Identification and Elimination of Abnormal Information in Electromagnetic Spectrum Cognition

Haojun Zhao[1], Ruowu Wu[2], Hui Han[2], Xiang Chen[2], Yuyao Li[1], and Yun Lin[1(✉)]

[1] College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China
linyun_phd@hrbeu.edu.cn
[2] State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System (CEMEE), Luoyang 471003, Henan, China

Abstract. The electromagnetic spectrum is an important national strategic resource. Spectrum sensing data falsification (SSDF) is an attack method that destroys cognitive networks and makes them ineffective. Malicious users capture sensory nodes and tamper with data through cyber attacks, and make the cognitive network biased or even completely reversed. In order to eliminate the negative impact caused by abnormal information in spectrum sensing and ensure the desired effect, this thesis starts with the improvement of the performance of cooperative spectrum sensing, and constructs a robust sensing user evaluation reference system. At the same time, considering the dynamic changes of user attributes, the sensory data is identified online. Finally, the attacker identification and elimination algorithm is improved based on the proposed reference system. In addition, this paper verifies the identification performance of the proposed reference system through simulation. The simulation results show that the proposed reference system still maintain a good defense effect even if the proportion of malicious users in the reference is greater than 50%.

Keywords: Cognitive radio · Cooperative spectrum sensing · Spectrum sensing data falsification (SSDF) · Bayesian learning

1 Introduction

Secondary users in cognitive radio jointly explore spectrum holes through cooperative spectrum sensing (CSS), thereby effectively utilizing the idle spectrum and reducing the impact on the primary users. This is an effective means to improve spectrum utilization and solve spectrum shortages. However, the emergence of malicious attacks, especially spectrum sensing data falsification, poses a serious threat to cooperative spectrum perception, causing the fusion center to make false perceptions and ultimately undermine the performance of the entire cognitive network [1].

Therefore, spectrum sensing data falsification has received widespread attention, and many researchers have proposed different identification and defense solutions from

S. Liu and G. Yang (Eds.): ADHIP 2018, LNICST 279, pp. 77–88, 2019.
https://doi.org/10.1007/978-3-030-19086-6_9

multiple perspectives. Literature [2] proposed a sensing user anomaly detection scheme based on data mining. The biggest advantage of this scheme is that the Fusion Center (FC) does not need to know the user's prior information in advance, and is closer to our actual life. Literature [3] analyzes the limit performance of cooperative spectrum sensing under Byzantine attack. This method identifies and removes the attacker before data fusion, which is easy to implement and can eliminate malicious users in a short time, but also leads to users. The analysis of dynamic interactions with the fusion center is missing. In order to ensure the stability of spectrum sensing, the literature [4] studied a scheme of trusted node help based on the user's reputation value. When the user's reputation value reaches the set threshold value and thus improves the perceived stability, the user's sentiment information will be uploaded to the Fusion Center for integration. In [5], the authors propose a distributed scheme using spatial correlation and anomaly detection, which is used to receive signal strength between adjacent SUs to detect malicious users in cooperative spectrum sensing. The authors in [6] studied the use of Bayesian methods to deal with methods for secondary user attacks to enhance the robustness of cooperative spectrum sensing. The method uses a statistical attack model, and each malicious node has a certain degree of attack probability.

Based on the methods mentioned in different literatures, this paper studied the robust perceptual user evaluation reference system based on reputation value, and then considering the dynamic change of user attribute, the online identification mechanism is introduced. Finally, the attacker identification and elimination algorithm is improved based on the proposed reference system, which eliminated the impact of abnormal data on the perceived performance under the combined effect.

2 System Model

2.1 Perceptual Process

In order to determine whether the licensed band is occupied by a Primary User (PU), each secondary user (SU) can use an energy detection scheme for sensing. For each secondary user, CSS can often be regard as a binary hypothesis test with the following formula [7]:

$$\begin{cases} H_0 : r(t) = n(t) \\ H_1 : r(t) = h(t)P_0(t) + n(t) \end{cases} \tag{1}$$

The working status of the licensed band can be divided into H_0 and H_1. H_0 indicates that the frequency band operates in an idle state, and H_1 indicates that the frequency band operates in a busy state. $r(t)$ is the received signal strength at time t, $n(t)$ is Gaussian white noise, $P_0(t)$ is the signal transmitted by the primary user, and $h(t)$ is the channel gain of the authorized user to the perceived user.

At the same time, two metrics are introduced, the detection probability P_d and the false alarm probability P_f, λ is the determine threshold.

$$\begin{cases} p_f = P(v_i = 1|H_0) = Q(\dfrac{\lambda - \mu_0}{\sigma_0}) \\ p_d = P(v_i = 1|H_1) = Q(\dfrac{\lambda - \mu_1}{\sigma_1}) \end{cases} \tag{2}$$

Among them, $\mu_0 = 2U, \sigma_0^2 = 4U, \mu_1 = 2U(\beta + 1), \sigma_1^2 = 4U(2\beta + 1), \beta$ is the signal to noise ratio received by the SU, $Q(z) = \frac{1}{\sqrt{2\pi}} \int_z^\infty e^{-\frac{x^2}{2}} dx$, which is the complementary cumulative distribution function of the standard normal distribution.

2.2 Perceptual Process

In cooperative spectrum sensing, the local decision result of each secondary user i is represented by the final FC global decision result. Considering the perceptual information of the upload error in the sensing process, the perceptual error probability Pc is introduced here, combined with the formula (2), there are:

$$\begin{cases} p'_f = p_f \cdot (1 - p_c) + (1 - p_f) \cdot p_c \\ p'_d = p_d \cdot (1 - p_c) + (1 - p_d) \cdot p_c \end{cases} \tag{3}$$

In order to better analyze the impact on the sensing network, the attack probability is also introduced into the spectrum falsifying frequency. When the authorized band sensing result is idle, the probability that the malicious user reports as busy is P_a, when the perceived frequency of the authorized band is busy, the probability that a malicious user reports as idle is P_b. The relevant perceptual performance formulas of malicious users after passing SSDF are:

$$\begin{cases} p_f^b = p_f \cdot (1 - p_b) + (1 - p_f) \cdot p_b \\ p_d^b = p_d \cdot (1 - p_a) + (1 - p_d) \cdot p_a \end{cases} \tag{4}$$

Considering the probability of transmission errors in the data reporting process, the false alarm probabilities of the honest and malicious users, and the detection probabilities are as follows.

For honest users, there are:

$$\begin{cases} p_f^H = p_f \cdot (1 - p_e) + (1 - p_f) \cdot p_e \\ p_d^H = p_d \cdot (1 - p_e) + (1 - p_d) \cdot p_e \end{cases} \tag{5}$$

For malicious users, there are:

$$\begin{cases} p_f^B = p_f^b \cdot (1 - p_e) + (1 - p_f^b) \cdot p_e \\ p_d^B = p_d^b \cdot (1 - p_e) + (1 - p_d^b) \cdot p_e \end{cases} \tag{6}$$

3 Robust Perceptual User Evaluation Reference System

3.1 Review of Existing Reference Systems

In order to eliminate the negative impact of abnormal information on the electromagnetic spectrum, the existing defense reference system can be roughly divided into:

Global decisions as a reference (GDaR) [3, 8]. The final judgment is obtained by data fusion of the reported results of all the sensing nodes. Therefore, after the proportion of malicious users is greater than that of the honest users, the reference system will be invalid.

Trusted sensor's reports as a reference (TRaR) [4, 9]. The reference system assumes that some honest user sensors are known to the primary user, and the reported results are approximated by the true spectrum state and used to assess the reported values of other sensors.

3.2 The Proposed Reference System

Based on the limitations of the existing reference system performance, this paper discusses and proposes a robust cognitive user evaluation reference system.

The entire testing process consists mainly of the learning phase and the decision phase. The learning phase consists of a large segment of perceptual time slots in which the reference system will evaluate the perceptual users and update their reputation values cumulatively. Specifically, when the user is perceived as an attacker at a certain moment, the reputation value will be processed by +1. In the subsequent judgment stage, the obtained reputation value is compared with the credit threshold to judge the attribute of the current cognitive user.

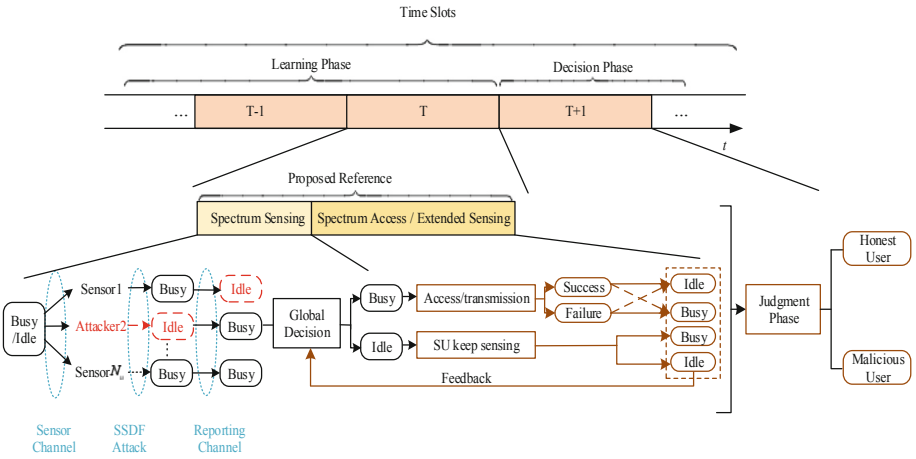


Fig. 1. The cognitive user evaluation reference system

As shown in Fig. 1, the sensing node reports the local sensing result, and the FC makes a decision on the band status according to the result of the fusion. However, due to the limitation of the decision mode, the result of the global decision alone is not reliable and cannot be given. Other perceptual users provide a reference. Therefore, the proposed reference combines the feedback information of the transmission result and the sensing mechanism of the full time slot. Specifically, when the frequency band working state of the global decision is busy, that is, when the global decision result $F = 1$, the SU or the FC continues to perceive, because the sensing performance of the SU itself may greatly increase with the sensing time slot. Increase, so a moderate expansion in time can improve its perceived performance. On the other hand, when the global decision result $F = 0$, that is, when the globally determined band operating state is idle, the SU will access the band to transmit data, and the following two situations often occur: the SU successfully accesses the licensed band, or the SU pair Access to the licensed band failed. In the case, if the SU successfully accesses the frequency band, then the result of the global decision F is correct. Otherwise, the result of the global decision F is wrong.

Obviously, after the SU access grant band transmission, there is an inferred error probability: $P(success|F = 0, H_1)$, that is, the probability of successful transmission when the band status is busy, and the probability $P(failure|F = 0, H_0)$ of failure transmission when the band status is idle.

4 Anomaly Identification Mechanism Based on Bayesian Learning

4.1 Bayesian Batch Learning Algorithm

To make the most of the historical data of spectrum sensing, this chapter first learns the known sample data D_T through the Bayesian batch learning algorithm, and combines the data $\mathbf{u}$ reported by the user in different time slots, realized the state judgment of the current authorized band H through secondary users.

In the cognitive wireless network, every i of the SU corresponds to an attribute w_i. Specifically, the attribute wi takes -1 or 1, 1 represents the user as an honest attribute, and -1 represents the user as a malicious attribute. Each SU has a corresponding weight k_i to measure the reputation. The weight ranged from 0 to 1. We can assume that the initial value of k_i is 0.5. Considering the independent features between samples, the joint probability $p(w)$ can be expressed as a multiplicative form:

$$p(\mathbf{w}) = \prod_i [k_i \delta(w_i - 1) + (1 - k_i)\delta(w_i + 1)] \tag{7}$$

From the literature [10], the posterior probability of the working state of the predicted licensed band can be expressed as follows:

$$p(H|\mathbf{u}^{T+1}, D_T) = \int p(H|\mathbf{w}, \mathbf{u}^{T+1}) p(\mathbf{w}|D_T) d\mathbf{w} \tag{8}$$

The Bayesian predicted H is:

$$H^{Bayes}(\mathbf{u}^{T+1}, D_T) = \mathrm{U}(\int \mathrm{U}(\mathbf{w} \cdot \mathbf{u}^{T+1}) p(\mathbf{w}|D_T) d\mathbf{w}) \tag{9}$$

4.2 Bayesian Online Learning Algorithm

Consider a more general and practical way of attack. User attributes are no longer fixed, but exhibit time-varying. At this point, the perceived user's performance in the historical phase is quite different from the real-time spectrum sensing result. In response to this situation, this section proposes an online algorithm based on Bayesian principle (Fig. 2).

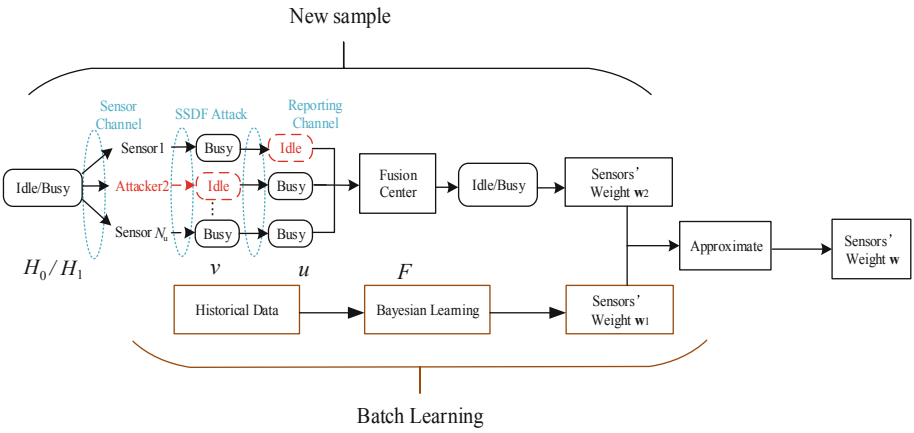


Fig. 2. Bayesian online learning identification mechanism

In general, the online learning model combines real-time learning of current perceptual data on the basis of a batch learning reference system based on Bayes theorem. In the batch learning phase, the Bayesian learning method is used to train the historical data of the cognitive users. Through the continuous iteration of the data to optimize the distribution $p(\mathbf{w})$ of the network parameters $\mathbf{w}$, the user can be found in the system. The weight value w_1. Then, for the current perceptual data, the user is assigned a weight value w_2 through the analysis processing of the system. The weight w_1 and the weight w_2 value are comprehensively processed, and finally the perceived weight of the user w is obtained.

The main idea of Bayesian online learning is to combine the results obtained from historical data with the results obtained from current data, and finally come to new conclusions. The advantage of such a process is that the historical data and the current data are taken into account first, so that the conclusions obtained are more reasonable; in addition, it is more in line with the actual situation, and the data is processed dynamically.

After observing the perceptual data $(F^{T+1}, \mathbf{u}^{T+1})$, the new observations are updated with the formula (8), and the online posterior probability after adding new data samples by the Bayesian criterion is [11]:

$$p(\mathbf{w}|D_T, (F^{T+1}, \mathbf{u}^{T+1})) \frac{p(F^{T+1}|\mathbf{w}, \mathbf{u}^{T+1})p(\mathbf{w}|D_T)}{\int p(\mathbf{w}|D_T)p(F^{T+1}|\mathbf{w}, \mathbf{u}^{T+1})d\mathbf{w}} \tag{10}$$

5 Abnormal Data Elimination Based on Proposed Reference System

5.1 Identification of Abnormal Data

As can be seen from Fig. 3, the reference system will evaluate the sensing nodes in each time slot, and update their reputation values cumulatively, and distinguish between honest data and malicious data according to the last obtained reputation value. Each sensing node is assigned a measured reputation worth indicator, indicating the number of times the final decision A of the reference system in the T-slot is inconsistent with the reported result u of the node i. The reputation value n_i of the perceived node can be shown as:

$$n_i = \sum_{t=1}^{T} \mathrm{I}_{(F[t] \neq u_0[t])} \tag{11}$$

Where I is an indication function, it can be found that the higher the reputation value of the sensing node, the more likely the uploaded sensing data is not adopted by the fusion center. Comparing the reputation value of the node n_i with the set threshold η, finally we can identify the abnormal user or abnormal data:

$$\begin{cases} n_i > \eta, & \text{attacker} \\ n_i < \eta, & \text{honest sensor} \end{cases} \tag{12}$$

5.2 Elimination of Abnormal Data

In order to measure the elimination of the anomaly data by the reference system, two indicators P_B^{iso} and P_H^{iso} are proposed here to measure the recognition and elimination of malicious users by the system. P_H^{iso} indicates the probability that an honest user is misjudged as a malicious user by the reference system after T time slots and is removed from the fusion center [3]:

$$P_H^{iso} = P(n_i > \eta) = \sum_{j=\eta+1}^{T} \binom{T}{j} P_H^j (1 - P_H)^{T-j} \tag{13}$$

And P_B^{iso} represents the probability that the malicious user is identified and eliminated by the reference after T time slots:

$$P_B^{iso} = P(n_i > \eta) = \sum_{j=\eta+1}^{T} \binom{T}{j} P_B^j (1 - P_B)^{T-j} \tag{14}$$

P_B and P_H indicate the probability that the perceived data reported by the malicious user and the honest user are different from the FC decision results. In the eliminating process, the reputation value is used to identify the malicious attack user. By sensing the n_i comparison with the threshold η, and then the sensory node whose reputation value is greater than the threshold is judged as a malicious node, the reported data can be regarded as abnormal data. It is then removed from the cooperative spectrum perception.

5.3 Threshold and Efficient Purification Standards

For the threshold η in the proposed reference, the selection of η plays an important role in whether the system can efficiently complete data purification. If the threshold is low, some honest nodes will be mistakenly judged as malicious users, thus eliminating normal data. Conversely, if the threshold is set higher, it will make it difficult for a malicious user to be identified, and eventually the elimination of the abnormal information cannot be completed. Mathematically, optimization tries to satisfy the following effects:

$$\max_{\eta} (P_B^{iso} - P_H^{iso}) \tag{15}$$

For the above problems, the optimal threshold obtained after optimization are as follows:

$$\eta_{opt} = \left\lceil T \frac{\ln\left(\frac{1-P_H}{1-P_B}\right)}{\ln\left(\frac{P_B(1-P_H)}{P_H(1-P_B)}\right)}) \right\rceil \tag{16}$$

Among them, this $\lceil \cdot \rceil$ represents the rounding function, and the threshold is rounded up. A detailed derivation of the formula can be found in [11–13].

6 Performance Analysis

6.1 Simulation Parameter Settings

In the simulation, 100 cognitive nodes are set to participate in the process of cooperative spectrum sensing. The probability that the authorized band works in the busy state is set to 0.2, $P_f^H = 0.2$, $P_d^H = 0.8$, $pb = P_{mal} = 1$. The simulation results took the

average of 2000 trials. In order to reflect the superior performance of the proposed scheme, it is compared here with the Global decisions as a reference (GDaR) [14].

6.2 Analysis of Results

Figure 3 shows the change in the weight value and sensing node attributes with the time slot. It can be concluded that as the user attributes change, the proportion of users in data fusion changes accordingly. Since the properties of the sensing node oscillate between 1 and −1, the weights also increase or decrease dynamically. When the user presents a malicious attribute at a certain stage, the proportion of the data fusion is reduced. Conversely, if the user presents an honest attribute at the next moment, the proportion of the data fusion will increase. From the results, online learning has better adaptability to the situation when the user attribute changes dynamically. The changes presented by the perceived data can be processed in real time, and the system as a whole maintains excellent performance.

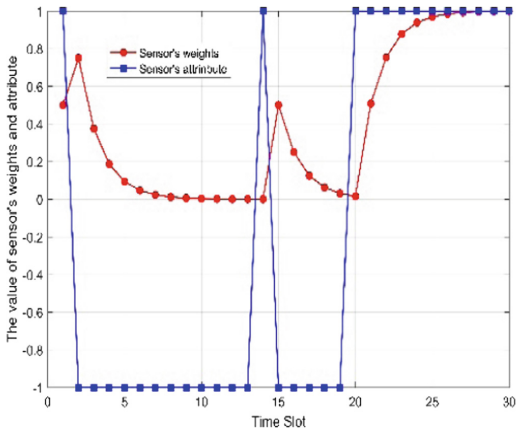


Fig. 3. The weight value and attribute of the sensory node change with the time slot

Figure 4 shows a comparison of false alarm probability and detection probability with Bayesian online learning and batch learning. Obviously, the performance of Bayesian online learning is further improved with the increase of time slots, and the overall performance of Bayesian batch learning is further reduced. From the perspective of false alarm probability, the performance of online learning algorithms is always better than the performance of batch learning. From the detection probability, with the increase of time slot, the performance of Bayesian batch learning algorithm decreases, and the performance of online learning seems better, and finally approaches 1 near. It can be seen that online learning has better adaptability to the situation when the user attribute changes dynamically, which reflects its reliability and feasibility.

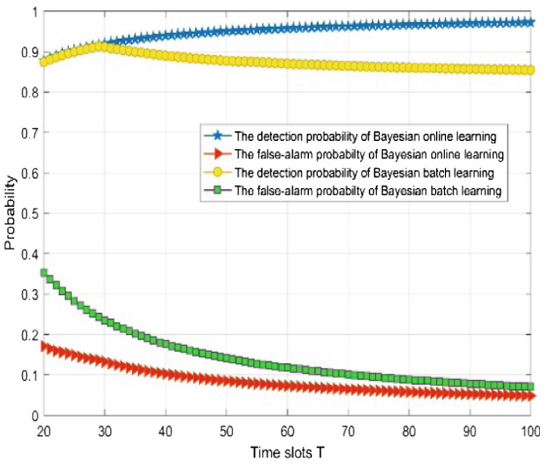


Fig. 4. Bayesian online learning and batch learning P_d and P_f changes with time slot T

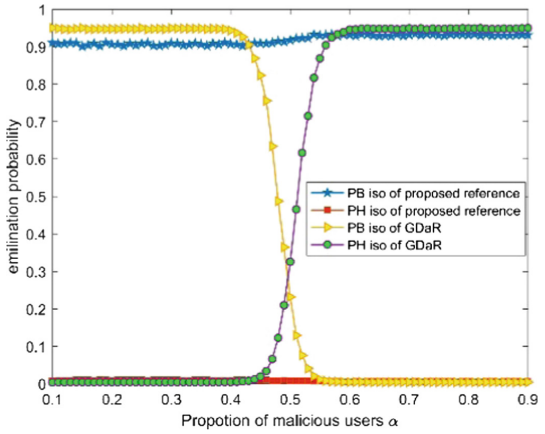
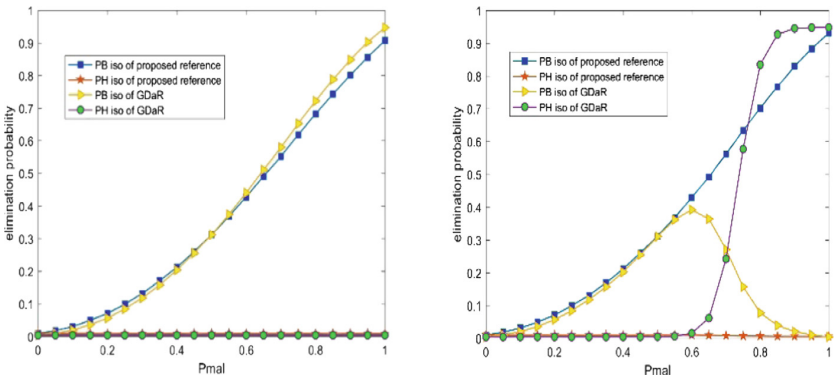


Fig. 5. Changes of P_B^{iso} and P_H^{iso} with attack users proportion α in two reference systems

Figure 5 shows the probability of a malicious user and an honest user being identified and eliminated in two references with the change of malicious users proportion α as follows. It can be found that the proportion α has little effect on the proposed reference system, and it always maintaining excellent performance. In contrast, with the increase of α, the performance of GDaR began to become unstable, especially when α is greater than 0.4, the GDaR reference system is reversed, and when it is greater than 0.5, the GDaR reference system is completely ineffective. This result shows the robustness of the proposed reference.



(a) $\alpha = 0.3$ (b) $\alpha = 0.7$

Fig. 6. Changes in two references and with the attack probability P_{mal}

Figure 6 shows the probability of malicious users and honest users being identified and eliminated under two references with the malicious attack probability P_{mal}. Figure 6(a) is a simulation when $\alpha = 0.3$. It can be seen that when the number of attackers is low, both reference systems maintain a relatively stable state. As the attack probability P_{mal} increases, the probability of the honest users elimination is close to 0, and the malicious user is identified and the probability of elimination is constantly rising. When $\alpha = 0.7$, it can be concluded from Fig. 6(b) that the elimination performance of the reference is basically the same as that at 0.3, which is stable and effective. However, the performance of GDaR increases with the probability of attack P_{mal}. The probability of elimination of honest users increases first and then increases. The probability of elimination of malicious users is the same as that of the reference system, and then gradually decreases to zero. In summary, the GDaR reference system exhibits similar performance to the proposed reference at $\alpha > 0.5$, with performance deteriorating at $\alpha > 0.5$, and the proposed reference is still stable.

7 Conclusion

This paper focuses on SSDF attacks in cooperative spectrum sensing, studied the robust perceptual user evaluation reference system based on reputation value, then introduced the online identification mechanism considering the dynamic change of user attribute. At last this paper improved the attacker identification and elimination algorithm based on the proposed reference. The simulation results verify the validity and robustness of the proposed reference system, and complete the online identification mechanism for dynamic users, which eliminates the influence of abnormal information on the reference system under the comprehensive effect.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (61771154), the Fundamental Research Funds for the Central Universities (HEUCFG20 1830), and the funding of State Key Laboratory of CEMEE (CEMEE2018K0104A).

This paper is also funded by the International Exchange Program of Harbin Engineering University for Innovation-oriented Talents Cultivation.

Meantime, all the authors declare that there is no conflict of interests regarding the publication of this article.

We gratefully thank of very useful discussions of reviewers.

References

1. Benjamin, R.: Security considerations in communications systems and networks. In: Communications Speech & Vision IEEE Proceedings I, vol. 137, no. 2, pp. 61–72, April 1990
2. Li, H., Han, Z.: Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks. IEEE Trans. Wirel. Commun. **9**(11), 3554–3565 (2010)
3. Rawat, S., Anand, P., Chen, H., et al.: Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks. IEEE Trans. Signal Process. **59**(2), 774–786 (2011)
4. Zeng, K., Paweczak, P., Cabri, D.: Reputation-based cooperative spectrum sensing with trusted nodes assistance. IEEE Commun. Lett. **14**(3), 226–228 (2010)
5. Chen, C., Song, M., Xin, C., et al.: A robust malicious user detection scheme in cooperative spectrum sensing. In: Proceedings of the IEEE Global Telecommunication Conference, pp. 4856–4861 (2012)
6. Penna, F., Sun, Y., Dolecek, L., et al.: Detecting and counteracting statistical attacks in cooperative spectrum sensing. IEEE Trans. Signal Process. **60**(4), 1806–1822 (2012)
7. Urkowitz, H.: Energy detection of unknown deterministic signals. Proc. IEEE **55**(4), 523–531 (1967)
8. Chen, R., Park, J.M., Bian, K.: Robust distributed spectrum sensing in cognitive radio networks. In: INFOCOM 2008, Phoenix, AZ, 13–18 April 2008
9. He, X., Dai, H., Ning, P.: A byzantine attack defender in cognitive radio networks: the conditional frequency check. IEEE Trans. Wirel. Commun. **12**(5), 2512–2523 (2013)
10. Solla, S.A., Winther, O.: Optimal perceptron learning: an on-line Bayesian approach. In: Saad, D. (ed.) On-Line Learning in Neural Networks, pp. 379–398. Cambridge University Press, Cambridge (1998)
11. Noh, G., Lim, S., Lee, S., et al.: Goodness-of-fit-based malicious user detection in cooperative spectrum sensing. In: Proceedings of the 76th IEEE Vehicular Technology Conference, pp. 1–5 (2012)
12. Althunibat, S., Denise, B.J., Granelli, F.: Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment. IEEE Trans. Veh. Technol. **65**(9), 7308–7321 (2016)
13. Zhao, Y., Song, M., Xin, C.: A weighted cooperative spectrum sensing framework for infrastructure-based cognitive radio networks. Comput. Commun. **2011**(34), 1510–1517 (2011)
14. Jo, M., Han, L., Kim, D.: Selfish attacks and detection in cognitive radio ad-hoc networks. IEEE Network **27**(3), 46–50 (2013)