The Analysis of Influence on Sensing Performance from the Malicious user for SSDF Attacks in Cognitive Radio

HONG DU, SHUANG FU, JIE XU
College of information technology
Heilongjiang Bayi Agricultural University
No.2 Xinyang Road, Gaoxin District, Daqing City, Heilongjiang Province
CHINA
duhong929@163.com

Abstract: - Cognitive radio (CR) can improve the utilization of the spectrum by making use of licensed spectrum. However, the security aspects of cognitive radio networks have garnered little attention. In this paper, we discuss a threat to cognitive radio networks, which we call the spectrum sensing data falsification (SSDF) attack. Specifically, malicious users can always send presence and absence of information for the authorized user, or always report the opposite sensing results. Collaborative sensing performance was deduced under different attack scenarios. Simulation results show that compromise collaborative sensing performance can be obtained when a malicious user always sends "1" with the AND rule, and always sends "0" with the OR rule; In addition, for a malicious user always report the opposite sensing results, q-out-of-N rule was adopted for the cooperative sensing. When the number of malicious users is less, q values should be smaller. On the other hand, from the perspective of make full use of spectrum resources, q values should be larger.

Key-Words: - Cognitive radio, Spectrum Sensing, SSDF attacks, Attack scenario, malicious user, fusion rule

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

SSDF attacks and defenses have been studied in previous work. For instance, the author develops a dynamic trust management scheme to reliably detect and mitigate SSDF attacks [1]. Besides, the author proposes a distributed density to countermeasure the SSDF attack [2]. A algorithm is proposed to assign 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 [3]. The author proposes a reputation based adaptive clustering algorithm to defense against cooperative SSDF attacks [4]. 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 [5]. 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 [6]. 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 [7]. 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 [8]. The author proposed a similarity-based clustering of sensing data to counter the above attack [9]. 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 [10]. 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 [11]. A novel trusted sequential probability ratio test scheme based on beta function is proposed to avoid the intermittent spectrum sensing data falsification attack [12].

However, all of the mentioned methods to defense the SSDF attacks do not consider the different attack scenarios. This article focuses on the impact on the cooperative spectrum sensing performance from SSDF attack in cognitive radio networks. Different attack scenarios in SSDF attack is investigated in detail. Specifically, malicious users can always send presence or absence information of the authorized user, or always report the opposite sensing result. The impact on the cooperative spectrum sensing performance is analyzed from the malicious users. The cooperative detection performance under different scenarios is deduced and discussed.

The rest of the paper is organized as follows. In Section 2, we introduced the principle of SSDF attack and described the cooperative spectrum sensing performance in security environment. In Section 3, we investigate the effects from SSDF attack on collaborative sensing performance and discuss the different attack scenarios from the malicious users. In Section 4, we provide the simulation results and discussion. Finally, Section 5 concludes this paper.

2 System Model

2.1 The SSDF attack model

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. Obviously, the last SSDF attacks will seriously impair the performance of cooperative spectrum sensing.

Fig.1 depicts the SSDF attacks impact on the performance of cooperative spectrum sensing. The malicious user sends altered sensing result; cooperative spectrum sensing performance will be affected depending on the false information. If a malicious user always sends "1", it will greatly reduce the frequency spectrum utilization; if a malicious user always sends "0", it will cause serious interference to authorized users; the most serious impact is that the malicious user sends sensing results opposite to the real, that is not only cause the interference to authorized users to a certain extent, but also reduces the chance of cognitive users to access the free band.

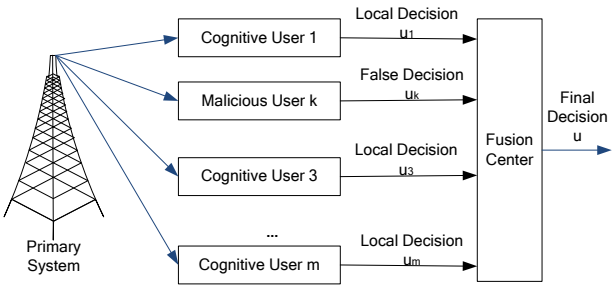

Fig.1 SSDF attack model in cooperative spectrum sensing

2.2 Local and cooperative sensing 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 sample.

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

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

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

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.

Common hard-merger judgment rules are OR rule, AND rule and K-out-of-N rule, collaborative sensing performance can be expressed as follows:

OR rule:
$$\begin{cases} Q_d=1-\left(1-P_{d,j}\right)^N \\ Q_f=1-\left(1-P_{f,j}\right)^N \end{cases} \quad (6)$$

AND rule:
$$\begin{cases} Q_d=\left(P_{d,j}\right)^N \\ Q_f=\left(P_{f,j}\right)^N \end{cases} \quad (7)$$

q-out-of-N rule:
$$\begin{cases} Q_d=\sum_{j=q}^{N}\binom{N}{j}P_d^j\left(1-P_d\right)^{N-j} \\ Q_f=\sum_{j=q}^{N}\binom{N}{j}P_f^j\left(1-P_f\right)^{N-j} \end{cases} \quad (8)$$

3 The analysis of cooperative spectrum sensing performance for the SSDF attack

In the SSDF attack of cognitive radio network, 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.

Assuming that the number of cognitive users is *N*, the number of malicious users is *k* (*1<k<N*), the following discussion is under the above SSDF attacks scenarios.

3.1 Attack scenario 1

If malicious users always send "0", which means the authorized user was always reported as not present, this situation caused great Interference to authorized users; In contrast, if malicious users always send "1", which means that authorized user was always reported to appears, this will cause cognitive users lose the opportunity to occupy the idle channel.

Suppose the cognitive user's detection probability and false alarm probability can be denoted P_d and P_f respectively, cooperative detection probability and cooperative false alarm probability are represented by Q_f and Q_d. In the following, collaborative sensing performance with the AND and OR rules were analyzed for the SSDF attack.

3.1.1 Malicious attacker always sends "1"

AND rule is that when all cognitive users judge the existence of an authorized user, the final judgment was considered an authorized user appears. The probability of the presence of authorized is 1 when *k* malicious users always send a "1". Therefore, the

final cooperative probability of detection and cooperative probability of false alarm were the probability for *N-k* normal cognitive users detects the authorized users, which can be expressed as follows:

$$\text{AND rule:} \quad \begin{cases} Q_d = \left(P_{d,j}\right)^{N-k} \\ Q_f = \left(P_{f,j}\right)^{N-k} \end{cases} \tag{9}$$

Compared with the collaborative detection performance under trust users assumptions, collaborative detection probability and collaborative false alarm probability with AND rule is larger for malicious user's attack. Although it can better protect the authorized user not to be interfered, but lose more spectrum opportunities for the price.

OR rule is that as long as there is an authorized user was determined to be existed, final judgment was an authorized user exists. Due to k malicious users always send "1", at least one authorize user was judge to be existed, so the final probability of detection and false alarm probability is 1, which can be expressed as follows:

$$\text{Or rule:} \quad \begin{cases} Q_d = 1 \\ Q_f = 1 \end{cases} \tag{10}$$

The impact with OR rule in this attack scenario, judgment results is that the authorized users occupy the channel always. Therefore, the cognitive user will lose the opportunity to access to available channels. Therefore, detection performance will be very poor when a malicious user always send a "1" with OR rule. As long as there is a malicious user with OR rule in this attack scenario, the cognitive user cannot use idle spectrum. In other words, a malicious user only needs to send a bit, which can totally affect sensing results.

3.1.2 Malicious attacker always sends "0"

For the AND rule, when an authorized user exists, the authorize user does not exist always which is judged by a malicious user, the presence of an authorized user was never able to be detected, therefore collaborative detection probability is 0, this will cause great interference to authorized users; and when an authorized user does not exist, a malicious user always send a "0" will not bring false alarms, so the final collaborative false alarm probability is 0, the spectrum opportunities will not be wasted.

$$\text{AND rule:} \quad \begin{cases} Q_d = 0 \\ Q_f = 0 \end{cases} \tag{11}$$

For the OR rule, in the presence of authorized users, the authorize user does not exist always which is judged by a malicious user, the final probability of detection is the detection probability for *N-k* trust cognitive users, which will bring interference to the authorized user; when the authorized user does not exist, a malicious user always send a "0" will not bring false alarms, so the final probability of false alarm is the probability of false alarm for N-k trust cognitive users.

$$\text{OR rule:} \quad \begin{cases} Q_d = 1-\left(1-P_{d,j}\right)^{N-k} \\ Q_f = 1-\left(1-P_{f,j}\right)^{N-k} \end{cases} \tag{12}$$

3.2 Attack scenario 2

Attack scenario 2 is that malicious attackers always send 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. When there are *k* malicious users in *N* cognitive users, 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, based q-out-of-N rule, the cooperative detection probability Q_d can be expressed as:

$$\begin{cases} Q_d = \sum_{j=q}^{N-k} \binom{N-k}{j} P_d^j \left(1-P_d\right)^{N-k-j}, & N-k > q \\ Q_d = 0, & N-k < q \end{cases} \tag{13}$$

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:

$$\begin{cases} Q_f = \sum_{j=q-k}^{N-k} \binom{N-k}{j} P_f^j \left(1-P_f\right)^{N-k-j}, N-k > q \\ Q_f = 1 \qquad\qquad\qquad\qquad\qquad\qquad , N-k < q \end{cases} \tag{14}$$

4 Simulation results and analysis

We use MATLAB software to simulate the performance influence for the SSDF attacks. Suppose the average SNR γ = -15dB, there are only a small number of malicious users in cognitive radio networks.

4.1 Attack scenario 1

Assuming the number of cognitive users N=10, the local detection probability P_d =0.9, the local false alarm probability P_f = 0.1.

Fig.2 and Fig.3 show the relationship between the number of malicious users and collaborative sensing performance. As shown, when a malicious user always send a "1", according to the OR rule, it will always report the presence of an authorized user. Authorized users are well protected, but cause the cognitive user to lose spectrum opportunities; when a malicious user always send a "0", according to the AND rule, the presence of an authorized user was never to be detected, which will cause the significant interference to authorized users.

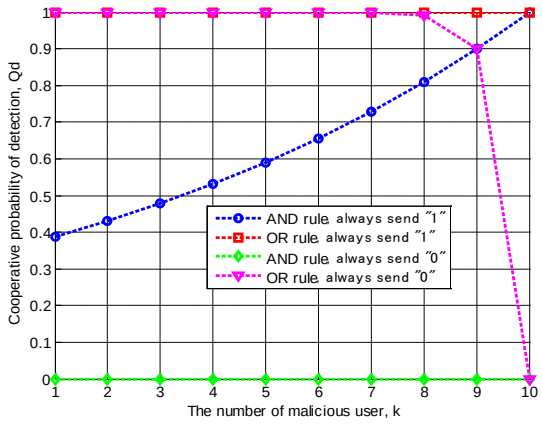

Fig.2 Relations between cooperative detection probability Q_d and the number of malicious users

Specifically, when the malicious user always sends "1" with the AND rule and the malicious user always sends "0" with the OR rule, it can obtain a compromise detection performance. When the malicious user always sends "1" with the AND rule, with the gradual increase in the number of malicious users, collaborative detection probability and collaborative false alarm probability increases gradually, this scenario can protect the authorized users at the expense of opportunity cognitive user access to spectrum. When a malicious user always sends "0" with the OR rule, with the gradual increase in the number of malicious users, collaborative detection probability and collaborative false alarm probability decreases, this scenario can improve the spectrum utilization, but may result in the interference to the authorized user.

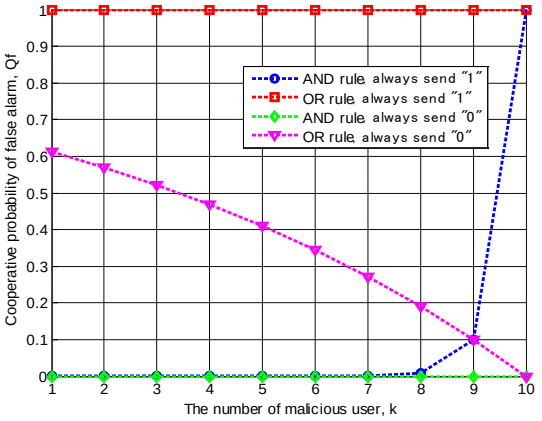

Fig.3 Relations between cooperative false alarm probability Q_f and the number of malicious users k

4.2 Attack scenario 1

In the following, the harsh attack scenario which is that the malicious attackers always send results on the contrary to the real. Fig.4 and Fig.5 show the cooperative sensing performance with q-out-of-N rule under k malicious attack users. Assumed that q = 10.

As shown in Fig.4, at the same the number of cognitive users, collaboration false alarm probability without malicious user (k=0) is significantly less than the one with malicious users. Furthermore, with gradually increasing the number of malicious users, it will leads to the gradual increase the probability of false alarm collaboration, thus causing a great waste of spectrum resources, spectrum utilization is low. This is because when the authorized user does not exist, a malicious user can always send presence information of the authorized user, resulting in a large number of false alarms that make the cognitive user lose opportunities to access to the spectrum. In particular, when the number of the cognitive user is N = 20, the collaboration probability of false alarm

without malicious users (k=0) is close to be 0.15, but collaborate false alarm probability with malicious users k =3 is close to be 0.3.

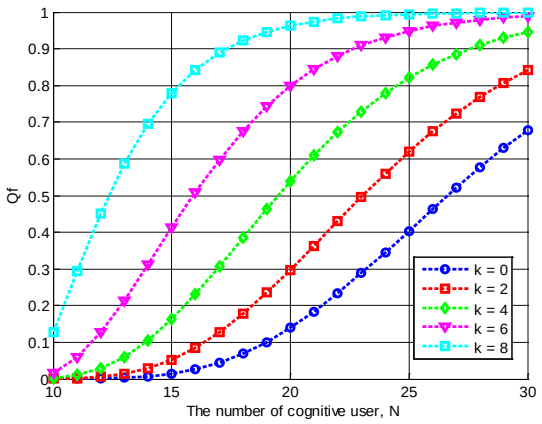

Fig.4 Relations between cooperative false alarm probability Q_f and the number of cognitive users N

Fig.5 shows the relationship between the cooperative probability of detection and the number of malicious users when the number of cognitive users is N=30. As shown, with gradually increasing the number of malicious users, collaborative detection probability is gradually decreased. This is because when the existence of an authorized user, malicious users always send the sensing results with the real information to the contrary, more and more malicious users report information that an authorized user is not exist. Thus, the probability of an authorized user can be detected gradually decreases.

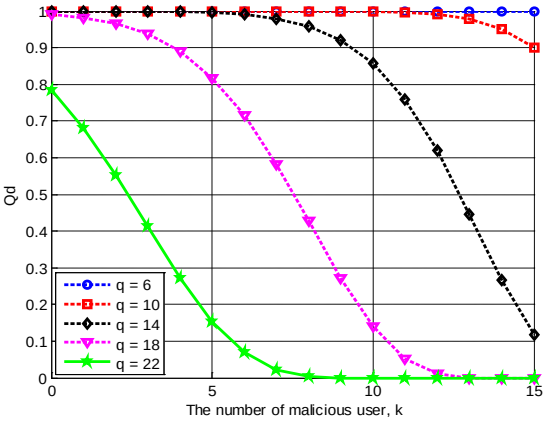

Fig.5 Relations between cooperative detection probability Q_d and the number of malicious users k, N=30

When the number of malicious users is fixed, the different values of q also has a great influence on the performance of cooperative spectrum sensing, with increasing values of q, collaborative detection probability decreases. When the number of the malicious user is k=10, collaborative detection probability is near to be 0.15 for q=18, and collaborative detection probability is near to be 0.85 for q=14. Therefore, in order to reduce interference to the authorized users, a lower value of q can bring the higher detection performance.

5 Conclusion

This paper focuses on the impact of malicious user's SSDF attacks on collaborative detection performance in cognitive radio networks. Different attack scenarios were considered to investigate the impact on the cooperative spectrum sensing performance. Collaborative sensing performance was deduced under different attack scenarios. Simulation results show that compromise collaborative sensing performance can be obtained when a malicious user always sends "1" with the AND rule, and always sends "0" with the OR rule; In addition, for a malicious user always report the opposite sensing results, q-out-of-N rule was adopted to research the cooperative sensing performance. When the number of malicious users is less, from the perspective of protecting authorized users, q values should be smaller. On the other hand, from the perspective of make full use of spectrum resources, q values should be larger, and thus get a better cooperative sensing performance.

Acknowledgment: This work is supported by Scientific Research Fund of Heilongjiang Provincial Education Department (No.12541583) and 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] Sagduyu,Y.E. "Securing Cognitive Radio Networks with Dynamic Trust against Spectrum Sensing Data Falsification," *in Proc. 2014 IEEE Military Communications Conference (MILCOM)*, 2014 , pp. 235-241.

[2] Changlong Chen, Min Song, ChunSheng Xin, "A density based scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks," in *Proc. 2013 IEEE Global Communications Conference (GLOBECOM)*, 2013 , pp. 623- 628.

[3] Althunibat, S. , Di Renzo, M. , Granelli, F. "Robust Algorithm against Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks," in *Proc. IEEE 79th Vehicular Technology Conference (VTC Spring),* 2014 , pp.1-5.

[4] Li Li, Fangwei Li,Jiang Zhu, "A method to defense against cooperative SSDF attacks in Cognitive Radio Networks," in *Proc. 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC),* 2013 , pp.1-6.

[5] Althunibat S, Denise BJ, Granelli F. "A Punishment Policy for Spectrum Sensing Data Falsification Attackers in Cognitive Radio Networks," *in Proc. IEEE 80th Vehicular Technology Conference(VTC Fall),* 2014, pp.1-5.

[6] Mingchen Wang, Bin Liu, Chi Zhang, "Detection of collaborative SSDF attacks using abnormality detection algorithm in cognitive radio networks," in *Proc. 2013 IEEE International Conference on Communications Workshops (ICC),* 2013, pp.342-346.

[7] Yadav, S. , Nene, M.J. "RSS based detection and expulsion of malicious users from cooperative sensing in Cognitive Radios," in *Proc.2013 IEEE 3rd International Advance Computing Conference (IACC),* 2013 , pp.181-184.

[8] Suqin Xu, Yitao Xu, Guoru Ding and Shuo Feng, "A method of evaluating negative utility of information in presence of SSDF attack," in *Proc. 2013 International Conference on Wireless Communications & Signal Processing (WCSP),* 2013, pp.1-5.

[9] Chatterjee, Sukanya , Chatterjee, Pinaki S. "A Comparison Based Clustering Algorithm to CounterSSDF Attack in CWSN, " in *Proc.* 2015 *International Conference on Computational Intelligence and Networks (CINE),* 2015 , pp.194-195.

[10] Hyder, C.S. , Grebur, B. , Li Xiao , 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 Trust in Cooperative Spectrum Sensing Environment," in *Proc. 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* 2013 , pp. 1656-1661.

[12] Jingyu Feng, Yuqing Zhang and Guangyue Lu, "A Soft Decision Scheme against Intermittent SSDF Attack in Cooperative Spectrum Sensing," in *Proc. 2014 IEEE International Conference on Computer and Information Technology (CIT),* 2014 , pp.293-298.