International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

SURVEY ON ANTI- PUE ATTACK BASED ON JOINT POSITION VERIFICATION IN COGNITIVE RADIO NETWORKS

1Megha Chopra,2 Sonika Soni
1Mtech Student, 2Assistant professor, ECE Department, JCDM College of Engineering Sirsa , India
meghachopra.chopra@gmail.com, soni_sonika80@rediff.com and 8814097663

Abstract-Cognitive Radio (CR) is a promising technology that can alleviate the spectrum shortage problem by enabling unlicensed users(SU) equipped with CRs to coexist with incumbent users(PU) in licensed spectrum bands without inducing interference to incumbent communications. Spectrum sensing is one of the essential mechanisms of CRs that has attracted great attention from researchers recently. An attack that poses a great threat to spectrum sensing is called the primary user emulation (PUE) attack, an adversary's CR transmits signals whose characteristics emulate those of incumbent signals. The author provides various methods (dealt in different papers) for authenticating primary users signals. This paper will review about the various methods for mitigating PUEA attack which dwindle the spectrum access likelihood of proper functioning. Most of the proposed security schemes are aiming at the location verification for incumbent transmitter to resist pue attack.

.

Keywords- Cognitive Radio(CR), Primary User(PU),Secondary User(SU), Spectrum Sensing, Primary User Emulation(PUE) Attack, Location Verification ,Location Verifiers(LVs).

INTRODUCTION

In CR networks unlicensed users (a.k.a. secondary users) "opportunistically" operate in fallow licensed spectrum bands without causing interference to licensed users (a.k.a. primary or incumbent users), thereby increasing the efficiency of spectrum utilization. This method of sharing is often called Opportunistic Spectrum Sharing (OSS)[1]. CRs are able to carry out spectrum sensing for the purpose of identifying fallow licensed spectrum i.e., spectrum "white spaces". Once white spaces are identified, CRs opportunistically utilize these white spaces by operating in them without causing interference to primary users. The above scenarios highlight the importance of a CR's ability to distinguish between primary user signals and secondary user signals. Distinguishing the two signals is non-trivial, but it becomes especially difficult when the CRs are operating in hostile environments. In a hostile environment, an attacker may modify the air interface of a CR to mimic incumbent signal's characteristics, thereby causing legitimate secondary users to erroneously identify the attacker as a primary user. This is called as primary user emulation (PUE) attack

COGNITIVE RADIO NETWORK

Cognitive Radio Network Architecture:- The Cognitive radio network architecture shown above in figure1 comprises of two network groups namely: Primary network and Cognitive radio network.

- **Primary Network:** An existing network infrastructure is called Primary network. The user in this network (Primary users) has rights to operate certain spectrum of band called licensed band. The examples of this network are Television Broadcasting network and cellular communication networks.
- **Cognitive Radio Network:** Otherwise called a Secondary network which does not have any desired band to operate and thus it operates in the unlicensed band.

Cognitive radio users can either communicate with each other in a multihop manner or can access the base-station.
The three different access types over heterogeneous networks used in the cognitive radio network architecture are:

- **Cognitive Radio Network Access:** Cognitive radio users can access their own cognitive radio base-station both on licensed and unlicensed spectrum bands. Since all the communications occur within the cognitive radio network, their medium access scheme is independent of that of primary network.
- **Cognitive Radio AdHoc Access:** Cognitive radio users can communicate with each other through ad hoc connection on both licensed and unlicensed spectrum bands. Also cognitive radio users can have their own medium access scheme.
- **Primary Network Access:** The cognitive radio user can access the primary base-station through the licensed band, if the primary network permits. Unlike other access types, cognitive radio users should support the medium access technology of primary network. Also, primary base-station should support cognitive radio capabilities.

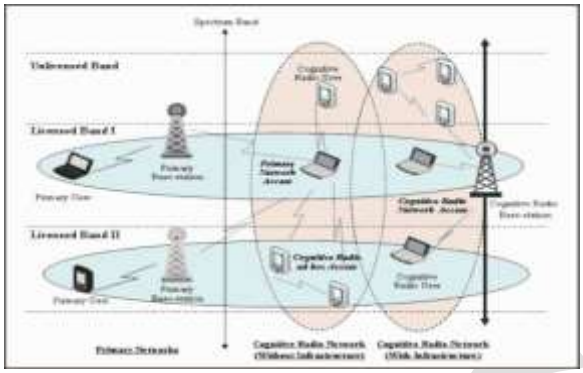

Figure 1:- **Cognitive Radio Architecture**

COGNITIVE RADIO FUNCTIONS

CR technique enables the users to have the "Best available channels". CR cycle functions are shown below in figure2 as:

- Spectrum sensing – Detects unused spectrum and share the spectrum without harmful interference with other users.
- Spectrum Management – Select best available channel.
- Spectrum Sharing – Coordinate access to this channel with other users.
- Spectrum Mobility – Vacate the channel when licensed user is detected.

Figure 2:- **Cognitive Cycle**.

PRIMARY USER EMULATION (PUE) ATTACK

Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack.

- Selfish PUE attacks: In this attack, an attacker's objective is to maximize its own usage of spectrum resources. When selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of incumbent signals.
- Malicious PUE attack: The objective of this attack is to obstruct the OSS process of legitimate secondary users i.e., prevent legitimate secondary users from detecting and using fallow licensed spectrum bands.

A TRANSMITTER VERIFICATION PROCEDURE FOR SPECTRUM SENSING

To thwart the PUE attack, a transmitter verification scheme based on location verification was proposed. They proposed two alternative techniques that are at the heart of the location verification scheme. The first technique is called the Distance Ratio Test (DRT), which uses received signal strength (RSS) measurements obtained from a pair of location verifiers to determine the location of transmitter The other technique is called Distance Difference Test (DDT), which utilizes the phase difference of the PU's signal observed at a pair of location verifiers to verify the transmitter's location. Assume that trusted location verifiers (LVs) exist for performing DRT or DDT. An LV can be a dedicated node, a secondary user with enhanced functions or a fixed/mobile base station. Assume that the area spanned by the CR network is populated with two types of LVs: one or more master LVs and slave LVs. A master LV has a database of the coordinates of every TV tower whose signal reaches the area spanned by the CR network. Each LV is assumed to know its location from a secure GPS system . In addition, assume that all of the LVs are synchronized and can communicate with each other through a common control channel. To increase the accuracy two mechanisms are used that are:

TDOA(Time difference of arrival) and FDOA(Frequency difference of arrival)[3].The FDOA needs the moving velocity and the direction of target. TDOA can be used to get the motion vector.

RELATED WORK

[1] In this paper, they describe an attack called primary user emulation (PUE) attack that poses a great threat to spectrum sensing, an adversary's CR transmits signals whose characteristics emulate those of incumbent signals. The highly flexible, software-based air interface of CRs makes such an attack possible. Their investigation shows that a PUE attack can interfere with the spectrum sensing process and significantly reduce the channel resources available to legitimate unlicensed users. As a way of countering this threat ,they propose a transmitter verification procedure. The transmitter verification procedure employs a location verification scheme to distinguish incumbent signals from unlicensed signals masquerading as incumbent signals. Two alternative techniques are proposed to realize location verification: Distance Ratio Test and Distance Difference Test. Simulation results show that several factors, such as the location of the attacker's transmitter relative to the LVs, can impact the performance of the two schemes.

[2] In this paper, they study the denial-of-service (DoS) attack on secondary users in a cognitive radio network by primary user emulation (PUE). Simulation studies and results from test beds have been presented but no analytical model relating the various parameters that could cause a PUE attack has been proposed and studied. They propose an analytical approach based on Fenton's approximation and Markov inequality and obtain a lower bound on the probability of a successful PUEA on a secondary user by a set of co-operating malicious users. They show that the probability of a successful PUEA increases with the distance between the primary transmitter and secondary users. This is the first analytical treatment to study the feasibility of a PUEA. They showed that their bounds enable in obtaining insights on possible ranges of exclusive regions in which an attack is most likely. Their results motivate the study of energy efficient PUEA attacks.

[3] In this paper, a joint position verification method of Time Difference of Arrival (TDOA) and Frequency Difference of Arrival(FDOA) is proposed to enhance the positioning accuracy. Simulation results show that the method is simple and achieves high accuracy on transmitter location verification in CR network, which can improve the ability to resist the pue attack. They consider the scenario that all users are in low-speed movement. Simulation results show that our method can improve the localization accuracy, which strengthens the ability to resist PUE attack.

[4] In this paper, they address the problem of authenticating the PU signal in order to mitigate PU emulation attacks. They propose a PU authentication system based on the deployment of "helper" nodes, fixed within the geographical area of the CRN. Our system relies on a combination of physical-layer signatures (link signatures) and cryptographic mechanisms to reliably sense PU activity and relay information to the CRN. Compared to prior work, the system can accommodate mobile secondary users and can be implemented with relatively low-power helpers. The security analysis showed that authentication system can withstand impersonation attacks of the PUs as well as of the helpers nodes.

[5] In this paper, they present a cross-layer attack to TCP connections in cognitive radio networks, analyze its impact on TCP throughput via analytical model and simulation, and propose potential countermeasures to mitigate it. This paper discuss the detailed lion attack. The main contribution of this paper is the evaluation of the impact of the Lion attack on TCP performance through an analytical model. Moreover, the model has been validated through simulations considering two implementations of TCP: the standard TCP Reno and the modified version proposed to mitigate the effects of the attack. The results obtained show that freezing TCP parameters reduces the effect of the handoffs (caused by the attack) on the throughput of TCP.

[6] This paper firstly discuss the security issues in cognitive radio that are High Sensitivity to primary user signal, Unknown primary receiver Location. Then they discuss about the security and its requirement in CR networks. This relates to the characteristics of different protocol layers. They also discussed the security mechanisms for different protocol layers. Then they have studied the analytical model named Neyman-Pearson Criterion for Detecting PUEA in cognitive radio network. They have done a detailed analysis and simulation of the network for PUE attack. Simulations were carried out to determine the performance of the network for PUE attack in terms of probabilities of miss detection and false alarm. Then a model is proposed named maximum likelihood criterion for PUE attack. Simulations were carried out to determine the performance of the proposed system model for PUEA attack in terms of probabilities of miss detection and false alarm.

[7] In this paper, they discuss various security issues in cognitive radio networks and then to discuss the PUEA with the existing techniques to mitigate it. They use various defence techniques against PUEA are Transmitter verification scheme, Fenton approximation method, Variance detection method, Fingerprint verification method, Location based method, Applying ANN, ALDO, PU authentication, Hybrid PUEA Defence , IRIS, Encryption and displacement method, Sybil Attack, MME, Cross-layer approach, SPUS and SVDD, LCM and SCS, RSDP, Hearing is believing, Belief propagation, DECLOAK, Cooperative spectrum sensing, Dogfight, Game theoretic approach .

[8] In this paper they focus on security problems arising from Primary User Emulation (PUE) attacks in CR networks. They present a comprehensive introduction to PUE attacks, from the attacking rationale and its impact on CR networks, to detection and defense approaches. In order to secure CR networks against PUE attacks, a two-level database-assisted detection approach is proposed to detect such attacks. Energy detection and location verification are combined for fast and reliable detection. An admission control based defense approach is proposed to mitigate the performance degradation of a CR network under a PUE attack. By reserving a

portion of channels for the handoff services, the dropping rate induced by successful PUE attacks could be evidently reduced. Illustrative results demonstrate that the reported detection and defense approaches are effective in discovering and defending PUE attacks in CR networks.

[9] This paper considers primary user emulation attacks (PUEA) in cognitive radio networks operating in the white spaces of the digital TV (DTV) band. They propose a reliable AES-encrypted DTV scheme, in which an AES encrypted reference signal is generated at the TV transmitter and used as the sync bytes of each DTV data frame. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and be used to achieve accurate identification of authorized primary users. It is shown that with the AES-encrypted DTV scheme, the primary user can be detected with high accuracy and low false alarm rate under primary user emulation attacks. Potentially, it can be applied to today's DTV system directly to mitigate primary user emulation attacks, and achieve efficient spectrum sharing. It is clear that the proposed AES-encrypted DTV approach achieves zero miss detection probability even under very low SNR values .

[10] This paper discusses a new approach, based on anomaly behavior detection and collaboration, to detect the PUE attack in CWSN scenarios. A nonparametric CUSUM algorithm, suitable for low resource networks like CWSN, has been used in this work. For example, the result shows that the number of collaborative nodes is the most important parameter in order to improve the PUE attack detection rates. If the 20% of the nodes collaborates, the PUE detection reaches the 98% with less than 1% of false positives. If the collaborative nodes are over 20% of the total, the PUE attack detection has satisfactory results, with a 98% of attacks detected and a false negative rate near 0%, independently of the number of nodes in the scenario. As the results show, the collaborative systems and the behavior models are valid to detect a PUE attack.

[11] In this paper a new approach, based on anomaly behavior detection and collaboration, is used to detect the primary user emulation attack in CWSN scenarios. Two non-parametric algorithms, suitable for low-resource networks like CWSNs, have been used in this : the cumulative sum and data clustering algorithms. The comparison is based on some characteristics such as detection delay, learning time, scalability, resources, and scenario dependency. Both algorithms have shown to be valid in order to detect PUE attacks, reaching a detection rate of 99% and less than 1% of false positives using collaboration. If the collaborative nodes are over 20% of the total, the PUE attack detection has satisfactory results, with 99% of attacks being detected and a false positive rate near 0%, independently of the number of nodes in the scenario. Both have demonstrated to be valid in order to detect the PUE attack anomalies.

[12] In this paper to counteract the PUE attack, a transmitter verification scheme called LocDef (localization based defense), is used to verify whether the given signal is from an incumbent transmitter by estimating its location and observing its signal characteristics. This can be integrated into the spectrum sensing process and LocDef employs a non-interactive localization scheme to detect and pinpoint PUE attacks under certain conditions. For the identification of attacks on Physical-layer , the modulation-based and transient-based fingerprinting techniques are performed. QAM provides higher data rates than QPSK.

[13] In this paper an advanced survey over attacks and common threats and the possibility of securing the available spectrum from the attackers is provided. They use the spread spectrum modulation techniques for secure communication. Here, a cross-layer is proposed for avoiding the selfish performance in the routing protocols for the dynamic cognitive radio network in preference to selfish nodes. Simulation results proposed that SAR provides better performance, by means of higher throughput, lower delay, and better delivery ratio. So, it can be said as the cross layer selfishness avoiding routing protocol.

[14] This paper will give a variety of security requirements for cognitive radio networks and then discusses the PUEA with the preventive procedures to mitigate it. There are few of the crucial features of CRNs like awareness, reliability and adaptability need to be deployed successfully for better communication. At the same time preventing the network from threats and malicious intent is equally important and a challenging task. The physical layer is significant in terms of detection of this malicious node. PUEA is one of the security issues in the physical layer of the protocol stack. The modus operandi of this paper is the mitigation methods for PUEA.

[15] In this paper, a new mechanism based on physical layer network coding is used to detect the emulators. When two signal sequences interfere at the receiver, the starting point of collision is determined by the distances among the receiver and the senders. Using the signal interference results at multiple receivers and the positions of reference senders, they can determine the position of the 'claimed' primary user and compare this localization result with the known position of the primary user to detect the PUE attack. They analyze the overhead of the proposed approach and study its detection accuracy through simulation.

CONCLUSIONS

This paper discusses about the various defence techniques for mitigating PUE attack found in the cognitive radio networks. Due to lack of available spectrum, and increase in the applications on wireless systems made the cognitive radio an adaptable method in the demanding wireless technology. The discussion provided here gives a reliable measure to make it as an analysis paper relating to the possible attack and verification procedures to mitigate this attack. This survey of the detection schemes motivates us to continue our research work and select one or two of the most suitable techniques to demonstrate the detection of the PUE attack by simulating the scenario. Although, some of the defense mechanisms have been proposed, they can't completely fulfill the need of CR networks operation. This leads us to our future research work which will give the ultimate solution to PUEA.

.

REFERENCES:

[1] Ruiliang Chen and Jung-Min Park "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks" Department of Electrical and Computer Engineering,2006.

[2] S. Anand, Z. Jin and K. P. Subbalakshmi "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks" Department of Electrical and Computer Engineering Stevens Institute of Technology,2008.

[3] Lianfen Huang, Liang Xie, Han Yu, Wumei Wang, Yan Yao "Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks" International Conference on Communications and Mobile Computing,2010

[4] Swathi Chandrashekar and Loukas Lazos "A Primary User Authentication System for Mobile Cognitive Radio Networks" Dept. of Electrical and Computer Engineering,2010.

[5] Juan Hernandez-Serrano, Olga Le´ on, and Miguel Soriano "Modeling the Lion Attack in Cognitive Radio Networks" EURASIP Journal on Wireless Communications and Networking, 2011.

[6] Deepraj S. Vernekar "An Investigation Of Security Challenges In Cognitive Radio Networks" Dissertations & Student Research in Computer Electronics & Engineering,2012.

[7] Deepa Das, Susmita Das "Primary User Emulation Attack in Cognitive Radio Networks: A Survey" International Journal of Computer Networks and Wireless Communications , June 2013.

[8] Rong Yu, Yan Zhang, Yi Liu, Stein Gjessing, Mohsen Guizani "Securing Cognitive Radio Networks against Primary User Emulation Attacks" IEEE , August 2013.

[9] AhLmed Alahmadi, Mai Abdelhakim ,Jian Ren, Tongtong I "Mitigating Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard" Department of Electrical & Computer Engineering,2013.

[10] Javier Blesa, Elena Romero, Alba Rozas, Alvaro Araujo, and Octavio Nieto-Taladriz "PUE Attack Detection in CWSN Using Collaboration and Learning Behavior" International Journal of Distributed Sensor Networks , 2013.

[11] Javier Blesa, Elena Romero, Alba Rozas and Alvaro Araujo "PUE attack detection CWSNs using anomaly detection techniques" Blesa et al. EURASIP Journa on Wireless Communications and Networking, 2013.

[12] T.Lakshmibai, B.Chandrasekaran, C.Parthasarathy "Primary User Authentication In Cognitive Radio Networks: A Survey "International Journal Of Advanced Research In Electrical ,Electronics and Instrumentation Engineering(IJAREEIE)",January 2014.

[13] S. Bhagavathy Nanthini, M. Hemalatha, D. Manivannan and L. Devasena "Attacks in Cognitive Radio Networks (CRN) — A Survey"Indian Journal of Science and Technology, April 2014.

[14] Shikha Jain , Anshu Dhawan, C.K Jha "Emulation Attack in Cognitive Radio Networks: A study" IRACST – International Journal of Computer Networks and Wireless Communications , April 2014.

[15] Xiongwei Xi*e*, Weichao Wang "Detecting Primary User Emulation Attacks in Cognitive Radio Networks via Physical Layer Network Coding" Journal of Ubiquitous Systems & Pervasive Networks, August 2014