Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

Improved Trust Node Selection Technique to Defend Spectrum Sensing Data Falsification Attack in Cognitive Radio Network

K.Gokulakrishnan[1], S.Baskar[2], V.Srinath[3], R.Amudhevalli[4], S.Jothimani[5], B.Kiruthiga[6]

[1]Assistant Professor, IFET College of Engineering, Villupuram, Tamilnadu, India

[2]Assistant Professor, Kongunadu College of Engineering and Technology, Trichy, Tamilnadu, India

[3]Assistant Professor, Indra Ganesan College of Engineering, Trichy, Tamilnadu, India

[4] Research scholar, Rathnavel Subramaniam College of Arts and Science, Coimbatore, Tamilnadu, India.

[5]Assistant Professor, M.Kumarasamy College Engineering, Karur, Tamilnadu, India

[6]Assistant Professor, K.Ramakrishnan College of Technology, Trichy, Tamilnadu, India

Abstract: Cognitive Radio is the current trending wireless technology which aims to avoid spectrum scarcity. Due to its dynamic spectrum accessing support it imposes lot of security issues. Two vulnerabilities of CRN are behavioral and configurability vulnerabilities. These vulnerabilities cause effect in the cognitive behavior. So it is necessary to overcome those security issues. In this research, solution is offered to handle issue in CRN Spectrum Sensing Data Falsification (SSDF) attack. In SSDF attack, attackers will share results of the modified spectrum sensing to the Fusion Center (FC). Hence the FC will take some incorrect decisions. To mitigate SSDF attack, trust-based algorithm is used to analyze the behavior of each user. Based on the trust value, attackers can be easily identified from the network.

1. INTRODUCTION

In this Section, the basics of the Cognitive Radio Network (CRN), Security issues in CRN and objective of the proposed research is presented. The wireless spectrum consists of electromagnetic radiation and frequency bands. The frequency of the wireless spectrum ranges up to 300GHz. The wireless spectrum is a limited resource, but the users are increasing every day. The spectrum should be utilized efficiently. The user who paid the bid amount during auction is a paid user or primary user. The underutilization of licensed spectrum and overutilization of unlicensed spectrum leads to a management of new spectrum policy. Such a policy is called Opportunistic Spectrum Access (OSA), Dynamic Spectrum Access (DSA) or Flexible Spectrum Use (FSU) [1]. These policies must not affect the performance of the licensed user. To use the spectrum efficiently, the spectrum must be sensed accurately that is whether the licensed user is present or not and the spectrum which is not occupied by the licensed user can be utilized by the primary user [2]. The sensing result of the cognitive radio sensors may encounter incorrect judgements because of multipath fading, shadowing and building penetration. Therefore, Cognitive radio sensors share their own sensing information among themselves to improvise the performance of spectrum sensing and accuracy[3-5]. Such a technique is called cooperative spectrum sensing. The

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

most commonly used spectrum sensing techniques are centralized and decentralized cooperative spectrum sensing. In the first sensing technique, the sensing results of each cognitive user are sent to the FC. The FC fuses all the sensing results of the cognitive users and made a final decision about the nature of the spectrum. If the cognitive user needs to send data, it requests for the channel information (details) to the FC. In the second spectrum sensing technique, there is no FC and cognitive users in a cluster share the sensing results among themselves and it requires a regular update regarding the spectrum information. In CRN, security is an important issue which is not addressed properly[5]. The typical attacks in CRN may include DoS attack, Spectrum Sensing Data Falsification, Primary User Emulation attack, spoofing, Authorisation violation etc. In this research, the problem arising due to Spectrum Sensing Data Falsification attack in a centralised spectrum sensing technique is addressed [6-11]. In such attacks, the attacker modifies the sensing result. An attacker sends a modified sensing results to the FC and it leads FC to take false decisions. Incorrect decision by FC leads to Denial of Service. Secondary Users cannot able to access the spectrum when falsified data is sent and the Primary User's transmission may be interrupted. First, the trusted node is selected and using the results of the trusted node trust value is calculated for each users and it is used to classify the real user and attackers.

The is organised as follows. In section 2, the literature survey for SSDF attack is discussed briefly. In section 3, the detection approach for SSDF attack is discussed. In section 4, simulation results for the proposed method is discussed briefly. The section 5 concludes the proposed method and also the future work for the proposed method is discussed.

2. LITERATURE SURVEY

In the literature, some detection approach for PUE attacks has been presented.

In Richard Yu et al., proposed a defence scheme against SSDF attacks in MANETs. They have used a consensus-based cooperative spectrum sensing algorithm to mitigate SSDF attacks in Cognitive radio based MANETs. In this approach FC is not needed to perform the data fusion to take the final decision to counter SSDF attacks. This scheme supports only distributed spectrum sensing method and nowadays, CSS is achieved in a centralized manner. It is suitable when only 25% of attackers are available in a network and its performance is very low when large malicious users are presented in a network.

In [12], Farmani et al., proposed a cooperative spectrum sensing method. They used Support Vector Data Description (SVDD) method to mitigate the effects of attackers inside the network. But this method is not effective, when number of attackers is more in a target area. Choosing target area is much difficult when there is more number of users. It may affect the performance of the legitimate user.

In [13], Shameek Bhattacharjee et al., proposed a new scheme for cooperative spectrum sensing for a distributed network. In this network, Fusion Center is absent. The SUs share their channel sensed information results with their neighbors. They compute a trust value on the basis of anomaly. The user with lower trust value which is below the threshold range, it is discarded from cooperative spectrum sensing. When the malicious users in the network increases, the probability of detecting the malicious user decreases.

In [14], Yong Han et al., proposed an approach based on enhanced D-S theory cooperative spectrum sensing algorithm to withstand the SSDF attack. They use traditional "and" & "or" logic fusion rule to enhance the performance of the global decision. This scheme is not suitable for blind condition.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

In [15], Sumit Yadav et al., proposed Received Signal Strength (RSS) based detection and expulsion of malicious users through cooperative spectrum sensing. They used RSS of Primary Users (PU) at the SU to localize its position and compare this with the calculated location using the RSS of SU transmissions at FC. In this method, the estimation of a location is difficult. Hence there may occur variations in the result. False detection of an attacker may occurs.

In [16], Abbas Ali Sharifi et al., proposed an attack aware Collaborative Spectrum Sensing Approach. They presented a hybrid method called Weighted Sequential Probability Ratio Test (WSPRT). They use k out of n rule to find an attacker. They reconstruct the probability density function of each reports for the normality based on a confidence interval. They are not suitable when large number of malicious users are present. But it is effective when 35% of malicious users are presented in a network.

In [17-20], Huifang Chen et al., proposed a cooperative spectrum sensing scheme with quantized data M-ary in CRN under SSDF attacks. They calculated the reporting frequency using history of reports generated by a SU. If the frequency of reporting is higher than the threshold value it is considered as an attacker otherwise, considered to be a normal user. Still, this approach is not suitable for large number of malicious users.

These methods are not suitable for large number of malicious users. Mostly they used distributive approach. In this research, defensive approach for SSDF attack under large number of malicious users is proposed by using trusted node selection analysis and trust value computations.

3. DETECTION APPROACH

In this section, the system model, trusted node selection, energy detection algorithm, flow diagram of the proposed work and the detection approach is discussed in detail.

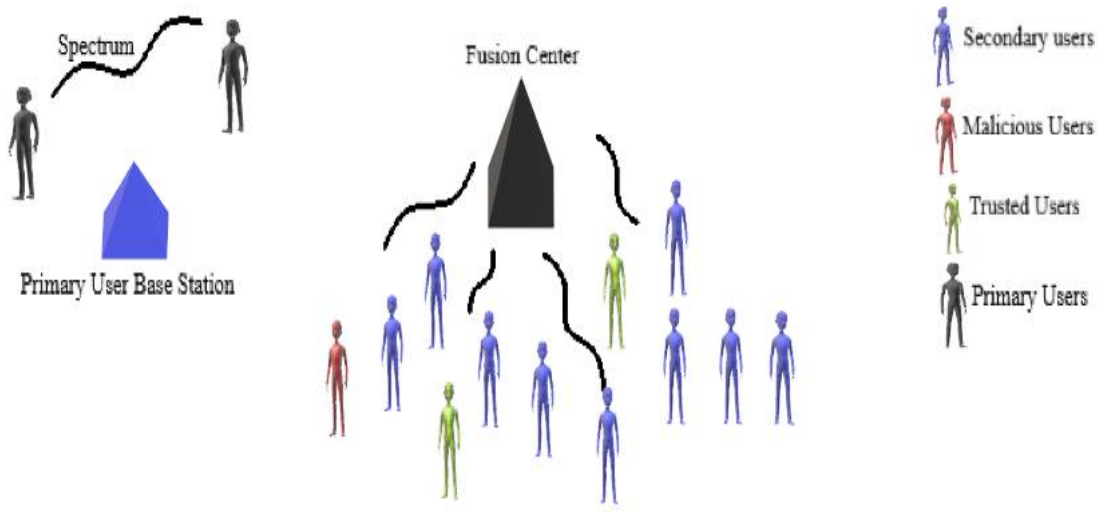

Fig 3.1 System Model for SSDF attack

Consider a network which consists of PU network and CRN network under 802.11 network standard model [14]. The PU network is a group of paid users. The SUs are going to access the licensed spectrum band when the spectrum is free. We focus on one primary transmission pairs, *N* secondary users, *S* trusted secondary users, and *M (0<M<N)* malicious users. [23] The proposed system model uses centralized mode of cooperative spectrum sensing. In centralized spectrum sensing technique, there is a FC who fuses all the sensing

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

results. Trusted users are authenticated users by the (FC). In this approach FC acts as Base Station for SUs. This system includes listening and reporting channel. Listening channel is the channel between PUs and reporting channel is the channel between SU and FC. These *N* SUs sends their result to FC to take global sensing decision. Attackers in the system transmits falsified data to the FC and make them to take false decision. Authenticated SU is a trusted user and also atleast one trusted user must be selected for cooperative spectrum sensing within *N* SUs. Finally, FC collects all the results from N SUs and performs global decision.
The detection of SSDF attack can be detected by using two steps, they are

- Trusted node selection and its report generation
- Trust Value based cooperative spectrum sensing.

3.1 TRUST NODE SELECTION AND ITS REPORT GENERATION

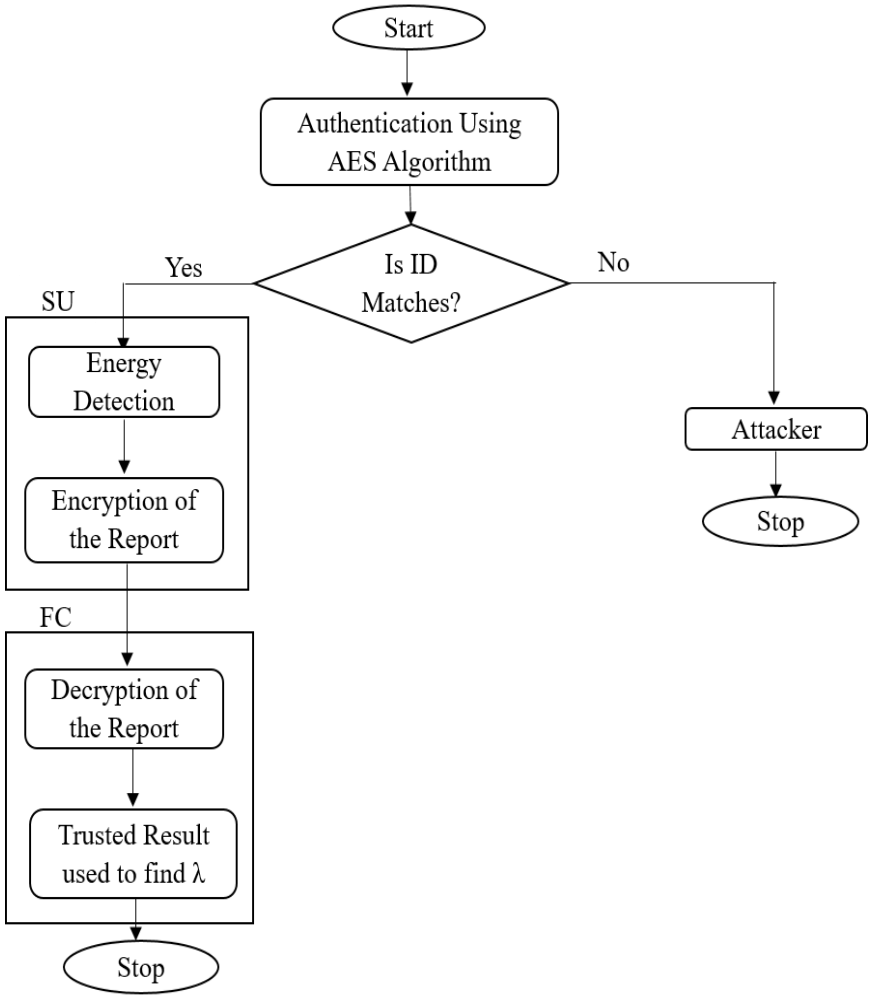

Fig 3.2 Flow chart for trusted node selection

In this detection approach, authentication is given to the trusted node. Each trusted node has certain ID. Fusion centre maintains a database. It consists of unique IDs of all trusted user. [24] Advanced Encryption Standard (AES) algorithm is used to encrypt the ID whenever the trusted node participates in a report generation. Symmetric key is shared between the nodes and FC. Public key cryptographic approach is used for trusted node authentication. The FC decrypts the AES encrypted ID or cipher text and compares the result

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

with the database. If it matches with any one of the IDs in its database, then the user is considered as a trusted user.

After the authentication of trusted node, the SUs performs the spectrum sensing and generates the local result. Energy detection technique is usedas a local spectrum sensing technique to generate the local result. Let *x(t)*, *h(t)*, *s(t)* and *n(t)* be the transmitting signal, impulse response of a signal, PU signal and noise respectively. The transmitting signal *x(t)* can be given as,

$$x(t) = \begin{cases} s(t), presence\ of\ PU \\ 0,\ absence\ of\ PU \end{cases} \quad (3.1)$$

The received signal *y(t)* can be given as,

$$y(t) = \begin{cases} h(t) * s(t) * n(t), presence\ of\ PU \\ 0, \qquad\qquad absence\ of\ PU \end{cases} \quad (3.2)$$

The received signal is sampled and pre-processed to calculate the energy value and it can be given as,

$$e = e[n](n = 1,2, \dots, n_s) \quad (3.3)$$

The aggregated energy value *E* can be given as,

$$E = \sum_1^{N_s} e[n] \quad (3.4)$$

To find the presence of a PU the aggregated energy value *E* is compared to the predefined threshold θ value. The local sensing result v_i can be given as,

$$v_i = \begin{cases} 1, E > \theta \\ 0, E < \theta \end{cases} \quad (3.5)$$

Each SU make a decision for different sensing intervals *T*, Hence the report generated by each SU over a time window T can be given as,

$$\mathrm{v_i} = \{v_i(1), vi(2), \dots, v_i(T)\} \quad (3.6)$$

where, $i=1,2,\dots,N$ indicates SU.

The report generated by SU is encrypted by using X-OR Cipher [18]. The report from each SU is verified by using the trusted SU's report. After the verification process, FC takes a global decision about the channel status. Attacker does not aware of the sensing result generated by trusted user until the pre-shared key between trusted user and FC. So, it is necessary to keep the key more secret. The received encrypted report from the trusted SU is decrypted by the FC. FC takes the decrypted report to verify the local decision results from other users. This result is used to calculate the trust value for each user. In this, FC calculates the trust value for each SU and it detects the attacker in a network. Finally, the global decision is taken by FC by linear combination [19].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

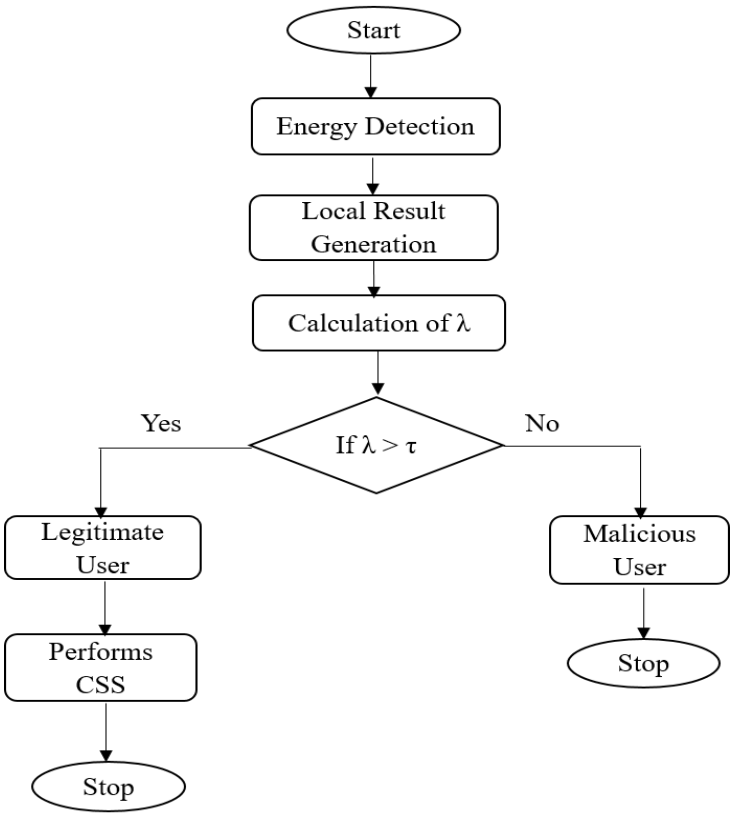

Fig 3.3 Flow chart for detection of SSDF attack

The detection of SSDF attack by using trust based algorithm is shown in the fig 3.3.

The first step of the detection algorithm is the generation of reports from each SU. They use energy detection algorithm to generate the reports. This process is as same as the process by a trusted user. In second step FC collects the reports generated by each SU. . In third step reputation value for each SU is calculated by the FC. In fourth step, FC considers the SUs with reputation value greater than the threshold value for cooperative spectrum sensing. Finally, FC takes global decision.

The report generated by the trusted SU is used to find the trust value of each SU. The Trust value for each SU is calculated for both consistent and inconsistent performance of each SU. Punishment level (μ) for each decision is predefined and $\mu \in (0, 1)$. Trust value (λ) can be given as,

$$\lambda_i(t) = (1 - \mu) * \lambda_i(t-1) + \mu . CON_i(t). \quad (3.7)$$

It is necessary to denote the consistency and inconsistency between trusted CR user's result and the information of i^{th} SU. If the results matches, then $\lambda_i(t)$ increases. Otherwise, $\lambda_i(t)$ value gets decreased. If the trust value is higher then the node is more trusted and taken into an account for making global decision by the FC. Any SU falls below the threshold value τ will be identified as an attacker. Such attacker will be excluded by the FC for the process of taking global decision. Trust value differentiates malicious users from trusted users. Therefore, two punishment levels $\mu 1$ and $\mu 2$ are used. $\mu 1 << \mu 2$, it denotes punishment for wrong decision is higher. Trust value slowly increases after the correct matching of results. But, trust value rapidly gets decreased, if the results are different.

The trust value for both cases can be given as,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

$$\lambda_i(t) = \begin{cases} (1-\mu_1) * \lambda_i(t-1) + \mu_1 . CON_i(t), if\ CON_i(t) = 1 \\ (1-\mu_2) * \lambda_i(t-1) + \mu_2 . CON_i(t), if\ CON_i(t) = 0 \end{cases} \quad (3.8)$$

This approach for detecting the attackers is very efficient for periodic attackers. Trust value decreases quickly when the attacker tries to modify the result continuously. Also they can be identified and blocked out easily from the CRN when their trust value falls below the minimum threshold value τ. Conditions for attacker and normal users can be given as,

$\lambda_i(t) > \tau, for\ normal\ SUs,$
$\lambda_i(t) \leq \tau, for\ attackers$

The users with trust value greater than the threshold value are considered for cooperative spectrum sensing. This method is efficient for large number of attackers and periodic attackers.

4. RESULTS AND DISCUSSION

In this chapter, the parameters used for AES encryption, the results for AES encryption, simulation parameters used for the proposed work and the simulation results generated is discussed. The simulation is done using MATLAB 2016a.

The parameters used for simulation is listed in the table

Simulation Parameters

Number of samples	2000
Number of cognitive users	10
Number of trusted users	1
Threshold value	0.6
Initial trust value	1

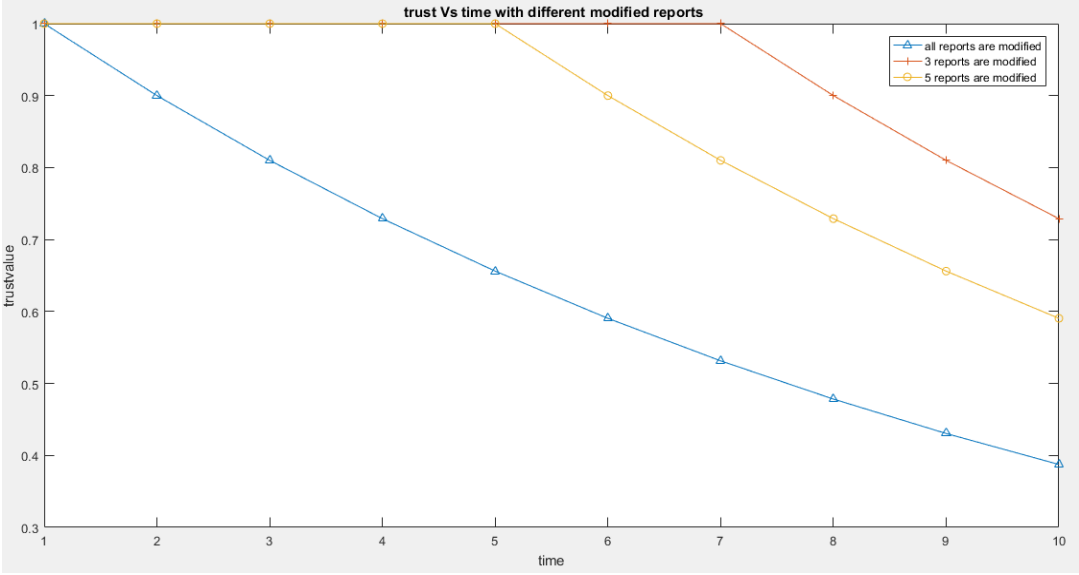

Fig 4.1 Trust value Vs Time with different altered reports

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

The fig 4.1 shows the graph between trust value of SUs at different time instants. In this the attacker modifies all of the report generated by a SU, 50 % of the report generated by a SU and 30% of the report generated by a SU. It is inferred that trust value gets decreased for each wrong decision sent by the SU. The trust value is lower for all modified reports and the next lower value is for 50% modified reports.

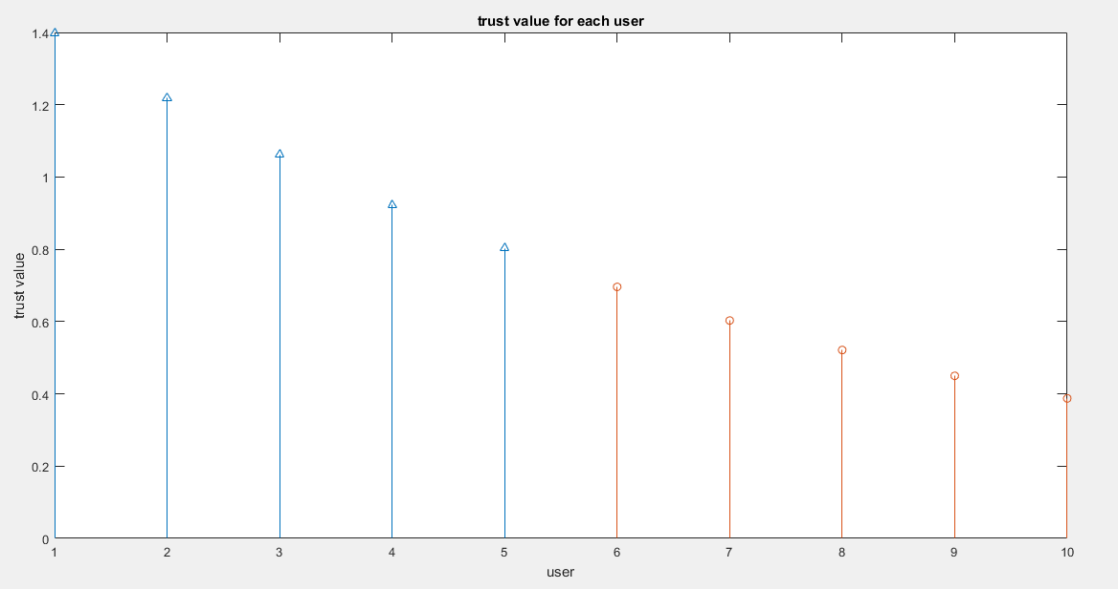

Fig 4.2 Trust value for each secondary users

The fig 4.2 shows that the trust value of each secondary user for various attack probabilities. The reward value for each correct detection is taken as 0.05. In this, user 1 is a legitimate SU with no modified result, user 2 has 1 modified result, user3 has 2 modified result such that user 10 has 9 modified result. If the trust value falls below the threshold value it is considered as an attacker. Then the attacker is exempted from CSS. In this result first 5 users are legitimate SUs others are malicious and they are exempted from CSS.

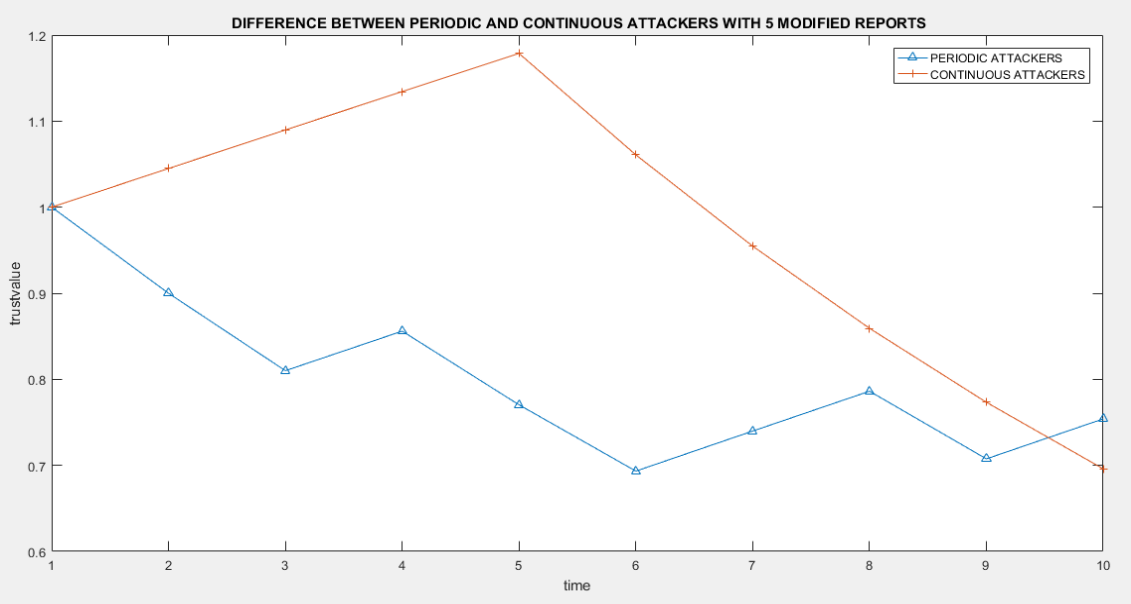

Fig 4.3 Trust value Vs Time for different types of attackers

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

The fig 4.3 shows the difference between continuous and periodic attackers. Both attackers modify 50% of the report. The Continuous attacker initially sends a correct report but after sometime it sends modified reports continuously. From the result it has been observed that the periodic attackers have slightly greater trust value than continuous attackers.

5. CONCLUSION

In this research, Spectrum Sensing Data Falsification attack (SSDF) is detected on the basis of trust value calculation using trusted users. The presence of SSDF attacker forced the FC to take false decisions about the status of the spectrum. It may leads to Denial of Service (DoS) for other secondary users. So it is necessary to detect these malicious users even though they are large in numbers and they are periodic attackers. Thus, these kinds of attacks are detected efficiently and performed cooperative spectrum sensing reliably in the proposed technique. In future, this scheme can be extended to a large area networks. Also implementation of this trust node analysis can be further helpful in detecting by zantine attack and sense of spectrum in other wireless networks applications.

REFERENCES

[1] Zhao.Q, Tong. L, Swami. A and Chen. Y, "Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMPD framework", IEEE transactions on Communications, 2007, pp.589–600.
[2] Ahmed Khattab, Dmitri Perkins and Magdy Bayomi, "Cognitive Radio Networks- from theory to practice", Springer, 2013.
[3] Steven M.kay and Stanely Lawrence, "Spectrum analysis – A modern perspective", Proceedings of the IEEE, vol. 69, 1981, pp. 1318-1480.
[4] Won-yeol lee and Ian F. Akyldiz, "A spectrum decision framework for cognitive radio networks", vol.10, 2010, pp. 1536-1233.
[5] Jianwu Li, Zeibing Feng, Zhiyong Feng and Ping Zhang, "A survey of security issues in cognitive radio networks", IEEE journal on china communications, vol. 12, 2015, pp.132-235.
[6] S.C. Wang and S.H. Kao, "A new approach for byzantine attack", IEEE conference on Information Networking", 2001, pp.518-524.
[7] Bhuvaneshwari C, Manjunathan A, "Advanced gesture recognition system using long-term recurrent convolution network", Proc. ICONEEEA, 2019 pp. 1-8.
[8] C Bhuvaneshwari, G Saranyadevi, R Vani, A Manjunathan, "Development of High Yield Farming using IoT based UAV", IOP Conference Series: Materials Science and Engineering 1055 (1), 012007
[9] A Manjunathan, C Bhuvaneshwari, "Design of smart shoes", Materials Today: Proceedings 21, 500-503
[10] C Bhuvaneshwari, SK Beevi, A Abhinaya, "Smart and Secure Industrial Environmental Pollution and Faults Identification Control System", 2020.
[11] C Bhuvaneshwari, A Manjunathan, "Reimbursement of sensor nodes and path optimization Materials" Today: Proceedings, 2020.
[12] F.Farmani, M.Abbasi-Jannatabad and R.Berangi, "Detection of SSDF Attack Using SVDD Algorithm in Cognitive Radio Networks", IEEE conference on communication system and networks", 2011.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1482 - 1491
Received 15 April 2021; Accepted 05 May 2021.

[13] ShameekBhattacharjee, SaptarshiDebroyand MainakChatterjee,"Trust computation through a nomaly monitoring in distributed cognitive radio networks", IEEE symposium on mobile radio communication, 2011, pp.593-597.
[14] Yong Han, Qiang Chen and Jian-Xin Wang, "An Enhanced D-S Theory Cooperative Spectrum Sensing Algorithm against SSDF Attack", IEEE conference on vehicular technology, 2012, pp. 1-5.
[15] Sumit Yadav and Manisha J. Nene, "RSS based detection and expulsion of malicious users from cooperative sensing in Cognitive Radios", IEEE conference on advanced computing, 2013, pp.181-184.
[16] Abbas Ali Sharifi and Mir Javad Musevi Niya, "Defense against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach", IEEE transaction on communication letters, 2016, pp.93-96.
[17] Mathew Gast, "802.11 wireless networks: The definitive guide, 2002.
[18] Saud Althunibat, Raúl Palacios and Fabrizio Granelli, "Energy-efficient spectrum sensing in Cognitive Radio Networks by coordinated reduction of the sensing users", IEEE conference on communications, 2012, pp.1399-1404.
[19] Sami Helif, Raed Abdulla and Sathish Kumar, "A review of energy detection and cyclostationary sensing techniques of cognitive radio spectrum", IEEE conference on Research and Development, 2015, pp.177-181.
[20] Ibrahim Salah, Waleed Saad, Mona Shokair and Mohamed Elkordy, "Cooperative spectrum sensing and clustering schemes in CRN: A survey", IEEE conference on Computer Engineering, 2017, pp.310-316.
[21] Dr.S.Palanivel Rajan, L.Kavitha, "Automated retinal imaging system for detecting cardiac abnormalities using cup to disc ratio", Indian Journal of Public Health Research & Development., vol. 10, pp.1019-1024, Mar. 2019.
[22] M.D.Udayakumar, G.Anushree, J.Sathyaraj, A.Manjunathan, "The impact of advanced technological developments on solar PV value chain", Materials Today: Proceedings, 2020.
[23] Raja Guru R., & Naresh Kumar P., (2021). Autonomous Unmanned Aerial Vehicle for Post-Disaster Management withCognitive Radio Communication. International Journal of Ambient Computing and Intelligence (IJACI), 12(1), 29-52.
[24] R Rajaguru, K. Vimala Devi, P Marichamy, A hybrid spectrum sensing approach to select suitable spectrum band for cognitive users, Computer Networks, Volume 180, 107387, 2020.