International Journal of Hybrid Information Technology
Vol.8, No.9 (2015), pp.269-280
http://dx.doi.org/10.14257/ijhit.2015.8.9.25

A Credibility-based Defense SSDF Attacks Scheme for the Expulsion of Malicious Users in Cognitive Radio

Hong Du[1], Shuang Fu[1] and Hongna Chu[2]

[1] *College of information technology, Heilongjiang Bayi Agricultural University, Daqing, China, 163319*
[2] *Beijing Branch, Daqing Oilfield Information Technology Company, Beijing, China, 100043*
duhong929@163.com; fushuang_dq@163.com

Abstract

Cognitive radio (CR) can improve the utilization of the spectrum by making use of licensed spectrum in an opportunistic manner. However, the security aspects of cognitive radio networks have garnered little attention. In this paper, we identify a threat to cognitive radio networks, which we call the spectrum sensing data falsification (SSDF) attack. SSDF attack can hugely degrade the achievable detection accuracy. To counter this threat, we proposed a new method to confront the SSDF attacks by excluding malicious users is cognitive radio. In detail, the proposed scheme defense the SSDF attacks by calculating and updating the credit value of the Secondary Users (SUs), malicious users are excluded to avoid the attacks affect in cooperative spectrum sensing. Simulations results show that both the detection probability and the false alarm probability are significantly improved compared to the case when all users are by default trusted to be normal users.

Keywords: *Cognitive Radio; Spectrum Sensing; SSDF Attacks, Credibility-Based; Malicious Users*

1. Introduction

Cognitive radio technology can not only improve the utilization of the spectrum, but also introduces a number of new security threats. In untrusted cognitive radio networks, security threats attacks by malicious users on the one hand may cause harmful interference to authorized users, on the other hand can also cause cognitive users to lose opportunities access to the spectrum.

In cognitive radio networks (CRNs), the main function of the physical layer is to detect and take advantage of free spectrum for data transmission. Therefore, the ability to sense the presence of the primary user (PU) correctly and quickly is a prerequisite for cognitive radio applications. When the primary user does not exist on the detected band, the cognitive user can use this band. In order to overcome the individual cognitive user susceptible to hidden terminal problems, multi-user cooperative spectrum sensing techniques have been proposed. Currently, most of the literature on cooperative spectrum sensing in the study, each cognitive user is generally assumed to be safe and reliable. However, in actual wireless environment, there are a variety of threats to system security. Therefore, it is necessary to analyze the influence on cooperative sensing performance from the malicious user's attack and further study the defense attack strategy accordingly in cognitive wireless networks. Typically, physical layer security threats in a cognitive radio network can be divided into Jamming Attack (JA), Primary User Emulation (PUE) attacks and Spectrum Sensing Data Falsification (SSDF) attack. The appropriate security

ISSN: 1738-9968 IJHIT

defenses scheme was investigated to confront the threats attacks above, the adverse effects can be eliminated which was caused by the malicious user.

Spectrum sensing data falsification attacks and defenses has been studied in previous work. In [1], the author develops a dynamic trust management scheme to reliably detect and mitigate SSDF attacks. In [2], the author proposes a distributed density to countermeasure the SSDF attack. In [3], the proposed algorithm assigns a specific weight to each user, which is able to completely eliminate the resulting effects on spectrum sensing caused by many types of SSDF attacks. In [4], the author proposes a reputation based adaptive clustering algorithm to defense against cooperative SSDF attacks. In [5], an attacker-punishment policy is proposed. The proposed policy is based on relating the scheduling probability for each user to its sensing performance, representing a punishment for attackers and a reward for honest users. In [6], the author proposes an abnormality detection algorithm to detect attackers. The only information we need to know is the bit error probability on secondary users' reporting channel. In [7], the author introduces a simple yet efficient technique to counter the SSDF attack. It makes use of primary user's Received Signal Strength at an SU to localize its position and compare this with that calculated using received signal strength of SU transmissions at data fusion center. In [8], the author proposes the utility self-information and the real utility entropy of information, which extends the range of information entropy from non-negative numbers to real numbers. In [9], the author proposed a similarity-based clustering of sensing data to counter the above attack. In [10], the author proposes a reputation based clustering algorithm that does not require prior knowledge of attacker distribution or complete identification of malicious users. We provide an extensive probabilistic analysis of the performance of the algorithm. In [11], the author proposes a defense scheme using trust, called Sensing Guard, to counter SSDF attack. This scheme provides a novel approach to evaluate the trustworthiness of SUs by analyzing their previous behaviors. In [12], a novel trusted sequential probability ratio test scheme based on beta function is proposed to avoid the intermittent spectrum sensing data falsification attack.

However, the mentioned methods to defense the SSDF attacks do not consider the different attack scenarios. In this paper, we illustrated different types of SSDF attack scenario, and proposed a new method to defense the SSDF attacks in CRNs by calculating and updating the credit value of the SUs, malicious users are excluded to avoid the attacks affect in cooperative spectrum sensing. The optimal decision rule for cooperative sensing is investigated with new trust spectrum sensing scheme. This method not only makes the SSDF attacks detection is more clear and concise, and greatly improves the detection accuracy.

The rest of the paper is organized as follows. In Section 2, we introduced the system model of SSDF attack in a cognitive radio network. In Section 3, we described effects on collaborate spectrum sensing performance from malicious users. In Section 4, we proposed the method of defensing SSDF attack by expulsing the malicious users. In Section 5, we provide the simulation results and discussion. Finally, Section 6 concludes this paper.

2. System Model

In the study of cooperative spectrum sensing techniques, all cognitive users are assumed normal usually. But in the actual network environment, it is impossible to ensure that all cognitive users will normally send the correct spectrum sensing results. In untrusted wireless network, a malicious attacker sends the wrong local sensing results to the fusion center, ultimately resulting in the fusion center to make the wrong decision.

In SSDF attack, a malicious user falsify the local spectrum sensing results, sends the wrong results to the fusion center, which affect the accuracy of judgment. SSDF attacks scene is usually divided into: a malicious user can always send "1", "0", and the results

contrast with the real data. If a malicious user can always send "1", it will greatly reduce the spectrum utilization in a wireless network; if a malicious user can always send "0", it will cause serious interference to authorized users, but also affect the quality of communication for cognitive users; The most serious effect is that a malicious user always send the results contrast with the real data, which cause interference to authorized users to a certain extent, but also reduces the chance of legal cognitive uses to access to the free band of authorized users.

2.1 Scene Model

In cooperative spectrum sensing, a malicious attacker sends the wrong local sensing result, attackers forced to modify the real test results, it always sends "0" or "1", or the results contrast with the real data, then send the modified results to the fusion center, thereby affecting the final judgment of the data fusion center.

Figure 1 shows that malicious users bring the security threats scene with false sensing in cooperative spectrum sensing. The cognitive wireless network includes an authorization primary system, a cognitive base station, a number of cognitive users and malicious users. Assuming that the cognitive user carried out the cooperative spectrum sensing, and sensing results are independent. Cognitive base station makes the final decision with fusion rules, and informs the use results of licensed spectrum users to the cognitive users. The above-described information exchange are based on the specific control channels, without loss of generality, it is assumed that the channel is an ideal channel.

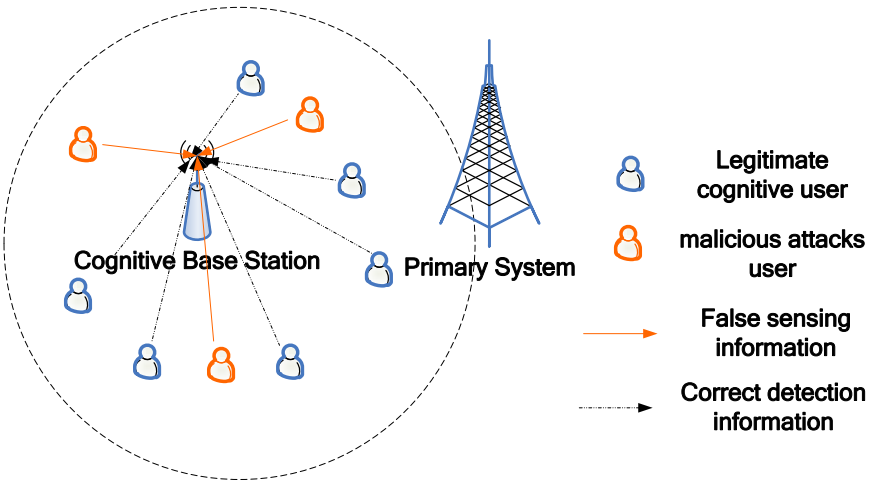

Figure 1: The false sensing information for malicious user in cooperative spectrum sensing scene

2.2 Energy Detection Model

In cognitive radio networks, each cognitive user performs energy detection technology, energy levels was detected to determine whether there is an authorized user. Assuming that $x(t)$ denotes the received signal by cognitive user, $s(t)$ denotes the signal emitted by the primary user, h denotes the channel gain, $n(t)$ denotes the additive white Gaussian noise. Spectrum sensing can be attributed to the binary hypothesis testing problem:

$$x(t) = \begin{cases} n(t), & H_0 \\ hs(t) + n(t), & H_1 \end{cases} \quad (1)$$

Where H_1 and H_0 represent the existence or not of the primary user.

The time-domain signal samples was modulo and square in energy detection, test statistic $T(x)$ was obtained, namely:

$$T(x) = \frac{1}{M}\sum_{t=1}^{M}\left|x(t)\right|^2 \quad (2)$$

Where M denotes the number of samples.

For the threshold value ε , the probability of detection P_d and the false alarm probability P_f can be expressed as:

$$P_d = P_r(T(x) > \varepsilon \left| H_1 \right.) = Q\left(\left(\frac{\varepsilon}{\sigma_u^2} - \gamma - 1 \right) \sqrt{\frac{M}{2\gamma + 1}} \right) \quad (3)$$

$$P_f = P_r(T(x) > \varepsilon \left| H_0 \right.) = Q\left(\left(\frac{\varepsilon}{\sigma_u^2} - 1 \right) \sqrt{M} \right) \quad (4)$$

Where the parameter γ is the signal to noise ratio, σ_u^2 is the noise variance.

For a given target false alarm probability $\overline{P}_f$, substitute the formula (4) into (3), the detection probability can be expressed as

$$P_d = Q\left(\frac{1}{\sqrt{2\gamma + 1}} \left(Q^{-1}(\overline{P}_f) - \sqrt{M}\,\gamma \right) \right) \quad (5)$$

For cooperative spectrum sensing, the information fusion center deals with the received sensing results for all cognitive users, and outputs the final decision. Suppose there are N cognitive users to participate in collaborative spectrum sensing, detection probability P_d and false alarm probability P_f denote the local detection performance of each cognitive user, assuming each cognitive user's sensing are independent and with the same performance, namely $P_{d,j} = P_{d,0}$, $P_{f,j} = P_{f,0}$, j=1,...,N. Q_d and Q_f represent the probabilities of collaborative detection and collaborative false alarm for fusion center collaborative detection performance.

3. Analysis of Influence on the Cooperative Spectrum Sensing With Attack from Malicious User

For the SSDF attack in cognitive radio networks, the result is that the fusion center may receive an incorrect sensing results, it can be divided into two attack scenarios: (1) whether or not the presence of an authorized user, a malicious attacker always sends "0" or "1"; (2) malicious attackers always sends results on the contrary to the real. Intuitively, the second case is more severe than the first one. Therefore, the second attack was selected to be analyzed the impact on cooperative spectrum sensing performance for the main emphasis.

Assuming that the number of cognitive users is N, the number of malicious users is k ($1<k<N$), attack scenario is that malicious attackers always sends results on the contrary to the real. Because the threat of above case is more severe and harsh, therefore, q-out-of-N rule is adopted to investigate the collaborative sensing performance under the above attack scenario, which is more eclectic with respect to the AND and OR rules. By using q-out-of-N rules, as long as q cognitive users judge that there exists the authorize user, the detection result is that authorized user exist.

When an authorized user exists, the judgment of k malicious user is that the authorized user does not exist. When *N-k>q*, the number of reliable cognitive users is more than q values, so the judge rule is q-out-of-N-k; and when *N-k<q*, the number of reliable cognitive users is less than q, therefore the detection results of malicious users determines the final verdict, the presence of an authorized user cannot be detected ultimately.

Therefore, for the q-out-of-N rule, the cooperative detection probability Q_d can be expressed as:

$$\begin{cases} Q_d = \sum_{j=q}^{N-k} \binom{N-k}{j} P_d^{\,j} (1-P_d)^{N-k-j}, & N-k > q \\ Q_d = 0, & N-k < q \end{cases} \tag{6}$$

Similarly, when an authorized user does not exist, *k* malicious users will send the presence information of an authorized user. When *N-k>q*, the number of reliable cognitive users is more than *q* values, the judge rule is q-out-of-N-k; when *N-k<q*, the number of reliable cognitive users is less than *q*, therefore the detection results of malicious users determines the final verdict, the presence of an authorized user was reported always.

Therefore, the probability of collaborate false alarm Q_f by using q-out-of-N rule can be expressed as:

$$\begin{cases} Q_f = \sum_{j=q-k}^{N-k} \binom{N-k}{j} P_f^{\,j} (1-P_f)^{N-k-j}, & N-k > q \\ Q_f = 1, & N-k < q \end{cases} \tag{7}$$

4. A Scheme for Defense SSDF Attack Based On Credibility By Excluding The Malicious User

In order to eliminate the impact of a malicious user to the collaborative detection performance, a defense attack scheme based on credibility is proposed. Specifically, after calculating the credit value of each cognitive user, not all users participate in the final judgment based on credit weighted, but by setting different thresholds (here set a higher threshold and a lower credit threshold), the user with lower than the minimum credit value is directly removed, the rest of the reliable users participate in the next spectrum sensing and judgments.

The proposed defense attack scheme consists of three components: compute the cognitive user's credit, removing the malicious users, and judge by reliable cognitive users. The user's credit was established by the sensing results, according to detection results of each cognitive user are consistent with the final decision or not, update the credit value. Then a weighted fusion rule was used to make a final judgment, the attributes of cognitive user was determined by comparing the reputation value and threshold. If the value is higher than the lower threshold, the users could participate in the next round of spectrum sensing; if the value is less than the minimum credit threshold, removing the user is not allowed to participate in the next cooperative sensing.

4.1 Computing the Credibility of Cognitive User

Assigned an initial credit value $r_i(0)$ for each cognitive user, the credibility value was associated with the reliability of the reported results. When the cognitive user's decision is consistent with the final decision, the credibility value plus 1, otherwise the credibility value minus 1. Here, the *i*-th cognitive user's reputation value at *j*-th sensing $r_i(j)$ can be calculated as follows:

$$r_i(j) = r_i(j-1) + (-1)^{d_i(j)+d(j)} \tag{8}$$

Where, *d(j)* means the results of the final decision, $d_i(j)$ denotes the *i*-th cognitive user's decision-making, which is calculated as follows:

$$d_i(j) = \begin{cases} 1, & \text{if } T_i(j) \geq \lambda \\ 0, & \text{otherwise} \end{cases} \quad (9)$$

Wherein, $T_i(j)$ represents the obtained energy value of *i*-th cognitive user with *j*-th sensing, λ represents the decision threshold.

Before the credibility weighted fusion, the weighting coefficient of each cognitive user was calculated based on the credibility value; w_i represents weighted value for the *i*-th cognitive user, $w_i \in (0,1]$. Weighting coefficients can be expressed as:

$$w_i(j) = \frac{r_i(j)}{\sum_{i=1}^{N} r_i(j)} \quad (10)$$

The calculation method of the weighting coefficient substantially reduces the effect of cognitive users with low credibility value, while improve the impact of cognitive users with the high reputation value to the final decision.

After obtaining the weighting coefficients of cognitive users, weighting coefficients w_i was introduced for weighted fusion in fusion center based on the detection results of each cognitive users, the judgment guidelines can be expressed as

$$d(j) = \begin{cases} 1, & \text{if } \sum_{i=1} w_i(j) T_i(j) \geq \lambda \\ 0, & \text{otherwise} \end{cases} \quad (11)$$

4.2 Remove the Malicious Users

Based on the calculation of cognitive user's credit value, the attribute categories of the cognitive user is judged based on the different credibility value of the cognitive users, set α and β to be the high and low thresholds reputable, set initial credit value of each cognitive user is $r_i(0) = (\alpha + \beta)/2$, specific judgments as follows:

(1) When the credibility value of *i*-th cognitive users meet to $r_i(j) \geq \alpha$, the cognitive user is determined to the trusted normal user, and allow it to participate in cooperative spectrum sensing and reputation value plus 1;

(2) When the credit value of *i*-th cognitive user meet to $r_i(j) < \beta$, the cognitive user is determined to the untrusted malicious users, which sensing results was excluded, prohibited from participating in cooperative spectrum sensing, and its reputation value minus 1;

(3) When the credit value of cognitive users meets $\alpha > r_i(j) \geq \beta$, the cognitive users were determined to the pending users, and its credibility value plus 1 or minus 1 according to their judgments whether or not consistent with the final decision.

Based on the above the judgment of cognitive user's reputation value, it will produce the following different cases: first, a part of normal cognitive users send the correct and reliable sensing results which consistent with the final decision every time, the credibility value increased until to a predetermined threshold α, then normal cognitive user was taken as the trusted user, participating in the cooperative spectrum sensing later; second, malicious attackers always sends results on the contrary to the real, the reputation value is gradually decreased, until less than the minimum threshold β, the malicious user was excluded; third, another part of the normal cognitive user sent the sensing results right or wrong sometimes, this may be due to the spectrum sensing inaccuracies caused by hidden terminals problems, the users were judged to be pending users by the credibility value.

4.3 Process Design Program

Figure 2 shows the flowchart of the proposed defense attack scheme, the detailing steps were explained below:

(1) First, each cognitive user set the initial credit value;

(2) Cognitive user performs local spectrum sensing;

(3) The fusion center receives the sensing results from the cognitive user, and performs the globally judgment in accordance with certain rules;

(4) Compare the local and global judgment results, update the credibility value, judgments of same result credibility value plus 1 or minus 1 when the comparison result is the same or different;

(5) The attribute of cognitive user is judged by comparing the credit value with the setting threshold, if the user is judged to be the normal or pending user, return to step (2), then performs the next round of spectrum sensing; If the user is judged to be the malicious user, the sensing results of the cognitive user is excluded, the malicious user is not allowed to attend the next time collaborative sensing.

By analyzing the above algorithm, the proposed defense SSDF attacks algorithm reduced the complexity of algorithm, which is due to the malicious user is removed when the credit value reduce to a certain threshold; on the other hand it improves the accuracy of collaborative sensing, which is because the trusted users with the high credibility value participate in the collaborative spectrum sensing.

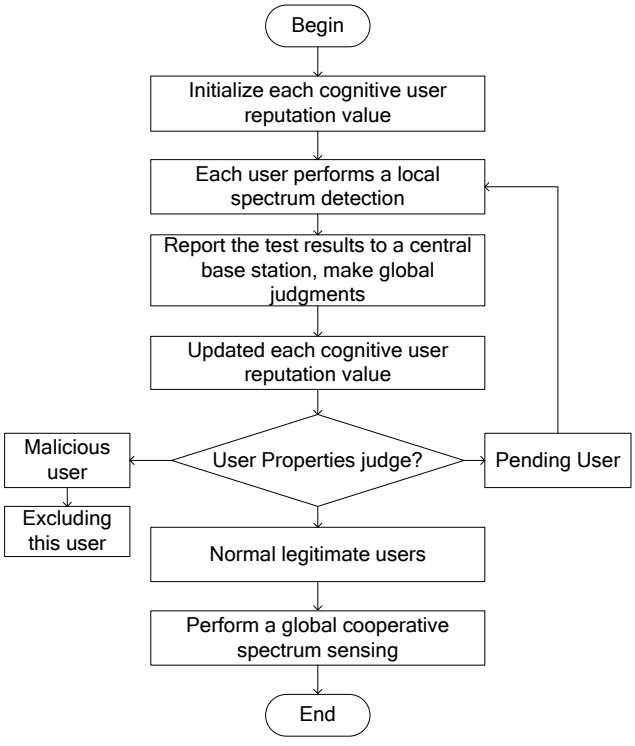

Figure 2: The Flowchart of Defense Attack Scheme by Excluding the Malicious User

5. Simulation Results and Analysis

We use MATLAB software to simulate the procedure of detect the SSDF attacks. Suppose the average SNR γ =-15dB, there are N=30 cognitive users in cognitive radio networks, only a small number of malicious users. Cooperative spectrum sensing scheme

adopts the q-out-of-N rule. The attack scenario is that the malicious user always sends the opposite result to fusion center to reduce the spectrum sensing accuracy.

The following study the relationship between the probability of false alarm and the number of cognitive users when the number of malicious users is k=5. As shown in Figure 3, along with the number of cognitive users increase, the collaborative probability of false alarm increase; when the number of cognitive users is fixed, different q values also have a great impact on the performance of cooperative spectrum sensing; when the value of q increases, the collaborative probability of false alarm decreases. When the number of the cognitive user is N = 25 and q= 22, the cooperative probability of false alarm is close to 0.1. The cooperative probability of false alarm is close to 0.8 when N = 25 and q =18. Therefore, in order to make full use of spectrum resources, the higher q values can bring a lower false alarm performance.

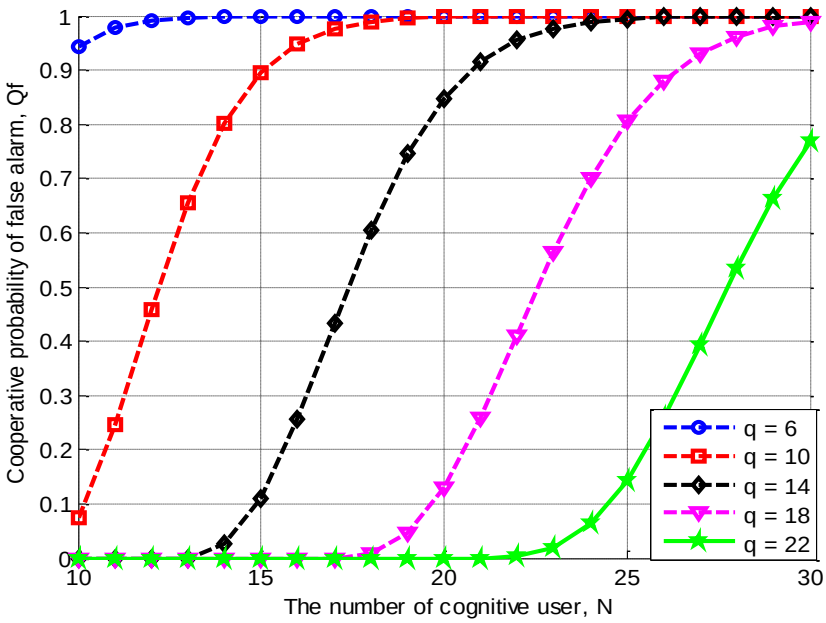

Figure 3: The Relation between Cooperative Probability of False Alarm And The Number Of Cognitive Users, K = 5

Figure 4 shows when N=30 and q=15, receiver operating characteristic (ROC) curve of the collaborative sensing performance attacked by the malicious user. As shown, the number of malicious users decreases gradually, the collaborative detection probability increases gradually. When the collaborative probability of false alarm is Q_f=0.1, the collaborative detection probability Q_d is close to 0.9 and 0.55 when the number of malicious user is k=3 and k=5, respectively. This is due to more malicious user transmits the opposite sensing result, more error sensing information affect the judgment accuracy of the fusion center.

In the following, we further study the feasibility of credibility-based defense SSDF attack scheme by removing the malicious user. Let higher and lower credit decision threshold value are $\alpha = 9$ and $\beta = 1$ respectively, then the initial credit value is 5. Figure 5 shows the performance comparison between the collaborative sensing scheme based on the q-out-of-N rule, the credit-based weighted sensing scheme and the proposed scheme by excluding the malicious user.

As can be seen from the Figure 5, with the gradual increase of the number of malicious users, collaborative detection probability Q_d also declined for scheme based on q-out-of-N rule which is not taken any defensive attack measures. For the same number of malicious user, collaborative sensing scheme based on q-out-of-N rule without any defensive attack

measures received poor sensing performance. The defense SSDF attack schemes based on credibility weighting and excluded malicious users obtain the higher probability of collaborative detection. Furthermore, compared to the algorithm based on credit weighted for all cognitive users, for the same number of malicious user, sensing performance of the proposed scheme has been further improved, collaborative detection probability Q_d reached to 0.8, which has increased about 0.06 compared to the algorithm based on credit weighted.

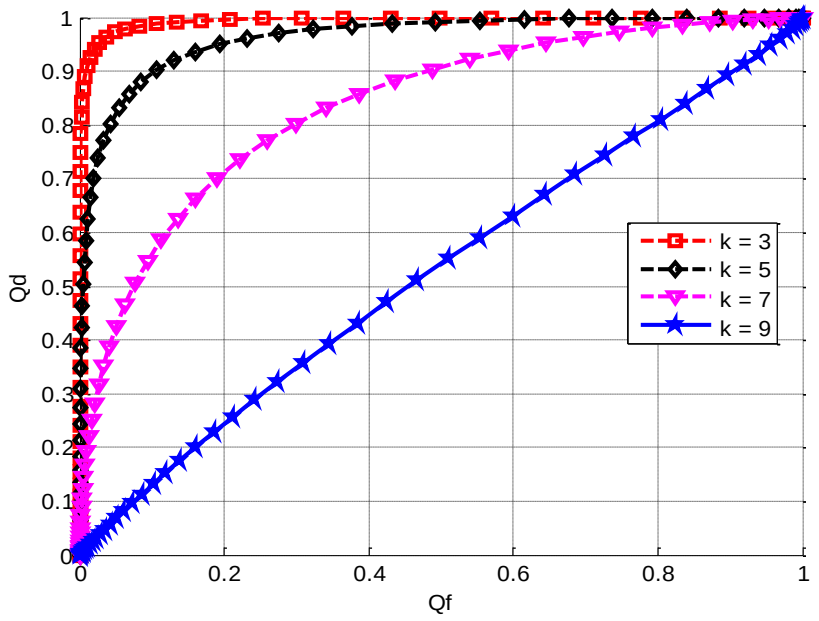

Figure 4: ROC Curve Of SSDF Attacks, Q = 15

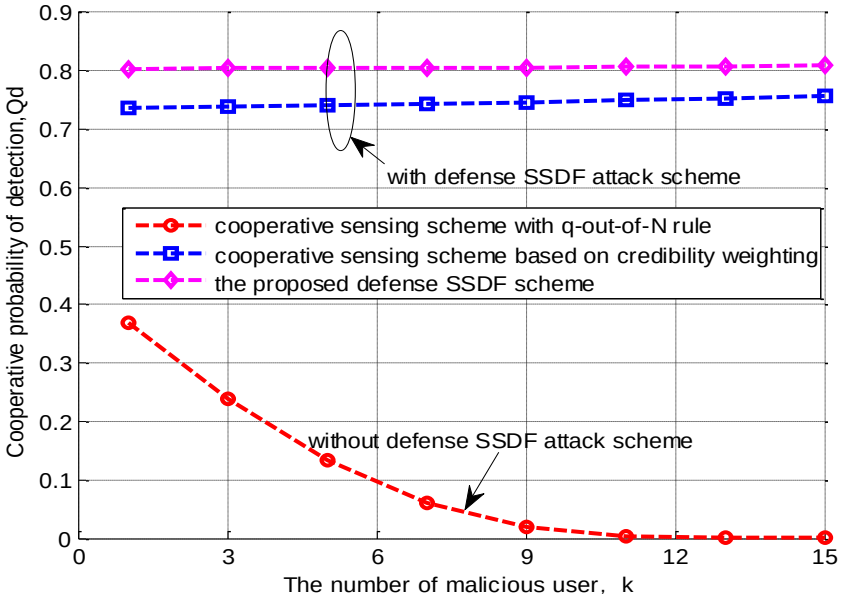

Figure 5: The Collaborative Detection Probability under Different SSDF Attack Defense Schemes

In addition, for the SSDF attacks, it is not only causing interference to authorized users, but also has the potential to lose the opportunity to access the spectrum. Therefore, the effect of the collaborative probability of false alarm by malicious users is studied in Figure 6.

As shown in Figure 6, with the malicious users gradually increases, the collaborative probability of false alarm increases for the scheme based on q-out-of-N rule without any defensive attacks measures. Credibility weighting scheme although set a lower credit weights for a malicious user, the false sensing information of a malicious user still affect the final sensing performance. Compared to the credit weighting scheme for all users, the proposed defense SSDF attack scheme by excluding malicious users obtains the lower probability of false alarm. The probability of false alarm does not vary with the number of malicious users, which is mainly due to the proposed scheme by excluding a malicious user based on reputation value judgment, eliminating the effects of malicious users.

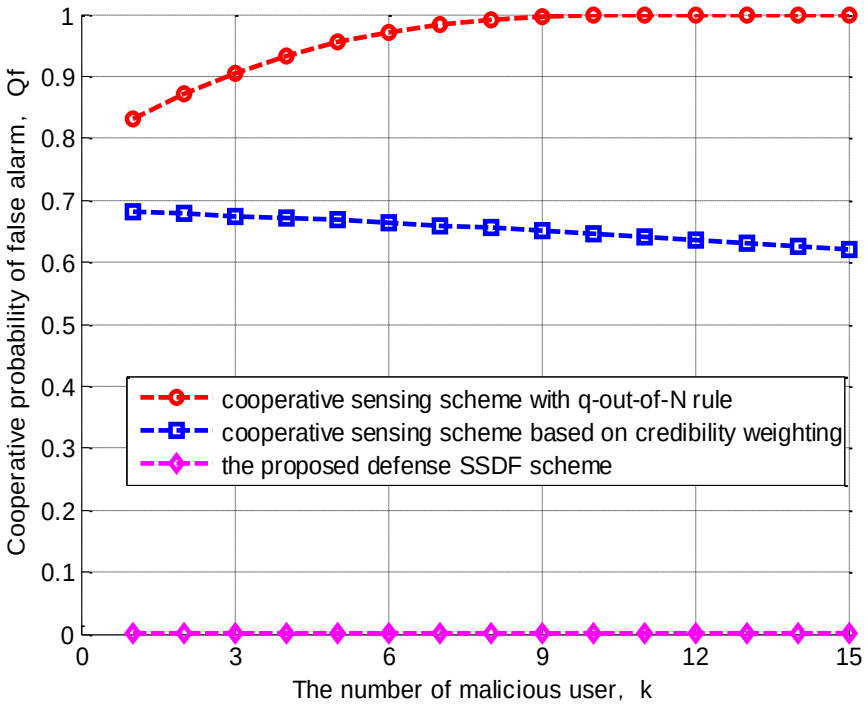

Figure 6: The Collaborative Probability Of False Alarm Under Different SSDF Attack Defense Schemes

6. Conclusion

Cognitive Radio is an effective technology and a hot research direction which can solve the problem of deficient resource and revolutionize utilization. And its safety technology attracts more and more researches. Spectrum sensing data falsification attacks are typically easy and largely affecting. In this paper, we proposed a new method to defense the SSDF attacks by calculating and updating the credit value of the SUs, malicious users are excluded to avoid the attacks affect in cooperative spectrum sensing. The scheme on the one hand reduces the computational complexity, on the other hand improves the accuracy of the spectrum detection. Compared to the credit weighting scheme for all users, the proposed defense SSDF attack scheme by excluding malicious users obtains the higher probability of detection and the lower probability of false alarm. Cognitive radio technology has a wide range of applications, such as television, mobile communications, military applications, and the Internet of things. At present, the cognitive radio technology is still in the research stage, and there are still many challenges in the practical application.

Acknowledgements

This work was supported by Scientific Research Fund of Heilongjiang Provincial Education Department (No. 12541583). This work was supported by research start-up funding project of Heilongjiang Bayi Agricultural University (No.XYB2013-23). This work was supported by Science Foundation of Heilongjiang Province for the Youth (No.QC2015070).

References

[1] Saduyu, Y.E. Securing Cognitive Radio Networks with Dynamic Trust against Spectrum Sensing Data Falsification, Proceedings of IEEE Military Communications Conference, **(2014)**, October 6-8; Baltimore, MD.
[2] Changlong Chen, Min Song,and ChunSheng Xin, A density based scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks, Proceedings of IEEE Global Communications, **(2013)**, December 9-13; Atlanta, GA.
[3] Althunibat, S. , Di Renzo, M. and Granelli, F. Robust Algorithm against Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks, Proceedings of 79th Vehicular Technology Conference, **(2014)**, May 18-21, Seoul.
[4] Li Li, Fangwei Li and Jiang Zhu, A method to defense against cooperative SSDF attacks in Cognitive Radio Networks, Proceedings of IEEE International Conference on Signal Processing, Communication and Computing, **(2013)**, August 5-8, KunMing, China.
[5] Althunibat, S. , Denise, B.J. and Granelli, F. A Punishment Policy for Spectrum Sensing Data Falsification Attackers in Cognitive Radio Networks, Proceedings of the 80th Vehicular Technology Conference, **(2014)**, September 14-17; Vancouver, BC.
[6] Mingchen Wang, Bin Liu and Chi Zhang, Detection of collaborative SSDF attacks using abnormality detection algorithm in cognitive radio networks, Proceedings of IEEE International Conference on Communications Workshops, **(2013)**, June 9-13; Budapest.
[7] Yadav, S. and Nene, M.J. RSS based detection and expulsion of malicious users from cooperative sensing in Cognitive Radios, Proceedings of the 3rd International Advance Computing Conference, **(2013)**, February 22-23; Ghaziabad.
[8] Suqin Xu, Yitao Xu, Guoru Ding and Shuo Feng, A method of evaluating negative utility of information in presence of SSDF attack, Proceedings of International Conference on Wireless Communications & Signal Processing, **(2013)**, October 24-26, Hangzhou, China.
[9] Chatterjee, Sukanya and Pinaki S. A Comparison Based Clustering Algorithm to Counter SSDF Attack in CWSN, Proceedings of International Conference on Computational Intelligence and Networks, **(2015)**, January 12-13; Bhubaneshwar.
[10] Hyder, C.S. , Grebur, B. , Li Xiao and Ellison, M. ARC: Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks, IEEE Transactions on Mobile Computing, vol.13 , no.8 , **(2014)**, pp.1707 – 1719.
[11] Jingyu Feng, Yuqing Zhang, Guangyue Lu and Liang Zhang, Defend against Collusive SSDF Attack Using in Cooperative Spectrum Sensing Environment, Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, **(2013)** , July16-18; Melbourne, VIC.
[12] Jingyu Feng, Yuqing Zhang and Guangyue Lu, A Soft Decision Scheme against Intermittent SSDF Attack in Cooperative Spectrum Sensing, Proceedings of the IEEE International Conference on Computer and Information Technology, **(2014)** , September 11-13; Xi'an, China.

Authors

Hong Du, she was born in Heilongjiang Province, China, in 1982. She received the B.S. degree from the Northeast Petroleum University, Daqing, in 2006 and the M.S. degree from the Northeast Petroleum University, Daqing, in 2009, both in communication engineering. She received the Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT), Beijing, in 2012. She is currently working in Heilongjiang Bayi Agriculture University. Her research interests include cognitive radio and internet of things.

Shuang Fu, she was born in Heilongjiang Province, China, in 1982. She received the B.S. degree from the Heilongjiang University, Haerbin, in 2004 and the M.S. degree from the Northeast Petroleum University, Daqing, in 2010, both in communication engineering. She received the Ph.D. degree from Haerbin Engineering University (HEU), Haerbin, in 2014. She is currently working in Heilongjiang Bayi Agriculture University. Her research interests include cognitive radio.

Hongna Chu, she was born in Heilongjiang Province, China, in 1983. She received the B.S. degree from the Northeast Petroleum University, Daqing, in 2006. She is currently working in Beijing Branch, Daqing Oilfield Information Technology Company. Her research interests include wireless communication.