Efficient Byzantine Defense Algorithm for Cooperative Spectrum Sensing in Cognitive Radio Networks

Ze Chen¹, *, Jun Wu¹, ²

¹School of Communication Engineering, Hangzhou Dianzi University Hangzhou, Zhejiang Province, China
²College of Information Science and Electronic Engineering, Zhejiang University Hangzhou, Zhejiang Province, China

*Corresponding author: 18081511@hdu.edu.cn

Abstract. Cooperative spectrum sensing (CSS) is a process of achieving spatial diversity gain to make global decision for cognitive radio networks (CRNs). However, the accuracy of the global decision effects owing to the presence of Byzantine during cooperative sensing, therefore causing severe performance degradation of CSS. In front of malicious users (MUs) launching Byzantine attack, a robust defense framework is proposed to defend against Byzantine attack and improve the efficiency of the CSS. For this aim, a novelty weighted single symbol (WSS) algorithm based on the reputation value update mechanism and the single symbol report method is proposed in this paper. We first propose a defense framework based on the reputation value distribution. In order to ensure the accuracy of Byzantine identification, we further evaluate the reputation value of secondary users (SUs)’ reports by mean of data transmission consistency verification. Moreover, the single symbol report method is utilized to improve the efficiency of Byzantine defense algorithm and reduce the report sample size. Finally, a series of mathematical analyses prove that the proposed defense framework improves the efficiency of CSS under Byzantine attacks.

1. Introduction

Cognitive radio (CR) allows the secondary users (SUs) to opportunistically access the spectrum band allocated to the primary user (PU) through the local spectrum sensing (LSS) technology without causing harmful interference to the PU’s normal communication, therefore solving the spectrum scarcity problem of the growing wireless applications. Since the single user spectrum sensing is often affected by the noise uncertainty, multipath fading, shadowing etc., cooperative spectrum sensing (CSS) is proposed to improve the detection accuracy of the PU. In the CSS, all SU independently detect the PU’s signal by LSS technology, and the submit own sensing result to the fusion center (FC) through the reporting channel. Finally, the FC is responsible for issuing global decision about the PU status according to a specific fusion rule.

Although the participation of multiple SUs in CSS contributes to the improvement of detection accuracy, the global decision making may be misguided when malicious users (MUs) intentionally or unintentionally send falsified sensing information to the FC during cooperation. This sort of attack in CSS, called Byzantine attacks, significantly degrades collaborative detection correctness. The MUs
report false sensing results and mislead the FC to make the wrong global decision, which severely deteriorates the performance of the cognitive radio network (CRN).

In order to mitigate the negative impact of Byzantine attack on CSS, a lot of efforts have been paid to combating Byzantine attack and Byzantine defense algorithms. Generally, ordinary Byzantine defense consists of three parts: design defense reference, reputation evaluation and global decision making [1].

In the reputation evaluation stage, the FC applies the reputation value to the data fusion process. SUs with high reputation value are considered to be more reliable in cooperative spectrum sensing. In [2], when the reputation value of a SU is lower than a threshold preset by the system, the SUs will no longer participate in spectrum sensing. In [3], the FC only selects SUs with high reputation value to participate in data fusion to improve the PU’s detection accuracy. However, for general MUs, the malicious reports may contain useful sensing information for the global decision. This motivated us to use Byzantine data, aiming at improving the performance and efficiency of CRN and secure the CSS process.

In order to take into account the efficiency and security of the defense algorithm, many Byzantine identification algorithms have been proposed. For example, In [4], M. Liu et al. used the maximum generalized correntropy to improve the spectrum sensing performance in low generalized signal-to-noise ratio conditions. In [5], a novel attack-proof CSS scheme with M-ary quantized data was proposed by H. Chen et al., mainly including a MU identification method and an adaptive linear combination rule. [6] considered the distributed energy-based detectors for spectrum sensing in CRNs and derives the optimal energy combining rule based on the Bayesian rule. W. Lee et al. used training sensing samples to independently learn the strategy of combining the single sensing results of SU through convolutional neural network (CNN) and consider the spectrum and spatial correlation of each sensing result, which improves the CSS performance.

Q. Wang et al. proposed a novel blockchain-empowered decentralized secure multiparty learning system with heterogeneous local models called BEMA (Blockchain-Empowered Secure Multiparty Learning) in [7]. Particularly, the authors considered two types of Byzantine attacks, and carefully design “off-chain sample mining” and “on-chain mining” schemes to protect the security of the proposed system. In [8], the location estimation problem in CSS was reformulated as a stochastic censoring model and derive the maximum likelihood estimator for the node’s location by P. Zhang et al. [9] developed a robust defense framework, where a reference is built based on the extended sensing, and the transmit results and sensors are continuously evaluated via the reference and identified at intervals. In the framework, except of data falsification, multiple practical factors are considered, including the variation characteristic of sensors’ attributes, imperfect reporting channel, and inference errors based on the transmitting results. J. Wu et al. proposed a robust sequential CSS against dynamic Byzantine attack by means of delivery-based assessment to check consistency of individual sensing report, and innovatively reuses the sensing information from Byzantines via a novel weight allocation mechanism in [10] ~ [11]. Although the aforementioned Byzantine defense methods have satisfactory detection performance, [4] ~ [9] need to traversal all samples in the process data fusion, ignore the reporting mechanism and [10] ~ [11] pay more attention to the dynamics of Byzantine attacks and fail to consider the efficiency of the algorithm.

Different from the above-mentioned work, this paper comprehensively considers the performance of CSS and the reduction of report sample size in the context of the Byzantine attack. In addition, the single symbol method is used to reduce the overhead problem between the SU and the FC, thereby improving the effectiveness of the algorithm. Therefore, this paper proposes a simple and effective weighted single symbol algorithm (WSS) for CSS, which can safely and effectively submit the local decision of the SU to the FC.

This paper is organized as follows. Section II describes the system model. Section III starts with the WSS algorithm. Then we analyze the communication overhead cost of the WSS algorithm and compare it with ordinary voting rules. Section IV concludes the paper.
2. System Model
We consider a centralized CRN consisting of a PU, a FC and $N$ SUs wherein the MU ratio is $\rho$, as shown in Fig. 1. When in the sensing time slot, the SUs will perform LSS (i.e., energy detection, matched filter detection, cyclostationary feature detection, wavelet detection, etc.) to detect the presence or absence of the PU. Among these spectrum sensing techniques, the energy detection is commonly adopted because of its low implementation cost and compatibility with legacy primary systems. For the $i$-th SU, the detection probability and the false alarm probability are respectively denoted as $P_{d,i}$ and $P_{f,i}$. Assuming that the probability of a Byzantine attack is certain, the global false alarm probability $P_{f_i}$ and the global detection probability $P_{d_i}$ of a SU can be easily obtained through a fixed channel performance and the probability of a Byzantine attack.

It is known that the periodic spectrum sensing frame for CRNs consists of a sensing slot, a reporting slot and a data transmission slot. After each SU individually detects the PU signal by energy detection in the sensing slot, then submit own sensing result to the FC by the reporting channel in the reporting slot.

Fig 1. The infrastructure-based CRNs.

However, due to the openness of the communication underlying protocol in CRNs, the MUs will mislead the FC to decide whether there is a PU using the channel by falsifying the sensing results. This malicious behavior can be classified into two types. On the one hand, the MU falsifies the sensing result $S_i = H_0$ into $R_i = H_1$, hence that the SU believes that there is a PU on the being detected channel. Based on the basic principles of the CRN, SUs has to switch another channel and continue to perform spectrum sensing band so that the MU could selfishly occupy it; On the other hand, the MU falsifies the sensing result $S_i = H_1$ into $R_i = H_0$, leading the SU accesses the busy channel and interferes with the normal operation of the cognitive communication system. There is no doubt that, the malicious behavior will have significantly negative impact on the CSS performance and undermine the premise of CRN technology.

3. WSS For CSS
According to the CSS model, when there exists Byzantine attack, we are inspired by various existing voting rules and sequential idea to propose WSS, aiming at achieving better security, efficiency and performance of CSS.
3.1. Existing data fusion techniques
Since Byzantine attack poses a severe threat to the CSS process, the risk of Byzantine attack on the CRN should be carefully considered, a lot of research work have proposed a variety of data fusion techniques from different perspectives, which can be divided into voting rule and hypothetical testing.

3.1.1. Voting Rule. The voting rule (a.k.a. K-out-of-N rule or decision rule) is a basic data fusion technique and contains three kinds of widely adopted rule, such as, And-rule, Or-rule and Majority-rule. Assuming that the FC has received N reports of SUs, and it needs to make a global decision from these reports to determine the status of the PU. The voting rules do not require a priori information of the PU signal, and is simple to implement. However, compared with other data fusion techniques, there is no security and efficiency at all.

3.1.2. Hypothesis Test. Hypothesis testing uses different design rules. Three hypothesis testing methods widely used in the process of spectrum sensing are Bayesian test, Neyman-Pearson test and sequence probability ratio test. Among them, Bayesian test is proposed to minimize the average detection cost or risk, and Neyman-Pearson test is introduced to minimize the probability of miss detection. The sequence probability ratio test can achieve the same detection performance as the fixed sample test while reducing the overhead cost.

Unlike voting rules, the implementation of hypothesis test depends on some prior information about PU signals or conditional probabilities of four possible decision.

3.2. WSS
Based on the existing data fusion techniques, a new data fusion method called WSS is proposed to combine the idea of the single symbol reporting and the reputation value distribution.

In order to reduce the threat of Byzantine attack to CR system, we pay more attention to the use of malicious data and data transmission verification by means of weighted sequential probability test (WSPRT) to improve the security and efficiency of CSS [12].

The WSPRT initializes the reputation value and weight for each SU and updates the SU’s reputation value and weight after each global decision is made. The reputation value updating mechanism can be described as

\[ T_{rv}(k) = T_{rv}(k-1) + (-1)^{r_i(k)}g(k) \]  

(1)

where \( g(k) \) represents the global decision of the \( k \)-th sensing. If a SU's decision is always the same as the global decision, then its reputation value will not decrease. On the contrary, if a SU is malicious, its report result will be likely to be different from the global decision. Then, the FC will assign weight to SUs based on the individual reputation value and proceed with the data fusion. The weight of each SU can be obtained by the following normalized function

\[ w_i(k) = \begin{cases} 0, & T_{rv}(k) \leq -g \\ \frac{T_{rv}(k)+g}{\max(T_{rv}(k)+g)}, & T_{rv}(k) > -g \end{cases} \]  

(2)

where \(-g\) is the presetting threshold. If the SU’s reputation value is less than \(-g\), its decision result will be eliminated in the collaboration process. However, it is not easy to select the appropriate threshold value in practice, therefore an honest SU may be misidentified as a MU so that the efficiency and accuracy of CSS is significantly declined.
To solve this issue, the reuse the reputation allocation mechanism is considered. In the case of a large proportion of MUs, the malicious reports often lead to incorrect global decisions, here the data consistency verification rules are introduced. The specific rules are as follows: after the FC makes a global decision, the channel situation is always monitored. If the global decision is 1, it means that the spectrum is occupied by the PU. At this time, if it is found that the channel is not occupied by the PU or the channel is occupied by the SU, then it means that the overall decision is wrong. Conversely, if the global decision is 0, it means that the spectrum is not occupied. If the channel is found to be occupied at this time, it means that the MU is taking the opportunity to invade spectrum resources.

So, the update rule of equation (1) can be written as

$$Trv_i(k) = Trv_i(k - 1) + (-1)^{v_i(k) + d(k)}$$

(3)

where $d(k)$ is the PU channel status obtained by the data transmission consistency verification? In addition, the data of the MUs will not be removed by us. These malicious reports will be used in the data fusion process, that is, (2) becomes

$$w_i(k) = \begin{cases} 1 & \frac{Trv_i(k)}{\max(Trv_i(k))} + g \leq -g \\ \frac{Trv_i(k)}{\max(Trv_i(k))} + g & \frac{Trv_i(k)}{\max(Trv_i(k))} + g > -g \end{cases}$$

(4)

Finally, for the decision variable $W_i(k)$, if it exceeds the threshold range, then FC will make a global decision, otherwise FC will continue to perform the fusion of the next sample in sequence, and $W_i(k)$ could be expressed as:

$$W_i(k) = \prod_{l=1}^{L} \left( \frac{p[i|H_1]}{p[i|H_0]} \right)^{w_i^l(k)}$$

(5)

The next thing comes into consideration is the efficiency of data fusion. Starting with the voting rule, we assume that the LSS performance of each SU is the same (i.e., $P_{f,l} = P_{f}$, $P_{d,l} = P_{d}$, $P_{e,l} = P_{e}$), then the global false alarm probability and global detection probability of the voting rule can be given by

$$Q_{f,g} = \sum_{k=1}^{N} \binom{N}{k} P_f^k (1-P_f)^{N-k}$$

(6)

$$Q_{d,g} = \sum_{k=1}^{N} \binom{N}{k} P_d^k (1-P_d)^{N-k}$$

(7)

Such a voting rule needs to traversal the entire sensing sample, and perform poorly in terms of efficiency. This inspires us to propose a new reporting mechanism to report samples from the SU to the FC. In high spectrum usage urban areas, the PU is more likely to use the channel. Therefore, we consider...
that only reports \( R_i = 0 \) could be transmitted to reduce the number of reports. This reporting rule is known as single symbol voting (S2V) rule. The single symbol rule can naturally counter Byzantine attack that falsify 0 to 1, because when MUs attempt to send report 1, the malicious sensing information will not be transmitted.

Combining the idea of single symbol reporting and the use of malicious data, using WSPRT as a method of data fusion, the novel data fusion method of WSS is proposed.

3.3. Performance Analysis
Based on the generalized voting rule, the proposed S2V and WSS have improved in terms of security and efficiency. Compared with the generalized voting rule, S2V and use the single symbol reporting method and the sequential detection to improve the detection efficiency and do not change the decision condition, therefore it provides the consistent performance with the best case in the generalized voting rule. Further, WSS uses the differential reporting and the reputation value distribution to further improve the security and efficiency of the algorithm. In addition, since S2V and WSS adopt differential reporting methods related to the spectrum sensing interval structure, therefore a closed-form expression cannot be given.

3.4. Report Sample Size
The WSS algorithm has relatively satisfactory performance in terms of the security and efficiency. In this subsection, we will further analyze and evaluate the report sample size determining the efficiency of the algorithm. S2V uses a single symbol reporting method to report only 0s in high spectrum usage urban areas. Due to the special reporting method, its efficiency is obviously better than the voting rule. Assuming that the probability of reporting 0 is represented by \( P \), then the average report sample size of S2V can be expressed as

\[
\Phi_2(N,K,P) = \sum_{i=0}^{N-K} (N-i) \phi(N,i,1-P) + \sum_{i=K}^{N} i \phi(N,i,P) \tag{8}
\]

where \( \phi(n,r,p) = \binom{n}{r} p^r (1-p)^{n-r} \) is the probability mass function of the binomial distribution, which represents the probability of getting \( r \) successes in \( n \) trials? The first and the second item on the right side of (11) represent the average report sample size when the global decision is 1 and 0, respectively.

According to Bayes’ theorem, the report sample size of S2V can be expressed as

\[
N_2 = \Phi_2(N,K,P|H_1) P(H_1) + \Phi_2(N,K,P|H_0) P(H_0) \tag{9}
\]

\[
= \Phi_2(N,K,\overline{P}_d|H_1) P(H_1) + \Phi_2(N,K,\overline{P}_f) P(H_0) \tag{10}
\]

4. Simulation
In this section, we simulate 10000 times of spectrum sensing to verify the performance of the WSS algorithm. We set the local spectrum sensing parameters as shown in the table 1, and set the Byzantine attack probability \( \alpha_{01} \) and \( \alpha_{10} \) (the probability that the MU falsifies the sensing result \( S_i = 0 \) to \( R_i = 1 \) and the probability that the MU falsifies the sensing result \( S_i = 1 \) to \( R_i = 0 \)) to 0.5. The research could be also applied for other attacker probabilities.
Fig 3. The detection accuracy of various voting rules v.s. MUs ratio ($\alpha_{01} = 0.5, \alpha_{10} = 0.5$).

Fig 4. The detection efficiency of various voting rules v.s. MUs ratio ($\alpha_{01} = 0.5, \alpha_{10} = 0.5$).

Table 1. related parameter settings.

| $N$ | $P(H_0)$ | $P(H_1)$ | $P_f$ | $P_d$ | $g$ |
|-----|----------|----------|-------|-------|-----|
| 100 | 0.3      | 0.7      | 0.1   | 0.9   | -5  |
In Fig. 3, the detection accuracy of GV, S2V, WSPRT and WSS algorithms are presented. It can be seen that for GV and S2V, when the MU ratio $\rho$ is greater than 70%, the detection accuracy of these two algorithms begins to decline and finally drops to 0.8. For WSPRT, because of the reputation distribution mechanism, the detection accuracy $A$ is maintained at a high level when the MU proportion increasing. Because of the novel reputation update rule, the WSS algorithm we proposed goes further than WSPRT in terms of security performance.

In order to evaluate the CSS efficiency, the detection efficiency $\eta$ is defined as as

$$\eta = \frac{A}{N}$$  \hspace{1cm} (11)

where $A$ is the probability of correctly detection, and $N$ is the number of report samples?

In Fig. 4, we compare the efficiency of GV, S2V, WSPRT and WSS. It can be seen that for the ordinary voting rules GV and S2V, because they do not use the reputation value distribution mechanism, their efficiency is relatively low due to the low detection accuracy, but S2V uses the single symbol report rule, its efficiency is better than GV is slightly better. For WSPRT, due to the weight distribution mechanism, the security will be better. In addition, considering the advantage of the sequential detection, the sample size of WSPRT is also smaller. The proposed WSS reuses malicious data on the basis of WSPRT and uses a single symbol report mechanism, hence the efficiency is higher than the original WSPRT, which corroborates the effectiveness of WSS algorithm.

5. Conclusions
In this paper, we propose an efficient Byzantine defense algorithm for CSS of CRNs. To this end, on the one hand, we learn from the concept of reputation value to ensure the security of the algorithm. On the other hand, we make use of the single symbol report method to improve the efficiency of the algorithm. Therefore, a simple and effective WSS rule is also formulated to realize secure and efficient CSS against Byzantine attack. Through simulation, it is demonstrated that WSS achieves a reduction in report sample size in the presence of Byzantine attacks.

Acknowledgments
This work is supported by the 2020 Annual Teachers' Professional Development Project of Domestical Visiting Scholars in Institutions of Higher Education (No. FX2020009) and the Fundamental Research Funds for the Provincial Universities of Zhejiang (No. GK209907299001-023).

References
[1] L. Zhang, G. Ding, Q. Wu and F. Song, "Defending against byzantine attack in cooperative spectrum sensing: Defense reference and performance analysis," IEEE Access, vol. 4, pp. 4011-4024, 2016, doi: 10.1109/ACCESS.2016.2593952.
[2] A. S. Rawat, P. Anand, H. Chen and P. K. Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks," IEEE Transactions on Signal Processing, vol. 59, no. 2, pp. 774-786, Feb. 2011, doi: 10.1109/TSP.2010.2091277.
[3] 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, March 2010, doi: 10.1109/LCOMM.2010.03.092240.
[4] 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, doi: 10.1109/TVT.2019.2931949.
[5] 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, doi: 10.1109/TWC.2017.2707407.
[6] 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,
[7] 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, doi: 10.1109/JIOT.2020.2987843.

[8] 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, doi: 10.1109/JIOT.2017.2753579.

[9] 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, 1 Sept. 2019, doi: 10.1109/TMC.2018.2869390.

[10] J. Wu, Y. Yu, T. Song 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, April 2019, doi: 10.1109/LWC.2018.2877665.

[11] J. Wu, T. Song, Y. Yue, Y. W. Cong, J. Hu, "Sequential cooperative spectrum sensing in the presence of dynamic byzantine attack for mobile networks," PLoS ONE, vol. 13, no. 7, pp. e0199546, 2018, doi: 10.1371/journal.pone.0199546.

[12] R. Chen, J. Park and K. Bian, "Robustness against byzantine failures in distributed spectrum sensing," Computer Communications, vol. 35, no. 17, 2115-2124, 2012, doi: 10.1016/j.comcom.2012.07.014.