The Primordial model for eliminating the malevolent secondary user from LTE based Cognitive Radio Network

[1]C.Kiruthika,[1]PG Scholar,
[1]Department of Computer Science and Engineering
[1]SNS College of engineering, Coimbatore,India.

Abstract--**The radio spectrum is used for communication and most of this spectrum space is underutilized. Due to rapid increase in wireless communication FCC introduced a new technology called Cognitive Radio Networks (CRN), which uses IEEE 802.22 Standard. The unused spectrum spaces are reserved by the licensed Primary Users (PU) and they allow the unlicensed Secondary Users (SU) to access the spectrum resources when it is not used by PU. Some SU does not vacate the channel when the PU wants to access the spectrum which causes the Primary User Emulation Attack (PUEA). The proposed primordial model is applied in the LTE network. This novel approach can eliminate the malicious SU in a proactive way and provides high performance than the existing techniques.**

Index terms--Cognitive Radio Network, PUEA, LTE network.

INTRODUCTION

The spectrum scarcity problem and the demand for spectrum scarcity is solved by the Cognitive Radio Network (CRN) technology [1]. There are two types of users in the CRN called the Primary Users (PU) that is the licensed users and the unlicensed users, that is the Secondary Users (SU). Each PU can share its spectrum resources with any number of SU.

The Federal Communications Commission (FCC) takes necessary steps to improve the use of unused spectrum spaces. The radio spectrum is mainly used for communication. The FCC has introduced a new spectrum sensing technology, called Cognitive Radio Networks (CRN). The CRN used the Radio waves for communication [1].

There are two types of users that mainly uses the spectrum spaces namely the Primary User and the Secondary User. The Primary stations are the service providers who allow the use of spectrum to the SU when it is not used by them. Some of the selfish SU emulate themselves as the PU and cause DoS to the network.

The IEEE 802.22 is the standard for cognitive wireless regional area networks (WRANs) [2].There are many detection techniques available for the PUEA[3]. The available defence technique does not fully eliminate the PUEA [4]. The major challenge is to differentiate the PU from the SU. The emulating attacker must be sensed and identified by the Secondary User (SU).

Due to Dynamic Spectrum Access (DSA) CR network gives opportunity to the attacker to damage the routine activities of the communication networks. CR are capable of sensing the unused spectrum—i.e., spectrum "whitespaces" [4]. The key problem is to distinguish the primary user signal from the secondary user in an efficient way. On the other hand, the detection of Primary User Emulation (PUE) attack is important. The secondary users must sense and identify the emulation attacker.

The third generation partnership project (3GPP) long-term evolution (LTE) is the most reliable and promising standard for wireless networks [2]. The LTE network has increased data rates both for uplink and downlink. LTE is highly efficient and robust towards interference.

I. PRIMARY USER EMULATION ATTACK

The major threat to the physical layer of CRN is the PUEA. In the PUEA the unlicensed SU can use the spectrum when the licensed PU is not using the spectrum. When the PU approaches the spectrum access, then the SU should vacate the channel. But some SU uses the channel by emulating themselves as the PU and causes DoS to the network [9].

The PUEA can cause intervention to the spectrum sensing and reduces the availability of channel to the incumbent SU. This attack can be carried out by the selfish PUE and the malicious PUE [9]. On the other hand in learning radios, information about the primary users current and the past behaviours are gathered in order to know when the channel gets idle. The attackers perform this attack when the channel gets idle.

II. PUEA DEFENSE TECHNIQUES

Despite of all the attacks in CRN the PUEA causes adverse effects so the prevention of PUEA is important in CRNs. The methods discussed here focus on the mitigation of PUEA and some assumptions are made to produce better results. Here the PU is TV transmitters. AT first mobile FM wireless microphone is considered as PU and PUEA is defined by Shaxun Chen et al in [7].

PU Authentication

The stationary helper nodes are used to authenticate PU using link signature and the broadcast spectrum availability information to the SU [8]. The extra helper nodes which are fixed must be authenticated by the trusted authority with the help of public key and certificate. The helper resolution (HR) algorithm is used for the mobile users and the analysis has been done on different attacks. Without repeated training more SU can be served and the successful defense against the attack can be provided.

Location based method

Based on the location of PU there are three types of defense techniques. In the wavelet transform scheme the fingerprint is extracted using the multi-resolution time frequency property which can be used to distinguish the PUE attacker and the incumbent PU signal. The Time Difference of Arrival (TDOA) scheme is used to detect the PUE attack and to find the position of the emitter. The quadratic error can be minimized by the Weighted Least Square (WLS) method. In order to find the PUEA, tier hierarchical CRN and M-ary hypothesis is done in the two-tier scheme [10].

Fingerprint verification method

The phase noise is extracted from the received signal in the ANN based scheme. The ANN can identify the transmitter by using the wavelet analysis [11]. Fingerprint is considered as the unique characteristics in [11]. To get the false alarm rate the channel based hypothesis testing can be done. The OFDM uses this technique. Hence the detection probability can be increased by increasing the SNR.

Transmitter verification scheme

In this scheme three defense techniques are used. In the Distance Ratio Test (DRT), using the pair of verifiers the distance ratio of received signal strength can be obtained. To identify the transmitter location the phase difference of the received signal is obtained using the Distance Difference Test (DDT). In this method the location of all the users is assumed to be fixed and the verifiers must have tight synchronization. When the attacker is close to the SU performance of the system will be degraded. The peak of the RSS signal can be used to locate the transmitter by using the Location-based Defense (LocDef) [12].

Sybil attack

Sybil attack is similar to the Byzantine attack in which the Sybil identities are created to modify the decision of SU and launches PUEA. Spider radio, the CR test-bed is used to prove the feasibility [13]. With the decrease in the number of good nodes the cost increases adversely. The fusion center helps to estimate the expected cost.

Belief Propagation

Belief propagation of the location information can be calculated. Here the location and compatibility function, the message computation, message exchange between neighboring users and until its coverage calculation of belief is done. The PUE attacker can be found when the calculated mean of belief is less than the threshold [14]. Markov random process can be used to achieve better results. The attacker's transmission power and range is limited. All the SUs must be aware of the location information of the PU. When the distance between the PU and the attacker is less, then the calculated belief mean will be more.

III. SYSTEM MODEL

A typical LTE based CRN architecture is considered for illustration shown in Fig.1. The network consists of Primary Users denoted as eNBs (PBs) numbered PB1, PB2, . . . , PBn, and m Secondary Users (unlicensed) eNBs (SBs) numbered SB1, SB2, . . . , SBm. The PU are connected to the centeralized server called the fusion centre which contains information about all the nodes . Each PB operates on its fixed licensed spectrum band (primary channel) with some certain serving capacity. It can share its primary channel with one or more SBs, which do not have a fixed licensed spectrum band. The PBs have prioritized access to their primarychannels. The network operates on a slotted-time basis.

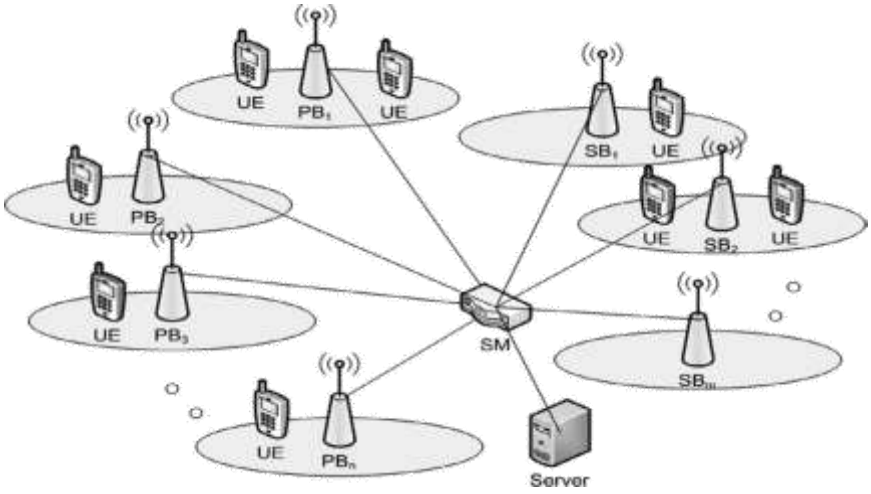

Fig. 1. A typical CRN architecture.

IV. PROPOSED SOLUTION

Various security issues of the CRN are discussed in section 2 and the section 3 provides the overview of PUEA. Usual approaches, such as embedding a signature in a primary user's signal or employing an interactive protocol between a primary user and secondary user, cannot be used [14]. Identifying the primary user signal is considered to be a major challenging task.

Our proposed method consists of detecting malicious user signal by a novel approach called Intense explore. It is a continual diagnosis of existing secondary users signal in which few of them may threatens to be a malicious user in future. This proactive detection method is done in a cooperative way.

To enhance the sensing performance, cooperative spectrum sensing [10] is involved. A centralized fusion centre will collect the sensing results from the cooperating secondary users. In our proposed method, we consider the centralized cooperative pre-detection. Here, a central identity called fusion centre (FC) [11] will collect the diagnose results from the cooperative secondary users.

Early detection of PUEA in LTE

An infrastructure based network of CRs where multiple nodes (or Secondary Users, SUs) may be associated with a centralized fusion centre as stated in [12], [13] is considered.

The fusion centre will collect the diagnose results from the cooperative secondary user in a regular interval. Each of the cooperative secondary users will diagnose the signals of other neighbour secondary users at a regular interval. The main objective of diagnosing neighboring secondary users signal is to anticipate that any of these secondary users may become a malicious user in future and threaten the cognitive radio network with PUE attack.

Assuming any of the neighboring secondary users signal suspected to emulate the primary signal, then it is reported the fusion centre. The fusion centre which may receive similar reports from other cooperative secondary users ,in turn alert all the cooperating secondary users in the network about the anticipated PUE attack and relinquishes the suspected secondary user from the CRN.

Here the LTE is considered as the Primary User. Consider two set of nodes Pi and Qj. Each node in the set is considered to sense the spectrum at regular interval. Suppose a node in set Qj is assumed to be sensing any of the two of its neighbouring node in set Pi. Then based on the transmission power and the bandwidth of the LTE the node can report the fusion centre about the emulation SU.

If the bandwidth and the transmission power of the SU exceeds the threshold then the node in set Qj reports the fusion centre about the malicious SU. If any of the two nodes in the set Qj reports about the malicious SU then the fusion centre alerts all other nodes about the malicious SU and sends a warning signal.

V. SIMULATION RESULTS

Primordial model

In the Primordial model the number of SUs in set Pi senses the neighboring SUs in Qj. Fig.3 represents the number of cooperative SUs in set Pi senses the neighboring SUs in Qj at the regular interval.

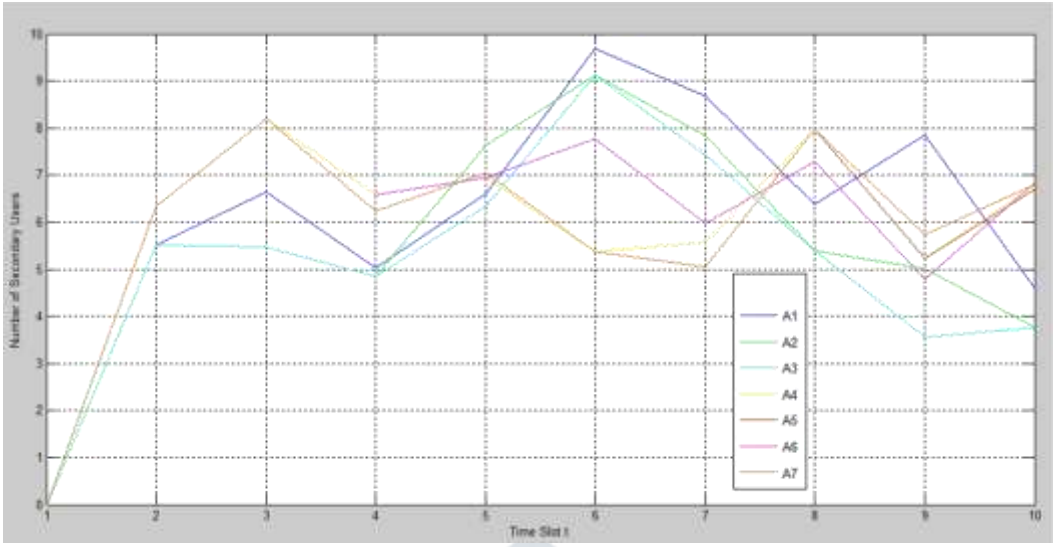

Fig.2. Each SU in Pi senses same SUs Qj in Qt

VI. CONCLUSION

In this paper, various Security issues in Cognitive Radio Networks and the Primary User Emulation has been discussed in detail. The solution for the early detection of Primary User Emulation Attack (PUEA) in LTE based Cognitive Radio Network has been identified. The proposed solution can eliminate the malicious Secondary User in a proactive way through cooperative sensing. This proposed solution can improve performance of the CRN when compared to the existing techniques.

REFERENCES

[1] Mitola J III. Software radios – survey, critical evaluation and future directions. IEEE Aero Electron Syst Mag. 1993 Apr; 8(4):25–36.
[2] R. G. Gallager, Principles of Digital Communications. UK: Cambridge University Press, 2008.
[3] Deepa Das, Susmita Das, “Primary User Emulation Attack in Cognitive Radio Networks: A Survey”, IRACST, Vol.3, No3, June 2013.
[4] M. T. Mushtaq, M. S. Khan, M. R. Naqvi, R. D. Khan, M. A. Khan, Prof. Dr. Otto F. Koudelka,” Cognitive Radios and Cognitive Networks: A short Introduction”, J. Basic. Appl. Sci. Res., 3(8)56-65, 2013.
[5] Zhao C, Xie L, Jiang X, Huang L, YaoA Y. PHY-layer authentication approach for transmitter identification in cognitive radio networks. 2010 International Conference on Communications and Mobile Computing (CMC). 2010 Ap 12–14; Shenzhen. IEEE. p. 154–58.
[6] Anand S, Jin Z, Subbalakshmi K. An Analytical model for primary user emulation attacks in cognitive radio networks. 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks. DySPAN; 2008 Oct; Chicago, IL. IEEE. p. 3905–14.
[7] Wang H, Lightfoot L, Li T. On PHY-layer security of cognitive radio:collaborative sensing under malicious attacks. 44th Annual Conference on Information Sciences and Systems (CISS); 2010 Mar 217–19; Princeton, NJ. IEEE. p. 66–73.
[8] Zhou, Xiao; Xiao, Yang; Li, Yuanyuan, "Encryption and displacement based scheme of defense against Primary User Emulation Attack," Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on , vol., no., pp.44,49, 27-30 Nov. 2011.
[9] Hernandez-Serrano J, León O, Soriano M. Modeling the Lion Attack in Cognitive Radio Networks. EURASIP Journal on Wireless Communications and Networking. 2011; 10:242–304.
[10] K. Ben Letaief and W. Zhang, “Cooperative communications for cognitive radio networks,” Proc. IEEE, vol. 97, no. 5, pp. 878 –893, May 2009.
[11] D. Niyato and E. Hossain, “Competitive spectrum sharing in cognitive radio networks: a dynamic game approach,” IEEE Trans. Wireless Commun., vol. 7, no. 7, pp. 2651 –2660, Jul. 2008.
[12] Zhu L, Zhou H. Two types of attacks against cognitive radio network MAC protocols. International Conference on Computer Science and Software Engineering; 2008 Dec; Wuhan, China. IEEE. p.1110–13.
[13] Chandrashekar, S.; Lazos, L., "A Primary User authentication system for mobile cognitive radio networks," Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on , vol., no., pp.1,5, 7-10 Nov. 2010.
[14] Tarun Bansal, Bo Chen and Prasun Sinha, “FastProbe: Malicious User Detection in Cognitive Radio Networks Through Active Transmissions”, INFOCOM, May 2014.
[15] Ian F.Akyildiz, Brandon F.Lo *, Ravikumar Balakrishnan, “Cooperative spectrum sensing in cognitive radio networks: A survey”, Iournal Physical Communication, Volume 4 Issue 1, March, 2011 Pages 40-62.