I. J. Computer Network and Information Security, **2016, 12, 44-50**
Published Online December 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.12.06

A Novel Technique to Prevent PUE Attack in Cognitive Radio Network

Poonam [1a], Ekta gupta [2a], C.K. Nagpal [a]
[a] YMCA University of Science and Technology, India
E-mail: poonamgarg1984@gmail.com [1], ektagupta43@gmail.com [2]

***Abstract*—**Need of wireless communication is increasing to work from distance. That is why new applications are made everyday which increases demand of spectrum but due to limitation of spectrum and inefficient utilization of spectrum. A new paradigm is constituted which is called Cognitive Radio Network (CRN). It get more attention in recent times due to most promising solution for the efficient utilization of spectrum. Spectrum sensing in CRN makes it prone to many attacks on each layer. One of these attacks is PUE attack where a malicious user pretends to be a primary user and not let others to use primary user's channel in its absence. It may cause Denial of Service attack in the network. There are many techniques available in the literature for detection and prevention of PUE attack but still there are some limitations in these approaches. Current research provides detection results based on the energy level of all users in the network. In this paper we provide a novel approach to prevent PUE attacker based on signal activity patterns. Simulation is done in MATLAB-2013 and results show that proposed method gives excellent performance.

***Index Terms*—**Cognitive radio network, security, primary user emulation attack, trust-based mitigation, reputation-based mitigation, primary user emulation attack prevention.

I. Introduction

Wireless communication is done by radio spectrum. For this the spectrum is divided into number of channels and these channels are distributed among many groups of users which may be either any government organization, any business firm or may be a group of users. These users have to pay to the service providers so that they can become the licensed users for that channel. Then this channel will be dedicated only to that group of user who owns it. Now everybody in that group is using that channel as per their need. But the problem here is that these users are not using these channels all the time even if they are doing their work and paying for the spectrum [16] [20]. Another problem is the ever increasing demand for the wireless applications for which there is need of extra spectrum. As the radio spectrum is a natural resource no one can increase it for extra usage and almost all the spectrum is already allocated to licensed users leaving some part of the spectrum for unlicensed users. So to counterbalance all these problems a solution was proposed which is called Cognitive Radio Network (CRN) [31] [32]. In this network when the licensed users are not using their channels other unlicensed users come and use their channels till the licensed users do not come again on their channels. These licensed users are called primary users and unlicensed users are called secondary users. To use the primary user's channel secondary users need to sense their channels continuously to find holes in the network [18] [23]. This process of using the primary user's channels is divided into many layers in the network. On each layer there is presence of secondary users which are continuously sensing the channels. So to increase their time of presence in the network or to stop primary users to use their channels some secondary users may behave maliciously. One of these malicious activities is to capture the identity of any primary user to use its channel and to stop other secondary users to use it. It leads to a very harmful attack in the network called Primary User Emulation Attack as shown in Fig 1. This is done on the physical layer in the network. In this paper we will give a brief about many detection and prevention techniques for this attack those are proposed till now. We propose a method to prevent this attack that is based on Signal Activity Pattern and give the simulation results using MATLAB 2013(b) which shows our proposed method gives better performance than previous.

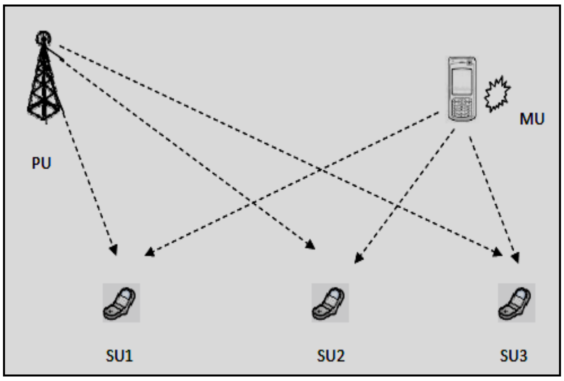


Fig.1. PUE Attack

II. Related Work

There is much vulnerability in the network at each layer. But attacks during the sensing of spectrum most affect the network. There are many techniques for detection and prevention of PUE Attack in the literature [30].

A technique is proposed to detect malicious user by taking the difference of secondary user from primary transmitter and by calculating ratio. This is done by using GPS [10]. Another approach based on threshold value which is calculated by taking the ratio of maximum and minimum Eigen value [2]. Energy detection is also used by Fenton's approximation method to calculate mean and variance of distribution [3]. An attacker is found on the basis of signal characteristics and position of primary user is located by GPS [4]. Another technique is based on the probability of missing the primary user and probability of successful PUEA [5]. Now a new technique is proposed based on the trust value of secondary user [6]. In the next approach signal strength is calculated to find the attacker [30]. Another technique is based on increasing the detection probability of PU which decreases attacker's probability [8]. Attacker can also be found by calculating the belief value and compared with the threshold value [9]. Another method to detect attacker is to focus on the authentication of primary user [15]. Now a new method is proposed by making interference signals and then compared with the position of primary user to locate the attacker [11]. After this a new method is proposed where a reference signal is generated then it is encrypted with AES and it is regenerated at the receiver's end [12]. After this a new proposal came which combines both energy detection and location verification to provide better results [13]. After this in a method sensing results are combined with routing information [14]. In the current research energy level of users are checked by cyclostationary feature [1]. A comparative study of all mentioned techniques is in table 1.

Table 1. Brief Summary of PUE Attack Solutions

Technique	Year	Advantage	Limitation
Physical layer approach	2005	Easy to implement antennas	Require prior knowledge about signal characteristics
Network layer approach	2005	Network bandwidth is not wasted due to ignorance of some SUs in path	Require prior knowledge about location of attacker
DRT&DDT	2006	GPS system is used	Deprivation in result
MME	2007	Doesn't require prior knowledge	Calculating Eigen values is quite complex
Mac layer approach	2008	QoS of network improved	Do not have focus on preventing malicious activity
Fenton's approximation method	2008	Easy to implement	Mean & variance is calculated for all users at SU
Loc based verification	2008	Works effectively in hostile environment	Might not useful when transmitter power is low
NPCHT& WSPRT	2009	Flexible in maintaining successful PUEA high	More time complexity
Collaborative spectrum sensing	2009	Works effectively for one malicious user	Doesn’t check for multiple malicious users
Robust spectrum decision protocol	2010	Probability of successful PUEA detection is quite good	Individual detection is applied for all users
Cooperative Spectrum Sensing	2011	Maximize detection probability of primary user	Focus is on detection of primary user
Cross layer approach	2011	Works effectively after combining the results from both layers	Conveying the information between layers may be sensitive
Belief Propagation	2012	Probability of accuracy is more	Node may pass wrong belief value
Primary User Authentication	2012	Authentication of every primary user reduces presence of malicious user	Require knowledge of cryptography
PNC	2013	Use additive nature of electromagnetic waves	Quite complex to find the location
AES	2013	Work effectively even under very low SNR values	May not be that much effective after a range
SPARS	2014	Doesn't need any prior knowledge about primary users	Works when Pus having same SAP
Database Assisted Approach	2015	A fruitful technique to increase probability of false alarm	Somewhat complex
Intense explore algorithm	2015	Robust technique	Results are based on energy detection technique

III. Problem Definition

Current research in prevention of Primary User Emulation Attack is based on either energy detection or location based technique. Here two sets of secondary users are made, users from one group sense the behavior of their neighboring users in other group by using energy detection technique. If the energy level of any user is found to be greater than the threshold value of signal energy then it is considered to be suspected user. Further if another user in first group sense the same behavior about that user then fusion center believe it to be a malicious user and alerts all other secondary users about it.

Energy detection technique provides good results but due to environment conditions energy level of signal may change under the noise uncertainty. In that condition it may not work accurately.

In location based techniques position of users are found by using GPS, which is not convenient because GPS may not work everywhere and all the time.

IV. Proposed Work

Security in CRN is an important topic of research and attacks in CRN is an important component. Here a solution is proposed to provide better results based on Signal Activity Pattern (SAP) of a transmitter that works on the ON and/or OFF periods of the transmitter. An ON period refers to the duration of a busy period that the transmitter is transmitting and SUs must be denied from communications. An OFF period refers to the time limit of an idle period between two adjacent ON periods.

A. Working environment

Figure 2 shows environment of working where sensing result table contains SAPs of secondary users obtained by their neighboring secondary users. Table fusion center contains SAPs of all secondary users and primary users. Fusion center derives the result by comparing these SAPs.

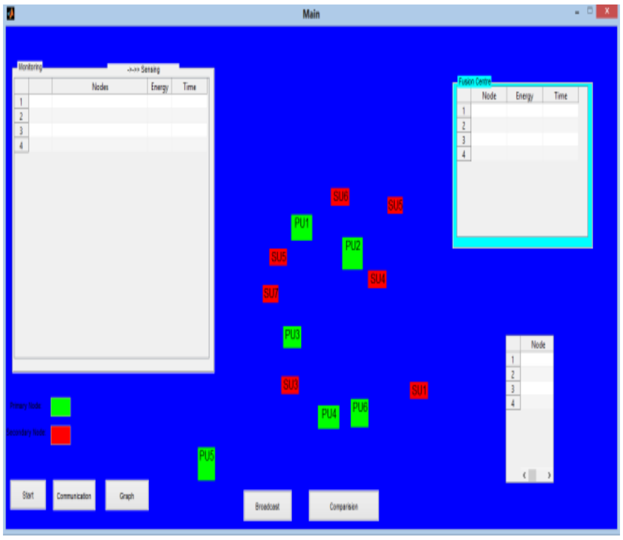


Fig.2. Working Environment

B. Procedure

To set up the environment two types of nodes are taken one is fixed and the other is movable. Nodes which are kept fixed called primary user nodes and the nodes which are movable called secondary user nodes. Secondary user nodes keep moving in the network to locate the holes in the network and whenever finds a vacate channel of primary user use it.

SAP contains information of activation and deactivation time of that node in the network along with the energy levels of the signals produced by the node at any particular time. So one secondary user node senses the behavior of its neighboring secondary user node and makes its SAP, store it in a table. Similarly all the secondary nodes make SAP of their neighboring nodes and store the SAPs in a table named 'Sensing Results'. This process continues for 5 seconds after starting.

Now these SAPs are given to the fusion center. As the same node may be in neighborhood of more than one node so, all these neighboring nodes sense the behavior of that particular node and make its SAP. Now when there is more than one entry in the sensing table for the same node then the SAP of that node is selected on the basis of maximum energy level. Similarly SAPs of all the secondary nodes are selected and given to the Fusion Center.

It is considered that all the primary users are active at the same time in the network i.e. their ON/OFF period is same in the network and their energy level is also same due to equal priority of licensed users in the network. So SAP of all primary users will be same and it is saved in the Fusion Center already.

Now all the SAPs are with Fusion Center. It compares the SAPs of all secondary user nodes with the SAP of primary user nodes. Then the secondary user node which is active in the off period of primary user node and its energy level is also equal to or greater than the primary user node is considered as attacker node.

After detection of attacker node it is blocked by the Fusion Center and then it broadcasts a message in the network telling all the nodes about the attacker node.

Now detection latency is obtained by calculating the number of malicious users that are detected by our proposed method within the given time.

Throughput of the network is also calculated on the basis of results obtained by the simulation.

Then these results are compared with the previous technique and it seems to give better results.

Step by step working is shown as under:-

E (p) – Signal energy level of primary user
E(s) - Signal energy level of secondary user
T (p) - Time of activation of Primary user in network
T (s) - Time of activation of Secondary user in network

Step 1: Set up CRN environment.

Step 2: Initially Signal Activity Pattern (SAP) of all SUs is same and these patterns are stored at Fusion Centre (FC).

Step 3: Get SAPs of each SU from their neighboring SUs.
Step 4: Give all SAPs to FC after each interval of time.
Step 5: If ((E (p)>= E(s))&& (T (s)!=T(p)) then

i. SU is malicious.
ii. FC will block it.
iii. FC broadcast this message about attacker in the network.

Step 6: Else SU is not malicious.

V. Implementation Results

A simple network terminology is used for simulation. Simulations are conducted with six primary users and 7 secondary users that are located randomly surrounding the primary users. PUs are fixed whether SUs are moving with random speeds in random directions. Here we consider the minimum distance between primary and secondary user 200 meter and maximum distance is considered 400 meter. Parameters used for implementation are given in table 2.

Table 2. Parameters used in Implementation

Parameter	Parameter value
Total number of nodes, N	13
Number of PU nodes	6
Number of SU nodes	7
Number of channels	1
Maximum velocity with which SU nodes can move	10kmph
Total area	1000m*1000m
Area within which nodes are considered adjacent to each other	200m

The implementation results of the proposed method are as follows:

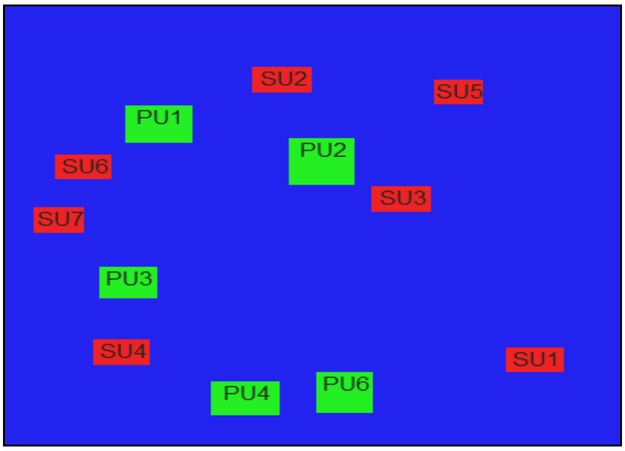


Fig.3. Nodes Positions before Start

Fig. 3 shows the positions of Pus and SUs in the environment at a time before starting the implementation.

Fig. 4 shows the positions of Pus and SUs in the environment after starting the implementation.

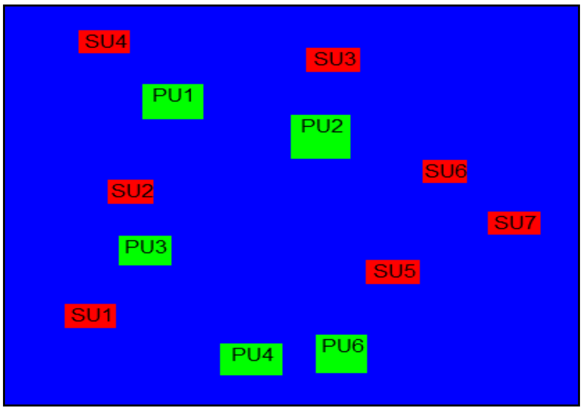
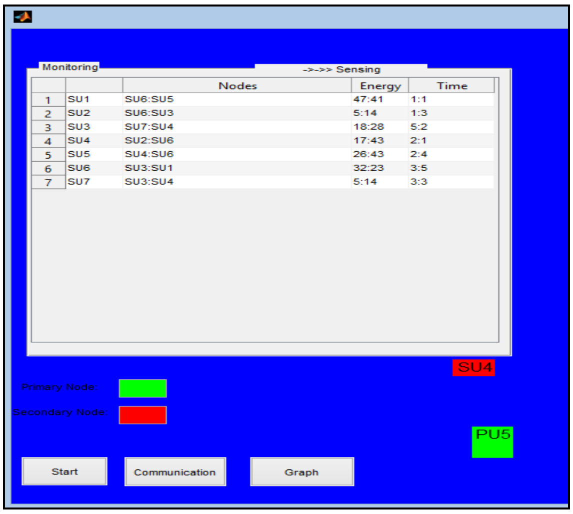


Fig.4. Nodes Positions after Start

Step 1: Secondary nodes start moving and sense their neighboring secondary nodes for 4 seconds and make their SPA.



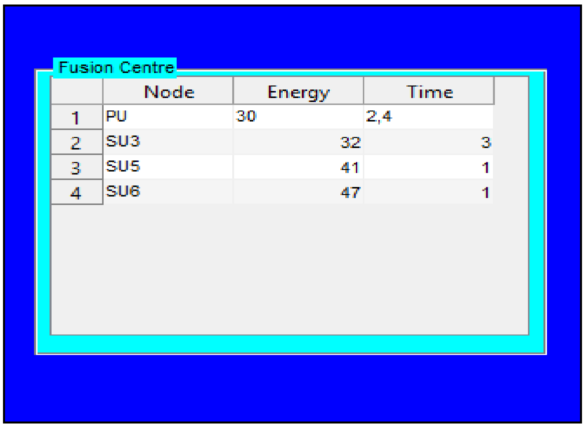
		Nodes	Energy	Time
1	SU1	SU6:SU5	47:41	1:1
2	SU2	SU6:SU3	5:14	1:3
3	SU3	SU7:SU4	18:28	5:2
4	SU4	SU2:SU6	17:43	2:1
5	SU5	SU4:SU6	26:43	2:4
6	SU6	SU3:SU1	32:23	3:5
7	SU7	SU3:SU4	5:14	3:3

Fig.5. Sensing Results

Fig 4 shows corresponding sensing results in sensing table 5 after sensing for 4 seconds.

Step 2: SUs give sensing results to FC and nodes having energy > PUs' energy is shown in FC database.

Fig 6 shows the corresponding results in FC's database



	Node	Energy	Time
1	PU	30	2,4
2	SU3	32	3
3	SU5	41	1
4	SU6	47	1

Fig.6. FC Database

Step 3: Plot SPAs of all SUs and PUs

Fig 7 shows the corresponding results in graphs

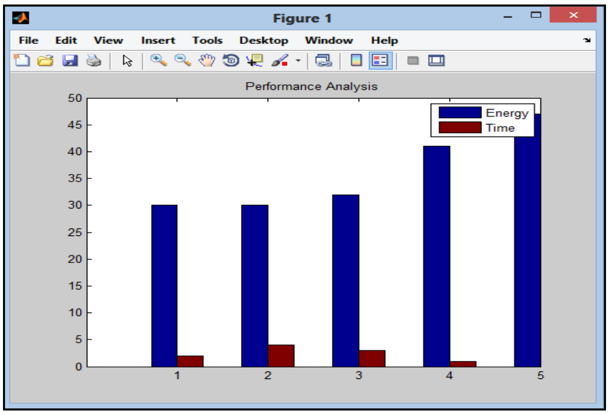
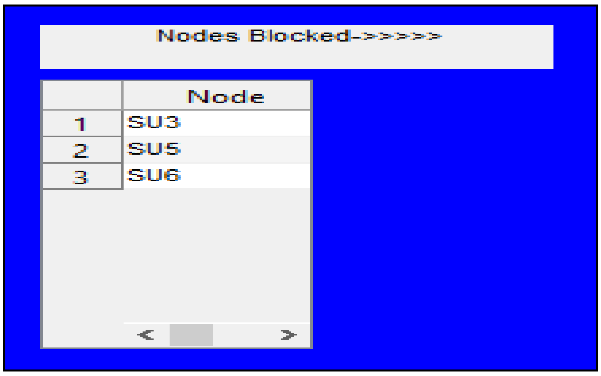


Fig.7. SPAs of SUs and PUs

Step 4: FC finds attacker nodes, block them and broadcasts message in the network.

Fig 8 shows the corresponding results in nodes blocked table



Nodes Blocked->>>>>

	Node
1	SU3
2	SU5
3	SU6

Fig.8. Blocking Nodes and Broadcasting Message by FC

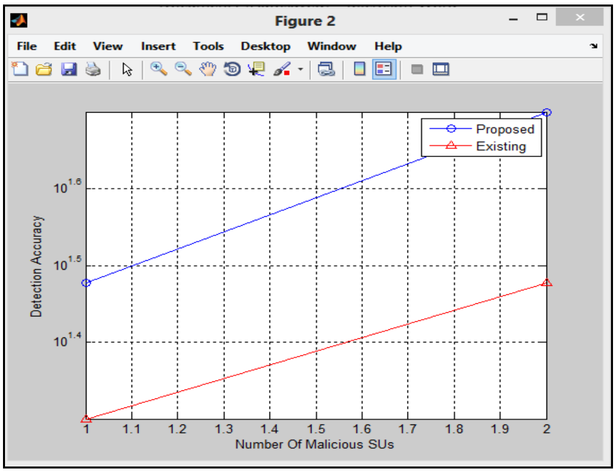


Fig.9. Comparison of Detection Accuracy

Fig 9 shows no. of malicious users versus detection accuracy in our proposed method and its comparison with the existing technique. In our approach detection accuracy increases as the number of malicious users increases because every secondary user that is active in the network continuously sense the activity of its neighboring secondary users and give its SPA to FC at an interval of time.

Fig 10 shows no. of malicious users versus throughput of network in our proposed method and its comparison with the existing technique. In our approach throughput increases as the number of malicious users increases because probability of detection of attackers increases as the number of malicious users increases. Due to this the channels are utilized efficiently thereby increasing the throughput of network.

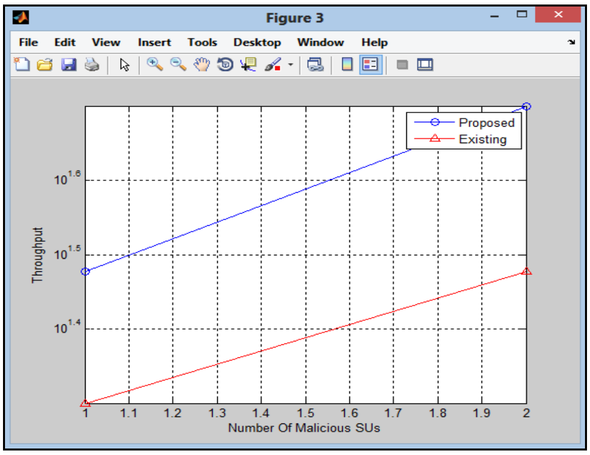


Fig.10. Comparison of Throughput

VI. Conclusion and Future Work

Cognitive radio was introduced to utilize the unused spectrum efficiently to improve the spectrum utilization and hence to reduce spectrum scarcity. Spectrum sensing is one of the important aspects of cognitive radio network. In this paper, we address the problem of preventing PUE attacks in mobile CRNs. Its various detection and prevention methods are also presented. Mitigation of PUE attack is considered in this paper through our novel approach, Signal Activity Patterns. The simulation results prove the method is robust.

Table 3. Comparison between Existing and Proposed Technique

Parameters Techniques	Detection accuracy	Throughput
Existing	Up to 65%	Up to 60%
Proposed Model	Up to 70	Up to 65%

In our future work, we will improve the accuracy of detecting malicious user by taking variable activation time with energy and acquiring SUs trust value. . In our future work, we will improve the accuracy of detecting malicious user by taking variable activation time with energy and acquiring SUs trust value. Since all secondary user nodes are not trustworthy so, to find attacker node among these secondary user nodes is difficult task.

REFERENCES

[1] C. Sumathi, & R. Vidhyapriya, “Intense explore algorithm-A Proactive Way to Eliminate PUE attacks in cognitive radio networks”. International Journal of Applied Engineering Research, 2015, 10 (2), 3827–3842.

[2] Y. Zeng, & Y.C. Liang,, “Maximum-Minimum Eigen-value Detection for Cognitive Radio”. IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications, 2007, 1-5.

[3] S. Anand, Z. Jin, & K. P. Subbalakshmi, “Analytical model for primary user emulation attacks in cognitive radio networks”. IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN’2008), 1-6.

[4] R. Chen, J.-M. Park & J. H. Reed, “Defense against Primary User Emulation Attacks in Cognitive Radio Networks”. IEEE Journal on Selected Area in Communications, 2008, 26(1), 25-37.

[5] Z. Jin, S. Anand, & K. P. Subbalakshmi, “Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing”. ACM Mobile Computing and Communications Review (MC2R): Special Issue on Cognitive Radio Networks, 2009, 13(2), 74-85.

[6] W. Wang, “Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks”, 130–134.

[7] S. Bhattacharjee, S. Sengupta, & M. Chatterjee, “Vulnerabilities in cognitive radio networks” A survey. Elsevier-Computer Communications, 2013, 36(13), 1387–1398.

[8] Chen, H. Cheng, & Y. Yao, “Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack”, IEEE Transactions on Wireless Communications, 2011,10(7), 2135–2141.

[9] Z. Yuan, D. Niyato, H. Li, J.B. Song & Z. Han,“ Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks”. Selected Areas in Communications, IEEE Journal, 2012, 30 (10), 1850-1860.

[10] R. Chen & J.-M. Park, “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks” Networking Technologies for Software Defined Radio Networks. SDR ’06.1st IEEE Workshop on, 2006, 110–119.

[11] X. Xie, & W. Wang, “ Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding”, Proceeding of Computer Science, 2013, 21, 430–435.

[12] Alahmadi, M. Abdelhakim, J. Ren, & T. Li, “Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard”. Global Communications Conference (GLOBECOM), IEEE, 2013, 3229–3234.

[13] R. Yu, Y. Zhang, Y. Liu, S. Gjessin, & M. Guizani, “Securing cognitive radio networks against primary user emulation attacks”. IEEE Networks, 2015, 29(4), 68–74.

[14] Sorrells, P. Potier, L. Qian & X. Li, “Anomalous spectrum usage attack detection in Cognitive Radio Wireless Networks”. IEEE International Conference on Technologies for Homeland Security (HST), 2011, 384-389.

[15] Meena Thanu, “Detection of Primary User Emulation Attacks in Cognitive Radio Networks”. International Conference on Collaboration Technologies and Systems (CTS), 2012, 605-608

[16] Clancy, C., Hecker, J., Stuntebeck, E., and O'Shea, T., “Applications of machine learning to cognitive radio networks”, Wireless Communications, IEEE, 14(4):47-52, (2007).

[17] S. Haykin, “Cognitive Radio : Brain-Empowered wireless communications”, IEEE Journal on Selected Areas in Communications , 2005, 23(2), 201–220.

[18] Das, “Primary User Emulation Attack in Cognitive Radio Networks ” A Survey. International Journal of Computer Networks and Wireless Communications, 2013, 3(3), 312–318.

[19] Y. C. Liang, K. C. Chen, G. Y. Li, &, P. Mahonen, “Cognitive radio networking and communications: An overview. IEEE Transactions on Vehicular Technology”, 2011, 60(7), 3386–3407.

[20] Z. Jin, S. Anand& K. P. Subbalakshmi, “Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks”. IEEE Transaction Communications, 2012, 60(9), 2635–2643.

[21] Abhilasha Singh, Anita Sharma,” A Survey of various Defense Techniques to detect Primary User Emulation Attacks”, International Journal of Current Engineering and Technology, Vol.4, No. 2, April 2014.

[22] Deepa Das, Susmita Das, “Primary User Emulation Attack in Cognitive Radio Networks: A Survey”, IRACST, Vol.3, No3, June 2013.

[23] Carl R. Stevenson, Gerald Chouinard, “IEEE 802.22: The First Cognitive Radio Wireless Regional Area Network Standard”, IEEE Communications Magazine, January 2009.

[24] Zeng, Y., Liang, Y.-C., Hoang, A. T., and Zhang, R., “A review on spectrum sensing for cognitive radio: challenges and solutions”, EURASIP J. Adv. Signal Process, 2010.

[25] V. Kukreja, S. Gupta, B. Bhushan, & P. Mittal, “Enhancement of Spectrum Efficacy using Cognitive Radio Networks”. International Journal of Future Generation Communication and Networking, 2015 8(2), 265–272.

[26] C. Kiruthika, A.C. Sumathi, “A Study on Primary User Emulation Attack in Cognitive Radio Networks”, International Journal of Computer Science Engineering and Technology (IJCSET), 2014, 4(10), 260–262.

[27] Adelantado, & C. Verikoukis, “Detection of malicioususers in cognitive radio ad hoc networks”, A non-parametric statistical approach. Ad Hoc Networks, 2013, 11 (8), 2367–2380.

[28] Jin, Z. Anand, S., "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks, "Communications, IEEE Transactions, vol.60, no.9, pp.2635, 2643, September 2012.

[29] Z. Jin, S. Anand, & K.P. Subbalakshmi, “Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks”. Global Telecommunications Conference (GLOBECOM) IEEE, 2010, 1-5.

[30] E. Gupta, Poonam & C. K. Nagpal, “Survey on PUE Attack Detection and Prevention Techniques”, International Journal of Emerging Technologies in Engineering Research (IJETER-2016), *4*(4), 90–95.

[31] Vivek Kukreja, Shailender Gupta, Bharat Bhushan and Chander Kumar, “Towards Performance Evaluation of Cognitive Radio Networks in Realistic Environment”, published in IJCNIS-2014, pp. 61-77, DOI: 10.5815.

[32] Poonam Mittal, Mehak Jain and C. K. Nagpal, “A Throughput and spectrum aware fuzzy logic based routing protocol for CRN”, published in IJCNIS-2016, pp. 58-64, DOI: 10.5815.

Authors' Profiles

Poonam received her B.Tech. and M.Tech. from YMCA University of Science and Technology, Faridabad, India. She is currently working as an Assistant Professor in Computer Engineering Department in the same university. She is currently pursuing Ph.D. Her interests include networking and algorithm design.

Ekta Gupta, received her B.Tech. from MVN University and pursuing M.Tech. from YMCA University of Science and Technology, Faridabad, India. Her area of interest is Security in MANET.

C.K. Nagpal, Professor, head of department and Ph.D. supervisor in Computer Engineering Department in YMCA University of Science and Technology, Faridabad, India. His interests include networking and fuzzy expert system. He has published more than 35 papers in various national and international publications.

How to cite this paper: Poonam, Ekta gupta, C.K. Nagpal,"A Novel Technique to Prevent PUE Attack in Cognitive Radio Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.12, pp.44-50, 2016.DOI: 10.5815/ijcnis.2016.12.06