International Journal of Students' Research in Technology & Management
Vol 3 (6), June-August 2015, ISSN 2321-2543, pg 389-395

A SURVEY OF IMPLEMENTATION OF OPPORTUNISTIC SPECTRUM ACCESS ATTACK WITH ITS PREVENTIVE SENSING PROTOCOLS IN COGNITIVE RADIO NETWORKS

Monisha Ravi [#1], Nisha Ravi [*2], Dr. N. Ravi[^3]

[#]*Department of Electronics and Communication Engineering, RMD Engineering College*
[*]*Department of Electrical and Electronics Engineering, RMD Engineering College*
[^]*Advisor and Mentor, EPI*
[1]moni.ravi@gmail.com, [2]nish.nisharavi@gmail.com, [3]drnriitmas@gmail.com

DOI: 10.18510/ijsrtm.2015.362
Article History: Received 20th Feb 2015, Revised on 05th April 2015, Published on 20th September 2015

***Abstract*—Recently, the expansive growth of wireless services, regulated by governmental agencies assigning spectrum to licensed users, has led to a shortage of radio spectrum. Since the FCC (Federal Communications Commissions) approved unlicensed users to access the unused channels of the reserved spectrum, new research areas seeped in, to develop Cognitive Radio Networks (CRN), in order to improve spectrum efficiency and to exploit this feature by enabling secondary users to gain from the spectrum in an opportunistic manner via optimally distributed traffic demands over the spectrum, so as to reduce the risk for monetary loss, from the unused channels. However, Cognitive Radio Networks become vulnerable to various classes of threats that decrease the bandwidth and spectrum usage efficiency. Hence, this survey deals with defining and demonstrating framework of one such attack called the Primary User Emulation Attack and suggests preventive Sensing Protocols to counteract the same. It presents a scenario of the attack and its prevention using Network Simulator-2 for the attack performances and gives an outlook on the various techniques defined to curb the anomaly.**

Keywords----primary user emulation, primary user, sensing technique, network simulator, effective spectrum usage, secondary users, malicious users

I. INTRODUCTION

Wireless networks have involved a lot of interest in the research area due to their potential applicability in innumerable real-world practical applications. However, due to the distributed nature and their usage in critical applications without human interventions, sensitivity and criticality of data communicated, these networks are highly vulnerable to security and/or privacy threats that can unfavorably affect their performance. These issues become further critical in cognitive networks in which the nodes have the capabilities of changing their transmission and reception parameters according to the radio environment under which they operate, in order to achieve reliable and efficient communication and optimum utilization of the network resources.

The increasing demand for spectrum in wireless communication has made efficient spectrum utilization a big challenge. To address this important requirement, Cognitive Radio (CR) technology has evolved as the answer. A CR is an intelligent wireless communication system that is aware of its surrounding environment, and adapts its internal parameters to achieve reliable and efficient communication and optimum utilization of the resources [1]. The cognitive technique is the process of knowing through perception, planning, reasoning, acting, and continuously updating and upgrading with a history of learning [4]. It has the ability to know the unutilized spectrum in a license and unlicensed spectrum band, and utilize the unused spectrum opportunistically. The incumbents or primary users (PU) have the right to use the spectrum anytime, whereas secondary users (SU) can utilize the spectrum only when the PU is not using it. Each country has its own spectrum regulation rules. A certain band available in one country might not be available in another. Traditional wireless networks with a preset working frequency might not work in cases where the manufactured wireless nodes are deployed in different regions. On the other hand, if nodes are equipped with cognitive radio capability, they can overcome the spectrum incompatibility problem by changing their communication frequency band. Therefore, CR wireless devices have the potential to be operated almost anywhere in the world [4].

Design of a CR network poses many new technical challenges in protocol design, power efficiency, spectrum management, spectrum detection, environment awareness, novel distributed algorithms design for decision making, distributed spectrum measurements, quality of service (QoS) guarantees, and security [1]. In CNs, the cognitive engine in a sensor node has many radio parameters under its control. The cognitive engine determines the suitable values of these parameters over time in order to optimize its multi-goal objective functions. Various attacks are possible on the learning algorithms of the cognitive engines so that these algorithms produce suboptimal outputs [1]. Since these attacks are targeted on the learning algorithms, they are also known as the belief- manipulation attacks. The cognitive radio may have three goals such as achieving low-transmit power, high rate of transmission, and high security in communication. Based on the application currently under use, the cognitive engine assigns different weights to these three goals to maximize its overall objective function. An attacker can compromise a user by breaking the Dynamic Spectrum Access (DSA) mechanism by implementing spectrum misuse or by exhibiting selfish behavior [1]. For example, the attacker node can transmit in an unassigned band or it can ignore the cognitive messages sent by the

other users in the network. Hence identification of various possible attacks on CNs is critical in order to design appropriate security schemes to defend against those attacks.

A well-known malicious attack is the primary user emulation attack (PUEA). In PUEA, malicious users mimic the primary signal over the idle frequency band(s) such that the authorized secondary users cannot use the corresponding white space(s) [6]. This leads to low spectrum utilization and inefficient cognitive network operation. The PUE attack means that an attacker sends out primary-user-alike signals during the spectrum sensing period of secondary users, thus "scaring away" the secondary users since they are unable to distinguish the signals from primary users and the attacker [2]. The goal of the adversary is to mislead the SUs regarding the available spectrum opportunities, thus preventing them from utilizing idle channels [5]. This attack is particularly easy to launch in CRNs due to the highly flexible and software-based air interfaces of CR nodes. The PUE attack can be catastrophic, since it severely interferes with spectrum sensing process.

II. DESIGN

The steps for development of an attack can be (shown in Fig.1):

1. Consider two wireless networks.
2. Users check the availability of channel in one of the two networks.
3. Secondary users sense the channel according to the channel availability.
4. SUs check for free/available channel (i.e. unlicensed channel).
5. The band width may be limited to access maximum number of users.
6. The attackers will be formed.
7. The attacker emits signal similar to the Primary user's signal.
8. Secondary users will be informed that there are no unused channels.
9. Secondary users won't get access from any access point.

The conditions that would lead to effective PUE attacks are: little or no PU-SU interaction, different signal characteristics of PU and SU signals, primary signal learning and channel measurement and avoiding interference with primary network [7]. Some potential consequences of PUE attack are Bandwidth wastage, QoS degradation, connection unreliability, Denial of Service and interference with primary network [7]. Mitigating such a threat would allow high global operability and hence, can become an effective solution for rapid deployment of mobile users during rescue missions, disaster relief operations and emergencies, like the 9/11 attack on the twin towers in the US.

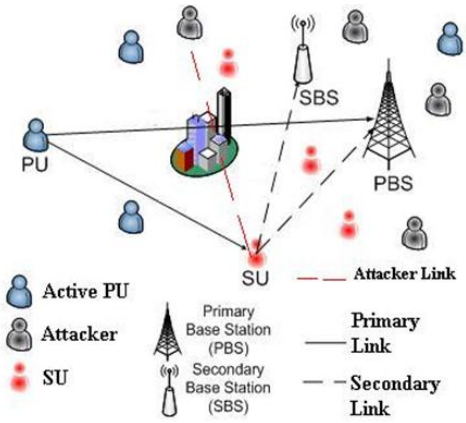

Fig. 1 Attacker illustration

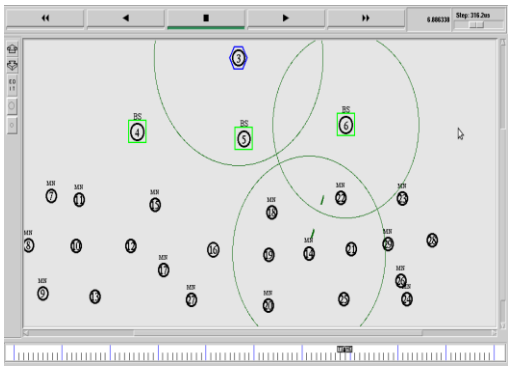

Fig. 2 SUs sensing for channels among 2 networks before attack formation

To mitigate the effectiveness of such an attack, cognitive radios should [9]:

- Always assume sensory input statistics are "noisy" and subject to manipulation;
- Be programmed with some amount of "common sense" to attempt to validate learned beliefs;
- Compare and validate learned beliefs with other devices on the network;
- Expire learned beliefs to prevent long-term effects of attackers; and
- Attempt to perform learning in known-good environments

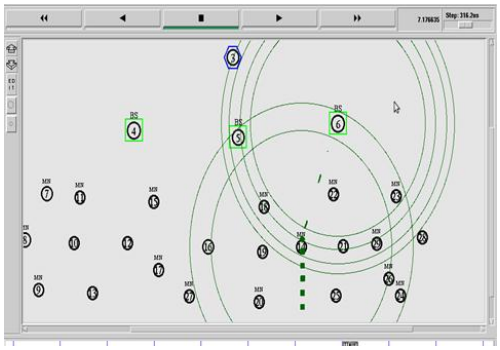

Fig. 3 Representing the PUEA

Node 14 in Fig. 3 tries to sense for any available channel by requesting the base station of WLAN network (shown in green). Since it does not avail any channel for transmission, due to the malicious node, it experiences packet loss.

III. Methodologies And Techniques

A. *Robust PUE Detection method*

This algorithm, as stated in [8], analyzes the effect of forged reports on the location process of a given emitter and provides a set of countermeasures in order to make it robust to undesired behaviors or false feedback.

It has considered Least Square (LS) methods over a linearized set of TDoA (Time Difference of Arrival) error equations (by means, for example, of Taylor-Series Estimations) for stationary networks such as CRNs. LS estimation methods are iterative schemes that start with a rough initial guess (xv; yv; zv) and improve the guess at each step (xv + δx; yv + δy; zv + δz) by determining the local linear least-sum squared-error correction (δx; δy; δz). The target is to iterate the method until the components of the correction are below a given threshold, that is to say, that the estimation converges.

B. *The algorithm*

1. Obtain a linear estimation of the measurement errors.

According to this, given a set of n TDoA measurements r_i taken by the pairs made up of the BS and each one of the CRs, the measurement errors assuming a prediction (x_v; y_v; z_v) can be expressed as in (2), with $f_i(x; y; z)$ as in (1) the real TDoA measurement for the pair BS and anchor node *i* for position (x; y; z)

$$f_i(x,y,z) = \frac{\sqrt{(x-x_i)^2+(y-y_i)^2+(z-z_i)^2}}{-\sqrt{x^2+y^2+z^2}} \quad (1)$$

$$\mathbf{e} = \begin{pmatrix} v_p\tau_1 - f_1(x_v,y_v,z_v) \\ v_p\tau_2 - f_2(x_v,y_v,z_v) \\ \vdots \\ v_p\tau_n - f_n(x_v,y_v,z_v) \end{pmatrix} \quad (2)$$

2. From the 1st-degree Taylor polynomial of **e**, the matrix representation of the linearized forms of the distance error can be expressed as in (3), with **A** an *n*-by-3 matrix with the Taylor coefficients and δ a 3-by-1 column vector with the corrections (δ_x; δ_y; δ_z).

$$\hat{\mathbf{e}} = \mathbf{A}\delta + \mathbf{e} \quad (3)$$

3. Assuming that ê is full rank, the value of δ that minimizes the sum of quadratic errors $\hat{e}^T\hat{e}$ can be computed as in (4).

$$\delta = -(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{e} \quad (4)$$

4. However, in the real world, measurements performed by different nodes are subjected to different errors and then their measures may contribute to the LS estimation with different weights. Moreover, measurement errors are often correlated. Consequently, localization methods, instead of the previous approach, often minimize $\hat{e}^T\mathbf{W}\hat{e}$, with **W** an *n*-by-*n* matrix with the assigned weights to every measure. In such case, the most common approach is to define $\mathbf{W} = \mathbf{R}^{-1}$ with **R** the matrix of covariances between measures. Therefore, the optimal δ can be derived as in (5).

$$\delta = -[\mathbf{A}^T\mathbf{W}\mathbf{A}]^{-1}\mathbf{A}^T\mathbf{W}\mathbf{e} \quad (5)$$

5. False reports provided by compromised nodes can severely undermine the location method, thus leading to false positives or negatives regarding the detection of primary users. Consequently, there is a need for identifying false measurements in order to discard them for the location process. This task could be accomplished by comparing measurements from different nodes and looking for large deviations.

However, measurements can considerably vary depending on the position of the CR within the CRN. Therefore, the most intuitive way would be to group nodes into clusters and compare measurements among nodes belonging to the same cluster. Usually, outlier measurements may be (badly) detected by means of LS fitting, but it is recommended to use Least Median Square (LMS) fitting instead. LMS aims to minimize the median of the residue squares as in (6) increasing its robustness to deviated measurements.

$$(x_v,y_v,z_v) = arg\,min\ [median_i\,(v_p\tau_i - f_i(x_v,y_v,z_v))] \quad (6)$$

6. However, the process of minimizing the median of the residue squares is prohibitive and then the final position estimation should be obtained with a mixed solution:

a. Divide the set of n CRs into c several clusters of equal size $s = \frac{n}{c}$

b. Apply the location process described separately in every cluster obtaining an estimation of the position of the emitter for each cluster (x_{v1}; y_{v1}; z_{v1})…. (x_{vj} ;y_{vj} ; z_{vj})….. (x_{vc}; y_{vc}; z_{vc})

c. Compute the median of residue squares for each cluster *j* as,
$$r^2_{cluster_j} = median(r_1^2 \ldots r_i^2 \ldots r_s^2) \quad (7)$$
wherer_i = $v_p r_i$- f_i (x_{vj} ; y_{vj} ; z_{vj}) is the residue for node *i* of cluster *j* and f_i (x_{vi} ; y_{vi}; z_{vi}) as in (1) is an "error-free" TDoA measure for the position estimation obtained by means of LS method for cluster *j*.

d. Select as tentative estimation (xv; yv; zv) the one given by the cluster with the lowest median of residues squares.

e. Compute the residue squares for all the n nodes considering the tentative estimation (xv; yv; zv)

f. Perform new position estimation by applying a LS method assigning a different weight to each node's measurement according to its residue square.

This is an implementation of Weighted Least Squares (WLS) method

Finally, as compromised nodes are likely to report false data repeatedly, a trust mechanism should be integrated into the system so as to keep track of node's behavior over time.

C. *RSSI based PU localization*

The algorithm given in [11], proposes a PU authentication system that securely and reliably delivers PU activity information to SUs. The direction of arrival (DOA) and the received power level are exploited jointly to obtain the transmitter's location and hence detect the malicious devices. That is, given the locations of the primary TV stations, the secondary user can distinguish the actual primary signal from the malicious user's signal by estimating the transmitter's DOA and the power level [6].

Received Signal Strength (RSS) based detection approach analyzes the PUE attack in the CR network without using any location information. Thus, this detection approach does not need dedicated sensor networks [7]. The PUE attackers

are assumed to be distributed randomly around the SUs. Hence, Received Signal Strength (RSS) seem to be the most suitable for detecting PUE attacks.

Location verification is achieved by using two techniques [3]:

1) Distance Ratio Test (DRT), which uses the received signal strength indicator (RSSI) of a signal source and

2) Distance Difference Test (DDT), which uses relative phase difference of the received signal as the signal is received at different receivers.

It is assumed that the location information of some of the CR nodes in the network is always known a priori either because these nodes are fixed or they use trusted GPS information. These CR nodes perform DRT and DDT operations within their coverage areas and also serve as the Location Verifiers (LVs). The LVs exchange the location information of incumbent transmitters through a cognitive pilot channel. This authentication approach is intended to prevent the PUE attack in CR networks.

With RSS-based techniques, assuming that the transmission power and the path loss model are known, it is possible to estimate the distance from the source to the reference node. When transmission power is not known, differences between RSS measured at pairs of receivers can be considered removing in this way the dependency on the actual transmit power. A set of at least three RSS measurements is then used to estimate the position of the emitter by applying trilateration [8]. Although RSS measurements are relatively inexpensive and simple to implement in hardware, they are susceptible of high errors due to the dynamics of indoor/outdoor environments mainly due to multipath signals and shadowing. Now, DRT uses a Received Signal Strength (RSS) based method, where two dedicated cognitive nodes measure the RSS of the signal source and calculate the ratio of these two RSSs to check whether it coincides with their distances to the true PU (e.g., a TV broadcast tower). Using DDT, the arrival time of the transmitted signal from the source is measured by the two dedicated cognitive nodes [7]. The product of the time difference and the light speed is then compared to the distance difference from the true PU to the two dedicated nodes in order to identify the source.

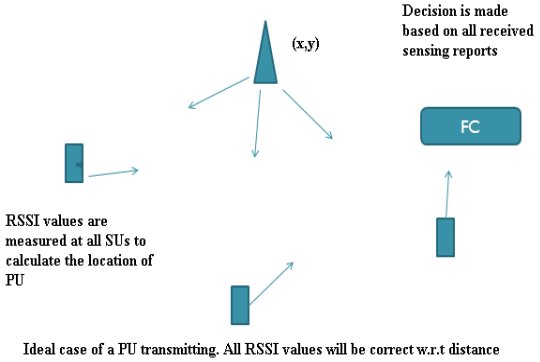

Fig. 4 RSSI

The model [11] uses localization schemes to estimate and authenticate the location of PU. The scheme is based on Received signal power. It is calculated as follows:

$$Pr = Pt + a\,10\,log\,(do/d) + w \quad (8)$$

Where,
Pr- Received signal power
Pt- Transmitted signal power
a- Constant
do- Reference distance
d- Calculated distance
w- Weight
FC- Fusion Centre

Certain assumptions taken with this regard are- All nodes must be loosely time synchronized, Location of PU should be fixed and known to all SUs, Fusion Center should be used to make decision about presence of PU, All SUs must be connected to FC using a secure link and There is should be no LOS (Line of Sight) path between every SU and PU.

But, this model fails all the localization based solutions for PUEA as the attacker can use a multi antenna array or MIMO technology with directional antennas to send PU-TX like signals to different SUs with various power levels faking the presence of PU. That is, a malicious user can be at a location where it has the same DOA and comparable power level as that of the actual primary transmitter.

D. Time of Emission Estimation

The assumptions taken for this algorithm, as stated in [11], are that the Secondary Users and Fusion Center must be loosely synchronized and must have a secure communication. The Fusion Center cannot be compromised as it knows locations of all users (secondary as well as primary) and has a good computational power and storage. The model proposes ways to eliminate the attacker based on certain calculations that are needed for the algorithm. But, attacker capabilities must also be kept in minds, as these can use antenna arrays, but transmitting with a beam formation at different locations at different times is restricted. Multiple Attackers can coordinate as the Attackers know location of all nodes which can ultimately lead to SU being compromised.

Now, the proposed approach must have Sensors that measure Time of Arrival (TOA), a Fusion Center which estimates Time of Emission (TOE) and must have Robustness against Multiple coordinated attackers, multiple compromised secondary users and Node with an Antenna Array. This algorithm has got its reach to every SU which receives PU like signals from the malicious nodes.

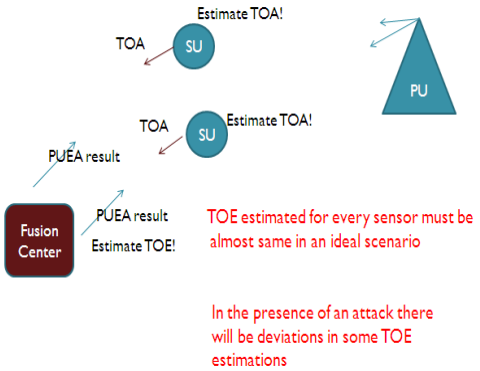

Fig. 5 Design

The algorithm

1. The Time Of Emission (TOE) must be measured for each node present in the network.

$$TOEi = TOAi - Dist/c + \xi \quad (9)$$

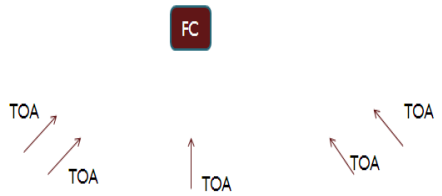

Fig. 6 Computation method

2. Get the mean value of all the computed Time Of Emissions from the nodes in the CRN.

$$COMPUTE\ MEAN \rightarrow TOEmean \quad (10)$$

3. After computing the mean of average of all the TOEs, find the deviation value for each node present in the network.

$$\delta i = TOEavg \sim TOEi \quad (11)$$

4. Then, compute the following parameters:
   I. Determine μ

   This is the maximum deviation in the measurement by a node under a non-attack scenario in the network.

   II. Determine k

   a) If the value is too small? Increase in false negative!

   b) If the value is too large? Increase in false alarm!

   c) Tradeoff is needed!
5. Then, the following conditions must be considered to find the scenario result
   If, δi >μ
   Then, Increment C
   Where,
   μ -> Maximum allowable deviation
   C -> number of deviated values
6. Also,
   If, C > k
   Then, PUEA- Primary User Emulation Attack has been formed or detected
   Where,
   k ---> Maximum no. of allowable deviated reports
   Note: A threshold is used to tolerate certain number of configured node compromises. But, if almost all nodes in network are compromised, then the network is not useful.
   In short,
   1. Access point checks the user location.
   2. Distance ratio is calculated where the user is located.
   3. Frequently, the beacon messages are sent to check the user access probability.
   4. Checks for the user probability ratio in order to detect the actual user available.
   5. Localization based transmitter verification takes place in access points.
   6. Channel identification and differentiation of the user's location would be done.
   7. This reduces the faked primary user count.

E. PUE Database Assisted Detector based on Action Recognition

This model, prescribed in [10], introduces a relational database system in order to overcome the problem of intensive computation. This approach records the feature vectors of primary users in the database system, then it monitors each user's FFT (Fast Fourier Transform) sequence and compares the unknown users' feature vectors with those in the database. PUs they have a limited number of feature vectors, which means the resulting database is stable and limited in size. In case that an unknown user's feature vector has a match entity in the database, this approach will continue to double check its action in the frequency domain using artificial neural network. Otherwise, this unknown user will be classified as a PUE.

The algorithm makes the following assumptions:(i) All the users, including the malicious users and primary users, are located within the same frequency band; (ii) Each user's transmission power is much higher than the ambient noise in the channel; (iii) The actions and the corresponding feature vectors of primary users are known, and they are different from the other users.

Two different experiments can be conducted in order to validate the performance of the database assisted classifier. The first experiment uses a computer simulation based on Simulink, while the second experiment is based on a hardware implementation using the Universal Software Radio Peripheral (USRP) Software-Defined Radio (SDR) platform.

In the Simulink experiment, the classification time is highly related to the number of primary users. When there are more primary users in the system, it costs more time to get the conclusion. However, it is noted that with a larger number of primary users, it is approximately a linear growth, because the classification time is dominated by the database searching time. Higher SNR (Signal-Noise Ratio) values yield better algorithm performance in terms of successfully classifying primary signals and PUE signals. It is very reliable and robust.

Now, in the SDR platform, the percentage of correct classification can be as high as 87.8%, which means that the majority of the classification results are correct, so the proposed algorithm possesses the potential to be a viable PUE detector operating under real world conditions. Hence, it is a good candidate for the real world implementation.

F. Intense Explore System Model

For novel Intense explore model [12], an infrastructure based network of CRs is considered, where multiple nodes (or Secondary Users, SUs) may be associated with a centralized fusion centre. For the sake of simplicity, existence of only one fusion centre is assumed. The fusion centre will collect the diagnose results from the cooperative secondary user in 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.

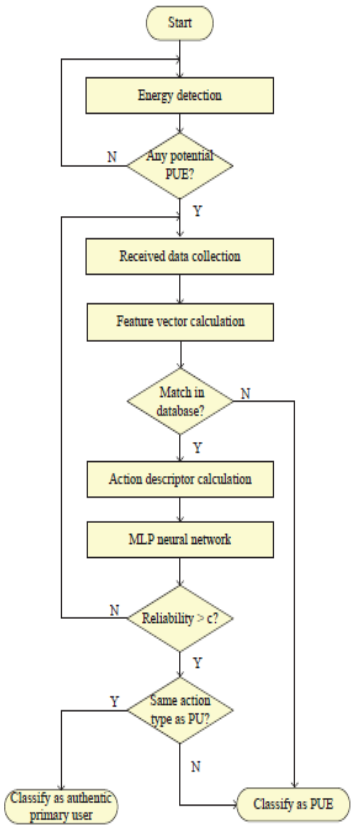

Fig. 7 Relational database with artificial neural network

In the Intense Explore algorithm, two sets of secondary users (SUs) such as At and Bt, are considered. The fusion center takes the decision about the suspected malicious user based on the reports from the At. Each users in At is assumed to be sensing their neighboring users in Bt. Assume that if any two SUs in At report the same sensing result about the same SU in Bt say Bj, whereby the energy level of it exceeds the threshold, then it is suspected to be the malicious SU. Thus the fusion center alerts all other SU about the suspected user as the malicious SU. The energy detection of Bj is done by a separate function specified as Energy detection. The energy detection function exploits spectral correlation property of cyclostationary feature for detecting the energy. This function reports At about the suspicious secondary user Bj, if any. This algorithm proactively identifies the suspected malicious Secondary user. The algorithm is robust and throughput loss along with detection latency can be minimized to for about 65%. The Intense Explore algorithm and Energy detection function is as follows:

Algorithm: Intense Explore

1) **Input:** *Set* of SUs
2) **Output:** *Decision* report from fusion center
3) **for each** slot t *do*
4) f ← Fusion *Center*
5) *At* ← Set of *cooperative* SUs
6) *Bt* ← *Neighboring* SUs of *At*
7) **for each** *Ai* in *At* do
8) Assume *Bt* as *neighboring* SUs of *Ai*
9) **for each** *Bj* in *Bt* do
10) //Call function for Energy detection of *Bj*
11) R(*Ai*,*Bj*)←*Energy* Detection (*Bj*)
12) **end for**
13) // Fusion *Center* Decision
14) for the same *Bj*
15) **if** (R(*Ai*, *Bj*) ← True) for all *Ai* **then**
16) *Bj* ← Suspected SU
17) f alerts all the SUs about *Bj*

Function: Energy Detection

1) **Input:** Bj
2) **Output:** SCF(Bj), the suspected malicious Su
3) Pi ← Threshold
4) Si ← Sensed Signal of Bj
5) **for** Si in Bj do
6) I ← Identify the autocorrelation function
7) C ← Fourier transform of autocorrelation function
8) SCF(Bj) ← Sensing result of Bj obtained from SCF generator
9) if (SCF(Bj) > Pi) then
10) SCF(Bj) ← True // Here Bj is suspected to be malicious user
11) return SCF(Bj)

G. Light weight IDS using CuSum

The conventional IDSs (Intrusion Detection System) usually follow either misuse or anomaly based attack detection methods. The misuse based detection method uses signatures of already known attacks. However, the misuse based approach cannot discover new types of attacks effectively[13]. On the other hand, as its name implies, the anomaly based detection methodology relies on finding the "anomaly", which represents an abnormal mode of operation in the system. However, many of the existing statistical detection techniques may not be adequate for designing an IDS for CRN as it presents a unique challenge. Specifically in CRN, a centralized IDS may not be able to detect a malicious attack and notify the secondary users quick enough, and therefore, it is important to facilitate lightweight yet effective IDSs in the secondary users themselves. It uses time-series Cumulative Sum (CuSum) hypothesis testing [13]. The reason behind choosing CuSum is due to its low complexity and overhead. Each secondary user is assumed to have an IDS. The IDS operates in two steps, namely learning or profiling phase and detection phase.

1. Learning phase-

To effectively detect anomalies due to various types of attacks, the IDS needs to be designed in such a manner that it may learn the normal behavior of protocol operation, traffic flow, primary user access time, packet delivery ratio (PDR), signal strength (SS), and so forth. The IDS may learn these information by constructing a statistical profile during normal CRN conditions or with acceptable (i.e., low) level of suspicious activities. The acquired information can facilitate the detection phase of the IDS to discover unknown intrusions or attacks against the targeted CRN.

2. Detection phase-

The proposed IDS detection phase relies on finding the point of change in the CRN operation as quickly as possible under an attack. Assume that the IDS operates over equal time-rounds, Δ_n (where n = 1, 2, 3,...). Let the mean of F_n

during the profiling period be represented by m. The idea is that the IDS continues to monitor a significant change in the value of m that can be considered as the influence of the attack. m remains close to one until an anomaly occurs. However, an assumption of the nonparametric CuSum algorithm suggests that the mean value of the random sequence should be negative during the normal conditions and becomes positive upon a change. Therefore, a new sequence $G_n=\beta-F_n$ is obtained where β is the average of the minimum/negative peak values of F_n during the profiling period. During an attack, the increase in the mean of G_n can be lower bounded by $h=(2\beta)$. Then, the CuSum sequence

Y_n is expressed as follows:

$$Y_n = (Y_{n-1} + G_n)^+; \quad Y_0 = 0 \tag{12}$$

Where $x^+=x$, if $x>0$; otherwise $x^+=0$.

A large value of Y_n strongly implies an anomaly. The detection threshold θ is computed as follows:

$$\theta = (m - \beta)t_{des} \tag{13}$$

where tdes denotes the desired detection time, which should be set to a small value for quickly detecting an anomaly.

At the detection phase, the IDS computes Yn over time. Yn remains close to zero as long as normal conditions prevail in the CRN. Upon an attack, Yn starts to increase. When Yn exceeds θ and as long as the SS measured at the secondary user is high, the IDS generates an alert of a possible attack. IDS will be able to detect the attack with low detection latency.

IV. CONCLUSION

In this paper, an overview of Primary User Emulation attack has been given, with its design strategy. In order to overcome this attack, found in Cognitive Radio Networks, a survey of some of the best techniques has been briefly specified. A gist of the methods is given in Table 1. Further work will be to develop prototypes of such methodologies.

REFERENCES

[1] Jaydip Sen, "Security and Privacy Challenges in Cognitive Wireless Sensor Networks", Book Chapter in Cognitive Radio Technology Applications for Wireless and Mobile Ad hoc Networks, Natarajan Meghanathan and Y. B. Reddy (Eds.), IGI-Global, USA, July 2013.

[2] Husheng Li and Zhu Han," Dogfight in Spectrum: Combating Primary User Emulation Attacks in CognitiveRadio Systems–Part II: Unknown Channel Statistics", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 1, January 2011.

[3] Sandip Dash, "Cognitive Wireless Sensor Network: Security and Privacy Challenges", NIST thesis, 2013.

[4] Gyanendra Prasad Joshi, Seung Yeob Nam and Sung Won Kim, "Cognitive Radio Wireless Sensor Networks: Applications, Challenges and Research Trends", Sensors 2013, 13, 11196-11228, 2013.

[5] Swathi Chandrashekar and Loukas Lazos, "A Primary User Authentication System for Mobile Cognitive Radio Networks", Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium, IEEE, 2010.

[6] Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, Tongtong Li, "Mitigating Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard", GLOBECOM2013-Signals Processing for Communications Symposium, IEEE, 2013.

[7] Rong Yu, Yan Zhang, Yi Liu, Stein Gjessing, Mohsen Guizani, "Securing Cognitive Radio Networks against Primary User Emulation Attacks", arXiv:1308.6216 [cs.ET], 2013.

[8] Olga León, Juan Hernández-Serrano, Miguel Soriano, "Robust Detection of Primary User Emulation Attacks in IEEE 802.22 Networks", CogART '11 Proceedings of the 4th International Conference on Cognitive Radio and Advanced Spectrum Management, ISBN: 978-1-4503-0912-7, Article No. 51, 2011.

[9] T. Charles Clancy, Nathan Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation", Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference, 2008.

[10] Pu, Di, "Primary User Emulation Detection in Cognitive Radio Networks", Diss. Worcester Polytechnic Institute, 2013.

[11] Natraj Jaganmohan, Sandeep A Rao, "Mitigation of Primary User Emulation Attack using Time of Emission Estimation", Advanced Network Security, NCSU Presentation.

[12] A.C.SUMATHI, Dr.R.VIDHYAPRIYA, "Intense Explore Algorithm – A Proactive way to eliminate PUE attacks in Cognitive Radio Networks", WSEAS Conference 2015, Advances in Information Science and Computer Engineering, ISBN: 978-1-61804-276-7,2015.

[13] Zubair Md. Fadlullah, Hiroki Nishiyama, Nei Kato, and Mostafa M. Fouda, "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks," IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, May-June 2013.

TABLE 1SUMMARY

Method	Description	Evaluation
Robust PUE Detection Method	Analyzes forged reports to remove false alarms using trust model in the end	Effective Performance
RSSI based PU localization	RSS based method to detect anomaly with or without using location information	Poor Performance
Time of Emission Estimation	TOA, Fusion Centre and Deviations based algorithm to distinguish PUs from malicious users	Effective Performance
PUE Database Assisted Detector based on Action Recognition	Uses a relationship database in order to simplify complex computations and feature vectors to find matching entities	Highly Effective Performance
Intense Explore System Model	Multiple nodes associated with a Fusion Centre and utilizes Energy Detection function	Effective Performance
Light weight IDS using CuSum	Time series CuSum series utilized, for its low complexity and advantageous for low latency	Highly Effective Performance