Beta Distribution Function for Cooperative Spectrum Sensing Against Byzantine Attack in Cognitive Wireless Sensor Networks

Jun Wu *, Tianle Liu , Rui Zhao

Posted Date: 15 July 2024

doi: 10.20944/preprints202407.1194.v1

Keywords: Cognitive wireless sensor networks; cooperative spectrum sensing; Byzantine attack; sequential process; beta reputation model

Article

Beta Distribution Function for Cooperative Spectrum Sensing against Byzantine Attack in Cognitive Wireless Sensor Networks

Jun Wu [1,2,*], Tianle Liu [1] and Rui Zhao [1]

[1] School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, Zhejiang 310018, China; wojames2011@163.com (J.W.); tianle@hdu.edu.cn (T.L.); zhaorui5925@163.com (R.Z.)
[2] National Mobile Communications Research Laboratory, Southeast University, Nanjing, Jiangsu 211189, China;
* Correspondence: wojames2011@163.com

Abstract: In order to explore more spectrum resources to support sensors and its related applications, cognitive wireless sensor networks (CWSNs) have emerged to identify available channels being underutilized by the primary user (PU). To improve the detection accuracy of the PU signal, cooperative spectrum sensing (CSS) among sensors paradigm is proposed to make a global decision about the PU status for CWSNs. However, CSS is susceptible to Byzantine attack from malicious sensor nodes due to its open nature, resulting in wastage of spectrum resources or causing harmful interference to PUs. To suppress the negative impact of Byzantine attack, this paper proposes a beta distribution function (BDF) for CSS among multiple sensors, which includes a sequential process, beta reputation model, and weight evaluation. Based on sequential probability ratio test (SPRT), we integrate the proposed beta reputation model into SPRT, while improving and reducing the positive and negative impacts of reliable and unreliable sensor nodes on the global decision, respectively. Finally, the numerical simulation results demonstrate that compared to SPRT and weighted sequential probability ratio test (WSPRT), the proposed BDF has outstanding effects in terms of the error probability, and average number of samples under various attack ratios and probabilities.

Keywords: cognitive wireless sensor networks; cooperative spectrum sensing; byzantine attack; sequential process; beta reputation model

1. Introduction

1.1. Background

In recent decades, wireless communication technology has developed rapidly, limited spectrum resources are no longer sufficient to meet the widely used and growing demand for sensors and their related applications and services. According to research by the Federal Communications Commission (FCC), spectrum resources are not fully utilized in both the time and spatial domains. But in order to popularize wireless sensor networks and improve their service quality, cognitive radio (CR) empowerment technology has emerged to support sensors in identifying and utilizing spectrum resources that are not used by the primary user (PU) and allowed to opportunistically be accessed without causing harmful interference to the PU [1], which is known as cognitive wireless sensor networks (CWSNs) [2].

In a CWSN, cooperative spectrum sensing (CSS) is the most critical technology, which refers to multiple sensors using local sensing technology to detect the signal of the PU, and then submit the sensing information to the fusion center (FC). The FC makes the final decision on the status of the PU through a specific rule. Therefore, those sensors are allowed to opportunistically access the channel being underutilized by the PU according to the final decision regarding the presence of the

 doi:10.20944/preprints202407.1194.v1

phenomenon. However, the cooperative process also provides malicious sensor nodes an opportunity to falsify sensing information after completing local sensing and submit it to the FC [3], misleading the FC to make an incorrect global decision and selfishly occupying spectrum resources or causing excessive interference to the PU [4]. This is Byzantine attack [5], and there is already a lot of research work in this field.

1.2. Related Works and Motivation

Byzantine attack in CSS, a.k.a. spectrum sensing data falsification (SSDF) attack, is one of the key adversaries to the success of CR networks. In recent years, research on Byzantine attacks and defense strategies has attracted attention and become a hot topic. In [6], L. Zhang et al. conducted extensive research and in-depth analysis on Byzantine attack and defense for CSS in CR networks. In [7], J. Wu et al. analyzed strategies between Byzantine attack and the FC in CSS for CR networks, and further evaluated the safety factor from Byzantine attacker's perspective by a trust-value algorithm in [8]. In [9], K. Zeng et al. presented a secure CSS scheme based on a reputation accumulation mechanism to mitigate the adverse impact of misbehaved CRs. A secure CSS strategy based on reputation mechanism for CWSNs is proposed by X. Luo to defend against Byzantine attack in [10]. In [11], R. Chen et al. proposed a weighted sequential probability ratio test (WSPRT) against Byzantine attack to improve the robustness of data fusion which integrates reputation accumulation of [9] into sequential probability ratio test (SPRT) and reduce the data collection communication overhead at the FC. However, these studies did not consider the situation of many Byzantine attackers, which would completely make the FC blind, resulting in the failure of these reputation methods based on global decision. In the presence of massive Byzantine attackers, Z. Sun et al. proposed a scheme, in which the reliability value is used for dynamically selection of the sensing strategy between CSS and independent spectrum sensing in [12] and [13]. But the authors did not mitigate the negative impact of massive Byzantine attackers, but instead replaced CSS with independent spectrum sensing. R. Lin et al. made use of blockchain to prevent independent and cooperative Byzantine attacks from malicious vehicle users in [14]. It is obvious that this decentralized method has lower efficiency in combating Byzantine attack. In [15], Y. Fu et al. proposed a scheme to identify probabilistic Byzantine attackers by using consistent property of each sensing user's historical reported data. This consistency property method has certain requirements for the scenario of the primary network.

Further, Z. Li et al. studied the sequential binary hypothesis test problem with Byzantine agents in both the FC and fully distributed formulations in [16]. In [17], an estimation diffusion least-mean-square-H (H represents the average node degree of all nodes) algorithm was proposed by F. Wan et al. to achieve better sensing performance against Byzantine and manipulation attack. In [18], C. Quan et al. investigated the negative effect of Byzantine attack on the CSS performance and used ordered transmission scheme to solve the binary hypothesis test problem, further in [19][20], the authors proposed the reputation and audit-based clustering with/without auxiliary anchor node algorithm against Byzantine attack in wireless sensor networks. These Byzantine attack defense algorithms or strategies have high computational complexity and require certain prior information (strategy analysis of both the FC and Byzantine agents) or ideal assumptions (auxiliary anchor node), but its applicability is limited to a certain extent.

In [21], a Dempster-Shafer evidence theory-based CSS for CWSNs was introduced by D. Yao et al. to deal with Byzantine attack. M. Ridouani et al. proposed authentication process and shifted spectrum sensing process to enhance the detection performance in [22]. Considering an erroneous feedback channel, a single decision reporting algorithm was developed by A. Chouhan et al. to mitigate the effect of Byzantine attack in [23]. Furthermore, the authors proposed a machine learning technique in [24] to identify malicious users in a CR network using the principal component analysis algorithm. To resist the dominated cooperative probabilistic Byzantine attack, L. Chen et al. proposed a JS-divergence based reputation algorithm to identify Byzantine attackers in [25]. In [26], A. Parmar et al. used a Gaussian mixture model to formulate an anomaly detection algorithm for detecting Byzantine attack. Although the above defense algorithms can identify and suppress Byzantine attack and secure the CSS process to some extent, they still cannot effectively defend against large-scale

 doi:10.20944/preprints202407.1194.v1

attack (with a high attack ratio) and low-intensity attack (with a low attack probability) and ensure the performance and efficiency of CSS in CWSNs.

Additionally, machine learning has gradually become one of the effective methods to solve network security problems in recent years. In [27], one class supporting vector machine (SVM) to obtain a modified SPRT test was used by J. Parras and S. Zazo to not only detect Byzantine attacker and potentially any other attack mechanism that has not a similar spectrum to the expected signal from normal sensors. N. Marchang et al. investigated a series of machine learning techniques for Byzantine identification in [28,29]. Z. Luo et al. proposed influence-limiting defense against learning evaluation-beating attack or other similar attack in [30]. Moreover, by providing a maximum margin hyperplane, Z. Zhang et al. used SVM to identify Byzantine attacker, in which the generated spectrum sensing data features benefit from the PU status in the training process. Although these machine learning algorithms have certain advantages in prior information, performance, and application scenarios, achieving these goals requires a large number of training sequences and computational costs, which is not suitable for low energy wireless sensor networks. Especially in large-scale CWSNs, lightweight computing and efficiency for CSS are indispensable.

1.3. Our Contributions

In order to guarantee the premise of CWSNs, the CSS process should be carefully taken into consideration in the context of Byzantine attack. Therefore, a widely applicable Byzantine attack model should be modeled first, and considering the robustness of subsequent Byzantine identification and suppression algorithm, the attack probability and attack ratio are not limited. Also, we consider the sequential binary hypothesis test to improve the CSS efficiency and beta distribution function (BDF) to guarantee the CSS performance. Then, the contributions of our work can be summarized as

To characterize Byzantine behavior from malicious sensor nodes in the CSS process, we design a pair of flexible attack parameters, i.e., attack probability and attack ratio, to carry out various attack strategies (i.e., always attack, probabilistic attack) and attack scales (i.e., small/large-scale attack).

Further, we convert the binary hypothesis test problem regarding the phenomenon of the presence about the PU into the sequential process to realize CSS among multiple sensors. To accurately evaluate the reputation value of each sensor, we formulate a beta reputation model to identify malicious sensor nodes.

Considering the storage capacity of the FC, the positive total evaluation and negative total evaluation within a window period is designed to quantify reliable and unreliable sensor nodes. Moreover, we exploit tuning parameters that reflect linear and multiplier growth to accurately to determine the weight of the likelihood ratio in the sequential process.

1.4. Organization

The rest of this paper is organized as follows. In Sections 2, a CWSN and Byzantine attack model are presented. Section 3 formulates BDF for CSS to defend against Byzantine attack from malicious sensor nodes. The correctness and effectiveness of BDF are verified in Section 4, in terms of the error probability, and the average number of samples. Finally, Section 5 concludes this paper.

2. System Model

In this section, we propose a centralized CWSN model in the presence of malicious sensor nodes. On basis of this, we further model a CSS paradigm among multiple sensor nodes, in which malicious sensor nodes launch Byzantine attack including various attack strategies and attack scales.

2.1. CWSN Model

Considering a centralized CWSN where consists of a PU, a FC, and N collaborative sensors, where the proportion of malicious sensor nodes is ρ, as shown in Figure 1. In a spectrum sensing frame structure, a frame duration includes a sensing slot, a reporting slot, and data transmission slot

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2024 doi:10.20944/preprints202407.1194.v1

[32], as shown in Figure 2. To opportunistically access the available channel and avoid harmful interference to the normal communication of the PU, all sensors detect the PU's signal with the help of the local sensing technology to at a sensing slot. Then, at the reporting slot, each sensor individually submits own sensing result to the FC via the error-free common control channel. After receiving the sensing results, the FC needs to make a global decision about the PU's status through a specific rule. Finally, according to the global decision, the FC broadcasts a message to sensors, which determines whether allows sensor nodes to access the channel or not. In details, if the global decision is 1, sensors will be allowed to transmit data at the data transmission slot, otherwise will be forbidden to access the channel and continue spectrum sensing at the next sensing frame.

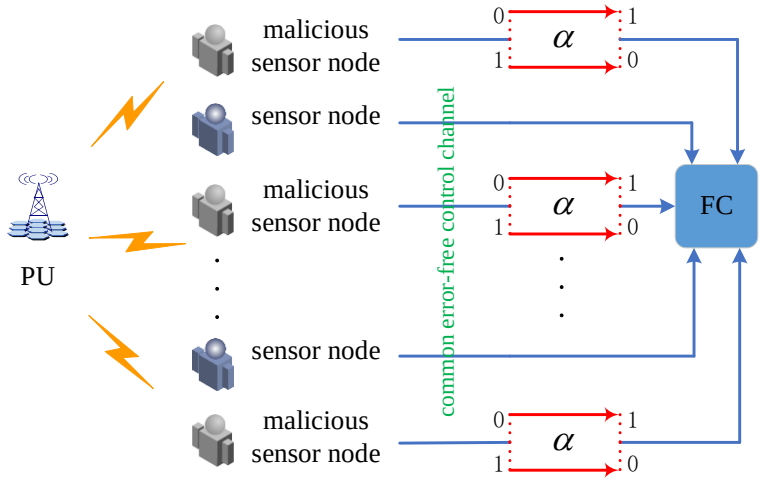

Figure 1. CSS in the presence of Byzantine attack.

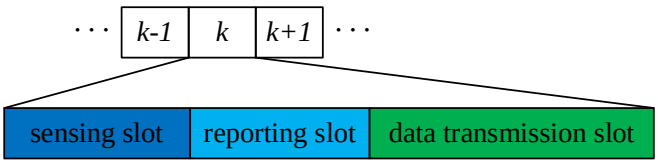

Figure 2. The spectrum sensing frame structure.

2.2. Byzantine Attack Model

On basis of CSS paradigm and its open nature, some malicious nodes may take advantage of this opportunity to launch Byzantine attack. Specifically, after completing the local sensing, the malicious sensor nodes will falsify own sensing result and submit it to the FC, aiming to mislead the FC into making an incorrect decision about the PU's status. To further analyze Byzantine behaviors, the local spectrum sensing performance, i.e., the local false alarm and miss detection probabilities, are assumed to be the same for each sensing node, denoted by P_f and P_m. Then, at the k-th sensing, the local sensing result and the received sensing result are denoted by $L_i(k)$ and $R_i(k)$, respectively, Byzantine behaviors from the malicious sensor node can be described by an attack probability as

$$\alpha = \begin{cases} P(R_i(k) = 1 | L_i(k) = 0) \\ P(R_i(k) = 0 | L_i(k) = 1) \end{cases} \quad (1)$$

where α varies from 0 to 1. Such an attack strategy represents the attack probability of that the malicious sensor nodes flips the sensing result 1 to 0 or 0 to 1. Therefore, the false alarm and miss detection probabilities at the malicious sensing nodes can be given by

$$P_{fa} = (1 - P_f)\alpha + P_f(1 - \alpha) = \alpha + P_f - 2\alpha P_f \quad (2)$$

$$P_{ma} = (1 - P_m)\alpha + P_m(1 - \alpha) = \alpha + P_m - 2\alpha P_m \quad (3)$$

Specifically, if the attack probability α is set to 1, the malicious sensor node carries out always attack strategy. In addition to the attack strategy, the proportion of malicious sensor nodes should also be taken into consideration. Many current research works only consider the situation where there are relatively few malicious nodes, because the global decision at the FC cannot be distorted by a

 doi:10.20944/preprints202407.1194.v1

small number of malicious sensor nodes, so malicious sensor nodes can be easily identified through global decision. Once there are a large number of malicious sensor nodes in CWSNs, i.e. $\rho > 50\%$, traditional algorithms will no longer be effective. Therefore, in order to achieve more secure CSS algorithm, defense against large-scale attack should also be indispensable.

3. Beta Distribution Function

In this section, encouraged by SPRT, we adopt SPRT as the fundamental CSS framework to reduce samples required at the FC. On basis of this, a beta reputation model is formulated to distinguish malicious sensor nodes and integrated into the sequential process of CSS.

3.1. Sequential Process

According to the received sensing results, the FC adopts a specific fusion rule to mitigate the negative impact of Byzantine attack on CSS. In addition, considering the number of sensors, the cooperative efficiency should be also taken into consideration to decrease the samples required by the FC, therefore reduce the communication overhead from the sensor node to the FC. To this end, we propose BDF for CSS against Byzantine attack.

At the beginning, we adopt SPRT as a CSS framework to improve the cooperative efficiency when the FC collects the sensing information from sensor nodes. In details, SPRT requires the knowledge a priori probabilities of $L_i(k)$ when the hypotheses $\mathcal{H}_0$ or $\mathcal{H}_1$ of that the PU is absent or present, i.e., $P_r(L_i(k)|\mathcal{H}_0)$ and $P_r(L_i(k)|\mathcal{H}_1)$. Relying on these assumptions, the FC sequentially calculates the likelihood ratio and makes a global decision according to the following decision variable, i.e.,

$$S_n = \prod_{i=1}^{n} \frac{P_r(L_i(k)|\mathcal{H}_1)}{P_r(L_i(k)|\mathcal{H}_0)} \tag{4}$$

where n represents the number of sensing results/samples required by the FC at a sensing frame and varies from 1 to N. Further, the global decision will be made according to the following criterion

$$\begin{cases} S_n \geq \xi_u, & the\ FC\ accepts\ \mathcal{H}_1 \\ S_n \leq \xi_l, & the\ FC\ accepts\ \mathcal{H}_0 \\ \xi_l < S_n < \xi_u, & the\ FC\ takes\ next\ obseravtion \end{cases} \tag{5}$$

where ξ_u and ξ_l are defined as

$$\xi_u = \frac{1-\bar{P}_f}{\bar{P}_m}, \tag{6}$$

and

$$\xi_l = \frac{\bar{P}_f}{1-\bar{P}_m}, \tag{7}$$

respectively, $\bar{P}_f$ and $\bar{P}_m$ are tolerated false alarm and miss detection probabilities, respectively.

Compared to Bayesian detection and Neyman-Pearson, SPRT to a certain extent saves the number of samples required for the FC to efficiently make a global decision, without any performance loss. However, similar to Bayesian detection, Neyman-Pearson, it also cannot defend against Byzantine attack. Therefore, it is necessary to take the security and performance into consideration. Motivated by this disadvantage of SPRT, a reputation mechanism is usually integrated into the weighted sequential process, as given in

$$\begin{aligned} S_n &= \prod_{i=1}^{n} \left[\frac{P_r(L_i(k)|\mathcal{H}_1)}{P_r(L_i(k)|\mathcal{H}_0)}\right]^{w_i(k)} \\ &= \prod_{i=1}^{n} \left\{\left[\frac{P_r(L_i(k)=1|\mathcal{H}_1)}{P_r(L_i(k)=1|\mathcal{H}_0)}\right]^{d_i(k)} * \left[\frac{P_r(L_i(k)=0|\mathcal{H}_1)}{P_r(L_i(k)=0|\mathcal{H}_0)}\right]^{1-d_i(k)}\right\}^{w_i(k)} \\ &= \prod_{i=1}^{n} \left\{\left[\frac{1-P_m}{P_f}\right]^{d_i(k)} * \left[\frac{P_m}{1-P_f}\right]^{1-d_i(k)}\right\}^{w_i(k)} \end{aligned} \tag{8}$$

 doi:10.20944/preprints202407.1194.v1

To be specific, the reputation of the i-th sensor nodes after the k-th sensing is obtained by following reputation mechanism [6]

$$T_i(k) = T_i(k-1) + (-1)^{R_i(k)+g(k)} \tag{9}$$

Thus, the likelihood ratio weight of the i-th sensor node is designed as [8]

$$w_i(k+1) = \begin{cases} 0, & T_i(k) \le -g \\ \dfrac{T_i(k)+g}{max\left(T_i(k)\right)+g}, & T_i(k) > -g \end{cases} \tag{10}$$

However, when the FC makes global decision, WSPRT is easily affected by large-scale attack and cannot accurately output reputation values, leading to the failure of weight. Hence, a reputation mechanism still remains a major challenge. To this end, we integrate a beta reputation model into the sequential process in the following subsection.

3.2. Beta Reputation Model

Following above purpose, we consider that during the local sensing, the sensing results can be categorized into two possibilities, following a binomial distribution. The beta distribution is suitable for describing the probability distribution characteristics of binomial events. Hence, we can establish a reputation model to allocate member reputation values. This approach helps mitigate reputation fluctuations caused by factors such as noise uncertainty, multipath fading, or shadowing, thereby safeguarding the normal senor nodes from excessive defensive actions by the FC.

Let x represent the actual local sensing result transmitted by sensors and y represent the local sensing result after being falsified by malicious sensors. Using r to denote the number of occurrences of event x and s to represent the number of occurrences of event y. By setting $\beta_0 = r + 1$ and $\beta_1 = s + 1$, the probability density function can be derived by [7]

$$f(p|\beta_0, \beta_1) = \frac{\Gamma(\beta_0+\beta_1)}{\Gamma(\beta_0)\Gamma(\beta_1)} p^{\beta_0-1}(1-p)^{\beta_1-1} \tag{11}$$

where $\Gamma(\cdot)$ is a Gamma function, p represents the probability of sensing behaviors and $0 \le p \le 1$. Besides, $\beta_0 > 0$, $\beta_1 > 0$. The expectation of event x is

$$E[Beta(\beta_0, \beta_1)] = \frac{\beta_0}{\beta_0+\beta_1} \tag{12}$$

Then, the reputation value of the i-th sensor node is evaluated by beta function, i.e.,

$$T_i = Beta(r_i+1, s_i+1) = \frac{r_i+1}{r_i+s_i+2} \tag{13}$$

3.3. Weight Evaluation

To effectively combat Byzantine attack, the FC employs a beta reputation system to allocate reputation value to sensor nodes based on historical sensing behavior. This approach establishes a dynamic reputation evaluation for CSS by means of data delivery mechanism. It is known that a fixed frame duration consists of a sensing slot, a reporting slot, and a data transmission slot in a periodic spectrum sensing frame. After at the reporting slot, the FC makes a global decision about the PU status according to (2), such as, when the global decision is 1, all sensors are forbidden to access the channel, while the global is 0, all sensors are allowed to access the channel. Nevertheless, due to the negative impact of Byzantine attack, the global decision may be unreliable. Hence, we have following consideration, such as, a) if global decision 1 is incorrect, then the original channel must be idle, and malicious sensor nodes selfishly occupy the channel by tampering with the sensing results, b) if global decision 0 is incorrect, then the original channel must be busy, and malicious sensor nodes must have interfered with the PU by tampering with the sensing results.

This data delivery mechanism can be observed by the FC to determine the reliability of the global decision in the current frame, and to measure the local sensing results without being affected by Byzantine attack. We label it as $G(k)$ and use it as a standard to measure the reliability of local sensing results. By comparing the local sensing results with $G(k)$, the result deviation at the k-th sensing can be given by

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2024 doi:10.20944/preprints202407.1194.v1

$$D_i(k) = \sqrt{\frac{(L_i(k) - G(k))^2}{N}} \tag{14}$$

Further, the average value of the sensing result deviation is

$$\bar{D}_\iota(k) = \frac{1}{N}\sum_{i=1}^{N} D_i(k) \tag{15}$$

where $e_i(k)$ represents the positive and negative evaluation of the sensing results obtained by the i-th sensor. If $\bar{D}_\iota(k) \geq D_i(k)$, it indicates that the local sensing results of the i-th sensor at the k-th sensing are reliable, and a positive evaluation $e_i(k) = 1$ is assigned to the i-th sensor. Conversely, if the local sensing result is deemed unreliable, it is assigned a negative evaluation $e_i(k) = 0$.

Considering the storage capacity of the FC, we assume that the historical evaluation values of the sensor is L, which means the FC retains the evaluation values derived from L instances of sensing results. Thus, the positive total evaluation $p_i(k)$ and negative total evaluation $n_i(k)$ of the i-th sensor at the k-th sensing are computed as

$$p_i(k) = \begin{cases} \sum_{j=1}^{L} e_i(k)\left(w_i(k)\right)^{L-n}, & if\ k < L \\ \sum_{j=k-L+1}^{L} e_i(k)\left(w_i(k)\right)^{L-n}, & otherwise \end{cases} \tag{16}$$

and

$$n_i(k) = \begin{cases} \sum_{j=1}^{L} (1 - e_i(k))\left(w_i(k)\right)^{L-n}, & if\ k < L \\ \sum_{j=k-L+1}^{L} (1 - e_i(k))\left(w_i(k)\right)^{L-n}, & otherwise \end{cases} \tag{17}$$

respectively.

The total evaluation is then incorporated into the beta reputation system. Specifically, for the i-th sensor during the k-th sensing, the accumulated evaluation values are considered. The reputation parameters $r_i(k)$ and $s_i(k)$ are expressed as

$$r_i(k) = p_i(k) + \phi_r \tag{18}$$

$$s_i(k) = n_i(k) * \phi_s \tag{19}$$

where ϕ_r and ϕ_s represent tuning parameters that reflect linear and multiplier growth of different types of sensing results, respectively.

Finally, the reputation value/weight of the i-th sensor after the k-th sensing can be expressed as

$$T_i(k+1) = w_i(k+1) = \frac{p_i(k) + \phi_r + 1}{p_i(k) + n_i(k) * \phi_s + \phi_r + 2} \tag{20}$$

To be specific, the higher the reputation value of the sensor, the higher sensing result will be prioritized in the likelihood ratio at the next sensing, thereby further improving the efficiency of collaboration. The whole process of BDF is illustrated in Figure 3.

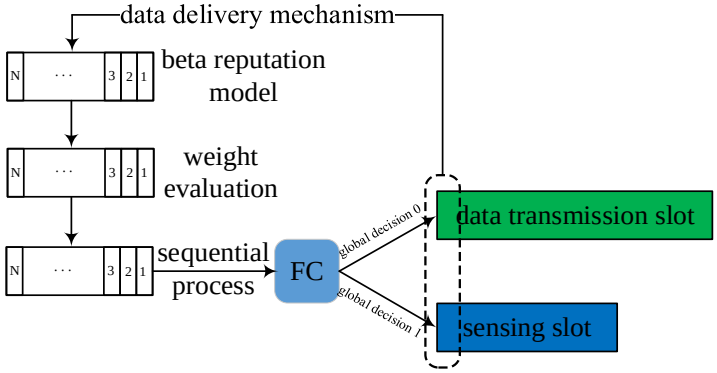

Figure 3. The flowchart of BDF.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2024 doi:10.20944/preprints202407.1194.v1

4. Simulation Results

In this section, simulation results are presented to demonstrate the effectiveness of the proposed BDF by comparing to SPRT and WSPRT in terms of the error probability Q_e, and the average number of samples N_{ave}. In a sensing observation period (2000 sensing frames), the attack probability α varies from 0 to 1 at an interval of 0.02, and the attack probability $\rho = [0.1, 0.2, 0,3]$ and $\rho = [0.7, 0.8, 0,9]$ are presented to characterize the small/large-scale attack, respectively. The values for other simulation parameters are set as follows. The number of sensors N participating in CSS is 100. Regardless of whether the sensor nodes are malicious or normal, their local detection probability P_d and local false alarm probability P_f are both 0.7 and 0.3, respectively. Assuming that the probability $P(\mathcal{H}_0)$ of the PU's status $\mathcal{H}_0$ is 0.1 and the probability $P(\mathcal{H}_1)$ of the PU's status $\mathcal{H}_1$ is 0.9. In addition, in the sequential process, the tolerated miss detection probability $\bar{P}_m$ and the tolerated false alarm probability $\bar{P}_f$ are set to be 10^{-3} and 10^{-4}, respectively. The reputation threshold g of WSPRT is 5.

4.1. Always Attack

The always attack is a common attack strategy that is often considered in many Byzantine identification and suppression algorithms. Therefore, we consider the error probability and average number of samples in the context of this attack strategy. The attack ratio ρ varies from 0 to 0.8 at an interval of 0.02.

As illustrated in Figure 4, when those malicious sensor nodes launch always attack, the error probability of SPRT starts to shake when the attack probability is 0.3, and increases to 1 when the attack probability exceeds 0.5. At the same time, the error probability of WSPRT performs very well before the attack ratio reaches 0.5, but once ρ exceeds 0.5, it also shakes up to 1 and remains stable. In contrast, the proposed BDF has consistently maintained very accurate PU detection. The above results strongly confirm that both SPRT and WSPRT are negatively affected by the blind problem to varying degrees.

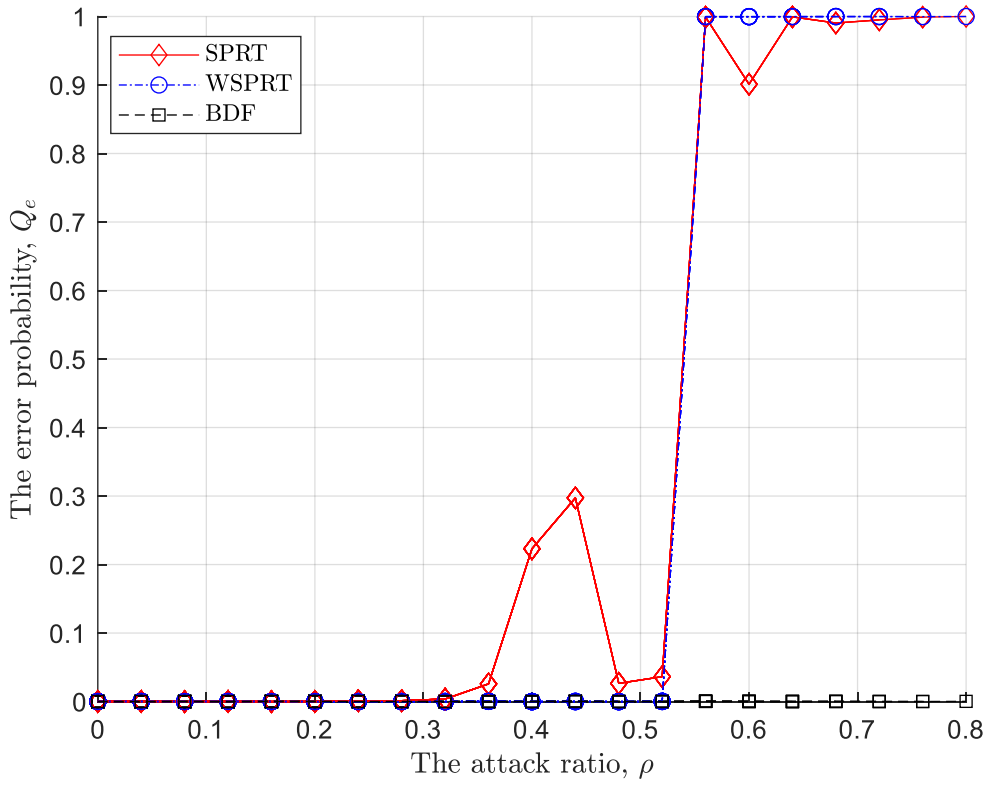

Figure 4. The error probability in the context of always attack.

 doi:10.20944/preprints202407.1194.v1

Following the error probability in the context of always attack, the average number of samples is presented in Figure 5. It can be seen from Figure 5 that when the attack probability is low, because of the sequential idea, all three fusion rules only require a small number of samples to accurately detect the PU. However, as the attack probability increases, the FC of SPRT and WSPRT begins to require more samples to make a global decision (although the global decision is not accurate at this time), and the required number of samples increases first and then decreases (constantly shaking during the process), because of the randomness of the sequential process (samples may come from malicious or normal sensor nodes) and the unreliability of global decision. At last, since the FC is distorted, the performance has significantly degraded, and the number of samples does not need to be greater. In contrast, the sample size of BDF remained unchanged at around 5.

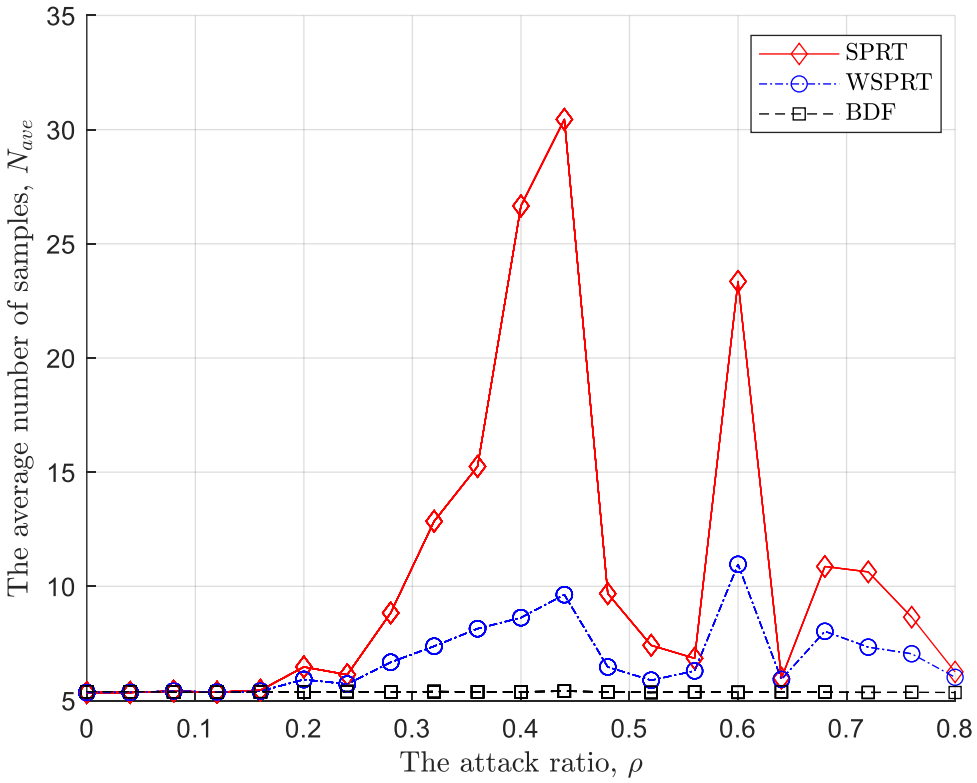

Figure 5. The average number of samples in the context of always attack.

Although always attack is a common attack strategy and many algorithms have paid attention to it, they only consider situations with lower attack ratios, so always attack is also easy to be identified and suppressed. Here, we not only consider always attack, but also various attack ratios. However, from the above simulation results, our proposed BDF exhibits excellent performance in both the error probability and sample size during the sequential process due to considering data delivery mechanism and adapting corresponding weight evaluation.

4.2. The Error Probability

In order to get an insight into small/large-attack's influence on the error probability, we compare the error probabilities of SPRT, WSPRT, and BDF under various attack probabilities in the context of small/large-attack.

4.2.1. Small-Scale Attack

As shown in Figure 6, regardless of the attack probability adopted by malicious sensor nodes, SPRT, WSPRT, and BDF in the context of small-scale attack can basically achieve 100% detection

 doi:10.20944/preprints202407.1194.v1

accuracy for the PU signal because even SPRT has a certain level of Byzantine fault tolerance. From this, it can be seen that under small-scale attack, even always attack cannot make the FC blind (Byzantine attack makes the global decision of the FC not more accurate than random guesses). It should be noted that since SPRT does not have any defense capabilities to resist Byzantine attack, once the attack ratio gradually increases, i.e., when $\rho = [0.2, 0{,}3]$, the error probability will also increase to some extent.

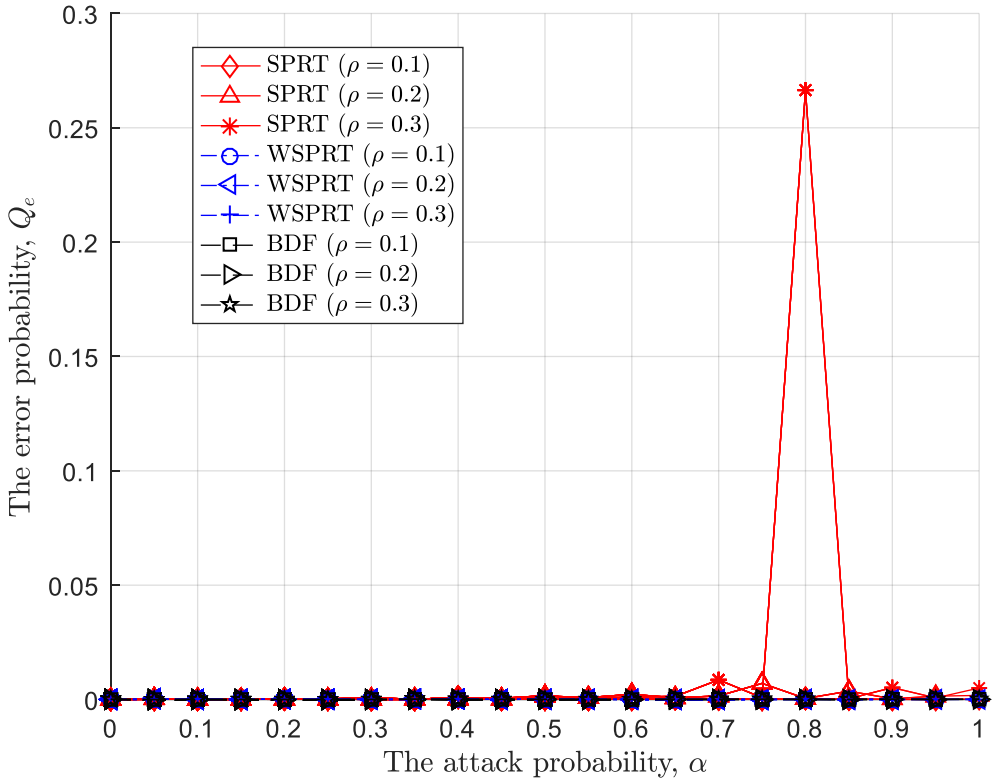

Figure 6. The error probability vs the attack probability in the context of small-scale attack.

4.2.2. Large-Scale Attack

Different from small-scale attack, the negative impact of large-scale attack on the error probabilities of SPRT, WSPRT, and BDF is more significant. As illustrated in Figure 7, the error probabilities of SPRT, WSPRT, and BDF keep zero when the attack probability is less than 0.2. But as the attack probability further increases, three methods exhibit different variations in the error probability. In details, the error probability of SPRT fluctuates upwards, and the larger the attack ratio, the higher the error probability until it stabilizes. Moreover, WSPRT suppresses Byzantine attack to a certain extent through the weight of likelihood ratio based on SPRT, presenting the following differences: 1) the performance of WSPRT deteriorates slower than that of SPRT under the same attack strategy before the FC is blind; 2) once the FC is blind, the error probability jitter of WSPRT is more severe than that of SPRT; 3) The attack probability further increases, and the error probability of WSPRT is also higher than that of SPRT. This is because the ratio and probability of attack gradually increase, making the global decision of the FC unreliable. WSPRT relies on the global decision to measure the reliability of the local sensing result and design weight, resulting in unstable performance once the global decision is incorrect, coupled with the random calculation of likelihood ratio, and ultimately worse performance (normal sensor nodes are considered malicious, and vice versa).

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2024 doi:10.20944/preprints202407.1194.v1

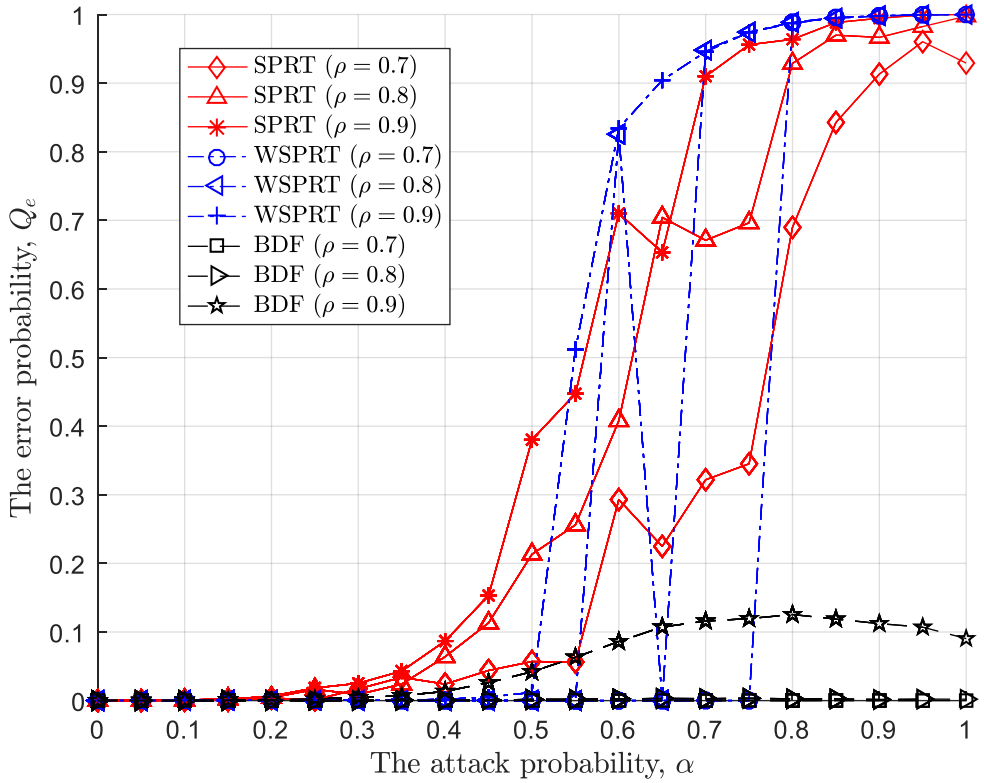

Figure 7. The error probability vs the attack probability in the context of large-scale attack.

In contrast to SPRT and WSPRT, BDF shows significant performance at $\rho = [0.7, 0{,}8]$, indicating that the beta reputation model can accurately identify malicious sensor nodes. That is to say, the reputation value is accurately evaluated and not affected by the accuracy of the global decision. Based on this, the positive and negative total weight evaluation accurately amplify and reduce the positive and negative impact on the global decision-making of the FC, respectively. Further, when $\rho = 0.9$, the error probability of BDF increases (first increases and then decreases), which also indicates that always attack is relatively easy to overcome, but overall, its error probability is still not higher than 0.12.

4.3. The Average Number of Samples

The cooperative performance of SPRT, WSPRT, and BDF is presented by means of the error probability in the context of small/large-attack, the next thing comes into consideration is to evaluate the cooperative efficiency by means of the average number of samples.

4.3.1. Small-Scale Attack

In the context of small-attack, the average number of samples of SPRT, WSPRT, and BDF are simulated in Figure 8. Since in the case of $\rho = [0.1, 0.2, 0{,}3]$, no matter what attack probability the malicious sensor node adopts, it cannot make the FC blind. However, due to the malicious sensor node tampering with the sensing result, the sequential process of SPRT and WSPRT randomly calculates the likelihood ratio, so the required number of samples is also random and less likely to make the decision variable Λ_n satisfy the upper and lower threshold conditions. Moreover, as the attack probability increases, the fluctuation of the average sample size also increases.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2024 doi:10.20944/preprints202407.1194.v1

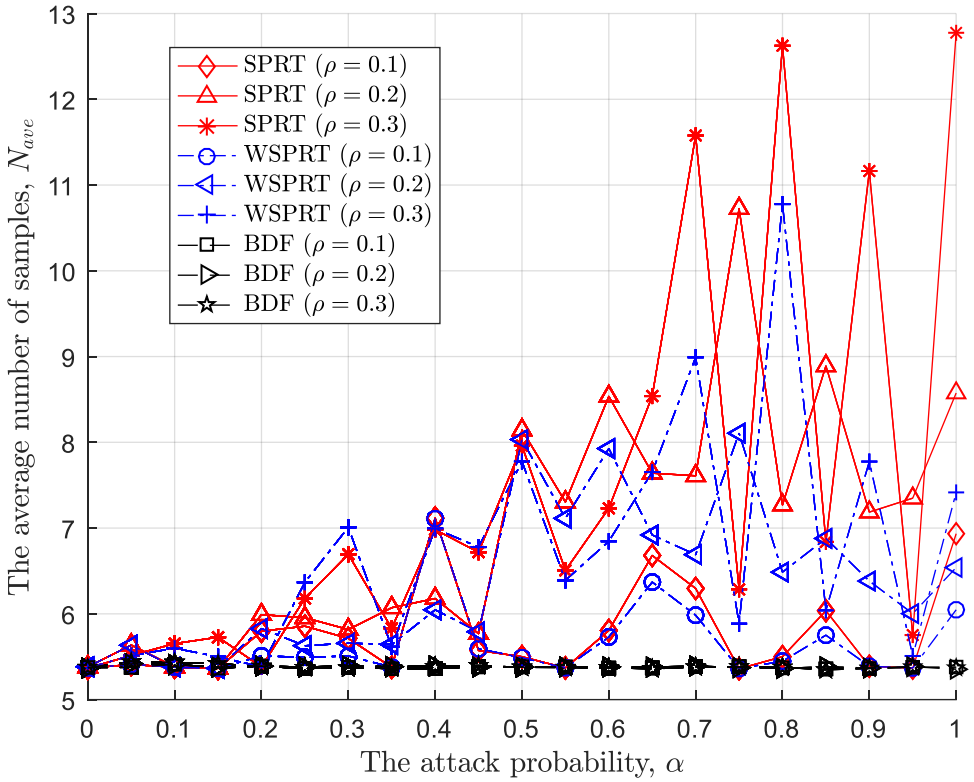

Figure 8. The average number of samples vs the attack probability in the context of small-scale attack.

Unlike SPRT and WSPRT, the number of samples required for BDF always does not exceed 5.5. On the one hand, BDF accurately identifies malicious sensor nodes through data delivery mechanism, and on the other hand, the beta reputation model enables the FC to rely on normal sensor nodes to the greatest extent possible while suppressing malicious sensor nodes. In addition, BDF can prioritize the sensing results of sensors with high credibility, enabling the FC to complete global decision quickly and accurately.

4.3.2. Large-Scale Attack

The sample size under large-scale attack appears to be more regular, as at a certain attack probability, Byzantine attack may make the FC blind, as shown in Figure 9. Firstly, the sample size of the three methods basically increases and then decreases with the increase of attack probability, except that WSPRT has the largest amplitude. Undoubtedly, the increase in attack probability may make the global decision less reliable, but the weight of WSPRT makes the global decision more unreliable and random. In order to ensure that the decision variable meet the upper and lower thresholds in the sequential process, the FC has to require more sample sizes. Once the FC is blind, it indicates that the global decision is completely unreliable, and the FC only needs a small number of samples to make an incorrect global decision.

 doi:10.20944/preprints202407.1194.v1

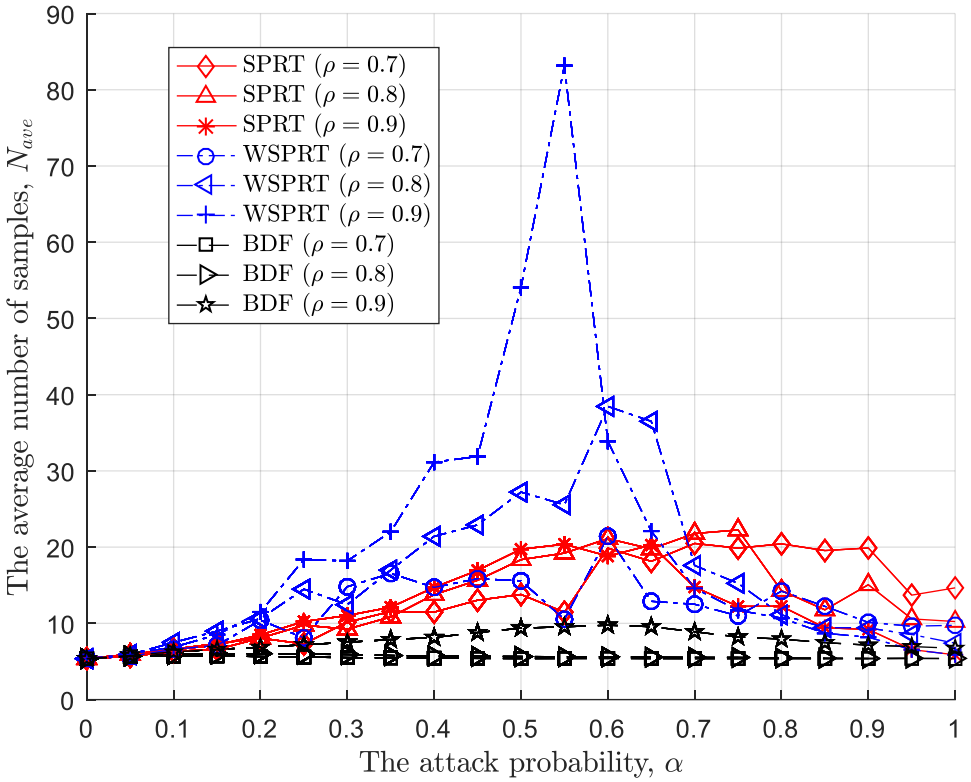

Figure 9. The average number of samples vs the attack probability in the context of large-scale attack.

5. Conclusion and Future Work

In this paper, we make an investigation on Byzantine attack for CSS in CWSNs. To mitigate the negative impact of Byzantine attack on CSS, we propose BDF which includes sequential process, beta reputation model, and weight evaluation. In BDF, we are motivated by SPRT to integrate the beta reputation function into a weight of weight sequential process and sequentially calculate the likelihood ratio in a reputation descending order. Finally, in contrast to SPRT and WSPRT, a series of numerical simulation results demonstrate the correctness and effectiveness of the proposed BDF regarding the error probability and the average number of samples under small/large-attack and attack probabilities.

In the future, there are still many interesting questions that remain to be explored such as Byzantine attack strategy based on soft combining. Additionally, the sequential idea may be further extended to machine learning methods to ensure the accuracy, security, and efficiency of CSS.

Author Contributions: Conceptualization, J.W.; methodology, J.W.; software, J.W.; validation, J.W.; formal analysis, J.W.; investigation, J.W.; resources, J.W.; data curation, J.W.; writing—original draft preparation, J.W.; writing—review and editing, J.W. and R.Z.; visualization, J.W.; supervision, J.W.; project administration, J.W., and T.L.; funding acquisition, J.W., and T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China under Grant No. 62201186 and 62301200, and Zhejiang Provincial Natural Science Foundation of China under Grant No. LQ22F010004.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yu, H.; Zikria, Y.B. Cognitive Radio Networks for Internet of Things and Wireless Sensor Networks. Sensors 2020, 20, 5288.
2. Vijay, G.; Bdira, E. B. A.; Ibnkahla,M. Cognition in wireless sensor networks: A perspective. IEEE Sensors Journal 2011, 11, 582-592.
3. Araujo, A.; Blesa, J.; Romero, E.; Villanueva, D. Security in cognitive wireless sensor networks. Challenges and open problems. EURASIP Journal on Wireless Communications and Networking 2012, 2012, 1-8.
4. Gan, J.; Wu, J.; Zhang, J.; Chen, Z.; Chen, Z. Throughput and interference for cooperative spectrum sensing: A malicious perspective. KSII Transactions on Internet & Information Systems 2021, 15, 4224-4243.
5. Liu, M.; Xu, D.; Huo, Z. M.; Sun, Z. X. Research on spectrum sensing data falsification attack detection algorithm in cognitive Internet of Things. Telecommunication Systems 2022, 80, 227-338.
6. Zhang, L.; Ding, G.; Wu, Q.; Zou, Y.; Han, Z.; Wang, J. Byzantine attack and defense in cognitive radio networks: A survey. IEEE Communications Surveys & Tutorials 2015, 17, 1342-1363.
7. Wu, J.; Song, T.; Yu, Y.; Wang, C.; Hu, J. Generalized Byzantine attack and defense in cooperative spectrum sensing for cognitive radio networks. IEEE Access 2018, 6, 53272-53286.
8. Wu, J.; Li, P.; Chen, Y.; Tang, J.; Wei, C.; Xia, L.; Song, T. Analysis of Byzantine attack strategy for cooperative spectrum sensing. IEEE Communications Letters 2020 , 24, 1631-1635.
9. Zeng, K.; Pawelczak, P.; Cabric, D. Reputation-based cooperative spectrum sensing with trusted nodes assistance. IEEE Communications Letters 2010, 14, 226-228.
10. Luo, X. Secure Cooperative Spectrum Sensing Strategy Based on Reputation Mechanism for Cognitive Wireless Sensor Networks. IEEE Access 2020, 8, 131361-131369.
11. Chen, R.; Park, J. M. J.; Bian, K. Robustness against Byzantine failures in distributed spectrum sensing. Computer Communications 2012, 35, 2115-2124.
12. Sun, Z.; Xu, Z.; Hammad, M. Z.; Ning, X.; Wang, Q.; Guo, L. Defending against massive SSDF attacks from a novel perspective of honest secondary users. IEEE Communications Letters 2019, 23, 1696-1699.
13. Xu, Z.; Sun, Z.; Guo, L.; Muhammad, Z. H.; Chintha, T. Joint spectrum sensing and spectrum access for defending massive SSDF attacks: A novel defense framework. Chinese Journal of Electronics 2022, 31, 240-254.
14. Lin, R.; Li, F.; Wang, J.; Hu, J.; Zhang, Z.; Wu, L. A blockchain-based method to defend against massive SSDF attacks in cognitive internet of vehicles. IEEE Transactions on Vehicular Technology 2024, 73, 6954-6967.
15. Fu, Y.; He, Z. Massive SSDF attackers identification in cognitive radio networks by using consistent property. IEEE Transactions on Vehicular Technology2023, 72, 11058-11062.
16. Li, Z.; Mo, Y.; Hao, F. Distributed sequential hypothesis testing with Byzantine sensors. IEEE Transactions on Signal Processing 2021, 69, 3044-3058.
17. Wan, F.; Ma, T.; Hua, Y.; Liao, B.; Qing, X. Secure distributed estimation under Byzantine attack and manipulation attack. Engineering Applications of Artificial Intelligence 2022, 116, 105384.
18. Chen, Q.; Bulusu, S.; Geng, B.; Varshney, P. K. Ordered transmission-based detection in distributed networks in the presence of Byzantines. arxiv preprint arxiv:2201.08737, 2022.
19. Chen, Q.; Geng, B.; Han, Y. S.; Varshney, P. K. Enhanced audit bit based distributed Bayesian detection in the presence of strategic attacks. IEEE Transactions on Signal and Information Processing over Networks 2022, 8, 49-62.
20. Chen, Q.; Han, Y. S.; Geng, B.; Varshney, P. K. Reputation and audit bit based distributed detection in the presence of Byzantines. 2022 56th Asilomar Conference on Signals, Systems, and Computers 2022, 548-552.
21. Yao, D.; Yuan, S.; Lv, Z.; Wan, D.; Mao, W. An enhanced cooperative Spectrum sensing scheme against SSDF attack based on Dempster-Shafer evidence theory for cognitive wireless sensor networks. IEEE Access 2020, 8, 175881-175890.
22. Ridouani, M.; Benazzouza, S.; Salahdine, F.; Hayar, A. A novel secure cooperative cognitive radio network based on Chebyshev map. Digital Signal Processing 2022, 126, 103482.
23. Chouhan, A.; Captain, K.; Parmar, A.; Kumar, R. Single decision reporting for cooperative spectrum sensing under erroneous feedback channels with Byzantine attack. Physical Communication 2022, 55, 101891.
24. Chouhan, A.; Parmar, A.; Captain, K.; López-Benítez, M. Defending against Byzantine attacks in CRNs: PCA-based malicious user detection and weighted cooperative spectrum sensing. IEEE Wireless Communications Letters 2024, 13, 1488-1492.

 doi:10.20944/preprints202407.1194.v1

25. Chen, L.; Shen, X.; Zhao, X.; Wang, Z.; He, W.; Xu, G.; Chen, Y. Defending dominant cooperative probabilistic attack in CRNs by JS-divergence-based improved reputation algorithm. Pervasive and Mobile Computing 2024, 101, 101921.
26. Parmar, A.; Shah, K.; Captain, K. M.; López-Benítez, M.; Patel, J. R. Gaussian mixture model-based anomaly detection for defense against Byzantine attack in cooperative spectrum sensing. IEEE Transactions on Cognitive Communications and Networking 2024, 10, 499-509.
27. Parras, J.; Zazo, S. Using one class SVM to counter intelligent attacks against an SPRT defense mechanism. Ad Hoc Networks 2019, 94, 694-706.
28. Sarmah, R.; Taggu, A.; Marchang, N. Detecting Byzantine attack in cognitive radio networks using machine learning. Wireless Networks 2020, 26, 5939-5950.
29. Taggu, A.; Marchang, N. Detecting Byzantine attacks in cognitive radio networks: A two-layered approach using Hidden Markov model and machine learning. Pervasive and Mobile Computing 2021, 77, 101461.
30. Luo, Z.; Zhao, S.; Lu, Z.; Xu, J.; Sagduyu, Y. E. When attackers meet AI: Learning-empowered attacks in cooperative spectrum sensing. IEEE Transactions on Mobile Computing 2022, 21, 1892-1908.
31. Zhang, Z.; Wu, J.; Gan, J.; Chen, Z.; Shen, J. Support vector Machine process against probabilistic Byzantine attack for cooperative spectrum sensing in CRNs. Proceedings of the 2023 8th International Conference on Machine Learning Technologies 2023, 269-276.
32. Liang, Y.; Zeng, Y.; Peh, E.C.Y.; Hoang, A.T. Sensing-throughput tradeoff for cognitive radio networks. IEEE Transactions on Wireless Communications 2008, 7, 1326-1337.