A survey of Detection and Mitigation Techniques of Primary User Emulation Attacks in Cognitive Radio Networks

Md. Al-Amin, Md. Ibrahim Abdullah, Md. Jahangir Alam, Sheikh DobirHossain, NazmulHossain

Abstract—Cognitive Radio is promising technologies, which can be used to solve the spectrum shortage problems. The success of cognitive approach depends on detection of licensed or primary users. If a malicious user transmit signal similar to licensed user, cognitive users do not find spectrum holes and cannot communicate with other unlicensed user. This behavior launched the primary user emulation attacks. In this paper we survey the detection and mitigation techniques of primary user emulation attacks. In our survey it is found that primary user emulation attack detection depends on prior knowledge of primary user location, signal transmission, radio environment mapping etc.

Index Terms—Primary User, Secondary User, Cognitive Radio, Cognitive Radio Network, Primary User Emulation Attack, DRT, DDT, LV,NPCHT, WSPRT, DECLOAK .

1 Introduction

Today people are becoming dependent on radio frequency spectrum for using Smart Phones, Internet, Wireless devices applications and many others wireless services. Also diversity of wireless communications through wireless applications (voice, short message, Web and multimedia) and demand of high Quality-of-Service (QoS) applications are increasing with times. Thus more and more spectrum resources are needed. But within the current spectrum framework, most of the spectrum bands are exclusively allocated to specific licensed. The licensed users known as Primary User (PU) use the specific wireless spectrum on a long term basis for large geographical regions. It is found that major portion of the licensed spectrum are unused [1-2]. Cognitive radio technology is proposed to solve these problems. Cognitive radio technology can efficiently utilize the unused spectrum for unlicensed users without creating any interference to primary users [3-5]. Cognitive Radio (CR) capabilities of frequency agility, dynamic frequency selection, adaptive modulation, transmit power control, location awareness and negotiated use; make it very suitable to use the wireless spectrum opportunistically. Some of the benefits of CR are Dynamic Spectrum Access, Common Hardware Platform, Higher Bandwidth Services, Communication under Different Spectrum Regulations, Commercial Exploitation, Improved Quality of Service, and etc.

Compared with traditional radio, CR is more flexible and exposed to the wireless network. Cognitive radio has its special safety problems: spectrum abuse and selfish behavior, to attack by imitating Primary Users, public control channel obstruction, and cognitive nodes evolution into malicious nodes etc. As a result, there are more security threats than the traditional radio environment. There are mainly two type threats in Cognitive Radio Networks (CRN) and they are Artificial intelligence behavior threats and Dynamic spectrum access threats [6, 7]. These threats raise new problems either because they only exist in networks or they require different solutions because of the unique characteristics of CR networks. Artificial intelligence behavior threats include Policy threats [8], Learning threats [8-12], and Parameters threats [13, 14]. Dynamic spectrum access threats could be classified as Primary User Emulation Attack [15-28], Spectrum Sensing Data Falsification Attack [17-27], and Denial of Services Attacks [21-24, 30-31]. In Cognitive Radio Network (CRN), a Secondary User (SU) can use spectrum band when a PU does not use the spectrum band. If a PU wants to use the spectrum band then SU free the captured band and try to find another spectrum hole [5] to continue services. In CRN a SU can share spectrum with another SU. Malicious users may generate signals similar to PU. This is known as Primary User Emulation (PUE) attack. It seems to other SUs that PU wants to use its licensed spectrum. As a result SU free the present spectrum. Malicious users use the spectrum band and do not share it other SUs [32].

Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack. In selfish PUE attack an attacker's objective

- *Md. Al-Amin is currently serving as Lecturer in Computer Science and engineering Department in Jessore University of Science & Technology, Bangladesh. E-mail: malamin.ali@gmail.com*
- *Md. Ibrahim Abdullahis currently serving as Professor in Computer Science and engineering Department in Islamic University, Kushtia, Bangladesh.E-mail: ibrahim25si@yahoo.com*
- *Md. Jahangir Alamis currently serving as Manager inInternal IT Audit Department in NRB Commercial Bank Limited, Dhaka, Bangladesh. E-mail: jahangircsebd@gmail.com*
- *Sheikh DobirHossainis currently serving as Assistant Professor inPhysics Department in Jessore University of Science & Technology, Bangladesh. E-mail: dobir.aece@gmail.com*
- *NazmulHossain is currently serving as Lecturer in Computer Science and engineering Department in Jessore University of Science & Technology, Bangladesh, PH-042172058. E-mail: nazmul.justcse@gmail.com*

is to maximize its own spectrum usage. The objective of malicious PUE attack is to obstruct the DSA process of legitimate secondary users - i.e., prevent legitimate secondary users from detecting and using fallow licensed spectrum bands, causing denial of service. In this paper we have surveyed various detection and mitigation techniques against Primary User Emulation attack.

The remainder of this paper is organized as follows: Section 2 presents related work. In section 3 we describe basics of primary user emulation attack. In section 4 we discuss work related to the detection techniques of PUE attacks. Section 5 presents related work to mitigate the PUE attacks. Finally we concluded in section 6.

2 Related Works

In [33, 34], authors conducted a survey of Various Defense Techniques to Detect Primary User Emulation Attacks based on various detection techniques such as Fenton's Approximation, Location Based, Transmitter Verification, Dogfigh, Belief Propagation, PU Authentication, Encryption and Displacement method, Fingerprint verification method, Game Theoretic Approach, Dogfight, Cooperative spectrum sensing, DECLOAK, Hearing is believing, RSDP, LCM and SCS, SPUS and SVDD, MME, ALDO, Applying ANN, IRIS, and so many others. Authors also summarized the Tests/ Models used by the different authors.

A survey on Link Layer Attacks in Cognitive Radio Networks is presented in [35], where authors mentioned few techniques like Weighted Sequential Ratio Test, Weight based fusion scheme, Neyman-Pearson Test, Detection mechanism based on trust, and etc. In this paper authors also evaluated of those techniques.

Authors in [36] presented a survey on Primary User Emulation Detection Mechanisms in Cognitive Radio Networks. Passive anti-PUE approach, nonparametric classification method, Localization based defense method, Fully unsupervised dynamic sparse coding approach, Mixture sparse coding model, and etc. are mentioned in this paper. Authors also evaluated advantages and disadvantages of each conducted method.

3 Primary User Emulation Attack

In the Dynamic Spectrum Access (DSA) paradigm, when a PU is detected in a given band, all SUs should avoid accessing that band. When a SU detects free spectrum hole it may share with other SUs. In a PUE attack [15-28], a malicious secondary tries to gain priority over other secondary users by transmitting signals that emulate the characteristics of a primary user's. Primary user emulation attack is shown in the Figure -1.

3.1 Classification

Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack.

1) Selfish PUE Attacks [15-18]: In this attack, an attacker's objective is to maximize its own spectrum usage. When selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of primary user signals. This attack is most likely to be carried out by two selfish secondary users whose intention is to establish a dedicated link.

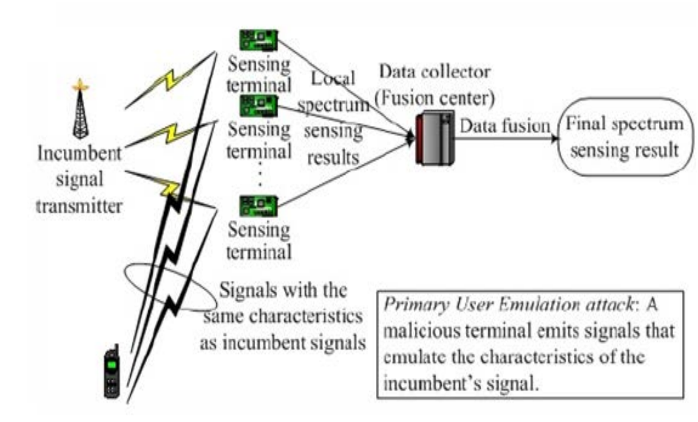

Fig. 1.Primary User Emulation Attack [17].

2) Malicious PUE Attacks [15-18]: The objective of this attack is to obstruct the DSA process of legitimate secondary users—i.e., prevent legitimate secondary users from detecting and using fallow licensed spectrum bands, causing Denial of Service (DoS). Unlike a selfish attacker, a malicious attacker does not necessarily use fallow spectrum bands for its own communication purposes. It is quite possible for an attacker to simultaneously obstruct the DSA process in multiple bands by exploiting two DSA mechanisms implemented in every CR. The first mechanism requires a CR to wait for a certain amount of time before transmitting in the identified fallow band to make sure that the band is indeed unoccupied. The second mechanism requires a CR to periodically sense the current operating band to detect primary signals and to immediately switch to another band when such signals are detected. By launching a PUE attack in multiple bands in a round-robin fashion, an attacker can effectively limit the legitimate secondary users from identifying and using fallow spectrum bands.

4 PUE Attack Detection Techniques

In paper [12], a transmitter verification procedure proposed that employs a non-interactive location verification scheme to exploit the fact that the incumbent signal transmitters are placed at fixed locations. Because the location verification scheme is non-interactive, no modification to the incumbent signal transmitters is needed. In the proposed location verification scheme, designated verifiers cooperatively verify the legitimacy of an incumbent signal transmitter's location by passively listening to its signal without interacting with the transmitter. Two alternative techniques are proposed that are at the heart of the location verification scheme. The first technique, the Distance Ratio Test (DRT) [ref], uses received signal strength (RSS) measurements obtained from a pair of verifiers to verify the transmitter's location. The second technique, Distance Difference Test (DDT) [ref], utilizes the phase difference of the primary user's signal observed at a pair of verifiers to verify the transmitter's location.

In this work few assumptions proposed to be made to support the operations of DRT and DDT. Trusted location verifiers (LVs) [ref] exist for performing DRT or DDT. An LV can be a dedicated node, a SU with enhanced functions (to carry out DRT/DDT), or a fixed/mobile base station. Two types of LVs: one or more master LVs and slave LVs are considered and they know their location from a secure GPS system. A master LV has a database of the coordinates of every primary user.

4.1 Distance Ratio Test (DRT)

RSS-based localization is based on the fact that there is a strong correlation between the length of a wireless link and RSS. In a single iteration of DRT, a pair of LVs, represented by LV1(x1, y1) and LV2(x2, y2) and obtaining RSS results R1 and R2, respectively. The values of R1, R2, (x1, y1), and (x2, y2) are sent to a master LV (note that LV1 or LV2 or even another LV may act as a master LV). After receiving the parameters, the master LV goes through the following procedure for each TV tower's coordinate in its database.

Suppose that the two dimensional coordinate of the first TV tower is (u1, v1). The master LV calculates the reference distance ratio as:

$$\rho = \frac{\sqrt{(x_1-u_1)^2+(y_1-v_1)^2}}{\sqrt{(x_2-u_1)^2+(y_2-v_1)^2}} \quad (1)$$

The master LV calculates the measured distance ratio, given by the following equation, using the RSS measurements:

$$\rho' = \frac{d_1}{d_2} = \sqrt{\frac{R_1}{R_2}} \quad (2)$$

where d1 and d2 are the respective distances between LV1 and the signal source and LV2 and the signal source.

The master LV checks whether

$$\rho' \in \left[\frac{\rho}{1+\varepsilon_1}, (1+\varepsilon_1)\rho\right] \quad (3)$$

whereε_1 (≥ 0) is the expected maximum error.

There are two caveats about the DRT. First, since DRT relies on a large-scale propagation model, the possible fluctuations in RSS caused by small-scale fading are not considered. Second, DRT does not consider the fact that the radio propagation model is affected by various environmental variables.

4.2 Distance Difference Test (DDT)

DDT that verifies the difference in the two distances between a primary user and a pair of LVs. The difference in distance can be measured by measuring the phase shift of a signal at the two LVs. DDT does not suffer from DRT's drawbacks. The distance difference between a signal source and two LVs can be estimated by calculating the time difference in which each LV sees the same synchronization pulse. The time difference is readily converted to distance difference by multiplying the speed of light to the time difference. Two synchronized LVs, LV1 and LV2, simultaneously record the time at which they see the synchronization pulse of the incumbent signal, and record the time values as t1 and t2, respectively. The time difference is calculated as t∆ = t1 – t2.

Suppose that the coordinates of LV1 and LV2 are (x1, y1) and (x2, y2), respectively. The values of t1, t2, (x1, y1), and (x2, y2) are sent to the master LV. After receiving the parameters, the master LV goes through the following procedure for each incumbent user's coordinate in its database.

Suppose that the two dimensional coordinate of the first TV tower is (u1, v1). The master LV calculates the reference distance difference as:

$$s_1 = \sqrt{(x_1-u_1)^2+(y_1-v_1)^2} \quad (4)$$

$$s_2 = \sqrt{(x_2-u_1)^2+(y_2-v_1)^2} \quad (5)$$

From equation (4) and (5) we have

$$s = s_1 - s_2 \quad (6)$$

Then the master LV calculates the observed distance difference using the time difference:

$$s' = c(t_1 - t_2) = ct_\Delta \quad (7)$$

where c is the speed of light.

The master LV checks whether

$$s \in [s - c\varepsilon_2, s + c\varepsilon_2] \quad (8)$$

where$\boldsymbol{\varepsilon_2}$ is the expected maximum time measurement error.

If (8) does not hold, the signal source under scrutiny fails the location verification for the primary user used in Step 1; otherwise, it passes the location verification. The above steps are repeated using the coordinates of the next PU, and the process is repeated until all of the coordinates in the database have been exhausted. If the signal source fails all of the location verifications, then the master LV concludes that the location of the signal source is not consistent with any of the PU in its database.

To counter PUE threat, authors also propose a transmitter verification scheme in [13], called LocDef (localization based defense), which verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. To estimate the location of the signal transmitter, LocDefemploys a non-interactive localization scheme. An alternative approach is also investigated in this paper that uses the intrinsic characteristics of RF signals to distinguish and identify emitters—i.e., RF fingerprinting. But if the primary transmitters are mobile and have low power, localization-based approaches for thwarting PUE attacks do not work.

In [14] an analyzing method of primary user emulation attacks is developed without using any location information. It can be implemented with any sensor networks. Fenton's approximation and Wald's sequential probability ratio test

(WSPRT) are used to detect PUEA. Through this analysis the users can set thresholds on probability of missing the primary user and the probability of successful. In [15], authors propose another method to detect primary user emulation attacks (PUEA) in fading wireless channels in the presence of multiple randomly located malicious users in cognitive radio networks. Based on Neyman-Pearson composite hypothesis test (NPCHT) and a Wald's sequential probability ratio test (WSPRT) the detection method is implemented in [15].

An analytical approach based on Fenton's approximation and Markov inequality proposed in [16], and obtains a lower bound on the probability of a successful PUEA on a secondary user by a set of co-operating malicious users. In [17, 18] a robust spectrum decision protocol is proposed that can mitigate PUEA using individual spectrum decisions made by secondary nodes in the network. By using a flexible log-normal sum approximation the received power is characterized for the decision. A non-cooperative dynamic multistage game between the secondary nodes and the adversaries generating the PUEA is formulated in [19]. The pure-strategy and mixed-strategy Nash equilibria for the secondary user and malicious attacker are investigated. Moreover, author propose a novel belief updating system for the secondary user to learn the state of the primary user as the game evolves and defend against the MA in the multistage version of the game, based on which the SU can learn the state of the primary user and intelligently adjust its strategy stage by stage.

A novel method to detect the PUE attack of mobile primary users is proposed in [20]. The authors exploit the correlations between RF signals and acoustic information to verify the existence of primary user to mitigate primary user emulation attack in white space. Authors in [21] develop a theory behind manipulating the decision regions in a neural network using self-organizing maps to mitigate primary user emulation attacks for unsupervised learning in signal classifiers, and attacks against self-organizing maps.

Detection of primary user is proposed in [22] based on Radio Environment Map" (REM). REM is an integrated database that consists of comprehensive multi-domain information for a CR network, including the locations and activities of radio devices. Given that such information is reliable and accessible to location verifiers (LVs) (e.g., an REM is installed in an LV), it is possible to verify an incumbent transmitter by comparing its observed location and activities with those stored in the REM. Cooperative location of a primary source can be a valuable tool for distinguishing between a legitimate transmission and a PUE attack whenever the position of primary users is known. However, the location process can be undermined due to false data provided by malicious or faulty nodes. In [23], authors analyze the effect of forged reports on the location process of a given emitter and provide a set of countermeasures in order to make it robust to undesired behaviors.

In paper [24], PUE attack is detected by energy detection to locate the existing users on the frequency band. The approach employs a cyclostationary calculation to represent the features of the user signals, which are then fed into an artificial neural network for classification. Proposed approach does not require any special hardware or time synchronization algorithms in the wireless network. Consequently, existing systems can readily employ the proposed approach without significant structural and functional modifications.

5 PUE Attacks Mitigation Techniques

Newman et. al. [25] proposed a defense strategy against the PUE attack in CR networks using belief propagation. In this defense strategy each SU calculates the local function and the compatibility function, computes the messages, exchanges messages with the neighboring users, and calculates the beliefs until convergence. On detection of PUE attacker all SUs can avoid the PUE attacker's primary emulation signal in the future. An advanced countermeasure against PUE attack is characterized in paper [26]. Both the attacker and the defender can apply estimation techniques and learning methods to obtain the key information of the environment and thus design better strategies. It is also demonstrated that the advanced attack strategy can defeat the naive defense technique that focuses only on the received signal power, whereas the advanced defense strategy that exploits the invariant of communication channels can counteract the advanced attack effectively.

In paper [27], PUE attack is studied using game theoretic argument. A stochastic game is used to model the attack and defense. The Lyapunov drift is considered as the reward in each round and explicit expressions of the Nash equilibrium strategies are obtained through the game. The interaction between the PUE attacker and the SU is modeled as a constant sum differential game which is called PUE attack game in [28]. The SU's objective is to maximize its overall channel usability, while the attacker's objective is to minimize the secondary user's overall channel usability. The Nash equilibrium solution of this PUE attack game is deprived, and the optimal anti-PUE attack strategy is obtained. By following the differential game solution, the secondary user can always optimize its channel usability when confronting PUE attacks.

A passive anti-PUE approach is proposed in [29], in this scheme, the defenders randomly choose channels to sense and avoid the PUE attack. It is assumed that the channel statistics like availability probabilities are known; then the PUE attack and the random hopping are modeled as a zero-sum game between the attacker and defending SU(s). The Nash equilibrium of the game is found. The anti-jamming efficiency is also obtained. The authors also proposed defense against PUE attack in [30] in the scenario of unknown channel statistics (coined blind dogfight in spectrum). The algorithm of the adversarial bandit problem is adapted to the context of blind dogfight. Both cases of complete and partial information about the rewards of different channels are analyzed. Performance bounds are obtained subject to arbitrary channel statistics and attack policy. Several attack strategies, namely uniformly random, selectively random and maximal interception attacks, are also discussed.

In [31] using device specific features, authors propose a passive, nonparametric classification method DECLOAK to determine the number of transmitting devices in the PU spectrum. Channel independent features are selected forming fingerprints for devices, which cannot be altered postproduction. The Infinite Gaussian mixture model (IGMM) is adopted and a modified collapsed Gibbs sampling method is proposed to classify the extracted fingerprints. Due to its unsupervised nature, there is no need to collect legitimate PU fingerprints. In combination with received power and device MAC address, the proposed method can efficiently detect the PUE attack. The performance of DECLOAK is also shown to be superior than that of the classical non-parametric mean shift (MS) based clustering method.

A Bayesian game framework is modeled in [32] to analyze primary user emulation problem, in which users are unsure of the legitimacy of the claimed type of other users. Depending on radios' beliefs about the fraction of PUs in the system, a policy maker can control the occurrence of emulation attacks by adjusting the gains and costs associated with performing or checking for emulation attacks. Maximum likelihood (ML) estimation is widely applied to estimate the state transition probabilities of primary users. In [33] derives a precise expression of the probability mass function (PMF) for the ML estimator. By leveraging the exact PMF expression, the essential relation among the number of samples, transition probabilities, and estimation accuracy is revealed.

A novel model to parameterize the PU traffic in a more efficient and accurate way in order to overcome the drawbacks of the Poisson modeling is proposed in [34]. The proposed model makes this possible by arranging the first-difference filtered and correlated primary user data into clusters. In this paper, a new metric called the Primary User Activity Index, is introduced, which accounts for the relation between the cluster filter output and correlation statistics. The performance of the proposed model is evaluated by means of traffic estimation accuracy, and false-alarm.

Authors in [35] focus on the PUEA problem in a system model where the secondary users are motional. Based on the network model with motional secondary users, how the attacker emulates the primary user is discussed in this paper. Then, a hybrid PUEA defense strategy based on a combination of energy detection and variance detection is proposed. A cooperative localization method specifically suited to CRNs is proposed in [36] to detect primary user emulation (PUE) attack which relies on TDoA measurements and Taylor-series estimations.

In [37-39] authors proposed cryptographic link signature and wireless link signatures (derived from physical radio channel characteristics) based techniques to enable primary user detection in the presence of attackers. Authors [37] describe two schemes to add a signature, one using modulation, and the other using coding. In [38, 39] a helper node placed physically close to a primary user. The helper node serves as a "bridge" to enable a secondary user to verify cryptographic signatures carried by the helper node's signals and then obtain the helper node's authentic link signatures to verify the primary user's signals. This approach explores the geographical proximity of the helper node to the primary user, and thus does not require any training process.

TABLE 1
SUMMARY FOR PRIMARY USER EMULATION ATTACK

Authors	Countermeasure	Remarks/ Evaluation
Chen *et al.* [37]	Distance Ratio Test (DRT) based on received signal strength (RSS) measurements, and Distance Difference Test (DDT) based on signal phase difference are used to verify the transmitter's location. Both methods use Non-interactive location verification scheme. DRT relies on a large-scale propagation model, the possible fluctuations in RSS caused by small-scale fading are not considered. DRT does not consider the fact that the radio propagation model is affected by various environmental variables.	No modification to the incumbent signal transmitters is needed, because the location verification scheme is non-interactive. Depends on trusted nodes called Location Verifiers (LV's) and RSS value. Major drawback is that tight synchronization among LVs is required and it can be fooled if the attacker is enough close to the tower. GPS system is not available always.
Chen *et al.* [38]	LocDef (localizationbased defense), which verifies primary transmitter by estimating its location and observing its intrinsic signal characteristics of RF signals to distinguish and identify emitters—i.e., RF fingerprinting.	If the primary transmitters are mobile and have low power, this approach for thwarting PUE attacks does not work.
Jin *et al.* [39]	Fenton's approximation and Wald's Sequential Probability Ratio Test (WSPRT)	These methods do not require any location information about primary transmitter.
Jin *et al.* [40]	Neyman-Pearson Composite Hypothesis Test (NPCHT) and Wald's Sequential Probability Ratio Test (WSPRT).	Can detect malicious users in fading wireless channels in the presence of multiple randomly located malicious users in CRNs.
Tan *et al.* [44]	Game strategy based on the Pure-strategy and Mixed-strategy Nash equilibria techniques. It also provides novel belief updating system for the secondary user.	In wireless communication system, maintaining belief updating system by base station is not easy.
Shaxun *et al.* [45]	Calculating correlations between RF signals and acoustic information.	Always availability of pure acoustic information is uncertain.
Zhao *et al.* [47]	Based on Radio Environment Map (REM). REM consists of comprehensive multi-domain information for a CR network, including the locations and activities of radio devices.	Building and maintaining REM database of location and activities of radio devices can be undermined due to false data provided by malicious or faulty nodes.
Di Pu *et al.* [49]	An artificial neural network (ANN) is used to classify the user signals by calculating cyclostationary calculation of the signals features.	Although the proposed approach does not require any special hardware or time synchronization algorithms but it requires the prior knowledge of signals' cyclostationary features (prefixes, pilots, cyclic, modulations, carriers and other repetitive characteristics).
Husheng *et al.* [51]	A stochastic game based on Nash equilibrium strategies for modeling and defensing attacks.	The Lyapunov drift is considered as the reward in each round based on performance for the SUs.
Nguyen *et al.* [55]	Forming fingerprints for devices from channel independent features. Infinite Gaussian mixture model (IGMM) and Modified Collapsed Gibbs Sampling Method (MCGSM) is used to classify the extracted fingerprints. DECLOAK is used for detecting PUE attack and to determine the number of transmitting devices in the spectrum.	There is no need to collect legitimate PU fingerprints, due to its unsupervised nature. DECLOAK is superior than that of the classical non-parametric mean shift (MS) based clustering method.
Canberk *et al.* [58]	A new metric Primary User Activity Index which accounts for the relation between the cluster filter output and correlation statistics.	Performance is evaluated by means of traffic estimation accuracy, and false-alarm. It overcomes the drawbacks of the Poisson modeling.
LeóN *et al.* [60]	Localization method that applies Time Difference of Arrival (TDoA) measurements and Taylor-series estimations.	Major drawback of this approach is that it relies on many assumptions that make them very restrictive and not applicable to general Cognitive Radio Networks.
Xi Tan *et al.* [61]	Cryptographic link signature based techniques. Two schemes are proposed to add a signature, one using modulation, and the other using coding.	It requires the modification or altering the primary user system which violets FCC regulations for Cognitive Radio Networks.
Liu *et al.* [62]. Swathi *et al.* [63]	Wireless link signatures (derived from physical radio channel characteristics) based techniques. The helper nodes are used and serve as "bridge" to verify the primary user's signals.	This approach explores the geographical proximity of the helper node to the primary user, and thus does not require any training process.

Table 1 represents the key points of primary user emulation attack detection and mitigation techniques.

6 Conclusion

Cognitive radio is a highly multidisciplinary area currently attracting numerous research efforts, which provides a large number of challenges regarding security and accurate sensing. Primary user emulation attack limits the uses of spectrum holes of cognitive users. As discussed throughout the survey, many of them are not practical from a deployment point of view. For instance, many current proposals require the deployment of additional sensors (helping devices) or the comparison of observations against characteristics known a priori, particularly the locations of the primary users. The cost of such solutions, the unavailability of location information, or the lack of accuracy of the positioning mechanisms may complicate the design and effectiveness of new security approaches. Also, the assumption about the primary users' locations being known a priori may be both simplistic and unrealistic. In our point of view, these are the main issues still open regarding the identification of attacks against the detection of primary user activity.

In terms of security, distributed cognitive radio networks may provide a better approach than centralized approaches, despite complicating the design of appropriate mechanisms. By allocating spectrum and security decisions to several secondary users, the risk of DoS attacks against a single point of failure (i.e., the central entity) is eliminated. In this context, clustering schemes may be an intermediate alternative, with each cluster having its own central entity (i.e., decision and fusion center) and the secondary users being able to elect another central entity or migrate to another cluster in case of failure or attack.

References

[1] Federal Communications Commission, "Spectrum Policy Task Force," Report ET Docket no. 02-135, Nov. 2002.

[2] Federal Communications Commission, "Notice of proposed rulemaking and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies," ET Docket No. 03-108, Feb. 2005.

[3] Federal Communications Commission, "Establishment of interference temperature metric to quantify and manage interference and to expand available unlicensed operation in certain fixed mobile and satellite frequency bands," ET Docket 03-289, Notice of Inquiry and Proposed Rulemaking.

[4] M. subhedar and G. Birajdar, "Spectrum Sensing Techniques in Cognitive Radio: a Survey," in International Journal of Next Generation Networks, Volume: 3, Issue: 2, 2011.

[5] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation / dynamic spectrum access / cognitive radio wireless networks: a survey," in Computer Networks Journal (Elsevier), Volume: 50, Pages: 2127-2159, Sep. 2006.

[6] L. Tang, and J. Wu, "Research and Analysis on Cognitive Radio Network Security," in Wireless Sensor Network, 2012, Volume: 4, Pages: 120-126, April 2012.

[7] Y. Zhang, G. Xu, and X. Geng, "Security Threats in Cognitive Radio Networks", in the 10th IEEE International Conference on High Performance Computing and Communications, Pages: 1036-1041.

[8] T. Clancy, and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," in Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), Singapore, Pages: 1- 8, May 15-17, 2008.

[9] K. Takeuchi, S. Kaneko and S. Nomoto, "Radio Environment Prediction for Cognitive Radio," in 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Singapore, Pages: 1-6, May 15-17, 2008.

[10] Q. Zhao, and Brian M. Sadler, "A survey of dynamic spectrum access," in IEEE Signal Processing Magazine, Pages: 79-89, MAY 2007.

[11] D. Cabric, S. M. Mishra and R. W. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios," in Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, Asilomar, Pages: 772-776, November 7-10, 2004.

[12] Y. Xing, R. Chandramouli, Stefan Mangold, and S. Shankar N, "Dynamic spectrum access in open spectrum wireless networks," in IEEE Journal on Selected Areas in Communications, Volume: 24, Number: 3, March 2006.

[13] Jack L. Burbank. Laurel, and MD, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," IEEE, 2006.

[14] Burbank, J.L, "Security in cognitive radio networks: the required evolution in approaches to wireless network security," in Proceedings the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Pages: 1–7, 2008.

[15] Z. Yuan, D. Niyato, H. Li, and Zhu Han, "Defense Against Primary User Emulation Attacks Using Belief Propagation of Location Information in Cognitive Radio Networks," in IEEE Wireless Communications and Networking Conference, Cancun, Mexico, March 28-31, 2011.

[16] Sanket S. Kalamkar, A. Banerjee, and A. Roychowdhury, "Malicious User Suppression for Cooperative Spectrum Sensing in Cognitive Radio Networks using Dixon's Outlier Detection Method," in 2012 National Conference on Communications (NCC), Page(s): 1 – 5, February 3-5 2012..

[17] R. Chen; J. M. PlacePark; Y.T. Hou, and J.H. Reed,"Toward secure distributed spectrum sensing in cognitive radio networks," in IEEE Communications Magazine, Volume: 46, Number: 4, Pages: 50-55, April 2008.

[18] Z. Gao, H. Zhu, S. Li, S. Du and X. Li, "Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks," in IEEE Wireless Communications, Pages: 106-112, December 2012.

[19] P. Morerio, K. Dabˇcevi´c, L. Marcenaro, and C. S. Regazzoni, "Distributed cognitive radio architecture with automatic frequency switching,"

[20] R. Chen, J. M. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in IEEE (2008) International INFOCOM: The 27th Conference on Computer Communications, Pages: 1876–1884.

[21] Saman T. Zargar, Martin B. H. Weiss, Carlos E. Caicedo, and James B. D. Joshi, "Security in Dynamic Spectrum Access Systems: A Survey," in International Wireless Communications and Mobile Computing Conference (IWCMC'2009), Pages: 309-313, 2009.

[22] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," in Journal of Internet Technology, Volume: 12, Number: 2, Pages: 1-18, 2011.

[23] Z. M. Fadlullah, H. Nishiyama, N. Kato, and M. M. Fouda, "Intrusion

Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks," in IEEE Network Magazine, Volume: 27, Number: 3, Pages: 51-56, May- June 2013.

[24] O. Le´on, J. Hern´andez-Serrano and M. Soriano, "Securing cognitive radio networks," in International Journal of Communication Systems, Volume: 23, Pages: 633–652, February 2010.

[25] T. R. Newman, T. Charles. Clancy, M. McHenry and J. H. Reed, "Case Study: Security Analysis of a Dynamic Spectrum Access Radio System," in the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings, 2010.

[26] K. Bian, and P. J. M.J. Park, "Security vulnerabilities in IEEE 802.22," in Proceedings of the 4th Annual International Conference on Wireless Internet (WICON 2008), Volume: 9, Pages: 1–9, 2008.

[27] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a Trust Aware Cognitive Radio Architecture," in Mobile Computing and Communications Review, Volume: 13, Number: 2, Page: 86-95.

[28] G.A. Safdar, M. O'Neill (née McLoone), "Common Control Channel Security Framework for Cognitive Radio Networks," in IEEE 2009.

[29] J. Hern´andez-Serrano, O. Le´on, and M. Soriano, "Modeling the Lion Attack in Cognitive Radio Networks," in EURASIP Journal on Wireless Communications and Networking 2011.

[30] C. N. Mathur, and K. P. Subbalakshmi, "Security Issues in Cognitive Radio Networks," in Cognitive Networks: Towards Self-Aware Networks, Edited by Qusay H. Mahmoud, 2007 John Wiley & Sons, Ltd.

[31] X. Zhang, and C. Li, "The security in cognitive radio networks: a survey," in International Wireless Communications and Mobile Computing Conference (IWCMC), 2009, Pages: 309-313.

[32] S. Alrabaee, A. Agarwal, D. Anand, M. Khasawneh, "Game Theory for Security in Cognitive Radio Networks," in 2012 International Conference on Advances in Mobile Network, Communication and its Applications (MNCAPPS), Pages: 60 – 63, 2012.

[33] A. Singh, and A. Sharma, "A Survey of Various Defense Techniques to Detect Primary User Emulation Attacks" in International Journal of Current Engineering and Technology, Vol.4, No.2 (April 2014).

[34] D. Das, and S. Das, "Primary User Emulation Attack in Cognitive Radio Networks: A Survey" in International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, No3, June 2013.

[35] S. Rajalakshmi, and K. Saravanan, "Survey on Link Layer Attacks in Cognitive Radio Networks", in International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3,No. 6,December 2013.

[36] V. Jayasree, and R. Suganya, "A Survey on Primary User Emulation Detection Mechanisms in Cognitive Radio Networks" in International Journal of Computer Trends and Technology (IJCTT), Volume 14, Number 2, Pages: 75-79, Aug 2014.

[37] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in Proceedings, IEEE Workshop on Networking Technology for Software Defined Radio Networks (SDR) 2006, Pages: 110– 119, September 2006.

[38] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," in IEEE Journal on Selected Areas in Communications: Special Issue on Cognitive Radio Theory and Applications, Volume: 26, Number: 1, Pages: 25–37, January 2008.

[39] Z. Jin, S. Anand, and K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in IEEE International Conference on Communications (ICC ' 09), Dresden, Germany, Pages: 1-5, June 14-18, 2009.

[40] Z. Jin, S. Anand and K. P. Subbalakshmi, "Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing," in ACM SIGMOBILE Mobile Computing and Communications Review, Volume: 13, Number: 2, Pages: 74-85, April 2009.

[41] Z. Jin, S. Anand, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in International Proceedings IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2008), Pages: 1–6, 2008.

[42] Z. Jin, S. Anand and K. P. Subbalakshmi, "Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks," in 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), Pages:1 – 5, December 6-10, 2010.

[43] Z. Jin, S. Anand, and K. Subbalakshmi," A NEighborAssisTed Spectrum Decision Protocol for Resilience against Primary User Emulation Attacks," in Stevens Institute of Technology, December 2009.

[44] Y. Tan, S. Sengupta, and K.P. Subbalakshmi," Primary User Emulation Attack in Dynamic Spectrum Access Networks: A Game Theoretic Approach," in IET Communications, Volume: 6, Issue: 8, Page(s): 964 – 973, May 22 2012.

[45] S. Chen, K. Zeng, and P. Mohapatra, "Hearing is Believing: Detecting Mobile Primary User Emulation Attack in White Space," in IEEE Transactions on Mobile Computing, Volume: 12, Issue: 3, Pages: 401 – 411, March 2013.

[46] T. C. Clancy and A. Khawar, "Security Threats to Signal Classifiers Using Self-Organizing Maps," in 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2009 (CROWNCOM '09), Page(s): 1 – 6, 22-24, June 2009.

[47] Y. Zhao, J. H. Reed, S. Mao, and K. K. Bae, "Overhead analysis for radio environment map-enabled cognitive radio networks," in 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 2006. SDR '06. Page(s): 18 – 25, September 25-25 2006.

[48] O. León, J. Hernández-Serrano, and M. Soriano, "Robust detection of primary user emulation attacks in IEEE 802.22 networks," in Proceedings of the 4th International Conference on Cognitive Radio and Advanced Spectrum Management, Barcelona, Spain, Pages:1-5, October 26-29, 2011.

[49] D. Pu, Y. Shi, A.V. Ilyashenko, A. Wyglinski, "Detecting Primary User Emulation Attack in Cognitive Radio Networks," in IEEE Global Telecommunications Conference (GLOBECOM 2011), Pages: 1 – 5, December 5-9, 2011.

[50] Z. Yuan, D. Niyato, H. Li, and J. Bin Song, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," in IEEE Journal on Selected Areas in Communications, Volume: 30, Issue: 10, Page(s): 1850 – 1860, November 2012 .

[51] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in IEEE 28th International Performance Computing and Communications Conference (IPCCC' 2009), Pages: 208 – 215, December 14-16, 2009.

[52] H. Li, V. Chakravarthy, S. intayehuDehnie, and Z. Wu, "Primary User Emulation Attack Game in Cognitive Radio Networks: Queuing Aware Dogfight in Spectrum," in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume: 105, Pages: 192-208, 2012.

[53] D. Hao, and K. Sakurai, "A Differential Game Approach to Mitigating Primary User Emulation Attacks in Cognitive Radio Networks,", in 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (aina), Pages: 495-502, 2012.

[54] H. Li, and Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics," in IEEE Transactions on Wireless Communications, Volume: 9, Issue: 11, Page(s): 3566 – 3577, November 2010.

[55] H. Li and Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems—Part II: Unknown Channel Statistics," in IEEE Transactions on Wireless Communications, Volume: 10, Issue: 1, Page(s): 274 – 283, January 2011.

[56] N.T. Nguyen, R. Zheng, and Z. Han, "On Identifying Primary User Emulation Attacks in Cognitive Radio Systems Using Nonparametric Bayesian Classification," in IEEE Transactions on Signal Processing, Volume: 60, Issue: 3, Page(s): 1432 – 1445, March 2012.

[57] R.W. Thomas, R.S. Komali, B.J. Borghetti, P. Mahonen, "A Bayesian game analysis of emulation attacks in dynamic spectrum access networks," in International Proceedings of IEEE International Symposium of New Frontiers in Dynamic Spectrum Access Networks, DySPAN (2008), Page(s): 1 – 11.

[58] X. Li, D. Wang, X. Mao, and J. McNair, "On the Accuracy of Maximum Likelihood Estimation for Primary User Behavior in Cognitive Radio Networks," in IEEE Communications Letters, Volume: 17, Issue: 5, Page(s): 888 – 891, May 2013.

[59] B. Canberk, I.F. Akyildiz, and Oktug, "Primary User Activity Modeling Using First-Difference Filter Clustering and Correlation in Cognitive Radio Networks," in IEEE/ACM Transactions on Networking, Volume: 19, Issue: 1, Page(s): 170 – 183, February 2011.

[60] F. Bao; H. Chen, and L. Xie, "Analysis of primary user emulation attack with motional secondary users in cognitive radio networks," in 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Pages: 956 – 961, September 9-12 2012.

[61] O. LeóN, J. HernáNdez-Serrano, and M. Soriano, "Cooperative detection of primary user emulation attacks in CRNs," in Computer Networks: the International Journal of Computer and Telecommunications Networking, Volume: 56, Issue: 14, Pages: 3374-3384, September 2012.

[62] X. Tan, K. Borle, W. Du and B. Chen, "Cryptographic Link Signatures for Spectrum Usage Authentication in Cognitive Radio," in Proceedings WISEC, Pages: 79-90, 2011.

[63] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in Proceedings of the 2010 IEEE Symposium on Security and Privacy, Pages: 286–301, 2010.

[64] S. Chandrashekar and L. Lazos, (2010), "A Primary User Authentication System for Mobile Cognitive Radio Networks," in the 3rd International Workshop on Cognitive Radio and Advanced Spectrum Management (COGART).