Detection & Defensive Approach for Primary User Emulation Attacking Cognitive Radio Network

K.Gokulakrishnan¹, B.Kiruthiga²*, N.Jayapal³, S.P.Karthi⁴ and Albert Alexander Stonier⁵

¹IFET College of Engineering, Villupuram, Tamil Nadu, India.
²K.Ramakrishnan College of Technology, Samayapuram, Trichy, Tamil Nadu, India.
³Kongunadu College of Engineering and Technology, Trichy, Tamilnadu, India
⁴Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India
⁵Department of Electrical and Electronics Engineering, Kongu Engineering College, Perundurai, Tamilnadu, India

*Email id: kiruthigabalu94@gmail.com

ABSTRACT: Cognitive Radio Network (CRN) is the future scope wireless technology that aims to enhance the spectrum utilization. It meets out the increasing demand in spectrum access by all possible wireless applications and services. Security is an important issue but not focused much in CRN. In this research, the detection and defensive approach for Primary User Emulation Attack (PUEA) is presented. In order to secure cognitive radio network against PUEA, two level of detection algorithm is proposed. Energy detection with three threshold value and localization technique is used to detect the attackers. To enhance the Quality of Service (QoS) of the Secondary Users (SU), guard channel is allocated to the secondary user by the fusion center. This process is carried out whenever the communication between the SUs is intervened by the licensed primary user or an attacker.

Keywords: Cognitive radio network; security; localization; primary user; secondary user; QoS; primary user emulation attack; throughput; delay; energy consumption; guard channel.

I. Introduction

The tremendous growth in mobile traffic data has evolved the need for next generation network. An implementation of cognitive concept can be one of the optimal solutions to meet out the above demand. In this technology, the licensed users are termed as Primary User (PU) and unlicensed user are termed as Secondary User (SU). Whenever the spectrum band allocated for the PU is free, the SUs can use that spectrum opportunistically [1]. The transmission of SU must not affect the performance of the PU. In order to avoid the collision between PU and SU, each SUs performs spectrum sensing. In spectrum sensing, the SU senses the spectrum to identify the presence of PU. The sensing result of the individual SU may encounter incorrect judgments because of multipath fading, shadowing and building penetration. In order to increase the sensing performance and accuracy Cooperative Spectrum Sensing (CSS) technique is used. In CSS, each SUs shared their sensing information with each other. The commonly used CSS techniques are centralized and decentralized spectrum sensing [2]. In centralized spectrum sensing technique, all the sensing results are forwarded to the Fusion Centre (FC). The FC combines all the results from the SU and takes a final decision. In decentralized spectrum sensing the FC is not present, the sensing results of all SUs involved in CSS are shared among themselves. In this method periodic update on the spectrum information is necessary; hence it requires more storage and complexity. In CRN,
security is one of the most important issues. The Dynamic Spectrum Accessing (DSA) nature of CRN leads to several vulnerabilities for various kinds of attacks. It has more security issues than the traditional wireless networks. It is necessary to identify the types of security attacks and its related protection measures. The PUEA is one of the popular malicious attack specified in CRN [3]. In such attacks, the attacker emulates the transmitting signal of PU. If the SUs does not aware of this attack, it cannot able to access the spectrum. Thus, the legitimate SUs transmission is affected by the PUEA. In this research, the problem arising due to PUEA is addressed. There are two types of attackers [4]. They are power-fixed attacker and power adaptive attacker. A power fixed attacker used its own power level instead of using the transmission power of real PUs. So, it can be easily identified by the energy detection technique. But power adaptive attacker is smarter than the power fixed attacker. It estimates the power level and other transmission parameters of PU and it emulates the PU.

II. Literature Survey

In this, some detection approach for PUE attacks has been presented. The existing detection approaches for PUE attacks are based on energy detection; RSS based detection, feature detection, location verification and cooperative detection.

In [5], the attacker detection is based on optimal different methods like energy detection. The threshold of energy is chosen on the basis of false alarm probability and missed detection probability. It uses the voting rule of estimation and optimal samples number to detect the attacker. If the received signal energy is lesser than the threshold value, then the detected user is classified as an attacker else a legitimate PU. In this approach, the attacker is detected approximately and hence the probability of misdetection can be high.

In [7], Energy detection is done to find the frequency location of the potential PUEA. It is determined from the received signal. It is then compared with the database which contains the feature of the primary user signal. Feature includes velocity, velocity gradient, divergence and vortices. The feature of the PU is mapped to a vector space by using matrix algorithm. When the feature matches with the database then it is a real PU, else it is an attacker.

In [8], the channel tap power is used as radio-frequency fingerprint to identify the PUEA over multipath Rayleigh fading channels. When PU or an attacker accesses the spectrum, its channel tap power is calculated by the SU. If the estimated tap power matched with the fingerprinting database it is a real PU, else it is an attacker. The cross layer intelligent learning ability of a mobile SU is exploited to increase the accuracy of detection. If the attacker uses same channel tap power, it is difficult to classify the attacker from real PU.

In [9], the combined approach of energy detection and localization technique is used. Traditional energy detection using single threshold value is used to classify the attacker from real PU and RSS based localization approach is used to locate the position of the attacker. The accuracy of the energy detection technique using threshold value is low. In this research, adaptive energy detection technique using three threshold value combined with RSS based localization technique is proposed to detect the attacker. Also guard bands are used to continue the ongoing communication of secondary users.

III. Methodology

The proposed methodology is detailed in this section. Fig.1, Present the system model considered in the proposed research. It consists of Primary Base Station, Secondary Base Station or FC, Primary Users (PU), Secondary Users (SU) and attackers. Let us consider a spectrum which consists of six channels indexed by frequencies namely $f_1$, $f_2$, $f_3$, $f_4$, $f_5$ and $f_6$. Let PU1, PU2 and PU3 be the primary users. Let SU1, SU2 and SU3 be the secondary users and PUEA1, PUEA2 be the attackers.
The attackers in a system model can be either static or quasi stable state. Assume that in a given moment; only one of the attackers can emulate a primary signal. The presence of PUEA prohibits the secondary user from using the idle channel, since it mimic the primary user. For example, the access of channel with frequency $f_5$ by SU3 is prohibited by PUEA1, because SU3 detects PUEA as PU. In this, secondary user is assumed to consist of four main units. They are signal processing unit, energy detection unit, location verification unit and local database. Local database consists of fingerprinting database [10]. In fingerprinting database, the location of the primary users with corresponding RSS and the device information are stored.

![System model](image.png)

**Fig.1. System model**

The PUEA detection scheme is presented in Fig 2. The sensed signal is processed in the signal preprocessing unit [12]. It is followed by the energy detection technique using three threshold value. Based on the threshold value it classifies the attacker and real PU. If it is detected as an attacker, then the localization technique based on RSS is used to detect the attacker. Such decision taken by the secondary user is a local decision. The FC collects all the local decision from the SUs and takes global decision.

**IV. Energy Detection**

Let $x'(t), h'(t)$, and $n'(t)$ be the signal of transmission, response of an impulse signal and noise respectively. Let $s(t)$ be the signal of real primary user and $s'(t)$ be the signal of primary user emulators. The transmitting signal $x(t)$ can be given as

$$x'(t) = \begin{cases} s(t), & \text{for real PU} \\ s'(t), & \text{for PUEA} \\ 0, & \text{no PU signal} \end{cases} \quad (1)$$
Let $y(t)$ be the received signal at the Secondary user which acts as a PUE detector and it can be given as

$$ y(t) = \begin{cases} h(t) * s(t) * n(t), & \text{for real PU} \\ h(t) * s'(t) * n(t), & \text{for PUEA PU} \\ n(t), & \text{no PU signal} \end{cases} \quad (2) $$

Let $N_s$ be the total samples sensed by the SU in one sensing period. These samples are then squared and aggregated. The signal processing unit preprocesses the signal and generates the energy vector ($e$) which is given as

$$ e = e[n], \quad \text{where, } (n = 1, 2, \ldots, N_s) \quad (3) $$

Then, the aggregated energy of the sampled signal is given as

$$ E = \sum_{1}^{N_s} e[n] \quad (4) $$

$E$, the energy of the aggregated signal, is then forwarded to the unit of energy detection. The three threshold values namely $\theta_1$, $\theta_2$ and $\theta_3$, where $\theta_1 < \theta_2 > \theta_3$ are considered. The signal from licensed user or PUE attacker is differentiated on the basis of the threshold values. If $E$ is less than $\theta_1$, then there is no PU signal. When $E$ lies between $\theta_1$ and $\theta_2$, initially it is considered as an attacker. Also, when $E$ is greater than $\theta_3$ then it is a real PU. Otherwise, it is considered as an attacker.

After comparing the energy with the threshold values, local decision on each SU is sent to the FC. The FC receives all the local decision from all other SUs. The FC maintains a global database, in that database all
the copies of SUs database are stored. Let $T_s$ be the local decision of $s^{th}$ node by SU and $T_m$ be the aggregated results by m SUs. $T_s$ become 1 for real PU and 0 otherwise.

The aggregated results $T_s$ can be given as

$$T_m = \sum_2^m T_s$$  \hspace{1cm} (5)

The global decision can be given as

$$D = \begin{cases} 1, & T_m \geq m/2 \\ 0, & T_m < m/2 \end{cases}$$  \hspace{1cm} (6)

The global result is shared to all SUs. If the FC detects an attacker, its information is shared to all the SUs and the information about the attacker is stored or updated in the SUs database and also in the global database.

V. Localization

In this approach, Received Signal Strength (RSS) based localization is used to verify the location of the PU and identify the location of PUE attackers. The RSS based localization is less accurate than GPS based localization and Time of Arrival (TOA) [12]. But RSS approach does not need any special hardware’s but other approaches require additional hardware’s. This approach is highly energy efficient.

In this method, the RSS of the PU is calculated by using the RSSI indicator in the received circuit [10]. The Location of the PU can be estimated by using the RSS of the received signal by comparing it with the fingerprinting database. Each Unlicensed user sends its location information to the Fusion Center.

The FC takes a final decision whether it is a real user or an attacker. It receives the information from all other secondary users. It performs data fusion to take the final decision about the user.

In CR network, secondary User’s ongoing process is interrupted due to the presence primary users or PUEA and its dynamic spectrum access nature. Under the presence of an attacker the dropping rate is increased so that it leads to the break of unlicensed user services. So that defender channel is introduced to protect the ongoing services of a secondary user. The handoff services needs new channel to continue the ongoing process. In this approach when SU needs a new channel it sends a request to the Meeting point [FC] [13]. The fusion center observes the remaining available channel. On receiving the request the fusion center allocates the SU to the new channel if reservation number is lesser than number of available channel present. Otherwise request from the SU is denied. Hence the dropping rate is significantly alleviated.

VI. Results and Discussion

The performance analysis of the proposed work is analyzed and the simulation results are discussed in this section.

![Fig.3. Deployment of nodes](image-url)
Initially, both primary users and secondary users are randomly deployed in the 1000 × 1000m square monitoring region as shown in figure 4. In that region 200 nodes which includes both primary and secondary users are randomly and evenly distributed in the square simulation area, including 50 secondary users (includes PUE) and 150 primary users. The “o” indicates primary users with unknown location and * indicates secondary users.

![Neighborhood chart of randomly distributed PUs and SUs](image)

**Fig. 4.** Neighborhood chart of randomly distributed PUs and SUs

In CRN, each SU has its own communication range. In this localization The SUs obtain the location relations of PUs within its communication range. In fig.4.each SUs verifies the location of PUs whether it satisfies the location requirements or not. If the location requirements do not matches, then it is considered as an attacker. Since the attacker may be one of the SU in a CRN.

![Throughput Comparison](image)

**Fig. 5.** Throughput Comparison

In Fig. 5, the throughput comparison between PUEA detection scheme with guard channel and without guard channel is shown. The result shows that throughput of the network with guard channel is higher than that of the network with guard channel.
In Fig. 6, the delay comparison between PUEA detection scheme with guard channel and without guard channel is shown. The result shows that the total delay of the network with guard channel is lower than that of the network with guard channel.

In Fig. 7, the energy consumption comparison between PUEA detection scheme with guard channel and without guard channel is shown. The result shows that total energy consumption of the network with guard channel is lower than that of the network with guard channel. Since, retransmission requires more energy.

VII. Conclusion

This research has focused in security issues in CRNs so that it shows an improved energy detection method by using many thresholds and localization technique is used to detect the attacker. The Guard channels are used to continue the ongoing process of the victim SU.

VIII. Future Scope

The future work of this research is by considering the mobile PUs and cyclostationary characteristics of the signal source is used to find the PUE attacker.

REFERENCES

[1]. Senhua Huang, Xin Liu and Zhi Ding.(2008). Opportunistic Spectrum Access in Cognitive Radio Networks, IEEE conference on Computer and Communications. pp.2101-2110
[2]. Ahmed Khattab, Dmitri Perkins and MagdyBayomi.(2013). Cognitive Radio Networks- from theory to practice. Springer.
[3]. Jianwu Li, ZeibingFeng, ZhiyongFeng and Ping Zhang.(2015).A survey of security issues in cognitive radio networks. IEEE journal on china communications. vol. 12 pp.132-235.
[4]. Fan Jin, Vijay Varadharajan and Udaya Tupakula. (2015). Improved Detection of Primary User Emulation Attacks in Cognitive Radio Networks. International Telecommunication networks and Application conference.

[5]. Mohammad Javad Saber, Seyed Mohammad and Sajad Sadough. (2013). Optimal energy detection in cognitive radio networks in the presence of malicious users. International Conference on Computer and Knowledge Engineering.

[6]. Zhou Yuan, Dusit Niyato, Husheng Li, Ju Bin Song and Zhu Han. (2012). Defeating PUEAs using belief propagation in CRNs. IEEE journal on selected areas in communications. vol. 30 pp. 1850-1860.

[7]. Di Pu, Alexander M, and Wynlinski. (2014). Primary User Emulation Detection using Database-Assisted Frequency domain action recognition. IEEE transactions on Vehicular Technology. vol. 63 pp. 4372-4382.

[8]. Trong Nghia Le, Wen-Long Chin and Ya-Hsuan Lin. (2016). Non-cooperative and cooperative PUEA detection using physical layer in mobile OFDM-based cognitive radio networks. IEEE conference on Communications and Networking.

[9]. Yang Zhen, Yuebin Chen, Chuanxi Xing, Jnapei Chen and Ting Zheng. (2016). A scheme against Primary User Emulation Attack based on improved energy detection. IEEE conference on information and proceedings. pp. 2056-2061.

[10]. Guoqiang Mao and Baris Fidan, “Localization Algorithms and strategies for Wireless Sensor Networks”, pp. 282-300.

[11]. Bhuvaansehri C, Manjunathan A 2019 Advanced gesture recognition system using long-term recurrent convolution network Proc. ICONEEA, pp. 1-8.

[12]. Saud Althunibat, Raúl Palacios and Fabrizio Granelli. (2012). Energy-efficient spectrum sensing in Cognitive Radio Networks by coordinated reduction of the sensing users. IEEE conference on communications. pp. 1399-1404.

[13]. Ali Yassin, Youssef Nasser, Mariette Awad, Ahmad Al-Dubai, Ran Liu, Chau Yuan, Ronald Rulefs and Elias Aboutani. 2016. Recent Advances in Indoor Localization: A survey on Theoretical Approaches and Applications. IEEE communications surveys and tutorials. pp. 1327-1346.

[14]. Khan Tanjama Mustarin and Mostafa Zaman Chowdhury. 2016. Class-based service connectivity using adaptive guard channel reservation in wireless networks. International Conference on Electrical Engineering and Information Communication Technology (ICEEICT).

[15]. Lawson, et al. A. Survey and Evaluation of Acoustic Features for Speaker Recognition. In Proceedings of the 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), prague, Czech Republic, 22–27 May 2011; pp. 5444–5447.