ISSN (Online) 2456-1290

International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)

Vol 6, Issue 5, May 2021

Primary User Emulation Attack and countermeasures in Cognitive Radio Network: A Survey

[1] P.Sharmila Rani, [2] Dr.R.Hemalatha

[1] Associate Professor, ECE, TKR Engineering College, JNTUH, Hyderabad, India
[2] Associate Professor, ECE, University College of Engineering, OU, Hyderabad, India
Email: [1] sharmilakanchi@gmail.com, [2] hemalatha.r@uceou.edu

Abstract--- **In the scenario of dynamic spectrum access in a Cognitive Radio Network (CRN), the authorized frequency is always used by Primary Users (PU) or Licensed Users (LU) and Cognitive Radio (CR) users can use this spectrum when licensed users are not utilizing it. In some cases, a complete similar kind of signal is generated by the attacker, and it looks like an error created by the Licensed User. So, the CR user is confused, and it erroneously detects the attacker as licensed user and immediately vacates the spectrum. This type of attacker is named as Primary user Emulation Attack (PUEA). Detection and defense of PUE attack, recognizing the interferences produced by the multiple PUEA to the PU and also to analyze the various problems arising in the data transmission are an important aspects in successful functioning of a CRN. This paper mainly focuses on PUEA and its defensive strategies in a CRN.**

Keywords--- **CRN, Licensed User, CR User, PUEA**

I. INTRODUCTION

The need for frequency bands is increasing rapidly due to the development of the wireless communication systems. However, most portion of the frequency spectrum is occupied by the present systems, and it is a limited resource. Therefore, the dynamic spectrum access in a CRN is essential [1]. Accessing spectrum dynamically is made possible by CRN. Spectrum sensing (SS) is the crucial activity at the CRN. If the SS is not performed accurately, then the Cognitive Radio (CR) and licensed user's performance will be degraded [2].

Usage of the spectrum can be increased by addressing lack of the spectrum. CRN is a feasible spectrum shortage problem solving option [4]. The CRN enables the sensing of CR user, the sensing of adaptive communication factors as well as the monitoring of inactive frequency channels, lacking interfering the Licensed User (LU) [4]. Because of the unpredictable nature of wireless communication, CRN can be exposing to multiple cyber-attacks and this gives a depressing crash on their execution. The attacks are PUEA [5], Spectrum Sensing Data Falsification (SSDF), jamming attacks as well as asynchronous sensing attacks [4].

The physical as well as Medium Access Control (MAC) layers of CR is threatened through PUEA attacks, and it is one of the CRN's biggest attacks. In a PUEA attack, the malevolent user copies the transmitting features of the LU, and the legitimate CR Users are confused by the actions of this mimic. This form of attack can cause disruptive interference to the LUs, and prevents the other CR Users from using idle frequency channels [5].

The successful realization of a PUEA in a CRN relies on many important factors, such as no interference among the major as well as secondary networks. Otherwise, a LU verification protocol may be configured to detect a PUE attack if CR user is allowed to share information with the LU. Signals of LU and CR user must have different properties i.e., different modes of modulation, and statistical signaling features. The PUE attacker exploits this to mimic the primary signal. Attacker can estimate the primary signal power level and also the channel conditions to generate trickier signals. Attacker prevents main-network interference.

The most proficient approach to identify spectrum gaps is to recognize the essential clients that are receiving information inside the SUs communication range. However, in reality, it is troublesome for a CR user to have specific channel data between a primary recipient and a transmitter because of the intrinsic property of CR. Subsequently, the latest work takes part in initial transmitter recognition based on the nearby perceptions of CR user.

II. PUEA ATTACT IMPACT ON CRN

In *Fig. 1*, a scenario of CRN Operation is illustrated. Main task of a CRN is Spectrum Sensing. Co-operative Spectrum sensing (CSS) can be centralized otherwise distributed. In Centralized approach, the decisions of all the CR receivers are collected by a fusion center and based on that, final decision is made whether spectrum band is free or not. In distributed approach, SU's share their information to form individual decisions, i.e. spectrum allocation and access are controlled by CR users. In the procedure of SS, if a PU starts to transmit over a particular spectrum band possessed by an SU, the CR user is preferably required to empty the spectral band quickly and consequently look for an empty band. But when there is no dynamic PU/LU action in the spectrum, every CR user can appreciate rise to rights to get to the vacant spectral band. For a CR user to increase rise to rights as the LU, the CR user imitates the qualities of a PU making the CR user carry on maliciously. The consequence of this is another CR user will decide the malicious CR user as a LU and empty the involved spectrum for the malicious CR user trusting it is an LU. Along these, the malicious client gets unique access to the spectral band of the LU.

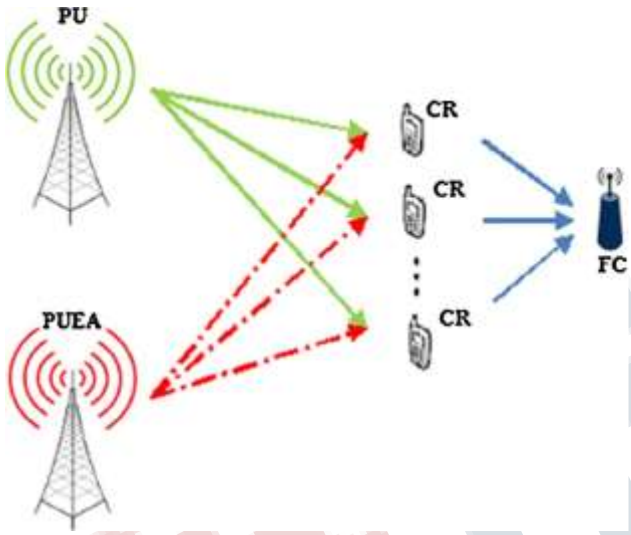

Fig. 1.Cognitive Radio Network Layout

In the dynamic spectrum get to condition, the LU dependably utilizes the approved frequency band, as well as CR users can use this spectrum band while LU is not utilizing it. In the presence of PUEA, it produces an entirely similar kind of signal as the LU to influence a mistake in the frequency band, as well as to complicate the SU. SUs wrongly decide the attacker as LU, and empty the spectrum band instantly. Correct decision by the SUs cannot be ensured dependably in all situations, especially, at the occurrence of PUEA, in that the attacker copies the signal qualities of the LU also transmits a related kind of signal.

CR users mistakenly recognize the aggressor as LU and abandon the authorized band. These activities incite underuse of spectral assets also produce interferences in the transmission of secondary data. During the SS process, new attacks have been presented, which are exceptional to CRNs, while malicious nodes utilize the weakness of the CR reliability problems to attack a CRN. The attack is dynamic as long as a system hub is acting in any of the attacker behaviour's and is influencing the system security.

A. Classification of Attackers

Now introducing various forms of PUE attackers linked to their classification criteria.

A *static attacker* has a set position which does not alter during the entire round of attacks. Location proficiencies, for instance, Time of Arrival (ToA) otherwise committed placing sensors may be used to decide the position of a static attacker. Due to the disparity between its position and that of the LUs a static intruder can be easily recognized. A *mobile intruder* can continuously adjust their location so it's hard to track and discover. In order to verify the presence of a mobile PUE intruder, a viable detection method is proposed in [6] which effort the similarities among RF signals as well as auditory knowledge.

A *selfish Attacker*/Greedy intruder tries to snatch the bandwidth for its own transmissions from legitimate CR Users. Upon discovery of an unoccupied spectrum unit, it will participate with legal Bands through copying the primary signal. If it is identified by valid CR Users and they detect the spectrum occasion through going backward to the band, then it takes towards depart that particular band. Nevertheless, a *malevolent attacker's* aim is to interrupt the legitimate CR Users dynamic spectrum exposure but not to manipulate the spectrum for their own communications. The malevolent attacker, being dissimilar from a selfish attacker, can mimic a primary signal in mutually an untenanted spectrum band also a band presently applied through legal SUs. If an intruder targets a band that is being used by a legal CR user, the risk exists that the CR user does not detect the signal; also thus intrusion happens among the intruder also the legal CR user.

A *power-fixed intruder* applies a fixed determine energy level, irrespective of the real transmission energy of the PUs also the radio situation around. Whereas the *power-adaptive attacker* will adjust its communicating energy along with the approximate transmission energy and channel parameters of the primary signal [7]. The intruder actually applies an evaluation method also a system of learning versus the valid CR user's identification. It is shown that this advanced attack capable overcome a simple strategy to protection which concentrates only on the established energy of signal.

B. PUE Attack Threats

There are a number of problems caused by the existence of PUEA for CRNs. The set of different impacts of PUEAs are:

Reduction in QOS: The emergence of a PUE attack could seriously degrade the CR network's Quality of Service by disrupting secondary network connectivity. For example, a malicious attacker might interrupt continuing services also force the CR users to update their current working spectrum bands continually. Frequent handover of spectrum would cause unsatisfactory delay and latency for secondary services.

Delay in service: Imagine PUE strikes with high attacking frequency; so several of the spectrum openings that be filled by attackers. The CR users would have inadequate bandwidth for their transmissions, so that will disrupt some of the CR user services. In some case, there might also be no channels for the CR network to arrangement a specific switch channel to transmit the regulator messages. Thus, the CRN will be halted; also it will not be capable to provide any CR user.

Wastage of bandwidth: The aim of implementing CR networks is to resolve the under-use of the spectrum generated by the existing strategy for fixed spectrum use. By accessing the "holes" of spectrum dynamically, the SUs can recover these otherwise wasted sources of spectrum happen. PUE attackers can however take the spectrum holes from the CR users, important to bandwidth waste from the spectrum once more.

Unreliable connectivity: If a PUE intruder targets a secondary service in real time also discovers no channel presented while conducting spectrum handoff, then the service has to be lost. Due of the existence of complex spectrum exposure, the secondary facilities in CRNs necessarily have no assurance which they will have secure radio resourcefulness. The existence of PUE attacks considerably enhances the unpredictability of CRNs connection.

Intervention with the primary network: If a PUE attacker is driven to take the CR user's bandwidth, there is a risk that the attacker may create extra trouble to the primary network. It arises while the attacker breaks to identify a PU. PUE attack, the real LU can also be misidentified as the intruder as well as interferes with the primary network function. in any event it is strictly prohibited to reason intervention with the primary network in CRNs.

C. Defence methods at various protocal layers

Active counter-measures may be in use at dissimilar layers of the transmission strategy load to protect against PUE attacks.

Physical layer: To cope with the expected interference beginning malevolent PUE attackers, physical-layer strategies for example source isolation, signal design, spread spectrum as well as directional antennas may be engaged. The key to designing an effective physical-layer counter-evaluate is to develop the theoretic information of the primary signal's features also its distinction through the intrusion signal.

MAC layer: Radio Resource Management (RRM) techniques, for example, spectrum scheduling, spectrum handoff also admission control would be explored to enable the SUs to preserve acceptable Quality of Service (QoS) performance.

Network layer: A location based cognitive routing technique may be used to handle PUEAs until the location of PUE attackers is estimated. End-to - end routing lacking journey the inaccessible CR user nodes should be created.

Cross layer: A cross-layer architecture system for defending against PUE attacks can be put in place. The activity of the identified PUEAs is noticed in the physical layer, also recorded to the upper layers, for instance, the MAC layer RRM method or the network layer routing mechanism. In the physical layer even the undetected PUE attacks may be calculated by taking into account the theoretically derived probability of detection. The upper layer control parameters are mutually optimized for the presence of PUEAs.

III. PUEA DETECTION METHODS

Security problems in CRNs have become threats that cannot be ignored, also however to address safety issues has suit a hot spot for research. Safety risks are mainly correlated with two cognitive radios' fundamental characteristics: cognitive capacity and re-configurability. The cognitive ability risks menaces comprise attacks through opponents which imitate primary senders also the communication of incorrect spectrum-related reflections. The main technology for addressing security threats is therefore SS, counting sensing of licensed users and detection of Attackers. If the licensed user signal is accurately discovered, it offers a means of separating the intruder signal from it. By observing its signal characteristics, primary signals can be accurately defined. SS strategies are introduced to detect the existence of the signal being transmitted also to identify the kind of signal. In this paper, three main types are discussed.

A. Energy Detection

Energy detection, with less calculation also execution complications, is the majority popular signal detection method. To detect signals from the spread spectrum it does not necessitate extensive information of the consumer's primary signal and particular intentions. The signal is detected, established on a comparison among the energy detector yield and the defined licensed user threshold. The drawbacks of this approach are the collection of the correct recognition threshold, the incapability to separate the exploded intrusion from the signal as well as noise of the primary consumer and the low signal to noise (SNR) values . Abundant research can be carried out on these challenges.

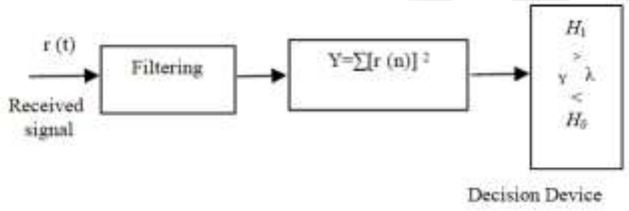

Fig. 2. Energy Detection Process

It is the majority generally utilized mechanism due to its effortlessness also less overhead computation. The weakest thing is it's not doing well in low SNR conditions.

B. Feature Detection

The identification of features stems from the basic characteristics of the regulated signals emitted through licensed users. In certain events, signals have episodic statistical characteristics including inflection rate as well as carrier frequency that are typically represented as

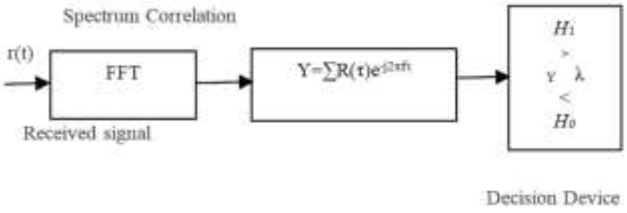

Fig .3. Cyclostomata Feature Detection process

cyclostomata features. In recognition, the cyclostomata gathering of a licensed user's signal may be eminent since noise in its arithmetical attributes, for example signify also autocorrelation. The detection process in this method is not prone to noise instability compared to energy detection, so it has greater strength in small SNR conditions.

This approach therefore needs extra detailed knowledge on the licensed user signals to assess licensed user's occupancy. As the result, characteristic recognition has a lot superior difficulty.

Cyclostomata detection can distinguish noise from licensed user signals, as well as may be utilized to efficiently identify the various cases of communications also licensed users. The key downside for their implementation of the cyclostomata function is its computational complexity.

C. Matched Filter Detection

Matched filter detection is an optimized mechanism of detection established on the licensed user's signal being preceding information for the secondary applications. The benefit of matching filter recognition is the short period needed to attain a confident possibility of misdetection or fake alarm.

The matched filter needs less signal samples that enlarge with low SNRs as for a objective possibility of fake alarm. Thus, SNR wall exists in matched filtering system. In addition to this, matched filter detection involves demodulation of the received signals. Perfect information of the licensed users signal is required, so a sensing unit's implementation complexity becomes impractical.

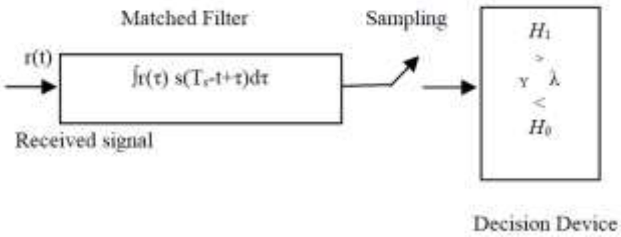

Fig. 4. Matched Filter Detection Process

Wave-form-based recognition is introduced to enhance the solution of the SNR wall problem when the numbers of samples are more. However, knowledge on the forms of the licensed user's signal is a precondition for waveform established recognition, thus reducing the difficulty of execution is silent a clear challenge. When the transmitted signal is known it is the best approach for detection. The key benefit of equated permeating is the limited period needed to attain a convinced possibility of fake alarm or neglected recognition equated with other mechanisms. It needs ideal information of key signal characteristics including bandwidth, functioning frequency, kind as well as order of modulation, pulse determining, frame size, etc.

IV. SOLUTIONS TO DEFENCE PUEA

In section III, licensed user detection methods are introduced, i.e. a CR user may use different methods to detect the licensed user's existence in the spectrum, for example energy recognition, matched filter detection as well as cyclostomata purpose recognition. Malevolent users are deliberately seeking to disrupt the networks instead of their have use.

Attacks of these types include mainly: Licensed PUEA which mimicker sitting signals to case Denial of Service (DoS) attacks, in disseminated networks. They may cooperatively disseminate false incumbent signals, causing a cognitive user jump of band-to-band as well as seriously interrupting their service. Most of the protection contributions suggest appropriate strategies for detecting malicious users, without having to change the incumbent signal. Moreover, some contributions presume that the primary transmitter location is identified and also in defence against licensed user emulation attack.

A Cooperative SS method with the occurrence of PUEA. This article introduced an attack-aware threshold selection technique based on CSS. As a countermeasure against PUEA, a suitable safeguard technique was introduced that evaluated two attack factors, possibilities of the nearness of a PUEA spurious signal in the nearness as well as absences of authorized PU signal, and connected to decide the ideal limits that limit the aggregate mistake possibility. Through the proposed strategy, less mistake possibility in the discovery of PU is acquired. It also noticed which while the normal signal noise ratio in CRN clients got from PU and PUEA are indistinguishable. The introduced approach enhanced the function of the CSS execution. The outcomes asserted the adequacy of the presented method contrasted with the established strategy.

Ta et al. [8] exhibited an entire performance about PUE assaults, from the attacking standard as well as its effect on CRN systems to the sensing and prevention accesses. For securing the CRN systems, a database- helped sensing mechanism also an affirmation control-based guard mechanism was proposed against PUE attacks. Multi-edge quick energy discovery and unique finger impression-based position confirmation are incorporated also repelled through a two-level database. Moreover, a confirmation control-based guard mechanism was introduced to ease the effect of PUEAs on the execution of CRN systems. During allowing a bit of channel for the hand-off benefits, the losing rate instigated by PUEA could be lessened. demonstrative outcomes showed that the presented reorganization as well as prevention mechanisms are powerful in finding also protecting against PUEAs in CRN systems.

Muñoz et al. [9] discovered an update power allotment approach for double threshold-based SDF with the consideration of PUEA. Primarily, the authors have deduced the problems which happen owing to the attacker that were then prepared as the restraints when developing the Energy Efficiency (EE) maximization issue. The introduced resolution mechanism initiated with the valuation of the maximal and minimal amount of CR users necessitated to attain the highest throughput. Then, an effective technique was introduced to choose the desirable CR users meant for SS also data communication. For minimizing the false alarm probability, sensing period was measured. Novel Adaptive Resource Allocation (NARA) technique. NARA technique, in that every CR user was adaptively allotted with dissimilar communication power levels to receive maximal system throughput (ST), minimal power utilization with entirely operated energy regrowth also evading intrusion to the LU. The function of the presented method was equated with the other existing approach also measured over dissimilar factors.

Pu et al. [10] proposed a distributed PUEA sensing technique, where every node identifies the energy levels across the spectrum. This method did not necessitate whatever specific hardware or software as well as can be used in mobile senders including nameless coordinates. The efficiency of the proposed approach has been demonstrated by numerical tests and computer simulations regarding the hardware implementations.

A spectrum access performance which determines the optimal communication mechanism of CRN. This method developed the optimal communication tactic issue into a class of optimization difficulties. In special, by considering the PUEA, the optimal spectrum access purpose was deduced. The introduced mechanism was examined numerically, also it was illustrated which it is of benefit throughout established energy reorganization regarding attaining secondary throughput also sensing precision.

Ali and Nam [11] proposed a method which is mainly involved in CSS, optimally with the objective of minimizing the supervising mistake possibility in the existence of malevolent users. As an initial part, this article proposed to set factor K in the long-familiar K-out-of-N vote find to minimize the CR possibility of fault. Secondly, the authors derived the amount of samples essential for energy recognition through reducing the possibility of fault per CR user. Lastly, the recognition threshold to minimize the fault possibility. The authors proposed at minimizing the possibility of mistake by optimally deducing type factors concerned in SS. additional accurately, this paper deduced optimal conclusion selection law, the amount of optimal examples as well as the recognition threshold to decrease the possibility of mistake in the occurrence of PUEA. The imitation outcomes suggested the advantage of the planned mechanism equated with the non-optimal current spectrum observing which do not think the occurrence of the PUEA in its recognition preparation.

Li et al. [12] proposed an Energy based recognition can be passed out in both the period as well as frequency domains. If every CRN sense the spectrum independently, the supervising procedure may not be dependable owing to signal fading also the less Received Signal Strength (RSS) that outcome in the hidden node difficulty. In the CSS procedure, several CR users cooperate with every other. Therefore, in CSS, this hidden node difficulty was resolved through attractive the benefit of collaboration between multiple CRs. In CSS, the last conclusion concerning spectrum access was depended on the fusion of sensing data transmit through several SUs to the Fusion Centre (FC). This procedure was either approved out through regular data FC or via each CR user in a dispersed technique. In central CSS, every CR user transmits its noticing outcome to FC that next merges the outcomes from entire CR’s as well as creates a last conclusion on whether LU was there or not. In disseminated CSS, every CR user exchange its limited SS outcomes with other CRs. therefore, every CR carried out the performance of FC also sense the spectrum also. In the central strategy of CSS, an FC may suit a single point of breakdown. Therefore, the disseminated strategy of CSS was favored more it. Because detection data was substituted between several CR users, it could guide to communication overhead. Even though CSS has an elevated possible to succeed, owing to the bendable as well as adjustable characteristics of CRs creates them a simple casualty of an attack like PUEA.

Chinnaiyan [13], proposed a CRN based on SS mechanisms for defining the free spaces in the spectrum vacant via LUs. An aggressor can exploit this highlight by miming the LUs signals as well as executes PUEA also keeps the CRN shape using the free spaces. In this article, the issue of PUEA was illuminated utilizing collaboration between the CRN users because of Time-Difference-Of-Arrival (TDOA) confinement strategy, wherever the area of the LU is recognized as on account of TV sender. The area of the electrode was estimated also contrasted and the situation of the TV tower to recognize possible attacks. At the time of spectrum detecting process, the signal is recorded by each CR user and sent it to the CRN base station, which inferred the TDOA estimation by utilizing cross connection techniques. The Particle Swarm Optimization (PSO) calculations approaches were utilized to limiting the nonlinear minimum squares cost, and these methodologies were created by changing the dormancy weights and speeding up constants of the PSO. The best PSO strategy was contrasted with the Taylor arrangement strategy. The introduced strategy got a low junction period also great exactness.

TABLE I. COMPARISION OF DIFFERENT METHODS TO DEFENCE PUEA

S.NO	Methods	Contributions	Simulation Results	Drawbacks
1	Methods	Minimizes total error probability	Total error probability reduced to 0.1	Under low SNR situations the function of the introduced approach was not efficient.
2	Attack-aware threshold selection approach	Dropping rate of CR users minimized	Probability of PUEA detection is about 0.93, 0.95, and 0.97 from various locations.	Proposed method efficiency was low in low SNR conditions and Cannot easily recognize the noise signals.
3	Database-assisted detection strategy also an affirmation control-based guard strategy	Selection of reliable SU’s and minimizing the total power consumption	System throughput is maximized by reducing total power consumption.	Applicable only for network layer and did not consider the attacks in other layers.

4	Double threshold detection scheme Novel Adaptive Resource Allocation (NARA) algorithm.	Did not necessitate any specific hardware otherwise software also able to use in mobile senders including unidentified coordinates.	Percentage of PUEA detection is around 180-200%	Did not address the problems related to the node selection in the CRN.
5	Distributed PUEA detection algorithm	Higher feasible secondary data rate and higher probability of detection.	Data rate and P_d of PU are of higher values compared with conventional method.	Did not address the interferences proposed to the PU in the SS
6	Spectrum access function for optimal transmission strategy of CRN networks.	Minimum CR probability of error.	Possibility of error in detecting PU in existence of PUEA is around 0.1.	Did not believe the effect of multiple smart malevolent users in the spectrum sensing process.
7	Optimal Cooperative Spectrum Sensing using K-out-of-N voting rule.	Energy consumption, Throughput and Dropping rates are measured.	For an SNR of 12, the System throughput is 12.35Mbps, more than conventional method.	Did not consider the network topology impacts also the cooperation among the system performances with SUs.
8	Energy based detection in both the time and frequency domains	Low convergence time and High exactness	The PUEA detected with higher accuracy and low convergence time of 267s	Did not address the problem created by the multiple PUEA.
9	PSO approach was contrasted with the Taylor arrangement strategy	Suppressed damage done to the SU throughput from PUEAs	SU throughput is above 1.4 bits/s/Hz against PUEA SNR	Future scope objectives at studying same difficult for smart PUEAs, numerous PUEAs as well as objectives to revise the intrusion induced to PU through PUEA.
10	Nelder Mead Simplex Algorithm	Higher possibility of recognition, low possibility of miss recognition also fake alarms, in the dissimilar environment.	Obtained Higher $P_{d,}$ lower P_m and P_f compared with conventional method.	Did not provide the details about cooperative sensing at the time of Multiple PUEA attacks.

Shivanshu et al. [14] discussed redesigning of the CR user throughput maximization scheme under PUEAs, Suppressed damage done to the CR user throughput from PUEAs. An optimally weighted CSS has been proposed to serve that purpose. The optimum weights are obtained by optimizing the CR user throughput while shielding the licensed user (PU) against interference in a PUEAs-facing network. Given the importance of simplicity and speed in CSS, Nelder Mead Simplex Algorithm was applied to solve the problem. The goal of future research is to study the same problem for smart PUEAs, several PUEAs also review the PUEA intrusion.

Elghamrawy, S. M. [15] presented the SS in CRN in the present of malevolent users that compete the PU signals. These PUEAs diminished the efficacy of CRN function. A Genetic Artificial Bee Colony technique has been introduced to optimize the use of spectrum, via discerning among PU as well as PUEA. GABC merged the GA's benefits with the ABC algorithm to maximize SS lacking exceeds the local optimum as a result from GA application. GABC used two main preset thresholds to denote the occurrence of LU and PUEA. Additionally, four CR factors were regarded for representation of the solution. Results of the simulations illustrated which the GABC is additional resistant to PUEA attacks owing to its capability to have a high possibility of reorganization in comparison to the other commodious approaches of reorganization also achieve a low possibility of miss reorganization also fake alarms in the specific environment.

V. FUTURE CHALLENGES

In this article, the security issues of PUEA are explored in the CRN. However, the safety issues in the environment of CRNs are still in their inception phase and need a more detailed review by the community of research. In this segment, the focus and aspirations of the future pursuit within CRNs regarding security effect are addressed briefly.

- The key dispute behind SS that significantly cooperation sensing efficiency is the question of receiver ambiguity, at the state of channel fading as well as the thus known as hidden terminal problem. This motivates CSS at the time of PUEA as a promising technique for combating shadowing, multi-path fading, and so on.
- In this regard, the researcher's Concentration is less at low SNR regions.
- Proposed solutions are not feasible for CRN with multiple/smart PUEA attacks.
- A cross-layer architecture system for defending against PUE attacks can be put in place. The research can be carried out at different layers of communication. By considering the theoretically derived probability of detection, the unrecognized PUEA is evaluated inside the physical layer. The upper layer control parameters are mutually optimized for the nature of PUEA.

VI. CONCLUSION

In this paper, security problems in CRN are discussed, and focused in the important contributions on emulation Attack. Introduced PUEA in CRNs and techniques to defense PUEA in a cooperative spectrum sensing, looked into the latest countermeasures to protect cognitive radio network against PUE attacks. Further, explored the scope and challenges of the forthcoming development of CRN security problems.

REFERENCES

[1] Sureka, N., & Gunaseelan, K. "Detection& Defense against Primary User Emulation Attack in Dynamic Cognitive Radio Networks," IEEE Fifth International Conference on Science Technology Engineering and Mathematics, Vol. 1, pp. 505-510, 2019.

[2] Sharma, R. K., & Wallace, J. W. "Correlation-based sensing for cognitive radio networks: Bounds and experimental assessment," IEEE Sensors Journal, vol.11, pp.657-666, 2011.

[3] Ruslan, R., & Ab Rahman, N. M. "Performance Evaluation of Dual Diversity Cognitive Ad-hoc Routing Protocol (D2CARP) on Primary User (PU) Activation Time: A Simulation Approach," Journal of Computing Research and Innovation, vol.2, pp.26-36, 2017.

[4] Masonta, M. T., Mzyece, M., & Ntlatlapa, N. "Spectrum decision in cognitive radio networks: A survey," IEEE Communications Surveys & Tutorials, vol.15, pp.1088-1107, 2013.

[5] Chaitanya, D. L., & Chari, K. M. "Performance analysis of PUEA and SSDF attacks in cognitive radio networks," Computer Communication, Networking and Internet Security, Springer, Singapore, pp. 219-225, May 2017

[6] S. Chen, K. Zeng, and P. Mohapatra. "Hearing is believing: detecting mobile primary user emulation attack in white space," IEEE International Conference on Computer Communications, April 2011.

[7] Fassi Fihri, W., El Ghazi, H., Abou El Majd, B., & El Bouanani, F. "A decision-making approach for detecting the primary user emulation attack in cognitive radio networks," International Journal of Communication Systems, 32(15), e4026, 2019.

[8] TA. D. T., Nguyen-Thanh, N., Maillé, P., & Nguyen, V. T. "Strategic surveillance against primary user emulation attacks in cognitive radio networks," IEEE Transactions on Cognitive Communications and Networking, 4(3), 582-596,2018.

[9] Muñoz, E. C., Rodriguez-Colina, E., Pedraza, L. F., & Paez, I. P. "Detection of dynamic location primary user emulation on mobile cognitive radio networks using USRP," EURASIP Journal on Wireless Communications and Networking, 2020(1), 1-19, 2020.

[10] Pu, D., Aygun, B., & Wyglinski, A. M. "Primary user emulation detection algorithm based on distributed sensor networks. International Journal of Wireless Information Networks," 24(4), 344-355, 2017.

[11] Ali, M., & Nam, H. "Optimization of spectrum utilization in cooperative spectrum sensing," Sensors, 19(8), 1922, 2019.

[12] Li, K., & Wang, J. (2019). Optimal joining strategies in cognitive radio networks under primary user emulation attacks. IEEE Access, 7, 183812-183822.

[13] Chinnaiyan, R. "Reliable Constrained Application Protocol to Sense and Avoid attacks in WSN for IoT Devices" In 2019 International Conference on Communication and Electronics Systems, (pp. 1898-1901, 2019.

[14] Shivanshu Shrivastava, A.Rajesh,P.K.Bora "Defence against primary user emulation attacks from the secondary user throughput perspective," IEEE Systems Journal, vol.12, pp. 3767 – 3774, 2018.

[15] Elghamrawy, S. M. "Security in cognitive radio network: Defense against primary user emulation attacks using Genetic Artificial Bee Colony (GABC) algorithm," Future Generation Computer Systems, 2018.