International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Review Article

A Survey of Various Defense Techniques to Detect Primary User Emulation Attacks

Abhilasha Singh[Á*] and Anita Sharma[Á]

[Á]Department of Electrical, Electronics and Communication Engineering, ITM University

Accepted 10 April 2014, Available online 15 April 2014, **Vol.4, No.2 (April 2014)**

Abstract

With the advancement in wireless technology, there is an increasing problem of spectrum scarcity. To resolve this issue, a technology called Cognitive Radio (CR), based on Joseph Mitola's Software Defined Radio (SDR) was introduced, in which the secondary users can sense the spectrum and utilize the licensed bands when the spectrum is not being utilized by the primary user. Because of its wireless nature, this device attracts various security threats common to all wireless technologies. In addition to these, there are various security concerns specific to CR, which these networks are vulnerable to. One of the most dominant threats among these is the Primary User Emulation Attack (PUEA). In this paper, our main purpose is to list out the various security threats faced by the cognitive radio networks and in particular, PUEA. Further, we enlist the different defense techniques which can combat the PUE attacks and ultimately compare these defense techniques on various parameters.

Keywords: *Cognitive Radio, Spectrum Sensing, Primary User Emulation Attack*

1. Introduction

In the past ten years, wireless services have witnessed an increase in the user demand. Much of the radio spectrum available, in numerous countries, which is established on fixed spectrum allocation methodology, has been appointed for diverse services. Whereas, it is reported by the investigations of the spectrum usage pattern that low utilization occurs in the allocated spectrum (Y.Liang *et al*, 2008).

Federal Communications Commission (FCC) in 1985 authorized few sections of the spectrum as 'licence-exempt' which forms a part of the ISM (Industrial, Scientific and Medical) Band. In this band, there is a free movement of the users and no licence is required to access this band (A Fragkiadakis *et al*, 2012).

This and in addition the use of IEEE 802.11a/b/g standards revolutionized the entire wireless domain. Moreover, unlicensed devices can now utilize the additional spectrum in the 3GHz band and below 900 MHz, as granted by FCC. Nonetheless, due to ISM band being license free, it witnessed an increase in the number of users, thus, overcrowding the entire band. This eventually led to a rise in the contention and interference among the networking devices because of the inherent features of the protocols used such as IEEE 802.11. Still, there exist various licensed bands in the spectrum that are presently not utilized to its full capacity (A Fragkiadakis *et al*, 2012).

Joseph Mitola III, in a seminar, in 1998, at Royal Institute of Technology, Stockholm (Joseph Mitola III, 1999), contributed a new domain in the field of wireless communication namely Cognitive Radio (CR). The purpose of this domain was the opportunistic utilization of the portions of the spectrum that are scarcely used at present (A Fragkiadakis *et al*, 2012). He along with Gerald Maguire published this work later on in IEEE Personal Communications (Joseph Mitola III and Gerald Maguire, 1999).

Cognitive Radios are the devices that have the capability of sensing the spectrum and utilize its free sections in an opportunistic way. These free sections of the spectrum are cited as 'white spaces' or 'spectrum holes'. The formal definition of a spectrum hole as given by (Simon Haykin, 2005) is: "A spectrum hole is a band of frequencies assigned to a Primary User (PU), but, at a particular time and specific geographic location, the band is not being utilized by that user". Generally, there are two classes of users: (i) incumbent or primary users (PUs) that own the license of a specific part of the spectrum, and (ii) secondary or cognitive users (SUs) that opportunistically utilize the portions of the spectrum, to avoid interference with PUs.

There are three important segments of the Cognitive Radio:

(1)*Spectrum Sensing:* It is the job of the SUs to sense and analyze the radio spectrum environment in their range of operation to detect those frequency bands which are not acquired by the PUs. This can be achieved by using various techniques such as energy detection, interference based detection, matched filter, cyclostationary feature

*Corresponding author: **Abhilasha Singh**

detection, and cooperative detection (sensing the spectrum with the cooperative hard work of multiple cognitive radios) (Yenumula B. Reddy, 2013); (2) *Dynamic Spectrum Management:* It is the responsibility of a CR Network to dynamically choose the most appropriate bands available for communications; and (3) *Adaptive Communications:* The transmission parameters such as bandwidth, carrier frequency, transmission power, etc can be configured by a CR device to make best use of the spectrum available in an opportunistic manner (Y.Liang *et al*, 2008).

A notice was issued by FCC in December 2003 ruling that cognitive radio be identified as an applicant for implementing spectrum sharing opportunistically. This led to the formation of IEEE 802.22 standard for WRAN (Wireless Regional Area Network) that is a substitute broadband access scheme with its operation in unused UHF/VHF TV bands. This ensured that the incumbent primary users faced no harmful interference. IEEE 802.22 standard (C.Cordeiro *et al*, 2006; C.Stevenson *et al*, 2009) is the first one to enable the utilization of fallow TV bands through infrastructure single-hop cognitive radio networks with the existence of one BS (Base Station) that carries out spectrum management. This standard has a security mechanism for data integrity, authentication, etc and it encourages the provision of fixed broadband wireless data in scarcely populated rural areas (A Fragkiadakis *et al*, 2012).

Cognitive radios have two main attributes (I.F.Akyildiz *et al*, 2006):

(1) Reconfigurability which allows a CR to alter certain parameters such as frequency modulation, etc and adjust to its environment. This is significant because CRs must utilize the fallow bands opportunistically and empty a band whenever any primary user transmission is detected (A Fragkiadakis *et al*, 2012).

(2) Cognitive Capability which prepares these devices to sense their environment and select the most appropriate transmission mode available in the fallow bands. This is attainable by the process of spectrum management where various parameters of the physical layer such as power, modulation type, frequency, etc are estimated (A Fragkiadakis *et al*, 2012).

The operations that a cognitive radio executes for adaptive operation are described as the cognitive cycle, as shown in Figure 1.

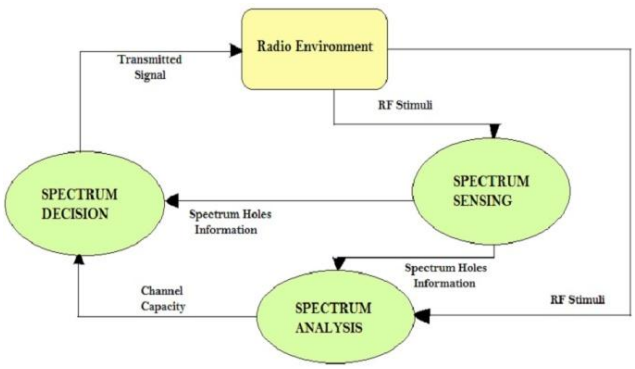

Fig.1 Cognitive Cycle

adaptive operation are described as the cognitive cycle, as shown in Figure 1.

The cognitive cycle comprises of the following mechanisms:

(a) Spectrum Sensing: This is one of the most significant components of a CR and it performs the detection of incumbent signals (T.Yucek and H.Arslan, 2009). Two time scales are indicated: (i) fast sensing, i.e. 1 ms/channel, and (ii) fine sensing, which is determined dynamically by the BS, dependent on the fast sensing output, and senses the spectrum more accurately. The BS collects the observations made by SUs and makes the final decision about the presence or absence of incumbent signals. Energy detection method is used by IEEE 802.22 to detect an incumbent signal because of the low computational overhead and simplicity of the method. Other than 'energy detection', there are various other methods that have been proposed in (T.Yucek and H.Arslan, 2009) such as cyclostationary based sensing, waveform based sensing, matched filtering and radio identification based sensing.

(b) Spectrum Analysis: This process is based on the available information of spectrum holes, i.e. feedback from spectrum sensing. It analyzes various channel and network features such as capacity, bit error rate, delay, etc for each spectrum hole and later provides this analysis to the spectrum decision process (A Fragkiadakis *et al*, 2012).

(c) Spectrum Decision: It is the process that selects the best spectrum hole for transmission. This process can be performed by a single cognitive radio, or can be the result of various cooperating cognitive radios (A Fragkiadakis *et al*, 2012).

2. Security Threats: Overview

It was expected that the spectrum scarcity problem will be evolved by the introduction of CRNs which will make an intelligent use of the fallow2 spectrum bands. But, due to the wireless nature of these networks, they face all the security threats commonly existing in the traditional wireless networks. Generally, as the wireless networks are open in nature, they are exposed to various attacks targeting the MAC (medium access control) layers and the physical layers. At the MAC layer, the attacks include transmission of spurious frames (e.g. CTS, RTS, ACK), MAC Spoofing, etc. Attacks directing at the physical layer via RF jamming can critically disturb the operation of the network.

The most familiar security objectives for the wireless networks are: *(i) availability* which ensures the availability of network's resources as and when required by the devices and individuals, *(ii) access control* in which only the authorized devices and individuals can access the network's resources, *(iii) confidentiality* which ensures that no unauthorized user can read the network data, and *(iv) integrity* which can detect any changes (intentional/unintentional) occurring in the data during transit. Other than the previously mentioned threats inherited due to their wireless nature, Cognitive radio networks face new challenges and security threats which

have emerged because of their unique cognitive attributes. CRs vacate the specific spectrum band whenever it detects a primary signal. This property of the CR is misused by malicious users who mimic the characteristics of primary users and force the CRs to empty the specific band. This attack is called Primary User Emulation Attack (PUEA).

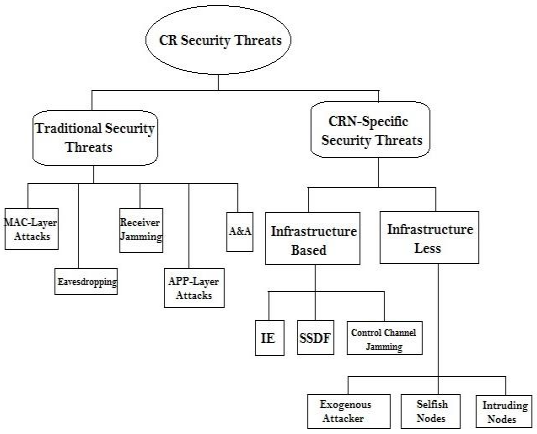

Fig. 2 Classification of various attack scenarios in a CRN architecture

Related to the technique of collaborative spectrum sensing, a technique used for improving spectrum sensing in a fading environment where multiple CRs collaborate, there exists another attack in which false observations are provided on purpose by a malicious CR. This attack is called Spectrum Sensing Data Falsification (SSDF) (A Fragkiadakis *et al*, 2012).

The attacks pertinent to Cognitive Radio Network architecture are demonstrated in Figure 2 (A.Attar *et al*, 2012).

The different attacks can also be classified according to their behaviour exhibited towards the protocol stack and its five layers (Wassim El-Hajj *et al*, 2011). This categorization has been demonstrated in Table 1 (Deepa Das and Sushmita Das, 2013).

A brief description of these five layers is as follows:

(1) Physical Layer: The attacks include PUEA, where the signal characteristics of the primary user are mimicked by the malicious user, thus, confusing the secondary user to identify the malicious attacker as the PU (R.Chen and J.M.Park, 2006); jamming attack, in which a continuous packet of data is sent into the channel by the jammer, thus, secondary user is unable to sense the channel as idle (Wassim El-Hajj *et al*, 2011); CCDA (Common Control Data Attack), which disturbs the transmission process by prohibiting the channel components to share spectrum usage information and also feeds all the information required for spectrum sensing to the attacker (Wassim El-Hajj *et al*, 2011); OFA (Objective Function Attack), in which the parameters of the utility resource might be changed by the malicious user, thus, the CR node becomes unsuccessful to adapt correctly (Wassim El-Hajj *et al*, 2011).

(2) Link Layer: This layer transfers data from one node to another. The three kinds of attacks include SSDF (Byzantine attack), where the malicious attacker sends the wrong result of the spectrum sensing, thus, falsifying the fusion centre decision (Wassim El-Hajj *et al*, 2011); SCN (Selfish Channel Negotiation), where wrong channel information is provided by the malicious node in order to change the route of the node; Control channel saturation DoS (Denial-of-Service) attack, where the control channel is reserved by the attacker and in turn gets saturated (Wassim El-Hajj *et al*, 2011).

(3) Network Layer: The two types of attacks include sink hole attack, where the attacker claims to be the most appropriate route to a specific destination in order to attract the neighbour node to use this route and pass on their packets so as to discard those packets (Wassim El-Hajj *et al*, 2011); Hello flood attack, where the transmitting power of the broadcast message sent to all the nodes in a network by the attacker is convincing enough to claim the attacker to be the closest neighbour in the network of those nodes (Wassim El-Hajj *et al*, 2011).

(4) Transport Layer: This layer transfers data between two end hosts. The two types of attack suffered include lion attack, where PUEA is launched by the attacker to force the CR nodes to undergo frequency hopping among the channels so as to disturb TCP; jellyfish attack, which affects the performance of the transport layer, mainly the TCP protocol, even though it is performed at the network layer (C.N.Mathur and K.P.Subbalakshmi, 2007).

(5) Application Layer: All the attacks corresponding to the previous four layers might have harmful effects on this layer (Deepa Das and Sushmita Das, 2013).

Table 1: Various attacks on the protocol stack

Protocol Layer	**Attacks**
Physical Layer	PUEA; OFA; CCDA; Jamming
Link Layer	SSDF; SCN; Control channel saturation DoS
Network Layer	Sink Hole attack; Hello Flood attack
Transport Layer	Lion attack; Jellyfish attack
Application Layer	All the above attacks have various harmful effects on this layer

3. Primary User Emulation Attack (PUEA)

R. Chen *et al* presented a major potential threat to the cognitive radios in (R.Chen and J.M.Park, 2006). When the spectrum band is free from use by the primary user, a malicious attacker emulates the signal characteristics of the primary user and sends a jamming signal. Thus, the secondary/cognitive users assume that the spectrum is busy and they do not access the network (F.Bao *et al*, 2007). In PUE attacks, the malicious attacker transmits only in fallow bands. Therefore, the purpose of these attackers is not to interfere with the PUs but to immune the spectrum resources that the SUs could have used (R.Chen *et al*, 2008).

A. Primary Exclusive Region (PER)

It is one of the deployment schemes in which the primary receivers are shielded. The secondary network should be dispersed outside the PER. This zone is also known as keep-out region and gives a protection area to the primary

receiver. In this way, a certain distance is imposed between the primary and secondary users, thus, interference between the two is reduced. The cognitive users do not have the permission to transmit within this region. Such a scheme is appropriate for a broadcast network, where a primary transmitter communicates with multiple primary receivers. For example, TV networks downlink in the cellular network, etc. Outside the PER, the SUs are uniformly and randomly distributed over a network radius from the primary transmitter outside the PER (M.Saxena *et al*, 2013).

B. Classifications of Attackers

After identifying the security problem stimulated by PUEA, different types of attacks have been studied. Here are the following types of classifications of these attacks (R.Yu *et al*, 2013):

- *Selfish and Malicious Attackers:* The *selfish* attackers steal bandwidth from legitimate secondary users for its own transmissions. After monitoring the spectrum and discovering it unoccupied, the attacker competes with the SUs by emulating the PU. While on the other hand, a *malicious* attacker disturbs the dynamic spectrum access of the legitimate secondary users rather than exploiting the spectrum for its own transmissions. Unlike the selfish attacker, it emulates the primary signal in both the unoccupied spectrum band and the band currently being used by the SUs. However, in this way, it might be possible that a SU might fail to discover the attacker and cause interference.
- *Power-Fixed and Power-Adaptive Attackers:* It is important for PUE attackers to emulate power levels since most of the secondary users deploy an energy detection technique while sensing the spectrum. A power-fixed attacker attacks using a predefined invariable power level which is not dependent on the power of the PUs. Comparatively, a power-adaptive attacker is smarter as it can adjust its transmitting power accordingly with the change in the transmitting power of the primary user (Z.Chen *et al*, 2009). Therefore, such an advance attack has the ability to defeat a plain defensive approach which only focuses on the power of the received signal.
- *Static and Mobile Attackers:* The location of a static attacker is fixed in all rounds of attacks. This location can be revealed using position techniques, for example, ToA (Time of Arrival) or dedicated positioning sensors (R.Chen *et al*, 2008). It can be easily recognized because of the difference between its location and that of the primary user. On the other hand, a mobile attacker makes it difficult to track and discover its location by constantly changing its position. Although, its existence can be verified by the use of variable detection approach that is proposed in (S.Chen *et al*, 2011), this scheme exploits the correlation between acoustic information and the RF signals.

C. Essential Conditions for Successful PUEA

There are several conditions for a successful PUE attack in the cognitive radio network. These conditions are as follows (R.Yu *et al*, 2013):

- *No PU-SU Interaction:* If the legitimate secondary users were allowed to exchange information with the primary users, a primary user verification process could be deployed to easily detect the PUEA.
- *Different characteristics of PU and SU signals:* The different characteristics include different signal statistical features and different modulation modes. The PUE attackers take advantage of a fundamental condition that the secondary user receiver designed is unable to decode and demodulate the primary signal. This way the attackers emulate the primary signal which the legitimate secondary user cannot recognize.
- *Channel measurement and Primary signal learning:* For the emulation of the primary signal, the attacker has to analyze the characteristics of the primary user. For a stronger attack, the attacker must learn estimate the channel conditions and the power levels also.
- *Avoiding interference with the primary network:* Not only is it a prime concern for the secondary users, but also a significant condition that all the PUE attackers must obey. The attackers, specifically the selfish attackers, should carefully examine the behaviours of primary users such that no extra interference is caused with the primary network.

D. Impact of PUEA on Cognitive Radio Networks

PUE attacks are the reason for a wide number of problems caused in a CR network (R.Yu *et al*, 2013). Underneath, is a list of potential effects of PUEA:

- *QoS Degradation:* The Quality-of-Service (QoS) can be degraded by the presence of PUE in a CRN. This is because of the discontinuity of the secondary services. For instance, an attacker could disrupt the ongoing services and force the secondary users to change their operating spectrum bands constantly. Frequent spectrum handoff will lead to jitter and unsatisfying delay (Z.Jin *et al*, 2012) for the secondary services.
- *Bandwidth waste:* The main aim of deploying CRNs is to address under utilization of the spectrum caused by the current fixed spectrum usage policy. The SUs can retrieve these by dynamically accessing the spectrum holes. However, these spectrum holes can be stolen by PUE attackers which will lead to spectrum bandwidth waste.
- *Connection Unreliability:* Under the PUE attack, when a real time secondary service is unable to find a channel available while performing the spectrum handoff, then the service has to be stopped. There is no guarantee of these services to have a stable radio resource die to its nature of dynamic spectrum access. The presence of PUE attacks greatly increases the unreliability of the connection of the CRN.
- *Interference with primary network:* Even though a PUE attacker steals the bandwidth from the SUs, it is possible that an additional interference is generated with the primary network. This case occurs when the attacker cannot detect the occurrence of a primary user. Now when the SUs tackle a PUE attack, there is a chance that

they erroneously identify the true primary user as the attacker and interfere with its network. This interference is strictly forbidden in cognitive radio networks.

- *Denial of Service:* Due to high frequency of PUE attacks, the SUs will not have sufficient bandwidth for their transmissions. It is also possible that the CRN might not find any channels to build a common control channel to deliver the control messages. As a result, the network will suspend and would not be able to serve any secondary user. This case is known as Denial-of-Service (DoS) in CRNs.

4. Various Defense Techniques against PUEA

It is important to prevent the PUE attacks in cognitive radio networks. Hence, the authenticity of the primary user signal must be verified by using various detection techniques. We now enlist various detection schemes used to mitigate PUEA along with their results and methods used in the contributions:

Fenton Approximation Method: (S.Anand *et al*, 2008) studied a fading wireless environment and used Fenton's Approximation method to derive expressions for successful PUEA probability. In order to provide a lower bound on the successful PUEA probability, Markov Inequality theorem was used. This analysis was extended in (S.Anand *et al*, 2008) to obtain the pdf (probability density function) of the received signal from the attacker. The simulations demonstrate that the proposed detection scheme rarely violates the spectrum evacuation etiquette. (Z.Jin *et al*, 2009) proposed a practical mechanism and an analytical model using Wald's Sequential Probability Ratio Test (WSPRT) to detect PUEA in CRNs. This test permits the user to set thresholds on the probability of missing the PU and the probability of successful PUE attack and thus can accustom a range of sensitivities.

Location Based Method: Among the various existing location schemes for wireless networks (N.Patwari *et al*, 2005), Time Difference of Arrival (TDoA) and Received Signal Strength (RSS) appears to be the most appropriate methods for detecting PUEA. RSS based technique is used to calculate the distance between the reference node and the source by assuming that the path loss model and transmission power are known. Even though this technique is simple to implement in hardware and inexpensive (R.Chen and J.M.Park, 2006), it is exposed to high errors because of it dynamics of the outdoor/indoor environments. This technique is not suitable for long range (kilometres) network links. Alternatively, TDoA is built on the difference between the times of arrival of a single signal at two distinct reference nodes. Because its measures are not dependent upon the transmitter's clock, TDoA can be used to locate asynchronous transmitters, which is the case of a PUE attacker. Although TDoA has considerably higher accuracy than RSS-based technique, a tight synchronization is requires between each pair of reference nodes. Also, the TDoA measurements are a little sensitive to multipath propagation (O.Leon *et al*, 2011).

Transmitter Verification Scheme: This scheme is used to distinguish between the transmitted signals from the primary user and the transmitted signals from the malicious user. This test comprises of three tests which have been contributed by (R.Chen and J.M.Park, 2006) and (R.Chen *et al*, 2008). The first test is the *Distance Difference Test* (DDT), which is dependent upon the relative phase difference of the received signals. It verifies the difference between the two distances of a primary user and a pair of location verifiers (LVs). The phase shift of the signal at the two LVs is used in measuring the difference in the distance. The second test is *Distance Ratio Test* (DRT), which uses the RSS (Received Signal Strength) of a signal source and is dependent upon a large scale propagation model since the possible fluctuations caused by small scale fading in RSS are not considered. The third test is *LocDef* (Localization based Defense), which uses both the location of the transmitter and the signal characteristics to verify the incumbent signal transmitters. It has the capability of detecting PUE attacks and can be incorporated into a spectrum sensing scheme to further detect PUEA under certain conditions.

Dogfight: (H.Li and Z.Han, 2011) have modelled a dogfight game between the attacker and the defending secondary user in the spectrum of a multichannel CR system. The game is played blind when the channel statistics such as the channel idle properties are not known to both the attacker and the defender. To fight the unknown channel statistics and the arbitrary strategies of the attacker, the defender assumes the unknown channel as a bandit arm and formulates a strategy of using the technique of adversarial multi-armed bandit. The test proposed in this scheme is the Nash equilibrium, in which the performance of anti-jamming is analyzed.

Sybil Attack: It is the most prevalent security threat in which a single malicious attacker masks multiple identities to attain various classes of attacks in secondary network (S.Bhattacharjee *et al*, 2013). (Y.Tan *et al*, 2011) has proposed a new technique where an attacker can launch PUE attack as well as Sybil based SSDF attack. Also a test-bed known as Spider Ratio test is used in which each radio comprises of two network interfaces: one for recording and receiving time stamps of beacon frames and the other for broadcast of WAN services. The investigation of issues such as allocation of Sybil interfaces for different attacks is carried out in the absence or presence of a reputation system. Both the malicious attackers and the secondary network have knowledge of candidate channels. There are two different interfaces of the malicious attacker: (a) Sybil attacker (SybA), in which the goal is to launch PUEA on candidate channels, and (b) Sybil Saboteur (SybS), in which the goal is to launch Sybil based SSDF attacks and influence spectrum decision at fusion centre.

Belief Propagation: This is an RSS based technique. (Z.Yuan *et al*, 2012) has proposed a defense mechanism based on BP (Belief Propagation) on location information to accurately identify the attacker. The exchange of messages takes place between each user and its neighbouring users in an iterative way using belief propagation. After convergence, the PUE attacker can be detected according to the mean of all final beliefs. If this mean is lower than the threshold value, then the suspect could be identified as a PUE attacker. Henceforth, a

broadcast message will be generated to inform all the secondary users about the characteristics of the attacker so that they can ignore the primary emulation signal of the attacker in future.

Primary User Authentication Scheme: (Meena Thanu, 2012) has stated that this is the best scheme to identify a genuine primary user. This technique is performed in the physical layer in two following ways: *Channel Impulse Response* or Link Signatures; and *Location estimation techniques*, in which received signal characteristics such as angle of arrival (AoA), received signal strength (RSS), time of arrival (ToA) and pattern matching with fingerprint are used.

Encryption and Displacement Method: To tackle the security issue of a CR network, the most important task is to differentiate between the malicious attacker and the primary user. The traditional encryption method to access the PU is very strict, but, extremely hard to defend the air interception attack. (X.Zhou *et al*, 2011) proposed an encryption and displacement method to solve the air interception problem in a better way. The simulation is carried out by NS2 software.

Robust Spectrum Decision Protocol: (Z.Jin *et al*, 2010) proposed an RSDP scheme for DSA networks against PUE attacks with centralized controller. This method makes the final spectrum decision for the complete network by using individual sensing results of the SUs. This spectrum decision can be obtained by characterizing the power received at good SU through a flexible log normal sum approximation technique. RSDP is resilient to PUE attacks and the probability of successful PUEA is significantly reduced in the presence of Byzantine attacks, while it is still adapting the spectrum evacuation etiquette.

MME: (Y.Zeng and Y.C.Liang, 2007) have proposed a method based on minimum and maximum eigen values of the sample covariance matrix of the signal received. It has been demonstrated that the ratio of the maximum eigen value to the minimum eigen value is used to detect the existence of the signal. This ratio can be quantized to find the threshold by the use of some latest random matrix theories (RMT). These theories also help in determining the probability of false alarm. This method can detect various signal applications without the knowledge of the channel, the signal and the noise power. This technique overcomes the noise uncertainty.

LCM and SCS: (S.Lio *et al*, 2012) has proposed two schemes for a fixed and a movable transmitter. In the case of a mobile transmitter, the property of log-scale path loss increasing linearly with the log-distance is exploited. A Linearity Check for Mobile transmitters (LCM) technique is then used in which the unauthorized transmitters are detected through a graph between dB energy vs. log-distance. In the case of a stationary transmitter, a notion of signal-prints is used, i.e. spatial pattern of received signal strength (RSS). Signal-print Check for Stationary transmitters (SCS) is then used in which the unauthorized transmitters are detected by the comparison of a current pattern of the authorized transmitter with that of a stored one.

Applying Artificial Neural Networks: (D.Pu *et al*, 2011) proposed a PUE detection approach which combined the cyclostationary feature calculation, energy detection and artificial neural networks (ANNs). Following are the advantages of the proposed scheme: (i) No special software, hardware or additional nodes needed to operate; (ii) can verify mobile transmitters with unknown coordinates; and (iii) robustness in the presence of fast processing and noise.

Hypothesis Testing: Since the DDT and DRT failed to take fading wireless networks in account while detecting PUEA, (Z.Jin *et al*, 2009) thus proposed a technique called Neyman-Pearson Composite Hypothesis Test (NPCHT) to especially detect PUEA in fading wireless environments. This test allows the SU to keep the value of the probability of missing the PU around a given threshold and at the same time it tries to reduce the probability of successful PUEA to a minimum level.

Game Theoretic Approach: (Y.Tan *et al*, 2009) proposed a game theoretic approach in which the secondary user attempts to use the free spectrum band with no interference with the incumbent user, whereas the malicious attacker tries to gain the monopoly of the bandwidth available by forcing the secondary user out. It is assumed that both the MA and the SU are unaware of the arrival schedule of the PU, and a mixed strategy for each one is derived to achieve Nash equilibrium. This system accomplishes better robustness to errors while estimating the state of PU.

Specific Primary User Sensing: (Z.Luo *et al*, 2011) proposed a scheme based on RF fingerprinting, caused by a complex difference between the hardware of the attacker and PU, known as Specific primary user sensing (SPUS). This scheme comprises of Analog to Digital Converter (ADC), Digital Down Converter (DDC), RF front-end, Fast & Fine sensing module and SPUS module. The SPUS module again comprises of noise adder, primary user database, pilot & symbol rate estimator and Support Vector Data Description (SVDD).

Cooperative Spectrum Sensing: In order to maximize the probability of detection of PU with the presence of PUE attack, (C.Chen *et al*, 2011) used the channel information between the MA & SU and PU & SU. This was done to derive optimal weights so that the probability of detection of the PU is optimized under the pressure of a required false alarm probability. In essence, to eliminate the malicious attacker signal, this technique takes advantages of a set of cooperative sensors. The simulation results demonstrate that this optimal combining scheme improves the detection performance.

Variance Detection: (Z.Chen *et al*, 2009) proposed a variance detection technique which has a much better performance than the learning methods, for example, mean-field approach and the estimation techniques, for example, maximum likelihood estimation that can be exploited by both the defender and the attacker. The channel parameters are different because the signals from the attacker and the primary user go through different channels. These parameters can be undertaken as the signatures of the attacker and the primary user. Therefore, these channel parameters are estimated in order to detect advanced PUE attack.

Hearing is Believing: (S.Chen *et al*, 2011) proposed this

Table 2: Comparison of different defense techniques

Defense Technique	Contributions	Tests/ Models used	Key Features/ Advantages/ Disadvantage
Fenton's Approximation	(S.Anand *et al*, 2008; Z.Jin *et al*, 2009)	Markov's Inequality, WSPRT	Fading wireless networks, rarely violates spectrum evacuation technique
Location Based	(R.Chen and J.M.Park, 2006; N.Patwari *et al*, 2005; O.Leon *et al*, 2011)	TDoA, RSS	TDoA-high accuracy, sensitive to multipath propagation, RSS-inexpensive, hardware implementation simple, high errors, not suitable for long range
Transmitter Verification	(R.Chen *et al*, 2008; R.Chen and J.M.Park, 2006)	DDT, DRT, LocDef	DRT-based on large scale propagation model; DDT-measures difference in distance LocDef-uses both signal transmitter and location
Dogfight	(H.Li and Z.Han, 2011)	Nash Equilibrium	Unknown channel characteristics, adapts passive way, no collaboration among SUs, collisions can occur
Sybil Attack	(S.Bhattacharjee *et al*, 2013; Y.Tan *et al*, 2011)	Spider ratio test	Attacker mask multiple identity
Belief Propagation	(Z.Yuan *et al*, 2012)	RSS	High accuracy, exchange of messages between user and neighbour,
PU Authentication	(Meena Thanu, 2012)	Channel Impulse response	Best method to identify primary user, Location estimation technique used
Encryption and Displacement method	(X.Zhou *et al*, 2011)	NS-2 Simulation	Solves air interception problem
RSDP	(Z.Jin *et al*, 2010)	Log-Normal Sum Approximation	Resilient to PUEA, probability of successful PUEA significantly reduced in presence of SSDF
MME	(Y.Zeng and Y.C.Liang, 2007)	RMT	Ratio of max and min eigen values used, signal detected without the knowledge of channel characteristics, overcomes noise uncertainty
LCM & SCS	(S.Lio *et al*, 2012)	LCM; SCS	LCM-Mobile transmitter, SCS-Stationary transmitter
Applying ANN	(D.Pu *et al*, 2011)	NA	Combination of cyclostationary, energy detection and artificial neural networks, No special hardware/software required, robustness in the presence of noise
Hypothesis Testing	(Z.Jin *et al*, 2009)	NPCHT	Fading wireless environment, probability of missing PU at threshold, min probability of successful PUEA
Game Theoretic Approach	(Y.Tan *et al*, 2009)	Nash Equilibrium	Better robustness to errors
SPUS	(Z.Luo *et al*, 2011)	Pilot Estimator; Symbol Rate Estimator	Based on RF fingerprinting, module contains SVDD
Cooperative Spectrum Sensing	(C.Chen *et al*, 2011)	Optimal Combining Scheme	Optimize detection probability of PU, set of cooperative sensors used
Variance Detection	(Z.Chen *et al*, 2009)	Naïve Detection	Better performance than mean field approach and max likelihood estimation, different channel parameters used
Hearing is Believing	(S.Chen *et al*, 2011)	NA	No complex hardware, acoustic sensor equipped in beacon
Hybrid PUEA Defense	(F.Bao *et al*, 2012)	Energy Detection, Variance Detection	Better performance, high probability, low resource consumption
Cross Layer Approach	(C.Sorrells *et al*, 2011)	SA-SMR	Based on Dynamic Source Routing, constructs maximum disjoint paths
DECLOACK	(N.T.Nguyen *et al*, 2012)	Dirchlet Distribution, FGMM, IGMM	Based on non-parametric Bayesian approach, no modification of the PU hardware required
IRIS	(A.W.Min *et al*, 2011)	NA	Checks consistency, high attack tolerance, small communication and computation overheads

method in It does not require any complex hardware. An acoustic sensor is equipped in each secondary user. A disabling beacon protocol has been used for detection of wireless microphone emulation attacks. In this protocol, a specially designed signal is transmitted before starting wireless microphones. This method can help SUs to differentiate between attackers and genuine wireless microphones when additional information such as signatures is embedded into the beacon. The correlation between the acoustic signal and the RF signal are exploited to cite differences between the genuine wireless microphones and attackers.

Hybrid PUEA Defense: (F.Bao *et al*, 2012) proposed a hybrid defense strategy, in which the target region has two sub-divisions. In the first part, the chosen defense mechanism is based on variance detection. In the second part, the chosen defense mechanism is based on energy detection. This hybrid technique achieves better performance by using variations in characters. This technique can defense PUE attacks successfully with high probability and low consumption of resources.

Cross Layer Approach: (C.Sorrells *et al*, 2011) has used SA-SMR (Spectrum Aware-Split Multipath Routing) as a base line routing for evaluating performance. This routing protocol has high demand and it constructs maximally disjoint path which provides much needed back up paths in cognitive radio ad hoc networks where the activities of primary user may constantly disturb secondary user traffic. It is based on Dynamic Source Routing (DSR) but uses another packet forwarding technique. DSR discards duplicate RREQ (routing request), whereas SMR permits intermediate nodes to pass on certain duplicate RREQ so that it can discover more disjoint paths.

DECLOAK: (N.T.Nguyen *et al*, 2012) proposed this non-parametric Bayesian approach for detecting PUEA. It exploits the infinite Gaussian mixture model, a collapsed

Gibbs sampling method and the OFDM signal features for classification. The simulation results show that DECLOAK significantly outperformed the Mean shift based clustering method, a baseline method and approached an upper bound performance. Although its nature is unsupervised, it is still desirable in practice. This scheme requires no modification of the primary user hardware and no training data.

IRIS: (A.W.Min *et al*, 2011) proposes this scheme called IRIS (robust cooperative sensing via iterative state estimation). This scheme checks the consistency among the sensing reports, through which it accurately detects the abnormal reports and removes them. Thus, impact of attacks is greatly reduced. IRIS has a high tolerance of attacks even under extremely challenging scenarios. It incurs only a small communication and computation overheads.

We compare these defense techniques in a tabular form in the Table 2.

Conclusion

It is certain that Cognitive Radio is the next generation in wireless network technology. In the near future, it would attract a lot of users because of its reliable nature. But then again it is still a wireless network, which means it will attract many potential security threats because a malicious attacker present may wish to gain monopoly of the complete communication network for its own selfish needs. Among these security threats, we have discussed the major security threat, i.e. PUEA in this paper. Along with this, we have enlisted out various defense mechanisms to detect the PUE attack by differentiating between the primary user and the malicious attacker. 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.

References

Y.Liang, Y.Zeng, E.Peh and A.Hoang (2008), Sensing throughput trade off for cognitive radio networks, *IEEE Transactions on Wireless Communications,* 7(4), pp. 1326-1337,

A.Fragkiadakis, E.Tragos and I.Askoxylakis (2012), A survey on security threats and detection techniques in cognitive radio networks, *IEEE Communications Surveys and Tutorials,* 15 (1), pp. 428-445,

Joseph Mitola III (1999), Cognitive Radio for flexible mobile multimedia communications, *Proc IEEE International Workshop on Mobile Multimedia Communications (MoMuC),* pp. 03-10,

Joseph Mitola III and Gerald Q. Maguire Jr. (1999), Cognitive Radio: Making software radios more personal, *IEEE Personal Communications,* 6 (4), pp. 13-18

Simon Haykin (2005), Cognitive Radio: Brain-empowered Wireless Communications, *IEEE Journal on Selected Areas in Communications,* 23 (2), pp. 201-220

Yenumula B. Reddy (2013), Security Issues and Threats in Cognitive Radio Networks, *AICT: The Ninth Advanced International Conference on Telecommunications,* pp. 85-90

C.Cordeiro, K.Challpali, D.Birru, and S.Shankar (2006), IEEE 802.22: An introduction to the first wireless standard based on cognitive radios, *Journal of Communications,* 1, pp. 38-47

C.Stevenson, G.Chouinard, W.Hu, S.Shellhammer, and W.Caldwell (2009), IEEE 802.22: The first cognitive radio wireless regional area network standard, *IEEE Communications Magazine,* 47, pp. 130-138

I.F.Akyildiz, W.Y.Lee, M.C.Vuran, and S. Mohanty (2006), Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey, *Computer Networks Journal (Elsevier),* 50, pp. 2127-2159,

Tevfik Yucek and Hüseyin Arslan (2009), A survey of spectrum sensing algorithms for cognitive radio applications, *IEEE Communication Surveys and Tutorials,* 11 (1), pp. 116-130

A.Attar, H.Tang, A.V.Vasilakos, F.R.Yu, and V.C.M.Leung (2012), A survey of security challenges in cognitive radio networks: Solutions and future research directions, *Proceedings of the IEEE,* 100 (12), pp. 3172-3186

Wassim El-Hajj, Haider Safa, and Mohsen Guizani (2011), Survey of Security issues in Cognitive Radio Network, *Journal of Internet technology,* 12 (2), pp. 181-198

Deepa Das and Sushmita Das (2013), Primary User Emulation Attack in Cognitive Radio Networks: A Survey, *IRACST-International Journal of Computer Networks and Wireless Communications,* 3 (3),pp. 312-318

Ruiliang Chen and Jung-Min Park (2006), Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks, *Networking Technologies for Software Defined Radio Networks, SDR'06, 1st IEEE Workshop,* pp.110-119

C.N.Mathur and K.P.Subbalakshmi (2007), Security issues in cognitive radio networks, *Cognitive Radio Networks; John Wiley and Sons, Ltd,* [chapter 11]

F.Bao, H.Chen and L.Xie (2012), Analysis of primary user emulation attack with motional secondary users in cognitive radio networks, *Personal Indoor and Mobile Radio Communications (PIMRC), IEEE 23rd International Symposium,* pp.956-961

R.Chen, J.M.Park and J.H.Reed (2008), Defense against primary user emulation attacks in cognitive radio networks, *IEEE Journal: Selected Areas of Communication,* 26 (1), pp. 25-37

M.Saxena, K.Chourasia and V.D.Bondre (2013), Analysis & Implementation of PUEA in Cognitive Radio Network, *International Journal of Advanced and Innovative Research,* 2(9), pp. 299-303

R.Yu, Y.Zhang, Y.Liu, S.Gjessing and M.Guizani (2013), Securing Cognitive Radio Networks against Primary User Emulation Attacks, *Cornell University Library, online: hhtp://arxiv.org/abs/1308.6216v1*

Z. Chen, T.Cooklev, C.Chen, and C.P.Raez (2009), Modelling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks, *Proc. Performance Computing and Communications Conference, IEEE 28th International,* pp. 208-2015,

S.Chen, K.Zeng, and P.Mohapatra (2011), Hearing is Believing: detecting mobile primary user emulation attack in white space, *Proceedings IEEE, INFOCOM,* pp. 36-40

Z.Jin, S.Anand, and K.P.Subbalakshmi (2012), Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks, *IEEE Transactions on Communications,* 6 (9), pp. 2635-2643

S.Anand, Z.Jin, and K.P.Subbalakshmi (2008), An analytical model for primary user emulation attacks in cognitive radio networks, *New Frontiers in Dynamic Spectrum Access Networks, 3rd IEEE Symposium,* pp. 01-06

Z.Jin, S.Anand, and K.P.Subbalakshmi (2009), Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks, *ICC'09 IEEE International Conference,* pp. 01-05

N.Patwari, J.Ash, S.Kyperountas, I.Hero, A.O.R.Moses, and N.Correal (2005), Locating the Nodes: Cooperative Localization in wireless sensor networks, *Signal Processing Magazine, IEEE,* 22 (4), pp. 54-69,

O.Leon, J.H.Serrano, and M.Soriano (2011), Robust Detection of Primary User Emulation Attacks in IEEE 802.22 Networks, *CogART 2011: 4th International Conference on Cognitive Radio and Advanced Spectrum Management*

R.Chen and J.M.Park (2006), Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks, *Networking Technologies for Software Defined Radio Networks, SDR'06, 1st IEEE Workshop*, pp. 110-119

H.Li and Z.Han (2011), Dogfight Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems-Part II: Unknown Channel Statistics, *Wireless Communications, IEEE Transactions*, 10 (1), pp. 274-283

S.Bhattacharjee, S.Sengupta, and M.Chatterjee (2013), Vulnerabilities in Cognitive Radio Networks: A survey, *Computer Communications*, 36 (13), pp.1387-1398

Y.Tan, K.Hong, S.Sengupta, and K.P. Subbalakshmi (2011), Using Sybil identities for primary user emulation and byzantine attacks in DSA networks, *Proceedings IEEE GLOBECOM*, pp. 01-05

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

Meena Thanu (2012), Detection of Primary User Emulation Attacks in Cognitive Radio Networks, *Collaboration Technologies and Systems (CTS), International Conference*, pp. 605-608

X,Zhou, Y.Xiao, and Y.Li (2011), Encryption and displacement based scheme of defense against primary user emulation attack, *Wireless, Mobile & Multimedia Networks, 4th IET International Conference*, pp. 44-49

Z.Jin, S.Anand, and K.P.Subbalakshmi (2010), Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks, *Global Telecommunications Conference (GLOBECOM) IEEE,* pp. 01-05

Y.Zeng, and Y.C.Liang (2007), Maximum-Minimum Eigenvalue Detection for Cognitive Radio, *18th Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications*, pp. 01-05

S.Lio, L.J.Greenstein, W.Trappe, and Y.Chen (2012), Detecting anomalous spectrum usage in dynamic spectrum access networks, *Ad Hoc Networks*, 10 (5), pp. 831-844

D.Pu, Y.Shi, A.V.Ilyashenko, A.M.Wyglinski (2011), Detecting Primary User Emulation Attack in Cognitive Radio Networks, *Global Telecommunications Conference (GLOBECOM) IEEE,* pp. 01-05

Z.Jin, S.Anand, and K.P.Subbalakshmi (2009), Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing, *Mobile Computing and Communications Review*, 13 (2), pp. 74-85

Y.Tan, S.Sengupta, and K.P.Subbalakshmi (2012), Primary User Emulation Attack in dynamic spectrum access networks: A game theoretic approach, *Communications, IET*, 6 (8), pp. 964-973

Z.Luo, C.Luo, S.Chen, S.Zheng, and S.Li (2011), Specific primary user sensing for wireless security in IEEE 802.22 network, *Communications and Information Technologies, 11th International Symposium*, pp. 18-22

C.Chen, H.Cheng, and Y.D.Yao (2011), Cooperative Spectrum Sensing in Cognitive Radio Networks in the presence of Primary User Emulation Attack, *IEEE Transactions on Wireless Communications*, 10 (7), pp. 2135-2141

Z.Chen, T.Cooklec, C.Chen, and C.P.Raez (2009), Modelling primary user emulation attacks and defences in cognitive radio networks, *International Performance Computing and Communications Conference, IEEE 28th International*, pp. 208-215

F.Bao, H.Chen, and L.Xie (2012), Analysis of primary user emulation attack with motional secondary users in cognitive radio networks, *Personal Indoor and Mobile Communications, 23rrd IEEE International Symposium*, pp. 956-961

C.Sorrells, P.Portier, L.Qian, and X.Li (2011), Anomalous spectrum usage attack detection in cognitive radio wireless networks, *Technologies for Homeland Security, IEEE International Conference* pp. 384-389

N.T.Nguyen, R.Zheng, and Z.Han (2012), On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification, *Signal Processing, IEEE Transactions*, 60 (3), pp. 1432-1445

A.W.Min, K.K.Han, and K.G. Shin (2011), Robust cooperative sensing via state estimation in cognitive radio networks, *New Frontiers in Dynamic Spectrum Access Networks, IEEE Symposium*, pp. 185-196