Primary User Emulation Attack in Cognitive Radio Networks: A Survey

Deepa Das
Department of Electrical Engineering
NIT, Rourkela, India
deepadas.ctc@gmail.com

Susmita Das
Department of Electrical Engineering
NIT, Rourkela, India
sdas@nitrkl.ac.in

Abstract— **Cognitive radio is a promising technology aiming to solve the spectrum scarcity problem by allocating the spectrum dynamically to unlicensed users. It uses the free spectrum bands which are not being used by the licensed users without causing interference to the incumbent transmission. So, spectrum sensing is the essential mechanism on which the entire communication depends. If the spectrum sensing result is violated, the entire networks activities will be disrupted. Primary User Emulation Attack (PUEA) is one of the major threats to the spectrum sensing, which decreases the spectrum access probability. In this paper, our objectives are to give the various security issues in cognitive radio networks and then to discuss the PUEA with the existing techniques to mitigate it.**

Keywords-cognitive radio; spectrum sensing; PUEA

I. INTRODUCTION

The rapid progress in wireless communication and a need for high data rate has increased the requirements of more spectrum. It has been found that, the licensed spectrum is not utilized to its full extent at all the time [1] due to inefficient fixed frequency allocation, whereas the cellular bands are overloaded. This has led the FCC to think about this underutilized spectrum and to allow the unlicensed users in licensed band, if they would not cause any interference to the licensed user. This initiative has focused on cognitive radio (CR) [2]. The main purpose of CR is to identify the unoccupied licensed spectrum for secondary usage without interfering with the primary user (PU), and with the awareness of the surrounding environment it can adapt its internal states with the corresponding changes in certain operating parameters such as transmit power, carrier frequency, modulation type etc. [3]. Due to these unique characteristics of CR and unreliable nature of wireless communication channel, cognitive radio networks (CRNs) acquire many research challenges, especially in aspects of security.

The special characteristics of CR networks give unique opportunities to the attackers, which introduce a new suite of threats targeting to damage the entire normal activities of the communication networks.

Organization of this paper is as follows: section II gives a brief overview of security issues in CRNs. Details of PUEA analysis is given in section III. In section IV, we give a framework of the existing defense techniques, and suggest some solutions for better performance. Finally, section V concludes the paper with our future work.

II. AN OVERVIEW OF SECURITY ISSUES

CR facilitates in secondary usage of licensed band by dynamically spectrum allocation manner. Therefore, secondary user (SU) must sense the spectrum accurately to avoid interference with the PU. With this, the CR management experiences different kinds of anomalous behavior from the other Access points (Aps) [4]. These are

- Misbehaving Access Point- It does not obey any rules for sensing, recognizing and managing the spectrum.
- Selfish AP- It occupies the channel for longer time to make profit to itself only.
- Cheat AP- It aims to increase its utility function by decreasing profit of other SUs.
- Malicious AP- It aims to vandalize the networks by falsely reporting the spectrum sensing results to SUs in order to cause interference between PU and SUs.

We first categorize the various attacks depending on their behavior shown towards the five layers of the protocol stack [5] as shown in Table 1.

The physical layer attack is classified as a primary user emulation attack (PUEA), where the malicious user(MU) mimics the primary user's signal characteristics, thereby causing SUs to erroneously identify the attacker as the primary user [9]; the objective function attack(OFA) is when the MU may try to change the parameters of utility resource, so that the CR node fails to adapt correctly [5]; jamming is when the jammer sends a continuous packet of data into the channel, making the SU to never sense the channel as idle [5]; common control data attack(CCDA) is a major risk which disrupts the transmission by preventing the elements of the channel from sharing information about the spectrum usage and also

provides all the information to the attacker i.e. required for spectrum sensing [5]. Link layer is responsible for data transferring from one node to another, and is suffered by mainly three types of attacks such as spectrum sensing data falsification (SSDF), which is also known as Byzantine attack, where the attacker falsifies the fusion center decision by sending wrong spectrum sensing result [5]; Control channel saturation Denial-of-service (DoS) attack is when the attacker saturates the control channel by reserving it [5]; selfish channel negotiation(SCN), where the malicious node provides wrong channel information, so that other nodes change their route. Then the network layer faces two types of attacks. These are sink hole attack and hello flood attack. In sink hole attack, the attacker advertises itself as the best route to a specific destination and lures the neighbor nodes to use this route and forward their packets so as to drop those packets [5]. Hello flood attack is when the attacker sends a broadcast message to all the nodes in a network with enough power to convince them that, it is the closest neighbor of those nodes [5]. Then the transport layer used for data transferring between two end hosts, is also suffered by lion attack and jellyfish attack.. In lion attack, the attacker launches PUEA and forces the CR nodes to perform frequency hopping among channels in order to disrupt TCP; jellyfish attack is performed on the network layer but it affects the performance of the transport layer, especially the TCP protocol [6]. The attack corresponding to all the layers may have an adverse effect on the application layer.

Table 1. Attacks on Protocol Stack

Protocol Layer	*Attacks*
Physical Layer	Jamming; PUEA; OFA; CCDA
Link Layer	SSDF; Control channel saturation DoS attack; SCN
Network Layer	Sink hole attack; hello flood attack
Transport Layer	Lion attack; jellyfish attack
Application Layer	Attacks corresponding to all the layers have an adverse effect on the application layer.

New type of attacks are then discussed, which violet the secondary user's location privacy by correlating CR reports and SUs' physical location [7].These are external CR report and location correlation attack, where the external attacker easily obtains the CR report of a specific sensing node by eavesdropping, and compromises its location privacy [7]; internal CR report and location correlation attack is when the malicious attacker(MA) participates as legitimate node and collects the sensing reports from other users so as to compromise any node's location privacy [7]; Internal differential CR report and location correlation attack is when MA estimates a specific node's sensing report by analyzing the aggregation result of the sensing reports, and infers its location information by comparing the aggregation result before and after the node joins or leaves the network [7].

The communication attack break-downs the communication process of CR nodes [8], and the overview of this attack is shown in Table 2.

Table 2. Communication Attack

Communication Attack	
Reply attack	
DoS Attack	Collision attack; ill-directing attack; flooding attack
Sybil Attack	

In communication attack, the MN disturbs the communication process of surrounding CR nodes [8]. This attack includes reply attack, Dos attack and Sybil attack. In reply attack, the messages are directed to other than the intended node or make delay to reach to the desired node [8]. Denial-of-service (DoS) attack is when the malicious node (MN) breakdowns the communication networks of other legitimate SUs [8]. Different kinds of DOS attacks are collision attack, in which the attacker simply violets the communication protocol to generate collision; ill-directing attack, where MN simply refuses to route message; and flooding attack, in which malicious node sends many connection requests to a susceptible node to render the node useless [8]. Sybil attack is when an attacker makes multiple identities to change the spectrum sensing information [8].

Physical layer is the lowest layer of the protocol stack and provides an interface to the communication medium. The CR is considered to be aware of any changes in its surroundings, adapts the physical layer parameters and accesses the spectrum dynamically, which make the operation more challenging. PUEA is one of the serious physical layer attacks and a great threat to spectrum sensing [9].

So, in the next section, the PUEA with its impact on wireless communication users are discussed and a detailed overview of PUEA defense techniques is given. This is the first paper to give a detailed discussion on PUEA along with its almost all existing mitigation techniques, and some proposed solutions.

III. PRIMARY USER EMULATION ATTACK (PUEA)

In the dynamic spectrum access environment, the PU always uses the authorized frequency band, and SUs can utilize this spectrum band when PU is not using it. In PUEA, the attacker generates fully similar type of signal as the PU to make an error in frequency band, and to confuse the SU. So that SUs erroneously identify the attacker as PU, and vacate the spectrum band immediately. This kind of attack is referred as PUEA [9].

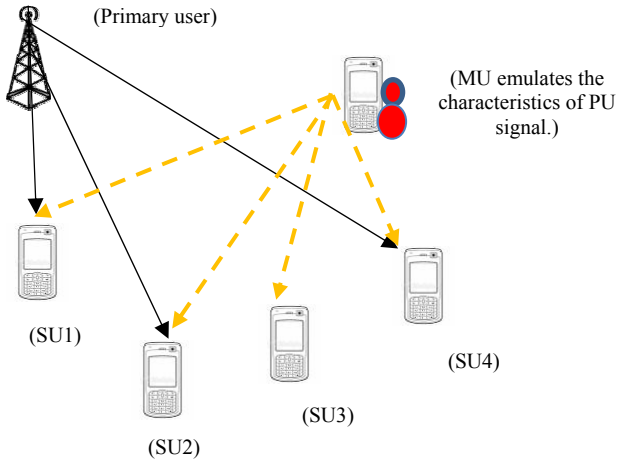

Fig. 1 Illustration of PUEA launching scenario

PUEA can produce serious interference to the spectrum sensing and significantly reduces the available channel resources of legitimate SUs. Mainly, the motivation of attack is two types [9].
These are malicious or obstructive attack and selfish or greedy attack.

- Malicious Attack- The attacker only launches PUEA on the spectrum band.
- Selfish Attack- The attacker prevents other SUs from using the idle spectrum band by launching PUEA and reserves those bands for its own profit.

Fig. 1 illustrates the PUE attack scenario. In the multi-hop channel environment, if PUEA is launched and there is no idle channel for SU, then the call is dropped or delayed [10]. A dropped call results in unreliable communication and the delayed call degrades the quality of service [10]. In the adverse environment almost all the channels are affected by both malicious users and greedy users [11].

IV. DEFENSE TECHNIQUES AGAINST PUEA

Prevention of PUEA is vital in CRNs. Hence the detection techniques have to verify the authenticity of PU signal. Here, we classify the defense techniques as per their methods used for PUEA mitigation, and present corresponding contributions, assumption made to get the results. Furthermore, most of the schemes assume T.V transmitter as PU. Shaxun Chen et al. first proposed PUEA by considering mobile FM wireless microphone as PU in [34].

Transmitter verification scheme: This scheme proposes three types of defense techniques. Distance ratio test (DRT) uses the cooperative distance ratio of received signal strength obtained from a pair of verifiers and Distance difference test (DDT) uses the phase difference of the received signal to identify the transmitter location [9]. Here, the position of all users is assumed to be fixed, and tight synchronization is required between the verifiers. Performance will be degraded when the attacker is close to the SU. In Localization-based Defense (LocDef), extra underlying wireless sensors are used to take "snapshot" of the received signal strength (RSS) distribution in a network and the transmitter location is identified by the peak of the RSS signal [12].

Fenton approximation method: The author proposed an analytical model for PUEA. The Fenton approximation method is used to determine the mean and variance of receiving power at the SU due to both PU and malicious user (MU). The result is then applied over Markov inequality for getting a lower bound on the probability of successful PUEA [13]. Then the Wald's sequential probability ratio test is made on probability density function of receiving signals to detect PUEA [14]. These mechanisms require collecting a number of sensing samples for analysis that results more sensing time and overhead, and here the position of PU and all users are assumed to be fixed and they emit constant power. The results show that probability of PUEA increases as the distance between PU and SUs decreases.

Variance detection method: Here advance PUEA and defense strategy is modeled, where the attacker uses maximum- likelihood estimator to infer the transmit power of the PU and a mean-field approach is used to generate PUE signal. SU uses a variance detection method to mitigate PUEA [15]. To get the results the position of the PU and the distance between the PU and SU and between the PU and the attacker must be known each other. Simulation results show that the advance variance detection method performs better than naive detection method in the presence of advanced attack strategy of PUE attacker.

Fingerprint verification method: In ANN based scheme, the phase noise of the noisy carrier is extracted from the received signal. After wavelet analysis, the feature vector is applied to ANN to identify the transmitter [16]. In [17], the author uses the unique characteristics of the channel as a fingerprint. The channel-based hypothesis testing is based on the log-likelihood ratio test, and the Neyman-Pearson detector is employed to get constant the false alarm rate. Especially, this technique performs better in OFDM system. Here, probability of detection increases with increase in SNR and number of bursts.

Location based method: There are three types of defense techniques which are based on location of PU. In wavelet transform scheme [18], multi-resolution time frequency property of the wavelet is used to extract the transmitter fingerprint from the frequency domain samples of transmitting signals, so as to distinguish between PU signal and PUE attacker. In Time Difference of Arrival (TDoA) and Weighted Least square (WLS) scheme [19], time difference of arrival is used to compute the difference in the time of arrival of a signal at two or more pairs of nodes, usually by means of correlation techniques, and estimate the position of an emitter and detect PUE attacks in CRNs, and weighted least square method is used to minimize the quadratic error, but extra anchor nodes are required with known position and tight synchronization is

required between these nodes. In Two-Tier scheme [20], Two-Tier hierarchical CRN is developed, and M-ary hypothesis testing is made to identify PUE attacker. Here extra relay nodes help to detect PUEA.

Applying ANN: The author proposed two detection techniques. Firstly, Cyclostationary features of receiving signals (based on modulation type) are given to ANN to distinguish between PU and MU [21]. Secondly, log-covariance descriptor output is given to ANN to distinguish between PU and MU [22]. Here the author assumes that, all the users including malicious users and PUs are located within the same frequency band; for each period of time, only one user can transmit, and their transmission power is much higher than the ambient noise of the channel; the modulation scheme of PU is known and it is different from other users. Both experimental and simulation results show high probability of detection.

ALDO: In [23], an anomaly detection framework, called ALDO is proposed, which develops a model to detect the anomalous spectrum usage both in the presence of noise and authorized signal, and considers the path-loss exponent in signal propagation. Based on propagation channel characteristics and some knowledge about the authorized signal, three different methods were proposed for three different conditions. Among linearity check-given location (LCL), support vector machine (SVM) and calibrating power (CAL) SVM does not require any information about the authorized signal. To achieve this, extra auxiliary spectrum sensing units such as policy makers and other spectrum sensors etiquettes are required. The receiver characteristic (ROC) curves are presented for different conditions.

PU authentication: Primary user authentication system relies on the deployment of stationary helper nodes, which authenticate PU by link signature and then broadcast spectrum availability information to secondary users [24]. The system requires extra deployment of fixed helper nodes, which must be initialized with public key and certificate from a trusted authority. Then the analysis is done for different attack scenario and uses a helper resolution (HR) algorithm, especially for mobile user. More number of SUs can be accommodated without the need for repeated training, and can defend the attack successfully.

Hybrid PUEA Defense: In [25], the author proposed a first hybrid PUEA defense strategy which is based on the combination of energy detection and variance detection methods, especially for motional secondary users. This method is discussed by assuming attacker's preset transmit power, and by considering a stationary primary transmitter, but the SU and MU can move within a certain range. The false alarm probability decreases as threshold factor increases from 0 to 1.

IRIS: In [26], the author proposes a simple attack detection framework, called robust cooperative sensing via iterative state estimation(IRIS) which estimates the system states (transmit power of the primary transmitter and path-loss exponent) based on the sensing reports, and monitors the measurement residual. When there is a large deviation between the sensing reports and the normal value of the received signal strength, the malicious sensing report is detected and removed from the process. Base station must know the location of primary transmitter and sensors. The detection threshold must be chosen carefully so as to maximize the detection performance. The result shows that, IRIS is highly robust even under very challenging scenario, such as when a significant fraction of sensors are compromised.

Encryption and displacement method: Encryption algorithm is useful for defending PUEA, but if the attacker can know the information by air interception, then displacement algorithm is useful. In this process, PU base station and SU base stations coordinate all the communication system [27]. Workflow of entire method is verified by NS2 software. The result shows that too many users lead to packet loss.

Sybil Attack: In Sybil attack, the attacker launches PUEA, and creates multiple Sybil identities to falsify the decision process of SU via Byzantine attack. Then to prove the feasibility, the attack is implemented on the CR test-bed, Spider Radio [28]. Then the optimal attack strategies are analyzed by assuming stationary PU. The results show that expected cost increases with decreases in the number of good nodes. The expected cost is calculated at the fusion center with and without a reputation mechanism.

MME: In [29], Maximum-minimum eigenvalue detection method is used, and fewer cooperative SUs with less spatial correlation (because of the spatially-correlated shadow fading) are selected to mitigate the effect of undetected PUEA. It is a challenging point to choose the optimal number of SUs for spectrum sensing due to the random variation of the channel. The undetected PUEA is mitigated successfully in the spatial correlated environment.

Cross-layer approach: In [30], the information from the physical layer spectrum sensing and statistical analysis of the routing information of the multipath collected from the network layer is combined to detect anomalous spectrum usage attacks. So, the author proposed spectrum-aware split multipath routing protocol (SA-SMR) to carry this spectrum sensing information. Then for pinpointing the PUE Attack, active checking is done by injecting controlled interference to the suspicious attacker. This method is based on the assumption that, the attacker and SU have the same processing power, and the transmission range of the attacker is less than PU. The routing result shows that the spectrum sensing is highly correlated in the spatial.

SPUS and SVDD: In [31], specific primary user sensing (SPUS) is used to detect the presence of an unknown PUE attacker by judging the RF fingerprint, where the zoom-FFT is used to estimate the accuracy of pilot frequency and symbol rate. Support vector data description (SVDD) is introduced to sense the fine difference of Radio Frequency Fingerprinting (RFF) to distinguish PUE attacker from PU. Here, the primary transmitter is assumed to be fixed. Obviously, the PU verification fraction increases with decreasing PUEA verification fraction at low training SNR.

LCM and SCS: In [32], the author proposes linearity-check-for mobile transmitter (LCM) method to examine the linear relation between log-scale received signal strength (RSS) and logarithmic link distance for mobile authorized transmitter. Signal-print-check for the stationary transmitter (SCS) method is used to compare the current RSS pattern with the stored pattern of the authorized transmitter. Initially it is assumed that collaborative sensors know the statistics of detecting energies. Random channel variation decreases the detection probability.

RSDP: In [33], the author developed a robust spectrum decision protocol to mitigate PUEA. Here, the attacker launches PUEA which is followed by Byzantine attack. Flexible log-normal approximation is used to find pdf of the received signal, which is then followed by individual detection mechanism from good SUs. The impact of this Robust spectrum decision protocol on call dropping performance is analyzed in [10] by considering the malicious attacker (MA), and the same is analyzed in [11] by considering both MA and greedy attacker. All users are assumed to be stationary. PU and MU transmit constant power. The results show the impact of the attacker on call dropping rate.

Hearing is believing: This is the first work dealing with PUEA with mobile FM wireless microphone as PU. The correlation between the energy level of received RF signals and acoustic information received from the sensors present in SUs are used to verify the authenticity of PU [34]. Then the same method is realized in noisy environments [35]. Here, SUs must be equipped with extra sound sensors. This is a real world experiment.

Belief propagation: To identify the attacker, a defense strategy based on belief propagation (BP) of location information is developed, where each SU calculates the local function and compatibility function, computes the message, exchanges the messages with the neighboring users, and calculates the belief until it converges. If the mean of final belief is lower than the threshold, the suspect is PUE attacker [36]. To make this detection process more accurate, the author proposes BP framework based on Markov random field [37]. The transmission power and transmission range of the attacker are assumed to be within a certain limit. The location of the primary user must be known to all SUs. The mean of final belief is more when the distance between PU and PUE attacker is less.

DECLOAK: In [38], the author proposed a new method, called DECLOAK, which utilizes device dependent radio-metrics as a fingerprint. It uses non-parametric Bayesian classification to model the feature space of a single device as a multivariable Gaussian distribution with unknown parameters, and feature space of multiple devices as an infinite Gaussian mixture. Collapsed Gibb's sampling algorithm is applied to get samples from the posterior distribution, and active devices found out. Then the MAC addresses are collected. If more than one physical device is sharing the same ID, then PUE attack is identified.

Cooperative spectrum sensing: In a cooperative environment, when PUEA is launched, the SUs give their sensing information to the fusion center, which is then optimally combined with some appropriate weight to maximize the detection probability [39]. The optimal weights are related to the channel state information between the SU and the PU and between the SU and the attacker. The position and transmission power of PU and attacker are assumed to be constant, because the perfect channel estimation cannot be obtained from motional users. This proposed scheme shows better performance as compared to the conventional MRC method.

Dogfight: The game between defending SUs and an attacker in multichannel scenario has been modeled as a dogfight game in the spectrum. To combat PUEA, different techniques were applied for different channel statistics. In blind channel statistics [40], multiple defenders with unknown channel statistics consider each channel as a bandit arm and use adversarial multi armed bandit technique as their strategies. This same method is analyzed for both full and partial information about channel statistics in [41]. With Known channel statistics [42], the author assumes the passive defense policy, and dogfight is modeled as a zero sum game. Nash equilibrium and partially observable Markov decision process framework is applied to get optimal attacking strategy for single round and multi-round dogfight. In all the cases, the maximal interception attack degrades the performance.

Game theoretic approach: The game theoretic approach is modelled for single attacker and a single defender to avoid more complexities in the real-time environment scenario. In [43], a non-cooperative dynamic multistage game is formulated between SU and attacker. Nash equilibrium strategy is derived. Then a new belief updating system is proposed for the SU to learn the state of PU, and effectively defend the attacker. The interaction between the SU and attacker is modelled as a constant sum differential game [44]. The optimal strategy for both the SU and attacker is based on Nash equilibrium. The results show that average per stage payoff for player decreases with increasing of the probability of PU being ON.

A. Performance Analysis

CR is the upcoming technology which will be widely applied in near future. So, before that it should pay more attention towards its safety. PUEA is one of the serious attacks, where the authorized user is known; still the PUE attacker disguises them by emulating the characteristics of an authorized user, which enforces the SUs to evacuate the spectrum band. For this spectrum sensing plays a vital role where SUs have to sense the spectrum to detect this unauthorized user. Most of the techniques include the shadowing factor and path loss in the wireless channel and is given as [15].

$$P_r = P_t r^{-\alpha} e^{\alpha\beta} \quad (1)$$

α is a path loss exponent and $2 \leq \alpha \leq 8$. Where $\alpha = \frac{\ln 10}{10}$.

β is log-normal shadowing parameter and follows a normal distribution $\beta \sim N(0, \sigma^2)$, and $4 \leq \sigma^2 \leq 12$.

Effectiveness of cooperative spectrum sensing get reduced due to spatial correlated shadow fading, because the SUs located

close to each other are affected by a similar level of fading, hence give same sensing results, which again provide more opportunities to the attackers to launch PUEA successfully. So, with the exclusion of spatial correlated SUs, and with the selection of optimal number of SUs, the detection probability can be improved significantly. Several techniques regarding this are discussed in the literature. A fully distributed user selection algorithm is developed in [45] which adaptively selects uncorrelated SUs. In [46], the author showed that little number of SUs spread over large distances is more effective than a dense sensing network, and suggested an exponential correlation function for shadowing effects at different locations. In [47], the CR users under shadowing effects are identified by examining the normalized covariance matrix of the received signal and excluded from the sensing group. The detection probability is improved by adopting one of these techniques along with the existing defense techniques.

In the practical wireless environment, the channel varies with the motion of SUs and the attacker. So, always the single threshold based detection method does not hold good for detecting malicious attacker, because the threshold is set primarily, and the probability of detection is achieved by comparing the received power with the threshold. The detection performance can be improved by adopting a technique to optimize the threshold according to the channel variation. Most of the techniques assume that the position of all the users are fixed and known to each other. So for motional users, the channel estimation can be applied to estimate the exact location of users, so as to identify the malicious users successfully.

V. CONCLUSION

The awareness, reliability and adaptability nature of CR networks make it more precious to be deployed successfully in near future. Along with this realization, it has also opened the door for lots of threats, especially in security because of the presence of malicious nodes, who want to vandalize the entire communication networks. The physical layer is more efficient in terms of detection of this MU, because this is the primary layer whose information is to pass to the upper layers. PUEA is one of the major security issues in physical layer. So, this paper mainly aims to discuss the PUEA with its mitigation techniques. Although, some of the defense mechanisms have been proposed, they can't completely fulfill the need of CR networks operation. This leads us to our future research work which will give the ultimate solution to PUEA by considering channel estimation error into the mechanisms for detecting PUE attacker, which can support both stationary and a wireless microphone as the primary user.

REFERENCES

[1] Mitola, J.; Maguire, G.Q., Jr., "Cognitive radio: making software radios more personal," *Personal Communications, IEEE* , vol.6, no.4, pp.13,18, Aug 1999.

[2] Marcus, Michael J., "Unlicensed cognitive sharing of TV spectrum: the controversy at the Federal Communications Commission," *Communications Magazine, IEEE* , vol.43, no.5, pp.24,25, May 2005.

[3] Haykin, S., "Cognitive radio: brain-empowered wireless communications," *Selected Areas in Communications, IEEE Journal on* , Vol. 23, no. 2, pp. 201,220, Feb. 2005.

[4] Arkoulis, S.; Kazatzopoulos, L.; Delakouridis, C.; Marias, G.F., "Cognitive Spectrum and Its Security Issues," *Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. The Second International Conference on* , vol., no., pp.565,570, 16-19 Sept. 2008.

[5] Wassim El-Hajj; Haider Safa; Mohsen Guizani, "Survey of Security issues in Cognitive Radio Network," journal of internet technology, volume 12 2011.

[6] Mathur CN, Subbalakshmi KP. Security issues in cognitive radio networks. In: Cognitive networks: towards self-aware networks. John Wiley and Sons, Ltd; 2007 [chapter 11].

[7] Zhaoyu Gao; Haojin Zhu; Shuai Li; Suguo Du; Xu Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE* , vol.19, no.6, pp.106,112, December 2012.

[8] Romero, E.; Mouradian, A.; Blesa, J.; Moya, J.M.; Araujo, A., "Simulation framework for security threats in cognitive radio networks," *Communications, IET* , vol.6, no.8, pp.984,990, May 22 2012.

[9] Ruiliang Chen; Jung-Min Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," *Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on* , vol., no., pp.110,119, 25-25 Sept. 2006.

[10] Jin, Z.; Anand, S.; Subbalakshmi, K. P., "Performance Analysis of Dynamic Spectrum Access Networks under Primary User Emulation Attacks," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* , vol., no., pp.1,5, 6-10 Dec. 2010.

[11] ---------, "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks," *Communications, IEEE Transactions on* , vol.60, no.9, pp.2635,2643, September 2012.

[12] Ruiliang Chen; Jung-Min Park; Reed, J.H., "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *Selected Areas in Communications, IEEE Journal on* , vol.26, no.1, pp.25,37, Jan. 2008.

[13] Anand, S.; Jin, Z.; Subbalakshmi, K. P., "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on* , vol., no., pp.1,6, 14-17 Oct. 2008.

[14] Jin, Z.; Anand, S.; Subbalakshmi, K. P., "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," *Communications, 2009. ICC '09. IEEE International Conference on* , vol., no., pp.1,5, 14-18 June 2009.

[15] Zesheng Chen; Cooklev, T.; Chao Chen; Pomalaza-Raez, C., "Modeling primary user emulation attacks and defenses in cognitive radio networks," *Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International* , vol., no., pp.208,215, 14-16 Dec.

[16] Caidan Zhao; Wumei Wang; Lianfen Huang; Yan Yao, "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio," *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on* , vol., no., pp.1,5, 24-26 Sept. 2009.

[17] Wen-Long Chin; Chun-Lin Tseng; Chun-Shen Tsai; Wei-Che Kao; Chun-Wei Kao, "Channel-Based Detection of Primary User Emulation Attacks in Cognitive Radios," *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th* , vol., no., pp.1,5, 6-9 May 2012.

[18] Caidan Zhao; Liang Xie; Xueyuan Jiang; Lianfen Huang; Yan Yao, "A PHY-layer Authentication Approach for Transmitter Identification in Cognitive Radio Networks," *Communications and Mobile Computing (CMC), 2010 International Conference on* , vol.2, no., pp.154,158, 12-14 April 2010.

[19] Olga León, Juan Hernández-Serrano, Miguel Soriano, Cooperative detection of primary user emulation attacks in CRNs, Computer Networks, Volume 56, Issue 14, 28 September 2012.

[20] Jin Wei; Xi Zhang, "Two-Tier Optimal-Cooperation Based Secure Distributed Spectrum Sensing for Wireless Cognitive Radio Networks," *INFOCOM IEEE Conference on Computer Communications Workshops , 2010* , vol., no., pp.1,6, 15-19 March 2010.

[21] Di Pu; Yuan Shi; Ilyashenko, A.V.; Wyglinski, Alexander M., "Detecting Primary User Emulation Attack in Cognitive Radio Networks," *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE* , vol., no., pp.1,5, 5-9 Dec. 2011.

[22] Di Pu; Wyglinski, Alexander M., "Primary user emulation detection using frequency domain action recognition," *Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference on* , vol., no., pp.791,796, 23-26 Aug. 2011.

[23] Song Liu; Yingying Chen; Trappe, W.; Greenstein, L.J., "ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks," *INFOCOM 2009, IEEE* , vol., no., pp.675,683, 19-25 April 2009.

[24] Chandrashekar, S.; Lazos, L., "A Primary User authentication system for mobile cognitive radio networks," *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on* , vol., no., pp.1,5, 7-10 Nov. 2010.

[25] Feijing Bao; Huifang Chen; Lei Xie, "Analysis of primary user emulation attack with motional secondary users in cognitive radio networks," *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on* , vol., no., pp.956,961, 9-12 Sept. 2012.

[26] Min, A.W.; Kyu-Han Kim; Shin, K.G., "Robust cooperative sensing via state estimation in cognitive radio networks," *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on* , vol., no., pp.185,196, 3-6 May 2011.

[27] Zhou, Xiao; Xiao, Yang; Li, Yuanyuan, "Encryption and displacement based scheme of defense against Primary User Emulation Attack," *Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on* , vol., no., pp.44,49, 27-30 Nov. 2011.

[28] Yi Tan; Kai Hong; Sengupta, S.; Subbalakshmi, K. P., "Using Sybil Identities for Primary User Emulation and Byzantine Attacks in DSA Networks," *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE* , vol., no., pp.1,5, 5-9 Dec. 2011.

[29] Fayu Liu; Huifang Chen; Lei Xie; Kuang Wang, "Maximum-minimum eigenvalue detection-based method to mitigate the effect of the PUEA in cognitive radio networks," *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on* , vol., no., pp.1,5, 9-11 Nov. 2011.

[30] Sorrells, C.; Potier, P.; Lijun Qian; Xiangfang Li, "Anomalous spectrum usage attack detection in cognitive radio wireless networks," *Technologies for Homeland Security (HST), 2011 IEEE International Conference on* , vol., no., pp.384,389, 15-17 Nov. 2011.

[31] Zhenxing Luo; Caiyi Lou; Shichuan Chen; Shilian Zheng; Shaowei Li, "Specific primary user sensing for wireless security in IEEE 802.22 network," *Communications and Information Technologies (ISCIT), 2011 11th International Symposium on* , vol., no., pp.18,22, 12-14 Oct. 2011.

[32] Song Liu, Larry J. Greenstein, Wade Trappe, Yingying Chen, "Detecting anomalous spectrum usage in dynamic spectrum access networks, "Ad Hoc Networks, Volume 10, Issue 5, July 2012.

[33] Jin, Z.; Anand, S.; Subbalakshmi, K.P., "Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* , vol., no., pp.1,5, 6-10 Dec. 2010.

[34] Shaxun Chen; Kai Zeng; Mohapatra, P., "Hearing is believing: Detecting mobile primary user emulation attack in white space," *INFOCOM, 2011 Proceedings IEEE* , vol., no., pp.36,40, 10-15 April 2011.

[35] ----------, "Hearing Is Believing: Detecting Wireless Microphone Emulation Attacks in White Space," *Mobile Computing, IEEE Transactions on* , vol.12, no.3, pp.401,411, March 2013.

[36] Zhou Yuan; Niyato, D.; Husheng Li; Zhu Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," *Wireless Communications and Networking Conference (WCNC), 2011 IEEE* , vol., no., pp.599,604, 28-31 March 2011.

[37] Zhou Yuan; Niyato, D.; Husheng Li; Ju Bin Song; Zhu Han, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," *Selected Areas in Communications, IEEE Journal on* , vol.30, no.10, pp.1850,1860, November 2012.

[38] Nguyen, N.T.; Rong Zheng; Zhu Han, "On Identifying Primary User Emulation Attacks in Cognitive Radio Systems Using Nonparametric Bayesian Classification," *Signal Processing, IEEE Transactions on* , vol.60, no.3, pp.1432,1445, March 2012.

[39] Chao Chen; Hongbing Cheng; Yu-Dong Yao, "Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack," *Wireless Communications, IEEE Transactions on* , vol.10, no.7, pp.2135,2141, July 2011.

[40] Husheng Li; Zhu Han, "Blind Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems with Unknown Channel Statistics," *Communications (ICC), 2010 IEEE International Conference on* , vol., no., pp.1,6, 23-27 May 2010.

[41] Husheng Li; Zhu Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics," *Wireless Communications, IEEE Transactions on* , vol.9, no.11, pp.3566,3577, November 2010.

[42] --------, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems—Part II: Unknown Channel Statistics," *Wireless Communications, IEEE Transactions on* , vol.10, no.1, pp.274,283, January 2011.

[43] Tan, Y.; Sengupta, S.; Subbalakshmi, K. P., "Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach," *Communications, IET*, vol.6, no.8, pp.964,973, May 22 2012.

[44] Dong Hao; Sakurai, K., "A Differential Game Approach to Mitigating Primary User Emulation Attacks in Cognitive Radio Networks," *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on* , vol., no., pp.495,502, 26-29 March 2012.

[45] Cacciapuoti, A.S.; Akyildiz, I.F.; Paura, L., "Correlation-Aware User Selection for Cooperative Spectrum Sensing in Cognitive Radio Ad Hoc Networks," *Selected Areas in Communications, IEEE Journal on* , vol.30, no.2, pp.297,306, February 2012.

[46] Ghasemi, A.; Sousa, E.S., "Asymptotic performance of collaborative spectrum sensing under correlated log-normal shadowing," *Communications Letters, IEEE* , vol.11, no.1, pp.34,36, Jan. 2007.

[47] Dinh Thi Thai Mai; Trang Cong Chung; Nguyen Quoc Tuan; Dinh-Thong Nguyen, "Improving Cooperative Spectrum Sensing under Correlated Log-Normal Shadowing," *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2010 International Conference on* , vol., no., pp.365,370, 10-12 Oct. 2010.

Deepa Das received her B.E. in 2005 from BPUT, Odisha, India and her M.Tech from KIIT University in 2008. She is currently a Ph.D. candidate of Department of Electrical Engineering, NIT, Rourkela, India. Her research interests are in the area of wireless communication, signal processing and cognitive radio.

Susmita Das received her B.Sc. Engineering from CET, Bhubaneswar, Odisha, and M.Sc. Engg. and Ph.D. both from NIT, Rourkela, Odisha, India. She is currently an Associate Professor of Department of Electrical Engineering in NIT, Rourkela. She is a life member of ISTE and Institute of Engineering, India. She is also a member of IETE, India and IEEE. Her research interests include mobile wireless communication, soft computing and signal processing.