{\partial \beta} \\
&= N\binom{N-K}{K-1}[L_{1,0}P(H_0)\frac{\partial P_{da}}{\partial \beta}P_{fa}^{K-1}(1-P_{fa})^{N-K} \\
&\quad - L_{0,1}P(H_1)\frac{\partial P_{da}}{\partial \beta}P_{da}^{K-1}(1-P_{da})^{N-K}] \\
&= \rho N\binom{N-K}{K-1}L_{1,0}P(H_0)P_fP_{fa}^{K-1}(1-P_{fa})^{N-K} \\
&\quad \cdot[\frac{L_{0,1}}{L_{1,0}}\frac{P(H_1)}{P(H_0)}\frac{(1-P_m)P_{da}^{K-1}(1-P_{da})^{N-K}}{P_fP_{fa}^{K-1}(1-P_{fa})^{N-K}} - 1] \qquad (31)
\end{aligned}$$

The above can also be restated as follows:

$$\frac{\partial L_g(\alpha,\beta)}{\partial \beta} = f_\beta(\alpha,\beta)[e^{g_\beta(\alpha,\beta)} - 1] \qquad (32)$$

where $f_\beta(\alpha,\beta) = N\rho L_{1,0}\binom{N-1}{K-1}P(H_0)P_fP_{fa}^{K-1}(1-P_{fa})^{N-K}$ and $g_\beta(\alpha,\beta) = ln(\frac{L_{0,1}}{L_{1,0}}\frac{P(H_1)}{P(H_0)}\frac{1-P_m}{P_f}) + (K-1)ln(\frac{P_{da}}{P_{fa}}) + (N-K)ln(\frac{1-P_{da}}{1-P_{fa}})$.

Because $f_\beta(\alpha,\beta) > 0$, we further figure out the sign of $g_\beta(\alpha,\beta)$. By a mathematical investigation, the partial derivative of $g_\beta(\alpha,\beta)$ with respect to β can be given as follows:

$$\begin{aligned}
\frac{g_\beta(\alpha,\beta)}{\beta} &= \rho(N-K)(\frac{1-P_m}{1-P_{da}} - \frac{P_f}{1-P_{fa}}) \\
&\quad - \rho(K-1)(\frac{1-P_m}{P_{da}} - \frac{P_f}{P_{fa}}) \qquad (33)
\end{aligned}$$

To confirm the sign of (33), an inequity is proposed as

$$\begin{aligned}
&(1-\frac{2}{N})\frac{P_{da}P_{fa}}{(1-P_{da})(1-P_{fa})} > -1 \\
&\Leftrightarrow (1-\frac{2}{N})(\frac{1}{1-P_{da}} - \frac{1}{1-P_{fa}}) > \frac{1}{P_{da}} - \frac{1}{P_{fa}} \\
&\Leftrightarrow (\frac{N}{2}-1)(\frac{1}{1-P_{da}} - \frac{1}{P_{da}}) - \frac{1}{P_{da}} \\
&> (\frac{N}{2}-1)(\frac{1}{1-P_{fa}} - \frac{1}{P_{fa}}) - \frac{1}{P_{fa}} \qquad (34)
\end{aligned}$$

which follows our assumption.

Further, since the fact that $\frac{1-P_m}{P_f} > 1$, we have

$$\begin{aligned}
&\frac{1-P_m}{P_f}(\frac{1}{1-P_{da}} - \frac{1}{P_{da}}) > \frac{1}{1-P_{fa}} - \frac{1}{P_{fa}} \\
&\Leftrightarrow \frac{1-P_m}{1-P_{da}} - \frac{P_f}{1-P_{fa}} > \frac{1-P_m}{P_{da}} - \frac{P_f}{P_{fa}} \qquad (35)
\end{aligned}$$

Depending on the above results, we will prove that (32) is a non-decreasing function when N is an odd or even number.

When the number of SUs N is odd, $K = (N+1)/2$,

$$\begin{aligned}
&(N - \frac{N+1}{2})(\frac{1-P_m}{1-P_{da}} - \frac{P_f}{1-P_{fa}}) \\
&\qquad > (\frac{N+1}{2} - 1)(\frac{1-P_m}{P_{da}} - \frac{P_f}{P_{fa}}) \qquad (36)
\end{aligned}$$

When the number of SUs N is even, $K = N/2 + 1$, using (35), we have

$$\begin{aligned}
&\frac{1-P_m}{P_f}[(\frac{N}{2}-1)(\frac{1}{1-P_{da}} - \frac{1}{P_{da}}) - \frac{1}{P_{da}}] \\
&\quad > (\frac{N}{2}-1)[(\frac{1}{1-P_{fa}} - \frac{1}{P_{fa}}) - \frac{1}{P_{fa}}] \\
&\quad \Leftrightarrow \frac{N-1}{2}(\frac{1-P_m}{1-P_{da}} - \frac{P_f}{1-P_{fa}}) \\
&\quad > \frac{N+1}{2}(\frac{1-P_m}{P_{da}} - \frac{P_f}{P_{fa}}) \\
&\quad \Leftrightarrow (N - \frac{N}{2} + 1)(\frac{1-P_m}{1-P_{da}} - \frac{P_f}{1-P_{fa}}) \\
&\quad > (\frac{N}{2} + 1 - 1)(\frac{1-P_m}{P_{da}} - \frac{P_f}{P_{fa}}) \qquad (37)
\end{aligned}$$

Since $\frac{\partial g_\beta(\alpha,\beta)}{\partial \beta} > 0$ follows the proof of (36) and (37), it is concluded that when $\rho < \min\left\{0.5 - P_f, 1 - \frac{N}{(2N-2)(1-P_m)}\right\}$, L_g is a quasi-convex function of β for a fixed α.

By analyzing the property of L_g with respect to α and β, the optimal attack strategy (α^*, β^*) can be easily determined, as depicted in the Section IV.

V. BYZANTINE ATTACK V. S. OPTIMAL FUSION RULE

In this section, we investigate a scenario where the FC has the knowledge of the attack strategy by means of an estimation algorithm. Once the FC knows the attack strategy, the optimal fusion rule is expected to minimize the global Bayes risk. Meanwhile, the MU's goal is to maximize the global Bayes risk by acting in the optimal attack strategy. Next, we will analyze the optimal strategies of both sides for own utilizes in details.

A. OPTIMAL FUSION RULE

According to the K-out-of-N rule, the global Bayes risk can be stated as:

$$\begin{aligned}
L_g &= L_{0,1}P(H_1)(1 - \sum_{n=K}^{N}\binom{N}{n}P_{da}^n(1-P_{da})^{N-n}) \\
&\quad + L_{1,0}P(H_0)\sum_{n=K}^{N}\binom{N}{n}P_{fa}^n(1-P_{fa})^{N-n} \qquad (38)
\end{aligned}$$

From (38), the global Bayes risk L_g is an objective function with respect to the value of K. In order to find the optimal

K_{opt}, we calculate the partial derivative of L_g with respect to K as follows:

$$\begin{aligned}\frac{\partial L_g(K)}{\partial K} &\approx L_g(K+1) - L_g(K) \\ &= L_{0,1}P(H_1)\binom{N}{K}P_{da}^K(1-P_{da})^{N-K} \\ &\quad - L_{1,0}P(H_0)\binom{N}{K}P_{fa}^K(1-P_{fa})^{N-K} \end{aligned} \tag{39}$$

When $\frac{\partial L_g(K)}{\partial K} = 0$, then we have

$$\frac{L_{0,1}P(H_1)}{L_{1,0}P(H_0)}\frac{P_{da}^K}{P_{fa}^K}\frac{(1-P_{fa})^K}{(1-P_{da})^K} = \frac{(1-P_{fa})^N}{(1-P_{da})^N} \tag{40}$$

Taking the Napierian logarithm on both sides of (40), when $P_{da} > P_{fa}$ ($\rho < \frac{1}{\alpha+\beta}$), the optimal fusion rule is given as:

$$K^* = \frac{Nln(\frac{1-P_{fa}}{1-P_{da}}) - ln(\frac{L_{0,1}}{L_{1,0}}\frac{P(H_1)}{P(H_0)})}{ln(\frac{1-P_{fa}}{1-P_{da}}\frac{P_{da}}{P_{fa}})} \tag{41}$$

When $P_{da} < P_{fa}$ ($\rho > \frac{1}{\alpha+\beta}$), the optimal fusion rule is given as:

$$K^* = \frac{Nln(\frac{1-P_{da}}{1-P_{fa}}) - ln(\frac{C_{1,0}}{C_{0,1}}\frac{P(H_0)}{P(H_1)})}{ln(\frac{1-P_{da}}{1-P_{fa}}\frac{P_{fa}}{P_{da}})} \tag{42}$$

Therefore, the optimal fusion rule can be expressed as K_{opt}, where $K_{opt} = K^*$ (K^* may not be an integer). According to (41) and (42), the optimal fusion rule is related to attack parameters, it is necessary to estimate attack parameters (ρ, α, β). The estimation algorithm is formulated in the following subsection.

B. ATTACK PARAMETERS ESTIMATION

There have been many estimation algorithms available to estimate attack parameters, but they often involve unrealistic assumptions such as a few MUs and/or the special type of attack, in addition to increasing the computational complexity. Here, we propose a simple and straightforward algorithm to estimate attack parameters. The main idea of our proposed estimation algorithm is to distinguish between the MU and reliable SU by observing the local sensing performance of all SUs. Due to the unfavorable channel condition of wireless transmission, it is a tough task to accurately identify the MU in a short time. A proper observation period is needed to observe the performance of all SUs. Next, we introduce an estimation algorithm consisting of consistency check and error-tolerant selection.

1) CONSISTENCY CHECK

Although cooperative spectrum sensing significantly improve the detection accuracy, the global decision may not be reliable because of the presence of Byzantine attack. Subsequently, the global decision as a criterion is not applicable for measuring the local decision. Therefore, an alternative method should be considered to confront Byzantine attack, even is also feasible in the presence of a large number of MUs. In the framework of CRNs, the whole knowledge about the channel is grasped by the primary network, but the PU has no obligation to convey the channel status for helping the CRN [40]. Therefore, it is necessary to reconsider the process of periodic spectrum sensing for consistency check of the local decision.

In retrospect, a sensing interval consists of a sensing slot, a report slot, a transmission slot in CRNs. In the sensing slot, each SU individually performs the local spectrum sensing, and then submits individual decision to the FC in the report slot. The FC is responsible for the global decision making on the presence or absence of the primary signal based on its received information and determines whether SUs can access idle channels to delivery data transmission or not. Encouraged by [41] and [42], the main idea of data transmission evaluation is to take advantage of the delivery of the transmitted data of the scheduled SU after the sensing slot. The difference, however, is that delivery-based assessment of [41] and [42] only considers one case when the licensed channel is decided as idle by the FC while our data transmission evaluation covers two cases, which is described in more detail below. In the one case, the FC declares the licensed channel as idle, which implies that at least one of SUs can be scheduled to access the unused channel for data transmission. The successful delivery of the transmitted data reveals that the global decision was correct and the channel is unused. If the transmitted data cannot be successfully delivered, the global decision is identified as incorrect, and the channel is occupied.

In the other case, the FC declares the licensed channel as busy, all SUs need to switch to another channel and sense its availability in the next sensing interval. If there is no data transmission (the reason for this is that the reliable SUs have switched another channel to continue spectrum sensing) which represents the global decision was correct, otherwise incorrect.

In the above two cases, the data transmission reveals the true channel status after a sensing interval, in other words, the FC can be used to check consistency of received reports. As an evaluation criterion, data transmission evaluation is much more reliable than the global decision, even in the worst scenario where Byzantine attack makes the FC blind. From implementation point of view, the data transmission evaluation approach can be easily applied in a centralized CRNs where each SU individually accesses the spectrum, the data transmission can be verified by the FC itself or another delegated reliable SU [41], [42].

It should be noted that data transmission evaluation itself is defect-free, however, the process of implementation is not absolutely reliable. For example, although the global decision is indeed correct in the first case, the data transmission failure is possible due to environmental conditions and malfunctioning. In the second case, the licensed channel is actually being utilized by the PU, the data transmission from the SU may also be successful, although it will the interfere with

the primary network. Therefore, a certain error-tolerant is considered in the next subsection.

2) ERROR-TOLERANT SELECTION

During the local spectrum sensing, Byzantine attack results in that the MU's sensing performance may not satisfy the target performance requirements, such as, the target false alarm probability $\bar{P}_f$ and the target miss detection probability $\bar{P}_m$. For a reliable SU, wireless network environment and the malfunction of hardware may also affect its performance. Hence, we take the error-tolerant into account and assume that ϵ_f and ϵ_m respectively represent the tolerant false alarm error and the tolerant miss detection error. In other words, the false alarm and miss detection probability not exceeding $\bar{P}_f + \epsilon_f$ and $\bar{P}_m + \epsilon_m$ for each SU is tolerable. Once the false alarm probability $P_{f,i}$ or the miss detection probability $P_{m,i}$ is larger than $\bar{P}_f + \epsilon_f$ or $\bar{P}_m + \epsilon_m$, the i-th SU is regarded as a MU during an observation period.

After a sensing interval, those SUs who do not meet the performance requirement constitute a set of MUs $|\hat{N}_a|$, thus the estimated value of the proportion of MUs is expressed as

$$\hat{\rho} = \frac{\hat{N}_a}{N} \tag{43}$$

where $\hat{N}_a$ is the estimated value of the number of MUs.

We further average the performance of MUs in $\hat{N}_a$, which is given as

$$\bar{P}_{fa} = \frac{\sum_i^{|\hat{N}_a|} P_{f,i}}{\hat{N}_a} \tag{44}$$

$$\bar{P}_{ma} = \frac{\sum_i^{|\hat{N}_a|} P_{m,i}}{\hat{N}_a} \tag{45}$$

Using (9) and (10), the estimated values of the attack probability can be calculated by

$$\hat{\alpha} = \frac{\bar{P}_{fa}(1-P_m) - (1-\bar{P}_{ma})P_f}{1-P_f-P_m} \tag{46}$$

$$\hat{\beta} = \frac{\bar{P}_{ma}(1-P_f) - (1-\bar{P}_{fa})P_m}{1-P_f-P_m} \tag{47}$$

Utilizing all features discussed above, the parameter estimation algorithm can be described in Algorithm 1.

3) OPTIMAL ATTACK STRATEGY

Utilizing the estimation algorithm, FC adopts the optimal fusion rule K_{opt} to minimize the global Bayes risk $L_g(K_{opt})$, while MUs try to maximize $L_g(K_{opt})$ by choosing the optimal attack strategy.

Proposition: Given the optimal fusion rule K_{opt} and $\rho \leq 0.5$, $L_g(K_{opt})$ is a monotonically increasing function of α for a fixed β if $g_\alpha(\alpha, \beta) > 0$. Similarly, $L_g(K_{opt})$ is a monotonically increasing function of β for a fixed α if $g_\beta(\alpha, \beta) > 0$.

Proof: Observing $g_\alpha(\alpha, \beta) > 0$ and $g_{beta}(\alpha, \beta) > 0$, when $g_\alpha(\alpha, \beta) > 0$, K satisfies the following inequity:

$$K < K_u \tag{48}$$

where $K_u = \frac{Nln(\frac{1-P_{fa}}{1-P_{da}}) + ln(\frac{P_{da}}{P_{fa}}) + ln(\frac{L_{1,0}P(H_0)}{L_{0,1}P(H_1)}) + ln(\frac{1-P_f}{P_m})}{ln[\frac{P_{da}(1-P_{fa})}{P_{fa}(1-P_{da})}]}$.

Algorithm 1 Estimation Algorithm

```
Initial N̂_a = 0, P_{f,i} = 0, P_{m,i} = 0, i = 1, 2, 3, ··· N.
for k = 1 : 1000 do
  for i = 1 : N do
    Count the local sensing performance: P_{f,i}, P_{m,i}.
    if P_{f,i} − P̄_f > ε_f or P_{m,i} − P̄_m > ε_m then
      N̂_a = N̂_a + 1;
    else
      continue;
    end if
  end for
  Calculate the estimated value of the proportion of MUs ρ̂;
  Average the false alarm and miss detection probabilities of MUs;
  Calculate the estimated values of the attack probability α̂ and β̂;
end for
```

Otherwise, when $g_\beta(\alpha, \beta) > 0$, K satisfies that

$$K > K_l \tag{49}$$

where $K_l = \frac{Nln(\frac{1-P_{fa}}{1-P_{da}}) + ln(\frac{P_{da}}{P_{fa}}) - ln(\frac{L_{0,1}P(H_1)}{L_{1,0}P(H_0)}) - ln(\frac{1-P_m}{P_f})}{ln[\frac{P_{da}(1-P_{fa})}{P_{fa}(1-P_{da})}]}$.

Proposition is definitely true if it is sufficient to show $K_u > K_{opt} > K_l$. Obviously, $K_{opt} > K_l$ is true if we can prove $K^* > K_l$. Since

$$K_l - K^* = ln(\frac{P_f}{1-P_m}\frac{P_{da}}{P_{fa}})/ln(\frac{1-P_{fa}}{1-P_{da}}\frac{P_{da}}{P_{fa}}) \tag{50}$$

Using the fact of $\frac{P_m}{1-P_m} < \frac{1-P_f}{P_f}$, we have the following inequity

$$\begin{aligned} &\frac{P_m}{1-P_m} + \rho(\beta - \frac{P_m}{1-P_m}\alpha) \\ &< \frac{1-P_f}{P_f} + \rho(\beta - \frac{1-P_f}{P_f}\alpha) \\ &\Leftrightarrow \frac{P_m + \rho((1-P_m)\beta - P_m\alpha)}{1-P_m} \\ &< \frac{1-P_f-\rho((1-P_f)\alpha - P_f\beta)}{P_f} \\ &\Leftrightarrow \frac{1-P_{da}}{1-P_m} < \frac{1-P_{fa}}{P_f} \end{aligned} \tag{51}$$

yielding $K^* > K_l$ which guarantees $K_{opt} > K_l$.

Besides, it can be observed that $K_u > K_{opt}$ is equivalent to $K_u - K^* > K_{opt} - K^*$. Considering $1 > K_{opt} - K^*$, $K_u > K_{opt}$ can follow by $K_u - K^* > 1$. Since

$$K_u - K^* = ln(\frac{P_m}{1-P_f}\frac{P_{da}}{P_{fa}})/ln(\frac{1-P_{fa}}{1-P_{da}}\frac{P_{da}}{P_{fa}}) \tag{52}$$

Using the fact of (25), $K_u > K_{opt}$ is true. Consequently, the proof is completed. Hence, according to ***Proposition*** and

the blind condition, we can summarize the optimal attack strategy to maximize the global Bayes risk as:

$$(\alpha^*, \beta^*) = \begin{cases} (1, 1), & if\ \rho \leq 0.5 \\ (\bar{\alpha}, \bar{\beta}), & if\ \rho > 0.5 \end{cases} \tag{53}$$

where $(\bar{\alpha}, \bar{\beta})$ satisfies $\rho(\bar{\alpha} + \bar{\beta}) = 1$.

VI. NUMERICAL RESULTS

Numerical results are presented to corroborate theoretical analyses in the context of various scenarios. The local and global Bayes risk are simulated by varying attack strategy. Given the importance of not causing interference to the primary network, the loss of mistakenly declaring primary absence $L_{0,1}$ is set to be 4, and the loss of mistakenly declaring primary presence $L_{1,0}$ is set to be 2.

A. UNKNOWN FUSION RULE

The local Bayes risk is of their concern when MUs are unaware of the FC's strategy. Thus, we first verify theoretical analyses of *Scenario I* through simulation results.

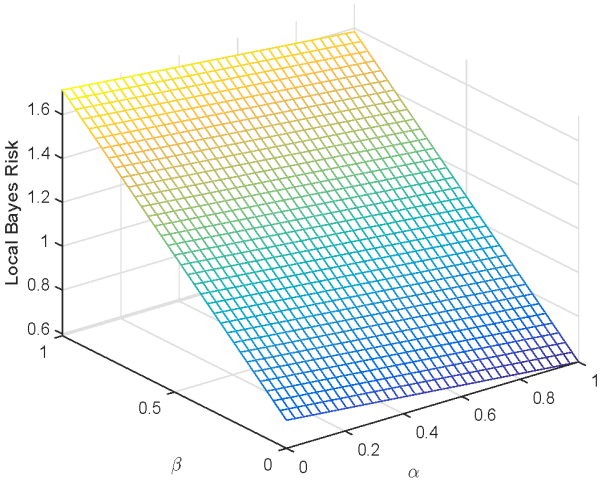

FIGURE 4. Local Bayes risk when $P(H_0) = 0.2$, $P_m = P_f = 0.2$.

In Figure 4, the local Bayes risk with respect to α and β is shown when $P(H_0) = 0.2$, $P_m = P_f = 0.2$. Such that $\frac{P(H_1)P_m}{P(H_0)(1-P_f)} = 1$, $\frac{P(H_1)(1-P_m)}{P(H_0)P_f} = 16$, thus $\frac{L_{1,0}}{L_{0,1}} < \frac{P(H_1)P_m}{P(H_0)(1-P_f)} < \frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, which is followed by (a) of (17). In fact, we can see from Figure 4 that there is a negative linear correlation between the local Bayes risk and α while a positive linear correlation between the local Bayes risk and β. Undoubtedly, the optimal attack strategy is $(\alpha^*, \beta^*) = (0, 1)$.

Figure 5 plots the local Bayes risk with respect to α and β when $P(H_0) = 0.8$, $P_m = P_f = 0.2$. Such that $\frac{P(H_1)P_m}{P(H_0)(1-P_f)} = 0.0278$, $\frac{P(H_1)(1-P_m)}{P(H_0)P_f} = 2.25$, thus we have $\frac{P(H_1)P_m}{P(H_0)(1-P_f)} < \frac{L_{1,0}}{L_{0,1}} < \frac{P(H_1)(1-P_m)}{P(H_0)P_f}$, which is followed by (c) of (17). The positive linear correlation between the local Bayes risk and α or β is shown in Figure 5. Obviously, the optimal attack strategy is $(\alpha^*, \beta^*) = (1, 1)$.

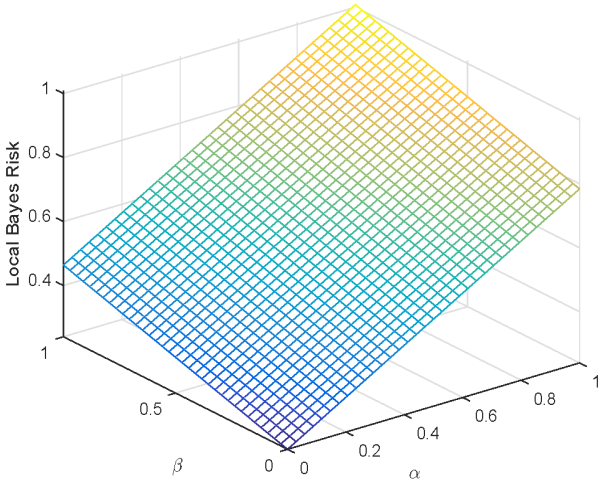

FIGURE 5. Local Bayes risk when $P(H_0) = 0.8$, $P_m = P_f = 0.1$.

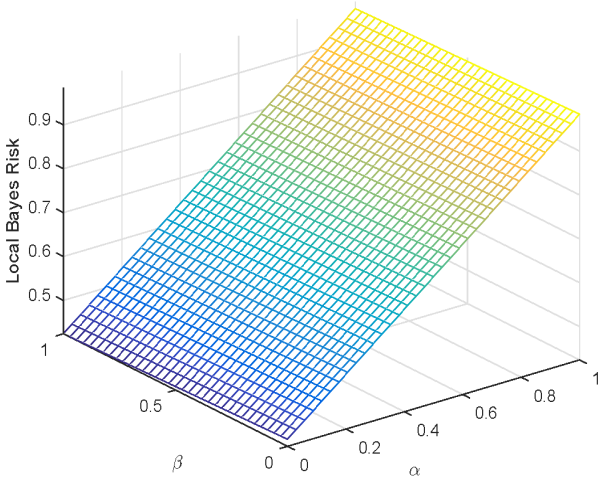

FIGURE 6. Local Bayes risk when $P(H_0) = 0.9$, $P_m = P_f = 0.2$.

When $P(H_0) = 0.9$, $P_m = P_f = 0.2$, Such that $\frac{P(H_1)P_m}{P(H_0)(1-P_f)} = 0.0278$, $\frac{P(H_1)(1-P_m)}{P(H_0)P_f} = 0.4444$, thus we have $\frac{P(H_1)P_m}{P(H_0)(1-P_f)} < \frac{P(H_1)(1-P_m)}{P(H_0)P_f} < \frac{L_{1,0}}{L_{0,1}}$, the result complies with (b) of (17). The positive or negative linear correlation between the local Bayes risk and α or β is illustrated in Figure 6, which implies that the optimal attack strategy is $(\alpha^*, \beta^*) = (1, 0)$.

B. MAJORITY FUSION RULE

In another scenario where MUs have known the fusion rule while the FC does not act in a strategic manner, MUs achieve the maximal global Bayes risk by the optimal attack strategy. In the following simulation environments, unless otherwise specified, we consider that the prior probability of the hypothesis H_0 is set to 0.8, the average SNR is 5 dB and the number of samples N_s over a sensing interval is equal to 20. The percentage of MUs ρ is taken as 0.4. The target false alarm probability $\bar{P}_f$ is fixed to constant value 0.02 as well as the target miss detection probability $\bar{P}_m$, and the detection threshold λ is determined by $\bar{P}_f$.

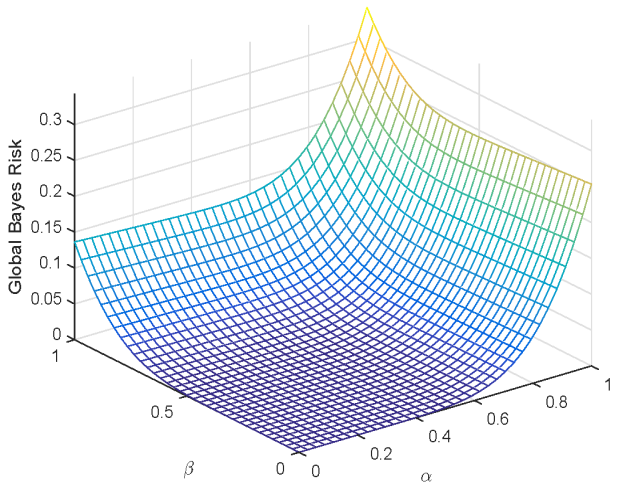

FIGURE 7. Global Bayes risk when $N = 21$.

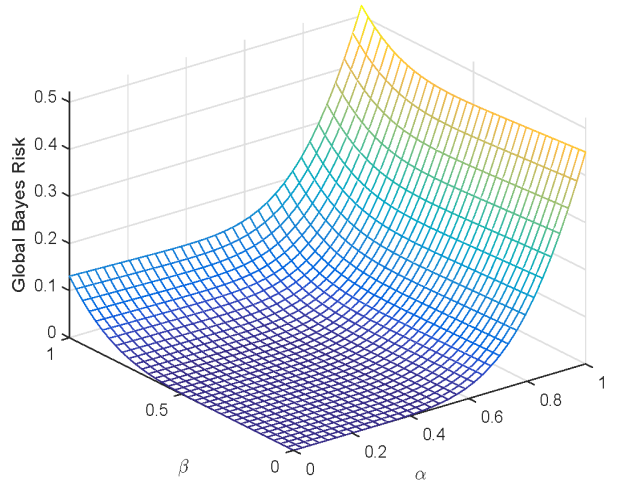

FIGURE 8. Global Bayes risk when $N = 20$.

The global Bayes risk with respect to α and β is displayed in the plot of Figure 7 when the number of MUs is odd, i.e., $N = 21$. As we can see in Figure 7, the global Bayes risk L_g is a quasi-convex function of α for a fixed β. Similarly, Figure 8 illustrates the global Bayes risk with respect to α and β in the presence of the even number of MUs, i.e., $N = 20$. The global Bayes risk L_g can also be recognized as a quasi-convex function of β for a fixed α. Given the malicious percentage ρ, it is concluded that simulation results are consistent with theoretical analyses on the relation between the global Bayes risk and the attack strategy (α, β). Considering quasi-convexity, the optimal attack strategy (α^*, β^*) can only be one of the following three possibilities: (1,0), (0,1), (1,1).

C. OPTIMAL FUSION RULE

Before simulating the optimal fusion rule, numerical results are first provided to illustrate the proposed estimation algorithm. The number of collaborative SUs N is assumed to be 20. The tolerant false alarm error ϵ_f is set to be 0.04 and the tolerant miss detection error ϵ_m is set to be 0.06 by several experiments, the larger or smaller ϵ_f or ϵ_m is not conducive to accurately estimate attack parameters.

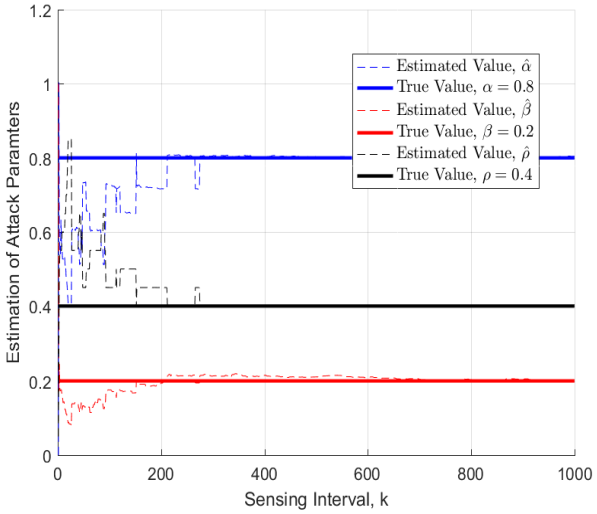

FIGURE 9. Estimation of attack parameters.

According to our proposed estimation algorithm, the convergence of attack parameters for $\alpha = 0.8$, $\beta = 0.2$ and $\rho = 0.4$ is depicted in Figure 9. The estimated value $\hat{\alpha}$ and $\hat{\alpha}$, $\hat{\beta}$ are converged to constant values after applying almost 600 rounds of sensing. This result corroborates the effectiveness of the estimation algorithm, in the simulation, the initial stage can be set as the first 600 sensing intervals where attack parameters are estimated and then used to obtain the optimal fusion rule.

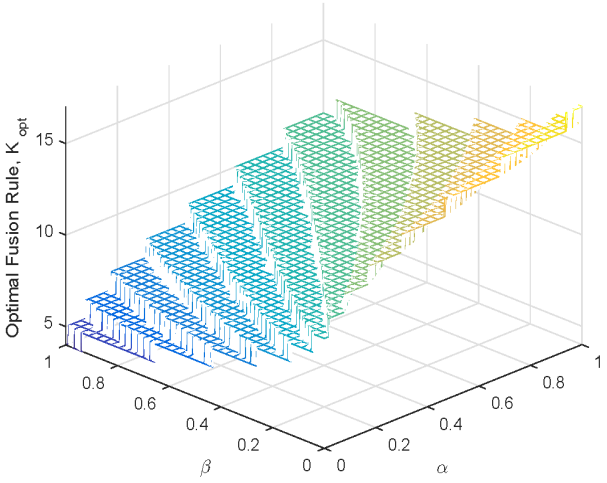

FIGURE 10. Optimal fusion rule when $\rho = 0.4$.

After estimating the attack strategy, the FC subsequently adopt the optimal fusion rule K_{opt} to suppress MUs. As shown in Figure 10, K_{opt} shows a step change under various attack strategies when $\rho = 0.4$. Moreover, Figure 11 plots the

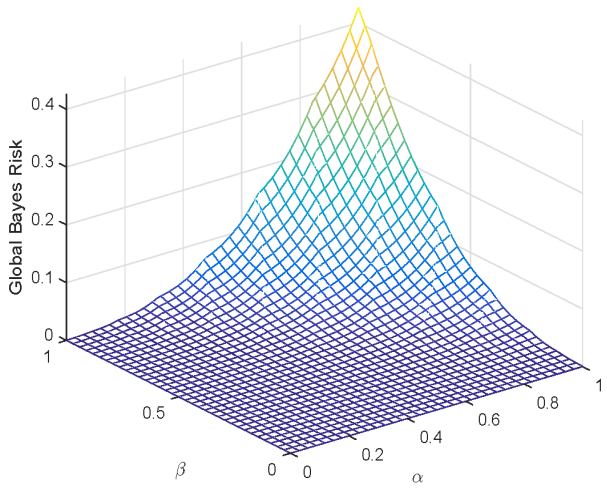

FIGURE 11. Global Bayes risk when $\rho = 0.4$.

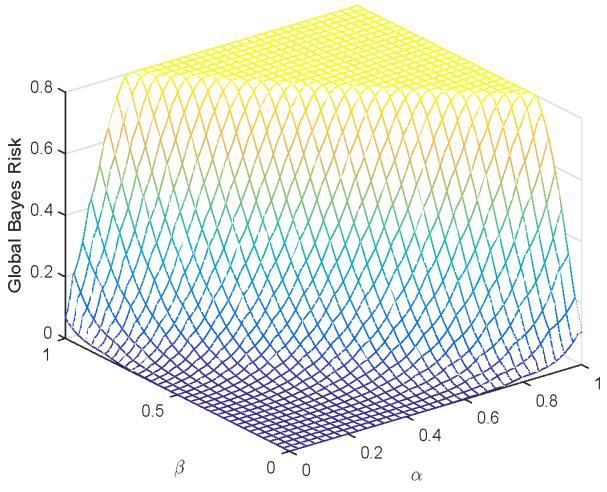

FIGURE 12. Global Bayes risk when $\rho = 0.8$.

global Bayes risk when the FC adopts the optimal fusion rule. It is observed that the global Bayes risk respectively increases as α and β varying from 0 to 1, thus the optimal attack strategy (α^*, β^*) to maximize the global Bayes risk is (1,1). For the other case $\rho = 0.8$, we can see that the optimal attack strategy is not unique in Figure 12. This is due to the fact that MUs can achieve the maximal global Bayes risk by setting appropriate attack parameters (i.e., ρ, α, β) when the attack strategy satisfies the blind condition. But once the blind condition is satisfied, such as $\rho = 0.8 \geq 1/(\alpha + \beta)$, in our simulation environment, the global Bayes risk L_g is fixed at 0.8. This is the worst performance that the FC offers and the best attack gain that MUs achieve in the scenario, unless either party change own strategies.

VII. CONCLUSION

In this paper, we make an in-depth investigation on strategies of both Byzantine attack and the FC in cooperative spectrum sensing for CRNs. First of all, a generic Byzantine attack model has been considered, a MU has a certain probability, varying from 0 to 1, to conduct attacks, followed by the condition which makes the FC blind. On basis of this generalized attack model, we analyze a sophisticated scenario where Byzantine attack makes the FC blind and derive the blind condition. Then, we show the optimal attack strategy which MUs maximize the local or global Bayes risk respectively in the context of the unknown and known K-out-of-N rule. Besides, numerous efforts on the scenario where the FC has the knowledge of attack strategy by means of the proposed estimation algorithm. Subsequently, the FC minimizes the global Bayes risk by the optimal fusion rule while MUs maximize the global Bayes risk by the optimal attack strategy. Finally, numerical results are presented that show the correctness of our theoretical analyses and the effectiveness of the estimation algorithm. Our work is different from existing works in that we provide recent advances and open research directions on applying the FC and Byzantine attack in various scenarios focusing on the optimal attack strategy as well as the optimal defense strategy for cooperative spectrum sensing.

APPENDIX
THE PARTIAL DERIVATIVE OF L_g W. R. T. α

$$\frac{\partial Q_f}{\partial \alpha} = \binom{N}{K}(K\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}(1-P_{fa})^{N-K} - (N-K)$$
$$\cdot \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K}(1-P_{fa})^{N-K-1}) + \binom{N}{K+1}((K+1)\frac{\partial P_{fa}}{\partial \alpha}$$
$$P_{fa}^{K}(1-P_{fa})^{N-K-1} - (N-K-1)\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K+1}$$
$$(1-P_{fa})^{N-K-2}) + \cdots + \binom{N}{N}(N\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{N-1} - 0)$$
$$= \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}(1-P_{fa})^{N-K}[(\binom{N}{K}K - \frac{P_{fa}}{1-P_{fa}}(N-K))$$
$$+ \binom{N}{K+1}((K+1)\frac{P_{fa}}{1-P_{fa}} - (N-K-1)\frac{P_{fa}^2}{(1-P_{fa})^2})]$$
$$= \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}(1-P_{fa})^{N-K}[(\binom{N}{K}K\frac{P_{fa}}{1-P_{fa}}(N-K))$$
$$+ \frac{P_{fa}}{1-P_{fa}}\binom{N}{K+1}((K+1) - (N-K-1)$$
$$\times \frac{P_{fa}}{1-P_{fa}}) + \cdots]$$

Because of $\binom{N}{K}\frac{K}{N} = \binom{N-1}{K-1}$, then

$$\frac{\partial Q_f}{\partial \alpha} = \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}(1-P_{fa})^{N-K}[\binom{N}{K}K + [-\frac{P_{fa}}{1-P_{fa}}\binom{N}{K}$$
$$\cdot (N-K) + \frac{P_{fa}}{1-P_{fa}}\binom{N}{K+1}(K+1)] + \cdots]$$

$$= \frac{\partial P_{fa}}{\partial \alpha} P_{fa}^{K-1}(1-P_{fa})^{N-K}\left[\binom{N-1}{K-1}N + \frac{P_{fa}}{1-P_{fa}} \cdot \left[\binom{N}{K+1}(K+1) - \binom{N}{K}(N-K)\right] + \cdots\right]$$

$$= \frac{\partial P_{fa}}{\partial \alpha}(1-P_{fa})^{N-K}\left[\binom{N-1}{K-1}N + \frac{P_{fa}}{1-P_{fa}} * 0\right]$$

$$= N\binom{N-1}{K-1}\frac{\partial P_{fa}}{\partial \alpha} P_{fa}^{K-1}(1-P_{fa})^{N-K}$$

Similarly, $\frac{\partial Q_d}{\partial \alpha} = N\binom{N-1}{K-1}\frac{\partial P_{da}}{\partial \alpha} P_{da}^{K-1}(1-P_{da})^{N-K}$.

REFERENCES

[1] 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, Apr. 2009.

[2] Z. Chen, L. Chen, and H. Zhong, "Towards secure and verifiable database-driven spectrum sharing," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 285–296.

[3] M. Grissa, B. Hamdaoui, and A. A. Yavuza, "Location privacy in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1726–1760, 3rd Quart., 2017.

[4] 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, pp. 1–15, 2010.

[5] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in *Proc. IEEE Symp. New Frontiers Dyn. Spectr.*, Apr. 2010, pp. 1–12.

[6] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. IEEE 3rd Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun. (CrownCom)*, May 2008, pp. 1–8.

[7] R. Lohia and I. Batra, "Reputation based proposed scheme to ensure reliable decision by fusion centre," *Indian J. Sci. Technol.*, vol. 9, no. 44, pp. 1–8, 2016.

[8] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Commun.*, vol. 12, no. 3, pp. 132–150, Mar. 2015.

[9] 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.

[10] 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.

[11] A. Vempaty, K. Agrawal, P. Varshney, and H. Chen, "Adaptive learning of Byzantines' behavior in cooperative spectrum sensing," in *Proc. IEEE Conf. Wireless Commun. Netw. (WCNC)*, Mar. 2011, pp. 1310–1315.

[12] M. Wang, B. Liu, and C. Zhang, "Detection of collaborative SSDF attacks using abnormality detection algorithm in cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2013, pp. 342–346.

[13] Z. Sun, C. Zhang, and P. Fan, "Optimal Byzantine attack and Byzantine identification in distributed sensor networks," in *Proc. IEEE Globecom Workshops*, Dec. 2016, pp. 1–6.

[14] D. L. Chaitanya and K. M. Chari, "Performance analysis of PUEA and SSDF attacks in cognitive radio networks," in *Computer Communication, Networking and Internet Security*. Singapore: Springer, 2017, pp. 219–225.

[15] S. Althunibat *et al.*, "On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1564–1567, Aug. 2013.

[16] S. Althunibat, M. Di Renzo, and F. Granelli, "Robust algorithm against spectrum sensing data falsification attack in cognitive radio networks," in *Proc. IEEE 79th Veh. Technol. Conf. (VTC Spring)*, May 2014, pp. 1–5.

[17] 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, p. 81, May 2014.

[18] X. Wang, M. Jia, Q. Guo, X. Gu, and G. Zhang, "Reputation-based cooperative spectrum sensing algorithm for mobile cognitive radio networks," *China Commun.*, vol. 14, no. 1, pp. 124–134, Jan. 2017.

[19] F. Ye, X. Zhang, Y. Li, and C. Tang, "Faithworthy collaborative spectrum sensing based on credibility and evidence theory for cognitive radio networks," *Symmetry*, vol. 9, no. 3, p. 36, Mar. 2017.

[20] K. Rina, S. Nath, N. Marchang, and A. Taggu, "Can clustering be used to detect intrusion during spectrum sensing in cognitive radio networks?" *IEEE Syst. J.*, vol. 12, no. 1, pp. 938–947, Mar. 2018.

[21] Q. Pei, H. Li, and X. Liu, "Neighbor detection-based spectrum sensing algorithm in distributed cognitive radio networks," *Chin. J. Electron.*, vol. 26, no. 2, pp. 399–406, 2017.

[22] A. S. Rawat, P. Anand, H. Chen, and R. K. Varshney, "Countering Byzantine attacks in cognitive radio networks," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Mar. 2010, pp. 3098–3101.

[23] A. H. S. Magdalene and L. Thulasimani, "Analysis of spectrum sensing data falsification attack in cognitive radio networks: A survey," *J. Sci. Eng. Educ.*, vol. 2017, no. 2, pp. 89–100, 2017.

[24] 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.

[25] 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.

[26] 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.

[27] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Asymptotic analysis of distributed Bayesian detection with Byzantine data," *IEEE Signal Process. Lett.*, vol. 22, no. 5, pp. 608–612, May 2015.

[28] 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.

[29] S. Madbushi, R. Raut, and M. S. S. Rukmini, "Security issues in cognitive radio: A review," in *Microelectronics, Electromagnetics and Telecommunications*. New Delhi, India: Springer, 2016, pp. 121–134.

[30] 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.

[31] H. Chen, M. Zhou, L. Xie, and J. Li, "Cooperative spectrum sensing with M-ary quantized data in cognitive radio networks under SSDF attacks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5244–5257, Aug. 2017.

[32] H. Rifà-Pous, M. J. Blasco, and C. Garrigues, "Review of robust cooperative spectrum sensing techniques for cognitive radio networks," *Wireless Pers. Commun.*, vol. 67, no. 2, pp. 175–198, 2012.

[33] A. Vempaty, O. Ozdemir, K. Agrawal, H. Chen, and P. K. Varshney, "Localization in wireless sensor networks: Byzantines and mitigation techniques," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1495–1508, Jun. 2013.

[34] 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.

[35] A. A. Sharifi and M. J. M. Niya, "Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 93–96, Jan. 2016.

[36] 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.

[37] P. K. Varshney, *Distributed Detection and Data Fusion*. New York, NY, USA: Springer, 1997.

[38] M. K. Vegi, "Study of Byzantine attackers and countermeasures in spectrum sensing," *Int. J. Health Promotion Educ.*, vol. 3, no. 3, pp. 1–61, 2014.

[39] L. L. Scharf, *Statistical Signal Processing*. Reading, MA, USA: Addison-Wesley, 1991.

[40] X. Chen, H.-H. Chen, and W. Meng, "Cooperative communications for cognitive radio networks—From theory to applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1180–1192, 3rd Quart., 2014.

[41] 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.

[42] S. Althunibat, B. J. Denise, and F. Granelli, "A punishment policy for spectrum sensing data falsification attackers in cognitive radio networks," in *Proc. IEEE 80th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2014, pp. 1–5.

JUN WU is currently pursuing the Ph.D. degree with the National Mobile Communication Research Lab, Southeast University, Nanjing, China. His research interests include sequential detection, game theory, machine learning and their application to the network security.

TIECHENG SONG received the B.S. and M.S. degrees from the Department of Radio Engineering, Southeast University, Nanjing, China, in 1989 and 1992, respectively, and the Ph.D. degrees from the School of Information Science and Engineering, Southeast University, in 2006.

In 1992, he joined the Department of Radio Engineering, Southeast University, as a Research Associate, where he is currently a Professor with the National Mobile Communication Research Lab, School of Information Science and Engineering. He has also served as the Executive Vice President of the Nanjing Institute of Communication Technology. The research interests of their group include 5G wireless systems, optical wireless communication technologies, and cognitive radio.

YUE YU is currently pursuing the Ph.D. degree with the National Mobile Communication Research Lab, Southeast University, Nanjing, China. His research interests include spectrum resource allocation, game theory, and network security.

CONG WANG is currently pursuing the Ph.D. degree with the National Mobile Communication Research Lab, Southeast University, Nanjing, China. Her research interests include spectrum resource allocation and its application to cognitive radio network.

JING HU was born in 1975. She received the Ph.D. degree from Southeast University in 2011. She is currently an Associate Professor and the Master Instructor with the National Mobile Communication Research Lab, Southeast University. Her research interests include cognitive radio, wireless sensor networks, and vehicle networks.