Secure and Efficient Cooperative Spectrum Sensing Against Byzantine Attack for Interweave Cognitive Radio System

Jun Wu[1,2,3,4*], Ze Chen[1], Jianrong Bao[1,2], Jipeng Gan[1], Zehao Chen[1], and Jia Zhang[1]
[1] School of Communication Engineering, Hangzhou Dianzi University
Hangzhou, Zhejiang 310000 China
[2]National Mobile Communications Research Laboratory, Southeast University
Nanjing, Jiangsu 211189 China
[3] Artificial Intelligence Key Laboratory of Sichuan Province, Sichuan University of Science and Engineering
Yibin, Sichuan 643002 China
[4] College of Information Science and Electronic Engineering, Zhejiang University
Hangzhou, Zhejiang 310000 China
[e-mail: wojames2011@163.com]
[*]Corresponding author: Jun Wu

Received January 19, 2022; revised May 12, 2022; revised August 1, 2022; revised September 12, 2022; accepted October 26, 2022; published November 30, 2022

Abstract

Due to increasing spectrum demand for new wireless devices applications, cooperative spectrum sensing (CSS) paradigm is the most promising solution to alleviate the spectrum shortage problem. However, in the interweave cognitive radio (CR) system, the inherent nature of CSS opens a hole to Byzantine attack, thereby resulting in a significant drop of the CSS security and efficiency. In view of this, a weighted differential sequential single symbol (WD3S) algorithm based on MATLAB platform is developed to accurately identify malicious users (MUs) and benefit useful sensing information from their malicious reports in this paper. In order to achieve this, a dynamic Byzantine attack model is proposed to describe malicious behaviors for MUs in an interweave CR system. On the basis of this, a method of data transmission consistency verification is formulated to evaluate the global decision's correctness and update the trust value (TrV) of secondary users (SUs), thereby accurately identifying MUs. Then, we innovatively reuse malicious sensing information from MUs by the weight allocation scheme. In addition, considering a high spectrum usage of primary network, a sequential and differential reporting way based on a single symbol is also proposed in the process of the sensing information submission. Finally, under various Byzantine attack

This work is supported by the National Natural Science Foundation of China under Grant No. 62201186, Zhejiang Provincial National Natural Science Foundation of Zhejiang Province under Grant No. LQ22F010013, Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (No. 2022D16), Open Fund Project of Sichuan Provincial Key Laboratory of Artificial Intelligence (No. 2021RYJ07), Fundamental Research Funds for the Provincial Universities of Zhejiang (No. GK209907299001-023 and GK209907299001-003), and National Natural Science Foundation of China under Grant No. U1809201.

types, we provide in-depth simulations to demonstrate the efficiency and security of the proposed WD3S.

Keywords: Byzantine attack, cooperative spectrum sensing, security and efficiency, trust value, sequential and differential.

1. Introduction

Because of the rapid advances in wireless communication, there has been an increasing demand for the new wireless devices and applications in the electromagnetic spectrum. However, this increasing demand faces a great barrier which is the limitation of radio resources. According to the federal communications commission, underutilization of the frequency spectrum by primary users (PUs) either temporally or spatially is the main reason of the spectrum scarcity problem. To meet the growing need for spectrum availability, cognitive radio (CR) technology has been extensively proposed as the most promising solutions.

In an interweave CR system, secondary users (SUs) make use of the local spectrum sensing (LSS) technology to opportunistically access the spectrum band allocated to the PU without causing excessive interference to the PU's normal communication, thus solving the problem of spectrum scarcity [1]. In light of the fact that the accuracy of single-user spectrum sensing is always inadequate, cooperative spectrum sensing (CSS) paradigm is proposed to mitigate the negative effect of channel shadowing and fading [2]. In the collaborative framework, the fusion center (FC) gathers sensing information from SUs and then makes a global decision about the PU status based on a specific data fusion rule.

However, the CSS paradigm opens a hole to malicious users (MUs) launching Byzantine attack. Through Byzantine attack, MUs send the falsified sensing information to mislead the FC into making an error global decision about the PU status and severely deteriorate the CR system's performance. Therefore, devising a secure and efficient algorithm for CSS to protect the CR system from Byzantine attack becomes essential.

1.1 Related Work

Recently, prospective investigation addressing emerging and future challenges for secure and efficient CSS algorithm also has become a heated area of research. Y. Shei et al. applied sequential probability ratio test (SPRT) in [3] to optimize the reporting channel bandwidth and total sensing time in CSS. R. Chen et al. formulated a weighted sequential probability ratio test (WSPRT), in which the idea of the weight allocation was introduced in [4]. J. Wu et al. introduced a CSS for sequential 0/1 which is low-complexity under Byzantine attack and ensured the correctness of the global decision through the monitoring process of data transmission in [5]. Using the Kolmogorov-Smirnov test under the uncertainty of the channel and non-Gaussian noise, G. Zhang et al. proposed a method for fast, robust spectrum sensing in the CR system [6]. On the basis of SPRT, K. Haghighi et al. analyzed the exact spectrum sensing performance of time varying threshold sequential detectors in [7]. To improve the performance of CR receivers operating at low signal-to-noise ratio (SNR), H. Hsieh et al.

proposed a sequential test detector based on higher-order statistics for detecting underutilized spectrum in [8]. In [9], S. Mapunya and M. Velempini proposed an extreme studentized consensus CSS to combat the negative effect of greedy attacker. In [10], Y. Yilmaz et al. proposed a new framework for CSS in asynchronous states based on non-uniform sample and SPRT. These works basically take greedy attacker into account. In fact, from a safety point of view, the MU may conduct out various Byzantine attack behaviors according to the CSS paradigm.

In another work, a suprathreshold stochastic resonance method was proposed to detect weak PU signals by artificially attaching noise resonance leading to signal enhancement by Q. Li and Z. Li in [11]. N. Marchang et al. proposed an intrusion detection scheme based on Markov chain model in [12]-[14]. [15] improved the performance of CSS in the case of low generalized SNR by using the maximum generalized correntropy. In [16], H. Chen suggested an attack-proof CSS system using M-ary quantized data. After learning the approach of combining each single sensing result from the SU using a convolutional neural network and taking into account both the spectrum and spatial correlation of each sensing result, W. Lee et al. and colleagues employed training sensing samples to enhance the CSS performance in [17]. Using blockchain technology, Q. Wang et al. introduced a secure, decentralized, and novel multiparty learning system in [18]. P. Zhang et al. in [19] recast the CSS location estimation issue as a stochastic censoring model and developed the maximum likelihood estimate for the node's position. L. Zhang established a robust defense framework in [20], in which a reference is built on the basis of extended sensing. Though the above-mentioned state-of-the-art CSS schemes study complex Byzantine attack behaviors, most of them ignore the CSS efficiency.

Different from the aforementioned works, K. Zeng introduced a reputation-based framework to identify misbehaviors in [21]. A trust value (TrV) based CSS algorithm for mobile SUs is proposed by X. Wang in [22], in which provides larger weighting coefficients for cells with preferable channel conditions. Both autonomous and distributed decision making are considered in [23], J. Wang and I. Chen separated the false sensing reports resulting from defective sensing capabilities from those caused by Byzantine attack, avoiding false penalties for honest users (HUs). J. Wu et al. in [24] proposed a novel CSS scheme in which the SU's TrV is updated after each sensing based on the delivery-based assessment, solving the FC's unreliability. In [25], a novel empirical analysis under a probabilistic Byzantine attack was performed by A. Sivakumaran et al., where a decentralized CR network is simulated using the Neyman-Pearson (N-P) algorithm for CSS. Apparently, the above CSS schemes design a TrV update mechanism to allocate weight of SUs' sensing results and restricts SUs who are considered to be malicious from participating in CSS, thereby directly eliminating them from the network. However, the FC may utilize the sensing data from those rational MUs to make a more accurate global decision. Otherwise, J. Wang et al. proposed a lightweight blockchain-based secure routing algorithm for swarm unmanned aircraft system networking in [26], and formulated a blockchain-based approach to mitigate the threats from accessing the malicious base stations in [27]. Further, the authors provided a holistic framework for the quickest and sequential detection of abnormalities and time-dependent abnormal events in internet of things in [28]. But these works focus more on the efficiency and security of decentralized routing algorithm or abnormal detection in unmanned aircraft system networks or internet of things.

In view of above reviews, [12]-[15] ignore the blind scenario of FC when the proportion of MUs increases to a certain extent, [16]-[18] do not exploit MUs' reports to improve CSS performance, [19]-[21] do not use novel reporting way to reduce communication overhead, [22]-[23] do not propose the dynamic Byzantine attack model, so the requirement naturally remains a big challenge to present an efficient and secure CSS, especially in the face of a

dynamic Byzantine attack. Therefore, we will focus more on improving the efficiency and security of the CSS model at the same time, using data transmission consistency verification, weight allocation and novel reporting way to improve the performance of CSS.

1.2 Our Contributions

This paper survey a series of studies on the efficiency and performance of CSS under Byzantine attack. Following these works, we formulate a dynamic Byzantine attack model from a malicious viewpoint, and on the basis of this, we also propose a secure and efficient weighted differential sequential single symbol (WD3S) and further evaluate the cooperative performance and efficiency for a series of data fusion technologies for CSS. We summarize our contributions as five-fold:

(a) From the MU's viewpoint, we propose a dynamic Byzantine attack model to exactly describe Byzantine behaviors in an interweave CR system. In the proposed attack model, the MU flexibly develops out various attack strategies from a series of generalized attack mode;

(b) Considering that the FC's global decision may be compromised by a large number of MUs, we use the data transmission status to update each SU's TrV in the spectrum sensing frame instead of the global decision;

(c) Following the data transmission consistency verification, we separate the sensing information useful from the sensing results of MUs so as to make a more accurate global decision. In addition, honest users (HUs) may also be mistaken for MUs. Therefore, unlike previous works, MUs are not directly removed from the system;

(d) To improve the reporting efficiency, we integrate the differential and sequential idea into the reporting channel to reduce the samples the FC required and improve cooperative efficiency; Further, we also perform an in-depth analysis on the cooperative performance and efficiency of the proposed WD3S and classical data fusion technologies.

1.3 Organization

The rest of this paper is organized as follows. Section 2 proposes the spectrum sensing and Byzantine attack model in an interweave CR system. In Section 3, some classical the state-of-art technologies and recent advances in data fusion for CSS are reviewed. Further, motivated by disadvantages of the existing data fusion technologies, WD3S is proposed. In Section 4, the performance and efficiency of WS3S are conducted an in-depth analysis. The simulation results of the performance and efficiency comparison are shown in Section 5. Section 6 is the conclusion of this paper.

2. System Model

In this section, an energy detection-based spectrum sensing model in an interweave CR system is introduced. Following the spectrum sensing model, we combine malicious behaviors from MUs into CSS to conduct a dynamic Byzantine attack model.

2.1 Spectrum Sensing Model

We assume that a centralized interweave CR system consists of a PU, a FC and N SUs (including HUs and MUs, and the MU ratio is ρ). The considered CSS model is shown in **Fig. 1**. It is known that each frame consists of a sensing slot, a reporting slot, and a data transmission slot in an interweave CR system. At the sensing slot, each SU individually detects the PU signal by means of LSS technology. Among these LSS techniques (i.e.,

energy detection, wavelet detection, cyclostationary feature detection, and matched filter detection etc.), we adopt the energy detection to detect the PU because there is no a priori knowledge about the primary signal and a low implementation cost. Therefore, following energy detection, the spectrum sensing is regarded as a binary hypothesis test problem, i.e., H_0 and H_1 represent the hypothesis on the absence and presence of the PU signal, respectively. Assuming that $s_i(t)$ and $u_i(t)$ are denoted by the PU's signal and additive white gaussian noise (AWGN) at the i-th SU, respectively, the signal received by the i-th SU can be expressed as [29]

$$y_i(t) = \begin{cases} u_i(t), & H_0 \\ s_i(t) + u_i(t), & H_1 \end{cases} \tag{1}$$

According to (1), at the k-th sensing frame, the test statistic at the energy detector is given by

$$E_i(k) = \sum_{t=1}^{S} |y_i(t)|^2 \tag{2}$$

where S is the sampling number. For a large S, using the central limit theorem, the probability density function of the test statistic $E_i(k)$ can be approximated by Gaussian distribution as

$$E_i(k) \sim \begin{cases} \mathcal{N}(S\sigma_u^2, 2S\sigma_u^4), & H_0 \\ \mathcal{N}(S(\gamma+1)\sigma_u^2, 2S(\gamma+1)^2\sigma_u^4), & H_1 \end{cases} \tag{3}$$

where σ_s^2 and σ_u^2 are signal variance and noise variance, $\gamma = \sigma_s^2/\sigma_u^2$ is SNR of the PU signal received at the i-th SU. Therefore, according to [30], the local spectrum sensing performance of the i-th SU, i.e., the false alarm probability and the detection probability which can be respectively given by

$$P_{f,i} = Q\left(\frac{\lambda - S\sigma_u^2}{\sqrt{2S\sigma_u^4}}\right) \tag{4}$$

$$P_{d,i} = Q\left(\frac{\lambda - S(\gamma+1)\sigma_u^2}{\sqrt{2S(\gamma+1)^2\sigma_u^4}}\right) \tag{5}$$

where $Q(\cdot)$ is the complementary distribution function of the standard Gaussian, and λ is the detection threshold. Otherwise, the miss detection probability $P_{m,i} = 1 - P_{d,i}$.

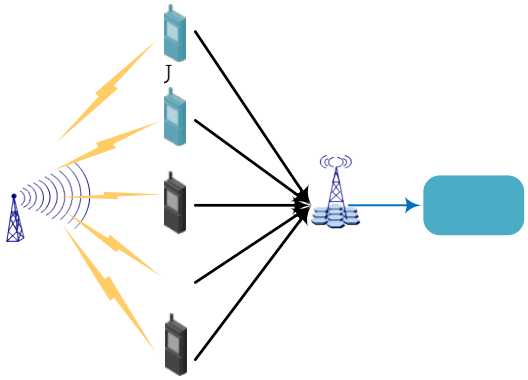


Fig. 1. The centralized interweaved-based CR system.

2.2 Dynamic Byzantine Attack Model

Due to the inherent nature (i.e., multipath fading and shadowing) of wireless channel, LSS performed by the individual SU is often in error, CSS has been proposed to exploit the multi-

user spatial diversity. However, the open nature of the underlying protocol stack of the CR system makes CSS suffer from Byzantine attack by MUs who can cause serious damage to the reliability of CSS by falsifying the sensing results.

Before delving into the intricacies of Byzantine attack, we introduce a specific type of attack, i.e., always attack. In an always attack, the MU always submits a falsified sensing result to the FC after LSS is implemented, i.e., always yes (AY), always no (AN), and always false (AF). That is to say, regardless of the sensing result, the MU always submits 1, 0 or the opposite result. The always attack model is commonly adopted by many Byzantine identification and suppression algorithms, but prone to be identified and removed from CR system. Apparently, a more covert and safe attack model is in line with the intentions of MUs. Motivated by this, we design a probabilistic attack instead of always attack to model a dynamic Byzantine attack.

Depending on the cooperative sensing framework, each SU makes a binary decision about the PU status at the sensing slot, i.e., H_0 or H_1, and further submits H_0 or H_1 to the FC at the error-free reporting slot. However, the MU may falsify the sensing result and submits it to the FC. For example, the MU falsifies the sensing result $S_i = H_0$ into the reporting result $R_i = H_1$ with a probability $\alpha_{0,i}$ or falsifies the sensing result $S_i = H_1$ into $R_i = H_0$ with a probability $\alpha_{1,i}$, as shown in **Fig. 2.** A pair of attack probabilities can be expressed as

$$\begin{cases} \alpha_{0,i} = P(R_i = H_1 | S_i = H_0) \\ \alpha_{1,i} = P(R_i = H_0 | S_i = H_1) \end{cases} \tag{6}$$

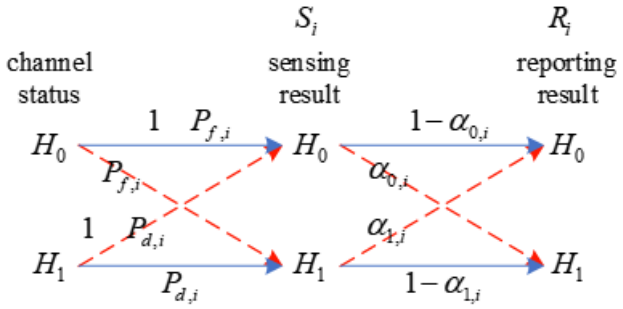


Fig. 2. Dynamic Byzantine attack model.

In the Bayesian testing framework, if the received data cannot convey any information about the hypothesis test to the FC, it is called blind. That is to say, the reporting results received by the FC and the hypothesis test are independent. Thus, the condition making the FC blind can be expressed as $P(\boldsymbol{R} \mid H_0) = P(\boldsymbol{R} \mid H_1)$, where $\boldsymbol{R} = [R_1, R_2, R_3 \ldots R_N]$ is the reporting vector received by the FC. Considering that each SU's sensing observation is subject to conditional independent and identically distribution. The false alarm probability and miss detection probability are assumed to be the same for every SU irrespective of whether they are reliable or not malicious, denoted by P_f and P_m, respectively. Each MU adopts the same attack probability, i.e., $\alpha_{0,i} = \alpha_0$ and $\alpha_{1,i} = \alpha_1$. Therefore, the blind condition of $P(\boldsymbol{R} \mid H_0) = P(\boldsymbol{R} \mid H_1)$ can be expressed as $\rho\left(\alpha_0\left(P_f + P_m - 1\right) + (1 - \alpha_1)\left(1 - P_f - P_m\right)\right) + (1 - \rho)\left(1 - P_f - P_m\right) = 0$. After simple algebraic operations, we have $\rho = 1/(\alpha + \beta)$ [5]. It can be seen that when $\alpha = \beta = 1$, the condition for making the FC blind is that the proportion of MUs to the total users reaches 0.5, which is the minimum proportion can blind the FC. Clearly, the small proportion of MUs and the always attack strategy allow many studies to circumvent the blind problem.

3. WD3S FOR CSS

Based on Byzantine attack and spectrum sensing model, we make a brief presentation of existing data fusion techniques, including hypothesis test, voting rule, and evolutionary variant. In view of a thorough review of advantages and disadvantages of these data fusion techniques, we propose a secure and efficient WD3S to defend against Byzantine attack, in which consists of data transmission consistency verification, weight allocation, and reporting way.

3.1 Data Fusion Technique

Considering the threat of Byzantine attack to the CR system, there are various data fusion techniques that have been proposed in existing works to suppress Byzantine attack and are also commonly categorized as hypothesis test and voting rule, and evolutionary variant [31].

3.1.1 Voting Rule

It is known that the voting rule (a.k.a. K-out-of-N rule or decision rule) is the simplest data fusion technique to make the global decision [32], in which if more than K SUs among N SUs decides that the PU is present, then the FC declares that the PU is present and vice versa. Additionally, the voting rule also involves three commonly used rules, i.e., And rule, Or-rule and Majority-rule, further we have the following descriptions.

(a) And rule: Only when all SUs decide that the PU is present, the FC finally determines that it is true, otherwise the PU is absence, that is, unless $\sum_{i=1}^{N} R_i = N$, the FC accepts H_1, otherwise accepts H_0. It is obvious that both of the detection probability and the false alarm probability for And rule are low.

(b) Or rule: If no less than one SU declares that the PU is present, the FC concludes that the PU is present, i.e., the FC accepts H_1 if $\sum_{i=1}^{N} R_i \geq 1$, otherwise accepts H_0. It is easily observed that the detection probability and the false alarm probability for Or rule are high.

(c) Majority rule: In addition to And and Or rule, Majority rule is the commonly adopted for the global decision making, in which the FC announces that the PU is present when more than half of SUs decide that the PU is present, the FC accepts H_1 when $\sum_{i=1}^{N} R_i \geq \lceil N/2 \rceil$.

Besides, the decision threshold K is usually used as a random variable in the voting rule to realize the performance optimization of CSS because the voting rule does not require some a-priori information about the probability distribution of primary signal or Byzantine.

3.1.2 Hypothesis Test

Unlike the simple voting rule, the implementation of hypothesis test requires a prior information, such as, the conditional densities $P(H_\vartheta|H_\theta)$ under the two hypotheses where $\vartheta, \theta = 0,1$, and a priori probabilities of the two hypotheses $P(H_\theta)$. Three classical hypothesis tests (i.e., Bayesian detection, N-P test, and SPRT [33]) are reviewed as follows:

(a) Bayesian detection: Bayesian detection assigns each of these possibilities to a specific cost and minimize the average cost, such as, $C_{\vartheta\theta}$ represents the cost of declaring H_ϑ when H_θ is true. The Bayes risk function or average cost C_{avg} is given by [33]

$$C_{avg} = \sum_{\vartheta=0}^{1} \sum_{\theta=0}^{1} C_{\vartheta\theta} P(R_i = H_\theta) P(H_\vartheta | H_\theta) \tag{7}$$

Then, Bayesian detection's likelihood ratio test (LRT) can be described as

$$\prod_{i=1}^{N} \frac{P(R_i|H_1)}{P(R_i|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \frac{P(H_0)(C_{10}-C_{00})}{P(H_1)(C_{01}-C_{11})} \tag{8}$$

where the right-hand side can be regarded as the threshold λ_{bayes} of Bayesian detection. If LRT is greater than λ_{bayes}, H_1 is accepted and vice versa.

(b) N-P test: To ensure that the false alarm probability is lower than an acceptable value of λ_{np} and maximize the detection probability, the N-P test's goal is to design a nonrandomized test. If LRT is greater than λ_{np}, H_1 is accepted and vice versa, then LRT of N-P test is described as

$$\prod_{i=1}^{N} \frac{P(R_i|H_1)}{P(R_i|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{np} \tag{9}$$

From (8) and (9), it can be seen that N-P test and Bayesian detection both use a fixed number of samples, but the difference of them is the way of the threshold selection [32].

(c) SPRT: Different from the methodology of N-P test and Bayesian detection, the sensing results are processed sequentially and then SPRT makes a global decision when the cooperative performance are satisfied. In the sequential process, the FC computes LRT after each sensing result as

$$W_l = \prod_{i=1}^{l} \frac{P(R_i|H_1)}{P(R_i|H_0)} \tag{10}$$

and compares it with a lower and upper threshold, where $\eta_l = \bar{P}_m/(1-\bar{P}_f)$ and $\eta_h = (1-\bar{P}_m)/\bar{P}_f$, $\bar{P}_m$ and $\bar{P}_f$ are the tolerated miss detection and false alarm probability, respectively. During the CSS process, the FC will make a global decision or take another sensing result, such as (a) $W_l \leq \eta_l$, the FC accepts H_0; (b) $W_l \geq \eta_h$, the FC accepts H_1; (c) $\eta_l < W_l < \eta_h$, the FC takes another sensing result.

Compared to approaches that need a fixed number of samples, such as N-P test and Bayesian detection, SPRT can achieve the same cooperative performance with fewer samples on an average [33].

3.1.3 Evolutionary Variant

In addition to the traditional hypothesis test and voting rule, there are a variety of data fusion technologies evolved from hypothesis test and voting rule to implement CSS.

(a) WSPRT: Motivated by the weight idea, WSPRT integrates the reputation-based mechanism into SPRT to realize CSS. Compared to the hypothesis test and voting rule, WSPRT provides a certain degree of CSS security under Byzantine attack. In details, the global decision is used as the consistency verification to evaluate the sensing result, then the SU's TrV can be expressed as

$$Trv_i(k) = Trv_i(k-1) + (-1)^{R_i(k)+g(k)} \tag{11}$$

where $g(k)$ is the k-th sensing slot's global decision. According to the SU's TrV, the weight can be expressed as

$$w_i(k) = \begin{cases} 0, & Trv_i(k) \le -g \\ \dfrac{Trv_i(k) + g}{\max\left(Trv_i(k)\right) + g}, & Trv_i(k) > -g \end{cases} \tag{12}$$

where g is the pre-setting value, $Trv(k)$ represents the TrV vector for all SUs at the k-th sensing slot.

When the SU's weight is integrated into likelihood ratio, WSPRT at the k-th sensing slot can be described as

$$W_l(k) = \prod_{i=1}^{l} \left(\frac{P(R_i|H_1)}{P(R_i|H_0)} \right)^{w_i(k)} \tag{13}$$

Sequentially, $W_l(k)$ is compared with a pair of decision thresholds η_l and η_h to conduct a global decision.

(b) Advance voting rule: On the basis of a generalized voting (GV) rule and sequential idea of SPRT, there are a variety of derivative voting rules, such as single symbol voting (S2V) rule [5], sequential single symbol voting (S3V) rule [34]. Since the PU is usually located in urban/suburban areas, the channel is at high/low usage, each SU is only required to submit a binary sensing result in S2V and S3V. Unlike S2V, all binary sensing results are sequentially arrived at the FC in S3V. In the end, both S2V and S3V must meet the decision condition, but the decision way of S3V's can be described as $\sum_{i=1}^{l} R_i \ge K$.

3.2 Problem Analysis

In front of Byzantine attack, the security and efficiency of CSS cannot be guaranteed in above-mentioned data fusion techniques at the same time. The previous work suffers from the following three problems:

(a) The previous Byzantine identification and suppression algorithms make use of the FC's global decision to update each SU's TrV, but the FC is prone to be compromised by Byzantine attack, resulting in a fact that MUs cannot be identified at this time.

(b) The weight allocation in the previous work is also prone to misidentify reliable SUs as MUs because reliable users may also be affected by shadowing and fading. Moreover, if the proportion of MUs increases to a certain extent, malicious identification strategies will restrict their participation in cooperation and significantly reduce the benefits of CSS.

(c) The previous work fails in considering the reporting way. The traditional reporting way in a large-scale CR system necessitates a lot of communication resources, which decreases the available cooperative gain and then results in a low cooperative efficiency.

Confronting the above problems of CSS in the presence of Byzantine attack, the following aspects need to be carefully taken into consideration before suppressing Byzantine attack and improving CSS performance and efficiency. The reliability of the global decision made by the FC or the measurement of the reporting results by means of the third party or mechanism should be guaranteed in a hostile sensing environment, with the aim of accurately distinguishing MUs and HUs. On the basis of (a), a weight allocation should be carefully designed to not only realize the suppression of Byzantine attack, but also maximize the cooperative gain of HUs. Since a large amount of sensing results will be submitted from each SU to the FC in an instant, at this time, the reporting way is implemented in the reporting channel. Therefore, an efficient reporting way is beneficial for SUs to quickly finish the PU detection and achieve more throughput. Through above analyses, we will propose WD3S to overcome problems mentioned above in the following section.

3.3 WD3S

In this section, we make use of the WSPRT framework to conduct WD3S, which consists of the data transmission consistency verification, the weight allocation, and the reporting way.

3.3.1 Data Transmission Consistency Verification

Data transmission consistency verification is one of the key components of our framework. In existing Byzantine identification and suppression algorithms, the global decision is not only a basis for SUs to access the channel but is used as a consistency verification of the local sensing results to update the SU's TrV as well. As shown in **Fig. 3**, by means of a specific fusion rule, the FC makes a global decision about the PU status according to the received sensing results after the sensing slot and reporting slot. When the FC declares that the PU is absent, i.e., H_0, the FC allows SUs to access the channel according to a specific resource allocation algorithm at the transmission slot. When the FC announces that the PU is present, i.e., H_1, the FC denies SUs to access to the channel and then all SUs need to continue sensing at the next frame. Through a brief description of the CSS process, it can be seen that the global decision is prone to be distorted by Byzantine attack. At this time, verifying the consistency of the local sensing results and updating the SU's TrV through the global decision is obviously unreliable. Therefore, the consistency verification should be carefully considered.

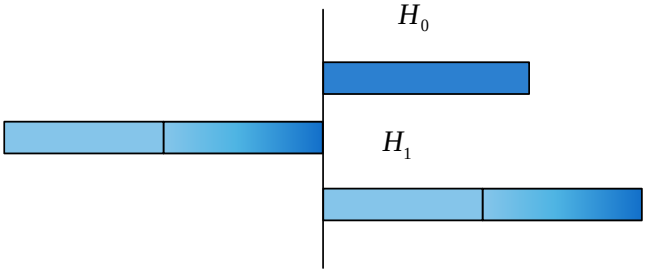


Fig. 3. The CSS frame structure.

A SU's ability to access the channel at the conclusion of its reporting time is determined solely by a global decision. But when the FC's global decision $g(k) = H_0$ is incorrect (the PU is actually present), SUs may access the channel, resulting in harmful interference at the channel; the FC's global decision $g(k) = H_1$ is incorrect (the PU is actually absent), neither the SU nor the PU will access the channel, the channel is not transmitting any data. It can be seen from these two aspects that the FC can distinguish the global decision's correctness by monitoring the data transmission on the channel, which can then be used to verify the consistency of the local sensing results and upgrade the SU's TrV. More importantly, the monitoring process of data transmission implemented by the FC is not affected by Byzantine attack strategy.

Based on the data transmission consistency verification, the SU's TrV can be expressed as

$$Trv_i(k) = Trv_i(k-1) + (-1)^{R_i(k)+d(k)} \tag{14}$$

where $d(k)$ is the PU channel status obtained by the data transmission consistency verification after the k-th sensing slot.

3.3.2 Weight Allocation

The next thing comes into consideration is how to design the weight allocation of likelihood ratio. Generally speaking, the weight of current sensing result is linked to the accuracy of historical sensing results. However, the accuracy evaluation of the historical sensing results depends on the global decision's accuracy. In a hostile environment, many works only take a simple Byzantine attack strategy, i.e., always attack or a small number of MUs, thereby MUs are easily identified in these scenarios and the global decision is still reliable. Considering the generality of the research and the robustness of the defense strategy, we adopt the data transmission consistency verification to conduct an accurate weight allocation for each SU's likelihood ratio. To this end, we take the following analyses about Byzantine attack into account as follows:

(a) According to the proposed attack model, two kinds of Byzantine attacks including miss detection attack and false alarm attack make the various negative impact on CSS. The false alarm attack can prevent HUs from using the underutilized channel so that MUs selfishly occupy it, while the miss detection attack will allure SUs to access the channel being utilized and cause excessive interference to the PU. Considering the influence of these two aspects, it is indispensable for the FC to accurately distinguish two kinds of Byzantine attacks, we define two decision abilities to describe the performance indicators of a SU according to the historical sensing results, such as, the ability of accurately detecting the PU's presence and absence. Then, after k sensing intervals, a pair of decision abilities of the i-th SU can be defined as

$$J_i^{\theta}(k) = T_i^{\theta}(k)/T^{\theta}(k) \tag{15}$$

where $T_i^{\theta}(k)$ represents the number of detecting the PU status θ and $T^{\theta}(k)$ is the number of the PU status θ.

(b) The useful information for making an accurate global decision may also be conveyed by the MUs' sensing results, and should not be eliminated from CSS process immediately. In fact, for the sake of its own security, MUs may sometimes launch Byzantine attack according to the proposed attack model and sometimes normally participate in CSS. If the FC arbitrarily eliminates MUs [35][36], Byzantine attack behaviors from MUs will be suppressed but HUs' spectrum sensing behaviors will be discouraged. To be specific, malicious sensing results are easily distinguished in some extreme cases, i.e., always attack, then the FC can benefit useful information from it to make the global decision. In details, a specific case for the decision abilities is considered, i.e., always attack. When a MU launches AY or AN attack, there is no doubt that $J_i^{\theta}(k)$ is approximate to 0, that is to say, the received result at the FC is flipped at this time and the result $1-\theta$ is more reliable. Inspires by the above considerations, we propose a new weight allocation method, in which MUs will never be eliminated, and may be reused.

According to the above analyses about Byzantine attack, the weight allocation $w_i^{\theta}(k)$ can be expressed as

$$w_i^{\theta}(k) = \begin{cases} 1 - J_i^{\theta}(k), & J_i^{\theta}(k) \le \delta_l \\ J_i^{\theta}(k), & J_i^{\theta}(k) \ge \delta_h \\ 0, \text{takes next senisng result} \end{cases} \tag{16}$$

where δ_l and δ_h are the threshold of the lower and upper decision ability. When the SU's decision ability is high, the decision ability is regarded as the weight to integrated into the likelihood ratio. When the SU's decision ability is low, the sensing result is flipped by $1 - J_i^{\theta}(k)$ at the calculation of the likelihood ratio. Furthermore, the sensing result will not be

computed into the likelihood ratio if the decision ability is between δ_l and δ_h. By this way, the FC can benefit from always attack and reduce the detrimental impact of other kinds of Byzantine attack.

Finally, the decision variable $W_l(k)$ is calculated as

$$W_l(k) = \prod_{i=1}^{l} \left(\frac{P(R_i|H_1)}{P(R_i|H_0)} \right)^{w_i^{\theta}(k)} \tag{17}$$

3.3.3 Reporting Way

Based on the data transmission consistency verification and weight allocation, theoretically, the negative effect of Byzantine attack can be mitigated and the CSS performance is also guaranteed, but the randomness of the likelihood ratio calculation process in SPRT remains a great barrier to CSS efficiency. In view of this, we further integrate the sequential idea and differential mechanism into the reporting way of SPRT, which can be described as follows:

(a) The sequential concept is extracted from the SPRT process, and its main idea is that the sensing results are collected in a sequential manner, and as time continues, more sensing information becomes available [32]. Then, the FC will process the sensing results sequentially as soon as the global decision is made, thereby resulting in degradation of sensing results required. Although the sequential idea has certain advantages over GV and traditional hypothesis test, it has no advantage in cooperative efficiency compared to SPRT and WSPRT. The mechanism for improving the cooperative efficiency needs further consideration.

(b) Based on the sequential idea, we make use of the differential mechanism to lessen the FC's need for a large number of sensing results. In details, when the previous and current sensing interval's sensing results are consistent for the i-th SU, the current sensing result of the SU does not need to be submitted to the FC, and the FC automatically regards the current sensing result as the same as the sensing result of the previous sensing results. Assuming that $R_i(k)$ is the sensing result of the i-th SU at the k-th sensing interval, if both $R_i(k)$ and $R_i(k-1)$ are H_0 or H_1, correspondingly, the FC regards the i-th SU's sensing result at the k-th sensing interval as H_0 or H_1. It is obvious that the number of sensing results required for the subsequent sensing interval will not be more than that for the previous sensing interval as time progresses.

It is worth noting that when the PU located in urban/suburban areas is at high/low channel usage, only 0 or 1 at the SU is sent to the FC, and the sequential idea and differential mechanism-based reporting way further reduces sensing results to quickly make a global decision. The following sensing results aren't required because the SU with the higher TrV is given priority to compute the likelihood ratio via the sequential and differential procedure. As a consequence, the FC can rapidly and accurately determine the PU status with the use of more reliable and valuable sensing information.

4. PERFORMANCE ANALYSIS

Based on a survey of data fusion techniques and the proposed WD3S, we make an in-depth analysis on its performance, in terms of the cooperative performance and the cooperative efficiency.

4.1 Cooperative Performance

4.1.1 Voting Rule

Though a variety of advanced voting rules evolve from the traditional GV, the decision condition remains unchanged. In other words, the cooperative performance for various voting rules under the same sensing environment is the same, i.e., the error probability.

Through summing the possibility of report results of satisfying the voting rule, when $\rho N \le K$, the global false alarm and miss detection probabilities can be obtained as (18) and (19); when $\rho N > K$, similar results are also obtained.

$$Q_{f,v} = \sum_{i=K}^{N} \left(\binom{N}{i} \sum_{k_m=0}^{\rho N} \left(\binom{\rho N}{k_m} P_{fa}^{k_m} (1-P_{fa})^{\rho N - k_m} \cdot \left(\sum_{k_n=K-k_m}^{N-\rho N} \binom{N-\rho N}{k_n} P_f^{k_n} (1-P_f)^{N-\rho N-k_n} \right) \right) \right) \tag{18}$$

$$Q_{d,v} = \sum_{i=K}^{N} \left(\binom{N}{i} \sum_{k_m=0}^{\rho N} \left(\binom{\rho N}{k_m} P_{da}^{k_m} (1-P_{da})^{\rho N - k_m} \cdot \left(\sum_{k_n=K-k_m}^{N-\rho N} \binom{N-\rho N}{k_n} P_d^{k_n} (1-P_d)^{N-\rho N-k_n} \right) \right) \right) \tag{19}$$

where P_{fa} and P_{da} are the probabilities of the false alarm and detection at the FC, and respectively given by

$$P_{fa} = (1-P_f)\alpha_0 + P_f(1-\alpha_1) \tag{20}$$

$$P_{da} = (1-P_d)\alpha_0 + P_d(1-\alpha_1) \tag{21}$$

4.1.2 Hypothesis Test

Different from voting rule, some a-priori information are assumed known in the hypothesis test, i.e., the conditional densities $P(H_\vartheta|H_\theta)$ and probabilities of the two hypotheses $P(H_\theta)$. In the observation space, the points are generated is consistent with conditional densities. Therefore, the likelihood ratio for the i-th SU can be obtained by

$$\frac{P(R_i|H_1)}{P(R_i|H_0)} = \left[\frac{P(R_i=H_1|H_1)}{P(R_i=H_1|H_0)}\right]^{R_i} \left[\frac{P(R_i=H_0|H_1)}{P(R_i=H_0|H_0)}\right]^{1-R_i} = \left[\frac{P_{d,i}}{P_{f,i}}\right]^{R_i} \left[\frac{1-P_{d,i}}{1-P_{f,i}}\right]^{1-R_i} \tag{22}$$

where $P_{f,i} = P_f$, $P_{d,i} = P_d$ for a HU, and $P_{f,i} = P_{fa}$, $P_{d,i} = P_{da}$ for a MU.

Since both Bayesian detection and N-P test adopt the same LRT and the only difference lies in the decision threshold, there is little difference in the cooperative performance between them. Furthermore, SPRT also adopts the same LRT as well as Bayesian detection and N-P test, the double threshold decision and sequential randomness make the cooperative performance unstable, especially in a hostile environment. Unlike the above hypothesis tests, both WSPRT and our proposed WD3S take Byzantine attack into

consideration. Nevertheless, the advantages of WSPRT and WD3S may not be obvious when there are no MUs in the CR system.

4.2 Cooperative Efficiency

4.2.1 Average Number of Samples

In addition to the cooperative performance, the cooperative efficiency should be taken into account because CSS uses a substantial amount of communication resources to report sensing results, which reduces or even undermines the available cooperative gain in a large-scale CR system [5]. Therefore, the number of sensing results required at the FC to make a global decision in a sensing observation period is our focus, that is, the average number of samples.

Regardless of MUs, all of Or, And, Majority, N-P test and Bayesian detection are employed for a fixed number of samples. When there are MUs in the CR system, the average number of samples for S2V and S3V have been given by (8) and (9)(10) in [5], respectively. Otherwise, though the average number of samples for SPRT in the absence of Byzantine attack has been given in [33], the presence of Byzantine attack may change the conditional probability of the CR system. Hence, the close-form expressions of the error probability and the average number of samples for the hypothesis test cannot be provided.

4.2.2 Detection Efficiency

In order to evaluate the detection efficiency of data fusion techniques, we take the error probability and the average number of samples into consideration to define a performance index as

$$\eta_e = \frac{1 - Q_e}{N_s} \tag{23}$$

where $Q_e = Q_f P(H_0) + (1 - Q_d)P(H_1)$ is the error probability, Q_f and Q_d are the global false alarm and detection probabilities respectively, N_s is the average number of samples.

According to (23), the detection efficiency is further normalized as

$$\eta = \frac{\eta_e}{\eta_m} \tag{24}$$

where η_m represents the maximum detection efficiency among data fusion techniques.

5. SIMULATION RESULTS

In this section, a series of simulation results are presented to verify the cooperative performance and efficiency of our proposed WD3S and other data fusion technologies in 1000 sensing intervals. To this aim, we consider that the percentage of MUs varies from 0 to 90% in an interval of 10% and a pair of attack probabilities are set to be 0.1, 0.5 and 1, respectively. The values of other simulation parameters are shown in **Table 1**.

Table 1. Simulation parameters

Parameters	**Symbol**	**Value**
Number of SUs	N	100
Probability of the hypotheses H_0	$P(H_0)$	0.3
Probability of the hypotheses H_1	$P(H_1)$	0.7
Local false alarm probability	P_f	0.1
Local detection probability	P_d	0.9
TrV threshold in WSPRT	g	-5
Tolerated false alarm probability	$\bar{P}_f$	10^{-3}
Tolerated miss detection probability	$\bar{P}_m$	10^{-4}
Cost of making H_0 under H_0	C_{00}	0
Cost of making H_1 under H_1	C_{11}	0
Cost of making H_0 under H_1	C_{01}	10
Cost of making H_1 under H_0	C_{10}	1
Threshold of N-P test	λ_{np}	100

5.1 CSS Performance

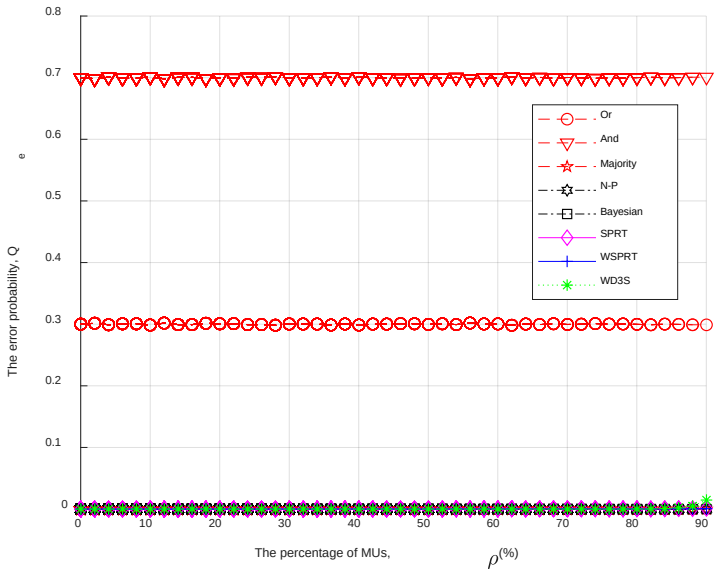


Fig. 4. The error probability v. s. the percentage of MUs when $\alpha_0 = \alpha_1 = 0.1$.

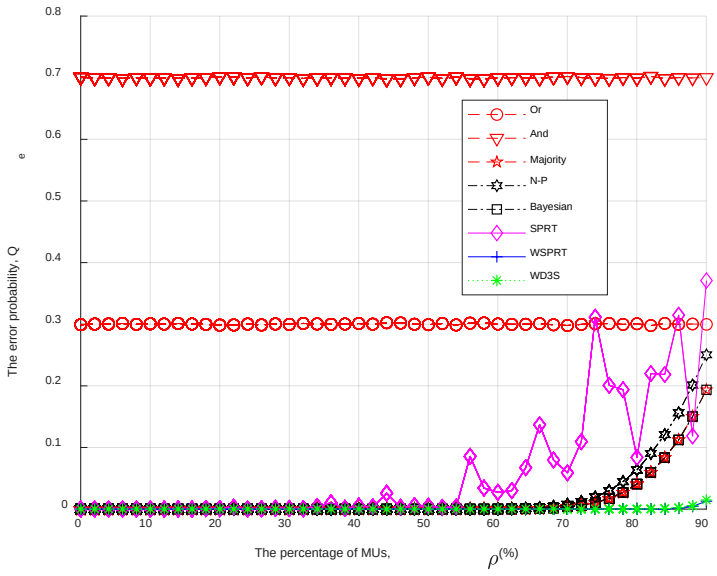


Fig. 5. The error probability v. s. the percentage of MUs when $\alpha_0 = \alpha_1 = 0.5$.

As illustrated in **Fig. 4**, the error probability for voting rule and hypothesis test are simulated when the attack probability $\alpha_0 = \alpha_1 = 0.1$. In the voting rule, the error probability of Or and And are stable at 0.3 and 0.7, respectively. This is because the both false alarm probability and the detection probability are high in Or rule while low in And rule, meanwhile $Q_e = Q_f P(H_0) + (1 - Q_d)P(H_1)$. Besides, the error probability for other data fusion technologies are basically 0. Apparently, for some MUs with a low attack probability, most data fusion technologies for CSS have a certain error tolerance rate and can maintain relatively good cooperative performance.

When the MU increases the attack probability, i.e., $\alpha_0 = \alpha_1 = 0.5$, the error probability the error probability is displayed in **Fig. 5**. Though Or and And still keeps the same error probability as well as $\alpha_0 = \alpha_1 = 0.1$, the error probability of other data fusion technologies has changed with the increase of MUs. For example, the error probability of Majority rule/Bayesian detection/N-P test begins to increase when the percentage of MUs is 70%/68%/64%. Specifically, the error probability of SPRT begins to jitter when $\rho = 0.3$, and the jitter becomes more severe as MUs increase because of the randomness of the LRT calculation process. Obviously, these traditional data fusion technologies are naturally resistant to Byzantine attack, but as the number and attack probability of MUs increase, the CSS performance will eventually decrease.

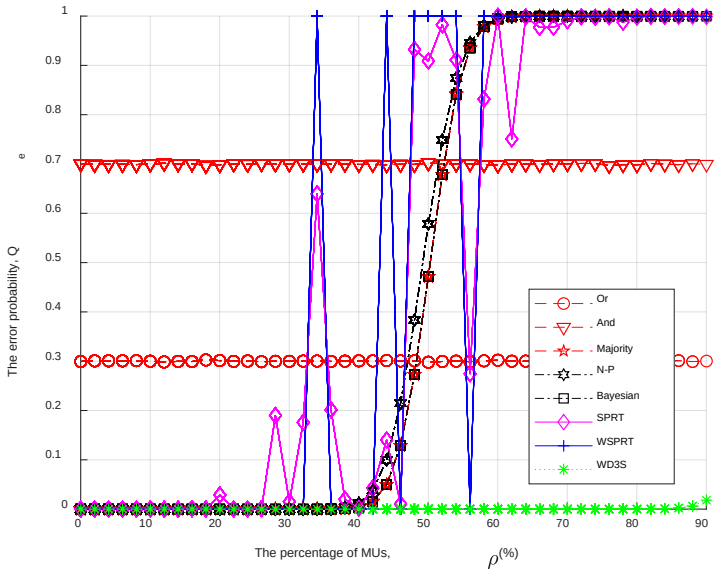


Fig. 6. The error probability v. s. the percentage of MUs when $\alpha_0 = \alpha_1 = 1$.

When there is an always attack in the CSS process, the error probability is simulated when the attack probabilities are 1. From **Fig. 6**, we can see that all data fusion technologies except for Or and And rule are capable of defending against always false attack when the malicious ratio is relatively small. Unfortunately, once the malicious ratio exceeds 50%, none of data fusion technologies other than WD3S can make an accurate decision. In this case, the error probability for Majority, N-P test, and Bayesian detection is higher than 50%, in other words, the cooperative performance is not much better than random guessing. In other words, MUs completely compromise the CR system, thereby making the FC incapable of decision-making. Further, the error probability of SPRT and WSPRT involving the sequential idea fluctuates as the MUs increase. Nevertheless, the SPRT fluctuates slowly 20% to 80% while WSPRT fluctuates quickly 30% to 60%. This is due to the fact that the weight of WSPRT suppresses always attack to a certain extent, but the further increase in the proportion of MUs makes the global decision unreliable, and the weight is no longer effective. After the attack ratio exceed 60%, the global decision of these data fusion technologies at the FC is completely distorted.

On contrary, regardless of the attack probability and attack ratio, WD3S always keeps remarkable performance. Undoubtedly, this is the benefit of the data transmission consistency verification. Since the data transmission monitoring process provides WD3S with a fundamental brick to evaluate the local sensing results and update SUs' TrV instead of the global decision, Byzantine identification and suppression are not affected by attack strategies at all.

5.2 CSS Efficiency

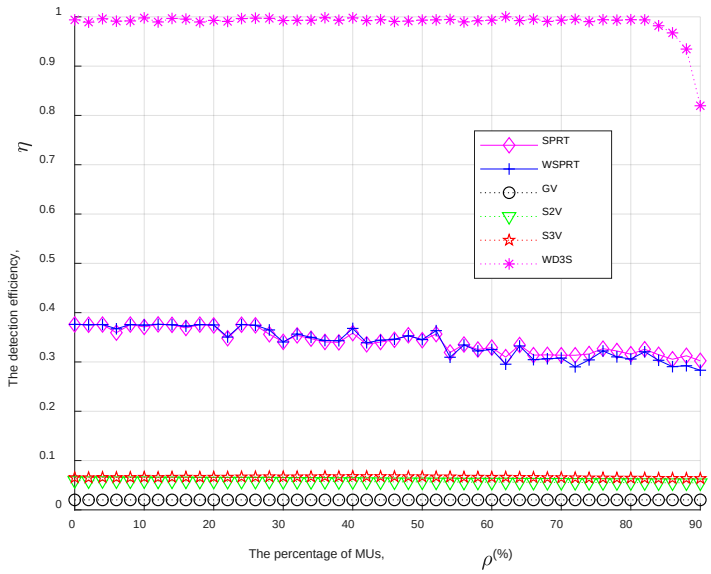


Fig. 7. The detection efficiency v. s. the percentage of MUs when $\alpha_0 = \alpha_1 = 0.1$.

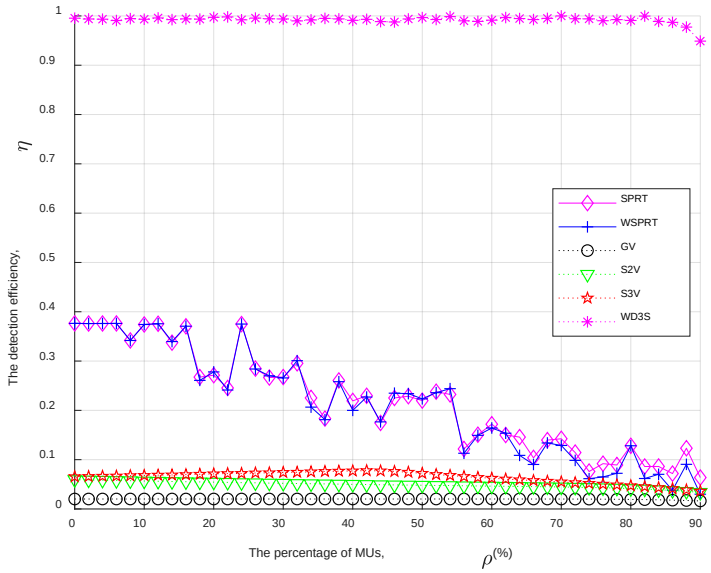


Fig. 8. The detection efficiency v. s. the percentage of MUs when $\alpha_0 = \alpha_1 = 0.5$.

Extensive simulation study has been performed and demonstrates that the proposed WD3S can guarantee the cooperative performance with a low error probability when a considerable number of MUs launch a probabilistic Byzantine attack. Now, there is continuing effort to present the detection efficiency for data fusion technologies. Since both N-P test and Bayesian detection adopt a fixed-sample-size methodology, we only

present the detection efficiency comparison of GV and other sequential methods and assume that GV, S2V and S3V adopt the decision condition of Majority rule to build a fair comparison framework.

From **Fig. 7**, GV needs sensing results of all SUs to make a global decision and has not advantages in the cooperative performance, thereby it has the lowest detection efficiency. Further, both S2V and S3V takes a specific scenario where the PU located in urban/suburban areas may be at high/low channel usage into consideration, specifically, S3V integrates the sequential idea into S2V to reduce the number of samples, all of them make no difference in the error probability, therefore the improvement of the detection efficiency is not obvious. Unlike the voting rule, the detection efficiency gradually decreases in SPRT and WSPRT as the percentage of MUs increases. This is reasonable, because Byzantine attack does not decrease the error probability at this time but makes the FC need more sensing results to make the global decision.

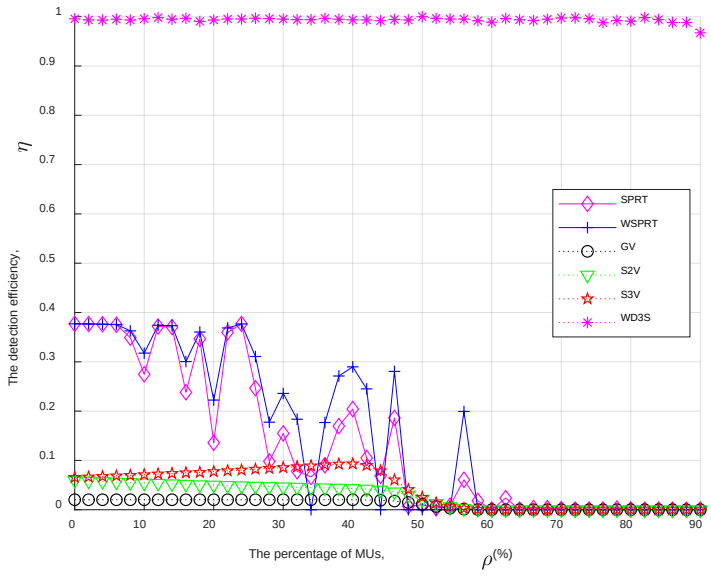


Fig. 9. The detection efficiency v. s. the percentage of MUs when $\alpha_0 = \alpha_1 = 1$.

When the attack probability and ratio increase, it is known in **Fig. 4** and **Fig. 5** that the error probability of the voting rule, SPRT and WSPRT begins to increase. Since the number of sensing results required by the FC also increases, the detection efficiency is expected to decrease in **Fig. 8**, which is a consequence of the joint effect of the attack probability and ratio. However, under a low attack probability, WSPRT does not play the advantage of the weight in the likelihood ratio calculation. In **Fig. 9**, there is no doubt that though the detection efficiency of WSPRT has jitter, it still has certain advantages compared with SPRT. The design of the likelihood ratio weight has a positive impact on the error probability and detection efficiency. Meanwhile, the increasing MUs implementing always false attack make the error probability of three voting rules decrease until it reaches 1, resulting in a detection efficiency of 0.

Under different attack probabilities and attack ratios, WD3S always maintains a very high detection efficiency, especially in a high attack probability. Following the remarkable error performance, the reason for this phenomenon is that the reporting way combining the sequential idea and differential mechanism reduces the sample size and the TrV

descending order helps LRT quickly make an accurate global decision at the FC. In particular, the reuse weight allocation makes the FC benefit from the malicious sensing results in WD3S. As a result, the higher the attack probability, the higher the detection efficiency.

In summary, with the assistance of the data transmission consistency verification, the reuse weight allocation and the sequential and differential -based reporting way enable the FC to efficiently make an accurate global decision.

6. Conclusions

In this paper, we study data fusion technologies for CSS in an interweave CR system. To defend against Byzantine attack, we review existing data fusion technologies by dividing them into voting rule and hypothesis test. On the basis of advantages and disadvantages, we propose a secure and efficient WD3S to mitigate the negative impact of dynamic Byzantine attack on CSS, in which makes use of the data transmission status to verify the correctness of the global decision, designs a weight allocation to selectively benefit from MUs' sensing results, and adopts the sequential and differential reporting way to submit the sensing results in the SU's TrV descending order. Moreover, the CSS performance and efficiency of a series of data fusion technologies are evaluated. Finally, numerical simulation results show the concreteness and effectiveness of our theoretical analysis on existing data fusion technologies and corroborate the superiority of WD3S in the error probability and the detection efficiency.

Acknowledgement

The authors declare that they have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

[1] Y. Al-Mathehaji, S. Boussakta, M. Johnston and J. Hussein, "Primary receiver-aware opportunistic broadcasting in cognitive radio ad hoc networks," in *Proc. of 8th International Conference on Ubiquitous and Future Networks*, pp. 30-35, 2016. Article (CrossRef Link)

[2] W. Saad, Z. Han, H. V. Poor, T. Basar and J. B. Song, "A cooperative Bayesian nonparametric framework for primary user activity monitoring in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1815-1822, Oct. 2012. Article (CrossRef Link)

[3] Y. Shei and Y. T. Su, "A sequential test based cooperative spectrum sensing scheme for cognitive radios," in *Proc. of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1-5, 2008. Article (CrossRef Link)

[4] R. Chen, J. M. Park and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. of IEEE INFOCOM 27th Conference on Computer Communications*, pp. 1876-1884, 2008. Article (CrossRef Link)

[5] J. Wu, Y. Yu, and J. Hu, "Sequential 0/1 for cooperative spectrum sensing in the presence of strategic Byzantine attack," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 500-503, Apr. 2019. Article (CrossRef Link)

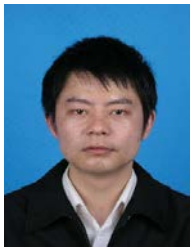
[6] G. Zhang, X. Wang, Y. Liang and J. Liu, "Fast and robust spectrum sensing via kolmogorov-smirnov test," *IEEE Transactions on Communications*, vol. 58, no. 12, pp. 3410-3416, December 2010. Article (CrossRef Link)

[7] K. Haghighi, A. Svensson and E. Agrell, "Wideband sequential spectrum sensing with varying thresholds," *IEEE Global Telecommunications Conference GLOBECOM*, pp. 1-5, 2010. Article (CrossRef Link)
[8] H. Hsieh, H. Chang and M. Ku, "Higher-order statistics based sequential spectrum sensing for cognitive radio," in *Proc. of 11th International Conference on ITS Telecommunications*, pp. 696-701, 2011. Article (CrossRef Link)
[9] S. Mapunya and M. Velempini, "The design of Byzantine attack mitigation scheme in cognitive radio Ad-hoc networks," in *Proc. of International Conference on Intelligent and Innovative Computing Applications*, pp. 1-4, 2018. Article (CrossRef Link)
[10] Y. Yilmaz, G. V. Moustakides and X. Wang, "Cooperative sequential spectrum sensing based on level-triggered sampling," *IEEE Transactions on Signal Processing*, vol. 60, no. 9, pp. 4509-4524, Sept. 2012. Article (CrossRef Link)
[11] Q. Li and Z. Li, "A novel sequential spectrum sensing method in cognitive radio using suprathreshold stochastic resonance," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1717-1725, May 2014. Article (CrossRef Link)
[12] N. Marchang, A. Taggu and A. K. Patra, "Detecting Byzantine attack in cognitive radio networks by exploiting frequency and ordering properties," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 4, pp. 816-824, Dec. 2018. Article (CrossRef Link)
[13] A. Taggu and N. Marchang, "Random-Byzantine attack mitigation in cognitive radio networks using a multi-hidden markov model system," in *Proc. of International Conference on Electrical and Computing Technologies and Applications*, pp. 1-5, 2019. Article (CrossRef Link)
[14] R. Sarmah, A. Taggu and N. Marchang, "Detecting Byzantine attack in cognitive radio networks using machine learning," *Wireless Networks*, vol. 26, no. 8, pp. 5939-5950, 2020. Article (CrossRef Link)
[15] M. Liu, N. Zhao, J. Li and V. C. M. Leung, "Spectrum sensing based on maximum generalized correntropy under symmetric alpha stable noise," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 10262-10266, Oct. 2019. Article (CrossRef Link)
[16] 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 Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5244-5257, Aug. 2017. Article (CrossRef Link)
[17] W. Lee, M. Kim and D. Cho, "Deep cooperative sensing: cooperative spectrum sensing based on convolutional neural networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 3005-3009, Mar. 2019. Article (CrossRef Link)
[18] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu and P. Li, "AI at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9600-9610, Oct. 2020. Article (CrossRef Link)
[19] P. Zhang, S. G. Nagarajan and I. Nevat, "Secure location of things (SLOT): mitigating localization spoofing attacks in the Internet of Things," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2199-2206, Dec. 2017. Article (CrossRef Link)
[20] L. Zhang, G. Nie, G. Ding, Q. Wu, Z. Zhang and Z. Han, "Byzantine attacker identification in collaborative spectrum sensing: A robust defense framework," *IEEE Transactions on Mobile Computing*, vol. 18, no. 9, pp. 1992-2004, Sept. 2019. Article (CrossRef Link)
[21] K. Zeng, P. Pawelczak and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226-228, Mar. 2010. Article (CrossRef Link)
[22] X. Wang, M. Jia, Q. Guo and X. Gu, "A trust-value based cooperative spectrum sensing algorithm for mobile secondary users," in *Proc. of IEEE International Conference on Communication Workshop*, pp. 1635-1639, 2015. Article (CrossRef Link)
[23] J. Wang and I. Chen, "Trust-based data fusion mechanism design in cognitive radio networks," in *Proc. of IEEE Conference on Communications and Network Security*, pp. 53-59, 2014. Article (CrossRef Link)

[24] J. Wu, T. Song, Y. Yue, W. Cong, J. Hu, "Sequential cooperative spectrum sensing in the presence of dynamic Byzantine attack for mobile networks," *PLoS ONE*, vol. 13, no. 7, p. e0199546, 2018. Article (CrossRef Link)
[25] A. Sivakumaran, A. S. Alfa and B. T. Maharaj, "An empirical analysis of the effect of malicious users in decentralised cognitive radio networks," in *Proc. of IEEE 89th Vehicular Technology Conference*, pp. 1-5, 2019. Article (CrossRef Link)
[26] J. Wang, Y. Liu, S. Niu and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Computer Communications*, vol. 165, pp. 131-140, 2021. Article (CrossRef Link)
[27] J. Wang, Y. Liu, S. Niu, H. Song, W. Jing and J. Yuan, "Blockchain enabled verification for cellular-connected unmanned aircraft system networking," *Future Generation Computer Systems*, vol. 123, pp. 233-244, 2021. Article (CrossRef Link)
[28] Y. Liu, J. Wang, J. Li, S. Niu, L. Wu and H. Song, "Zero-bias deep-learning-enabled quickest abnormal event detection in IoT," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 11385-11395, 2022. Article (CrossRef Link)
[29] H.A. Ghazijahani, A.A. Sharifi, J.M. Niya and H. Seyedarabi, "Attack-aware cooperative spectrum sensing in cognitive radio networks under byzantine attack," *Journal of Communication Engineering*, vol. 6, pp. 81-98, 2017. Article (CrossRef Link)
[30] Y. Liang, Y. Zeng, E. C. Y. Peh and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326-1337, April 2008. Article (CrossRef Link)
[31] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342-1363, thirdquarter 2015. Article (CrossRef Link)
[32] R. Chen, J. M. J. Park, K. Bian, "Robustness against Byzantine failures in distributed spectrum sensing," *Computer Communication*, vol. 35, no. 17, pp. 2115-2124, 2012. Article (CrossRef Link)
[33] P. K. Varshney, "Distributed detection and data fusion," *Springer Science & Business Media*, 2012. Article (CrossRef Link)
[34] J. Wu, P. Li, Z. Chen, C. Ze and J. Bao, "Sequential single symbol differential voting for cooperative spectrum sensing in the presence of byzantine attack and imperfect reporting channels," in *Proc. of 8th international Conference on wireless communication and sensor networks*, pp. 39-46, January 2021. Article (CrossRef Link)
[35] J. Wu, T. Song, C. Wang and J. Hu, "Reputation value ranking based sequential cooperative spectrum sensing against Byzantine attack," in *Proc. of IEEE International Conference on Communications Workshops*, pp. 1-6, 2018. Article (CrossRef Link)
[36] A. Al-Tahmeesschi, M. López-Benítez, V. Selis, D. K. Patel and K. Umebayashi, "Cooperative estimation of primary traffic under imperfect spectrum sensing and Byzantine attacks," *IEEE Access*, vol. 6, pp. 61651-61664, 2018. Article (CrossRef Link)

Jun Wu received the Ph.D. degree in Information and Communication Engineering from Southeast University, Nanjing, China, in 2018. He joined School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China, where he is currently a Lecturer from 2019. He has published over 20 IEEE/IET journal papers and conference papers, including IEEE Systems Journal, IEEE TVT, IEEE CL, IEEE WCL, IEEE Access, IET Communications and IEEE ICC, IEEE VTC. His current research interests include unmanned aerial vehicle, cognitive radio networks, internet of things, sequential detection, network security, machine learning and blockchain. He also severed as a reviewer for IEEE TCCN, IEEE Systems Journal, IEEE TVT, IEEE WCL, IET Communications and ETRI Journal etc., and a TPC member in several IEEE conferences.

Ze Chen is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, unmanned aerial vehicle, spectrum sensing, network security.



Jianrong Bao received his B.S. degree in Polymer Materials & Eng., and the M.S.E.E. degree from Zhejiang University of Technology, Hangzhou, China, in 2000 and 2004, respectively. He received his Ph.D. E.E. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2009. Currently, he is a professor at the Information Engineering School, Hangzhou Dianzi University, Hangzhou, China. He has been a postdoctoral researcher twice, at the Laboratory of Satellite Navigation, Zhejiang University, Hangzhou, China, from 2011 to 2013, and at the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, from 2014 to 2016, respectively. He also visited at the Department of Electrical Engineering, Columbia University in the City of New York, USA, as a Visiting Scholar under the supervision of Prof. Xiaodong Wang in 2015. His main research interests include space wireless communications, cooperative communications, communication signal processing, coordinated channel coding, and cognitive radio, etc. He has presided two general projects from the National Natural Science Foundation of China (NSFC) and two projects from the Zhejiang Natural Science Foundation of China (ZJNSFC), including one key program. He also received a Zhejiang Provincial Natural Science Progress Award about the Free Space Optical Wireless Signal Processing in Dec. 2016. He has been the authors or co-author of several IEEE Transaction papers and also the reviewer for the journal of IEEE Trans. Commun., IEEE Trans. Wireless Commun., IEEE Trans. Vehicular Tech., etc.

Jipeng Gan is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, network security, game theory.

Zehao Chen is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, unmanned aerial vehicle, spectrum sensing, network security.

J ia Zhang is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, unmanned aerial vehicle, spectrum sensing.