Survey on PUE Attack Detection and Prevention Techniques

Ekta Gupta
Department of Computer Engineering, YMCA University of Science and Technology, Faridabad, India.

Poonam
Department of Computer Engineering, YMCA University of Science and Technology, Faridabad, India.

Chander Kumar Nagpal
Department of Computer Engineering, YMCA University of Science and Technology, Faridabad, India.

Abstract-As the demand of wireless applications is increasing day by day therefore demand of the spectrum is also increasing. As nearly whole spectrum is allocated already the most promising solution for this is Cognitive Radio Network (CRN). In CRN unlicensed users sense the spectrum for availability to use without interfering the communication of primary users. As sensing the spectrum is very sensitive task it is feasible to many vulnerabilities. One of these vulnerabilities is Primary User Emulation Attack (PUEA). In this attack a malicious user pretends like a primary user. There are many techniques that are proposed to detect the PUE attack and prevent it but still there are many open issues regarding the security of network during sensing of spectrum. In this paper we discuss all these techniques and analyze the open issues which are still there in the cognitive radio network.

Index terms-CRN, Attack, PUEA detection, PUEA prevention.

1. INTRODUCTION

Demand of wireless communication is increasing tremendously that there is exponential growth in wireless services. Due to this exponential increase there is demand of spectrum for these services. As the spectrum is a natural resource it cannot be increased with the demand and nearly whole spectrum is allocated to the licensed users [1,2] which are also called primary users which have license to use the spectrum and some part of the spectrum is left unallocated for unlicensed users. Here the problem arise is inefficient utilization of spectrum because no primary user is using the spectrum every time and the part which is left unallocated is overcrowded every time.

So to use the spectrum efficiently a solution is proposed which is called Cognitive Radio Network. In this network unlicensed users which are also called cognitive users or secondary users can use the spectrum of primary users opportunistically [3,4] when they are not using it and they have to leave the spectrum when primary users come back in order to avoid any interference to the primary user. Sharing of spectrum starts from the sensing of spectrum so; cognitive users continuously sense the network and share the sensing information to other secondary users. During this spectrum sensing network configuration is exposed so this is the weakest point in the whole process and due to this the network is vulnerable to many attacks.

One of these attacks is PUE attack, in which a malicious user behaves like a licensed user and uses the resources of the network. The most difficult task in this attack is to distinguish the signal of primary user and malicious user because a malicious user sends a signal in the primary user's spectrum which has the same characteristics as of primary user's signal to pretend that it is a licensed user. When a secondary user come to sense this spectrum and finds a signal then it believes that primary user is here [9,10] to use the spectrum and stop sensing the spectrum. A malicious user then uses the resources of network or it may harm the network by not letting the secondary user to use the spectrum. So there is a need to find techniques which can detect the presence of malicious users in the network so that it can be saved by these harmful users.

By seeing this major problem to the Cognitive Radio Network researchers finds various techniques to detect the presence of malicious user [26] on the basis of signal strength, position of primary user and some other parameters which we will discuss in this paper and finally we will discuss all the pros and cons of these techniques and some open issues which are still there to work on to increase the security and efficiency of the network.

1.1. Layered Approach in CRN

As the network is divided into layers [5,6,7,8,27] of a protocol stack attacks are also described on the basis of vulnerability in each layer. There are 4 layers starting from physical layer which is at the bottom in the layered architecture of CRN, next layer is Link Layer, next to this is Network layer and the uppermost layer is Transport layer.

1.1.1 Attacks on Physical Layer

As the transmission, spectrum sensing and channel estimation is done at the physical layer malicious users come into state from this point.

PUE Attack

When a primary user left the channel, malicious user (MU) finds the opportunity to get into existence and starts sending the signals of wavelength exactly similar to the primary user thereby misleading the secondary user that the primary user (PU) is still present in the channel and make the secondary user (SU) not using the channel or it can use the resources of network for its own use as shown in figure 1.

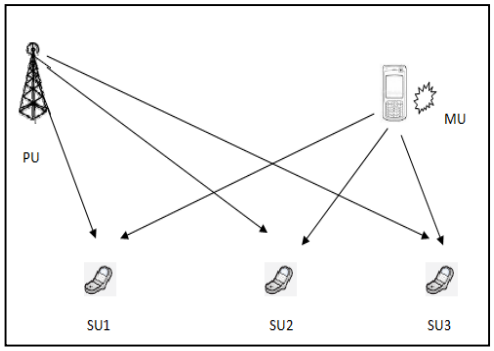

Figure 1: PUE attack

Objective Function Attack

A cognitive user has the ability to sense the environment and adapt to the changes of environment easily by calculating some parameters from the network to increase the data rate and to minimize the power. While calculating these parameters an attacker may manipulate these parameters to falsify the result of cognitive engine.

Jamming Attack

In this type of attack a jammer continuously send the packets in the network so that the intended user never send the signal in the network or receive the signal from the network, thereby making the Denial-of-service situation and wasting the network resources.

1.1.2 Attacks on Link Layer

After sensing the spectrum decision is taken by the secondary users. This is done at the link layer, here number of secondary users can join the existing users to share the result of sensing, while sharing this result to its neighborhood attacker goes in active state and perform these attacks:

Byzantine Attack OR Spectrum Sensing Data Falsification (SSDF) Attack

In a decentralized Cognitive Radio Network, when secondary nodes share their sensing data to their neighboring nodes attacker comes and propagate false sensing data to neighborhood as shown in figure 2. So it is difficult to detect in decentralized system while in a centralized system a fusion center is there to collect the sensing data from all secondary nodes and make decisions after analyzing their data , it is less immune to byzantine attack.

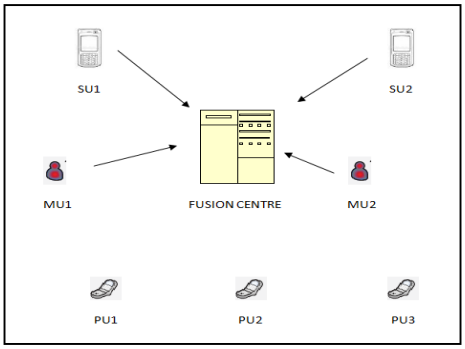

Figure 2: SSDF Attack

Control Channel Saturation DoS (CCSD) Attack

In multi-hop CRN after deciding which channel can be utilized a MAC frame are exchanged between CRs to reserve the channel. This phase is called negotiation phase. During the exchanging of this frame attack is possible and when many CRs are there to communicate attacker makes use of this situation and send a duplicate MAC frame to penetrate the control channel and thus decreasing the performance of network.

Selfish Channel Negotiation (SCN)

In multi-hop CRN any CR host may refuse to forward another CR's data just to save its energy and to increase its own throughput thereby reducing the overall throughput of the network.

1.1.3 Attacks on Network Layer

After sensing the spectrum and taking a decision on the basis of sensing results there comes the process of transferring the data in the network. This is done at the Network and transport layers that are the top layers in the CRN architecture. There are hinders in transferring the data in the network, these can be categorized as:

Sinkhole Attack

In multi-hop CRN when finding the best route to the specific destination a malicious user can falsely announce that it is the best route to this destination. This type of attack is particularly effective in infrastructure based network because all data goes through the base station and attacker can register itself as the best route. And including itself in the route of transferring the data it can alter or drop the data in id way thereby piercing the network security and throughput.

Hello Flood Attack

In this attack an attacker makes a signal and broadcasts it to all the nodes in the network. This signal have much power and uses a high quality link channel for broadcasting that all the nodes think that this is their neighbor node.

1.1.4 Attacks on Transport Layer

As of now routing has been done in the network to forward the packets between the nodes now the task is to actually transmit the packet in the way to destination. As this is done at the transport layer we now will consider all the attacks that may possible at this point. These attacks are:

LION Attack

In this attack an attacker interrupt the transmission of data through TCP protocol using PUE attack. When PUE attack is accomplished in the network all secondary users have to leave the channel for primary users using frequency handoffs. At that time TCP doesn't know about these things and continuously send packets when it doesn't get acknowledgements it starts retransmitting the packets now if an attacker intercepts these packets it knows about the frequency band which is tested and declare that it is using this band.

As of now we have discussed about layered architecture of CRN, corresponding attacks on each layer and their cause to occur. Now in the next section we will focus on one of these attacks appeared on the physical layer i.e. on PUE Attacks. It grabs most attention [22,28] because it occurs at the time of sensing the spectrum and there is a lot more work to be done to prevent this.

2. PUEA DETECTION TECHNIQUES

PUEA gets easy when energy detection technique is used for detecting the primary user because in this scheme only the energy of signal is checked with the threshold value other characteristics of signal are left unnoticed which can cause malicious user to crack the security of network easily.

There are many proposed techniques to detect the attack. These are:

2.1 Distance Ratio Test & Distance Difference Test

In [23] it is proposed that the basis of this technique is the length of wireless link and the strength of received signal. They detect a malicious user in the environment by calculating ratio and difference to the secondary user from primary transmitter and malicious user. Here to know the positions of users is found by using GPS.

2.2 Maximum Minimum Eigen Values (Mme)

In [11] it is proposed that the maximum and minimum Eigen values of the signal are calculated based on the covariance matrix of received signal. Ratio of maximum to minimum Eigen value is used to find the presence of signal. The value of ratio is quantized to find some threshold value in order to find false alarm probability.

2.3 Fenton's Approximation Technique

In [12] it was the first time when energy detection technique is used to detect malicious user. Here the received signal power at secondary user from malicious user transmission is represented as a log-normal distributed random variable and then mean & variance of this distribution is calculated by using Fenton's approximation method. Then this is used to detect PUEA using Markov inequality.

2.4 Transmitter Verification Scheme (Loc Based Defence)

In [29] here two things are taken into consideration location of primary transmitter and the characteristics of signal. Here detection of malicious user is done in three phases firstly there is verification of signal characteristics then the measurement is done for the received signal energy level and lastly source of the signal is localized. Here RSS measurement is done in a new model.

2.5 NPCHT WSPRT

In [13] Neyman Pearson Composite hypothesis test & Wald's sequential probability ratio test. Here the focus is on two things: first is probability of missing the primary and the second is probability of successful PUEA. The idea here is to keep first around the threshold value and minimizing the second. Balancing between two at the same time using NPCHT was quite difficult so the improved version of this was WSPRT which add more time complexity due to increased number of observations to get the accurate result. As theoretical value of missing the primary decreases successful PUEA probability increases this is achieved in WSPRT by enhancing the number of observations.

2.6 Collaborative Spectrum Sensing

In [14] it is proposed to secure the network. It detects the malicious users in the network and eliminates them. Here a defense scheme is proposed which uses trust value os secondary users then use another algorithm to take decision based on the trustworthiness of secondary users.

2.7 Robust Spectrum Decision Protocol

In [15] it is proposed that a centralized controller is used to take the final decision. All the secondary users give their sensing results to that centre and it makes a final decision based on the individual decision of all secondary users. Here spectrum decision is obtained on the basis of received power signal at the SU.

2.8 Cooperative Spectrum Sensing

In [16] it is proposed that all secondary users give their sensing results to the fusion center. Combined weights are optimized in order to maximize detection performance with the restriction of required false alarm probability. Here detection probability of primary user is maximized which in turn reduces the probability of attacker involvement in the network.

2.9 Belief Propagation

In [17] proposed belief propagation of each user. Each user share calculates some belief value about its neighboring nodes and shares it in the network. Then the mean value is calculated from these values for each node, if value is less than the threshold value then it is assumed to be an attacker.

2.10 Primary User Authentication

In [18] proposed this to authenticate the primary users. It can be achieved in two ways: link signatures or channel impulse response and location estimation techniques. Here characteristics of the received signals are used i.e. received signal strength, angle of arrival, time of arrival and pattern matching with fingerprint.

2.11 Physical Layer Network Coding (PNC)

In [19] proposed this to determine the positions of wireless nodes. In this technique a reference sender is made to send the signal in the network and these signals are interfered with the all other nodes' signal secondary users get these interfered signals making hyperbolas and compare the starting point of these sequences with the known positions of primary users to detect the PUE attack. This is location based technique.

2.12 Advanced Encryption Standard

In [20] proposed that a TV transmitter is used to generate a reference signal then this signal is encrypted with AES and send to the receiver and used as a sync byte of data frame of each DTV. Here data can be easily shared between sender and receivers secretly and reference signal can be regenerated at the receiver leading to detect authorized primary users.

2.13 SPARS

In [21] proposed a new system model is presented called signal activity pattern acquisition and recognition pattern. It obtains signal activity pattern on the basis of spectrum sensing and then this system reconstructs this pattern and then compare these two patterns in order to find attacker.

2.14 Database Assisted Approach

In [30] proposed two schemes i.e. energy detection and location verification are combined to produce better result for detection of PUE attacker. Received signal is sampled and energy vector is calculated for the same. Then from this vector location verification is done and then this information about signal source is given to fusion centre. It is easy to verify the attacker when it is far located from the base station of primary user.

TECHNIQUE	YEAR	ADVANTAGE	DISADVANTAGE
DRT&DDT	2006	GPS system is used to find the position	Deprivation in result than expected
MME	2007	Doesn't require prior knowledge about channel signal and noise power	Calculating Eigen values through matrix is quite complex
Fenton's approximation method	2008	Energy detection technique is 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

Belief Propagation	2012	Probability of accuracy is more as all nodes are participating in decision	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	Works when Pus having same SAP
Database Assisted Approach	2015	A fruitful technique to increase probability of false alarm	Somewhat complex

Table 1: Comparison table for detection techniques

3. PUEA PREVENTION TECHNIQUES

3.1 Physical Layer Approach

In this approach there should be antecedent knowledge about the characteristics of primary signal and its disparity with the interference signal then some techniques are applied to treat this interference. These are spread spectrum, signal design, directional antennas and source separation.

3.2 Network Layer Approach

This approach works after estimating the location of PUE attackers. Then the secondary users which come in the range of PUE attacker are made inaccessible for a limited period of time and routing is done excluding these SU nodes.

3.3 Transmitter Signal Location Verification

In [29] this scheme is also used for the detection of PUEA. In this scheme two type of tests are performed DDT & DRT. DDT calculates ratio of received signal strength at different location verifiers to the location of primary transmitters. In DRT phase difference of the received signal is calculated at different location verifiers.

3.4 Mac Layer Approach

In this approach focus is on the QoS parameter of the network. When any PUE attacker is left unnoticed in the network it continuously steals the bandwidth of the network. So to maintain the performance of the network some radio resource management techniques are applied i.e. spectrum hand off, admission control and spectrum scheduling.

3.5 Cross Layer Approach

In [24] information of the spectrum sensing from the physical layer is combined with the routing information from the network layer. A protocol is used here is SA-SMR, Spectrum Aware Split Multipath Routing Protocol to convey sensing information then the suspicious attacker is stopped by injecting controlled interference to it.

3.6 Intense Explore Algorithm

In [25] proposed a technique in which secondary users are divided into two groups. Users from a group sense their neighboring users in another group and apply energy detection technique to know their energy levels using cyclostationary feature. The results are given to the fusion centre, if results of two users are same then fusion centre decides that user is malicious and alerts all the users about its behavior thereby eliminating the malicious user.

TECHNIQUE	YEAR	ADVANTAGE	DISADVANTAGE
Physical layer approach	2005	Easy to implement e.g. directional	Require prior knowledge about signal
Network layer approach	2005	Network bandwidth is not wasted due	Require prior knowledge about location of attacker
DDT& DRT	2008	GPS system is used to find the position of	Deprivation in result than expected
Mac layer approach	2008	QoS of network improved	Do not have focus on preventing malicious activity
Cross layer approach	2011	Works effectively after	Conveying the information between layers may
Intense explore algorithm	2015	Robust technique	Results are based on energy detection technique

Table 2: Comparison table of prevention techniques

4. CONCLUSION

In this survey we discussed about the need of CRN. Its architecture and vulnerabilities in the network due to its design and framework. Then we explore various possible susceptibilities in the network and the most exposed part in the dynamic spectrum accessing. Then our focus is on the PUEA. We have investigated about proposed detection techniques for Primary User Emulation Attack and summarized our result in table 1. In the next section we scrutinize the prevention techniques for PUEA and summarized our result in table 2.The techniques which are proposed not completely effective in eliminating the malicious users from the network so the future work of our research is to implement a technique to prevent PUEA.

REFERENCES

[1] 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.
[2] 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.
[3] S. Bhattacharjee, S. Sengupta, & M. Chatterjee,"Vulnerabilities in cognitive radio networks" A survey. Elsevier-Computer Communications, 2013,36(13), 1387–1398.
[4] F. Adelantado, & C. Verikoukis,"Detection of malicious users in cognitive radio ad hoc networks" A non-parametric statistical approach. Ad Hoc Networks, 2013, 11(8), 2367–2380.
[5] D. Hlavacek, & J. M. Chang,"A layered approach to cognitive radio network security" A survey. Computer Networks, 2014, 75(A), 414–436.
[6] Bhagavathy S. Nanthini,, M. Hemalatha, D. Manivannan, & L. Devasena ,"Attacks in cognitive radio networks (CRN) " A survey. Indian Journal of Science and Technology, 2014, 7(4), 530–536.
[7] D. Das ," Primary User Emulation Attack in Cognitive Radio Networks " A Survey. International Journal of Computer Networks and Wireless Communications,2013, 3(3), 312–318.
[8] 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.
[9] S. Haykin,"Cognitive Radio : Brain-Empowered wireless communications", IEEE Journal on Selected Areas in Communications , 2005 ,23(2), 201–220.
[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] 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.
[12] 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.
[13] 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.
[14] W. Wang," Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks", Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on,130–134.
[15] 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
[16] C. 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.
[17] 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
[18] Meena Thanu, " Detection of Primary User Emulation Attacks in Cognitive Radio Networks". International Conference on Collaboration Technologies and Systems (CTS),2012, 605-608
[19] 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.
[20] A. 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.
[21] C. Xin, S. Member, M. Song, & S. Member," Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern", IEEE transactions on mobile computing , 2014,13(5), 1022–1034.
[22] H. Wen, S. Li, X. Zhu, L. Zhou, " A framework of the PHY layer approach to defense against security threats in cognitive radio networks". IEEE Network, 2013,27(3), 34-39.
[23] R. Chen , J.M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks". IEEE workshop on Networking Technologies for Software Defined Radio (SDR) Networks,2006, 110–119.
[24] C. 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.
[25] A. 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.
[26] C. T. Clancy, & N. Goergen, "Security in cognitive radio networks: Threats and mitigation". Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (Crown Com 2008), 1–8.
[27] C. R. Stevenson, "IEEE 802.22: The First Cognitive Radio Wireless Regional Area Network Standard", IEEE Communication Magazine, 2009,47(1), 130–138.
[28] 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.
[29] 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.
[30] 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.