Wireless Personal Communications (2020) 115:827–858
https://doi.org/10.1007/s11277-020-07600-y

Countermeasures for Primary User Emulation Attack: A Comprehensive Review

Nikita Mishra[1] · **Sumit Srivastava**[2] · **Shivendra Nath Sharan**[3]

Published online: 16 June 2020

Abstract
Cognitive radio (CR) is a flexible wireless network that can solve the scarcity and underutilization problem of the spectrum by permitting unlicensed users to access licensed bands. The dynamic nature of CR makes it more vulnerable in terms of security. This paper's emphasis is on the primary user emulation attack, which poses a severe threat to the spectrum sensing operation of CR. In this attack, a malicious user imitates the signal characteristics of a licensed user (primary user) to disguise its true identity. Although many survey papers enhance our knowledge of cognitive radio security, this paper is an attempt to culminate new findings with the old ones to keep up the pace of the research community. Finally, the paper summarizes with some recommendations and future strategies pertinent to energy-efficient and flexible security methods for next-generation wireless systems.

Keywords Cognitive radio · Primary user emulation · Security · Physical layer

1 Introduction

In the primitive years of radio spectrum, non-communicative RF energy based applications (oven, heating appliances to name a few) merely occupied the band until in recent times, incremental usage of communication based application compelled to create more space. The band regulations hence got modified by the international telecommunication union (ITU) and covered both energy and communication based applications. This worldwide regulation for such dedicated spectrum slot was majorly classified for applications in the field of industry, science and medical. Industrial Scientific and Medical (ISM) is a band which facilitates a free radio spectrum band in order to operate a cordless telephone, a Bluetooth device, a wi-fi, a garage door opener, an animal tracker or even a baby monitor. Due to phenomenal advancement in wireless technology, artificial intelligence, smart

✉ Nikita Mishra
nkthalia@gmail.com

[1] Department of Electronics and Communication Engineering, Manipal University, Jaipur, India

[2] Computer Science and Engineering, Manipal University, Jaipur, India

[3] Electronics and Communication Engineering, NIIT University, Neemrana, India

phones and the burst of social networking platforms (Instagram, Facebook, and Twitter), demand for the wireless network is increasing exponentially (Fig. 1).

Due to exponential demand, ISM band is heading towards a point of suffocation. Primitive allocation of spectrum and the governing policies has led to underutilized spectrum resources. Licensed users like television, cellular, and radio users are assigned a large spectrum portion which varies its operation (or is even turned OFF) with time and geographical location, resulting in underutilization or complete wastage of a limited spectrum [1–3].

To summarize, we work in an environment which is either congested at times or with no traffic at all. A study at Berkeley Wireless Research Center (BWRC) in year 2005 indicates that spectrum utilization is rising high at lower frequencies and dipping rapidly at higher frequencies [2]. The study indirectly supports the Federal Communications Commission (FCC) statement "the average utilization of numerous spectrum bands varies between 15 and 85% as most of them have been assigned through a fixed spectrum allocation policy, confined to specific geographical areas" [4]. As a result of spectrum scarcity and underutilization of spectrum at the same time, FCC releases analog TV bands known as white space (spectrum holes) for unlicensed users to cater to the congestion without disrupting the routine flow of traffic (licensed users).

A mechanism is desired which could supervise the overall traffic, allow unlicensed traffic to come in, ensure continuous smooth movement of licensed traffic (even in peak hours) without compromising on security. An intelligent radio tool referred as cognitive radio network (CRN) which works on dynamic spectrum scheme, envisages the emerging demands of users and efficient spectrum allocation [5]. There are two types of users in CRN: primary user/licensed traffic (PU) and secondary user/unlicensed traffic (SU). CRN uses artificial intelligence to assess all working parameter, observe, learn and dynamically accommodates new parameters without reducing the overall functionality or efficiency.

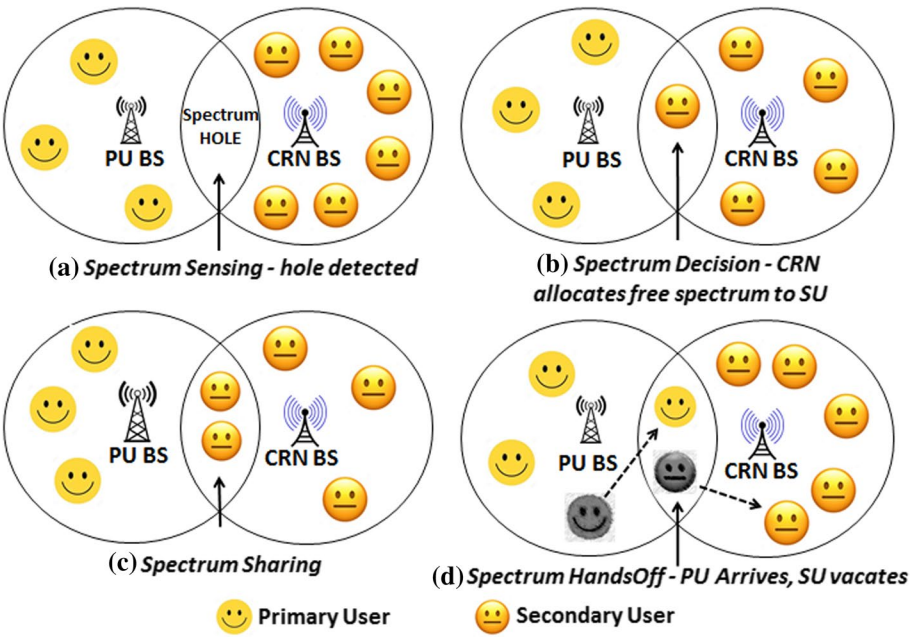

Fig. 1 Cognitive radio environment

Dynamic spectrum access is more vulnerable to security threats compared to a fixed spectrum allocation scheme. Cognitive radio faces security threats common to wireless networks affecting all layers of the protocol stack. In addition to this, CR is vulnerable to additional security threats due to its dynamic nature. Security is a serious threat as various attacks in cognitive radio occurs at different layers of the communication system. A cognitive radio monitors the spectrum using sensing ability and identifies spectrum holes. If results obtained after sensing the spectrum are not accurate, there is a possibility that secondary users may interrupt primary user transmission. Interfering with primary users leads to a violation of the FCC mandate: "There should be no modification or interference to the primary user transmission." And therefore primary user emulation attack (PUEA) is a significant threat to all the functions of CR [6].

In this attack, a secondary user behaves like the primary user by imitating its signal characteristics and forces secondary users to vacate the channel. The impact of this attack is the highest on spectrum sensing operation. Therefore security mechanism at the spectrum sensing stage should be dominant.

In the recent few years, there has been significant research on security threats and countermeasures in cognitive radio network. Overview of CR security threats, defense algorithms can be found in [7–11]. Although many survey papers enhance our knowledge of cognitive radio security, this paper attempts to culminate recent findings with the old ones to keep up the research community's pace. This survey paper aims to provide recent development towards security with more focus on PUEA countermeasures.

The paper is arranged in four sections. After a brief introduction, we have attempted to diagrammatically describe the basic operation of PUE attacker in Sect. 2. In Sect. 3, the principles and limitations of the PUEA countermeasures are explained. In Sect. 4, we describe unexplored areas related to the future development of cognitive radio security. Finally, in Sect. 5, the paper is concluded.

2 Primary User Emulation Attack

Primary user emulation attack is a significant obstacle to the spectrum sensing operation of CRN, which occurs at the physical layer of the protocol stack. A severe threat to spectrum sensing operation is to differentiate the primary transmitter signal from secondary user signals accurately. When the primary user reclaims the spectrum, the cognitive user leaves the frequency band and switch to another band for continuing its transmission [11]. A physical layer attack known as primary user emulation attack affects the spectrum sensing and other functions of the cognitive network. In this attack, a malicious secondary user imitates the characteristics of the primary user and behaves as a primary user to access the available frequency band when the primary user is inactive. The malicious user (MU) can force secondary user (SU) to vacate the spectrum by behaving as a primary user (PU). In this case, these attackers can occupy the entire licensed spectrum by themselves or waste the valuable radio spectrum [12] (Fig. 2).

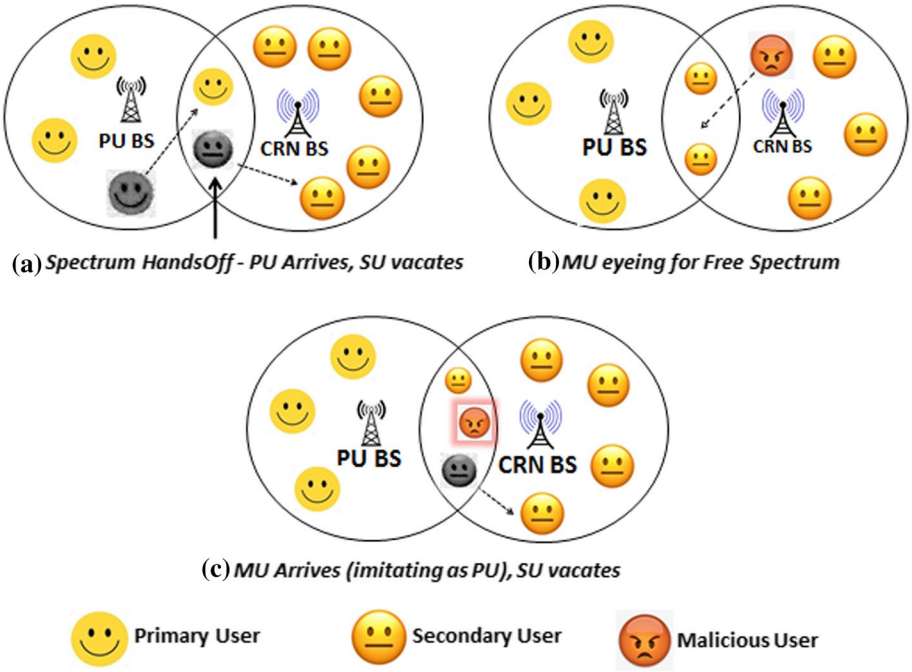

Fig. 2 Primary user emulation attack scenario

3 Countermeasures

Various defense mechanisms for the PUE attack have been introduced in the last 2 decades. All mechanism aims to achieve a common goal—enhanced spectrum management. Federal communications commission (FCC), an independent body that supervises communication regulations, has mandated "No interference or modification in Primary User transmission." Since a successful transmission in a CR network cannot supersede the FCC mandate, therefore, all Countermeasures for PUEA need to work within the specified compulsions of FCC, resulting in higher complexities in CR implementation.

All these strategies require a precise categorization of security methods to arrive at a holistic approach, which is robust enough to tackle various attacks. Existing countermeasures for PUEA are broadly classified under seven categories: (1) location and distance, (2) analytical model, (3) cryptography, (4) belief propagation, (5) wireless microphone, (6) game theory, (7) machine learning, (8) proactive MAC design and (9) blockchain for security in CRN against PUEA.

3.1 Distance and Location Based

Chen, Ruiliang, and Park presented the first method [12] for identifying a PUEA based on location and distance. This method uses a transmitter verification scheme to differentiate between signals from licensed user (PU) and secondary user (SU) imitating as a licensed user. A master location verifier (LV) and slave LV are two essential nodes in this process.

Master LV is equipped with a secure GPS to record the database of all TV tower coordinates present outside the cognitive radio network. The author makes few assumptions for the detection process: (1) all LVs need close synchronization and communication among each other through a common control channel. Master and slave location verifiers use identical radio propagation models. (2) TV broadcast tower is assumed to be a primary network with transmission range in tens of miles and output power in thousands of watts. Two tests conducted for verifying location of PU and MU.

1. *Distance ratio test* This method is based on the measurement of received signal strength (RSS) of the signal by LV with a cooperative distance ratio verification scheme. In each of the DRT iteration, RSS values measured by the pair of LVs are sent to Master verifier and compares the value with each TV tower coordinates from the database. If the signal received does not match with any of the existing TV tower coordinates, then location verification for the signal fails, and the signal is detected as an attacker.
2. *Distance difference test* This method uses the phase of a licensed signal measured by the master–slave LV pair to verify the transmitter location. Synchronized pair of LVs sends the time difference of the TV signal pulse and their coordinates to the master verifier. Once the parameters are received, the master LVs calculate the difference in distance using the time difference of signal and compare it with the entire TV tower database. If the received signal does not match with any of the existing TV tower coordinates, then location verification for the signal fails, and the signal is detected as an attacker.

Techniques mentioned above have certain limitations:

1. There is a need for tight synchronization between master and slave location verifiers in DRT and DDT, which makes the process expensive.
2. A large number of iterations required for DRT can increase system overhead.
3. False-negative ratio increases if there is less number of LVs.

The limitations of DRT and DDT [12], is addressed to some extent by Chen et al. in [13] by using RSS localization method. The primary signal transmitter's location is verified by measuring its location and observing its signal characteristics (carrier frequency, modulation frequency, power, e for this paper etc.). The localization technique collects synchronized RSS measurements with the help of wireless sensor network (WSN) attach to each secondary user. This RSS measurement helps in determining the TV transmitter location. Further, to distinguish between the primary transmitter and attacker, a comparison is made between measured RSS peak and TV transmitter location. However, the mechanisms described in this paper do not consider major aspects of the wireless channel: fading and shadowing. Also, the paper is limited to detection (and not mitigation) of the primary user emulation attack. Few drawbacks are associated with RSS measurements also as given below

1. The use of WSN makes the system more expensive and complicated.
2. The attacker's transmission power is assumed to be of constant magnitude; however, practically, it may differ.
3. Computation time is derived by the summation of the running localization algorithm and data collection by WSN. Due to the wireless sensor network, the delay could be induced in the network.

In [14], Rehman and Saeed have proposed to diminish PUEA in CRN by using radio-frequency (RF) fingerprinting. The work has explored the viability of applying RF fingerprinting through software-defined cognitive radios. The result shows that with high signal to noise ratio (SNR) at receiver end (in an ad hoc CRN), PUEA could be mitigated successfully. However the same technique may not yield similar results for a centralized network. The fingerprinting based solutions need large samples of data as well as extra storage, substantial computation with signal processing overhead. Also, damages in the low-end receiver affect the transmitter classification accuracy, and this accuracy differs across receivers. A slight improvement is seen in the outcome of false probability when RSS is combined with maximum likelihood estimation [15].

In [16], a wavelet transform (WT) method is used by Zhao and Caidan to distinguish between the primary transmitter and PUEA signal. To counter this threat, transmitter location fingerprints is extracted and analyzed in a multipath propagation environment. An assumption made to implement this approach is as follows. (1) The primary user transmitter location is fixed. (2) Primary and secondary users are low power handheld devices. (3) A verifier (secondary node) is used to distinguish between the primary transmitter and the PUE attacker. In this scheme, a verifier extract signal from the frequency band of interest using a bandpass filter. Then samples (transmitter location fingerprints) present in the time domain are converted into the frequency domain by power spectral density function. After that, the characteristics of transmitter fingerprints are extracted by the wavelet transform technique. Feature extraction is done by obtaining statistical parameters of the wavelet coefficient. The authors have considered a multipath fading indoor office situation with a time-invariant propagation channel to extract fingerprints of the transmitter. The real-time experiment is conducted at four locations using a spectrum analyzer and signal generator. This approach may identify the PUE attacker; however, mitigation of the attacker is again a limitation here. Since the primary transmitter location is fixed, it is not an efficient method for ad-hoc CRN or mobile PUs.

The location-based approach proposed by León et al. in [17] is a cooperation localization method suited explicitly for a centralized IEEE 802.22 network [39]. The primary objective of the IEEE 802.22 is to enable access to the vacant position (white space) in the digital television (DTV) channel. The CRN comprises of a base station (BS) and a batch of SUs with static positions (distributed arbitrarily in the network). This approach employs the time difference of arrival (TDOA) method to calculate the time observed by each node pair to distinguish between a PU and a bad secondary user (an attacker). This method needs tight synchronization between a pair of nodes. The base station in a database records the positions for all fixed PUs and SUs. SUs are used as anchor nodes to determine the location of the emitter signal. Secure synchronization is required between anchor nodes with stationary and known positions. All anchor nodes carry out spectrum sensing and send sensing results to the base station. If a primary transmission is sensed in submitted reports, the localization procedure is started by CRN to detect whether it is genuine or fake signals. The time to detect PU transmitter is bounded to 2 s (by IEEE 802.22). Location detection time in this method depends on following factors (1) time required by anchor nodes to measure and record primary user signal and send a recorded signal to the base station and (2) calculation time taken at the base station using weighted least square (WLS) and Taylor series (TS) estimation technique. TS estimation convergence depends on a reasonable guess of initial value; therefore, accuracy is low. This technique provides accurate results if there is cooperation between secondary nodes. If secondary nodes are compromised, they may provide incorrect results to the base station resulting in false signal detection. This method does not consider multiple attack scenarios.

In [18], the authors focus on two CRN attacks: spectrum sensing data falsification (SSDF) and PUEA affecting the centralized CRN network. A transmitter verification scheme (localization) is applied for PUEA detection. For the SSDF attacks, an optimum nonlinear cooperation framework is proposed to reduce the interference induced by the SSDF attacks. A secure distributed CR system is implemented where the fusion center decides for spectrum sensing after combining the results of individual SUs. The two-tier cognitive network is proposed: First-tier consists of a cluster of SUs. Second tier consists of relay nodes to process local spectrum sensing information from SUs and forwards it to FC in compressed form. The probability of false detection is shown through simulations for three different cases: No attacker, 2 SSDF attackers, and 2 PUEA attackers. This detection method needs extra relay nodes, which increases the possibility of infrastructure overhead.

A recent work [19] conducted by Adebo et al. is a combination of RSS and angle of arrival (AoA) location technique. This method measures (1) distance between SUs and transmitter (2) angle at which secondary user receives PUs signal (3) TV tower location is known. Therefore, the PU signal position determined by a hybrid technique is matched with the location of the PU to detect PUEA. This scheme is simulated with only two secondary users to estimate PUEA. A comparison is shown between the received signal strength (RSS), AOA, and hybrid localization scheme. This hybrid method requires only 20 iterations to converge, which is 30 iterations less than AOA and RSS. Whether the Hybrid work is suitable enough for a long communication range is still not covered. Hence the limitations related to RSS measurement may prevail in this scheme as well.

Another modified localization solution in [20] combines trilateration and RSSI technique with the Bayesian decision model with cost matrix involving conditional risk. Based on the estimated position of PUE by RSSI at the secondary node, the Bayesian model decides the legitimacy of the PU signal using the cost matrix. The conditional risk for each decision is calculated to reduced false alarm probability and increase the detection rate. The problem of localization of the PUE attack is reformulated as a multi-objective optimization problem, and game theory is used to solve it. This approach can be explored for other wireless communication applications as well.

In [21], another method for PUEA detection and mitigation by examining received signal power based on adaptive learning is proposed. The learning procedure implements cyclostationary feature analysis and distance variance estimation for differentiating malicious user and primary user in CRN. Through simulations in network simulator, it has been proved that the proposed learning method is stable, provides enhanced SU throughput with less time required for signal classification, and reduced miss detection probability. Hence this approach can detect attacks at different layers with minimum time for detection.

In most of the above solutions, static PU and MU is considered to implement the simulation. However, in practical scenario, location of PU, SU and MU is dynamic or mobile. Considering this aspect, a new detection scheme is designed for mobile primary users based on Kalman filter in [22]. In this model, the position of dynamic primary user is tracked, and the source of the incumbent transmitter is verified using a Kalman filter. Then, the free-space path loss model is used to calculated distance between the secondary node and the incumbent transmitter received power. If the difference between estimated distances is more than the predefined threshold, then it is assumed that signal is received from a malicious user, otherwise genuine primary signal. This result of the Kalman filter is satisfactory in a non-static environment and shows better than RSS based location method.

In [23], a combination of energy detection sensing and location identification is proposed to detect PUEA. This model depends on three major factors: energy detector with multi-threshold sensing, RSS Location verification, and the two-level database (local and

global). The local databank comprises of two components: RSS probability function and fingerprint data. Location details of PUE attacker, as well as primary user, are stored in the global database. The location verification technique identifies the originating source of the received signal coming from the PU or PUE attackers. Finally, the local and global database, RSS Probability function, and thresholds are updated.

In [24], a modified energy detection scheme is proposed for PUEA detection. A hypothesis problem is modeled representing three states of the channel: (1) idle channel, (2) channel accessed by PU and (c) channel attacked by malicious user. Energy statistics of SUs is extracted for accurate detection of PU and MU considering detection statistics and predefined threshold. Three values are set for threshold D0, D1, and D2. When energy statistics are less than D0, it is assumed that the channel is idle and can be accessed by genuine SU. When detection statistics are between D1 and D2, it is assumed that primary user accesses the channel, and finally, statistics higher than D2 indicated the presence of MU in the channel. This modified energy detection method is simulated with MATLAB software, and the accuracy of detection is computed.

Most of the existing literature on attack detection in a cognitive environment considers the location of the attacker fixed and only physical layer is considered. In [25], a cross-layer technique is applied for the detection of a dynamic attacker's location. A testbed of a mobile phone base station with software-defined radio is set up for real-time experimental validation. It combines energy detection, motion estimation, and information analysis at physical, MAC, user's application data, and PUE at motion. The experimental result shows that signal is detected with more than 93% accuracy and SNR equal to – 9 db (Table 1).

3.2 Analytical Model

There are few analytical methods for the detection of PUEA based on PDF of power received at secondary user interfaces.

An analytical model explaining the probability statistics of signal power received by SU (from both PU and attacker) has been described in this paper [26]. This method is a pioneer attempt to find the viability of PUEA using Fenton approximation (FA) and Markov inequality (MI). SU measures the received powers (from PU and MU), assuming Rayleigh fading and shadowing. If the difference between received powers at SU is less than a set threshold, the spectrum is considered as 'available' for SUs. However if the case is opposite, a decision is made to determine whether the signal is from PU or MU. Mathematical expressions are derived for computing (1) PDF of received power at SU due to PU and (2) received power PDF at SU due to MU. Subsequently, the FA method is applied to calculate the mean and variance of the power received. Eventually, lower bound probability of successful PUEA is estimated using MI.

There are a few limitations:

1. This analytical model cannot perform well in a highly dynamic environment. PU's location is assumed static and is known to all users in the system.
2. The assumption made does not work in a realistic hostile environment (1) transmission power of MU is assumed constant, and (2) SUs and MUs are uniformly distributed.

The extension of the above model is explained in [27]. The author explores the feasibility of PUEA using Fenton approximation (FA) and the Wald sequential probability ratio test (WSPRT). The simulation follows the same methodology of measuring powers

Table 1 Location and distance methods

Authors	Method(s)	Real time/Simulations	Limitations
Mishra et al. [9]	Distance ratio and difference test	False negative ratio is plotted with respect to measurement error assuming different location of primary user and attacker	Expensive, inaccurate Increased overheads Environmental variables excluded
Manesh and Kaabouch [10]	Wireless sensor network (WSN) RSS peak value	Localization error and computation time is plotted with respect to number of sensors from 100 to 10,000	High complexity High computation time Not suitable for LR communication
Thalia et al. [11]	RF fingerprinting	Real time experiment using universal software radio peripherals	Huge sample size Not suitable for centralized CRN
Chen and Park [12]	Wavelet transform method	IEEE 802.11b, using ITUR M.1225 tapped-delay line model for indoor office	Computationally intensive
Chen et al. [13]	Cooperation localization Time difference of arrival	Simulation result show how SNR and number of anchor nodes affect the accuracy of location estimator	TS estimation is highly dependent on initial value guess
Bouabdellah et al. [15]	RSS + AOA (angle of arrival)	Hybrid scheme is compared with RSS and AOA localization scheme with respect to root mean square error (RMSE)	PUEA not verified for more than 2 SUs May not be suitable for long range communication

and finding mean and variance through FA. However, instead of MI author uses WSPRT (hypothesis testing) to detect PUEA (H0: PU, H1: MU). The simulation result shows that (1) SU receive more power from attackers as compared to PU, if MUs are too close to SUs. In this scenario, the probability of false alarm as well as miss detection rises. (2) If MUs are too far from SU, false alarm and miss detection probability reduces. Limitations of this approach:

1. Uniform distribution of SU and MU still exists. Moreover, MU's transmission power is constant, and PU's location is static; both may differ in a realistic scenario.
2. A huge sample size and enormous testing time may only provide accurate results.

To achieve higher efficiency [28], the same author compared Neyman–Pearson composite hypothesis test (NPCHT) with the results of Wald's sequential probability ratio test (WSPRT). The simulation follows the same methodology of received signal power measurement and calculating mean and variance through FA. However, instead of WSPRT author has used NPHCT to detect PUEA (H1: PU H2: MU). The simulation result shows that the WSPRT achieved almost 50% reduced detection of PUEA compared to NPHCT; however, at the cost of an enormous sample size and enormous testing time.

Similar to [28], the power received at SU is statistically analyzed in [29]. This work uses channel transmission characteristics and received power probability density function at SUs. The author of this paper proposes a variance method to resist attackers and compares it with a naïve detection method, which is based solely on primary user power. An advanced attacker is designed, which may have variable transmitting power, knowledge of path loss exponent, and variance of SUs. A maximum likelihood estimator and mean-field approach are used by the attacker to infer the transmission power of the primary user and produce primary user emulated signals. The author significantly claims that the attacker can imitate various primary user signal characteristics except for the communication channel feature. However, these claims are under various assumptions like distances between SU and PU, the attacker and PU and the SU and attacker are known. The attacker's known location is another assumption that is not suitable in a real environment.

3.3 Cryptography

Post limitations of location and PDF-based countermeasures, researchers have explored cryptography to detect and mitigate PUEA. Authors have used channel impulse response and cryptographic techniques to determine the location of a primary transmitter (Table 2).

The author in [30] proposes a scheme based on the amalgamation of wireless link signatures and cryptography generated from channel impulse response. A helper node (HN) is positioned in close proximity with primary user at a constant location. HN acts as a signal messenger to SU, enabling SU to learn the signatures (both link and cryptographic), thus allowing SU to confirm PU's authenticity. The helper node transmits cryptographic signatures to SUs using channel assigned to its PUs (when the channel is idle). The attacker may copy PU signals and send false signals to the target channel. Finally, the helper node differentiates between PU signals and SU imitating PU signals.

In [31], a cryptography-based method modified by a DNA algorithm is proposed. Authors focused mainly on two aspects: (1) a new member is added in the cognitive group only after integrity verification. Data encryption is performed between spectrum manager and CR for secure transmission. (2) A reliable node situated in close proximity

Table 2 Analytical model

Authors	Principle(s)	Real time/simulations	Limitations
Zhao et al. [16–18]	Fenton approximation (FA) and Markov inequality (MI)	Simulation results are plotted for successful PUEA lower bound probability with respect to varying distance between PU and SU	Uniform distribution of SU and MU MU's transmission power constant
	Fenton approximation (FA) and Wald sequential probability ratio test (WSPRT)	Probability of false alarm and misdetection with respect to threshold value.	Same as above Huge sample size Long sensing time
	Neyman–Pearson composite hypothesis test (NPCHT)	Misdetection and false alarm probability for WSPRT and NPHCT	Same as above Reduced efficiency compared to WSPRT
Adebo et al. [19]	Variance detection method	Simulations result shows receiver operating characteristics of variance detection method and Naïve detection method	Assumptions made are unrealistic (Distance between PU, SU and MU are known)

with PU location detects and mitigates PUEA. When the spectrum is idle, this node sends a DNA algorithm based authentication tag to the CR. Information received by the CR without the authenticated tag is discarded and reported to the spectrum manager. Further, a malicious node is search by spectrum manager distance measurement and is removed from the cognitive group. Simulation outcome shows a comparison of detection probability with and without authentication tag. In order to make out if the signal is from PU or an attacker, a helper node equipped with amplitude ratio of multi-path element (AR) is developed. This is a physical layer authentication approach. A helper node can calculate AR using channel impulse response and compares it with the set threshold. If AR is greater than threshold, the received signal is marked as PU signal else it is considered as attacker signal and gets discarded. The efficiency of this approach is presented by mathematical modeling in terms of false-negative probability (attacker misinterpreted as PU) and false alarm probability (PU misinterpreted as an attacker). There are few drawbacks associated with this work:

1. It is assumed that an attacker's transmission power is much higher than PU's transmitting power.
2. An attacker cannot be close to PU.
3. It is assumed that an attacker cannot compromise the helper node, which is a possibility in a real scenario.
4. A security mechanism is required between helper nodes and secondary users to avoid the possibility of an attacker modifying messages.

The author in [32] illustrates denial of service (DoS) existence considering DSA network architecture as per standard IEEE 802.22. This approach is based on four elements: A certification authority (CA), PU, SU, and secondary base station (SBS). A public key cryptography is adopted where a PU encrypts the data (before transmitting) with digital signatures. A current timestamp, private key, and PU ID are used to generate digital signatures. SU continuously scans the spectrum in the sensing period for digital signature. The SU detaches the signature from the PU data unit once a signal is transmitted through the channel and forwards it to the base station for verification. The certification authority maintains a database of public keys used by PUs in a confined geographical space. A BS and a CA uses its database to confirm if the received signature is of PU or an attacker. If the existing public key does not decrypt the signature, it is considered as an attacker and discarded from the database. Thus, this method can successfully detect and mitigate MU from the network with few limitations as stated beneath.

1. Attaching a signature with PU transmission violates FCC rule (no modification or interference to PU transmission).
2. Infrastructure is costly for a substantial geographical area.
3. The complete detection and mitigation process depends on CA. IF CA fails or compromised, the entire system goes down.
4. If fake signals are sent by MU continuously, it can trench network resources badly. This would lead to congestion of the common control channel and making the secondary network inoperable.
5. For the encryption scheme, SU must exhibit capacity to synchronize and demodulate primary signals.

Another defense approach build on hash message authentication code is implemented [33] by the author, in which a key is shared between PU and SU. The shared key is attached to the message with a tag before transmitting it to the receiver. At the receiver, a SU regenerated a tag using a hash function and shared key. If the transmitted tag matches with the received one, it is considered that signal has arrived from PU; else it is attackers signal. This process is productive, but there are few limitations which makes it inapplicable

1. Bandwidth efficiency is degraded.
2. Noise sensitive method and adds attenuation to PU signal.
3. This process is useful, but modification in PU transmitter may disrupt the synchronization between the transmitter and receiver. It reduces coverage area of the primary network and violates the FCC statement ("no modification to the primary user system is mandatory to allow the opportunistic use of the spectrum by secondary users").

In [34], an advanced encryption standard is used for PUE detection. In this method, digital TV or PU transmitter sends a reference signal (RS) that works as segment synchronization bits of digital TV data frames. RS is created by following two steps—Step 1: generating a pseudo-random sequence (PN); Step 2: advanced encryption algorithm (AES) encrypting the PN sequence. For robust security, a 256-bit secret key (SK) is applied in Step 2. RS is regenerated at the receiver (by the virtue of shared SK amid receiver and transmitter) to achieve an accurate identification of PU and MU. To validate a PU signal, a comparison is performed by correlating the RS and the received signal with a set predefined threshold (T). If comparison yields a value higher than or equals to T, PU's presence is confirmed else the PU is absent. Malicious user (MU) is detected by evaluating the autocorrelation of RS. The detection performance for MU and PU is gauged through a false alarm graph and probability of miss-detection. Four hypotheses model for detection is formed: (1) H00: MU is absent given that PU is absent (alpha = 0); (2) H01: MU is present given that PU is absent (alpha = 0); (3) H10: MU is absent given that PU is present (alpha = 1); (4) H11: MU is present given that PU is present (alpha = 1).

Limitations of the AES method:

1. Plug-in AES chip is needed, which increases the cost of the process.
2. It is a symmetric key algorithm; the key needs to be shared with each recipient.
3. Due to key size (256), excessive time is required to encrypt and decrypt messages, which can hinder effective communication and upsurge overhead time (Table 3).

3.4 Belief Propagation

After location, distance analytical, and cryptography based methods, there was a strong need to develop a robust algorithm. Researchers proposed belief propagation claiming that this algorithm is more effective than localization and cryptography. Yuan and Zhou described the belief propagation algorithm [35] and Markov random field (MRF) for the detection and mitigation of PUEA. SU obtains the received signal strength measurement (RSS) to identify the location of the PU transmitter. Each SU compares the known location of PU with the received signal and computes its probability (of MU or PU)). The probability calculated by each SU is denoted as belief or messages. When a signal is received by cognitive radio network, SUs exchange belief with each other in the form of messages in an iterative mode. When all the beliefs are exchanged from all the secondary nodes, the

Table 3 Cryptographic based detection technique

Authors	Principle	Real time/Simulations	Limitations
Fassi Fihri et al. [20]	Link signatures channel impulse response	Experimental evaluation using USRP with GNU radio	Use of extra helper node An unrealistic assumption that attacker cannot be close to PU physically
Arun and Umamaheswari [21]	Cryptography used as digital signatures	A centralized dynamic spectrum IEEE 802.22	Violates FCC mandate A secure certificate authority is needed High computational complexity
El Mrabet et al. [22]	Hash message authentication code (HMAC)	Probability of false alarm is plotted against signal to noise ratio (SNR)	Bandwidth efficiency is degraded Decreases primary network coverage area Violates FCC rule
Selvapriya et al. [23]	Advanced encryption standard (AES)	False alarm rate and Miss detection probability is shown	Plug in AES chip is needed Large key size Time consuming

mean of final belief is computed. If this mean is lower than the set threshold, the incoming signal is considered as PUEA; else, it is an honest SU seeking spectrum. Subsequently, all the SUs in the network are informed about PUEA signal characteristics (broadcast) so that it can be circumvented in the future. There is a need for almost 8 iterations to complete the iteration process.

Limitations of this BP in terms of CR security are:

1. Cooperation between secondary users becomes challenging due to high computation complexity of local and compatibility function.
2. With rise in number of SUs, algorithm scalability and accuracy decreases.
3. The PUs position is known well in advance.
4. When the distance between MU and PU is less, firmer belief is achieved as the probability of suspecting a PU is higher.

Belief propagation approach is extended further in [36] as an effort to lessen the number of iterations and computation time. In the previous attempt, BP algorithm required approximately eight iterations before converging to a final belief. However, in this work, the new BP method has redefined protocol for ex-changing messages, and the method is modified to compute more straightforward beliefs at each SU. Modified BP method can detect and mitigate PUE attackers in a single iteration, and results are equally accurate as they were in the former approach (eight iterations). A BP framework based on pairwise Markov random fields (MRF) is exploited to achieve high accuracy and scalability. The location of the PU transmitter is recognized by using power observation at SU relatively. A comparison of computation time is made for both BP algorithms [36]. Results show that computation time is directly proportional to the number of SUs for both approaches. Limitations of this modified BP algorithm are:

1. When the distance between PU and MU reduces, mean of final belief is affected.
2. If secondary users are compromised, inaccurate results are produced.

3.5 Wireless Microphone

This work describes the detection of emulation attacks when the primary user is mobile. Wireless microphone (WM) and TV towers exist in the same white space. Wireless microphone location is not stationary, and its transmission power is also low. This property makes detection of attack difficult compared to stationary users. In [37], a novel experimental method is described to spot wireless microphone emulation attacks (WMEA).

In this paper, a real-time experiment is conducted to detect PUEA for wireless microphones, which is authorized to operate in TV bands. White space consists of TV towers and WMs. The relation amid received RF signal energy level and audio information received from the sensors (attached to the SUs) is exploited to verify the authenticity of PU. Ambient Noise mitigation of the experiment is done using collaborative sensing. The communication range of the WM radio frequency signal is < 100–150 m. The relationship between signals received by the SUs and the sound sensors output is calculated. If the received signal does not match the correlation test criteria, WM emulation attackers are assumed to be present. According to the IEEE 802.22 standard, sensors should be capable of identifying wireless microphone signals over 200 kHz bands within 2 s with both misdetection and false alarm probabilities < 0.1. So timing is an essential parameter in emulation

attack detection. A spectrum analyzer is used to measure RF signals power [38, 39]. The detection time of this method is approximately 3 s, which can be further reduced. SUs are equipped with extra sound sensors; therefore, if the number of secondary users increases, sound sensors also increase, making the system complicated and expensive. Nevertheless, this is a unique literature based on wireless microphones in a cognitive radio network. Therefore, there is a need for useful implementation of robust methodologies applicable for both stationary and mobile PUs and hence enhancing CRN security.

3.6 Game Theory

Game theory (GT) comes up with a mathematical model for analyzing the strategic interaction amid multiple decision makers. It is an emerging and effective structure for designing the CRN security mechanism to compute interactions among rational entities with conflicting interests. A classic multi-user game comprises of three elements (1) active users known as players (2) actions taken by the active users known as strategies and (3) outcome of the players based on the adapted strategies known as Payoff/Utility [40–43].

The author in [44] has adopted GT for PUEA detection using Nash equilibrium. A dynamic non-cooperative multistage game is developed between SUs and attackers. It is a two-player game in which both the players are rational and having conflicting purposes. SU strives to use an idle frequency band without intruding PU transmission, whereas MU makes an effort to acquire entire bandwidth by pushing SU out. It is assumed that the schedule of primary user arrival is unknown to both secondary and malicious users. Thus both users learn and build a probabilistic model to acquire the knowledge of PU arrival. Further, to know more about the state of PU, a Belief updating system is applied for SU. This system helps in fine tuning the strategy smartly and defends malicious attacker. In comparison with the other models, simulation outcome exhibits that the belief updating system attains better results in terms of considerable payoff and provide more sturdiness to the inaccurate approximation of the primary user's state.

In [45], a game model is designed to detect a PUE attack. A game theory-based defense strategy deals with a selfish and malicious PUE attacker. The time frame is divided into sensing and data frame. Selfish attacker occupies the spectrum band in data transmission duration after performing a PUE attack during the sensing period. Channel surveillance is adopted to monitor the attacker while accessing the channel. Once such attacker is narrowed down, it is punished by either limiting its bandwidth or completely isolating it from the network. It is assumed that the spectrum sensing process cannot differentiate between emulated and licensed primary user signals. Thus, an attacker cannot be detected in the sensing time frame. An extra sensing process is adopted, which helps in detecting the channel under PUEA. Once such a channel is sensed, it is again set free for the next data frame. This extra sensing process is cheaper compared to channel surveillance. This paper does not deal with avoiding the attacker. It detects the attacker before switching on to channel surveillance procedure. The key role is played by the manager of the network who acts like a superintendent. The strategies of the attacker and the superintendent are figured out in a closed-form, as Nash equilibrium (NE) point. This simulation is effective considering the scenario where attacker eyes only a single channel however the model is not suitable for a CRN dealing with multi-channel attack.

As the superintendent's role is limited to cater single channel attack [45], the capabilities got enhanced [46] to address a multichannel attack by adopting a channel surveillance procedure. An attacker learns and adapts the art of surveillance by monitoring the spectrum

for a fixed period before performing a selfish PUEA. In such a case, adopting Nash equilibrium may not give results as desired by the defender.

In the previous approach, Nash equilibrium (NE) is used to analyze a formulated non-zero sum game of a selfish user, malicious user, and mixed PUE. But a smart attacker can learn and adapt surveillance strategies by monitoring the spectrum for a fixed period before it attempts to occupy the channel or perform selfish PUEA. In this case, NE may not be used as an efficient defender strategy.

An advanced form of game theory based on strong Stackelberg equilibrium (SSE) is proposed in [47]. The algorithm revolves around a leader and a follower (which resonates to superintendent and attacker [45]) where the strategy is initiated by the leader who drives and defines the follower's strategy. The whole idea is to have a commitment model where follower's actions are committed to leader's strategy. A non-commitment model is analyzed using NE, whereas a commitment model is analyzed by strong Stackelberg equilibrium (SSE). The benefits and losses of both the players are evaluated and compared with the non-commitment model. PUEA cannot be detected during the sensing process, as it is assumed that the sensing engine cannot distinguish between emulated and genuine PU signal. The commitment model is examined through the proper modeling of strategic interaction between a leader and follower. Subsequently, attacker responds to a strategy used by the network manager lowering model's computation time and maximizing the expected payoff. If the net-work size increases, the game theory model becomes complicated and impractical.

In [48], another game theory approach is proposed by author Mohsen et al. In this work, a non-zero sum game is developed between good and bad secondary users in the synchronization phase. During data transmission phase, a genuine SU sends data randomly on the frequency channel in presence of a bad SU. Nash equilibrium point is obtained for this game with improvement in the SU throughput. Simulation results show that NE point is consistent as per Lemke and Howson algorithm.

Another GT based scheme is proposed to reduce the false alarm and miss detection probability [49]. A non-zero sum game is formulated between SUs and PUEA, which does not allow the attacker to use the channel. Each cluster is embedded with this game model so that SU does not switch channels when the attacker node arrives. A trust list table consisting of PU node ID and attacker ID is created and updated after every miss-detection. Therefore, SU switches and moves to another channel or stays on the same channel, which depends on the arriving node ID and trust list table. Simulation results show that chances of miss-detection and false alarms are reduced substantially.

General limitations of GT model:

1. The number of players can be finite. If network size increases, the game theory approach becomes complicated and impractical.
2. GT revolves around mathematical models that account for logical responses however real-world responses may vary.

3.7 Machine Learning

Human's ability to learn and get better at tasks with experience is part of being human. At the time of birth, our knowledge about things is nil and hence our capability to do anything for us is also nil. We learn with time and become more capable and computers have the same potential. Machine learning (ML) brings together statistics and computer science to

enable computers to learn and accomplish a given task without being programmed to do so. The way human brain uses experience to improve at a given task similarly computers can enrich their experience too [50, 51]. Feeding information, images helps the computer to recognize and translate the data numerically. It identifies patterns and establishes algorithms for better predictions. In the learning stage, it may give inaccurate results however with incremental data input, algorithm is finely tuned and becomes more accurate in its predictions. The technology behind facial recognition, text and speech recognition, SPAM filters in the inboxes, credit card forge detection, online shopping or online viewing recommendations is machine learning. From medical diagnosis to social media, the horizon of machine learning is vast [52].

Researchers thrives to achieve a combination of statistics and computer science to build algorithms that can solve complex problems more efficiently using less computing power. ML makes a system capable of thinking, analyzing, predicting, responding and automatically learning from the previous experience without the need for programming. Research areas implemented in the perspective of cognitive radio and ML are broadly categorized into two groups: pattern classification and decision making. The learning algorithm is broadly classified as supervised, unsupervised and reinforcement learning (RL) [53, 54].

CR well-versed with its radio frequency environment performs intellectual tasks smoothly. Besides being aware and truly cognitive, an effective CR is well equipped with learning and reasoning capabilities. Such capabilities are embedded in the engine of a cognitive radio which acts as a nucleus. Such CR engine makes use of machine learning algorithms to coordinate the entire actions of a CR.

3.7.1 Unsupervised and supervised learning solutions

The work in [55] describes secured spectrum sensing using unsupervised machine learning in the presence of PUEA and spectrum sensing data falsification (SSDF). The coexistence of PUEA and SSDF leads to unsafe spectrum sensing performance. If the emulation attacker is identified, the neighbor can send the wrong sensing report leading to falsification. The solution suggests that both the attacked SUs should be removed from the cooperative sensing process. A secure sensing algorithm is proposed, which uses a clustering mechanism to detect the malicious SU. This algorithm does not need prior information about SUs location and attacking strategy. Identification of SUs is checked for errors through the uniquely assigned identity value for each SU. Such values are updated intermittently. The process focuses on securing the spectrum sensing and making the decision making process more reliable irrespective of the threat—PUEA or SSDF.

A solution to make sensing report more accurate is to discarding the attacker from the average observation before finalizing the spectrum decision. To achieve the same, K-means unsupervised machine learning is used to filter out the anomaly which could lead to a deviation in the spectrum sensing. These reports are omitted from the cooperative spectrum sensing (CSS) process and therefore limiting the sensing report strictly on the result of trusted SUs. The bigger risk however exists if the fusion centre (FC) is compromised as it is overall responsible for the identification of attack, securing the spectrum sensing and ensuring a reliable decision making. Other limitations K-means unsupervised ML are (1) K means chooses K value manually. (2) K means clustering technique cannot be used for varying size and density. (3) K means clustering assumes spherical clusters and each cluster has equal numbers of observations. The algorithm does not work for clusters of unusual

size. (4) Clustering quality gets affected by the sensing history dimensions. Large dimensions lead to fewer identification errors as computational complexity increases.

In order to address spectrum occupancy issue, researchers have explored integrating conventional wireless sensing network with the cognitive features. A new method [56] has been devised which is based upon two non-parametric algorithms: the data clustering (DC) and cumulative sum (CUSUM) algorithms. The basic methodology is to analyze detection delay, scenario dependency, resources scalability and learning time. A CWSN simulator verifies the validity of the applied method. However, the DC algorithm is more appropriate for dynamic or intricate scenarios. The CUSUM is comparatively slow to respond to large shifts. Also, both the algorithms are not suitable for applications with large datasets. Both non-parametric algorithms have displayed competence to detect the PUEA behavior but the algorithms are slow (increase in the number of users reduces the network speed).

In [57], an effective PUEA detection method is presented, taking advantage of the recurrent neural network (RNN). In centralized CRN, throughout the preliminary stages of spectrum sensing (at SU or FC), the RNN model could be trained using the standard PU activity series. During spectrum sharing with primary users, the SU is able to continuously check the signal behavior with the application of PUEA detector and trained RNN. Due to the eminent issue of gradient vanishing, it is difficult for basic RNN to process activity series with long temporal dependency. Due to this gradient vanishing problem, RNN forgets long term data, which means RNN cannot use patterns taking place long before the current input series. Several other recurrent neural network structures are introduced to overcome these limitations.

An artificial expansion of RNN known as long short-term memory (LSTM) is widely used in deep learning. LSTM has connections of feedbacks comprising of memory cell and input, output and forget gates. The performances of the fundamental RNN detector are compared with the LSTM detector and the multi-layer LSTM detector in the presence of PUEA. The three-layer LSTM detector attains the finest performance because it is capable of learning intricate features and storing lengthy historical behavior [58].

In [59], a classification model based on machine learning is used for identifying primary user emulation attack detection. The detection process is divided into three stages: (1) channel estimation is done by treating channel impulse response as a link signature. (2) A four-dimensional feature space (mean, variance, skewness, and difference of maximum and minimum CIR values) is created by the raw channel impulse response (CIR) sample. (3) Pattern recognition of extracted features is carried out by 6 classification model: logistic regression (LR), linear discriminant analysis (LDA), K-nearest neighbors (KNN), decision tree classifier (DTC), Gaussian Naïve Bayes (NB), and support vector machine (SVM). Evaluation through above techniques was recorded in terms of accuracy; recall, precision, and F score. A real-time testbed software define radio was used to test the performance of the proposed scheme.

In [60], genetic crossover and mutation operators are combined with the artificial bee colony algorithm to attain stability between exploration and exploitation of solution. Primary user emulation attack is an intelligent model and devised as an optimization problem in this paper. Every secondary users is embedded with an energy detector to carry out spectrum sensing in the following channel scenarios—(a) White Gaussian noise (b) PU with noise (c) PUEA with noise and PU (d) PUEA with noise. The received signal strength from SUs is compared with two predefined thresholds instead of a single threshold. This double threshold method improves the probability of detection as compared to other recently proposed detection algorithm. Further in [61], artificial bee colony algorithm is combined with K-means to explore data clustering in an effective way.

Another ML secure sensing algorithm is proposed, which uses a clustering mechanism to detect the malicious SU. This algorithm does not need prior information about SUs location and attacking strategy. Identification of SUs is checked for errors through the uniquely assigned identity value for each SU. Such values are updated intermittently. The process focuses on securing the spectrum sensing and making the decision making process more reliable irrespective of the threat—PUEA or SSDF [62].

Traditionally, machine learning comes with the capability of learning, analyzing, and predicting radio frequency signals. However, it is challenging to classify RF signals disrupted by malicious activities such as jammer, eavesdropper and PUEA. A new machine learning model known as generative adversarial network (GAN) is implemented to discriminate between real and fake radio signals in the cognitive radio network. As this is a recently explored learning model, few research techniques have been proposed for attack detection based on GAN [63, 64].

In [65], a new solution is provided for the detection of a primary user emulation attack. The author designed the generative adversarial network (GAN) model to generate and detect malicious SUs. GAN arrangement consists of two neural networks. (a) Generator for generating data probabilistically and (b) discriminator for differentiating fake and real signals after getting trained by an artificial neural network. For the detection of MUs, a dumb generator with no PU signal information and smart generator with enough PU signal data are designed. These generated data from the generator are identified by the discriminator model, which is trained by the neural network for real (PU) and fake (malicious SU) signals. A universal Software Radio Peripheral test bed train the discriminator over primary user signal data. The models detect malicious users, and PU with a model than 98% accuracy GAN model is a good solution for PUEA detection and the security issues of the wireless communication network.

In [66], a discriminator model is built to distinguish between trusted and fake RF transmitter. This model learns signal characteristics of the RF signal by convolutional neural network (CNN) and deep neural network (DNN). Results show that CNN and DNN can detect trusted and malicious transmitters with 81.6% and 96.6% accuracy, respectively.

GAN is applied for creating a secure and self-aware CR network in [67]. This work focuses on the security of the physical layer by using two abnormality detection techniques—(1) conditional generative adversarial network (C-GAN), (2) dynamic Bayesian network (DBN). A high dimensional state vector acting as an input of radio frequency spectrum is extracted and learned by both the detection network.

In [68], a power allocation algorithm based on GAN is used to set up private communication under primary transmitter guidance. A generator and discriminator model is framed to learn power allocation solution strategy, covert or non-covert communication, and detection accuracy. This model learns from a fully connected deep neural network to provide a near-optimal power allocation solution to achieve fast convergence.

In [69], a distributed semi-supervised machine learning method running on the cloud is proposed. Data is first classified and labeled by a cognitive engine incorporated with self organizing map (SOM). Then, this labeled data is forwarded for the second classification based on past experiences to cloud core induced with convolutional deep learning network (CDLN). Both CDLN and rule-based learning are compared based on error rate percentage, false alarm probability, and detection accuracy with and without noise. The simulation outcome shows that the algorithm is 25% better than the conventional neural network and 40% better than a rule-based method. This is an effective technique to enhance system security when attack signature changes frequently.

In [70], cloud expansions nowadays has become a promising technology which can help in taking rapid decision due to simplified scaling and potent virtual machine based compute engine. This paper discovers prevailing real-time supervised learning-based PUEA detection merged with the edge computing engines and core cloud.

3.7.2 Reinforcement learning solutions

Reinforcement learning is a type of machine learning with no defined input database. The learning mechanism operates on four parameters: environment, agent, state, and actions. For example, the CR environment consists of the secondary node, primary node, cognitive, and primary base station [71, 72]. An agent on the fly observes, learns, and takes action based on environment, state and reward. The state is the decision making factor affecting rewards and the agent's actions. The action of an agent on its surrounding leads to a positive reward or a negative reward. Every agent's action is towards maximizing the network's rewards and improving the next state [73].

Reinforcement learning and cluster size adjustment based security systems for CRN are presented in [76]. The size of the cluster is adjusted to enhance network scalability, stability, and spectrum utilization efficiency. In this approach, the free spectrum is distributed as tokens to SU member nodes in the cluster by the cluster head (CH). It is the duty of the CH to monitor the token utilization performance of the secondary users. If a secondary node wastes a specific amount of token, its performance ratio decreases, and the node is removed from the cluster. MU can intentionally waste the token received to degrade utilization of radio frequency spectrum without being detected. RL model is integrated inside the cluster head as well as all SUs presumed as potential attackers. RL and cluster size adjustment arrangement provides excellent security and scalability for the network when attacker intensity is lower [74]. As the probability and intensity of attack increase, the cluster head cannot detect malicious nodes in the cluster. This RL approach is excellent for a cognitive radio network where SU can turn malicious over time. Continuous observation and learning of the node's behavior and surrounding are essential parameters for deploying a smooth security system.

In [74–76], RL learning and clustering application, model, features are explored. These papers explain the step-by-step procedure on how RL can address security, routing, scalability, and stability in cognitive radio network.

Most of the prevailing reinforcement learning-based structures are implemented using simulations. However, to the best of our knowledge, there are only a few implementations of RL-defined schemes in the CR hardware platform—universal software radio peripheral and software defined radio [77]. The real time implementation of the RL algorithms is significant for confirming their accuracy and precision in a practical CR environment. To this end, progressive research is needed to investigate the implementation and road blocks of the RL-based scheme on the CR hardware platform [78, 79].

3.8 Blockchain

Recently popular technology called blockchain is used for implementing security in a cognitive radio network. A chain of blocks (referred as blockchain) are linked in a distributed form using cryptography and are used for storing information which is difficult to modify. Blocks are comprised of three critical parts: data, hash, and hash of the previous block. An example of blockchain technology is exchange of cryptocurrency (Bitcoin) where the

transactions are recorded in a public ledger (in the chain of blocks). The ledger contains the details about the sender of Bitcoin, receiver and the volume of coins traded. If the hash of the second block changes due to some reason, it can make all the following blocks invalid since every block depends on the previous block's hash value [80]. A mechanism called 'proof of work' is used in the blockchain, which slows down the creation of a new block in case of block tampering. On creation of every new block, each node in the chain verifies the new block to check the authenticity. Once the consensus is created amongst all the network nodes, new block is created. Therefore, security of blockchain comes from the creative ideas of hashing, proof of work, decentralized and distributed time servers [82, 83].

In a recent paper [81], blockchain technology is implemented to detect and mitigate malicious users and improve the spectrum sensing process in the cognitive radio network. All primary and secondary users are altered into blocks and from a decentralized network. Each cognitive radio block consist of four kinds of information. (1) Hash: SHA256 algorithm generates a unique key known to the next block of the user. (2) Sensing result: outcome of sensing result. (3) Private key: A 16-bit unique key known to the user only. (4) Previous hash: the hash value of the previous node. Malicious user detection is done by verifying the digital signature (hash and private key) of nodes. Detected MU is filtered out from participating in the future spectrum sensing process. Complex simulations are performed in MATLAB software to compute miss detection and possibilities of false alarm using public and private keys.

In [84], another blockchain defined spectrum sharing protocol is designed against malicious users in CR internet of things environment. This work defines a proactive protocol to learn an attacker's behavior and blockchain to enhance CR system security. Along with enormous increases in blockchain technology, its complexity is also very low as compared to other existing models. Several blocks in blockchain can grow very large over time hence storage would be a bottleneck. High energy consumption is also a critical aspect of blockchain technology which is concerning at present (Tables 4, 5).

4 Past Present and Future

Spearing the ship in the right direction is vital. A step towards security is helpful when the assumptions are well written else the ship may lead to unsafe waters.

1. *Impractical Assumptions*—The contributions on PUEA detection covered in this paper are majorly relying on an underlying hypothesis that the location and transmission power of all users (primary secondary and malicious) are fixed and well-known. This assumption alone is naive and mainly impractical for the applications of CR.
2. *Learning and Reasoning*—To perform intellectual tasks, a CR is expected to be well-versed with its radio frequency (RF) environment, learning and reasoning capabilities. Several factors and policies need to be adjusted instantaneously (e.g. transmission power, coding method, modulation technique, sensing process, policy and communication protocol.) and a one-dimensional approach of assuming 'location' and 'transmission power' may not help in synchronizing multiple parameters simultaneously [52]. In existing approaches, security comes at a cost of affecting several system requirements. Therefore, research efforts in this direction would be a worthwhile contribution for evolving a security mechanism suitable for network of any kind (cooperative or non-cooperative, distributed or centralized) and doesn't trade off with system quality speci-

Table 4 Countermeasure for BP, WM, game theory and machine learning

Authors	Principle	Real time/simulations outcome	Limitations
Belief propagation			
Liu et al. [24]	Belief propagation: approx. 8 iteration	Simulation Results show probability of false alarm and misdetection with respect to threshold	Inaccurate results when PU and MU distance is less Scalability reduces as SU increases
Muñoz et al. [25]	Belief propagation: single iteration	Computation time and accuracy comparison with previous method	Inaccurate results when PU and MU distance is less Computation time increase with SU
WM			
Anand et al. [26]	RF signal energy level and sensor information	Real time experiment: false positive and false negative rates calculated	Extra sound sensors equipped with each SU
Game theory			
Chen et al. [29]	Non cooperative multistage: Nash equilibrium (NE)	Belief updating system performance in terms of greater payoff	Not suitable for multiple attackers Game model assumptions: unrealistic
Jayapalan et al. [31]	Channel surveillance and extra sensing process	Nash equilibrium is plotted with respect to penalty factor	long surveillance time Game model assumptions: unrealistic
Mathur and Subbalakshmi [32]	Strong Stackelberg equilibrium (SSE)	Expected payoff graph of defender and PUEA	Complex and impractical
Machine learning			
Alahmadi et al. [34]	Unsupervised learning clustering algorithm: K-means	Clustering quality versus sensing history dimension. Misdetection and false alarm probability is shown	K means clustering: Not suitable for varying size and density Clustering quality degrades due to sensing history dimension
Yuan et al. [35]	Data clustering and cumulative sum algorithms	CWSN simulator: performance of algorithm	Slow algorithm Efficiency affected by number of users

Table 5 ML countermeasure: reinforcement learning, GAN and blockchain

Authors	Method(s)	Real time/Simulations	Limitations
Ling et al. [76]	Cluster size adjustment and RL algorithm	Cluster size ratio improvement with respect to attack probability from 0.1 to 0.9	Algorithms gives unstable results when number of MU is high if attack probability is greater than 0.7, CH cannot detect MU (learns inaccurately)
Roy et al. [65]	GAN learning	Real time USRP B210 with tensorflow—98% accuracy after GAN training	Training is complex Unstable and need synchronization between discriminator and generator
Sajid et al. [81]	Blockchains: cryptography, and hash value	Simulation to compute detection of MU with respect to SNR	Storage of large number of blocks High energy consumption

fications (delay, throughput, reliability, energy consumption and spectral efficiency). Advanced machine learning methods are moving towards enhancing security and are independent of the coordinates of PU and SU [53]. Numerous introductory studies are using various machine learning techniques (supervised and unsupervised) such as clustering, object classification, reinforcement learning, pattern recognition, and artificial neural network (ANN) [55–78].

3. *Deep Reinforcement Learning*—Research in the field of cognitive radio security has found a fresh opening in the form of reinforcement learning. RL incorporated CR learns from state and surrounding environment and eliminates the need of knowing location (of PU and MU). In a practical CR scenario, a there is a possibility that a genuine secondary user can turn malicious during the operation. Such scenarios have helped researchers to evolve in their approach too. In a recent paper [76], author Mee Hong Ling et al. has integrated RL and clustering algorithms to detect and mitigate online malicious SUs. Such approach provides a pragmatic solution which is missing in most of the existing models (if SU turns malicious).

   Q learning is an RL algorithm used in this trust model. Q learning creates a matrix of state (S) and actions (A) by observing the environment. But there are few limitations associated with this algorithm. If the number of users rise or network is large, it has to create a huge S * A matrix which can exhaust the computational abilities of the system. To address the matter, deep reinforcement learning (DRL) is required to be thoroughly explored. There is limited recent research work on application of deep reinforcement learning for various cognitive radio operation and security. In [100] a reinforcement learning method is combined with graph neural network to enhance energy optimization in a distributed CSS process. In [101] resource allocation is carried out in cognitive network by applying deep learning concepts called doctive learning. Artificial neural network (NN) successfully combined with RL is the best possible scenario to attain greater goals.
4. *Physical Layer*—Enhanced security at the outermost layer is the foundation of all security controls in a cognitive radio network. Primary user emulation attack takes place in the physical layer of the protocol stack; therefore mitigation of this attack lies in achieving security at physical layer. A number of researchers are working on improving secrecy capacity and outage probability of a cooperative communication. The secrecy rate analysis shows how strong the security mechanism can perform against the potential threat in the cognitive radio networks. Various methods are implemented for improving physical layer security with energy harvesting and cooperative communication [88–91].
5. *Cross Layer Design*—Research may not require a focused strategic approach but a focused execution. Strategy formulation could be balanced and flexible. Excess of focus on studying the physical layer alone has prevented the early researchers from changing the perspective. Most of the countermeasures covered in this paper focus on optimizing the physical layer features without considering the alteration of the upper layer parameters. An attack at the physical layer can affect MAC and upper layers of the network directly or indirectly. The notion of cross-layer security is not heavily investigated historically. There is a need for interaction between physical and upper layers to develop an effective security design. This has motivated just a few researchers to instigate new security ideas. A researcher has combined [85] detection of PUEA with the authentication of upper layers using SUs cross-layer learning ability. A radio-frequency fingerprint (RF) is utilized to detect PUEA, considering multipath Rayleigh fading channel for mobile SUs. To achieve secrecy, the author of [86] has proposed a cross MAC-PHY

layer security design, which is a combination of MAC layer ARQ (automatic repeat request) and physical layer artificial noise (AN) mechanism [87].

6. *Proactive Design*—Most of the countermeasures for PUEA detection are reducing the network's efficiency while implementing external algorithms. If the instances of attack increase, count for running the algorithms (countermeasures) also increases. This leads to slowing down the network and squeezing out its energy. A better alternative would be to have an integral (not external) mechanism to run the detection algorithms. These issues can be addressed by designing a robust and secure MAC protocol [92]. An ideal MAC protocol may depict the following characteristics. (1) MAC can detect and discard MU and its data from the network itself at the proactive stage of the spectrum sensing and decision-making process. (2) Post spectrum sensing stage, MAC is not required to run external algorithms to mitigate attacks and, therefore, avoid high energy consumption. A design that incorporates a proactive outlook and can predict when and where the communication pathway would exist is significant. Recent work based on similar security concept in [93], proposed a proactive learning MAC protocol for defense against two significant attacks taking place in Centralized and distributed CRN: PUEA and SSDF. This protocol is compared with PROMAC [94] and POMAC [95] in terms of channel utilization, back-off rate, and sensing delay. Designing a CR MAC model for building a sturdy security mechanism is still a difficult topic of research.
7. *Energy Harvesting*—Transmission power has always been a critical assumption for early researchers (going back to the aforementioned one-dimensional approach of assumption—location and 'power'). Researchers have assumed a constant magnitude of transmission power, assuming the energy shall always remain constant. Based on this, researchers have visualized certain test cases or the environment in which a PUEA occurs. To achieve the countermeasures (in the visualized and controlled environment), signal strength got consumed (external algorithms) and kept reducing. With the reduction of power, there were rarely any attempts to modify the test case scenarios to regain the strength of the signal to cater to lower efficiency and drained energy. This gave rise to a new concept of Energy Harvesting [95, 96]. Meng-Lin Ku has compiled various efforts towards this concept [97] and has shown a promising path to achieve a mechanism in CRN to conserve the energy. Energy concerns are majorly in two areas: energy efficiency and energy harvesting. In a CR network seeking to harvest energy, each node is stimulated by the energy sources such as wind, solar, or downlink radio frequency signals from the base stations. The energy harvesting process allows the CR network to do away with intermittent recharge or renewal of the batteries. It has potential to lead us in the direction of the green (communication) revolution [98, 99].

Blockchain and DRL are two competent areas with significant outcome which further needs exploration for deploying security as well as other spectrum management operations. Researchers have successfully initiated the work in this direction [102, 103].

5 Conclusion

Cognitive radio is a captivating technology to improve the efficiency of valuable radio frequency resources. The dynamic nature of CR makes it more vulnerable to security threats, compared to traditional wireless networks. The Primary user emulation attack is a significant threat to the spectrum sensing operation of CR. This paper presented the most

significant contributions for countering PUEA, describing their principles and shortcomings. Regardless of the utility and suggestions discussed in this paper, most of them are not suitable for practical CR environment. Most of the countermeasures for PUEA detection are reducing the network's efficiency while implementing external algorithms. Thus there is a need for security mechanisms to proactively detect and discard attacks from the system without affecting the crucial parameters such as delay, throughput, energy consumption and reliability. An innovative and sophisticated mechanism providing a secure, reliable, high speed, energy efficient and low-complexity network is desired to make CR network a feasible solution for the future spectrum management requirements. Accomplishing these quality features with highly cross-layer security design is still a stimulating area of research.

References

1. Marcus, M., Burtle, J., Franca, B., Lahjouji, A., & McNeil, N. (2002). Federal communications commission spectrum policy task force. *Report of the unlicensed devices and experimental licenses working group*.
2. Čabrić, D., Mishra, S. M., Willkomm, D., Brodersen, R., & Wolisz, A. (2005). A cognitive radio approach for usage of virtual unlicensed spectrum. In *14th IST mobile and wireless communications summit*.
3. Fcc, E. (2003). Docket No 03-222 Notice of proposed rulemaking and order.
4. Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications, 23*(2), 201–220.
5. Thalia, N., Ingle, A., Raut, K., & Tilak, M. (2015). Cognitive radio network—A new paradigm in wireless communication. *International Journal of Computer Applications, 975,* 8887.
6. Akyildiz, I. F., Lee, W. Y., Vuran, M. C., & Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks, 50*(13), 2127–2159.
7. Fragkiadakis, A. G., Tragos, E. Z., & Askoxylakis, I. G. (2012). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys and Tutorials, 15*(1), 428–445.
8. Sharma, R. K., & Rawat, D. B. (2014). Advances on security threats and countermeasures for cognitive radio networks: A survey. *IEEE Communications Surveys and Tutorials, 17*(2), 1023–1043.
9. Mishra, N., Srivastava, S., & Sharan, S. N. (2019). Cognitive radio network security threats: A review. In *2019 2nd international conference on intelligent communication and computational techniques (ICCT)* (pp. 333–338).
10. Manesh, M. R., & Kaabouch, N. (2018). Security threats and countermeasures of MAC layer in cognitive radio networks. *Ad Hoc Networks, 70,* 85–102.
11. Thalia, N., Ingle, A., Raut, K., & Tilak, M. (2016). A survey on security issues and primary user emulation attack detection techniques in cognitive radio network. *International Journal of Computer Applications, 975,* 8887.
12. Chen, R., & Park, J. M. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. In *1st IEEE workshop on networking technologies for software defined radio networks* (pp. 110–119).
13. Chen, R., Park, J. M., & Reed, J. H. (2008). Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications, 26*(1), 25–37.
14. Rehman, S. U., Sowerby, K. W., & Coghill, C. (2014). Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios. *IET Communications, 8*(8), 1274–1284.
15. Bouabdellah, M., Ghribi, E., & Kaabouch, N. (2019). RSS-based localization with maximum likelihood estimation for PUE attacker detection in cognitive radio networks. In *IEEE international conference on electro information technology (EIT)* (pp. 1–6).
16. Zhao, C., Xie, L., Jiang, X., Huang, L., & Yao, Y. (2010). A PHY-layer authentication approach for transmitter identification in cognitive radio networks. In *International conference on communications and mobile computing* (Vol. 2, pp. 154–158).
17. León, O., Hernández-Serrano, J., & Soriano, M. (2012). Cooperative detection of primary user emulation attacks in CRNs. *Computer Networks, 56*(14), 3374–3384.
18. Wei, J., & Zhang, X. (2010). Two-tier optimal-cooperation based secure distributed spectrum sensing for wireless cognitive radio networks. In *INFOCOM IEEE conference on computer communications workshops*, San Diego, CA (pp. 1–6).

19. Adebo, S. A., Onwuka, E. N., Usman, A. U., & Onumanyi, A. J. (2019). A hybrid localization scheme for detection of primary user emulator in cognitive radio networks. *International Journal of Computing and Digital Systems, 8*(03), 217–227.
20. Fassi Fihri, W., El Ghazi, H., Abou El Majd, B., & El Bouanani, F. (2019). A decision-making approach for detecting the primary user emulation attack in cognitive radio networks. *International Journal of Communication Systems, 32*(15), e4026.
21. Arun, S., & Umamaheswari, G. (2020). An adaptive learning-based attack detection technique for mitigating primary user emulation in cognitive radio networks. *Circuits, Systems, and Signal Processing, 39*(2), 1071–1088.
22. El Mrabet, Z., Arjoune, Y., El Ghazi, H., Abou Al Majd, B., & Kaabouch, N. (2018). Primary user emulation attacks: A detection technique based on Kalman filter. *Journal of Sensor and Actuator Networks, 7*(3), 26.
23. Selvapriya, T., Sharmila, S. S. S., Sindhuja, M., Sinthuja, V., & Jayasri, C. (2017). A database assisted detection against primary user emulation in cognitive radio network. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 5*(3), 1–6.
24. Liu, Z., Zhang, G., Meng, W., Ma, X., & Li, G. (2020). Multiple-phase energy detection and effective capacity based resource allocation against primary user emulation attacks in cognitive radio networks. *KSII Transactions on Internet and Information Systems*. https://doi.org/10.3837/tiis.2020.03.022.
25. Muñoz, E. C., Rodriguez-Colina, E., Pedraza, L. F., & Paez, I. P. (2020). 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.
26. Anand, S., Jin, Z., & Subbalakshmi, K. P. (2008). An analytical model for primary user emulation attacks in cognitive radio networks. In *3rd IEEE symposium on new frontiers in dynamic spectrum access networks* (pp. 1–6).
27. Jin, Z., Anand, S., & Subbalakshmi, K. P. (2009). Detecting primary user emulation attacks in dynamic spectrum access networks. In *IEEE international conference on communications* (pp. 1–5).
28. Jin, Z., Anand, S., & Subbalakshmi, K. P. (2009). Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. *ACM SIGMOBILE Mobile Computing and Communications Review, 13*(2), 74–85.
29. Chen, Z., Cooklev, T., Chen, C., & Pomalaza-Ráez, C. (2009). Modeling primary user emulation attacks and defenses in cognitive radio networks. In *IEEE 28th international performance computing and communications conference* (pp. 208–215).
30. Liu, Y., Ning, P., & Dai, H. (2010). Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In *IEEE symposium on security and privacy* (pp. 286–301).
31. Jayapalan, A., Savarinathan, P., Praveenkumar, P., & Karuppasamy, T. (2019). Detecting and mitigating selfish primary users in cognitive radio. *Wireless Personal Communications, 109*(2), 1021–1031.
32. Mathur, C. N., & Subbalakshmi, K. P. (2007). Digital signatures for centralized DSA networks. In *4th IEEE consumer communications and networking conference* (pp. 1037–1041).
33. Ghanem, W. R., Shokair, M., & Desouky, M. I. (2016). Defense against selfish PUEA in cognitive radio networks based on hash message authentication code. *International Journal of Electronics and Information Engineering, 4*(1), 12–21.
34. Alahmadi, A., Abdelhakim, M., Ren, J., & Li, T. (2014). Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. *IEEE Transactions on Information Forensics and Security, 9*(5), 772–781.
35. Yuan, Z., Niyato, D., Li, H., Song, J. B., & Han, Z. (2012). Defeating primary user emulation attacks using belief propagation in cognitive radio networks. *IEEE Journal on Selected Areas in Communications, 30*(10), 1850–1860.
36. Maric, S., Reisenfeld, S., & Goratti, L. (2016). A single iteration belief propagation algorithm to minimize the effects of primary user emulation attacks. In *International symposium on intelligent signal processing and communication systems (ISPACS)* (pp. 1–6). IEEE.
37. Chen, S., Zeng, K., & Mohapatra, P. (2011). Hearing is believing: detecting wireless microphone emulation attacks in white space. *IEEE Transactions on Mobile Computing, 12*(3), 401–411.
38. Bishnu, A., & Bhatia, V. (2019). Cognitive radio networks: IEEE 802.22 standards. In *Sensing techniques for next generation cognitive radio networks* (pp. 27–50). IGI Global.
39. Stevenson, C. R., Chouinard, G., Lei, Z., Hu, W., Shellhammer, S. J., & Caldwell, W. (2009). IEEE 802.22: The first cognitive radio wireless regional area network standard. *IEEE Communications Magazine, 47*(1), 130–138.
40. Wang, B., Wu, Y., & Liu, K. R. (2010). Game theory for cognitive radio networks: An overview. *Computer Networks, 54*(14), 2537–2561.

41. Maharjan, S., Zhang, Y., & Gjessing, S. (2011). Economic approaches for cognitive radio networks: A survey. *Wireless Personal Communications, 57*(1), 33–51.
42. Rawat, D. B., Bajracharya, C., & Yan, G. (2011). Game theory for resource allocation in wireless networks. In *Emerging technologies in wireless ad hoc networks: Applications and future development* (pp. 335–352). IGI Global.
43. Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., & Hubaux, J. P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys (CSUR), 45*(3), 1–39.
44. Tan, Y., Sengupta, S., & Subbalakshmi, K. P. (2012). Primary user emulation attack in dynamic spectrum access networks: A game-theoretic approach. *IET Communications, 6*(8), 964–973.
45. Nguyen-Thanh, N., Ciblat, P., Pham, A. T., & Nguyen, V. T. (2015). Surveillance strategies against primary user emulation attack in cognitive radio networks. *IEEE Transactions on Wireless Communications, 14*(9), 4981–4993.
46. Ta, D. T., Nguyen-Thanh, N., Maille, P., Ciblat, P., & Nguyen, V. T. (2016). Mitigating primary emulation attacks in multi-channel cognitive radio networks: A surveillance game. In *2016 IEEE global communications conference (GLOBECOM)* (pp. 1–6). IEEE.
47. Ta, D. T., Nguyen-Thanh, N., Maillé, P., & Nguyen, V. T. (2018). Strategic surveillance against primary user emulation attacks in cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking, 4*(3), 582–596.
48. Mahmoudi, M., Faez, K., & Ghasemi, A. (2019). Uncoordinated frequency hopping scheme for defense against primary user emulation attack in cognitive radio networks. *Computer Networks, 163,* 106884.
49. Yazdi, S. A. V., & Ghazvini, M. (2019). Countermeasure with primary user emulation attack in cognitive radio networks. *Wireless Personal Communications, 108*(4), 2261–2277.
50. Clancy, C., Hecker, J., Stuntebeck, E., & O'Shea, T. (2007). Applications of machine learning to cognitive radio networks. *IEEE Wireless Communications, 14*(4), 47–52.
51. Bkassiny, M., Li, Y., & Jayaweera, S. K. (2012). A survey on machine-learning techniques in cognitive radios. *IEEE Communications Surveys and Tutorials, 15*(3), 1136–1159.
52. Wang, J., Jiang, C., Zhang, H., Ren, Y., Chen, K. C., & Hanzo, L. (2020). Thirty years of machine learning: The road to pareto-optimal wireless networks. *IEEE Communications Surveys and Tutorials*.
53. Hossain, M. A., Noor, R. M., Yau, K. L. A., Azzuhri, S. R., Z'aba, M. R., & Ahmedy, I. (2020). Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks. *IEEE Access*.
54. Bhatti, D. M. S., Ahmed, S., Chan, A. S., & Saleem, K. (2020). Clustering formation in cognitive radio networks using machine learning. *AEU-International Journal of Electronics and Communications, 114,* 152994.
55. Li, Y., & Peng, Q. (2016). Achieving secure spectrum sensing in presence of malicious attacks utilizing unsupervised machine learning. In *MILCOM IEEE military communications conference* (pp. 174–179).
56. Blesa, J., Romero, E., Rozas, A., & Araujo, A. (2013). PUE attack detection in CWSNs using anomaly detection techniques. *EURASIP Journal on Wireless Communications and Networking, 2013*(1), 215.
57. Dong, Q., Chen, Y., Li, X., & Zeng, K. (2018). Explore recurrent neural network for PUE attack detection in practical CRN models. In *IEEE international smart cities conference (ISC2)* (pp. 1–9).
58. López, D., Rivas, E., & Gualdron, O. (2019). Primary user characterization for cognitive radio wireless networks using a neural system based on deep learning. *Artificial Intelligence Review*, 1–27.
59. Albehadili, A., Ali, A., Jahan, F., Javaid, A. Y., Oluochy, J., & Devabhaktuniz, V. (2019). Machine learning-based primary user emulation attack detection in cognitive radio networks using pattern described link-signature (PDLS). In *Wireless telecommunications symposium (WTS)* (pp. 1–7).
60. Elghamrawy, S. M. (2018). Security in cognitive radio network: Defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.08.022.
61. Kumar, A., Kumar, D., & Jarial, S. (2018). A novel hybrid K-means and artificial bee colony algorithm approach for data clustering. *Decision Science Letters, 7*(1), 65–76.
62. Mirza, M. A., Ahmad, M., Habib, M. A., Mahmood, N., Faisal, C. N., & Ahmad, U. (2018). CDCSS: Cluster-based distributed cooperative spectrum sensing model against primary user emulation (PUE) cyber-attacks. *The Journal of Supercomputing, 74*(10), 5082–5098.
63. Han, X., Xue, L., Shao, F., & Xu, Y. (2020). A power spectrum maps estimation algorithm based on generative adversarial networks for underlay cognitive radio networks. *Sensors, 20*(1), 311.

64. Shi, Y., Sagduyu, Y. E., Erpek, T., Davaslioglu, K., Lu, Z., & Li, J. H. (2018). Adversarial deep learning for cognitive radio security: Jamming attack and defense strategies. In *2018 IEEE international conference on communications workshops (ICC Workshops)* (pp. 1–6). IEEE.
65. Roy, D., Mukherjee, T., Chatterjee, M., & Pasiliao, E. (2019). Defense against PUE attacks in DSA networks using GAN based learning. In *IEEE global communications conference (GLOBECOM)* (pp. 1–6).
66. Roy, D., Mukherjee, T., Chatterjee, M., & Pasiliao, E. (2019). Detection of rogue RF transmitters using generative adversarial nets. In *IEEE wireless communications and networking conference (WCNC)* (pp. 1–7).
67. Toma, A., Krayani, A., Farrukh, M., Qi, H., Marcenaro, L., Gao, Y., et al. (2020). AI-based abnormality detection at the phy-layer of cognitive radio by learning generative models. *IEEE Transactions on Cognitive Communications and Networking, 6*(1), 21–34.
68. Liao, X., Si, J., Shi, J., Li, Z., & Ding, H. (2020). Generative adversarial network assisted power allocation for cooperative cognitive covert communication system. *IEEE Communications Letters*. https://doi.org/10.1109/LCOMM.2020.2988384.
69. Srinivasan, S., Shivakumar, K. B., & Mohammad, M. (2019). Semi-supervised machine learning for primary user emulation attack detection and prevention through core-based analytics for cognitive radio networks. *International Journal of Distributed Sensor Networks, 15*(9), 1550147719860365.
70. Srinivasan, S., & Shivakumar, K. B. (2018). AI based algorithm and framework for efficient PUE attack detection using dual classification method in CRN. *International Journal of Applied Engineering Research, 13*(4), 52–56.
71. Ling, M. H., & Yau, K. L. A. (2019). Can Reinforcement learning address security issues? An investigation into a clustering scheme in distributed cognitive radio networks. In *2019 International conference on information networking (ICOIN)* (pp. 296–300).
72. Raj, R. N., Nayak, A., & Kumar, M. S. (2020). A survey and performance evaluation of reinforcement learning based spectrum aware routing in cognitive radio ad hoc networks. *International Journal of Wireless Information Networks, 27*(1), 144–163.
73. Ling, M. H., Yau, K. L. A., Qadir, J., Poh, G. S., & Ni, Q. (2015). Application of reinforcement learning for security enhancement in cognitive radio networks. *Applied Soft Computing, 37,* 809–829.
74. Manohar, A. L., Yau, K. L. A., Ling, M. H., & Khan, S. (2018). A security-enhanced cluster size adjustment scheme for cognitive radio networks. *IEEE Access, 7,* 117–130.
75. Saleem, Y., Yau, K. L. A., Mohamad, H., Ramli, N., Rehmani, M. H., & Ni, Q. (2017). Clustering and reinforcement-learning-based routing for cognitive radio networks. *IEEE Wireless Communications, 24*(4), 146–151.
76. Ling, M. H., Yau, K. L. A., Qadir, J., & Ni, Q. (2018). A reinforcement learning-based trust model for cluster size adjustment scheme in distributed cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking, 5*(1), 28–43.
77. Syed, A. R., Yau, K. L. A., Qadir, J., Mohamad, H., Ramli, N., & Keoh, S. L. (2016). Route selection for multi-hop cognitive radio networks using reinforcement learning: An experimental study. *IEEE Access, 4,* 6304–6324.
78. Musavi, M., Yau, K. L. A., Syed, A. R., Mohamad, H., & Ramli, N. (2018). Route selection over clustered cognitive radio networks: An experimental evaluation. *Computer Communications, 129,* 138–151.
79. Ren, Y., Dmochowski, P., & Komisarczuk, P. (2010). Analysis and implementation of reinforcement learning on a GNU radio cognitive radio platform. In *Proceedings of the fifth international conference on cognitive radio oriented wireless networks and communications* (pp. 1–6).
80. Joshi, A. P., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing, 1*(2), 121–147.
81. Sajid, A., Khalid, B., Ali, M., Mumtaz, S., Masud, U., & Qamar, F. (2020). Securing cognitive radio networks using blockchains. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2020.03.020.
82. Kotobi, K., & Bilen, S. G. (2018). Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access. *IEEE Vehicular Technology Magazine, 13*(1), 32–39.
83. Weiss, M. B., Werbach, K., Sicker, D. C., & Bastidas, C. E. C. (2019). On the application of blockchains to spectrum management. *IEEE Transactions on Cognitive Communications and Networking, 5*(2), 193–205.
84. Patnaik, M., Prabhu, G., Rebeiro, C., Matyas, V., & Veezhinathan, K. (2020). ProBLeSS: A proactive blockchain based spectrum sharing protocol against SSDF attacks in cognitive radio IoBT networks. *IEEE Networking Letters*. https://doi.org/10.1109/LNET.2020.2976977.

85. Le, T. N., Chin, W. L., & Kao, W. C. (2015). Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks. *IEEE Communications Letters, 19*(5), 799–802.
86. Hamamreh, J. M., & Arslan, H. (2018). Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems. *IEEE Transactions on Wireless Communications, 17*(9), 6190–6204.
87. Chen, P., Ouyang, J., Zhu, W. P., Lin, M., El Shafie, A., & Al-Dhahir, N. (2020). Artificial-noise-aided energy-efficient secure beamforming for multi-eavesdroppers in cognitive radio networks. *IEEE Systems Journal*. https://doi.org/10.1109/JSAC.2018.2824622.
88. Yu, Y. C., Hu, L., Li, H. T., Zhang, Y. M., Wu, F. M., & Chu, J. F. (2014). The security of physical layer in cognitive radio networks. *Journal of Communications, 9*(12), 28–33.
89. Sharma, S., Roy, S. D., & Kundu, S. (2020). Physical layer security in cognitive cooperative radio network with energy harvesting DF relay assisted with cooperative jamming. In *Proceedings of the 2nd international conference on communication, devices and computing* (pp. 119–129). Springer, Singapore.
90. Salahdine, F., & Kaabouch, N. (2020). Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. *Physical Communication*, 101001.
91. Pahuja, S., & Jindal, P. (2019). Cooperative communication in physical layer security: Technologies and challenges. *Wireless Personal Communications, 108*(2), 811–837.
92. Chandran, T. A., Pal, R., Prakash, A., & Tripathi, R. (2020). Proactive spectrum handoff-based MAC protocol for cognitive radio ad hoc network. In *Advances in VLSI, communication, and signal processing* (pp. 91–101). Springer, Singapore.
93. Patnaik, M., Kamakoti, V., Matyáš, V., & Řchák, V. (2019). PROLEMus: A proactive learning-based MAC protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking, 5*(2), 400–412.
94. Narayanan, N. S., Patnaik, M., & Kamakoti, V. (2016). ProMAC: A proactive model predictive control based MAC protocol for cognitive radio vehicular networks. *Computer Communications, 93,* 27–38.
95. Kwon, S., Kim, B., & Roh, B. H. (2014). Preemptive opportunistic MAC protocol in distributed cognitive radio networks. *IEEE Communications Letters, 18*(7), 1155–1158.
96. Halima, N. B., & Boujemâa, H. (2020). Energy harvesting for cooperative cognitive radio networks. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07058-y.
97. Ku, M. L., Li, W., Chen, Y., & Liu, K. R. (2015). Advances in energy harvesting communications: Past, present, and future challenges. *IEEE Communications Surveys and Tutorials, 18*(2), 1384–1412.
98. Liu, Y., Mousavifar, S. A., Deng, Y., Leung, C., & Elkashlan, M. (2015). Wireless energy harvesting in a cognitive relay network. *IEEE Transactions on Wireless Communications, 15*(4), 2498–2508.
99. Ni, L., Da, X., Hu, H., Huang, Y., Xu, R., & Zhang, M. (2018). Outage constrained robust transmit design for secure cognitive radio with practical energy harvesting. *IEEE Access, 6,* 71444–71454.
100. He, H., & Jiang, H. (2019). Deep learning based energy efficiency optimization for distributed cooperative spectrum sensing. *IEEE Wireless Communications, 26*(3), 32–39.
101. Kwasinski, A., Wang, W., & Mohammadi, F. S. (2020). Reinforcement learning for resource allocation in cognitive radio networks. *Machine Learning for Future Wireless Communications*. https://doi.org/10.1002/9781119562306.ch2.
102. Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., & Zhang, Y. (2019). Blockchain and deep reinforcement learning empowered intelligent 5G beyond. *IEEE Network, 33*(3), 10–17.
103. Luong, N. C., Anh, T. T., Binh, H. T. T., Niyato, D., Kim, D. I., & Liang, Y. C. (2019). Joint transaction transmission and channel selection in cognitive radio based blockchain networks: A deep reinforcement learning approach. In *ICASSP 2019-2019 IEEE international conference on acoustics, speech and signal processing (ICASSP)* (pp. 8409–8413). IEEE.

Mrs. Nikita Mishra received the Bachelors (Hons.) and Master's degree in Electronics and communication engineering from Mumbai University, India in 2010, 2014 respectively. From August 2010 to October 2018, she was working as an Assistant professor at Viva Institute of Technology, Mumbai, India. Currently, she is pursuing Ph.D. degree in Electronics and communication from Manipal University, Jaipur. Her research interests are in the areas of security, cognitive radio networks, wireless communication and deep reinforcement learning.

Dr. Sumit Srivastava is currently Professor in Department of Information Technology, Manipal University Jaipur (MUJ). In the past he holds the post of Head of Department Information technology and currently working as Controller of Examination at MUJ. He has done his MCA from BITS Mesra Ranchi, Ph.D. in Data Mining from University of Rajasthan. He has 17 years of Teaching and nearly 12 years of Research Experience. His area of research involves algorithms, data science, knowledge discovery, computational, agent-based modeling, hybrid dynamic systems, decentralized decision making, feature extraction, process mining, and engineering education.

Dr. Shivendra Nath Sharan received doctorate degree from Indian Institute of Technology, Delhi. He worked as a director with School of Electronics and communication in Manipal University Jaipur from 2011 to 2019. Currently, he is Professor and Area Director with Electronics and Communication department in NIIT University, Neemrana, India. His research interest includes Signal Processing, Cognitive Radio network, wireless communication and security.