International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp.5024–5035

A Trust Based Cooperative Spectrum Sensing For Mitigating SSDF Attack

Kattaswamy Mergu [1]* Lathief K.A. [2] Temesgen G/Yesuse[3]

[1]*Assistant Professor, Department of Electrical and Computer Engineering, Wolaita Sodo University, Ethiopia*

[2]*Associate Professor, Department of Electrical and Computer Engineering, Wolaita Sodo University, Ethiopia*

[3]*Assistant Professor, Department of Hydraulic and Water Resource Engineering, Wolaita Sodo University, Ethiopia*

Abstract

Spectrum scarcity is the one of the major challenges in wireless communication networks. Unfortunately some frequency bands in the spectrum are largely unoccupied and also most of the time, some other frequency bands are partially occupied. This under-utilization of radio spectrum is minimized by a technique, called Cognitive radio. Due to openness of the cognitive radio, it is vulnerable to suffer from many security attacks at various layers of OSI stack. Among them, SSDF attack can incur severe impact on cooperative spectrum sensing performance, in which malicious secondary users (MUs) send false local sensing result to its neighboring secondary users or fusion center (FC). Mitigating or eliminating the SSDF attack in cognitive radio networks is a tough task. In this paper, we first discuss the various types of SSDF attacks and then concentrate on random false attack. Afterword, a trust based cooperative spectrum sensing algorithm is proposed to mitigating the random false attack. In this approach, the local sensing result of secondary users can be considered at the fusion center based on their trust values. The MATLAB simulation result shows that a trust based cooperative sensing gives better system performance comparing with traditional cooperative sensing network.

Keywords: *Cognitive Radio, Security Attacks, Spectrum Sensing, Primary User, Secondary User, Malicious User, Spectrum Sensing Data Falsification.*

1. Introduction

Joseph Mitola was introduced the concept of Cognitive Radio (CR) in a seminar in 1998 and published an article in 1999 [1]. The main goal of the cognitive radio is to evolve software defined radio as a fully reconfigurable wireless transceiver. So that it automatically changes its communication network parameters and user demands. According to many research studies, some parts of the spectrum are not used efficiently. The parts, which are underutilization are known as white spaces, have no active primary users. The basic idea behind this cognitive radio is, the secondary users (SUs) can sense the primary user's (PU) spectrum and occupy it when PU is absent. "Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind:

- Highly reliable communications whenever and wherever needed
- Efficient utilization of the radio spectrum."

ISSN: 2233-7857 IJFGCN

The four main functions of cognitive radio are: spectrum sharing, spectrum sensing, spectrum mobility, and spectrum management and decision [2].

1.1 Spectrum Sensing

Spectrum sensing is the first step in implementing the cognitive radio networks. Spectrum holes (bands not being used by the PUs) or white spaces in the spectrum, needs to be sensed efficiently, in ordered to avoid the interference. The most efficient method in this respect is the PU detection technique. Spectrum sensing techniques are classified as primary transmitter detection, cooperative detection and interference based detection [3].

1.2 Spectrum Management

Spectrum sensing can be used detect the available channels. The best channels is selected to allocate cognitive users based on channel's parameters such as data rate, error rate, primary user's statistics and secondary users QOS requirements [4]. Spectrum management decides the best available channel to be used by the cognitive users. Spectrum management is further divided into spectrum analysis and spectrum decision.

1.3 Spectrum Mobility

The change of operating frequency or band of a user is commonly referred to as spectrum mobility or handover. In cognitive radio networks, CR users don't have the idle channel information. Cognitive user should terminate its communication, when primary user of the channel becomes active in order to avoid the interference.

1.4 Spectrum Sharing

Once a cognitive radio knows about the empty spectrum or transmitting frequency band, it informs to its receiver about the transmitting frequency band so that a communication channel is established. The process is commonly referred as spectrum sharing. It can be regarded to be similar to generic MAC problems in existing systems [1].

In traditional wireless communication, the characteristics of propagation channel are uncertain and time variant. Due to shadowing effect and multipath fading, erroneous sensing results can occur frequently. Under deep fading, the cognitive user may not detect the presence of primary user at low SNR values, is called hidden node problem [5]. The reliability of spectrum sensing can be improved by cooperative sensing. Cooperative spectrum sensing can be categorized into centralized cooperative sensing and distributed cooperative sensing based on the architecture, availability of central entity and control channel quality [6] [7]. Cooperative sensing includes local sensing, fusion center and global decision making. In a centralized cooperative sensing system, all the SUs share their sensing reports to the data fusion center and receive instructions from the fusion center. In a distributed system, all the SUs share their sensing information among each other. SUs autonomously decide the channel availability by aggregating outcomes reported by other SUs.

Unfortunately, cooperative spectrum sensing is vulnerable to many security issues initiated by malicious secondary users. The most well-known and effected security threat is the spectrum sensing data falsification (SSDF) attack [8], where abnormal or malicious spectrum sensors falsify their true sensing results. SSDF attack can be further classified as hard SSDF attack and soft SSDF attack. Briefly, in hard SSDF attack, malicious SUs deal with local binary decision, where as in soft SSDF attack, malicious SUs deal with the received energy values [9].

In this paper, the author deals with the random false hard SSDF attack and propose a new cooperative spectrum sensing algorithm based on the trust vales of each secondary user.

ISSN: 2233-7857 IJFGCN

2. Literature Review

The well-known and very familiar approach to identify spectrum holes or underutilized spectrum band is the cooperative spectrum sensing network, but it is easy to incur various spectrum threats due to the openness of the cognitive radio. Among them, SSDF attack is the most vulnerable and degrades the performance of CR effectively. The motivation of the attackers behind this attack is to disturb the normal communication of primary usersand also to waste the spectrum resources by sending false information to the fusion center [10].

Several research works have been investigated to mitigate against SSDF attacks. The detection of malicious nodes in the network detected by calculating the trust factor and consistency factor for each user and the nodes, whose trust values and consistency values were less than a specific threshold value, were considered as the malicious nodes. The drawback of this method is that it assumed that only one attacker is active at a single time [11]. Hit and run attack was proposed by Noon and Li. They also proposed an algorithm to mitigate this attack, in which a suspicious point value has been calculated and this point value with a desired specific threshold. Decided whether the users is attacker or not based the point value [12]. In [13], Abhishek Kumar et.al., proposed an algorithm considers trust value of nodes along with their previous reputation. He only included nodes whose trust value and reputation values are above threshold in the sensing process and others are excluded. Another approach to mitigate SSDF attach proposed in [14], based on the analysis of node's result consistency degree and data deviation degree, a linear weighted combination scheme is designed to eliminate the effects of SSDF attacks on the final sensing decision. M. Y. Morozov et.al. proposed a combined approach to mitigate SSDF attack. On the first step tries to isolate the initially untrustworthy nodes based on a reputational method, on the second step specialized q-out-of-m fusion rule is utilized to mitigate the remains of attack [15]. Honest SU will be awarded with trust gain, while a malicious SU's trust will be penalized with trust loss approach proposed in [16] to mitigate the SSDF attack. Ping Bal et.al. [17], presented an approach based on beta reputation, in which time proportion coefficient is introduced. The reputation value of users can be obtained accordingly, besides, the rise factor and fall factor are introduced as well. In [18], in this study, the authors propose mechanisms for the detection and suppression of deleterious opportunistic users (DOUs) for hard and soft decision fusion. More specifically, a credibility-based mechanism for hard decision fusion using a hard decision combining beta reputation (HDC-BR) system is introduced. The main advantage of this method is it does not require knowledge of the total number of deleterious users in advance.

3. System Model

Consider a cooperative spectrum sensing based cognitive radio network N cognitive users transmit sensing information periodically to the central coordinator, called fusion center. In the first stage of CSS, each SUs conduct the local sensing and send it to the fusion center. The sensing results from all the SUs gathered at the FC and FC takes final decision about the presence of primary user. Local spectrum sensing for a specific spectrum band is generally formulated as a binary hypothesis as follows:

$$r_i[k] = \begin{cases} n_i[k] & \text{for } i = 1,2,..N \quad \text{under } H_0 \\ h_i[k] * s_i[k] + n_i[k] & \text{for } i = 1,2,..N \quad \text{under } H_1 \end{cases} \quad (1)$$

where H_0 is the null hypothesis, indicates the primary signal is absent and H_1 alternative hypothesis, indicates the PU is present, N is the number of cognitive users, $r_i(k)$ is the received signal of i^{th} Cognitive user's k^{th} sample , $s_i(k)$ is the transmit signal of

ISSN: 2233-7857 IJFGCN

primary user, $h_i(k)$ is the channel gain, and $n_i(k)$ denotes the additive white Gaussian noise (AWGN).

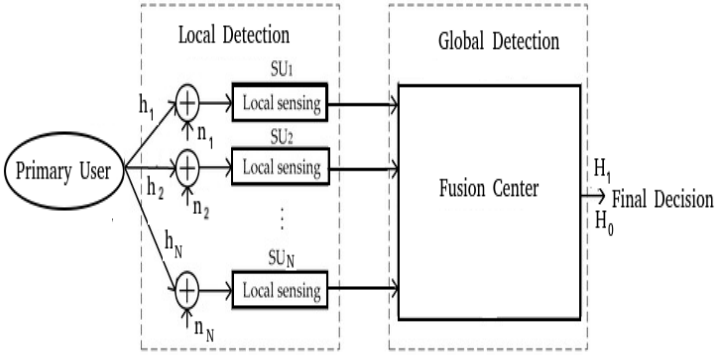

Figure 1. Typical Block Diagram of Cooperative Sensing

As shown in fig.1, cooperative sensing has two main blocks, local detection and fusion center. Local detection associated with local sensing performed by each secondary user. In the other hand, global detection is associated with fusion center. The sensing result of global detection can obtain by using fusion center. It may be either hard fusion rule or soft fusion rule. In this paper, we are considering only hard fusion rule for global sensing.

3.1 Local Sensing

The CR user itself performs spectrum sensing, is called local sensing. The most popular techniques for local sensing are energy detection (ED) and matched filter detection (MF).

Energy Detection: One of the simplest and most popular spectrum sensing techniques is the energy detection technique. Since, it does not require any prior information about the primary user signal, it is also called as blind detection [19]. Fig.2 shows the block diagram of spectrum sensing using energy detection.
The test static for energy detection is [20]

$$\text{Test Statistic} = T_{test} = \sum_{k=1}^{N} \left| r[k]^2 \right| \qquad (2)$$

The probability of false alarm and probability of detection can be defined as
The probability of false alarm is

$$P_{fa} = \int_{\gamma}^{\infty} f\left(r/H_0\right)dr = Q\left(\frac{\lambda_{ED} - N\sigma_n^2}{\sqrt{2N\sigma_n^4}}\right) \qquad (3)$$

where λ_{ED} is the threshold, Q is the Q-function
σ_n is the standard deviation of noise, P_{fa} is the probability of false alarm
The probability of detection is

$$P_d = \int_{\gamma}^{\infty} f\left(r/H_1\right)dr$$

$$= Q\left(\frac{\lambda_{ED} - N\left(\sigma_s^2 + \sigma_n^2\right)}{\sqrt{2N\left(\sigma_s^2 + \sigma_n^2\right)^2}}\right) \qquad (5)$$

ISSN: 2233-7857 IJFGCN

where σ_s is the standard deviation of signal 's' and P_d is the probability of detection.

form equation (3), the threshold can be derived as

$$\lambda_{ED} = \sigma_n^2\left(Q^{-1}\left(P_{fa}\right)\sqrt{2N} + N\right) \quad (6)$$

The main disadvantage of ED is that it is deeply affected by noise uncertainty.

Matched Filter Detection: Energy detection performs poor in the presence of additive white gaussian noise at low SNR values. Matched filter detection (MFD) can maximize the SNR for a given signal even in the presence of AWGN. Hence, MFD is the optimum detection method. The only problem with this method is, it requires the prior probabilities of the primary user's signal.

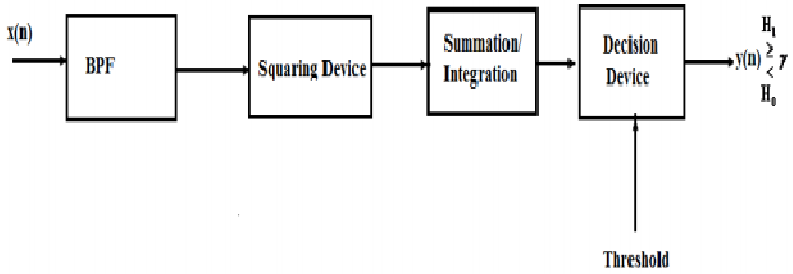

Figure 2. Block diagram spectrum sensing of Energy Detection [19]

Assuming that at time t, the received signal is r(t),
The likelihood ratio test (LRT) can be defined as

$$l(x) = \frac{f\left(r/H_1\right)}{f\left(r/H_0\right)} = \frac{P_1(r)}{P_0(r)} \gtrless \eta \quad (7)$$

Where η is the threshold value

$f\left(r/H_1\right)$ and $f\left(r/H_0\right)$ are prior probabilities of primary user und hypothesis H_1 and H_0 respectively.

According to the Neyman-Pearson criterion,
The test statistic can be defined as

$$T_{test} = \sum_{k=1}^{N} r[k]s^*[k] \quad (8)$$

Probability of false alarm and Probability of detection can be defined as
Probability of false alarm is

$$P_{fa} = Q\left(\frac{\eta'}{\sqrt{\xi\sigma_n^2}}\right) \quad (9)$$

The probability of detection is

$$P_d = Q\left(\frac{\eta' - \xi}{\sqrt{\xi\sigma_n^2}}\right) \quad (10)$$

From equation 8, threshold can be defined as

$$\eta' = \sqrt{\xi\sigma_n^2}\, Q^{-1}\left(P_{fa}\right) \quad (11)$$

ISSN: 2233-7857 IJFGCN

3.2 Global Detection

Global Detection results can be obtained by fusion center (FC). Generally, it is of two types named as hard fusion rule and soft fusion rule. In the case of soft fusion rule, each secondary user forwards only binary spectrum sensing to the FC. However, for the soft decision rule, each secondary user sends the entire energy result to the FC.

Hard fusion rule further classified as OR rule, AND rule and Majority rule. All these methods are special cases of K out N rule. This K out of N rule also referred as counting rule, where N is the total number of cognitive users and K is the number of cognitive users that have decided that spectrum band is occupied.

i. OR rule: In this case, if any one of the cognitive users send the sensing report as 'channel is busy' to the fusion center, then the FC decides the global decision as the channel is occupied i.e. K=1[21]. Sometimes, a secondary user may give false sensing results due to shadowing effect, multi path fading or noise uncertainty in the wireless communication channel. Hence, even though it increases PU protection, it is inefficient in spectrum utilization.

The global probability of detection and probability of false alarm can be obtained as

$$\left(P_{d\,OR}\right)_{global} = 1 - \prod_{k=1}^{N} 1 - \left(P_{dk}\right)_{local} \qquad (12)$$

$$\left(P_{f\,OR}\right)_{global} = 1 - \prod_{k=1}^{N} 1 - \left(P_{fk}\right)_{local} \qquad (13)$$

where Pfk and Pdk are the local probability of false alarm and probability of detection for kth cognitive user respectively.

ii. **AND-Rule:** In this rule, if and only if all the secondary users send their sensing report as 'channel is busy',then that channel decision taken by the FC is occupied i.e. K=N. Because of channel uncertainty, shadow effect in the wireless channel, even though it increases the spectrum utilization, it increases the risk of interference with the PU [20]. The global probability of detection and probability of false alarm can be obtained as

$$\left(P_{d\,AND}\right)_{global} = \prod_{k=1}^{N} \left(P_{dk}\right)_{local} \qquad (14)$$

$$\left(P_{f\,AND}\right)_{global} = \prod_{k=1}^{N} \left(P_{fk}\right)_{local} \qquad (15)$$

where P_{fk} and P_{dk} are the local probability of false alarm and probability of detection for k^{th} cognitive user respectively.

iii. Majority K out of N-Rule: if at-least half of the cognitive users decide that the channel (band) is busy, then the FC decides that the channel is occupied i.e. K=N/2 [20]. It compromises between the spectrum utilization and protection of PU.

The global probability of detection can be obtained as

$$\left(P_{d\,MAJORITY}\right)_{global} = \sum_{m=k}^{N} \binom{N}{m} P_{d,i}^{m} \left(1 - P_{d,i}\right) N - m \qquad (16)$$

where $P_{d,i}$ is probability of detection for each individual cognitive user.

4. SSDF Attack and Its Mitigation Strategy

ISSN: 2233-7857 IJFGCN

In cognitive radio, malicious secondary users send the false information about the presence of primary user to the fusion center causing the FC to make the final decision wrong. This type of attack is known as spectrum sensing data falsification (SSDF) attack. The main intention behind this attack is to disturb the primary user's communication and/or to gain the spectrum resources maximum. SSDF is the one of the most effective attack in the cognitive radio networks. The SSDF attack is illustrated in fig.3. The local spectrum sensing results must be robust and trusty in the CSS networks, to maintain adequate level of accuracy in the sensing decision.
Generally, SSDF attack further classified as follows

i. Always Yes Attack:The malicious secondary user always sends the sensing report to the fusion center as '1' even the channel is free i.e. it sends always the spectrum band is busy even though it is free. A special type of always yes attack is *Random Yes Attack*, in which malicious secondary user sends that the channel is busy with a probability of α .

ii.Always No Attack:The malicious user always sends the sensing report to the fusion center as '0' even the channel is busy i.e. even though channel is busy, the attacker sends the false information to the fusion center that channel is free. Random No Attack is special case of always no attack, in which the attacker sends that the spectrum is free with a probability of α .

iii.Always False Attack :The malicious user sends the sensing report always opposite to the sensing report obtained originally to the fusion center i.e. the attacker sends '1' when it receives '0' and '0' when it receives '1' i.e it gives always wrong decision to the FC.

A special case of always false attack is the random false attack, in which the attacker sends wrong information to the fusion center with a probability of α .
The proposed algorithm mainly concentrated on mitigating random false attack only. Firstly, we performed local spectrum sensing by energy detection and matched filter detection then global sensing can be performed by hard fusion rule based cooperative sensing.

4.1 The Proposed Algorithm

In this algorithm, the cognitive user or secondary user, who wants to find the empty spectrum for its operation, will find the local sensing report itself and sends it to the fusion center (FC).Then, FC will collects the local sensing reports from all the secondary users and compare the sensing report of each secondary users with the sensing report of honest cognitive user (who wants the empty spectrum). If any of cognitive radio sensing report does not match with the honest secondary user, the FC excludes its sensing result for the final decision. This process continued for a number of cycles. As the number of cycles increase, the cognitive radio network performs well.

ISSN: 2233-7857 IJFGCN

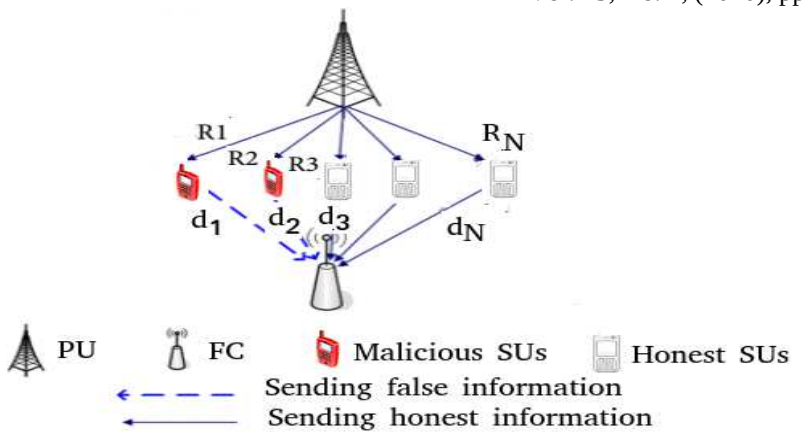

Figure 3. Random false SSDF attack

The algorithm is as follows.

step 1: Performing local sensing by using both energy detection and matched filter detection and sends it to the FC

step 2: FC collects the sensing results from all CRs

step 3: Compare the sensing results of each CR with the honest CR's sensing report

If decision belongs to malicious user decision

if rand(1,1)>pm % pm is the probability that a malicious cognizant user will misinterpret the perception, because there may be a shadowing effect, and some malicious users will occasionally provide the correct perception

sens_data(p,d)=honest_data(p)

else

sens_data(p,d)=1-honest_data(p)

else

if rand(1,1)>cm % cm is the probability of normal user error perception, because there may be a shadow effect, some users will occasionally provide false perception

sens_data(p,d)=honest_data(p)

else

sens_data(p,d)=1-honest_data(p)

response=response+1

if sens_data=honest_data

honest_response= honest_response+1

end

if response==0

trust_value=0

else

trust_value=honest_response/response

repeat for a number of cycles, as no. of cycle increases the better trust value.

5. Results and Discussion

We consider a cognitive radio network (CRN) with a total of 15 SUs and 20 percent of CRs as malicious users. The results obtained are averaged over 50 cycles or iterations. In this paper, we consider only Random False Attack, in which the attacker sends false information randomly with a probability of predefined value. Here, we consider probability of misperception by malicious secondary user as 0.7 and probability of mispercetion by honest secondary user as 0.3. The mispercetion probability is mainly based on the channel characteristics such as multipath fading, shadowing and time varying behavior of channel.

ISSN: 2233-7857 IJFGCN

Firstly, we compare the simulation results of cooperative sensing using energy detection and matched filter with and without trust value as shown in fig.4. It is clearly notified that comparing with energy detection based cooperative sensing matched filter based cooperative sensing performs very well. The detain Pf vs Pd observations are given in Table. 1

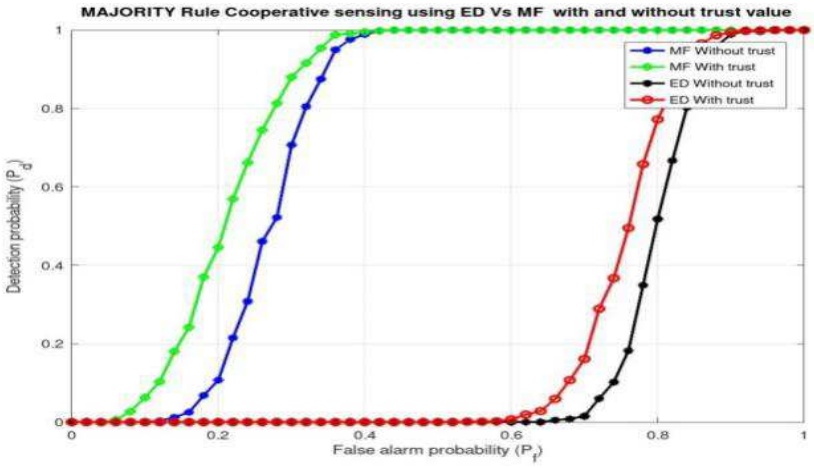

Figure 4. Comparison of Cooperative sensing using energy detection and matched filter with and without trust value

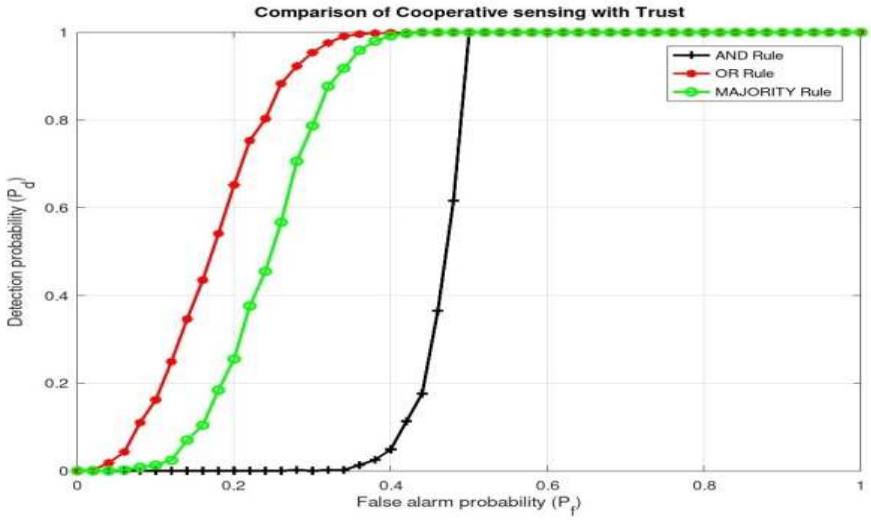

Figure 5. Comparison hard fusion rule based cooperative sensing

Second simulation result shows the comparison of basic three hard fusion rules such AND, OR and MAJORITY rule of cooperative sensing. It is given in Fig.5. From the figure, it is clearly observed that AND rule performs poorly and OR gives the better probability of detection whereas MAJORITY rule compromises both. Even though OR rule gives better probability detection or protection of primary user it is inefficient in spectrum utilization since the decision is based on single user.

We also compare the performance of cooperative sensing with matched filter detection with different number of cognitive users. As the number of cognitive users increases in the network, it is more vulnerable to the security threats. From fig.6, at false rate 0.3, the probability of detection is 0.45 for number of users is 5 and it is 0.25 and 0 for the case of number of users 10 and 20 respectively.

ISSN: 2233-7857 IJFGCN

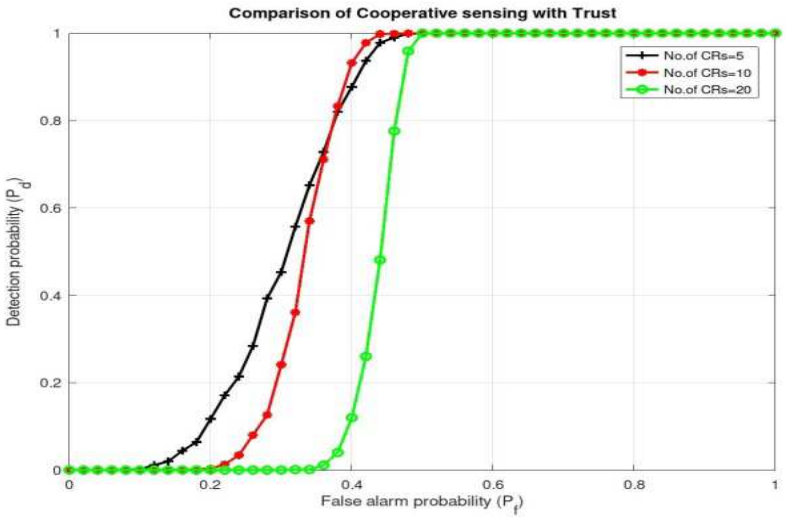

Figure 6. Performance of cooperative with different number of cognitive users

Table 1. Cooperative sensing using energy detection and matched filter detection with and without trust value

Probability of false alarm (Pf)	Energy detection		Matched filter detection	
	P_d without trust	P_d with trust	P_d without trust	P_d with trust
0	0	0	0	0
0.2	0	0	0.1	0.41
0.4	0	0	0.97	0.99
0.6	0	0.05	1	1
0.8	0.5	0.79	1	1
1	1	1	1	1

6. Conclusion

In this paper, we present a simple approach to mitigate SSDF attack based on the trust value. The FC restricts the SSDF attack by including or excluding a cognitive user for final decision of spectrum allocation based on its trust value. We observe through MATLAB simulation that the trust based cooperative sensing is more effective in determining attackers as comparing with the conventional cooperative sensing technique while false detection is minimal. We also observed that matched filter based cooperative sensing performed well as compared with energy detection based cooperative sensing.

ISSN: 2233-7857 IJFGCN

In this article, we consider only AWGN channel as experimental purpose, in future we will examine SSDF attack and mitigation of SSDF based on trust values in time varying channels such as Rayleigh and Rician channels.

Conflicts of Interest

The authors declare that there is no conflict of interest in this research work.

References

[1] J. Mitola III, "Cognitive radio: an integrated agent architecture for software defined radio", PhD thesis, KTH Royal Institute of Technology. Stockholm, Sweden, 2000.

[2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey", Computer Networks, 50(13), pp. 2127 – 2159, 2006.

[3] Jai Sukh Paul Singh, Jasvir Singh, A.S. Kang, "Cognitive Radio: State of Research Domain in Next Generation Wireless Networks - A Critical Analysis", International Journal of Computer Applications, 74(10), pp.1-9, 2013.

[4] Marinho, J. Monteiro, E., "Cognitive radio: Survey on communication protocols, spectrum decision issues, and future research directions", Wirel. Netw. pp. 147–164, 2012.

[5] I.F. Akuildiz, B.F. Lo and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey", Physical Communication, 4(1): pp. 40-62, 2011.

[6] T.Yucek and H.Aslan, "A survey of spectrum sensing algorithms for cognitive radio application", IEEE communication surveys and tutorial, 11(1), pp.116-130, 2009.

[7] Moshe Timothy Masonta, Mjumo Mzyece and Ntsibane Ntlatlapa, "Spectrum decision in cognitive radio networks: A survey", IEEE communications surveys & Tutorials, 15(3), pp. 1088-1107, 2013.

[8] R Chen, JM Park, YT Hou, "To ward secure distributed spectrum sensing in cognitive radio networks", IEEECommun., Mag. 46(4), pp.50–55, 2008.

[9] Linyuan Zhang, Qihui Wu, Guoru Ding, Shuo Feng and Jinlong Wang, "Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing", EURASIP Journal on Advances in Signal Processing, pp.1-9, 2014.

[10] Sharifi A., "Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach",IEEE Communication Letter, 20(1), pp.93–96, 2016.

[11] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks", 43rd Annual Conference on Information Sciences and Systems. IEEE. pp. 130–134, 2009.

[12] E. Noon and H. Li., "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system", IEEE 71st Vehicular Technology Conference. pp. 1–5, 2010.

ISSN: 2233-7857 IJFGCN

[13] Kumar, Abhishek, Gupta, Nitin, Tapwal, Riya, "Trust Aware Scheme based Malicious Nodes Detection under Cooperative Spectrum Sensing for Cognitive Radio Networks", TechRxiv. Preprint, 2020.

[14] Runze Wan , Lixin Ding, Naixue Xiong and Xing Zhou, "Mitigation strategy against spectrum sensing data falsification attack in cognitive radio sensor networks", International Journal of Distributed Sensor Networks, 15(9), pp. 1-12, 2019.

[15] M. Y. Morozov, O. Y. Perfilov, N. V. Malyavina, R. V. Teryokhin and I. V. Chernova, "Combined Approach to SSDF-Attacks Mitigation in Cognitive Radio Networks", Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, pp.1-4, 2020.

[16] J. Wang, I. Chen, J. J. P. Tsai and D. Wang, "Trust-based cooperative spectrum sensing against SSDF attacks in distributed cognitive radio networks", IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR 2016), Stevenson. pp. 1-6, 2016.

[17] P. Bai, X. Zhang and F. Ye., "Reputation-based Beta reputation system against SSDF attack in cognitive radio networks", Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL), Singapore. pp. 792-799, 2017.

[18] K. Arshad and K. Moessner, "Robust collaborative spectrum sensing in the presence of deleterious users", IET Communications, 7(1), pp. 49-56, 2013.

[19] Kattaswamy Mergu, "Spectrum sensing using Neyman-Pearson based matched filter detection in cognitive radio networks", Journal of basic and applied research international, 21(3), pp.143-149, 2017.

[20] Srinivas Nallagonda, Shravan Kumar Bandari, Sanjay Dhar Roy and Sumit Kundu, "On Performance of Weighted Fusion Based Spectrum Sensing in Fading Channels", Journal of computational engineering, 2013.

[21] Abdorasoul Ghasemi, and E.S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments", New Frontiers in Dynamic Spectrum Access Networks, DySPAN, 2005.

ISSN: 2233-7857 IJFGCN