IJE TRANSACTIONS C: Aspects Vol. 34, No. 6, (June 2021) 1468-1474

International Journal of Engineering

Journal Homepage: www.ije.ir

Mitigation of Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks using Trust Based Cooperative Sensing

K. Mergu*[a], H. Khan[b]

[a] *Department of Electronics and Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences, Madya Pradesh, India*
[b] *Department of Electronics and Communication Engineering, K. L. Deemed to be University, India*

PAPER INFO

Paper history:
Received 08 August 2020
Received in revised form 14 April 2021
Accepted 04 May 2021

Keywords:
Cognitive Radio
Security Attacks
Spectrum Sensing Data Falsification
Cooperative Spectrum Sensing Primary User
Secondary User

ABSTRACT

One of most emerging technology in recent years in the field of wireless communication is the Cognitive Radio (CR) technology, which reduces spectrum scarcity significantly. The main function of CR technology is detecting spectrum holes or unused spectrum of primary users (PUs), also called as licensed users, and assigning this unused spectrum to the secondary users (SUs), also called unlicensed users. As the CR technology is open to every user, there are many security issues such as Primary User Emulsion Attack (PUEA), Jamming Attack, Spectrum Sensing Data Falsification (SSDF) Attack, Lion Attack, and Sink Hole Attack and so on. SSDF attack is the one of major security attack in cognitive radio in which a malicious user sends false data intentionally to the other secondary users. The main aim of the SSDF attack is to disturb the communication between the secondary users or to gain more channel resources. One of the solutions to mitigating SSDF attack is the cooperative spectrum sensing. In this paper, we propose a new algorithm of cooperative sensing based on trust values of secondary users, and compares with the conventional cooperative spectrum sensing with the proposed algorithm. In this algorithm, firstly the CR which is waiting for the channel allocation sense the information and compare the sensing information of other CRs. If any CR's sensing report not matches with the test CR's sensing with in the cluster, it will punish that CR otherwise it will give the reward. This procedure will be repeated for number of cycles. Finally test CR calculates the trust value. Based on the trust value fusion center will take the decision to include or exclude the trusting value of particular CR. The simulation of cooperative sensing also performed in both time variant channel and time invariant (Rayleigh) channel. The authors also compare the three basic hard fusion techniques such as AND, OR, MAJORITY rule.

***doi**: 10.5829/ije.2021.34.06c.10*

NOMENCLATURE

CR	Cognitive Radio	H_1	Alternative Hypothesis
SS	Spectrum Sensing	P_{fa}	Probability of False alarm
PU	Primary User	P_d	Probability of Detection
SU	Secondary User	P_m	Probability of Miss Detection
MU	Malicious User	N	Number of Cognitive Radio Users
Centralized CSS	Centralized Cooperative Sensing	**Greek Symbols**	
Distributed CSS	Distributed Cooperative Sensing	λ_{ED}	Threshold of energy detection
H_0	Null Hypothesis	σ_W	Variance of noise

1. INTRODUCTION

The applications of wireless communications networks increase rapidly in the recent years; which lead to a major problem of spectrum scarcity. Since the available spectrum is fixed. However, a large amount of assigned spectrum is not utilized efficiently by the licensed user. One solution to the spectrum scarcity and utilization of low spectrum is that opportunistic access of the valid spectrum band should be assigned to unlicensed secondary users [1].

*Corresponding Author Email: kattaswamy@gmail.com (K. Mergu)

Please cite this article as: K. Mergu, H. Khan, Mitigation of Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks using Trust Based Cooperative Sensing, International Journal of Engineering, Transactions C: Aspects Vol. 34, No. 6, (2021) 1468-1474

Cognitive Radio uses a technology called spectrum sensing that sense the unused spectrum or ERD empty spectrum and assigns this spectrum to unlicensed users and avoid any collision and minimize harmful interference to the licensed users. The detection accuracy of spectrum sensing determines the performance of the whole CR systems to a great extent [2]. According to Kattaswamy [3], the spectrum user signals are categorized into primary users (PUs) signals, having licensed spectrum band and secondary users (SUs) signals, do not have any licensed spectrum band. Cognitive Radio cycle includes, spectrum sensing, spectrum decision, spectrum sharing and spectrum mobility [3].

Spectrum Sensing: sense the surrounded RF spectrum to detect unused spectrum or spectrum hole and determine the presence of the primary user.

Spectrum Decision: finding which spectrum band/hole is suitable for satisfying the requirements of application.

Spectrum Sharing: share the information about the empty spectrum to other secondary user.

Spectrum Mobility: when primary user is present, switch to another suitable empty spectrum band to avoid interference.The performance of the whole CR system can be evaluated by the detection accuracy of the spectrum sensing techniques. The time varying characteristics of wireless channel, multipath fading and shadowing effect leads to erroneous sensing decisions and result in inefficient spectrum utilization or interference with the primary user [4]. Cooperative Spectrum sensing gives the better solution to the above. It improves the reliability of spectrum utilization. In cooperative sensing, the individual sensing nodes cooperate each other by sharing detection decisions to detect the presence of primary user.

Spectrum Sensing techniques are divided into two types:

i. Local Spectrum Sensing

ii. Cooperative Spectrum Sensing

Local spectrum sensing, performed by each individual CR. It is associated with many challenges which make it difficult to detect vulnerability. Some of them are sensitivity requirement, receiver uncertainty, hidden node problem [5]. Cooperative Sensing provides better way for all the above challenges. Cooperative spectrum sensing can be classified as either centralized or distributed based on the architecture, central entity availability, quality of the control channel [6], [7].

The process of CSS includes three main steps. They are local sensing, reporting to the fusion center (FC), and global decision making [5].

Centralized CSS: It is the most popular architecture. It consists of central entity also called fusion center and a number of SUs associated with it [8,9]. In this approach, each SUs executes local spectrum sensing individually and forward their decision to the FC as one bit (hard fusion) or as raw data (soft fusion). Finally, FC collects the data and combines the result of all SUs according to fusion rule and makes final decision about the PU existence.

Distributed CSS: all the SUs share their information among each other through the multiple iterations until a consensus is reached [10]. Cognitive user sends the local spectrum sensing results to other adjacent SUs, then the cognitive user fuses the received data to make final decision. Finally, if empty spectrum is not detected, SUs repeat the process iteratively until a unanimous final decision is reached [5].

As we know that, cognitive radio technology is open to every user, it is easy to incur various kinds of security attack at different layers. Some of them are, primary emulsion attack (PUEA), spectrum sensing data falsification (SSDF) attack, jamming attack and so on.

The SSDF attack is the attack made by a malicious user by false information intentionally to other secondary users or fusion center [11] during the process of cooperative sensing. It will leads a serious damage on reliability of cooperative spectrum sensing. Hence, it is necessary design a secure and effective cooperative spectrum sensing to resist SSDF [4].

In this paper, the authors discuss the various types of ssdf attacks and proposes a new algorithm for cooperative sensing based on trust values of individual cognitive users. The author also compares the detection performance of conventional cooperative sensing and proposed cooperative spectrum sensing with different hard fusion rules.

2. SYSTEM MODEL

Consider a cognitive radio network of N cognitive/secondary users and one fusion center (FC). A CR user uses conventional energy detection (ED) with threshold λ_{ED} makes the binary decision (either '0' or '1' bit) over a fading or shadowing channel.

We assumed that all the CR users use the same threshold. The detection of primary signal presence in the spectrum band can be obtained based on the binary hypothesis given below:

$$y[k] = \begin{cases} w[k] \text{under} H_0 \\ h * x[k] + w[k] \text{under} H_1 \end{cases} \quad (1)$$

where w[k]= additive white gaussian noise with zero mean and variance.

x[k]=the primary user's signal

h=channel gain

H0=null hypothesis, indicates the primary user's signal is absent

H1=null hypothesis, indicates the primary user's signal is present

2. 1. Local Sensing by Energy Detection It is the simplest and most popular spectrum sensing technique. It is also called as blind detection technique, does not require prior information about the primary user [3]. The block diagram of spectrum sensing using energy detection is shown in Figure 1.

The test static for energy detection is [12]:

$$\text{Test Statistic}=T_{test}=\sum_{k=1}^{N}|y[k]^2| \quad (2)$$

According to the central limit theorem, if the number of samples(N) is large (N>250) enough, the pdf of any signal approach to a Gaussian distribution [3]. Hence, the probability of false alarm and probability of detection can be defined in Equation (3). The probability of false alarm is:

$$P_{fa}=\int_{\gamma}^{\infty} f(y/H_0)dy=Q\left(\frac{\lambda_{ED}-N\sigma_w^2}{\sqrt{2N\sigma_w^4}}\right) \quad (3)$$

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

$$P_d=\int_{\gamma}^{\infty} f(y/H_1)dy=Q\left(\frac{\lambda_{ED}-N(\sigma_x^2+\sigma_w^2)}{\sqrt{2N(\sigma_x^2+\sigma_w^2)^2}}\right) \quad (4)$$

σ_x is the standard deviation of signal x form Equation (3), the threshold can be derived as:

$$\lambda_{ED}=\sigma_w^2\left(Q^{-1}(P_{fa})\sqrt{2N}+N\right) \quad (5)$$

2. 2. Hard Fusion Rule Firstly, every SU makes a decision locally and sends it to the fusion center. Then, FC applies a linear fusion rule and makes overall decision about the PU existence. Hard decision rules are classified as OR, AND, MAJORITY rules. These are special cases of Kout N rule [9]. Kout of N rule also known as counting rule. Here, N is the total number of cognitive users and K is the number of cognitive users that have decided that spectrum is used.

i. OR-Rule: The spectrum band is assumed to be occupied, if at-least one of the cognitive user decides that the channel (band) is busy i.e. K=1 [8]. Even though it increases PU protection, decreases the efficiency of spectrum utilization. Because, there is possibility that the given CR may sense the spectrum false due to shadowing and multipath fading. Hence, the final decision may be taken by fusion center that the channel is busy.

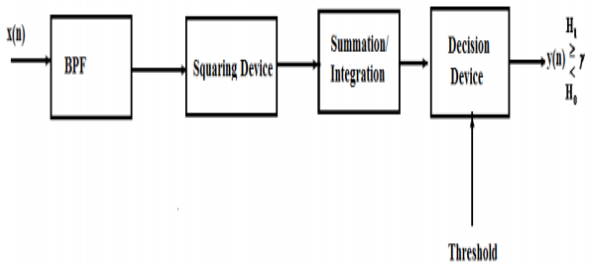

Figure 1. Block diagram of Spectrum sensing using Energy detection [3]

The global probability of detection can be obtained as:

$$Q_{dOR}=1-\prod_{k=1}^{N}(1-P_{dk}) \quad (6)$$

The global probability of false alarm can be obtained as:

$$Q_{fOR}=1-\prod_{k=1}^{N}(1-P_{fk}) \quad (7)$$

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

ii. AND-Rule: The spectrum band is assumed to be occupied, if all the cognitive users decide that the channel (band) is busy i.e. K=N. Although the AND rule based cooperative sensing increases the spectrum utilization but also it increases the risk of interference with the PU [12]. Due to the shadowing effect or multipath path there may be a possibility that any one of the CR reports false information. Then, FC declares that channel is free leads to CR inference with the PU.

The global probability of detection can be obtained as:

$$Q_{dAND}=1-\prod_{k=1}^{N}(1-P_{dk}) \quad (8)$$

The global probability of false alarm can be obtained as:

$$Q_{fAND}=1-\prod_{k=1}^{N}(1-P_{fk}) \quad (9)$$

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: The spectrum band is assumed to be occupied, if at-least K cognitive users decide that the channel (band) is busy i.e. K=N/2 [12]. It compromises between the spectrum utilization and protection of PU.

The global probability of detection can be obtained as:

$$Q_{dMAJORITY}=\sum_{m=k}^{N}\binom{N}{m}P_i^m(1-P_i)^{N-m} \quad (10)$$

where P_d is probability of detection for each individual cognitive user.

3. SSDF ATTACK AND ITS MITIGATION STRATEGY

SSDF is the most effective attack in the cognitive radio networks by the malicious secondary users. An attacker may send the false local spectrum sensing results to fusion center (FC) causing the FC to make the final decision wrong. The SSDF attack is illustrated in Figure 2. 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 attacks further classified as follows

i. Always Yes Attack: The malicious user sends the decision to the fusion center always '1' even the channel is free.

ii. Always No Attack: The malicious user sends the decision to the fusion center always '0' even the channel is occupied.

ii. Randomly False Attack: The malicious user sends the decision to the fusion center '1' when it receives '0' and '0' when it receives '1' i.e. it gives always wrong decision to the FC.

In this section, we are assumed that the local sensing technique is energy detection and also we concentrated only on mitigating randomly false SSDF attack based on the trust values of SUs.

3. 1. Proposed Algorithm

This algorithm is mainly based on trust value of the neighboring cognitive users. In this algorithm, firstly, the secondary user who want to use the spectrum hole, will find the local spectrum decision of itself. Then, it collects the spectrum result of neighboring secondary users. It compares spectrum results with the neighbor's spectrum result for number of cycles. If the spectrum decision of neighboring user's matches with its spectrum decision, it gives the trust value to them otherwise it neglects the decision of that user while performing the global decision. The flow chart of proposed trust based algorithm is shown in Figure 3.

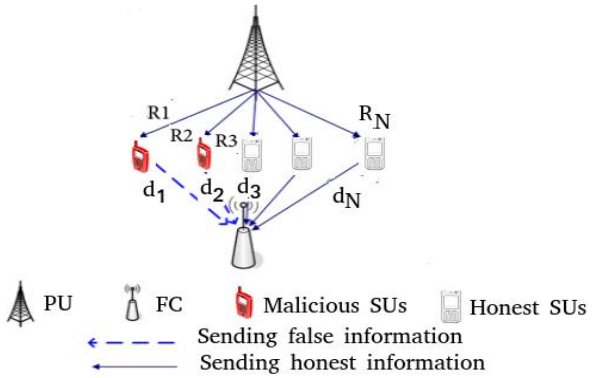

Figure 2. Random false SSDF attack

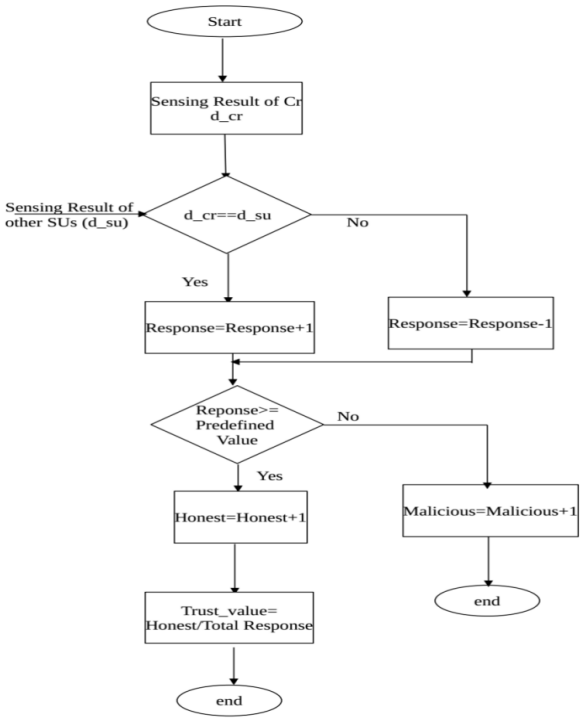

Figure 3. Flow chart of Proposed trust value algorithm

The algorithm is as follows

Input: No. of cognitive users (N), No.of cycles (Count)

Output: trust_value

Intialize: local sensing decision of cr (d_cr), local sensing decision of other secondary users (d_su), decision of malicious user (d_mu), decsion of honest user (d_hu).

1. **for** k=1 to count **do**
2. **if** d_cr==d_su **then**
3. response=response+1
4. **else**
5. response=response-1
6. **end if**
7. **if** response<= presdefined_value **then**
8. d_mu=d_mu+1
9. **else**
10. d_hu=d_hu+1
11. **end if**
12. trust_value=d_hu/total response
13. **end for**

4. RESULTS

The performance evaluation of proposed approach is obtained by using Matlab simulation. The simulation is performed based on cyclic fusion rule. At each cycle, only few of SUs are selected

for cooperation to calculate the trust value. The description of simulation elements are shown in Table 1.

Figure 4 shows the simulation of comparison between the hard fusion techniques without and without trust value. From the figure, it is clear that, OR rule based cooperative sensing gives the best probability detection and AND rule based cooperative technique gives poor performance comparing with MAJORITY rule. As we know that OR rule based cooperative technique decides that channel is busy if at-least one user decision is busy. It may gives the false decision because of misinterception of honest user due to shadowing and multipath fading.

Similarly, AND rule based cooperative technique gives false decision since it decides based on all secondary users decision. If any of honest user misinterception due to shadowing and multipath fading, it gives poor performance. Hence MAJORITY rule which takes the decision based on the majority of the secondary users. The comparison between the AND rule, OR rule and Majority rule with trust value and without trust value based cooperative sensing shown in Figure 4. It is observed that at probability of false alarm equals to 0.3, the probability of detection of AND rule, OR rule, Majority rule without trust value and with trust value are 0, 0.2, 0.5 and 1, respectively. Hence, trust value based cooperative sensing with majority rule perfoms better than the other three techniques.

The comparison of fixed threshold and adaptive threshold based on majority rule with and without trust value is shown in Figure 5. It is clear that adaptive threshold based cooperative sensing performs better than the fixed threshold based cooperative sensing. We also seen from the figure that adaptive threshold based cooperative sensing with trust value gives greater perfomance.

The performance of simulation of majority rule based cooperative sensing in both time variant and time invariant channel also compared as shown in Figure 6.

TABLE 1. Description of simulation elements

Parameter	Description	Value
N	No. of cognitive Users	10
P	No. Of PUs	2
Cycles	No. of cycle simulations	50
Mal	No. of malicious users	3
Threshold	threshold for trust value	0.6
pm	probability of misperception of malicious users	0.7
cm	probability of misperception of honest users	0.3
n	no. of CR selected randomly for cooperation	7

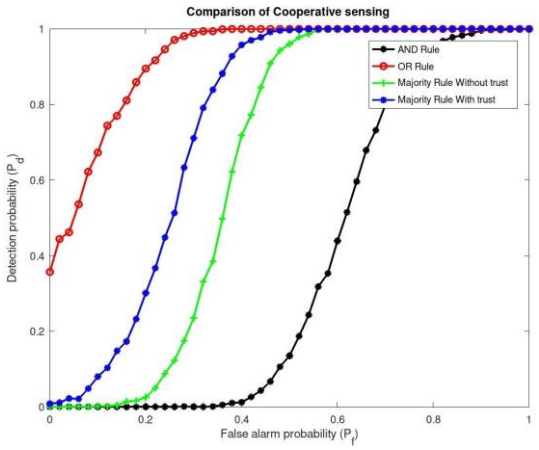

Figure 4. Comparison OF Cooperative sensing techniques with and without trust value

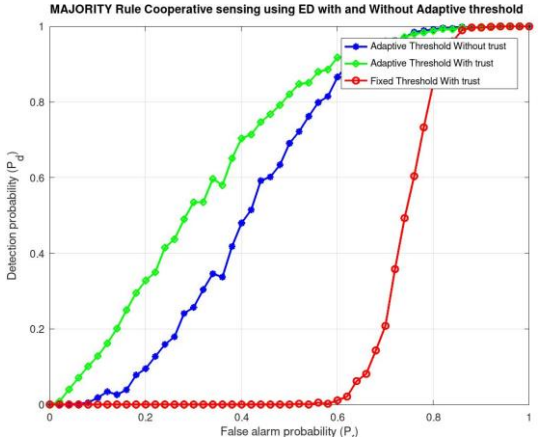

Figure 5. Comaprison of fixed threshold and adaptive threshold based majority rule with and without trust value

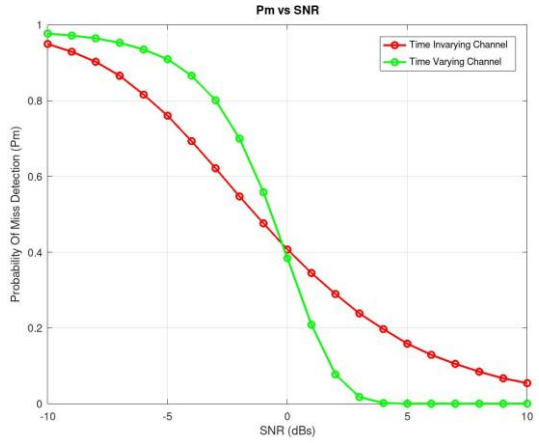

Figure 6. Comparison of Probability of miss dtection Vs SNR in both time variant and time invariant channel

The probability of miss detection in time varying channel is higher than the time in varying channel at low snr values. As SNR value increases, the probability

of miss detection decreases rapidly in time varying channel comparing with the time in varying channel based on the trust value.

The performance of three hard fusion rules such as AND, OR and MAJORITY rules with and without trust value with different probability of false alarm and probability of detection is given in Table 2.

TABLE 2. Comparison of Hard fusion cooperative sensing with and without trust

Probability of false alarm (Pf)	AND Rule		OR Rule		Majority Rule	
	P_d without trust	P_d with trust	P_d without trust	P_d with trust	P_d without trust	P_d with trust
0	0	0	0.35	0.33	0	0.08
0.2	0	0	0.86	0.83	0.01	0.52
0.4	0	0.05	1	1	0.59	0.95
0.6	0.06	0.48	1	1	1	1
0.8	0.8	0.95	1	1	1	1
1	1	1	1	1	1	1

5. CONCLUSION

The above simulation shows that the trust based cooperative sensing cognitive radio networks gives better performance comparing with conventional cooperative sensing. It is known that OR rule gives better detection probability but it suffers with the interference risk and it is not suggestible. Even though AND rule reduces the risk of interference but it suffers with another problem i.e. inefficient utilization of spectrum . Majority rule based cooperative sensing compromises the interference risk and inefficient utilization of spectrum. Hence majority rule suggestible in most of cooperative sensing cognitive networks. We also conclude that the adaptive threshold based cooperative sensing with trust value performs better than the fixed threshold cooperative sensing. In this paper we concentrated only randomly false attack. In future, we will further investigate about always yes attack and always no attack mitigation techniques.

6. REFERENCES

1. J. Mitola.,"Cognitive radio: An integrated agent architecture for software defined radio". Ph.D. Dissertation. Royal Institute of Technology (KTH), 2000, Stockholm, Sweden.
2. Ali A and Hamouda W, "Advances on spectrum sensing for cognitive radio networks: Theory and applications." ***IEEE Communications Surveys & Tutorials***, Vol. 19, No. 2, (2016), 1277-1304
3. Kattaswamy Mergu., "Spectrum sensing using Neyman Pearson based matched filter detection in cognitive radio networks". ***Journal of Basic and Applied Research International,*** Vol. 21, No. 3, (2017), 143-149
4. Runze Wan, Lixing 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,*** Vol. 15, No. 9, (2019), 1-12.
5. I.F. Akuildiz, B.F. Lo and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey". ***Physical Communication,*** Vol. 4, No. 1, (2011), 40-62.
6. Youness Arjoune and Naima Kaabouch, "A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions." ***Sensors,*** Sensors 2019, No. 1, 1-32. DOI: 10.3390/s19010126
7. Kenan kockaya1 and Ibrahim Develi, "Spectrum sensing in cognitive radio networks: threshold optimization and analysis". ***EURASIP Journal on Wireless Communications and Networking,*** (2020) 2020:255, 1-19. https://doi.org/10.1186/s13638-020-01870-7
8. Abdorasoul Ghasemi, and E.S. Sousa., "Collaborative spectrum sensing for opportunistic access in fading environments." ***New Frontiers in Dynamic Spectrum Access Networks,*** DYSPAN (2005).
9. E.Peh and Y.-C. Liang. "Optimization for cooperative sensing in cognitive radio networks." Wireless Communications and Networking Conference, IEEE (2007), 27-33.
10. Z.Li, F.R. Yu and M. Huang., "A cooperative spectrum sensing consensus scheme in cognitive radio." ***INFOCOM,*** (2009), 2546-2550
11. Sharifi A., "Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach". ***IEEE Trans Wireless Communication,*** Vol. 9, No. 8, (2010), 2488-2497
12. 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), DOI: 10.1155/2013/270612
13. Feng Zhao, Shaoping Li, and Jingyu Feng., "Securing Cooperative Spectrum Sensing against DC-SSDF Attack Using Trust Fluctuation Clustering Analysis in Cognitive Radio Networks." ***Wireless Communications and Mobile Computing,*** (2019), Wiley, 1-11, https://doi.org/10.1155/2019/3174304.

Persian Abstract

چکیده

یکی از فن آوری های نوظهور در سال های اخیر در زمینه ارتباطات بی سیم ، فناوری شناختی رادیو (CR) است که به طور قابل توجهی از کمبود طیف می کاهد. عملکرد اصلی فناوری CR شناسایی حفره های طیف یا طیف استفاده نشده از کاربران اصلی (PU) است که به آنها به عنوان کاربران دارای مجوز نیز گفته می شود و اختصاص این طیف بلااستفاده به کاربران ثانویه (SU) که به آنها کاربران غیر مجاز نیز گفته می شود. از آنجا که فناوری CR برای هر کاربر باز است ، بسیاری از مسائل امنیتی مانند حمله اولیه امولسیون کاربر (PUEA) ، حمله Jamming ، حمله جعل داده های سنجش داده طیف(SSDF) ، حمله شیر و حمله سوراخ سوراخ و غیره وجود دارد. حمله SSDF یکی از مهمترین حملات امنیتی در رادیو شناختی است که در آن یک کاربر مخرب داده های نادرست را عمداً برای سایر کاربران ثانویه ارسال می کند. هدف اصلی حمله SSDF ایجاد اختلال در ارتباط بین کاربران ثانویه یا به دست آوردن منابع کانال بیشتر است. یکی از راه حل های کاهش حمله SSDF ، سنجش طیف همکاری است. در این مقاله ، ما یک الگوریتم جدید سنجش تعاونی را براساس ارزش اعتماد کاربران ثانویه پیشنهاد می دهیم و با سنجش طیف تعاونی معمولی با الگوریتم پیشنهادی مقایسه می کنیم. در این الگوریتم ، ابتدا CR که منتظر تخصیص کانال است ، اطلاعات را درک کرده و اطلاعات سنجش CR های دیگر را مقایسه می کند. اگر هر گزارش سنجش CR با تست سنجش CR در خوشه مطابقت نداشته باشد ، در غیر این صورت پاداش می دهد. این رویه ها برای تعداد دوره هایی تکرار خواهد شد. سرانجام آزمون CR مقدار اعتماد را محاسبه می کند. بر اساس مرکز همجوشی ارزش اعتماد تصمیم خواهد گرفت که ارزش قابل اعتماد CR خاص را در آن گنجانده یا حذف کند. شبیه سازی سنجش تعاونی نیز در هر دو کانال نوع زمان و کانال بی تغییر زمان (ریلی) انجام می شود. نویسندگان همچنین سه روش اساسی همجوشی سخت مانند قانون AND، OR، MAJORITY را مقایسه می کنند.