Circuits, Systems, and Signal Processing (2020) 39:1071–1088
https://doi.org/10.1007/s00034-019-01123-z

An Adaptive Learning-Based Attack Detection Technique for Mitigating Primary User Emulation in Cognitive Radio Networks

S. Arun[1] · **G. Umamaheswari**[1]

Received: 27 February 2019 / Revised: 11 April 2019 / Accepted: 16 April 2019 / Published online: 29 April 2019

Abstract
Cognitive radio (CR) technology is designed to improve reliability in communication between users through efficient and dynamic spectrum exploitation. CRs address the problems in spectrum allocation and channel access and improve the rate of radio resource utilization. The flexibility of the CR networks (CRN) and communication medium exposes it to a variety of threats; primary user emulation attack (PUEA) is a malicious and denial-of-service kind of adversary that defaces CRN performance. This manuscript proposes an adaptive learning-based attack detection in CRN for detecting and mitigating PUEA by analyzing the received power of the transmitter. The learning process endorses some beneficial features by distinguishing low spectrum legitimate PU from an adversary. The learning process adopts cyclostationary feature analysis for distinguishing adversaries and low power PU in CR communications. The process of learning is further enhanced by estimating distance variance and communication time-based analysis for improving the rate of signal classification and SU communication rate. The experimental analysis proves the stability of the proposed detection method by improving the SU throughput, with lesser signal classification time and misdetection probability.

Keywords Adaptive learning · Cognitive radio · Cyclostationary feature detection · Primary user emulation attack · Signal classification

✉ S. Arun
arunphd95@gmail.com

G. Umamaheswari
gumabhaskar@gmail.com

[1] Electronics and Communication, PSG College of Technology, Coimbatore, India

1 Introduction

With the development in communication technology, the problem of spectrum scarcity increases due to heterogeneous wireless user communication. Cognitive radio (CR) is a widely adapted technology to cope up with the user demands by improving spectrum utilization and thus reducing the scarcity problem. Cognitive radio network (CRN) consists of licensed or primary users (PU) and un-licensed or secondary users (SU). The SUs share the unused PU spectrum without interrupting their communications. The licensed frequency spectrum of the PUs is engaged by the un-licensed SUs for improving user-level communications [4]. Spectrum sensing is the fundamental task to discover PU channels that exploit the spatial diversity of the SUs. Spectrum sensing is a challenging task in CRs due to channel overhearing, hidden terminals, shadowing and fading that result in path loss. SUs gain transmission over the PU spectrum by detecting the free spectrum through sensing process. If the PU gains control over the free leased spectrum, SU senses an alternate spectrum to swap their communication. An idle or spectrum un-allocated SU causes interference in the other neighboring channels [15].

Due to the openness and flexibility of the CR network, the network is exposed to threats that degrade the performance of the network. CR facilitates the existence of multiple primary and secondary users with a common spectrum sharing space. The sensing and spectrum detection characteristics are vulnerable for injection of threats in the network [1]. The advantages of the above features are mimicked by adversaries and malicious users to either utilize their spectrum completely or prevent the SUs from accessing resources. This type of attack is labeled as primary user emulation attack (PUEA). PUE is an easy to launch and hard to detect attack that interrupts the dynamic spectrum access of the SU by exploiting jamming [24]. Detection and elimination of these attacks are tedious as the mimicking user utilizes the spectrum band of the legitimate PU. This deceives the CR to get false information about the spectrum and prohibits spectrum access to the SUs. If a PUEA utilizes the entire spectrum, it is preventing the SUs to access radio resources, creating a denial-of-service kind of attack. PUEA also behaves in a selfish manner by occupying the entire spectrum due to which detection and sensing process of SU are retarded [3].

To mitigate the effects of PUE in CR, a range of solutions have been provided in recent years. Localization-based PUE detection is a common method that analyzes the signal characteristics of the PUs. This detection method relies on the channel occupancy of the PUs, differentiating the communicating channel and the occupied illegitimate channel [3, 18]. Physical layer security is designed for securing CR from PUE attacks by integrating authentication features to the PU signals. Contrarily, due to the improvement in channel flexibility, PUE attackers launch multi-channel emulations due to which both location-based and authentication-based securities are defaced [7]. The contributions of this manuscript are:

(i) Designing an adaptive learning method for observing and analyzing the PU spectrum characteristics to detect emulation attacks in CRN. Precise detection of emulation attacks minimizes misdetection and time delay.

(ii) Designing a learning case for differentiating low spectrum and malicious PU to improve the SU throughput and to facilitate higher detection. This differentiation improves the availability of least used spectrum in the network to cope up with the spectrum deficiency problem.
(iii) Analyzing the performance of the proposed ALAD method using different metrics and a comparative evaluation of the same with the existing methods to verify the consistency of the proposed method.

1.1 Related Work

Karimi and Sadough [12] proposed a spectrum access function to improve the rate of SU communication under PUEA. A new transmission rule is defined to maximize the transmission rate of SU by estimating the misdetection probability for the detected attackers. The transmission rule is built by considering the energy decay properties of the PU over each channel during spectrum access.

A novel adaptive resource allocation algorithm [5] is designed for mitigating PUEA and to improve energy efficiency of the CR networks. Resource allocation problem is based on soft decision fusion method that detects the presence of attackers to optimize the network performance. SU selection is approximated using nonlinear and convergence-free maximization of energy efficiency by minimizing energy utilization.

A cooperative spectrum sensing (CSS) scheme is introduced by Ghaznavi and Jamshidi [10] for detecting PUE in CR communications. This probabilistic sensing (P-CSS) method analyzes the power statistics of the users to detect an attacker. The fusion center (FC) decides upon the reliability of the CR user based on the analyzed statistics.

A network manager-based commitment model [21] is proposed to improve the attacker detection probability in CRNs. The network manager performs a channel surveillance strategy to aggregate channel properties and its characteristics. It analyzes the characteristics using string Stackelberg equilibrium to decide on its liability. The reliable PU information is broadcasted to the CR users for securing communication.

Lin et al. [14] proposed a spectrum management protocol for defending against threats in CR-assisted Internet of Things applications (IoT). This protocol incorporates the advantages of IoT architecture and physical CR properties to resolve the security issues in local processing. This protocol performs both dynamic spectrum management and attack detection as it is distributed.

A dynamic spectrum sharing method is introduced by Dong et al. [6] for improving the communication privacy two-tier cognitive networks. This spectrum sharing method employs a rank-based SU preference method for differentiating legitimate CR users. The rank of the SUs facilitates operation time allocation for the CR users based on availability.

Elghamrawy [8] proposed a hybrid genetic artificial bee colony (GABC) algorithm for improving spectrum utilization of the users in cognitive radio networks. This algorithm detects PUE to improve spectrum utilization. This algorithm facilitates precise PU signal detection by the SUs by minimizing the false alarms of the malicious users.

The performance of the algorithm is found to minimize the misdetection factor solving the convergence issues.

The authors in [20] designed a throughput maximization scheme for SUs in the presence of PUEA, in CR networks. Different from the conventional methods, this scheme endorses a weight-based cooperative spectrum sensing (CSS) scheme for minimizing the communication interference of PUEAs. The authors apply Nelder–Mead simplex algorithm to address the problems in weight-based CSS detection.

Madbushi et al. [16] proposed a chaotic tag-based sequencing for detecting and mitigating PUEA in cognitive radio networks. The base station monitors and reports the activity of CRs in the network at the initial stage for attack detection. The signal decoding procedure distinguishes the attacker from a legitimate CR, minimizing detection delay and improving the rate of detection.

A PUEA detection method is proposed in [11] by exploiting the channel information of the CRNs. This method analyzes the channel impulse response between PU and SU to identify the attacker. The impulse response is also used to detect unused spectrum to minimize errors in detection.

Cluster-based distributed cooperative spectrum sensing model [17] is proposed for detecting PUE attacks in cognitive radio networks. In this model, the cluster heads reduce communication delay and improve detection time by periodically communicating with the other clusters. The fusion center is responsible for electing cluster heads. The CHs analyze the receiver power to detect malicious PUs. Besides, this model also improves network performance by optimizing energy and minimizing delay.

A self-decision-based PUEA detection technique is introduced by Khaliq et al. [13] for improving user security in CRN. The adversaries are detected by verifying their location and detecting their energy. Based on the observations, a game-based decision making is adopted by the legitimate users to detect and utilize radio resources. This method achieves lesser cost and improves network lifetime.

Artificial neural network (ANN) is used for classifying known users in cognitive radio network. The classification is extended for identifying PUE by incorporating the advantages of distributed sensor network and node properties. The precision of the neural network improves through a voting system, and an in-range neighbor is used to classify unknown and known users. The software-defined radio (SDR) experiment of ANN classification minimizes signal sorting time with better classification results.

Sevcik fractal dimension in frequency domain (SSMS) and normalized Petrosian fractal dimension (SSMSP) are two spectrum sensing methods [9] proposed to mitigate the impact of PUEA in CR communications. The PUE is identified by classifying the received signal modulation using support vector machines. These methods improve the CR performance by minimizing false alarm and improving detection probability in the network [22].

From the above survey, the process of attack detection is formulated based on different techniques such as clustering [17], fusion center [10] and spectrum analysis [6, 8, 9]. These techniques are focused to improve spectrum utilization by mitigating PUEA, whereas the detection process is least concentrated. The process is complex in determining the presence of the malicious users due to frequent spectrum sharing and allocation. Considering this fact, to leverage the SU throughput, detection of

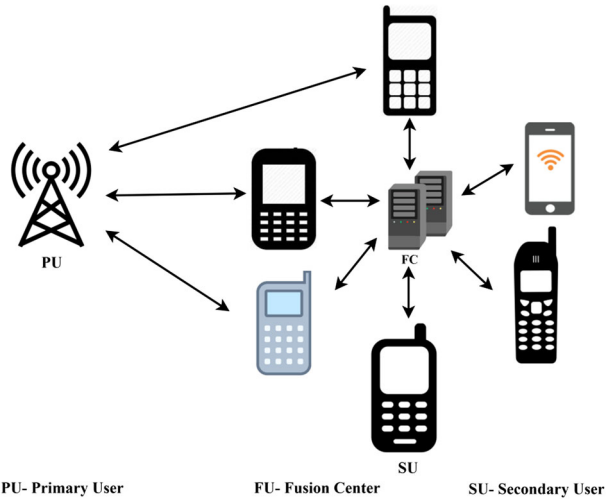

Fig. 1 Network model

attackers is a prominent task. The proposed learning method-based detection enhances the detection rate with the help of cooperative sensing feature of the CRs.

1.2 Adaptive Learning for Detecting PUE Attacks Through Signal Analysis

In the proposed detection method, CS is used to evaluate the PU signals through near to accurate reconstructions. The spares signal reconstruction relies on the distance and path loss errors observed in the transmitted signal. Adaptive learning process verifies the reconstructed signal for rationalizing the errors to differentiate original and PUEA signals [23].

1.3 Network Model

The network is modeled as an undirected graph $G = (N, M)$ where N is the set of CR SUs. The SUs are connected to a PU. The SUs communicate with each other and to the PU through wireless channels represented as M. Figure 1 illustrates the network model. SUs interact with PUs and fusion center (FC) or form independent SU–SU communication [19].

1.4 Attack Model

In this manuscript, primary user emulation attack (PUEA) is considered. The malicious PU mimics the signal of a legitimate PU to make the other user believe them. This kind of attack focuses in attracting the entire spectrum in a selfish manner to interrupt SU communication. The malicious PU replicates the power levels of the legitimate PUs and broadcasts them to lure other users to them. These attacks occupy the entire

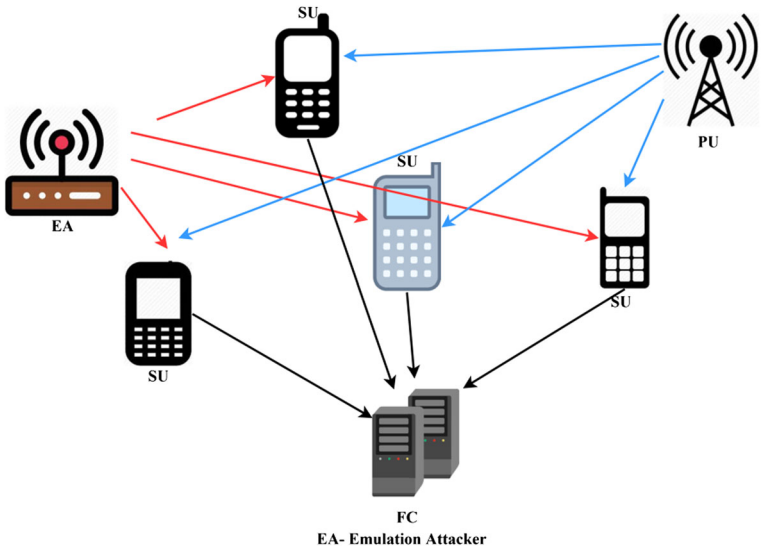

Fig. 2 PUE attack model

channel allocated for the other users to intervene the other radio communication. PUEA launches either a denial-of-service attack or a selfish attack to grasp the entire resource. A model of the PUE attack is represented in Fig. 2.

1.5 Channel and Communication Model

The N SUs communicate using $\{1, 2, \ldots, m\} \in M$ channels in a cooperative manner. The direct interaction between the SUs is enabled using common control channel. The local interference between SUs is controlled by assigning time slots by the FC to accumulate the sensed information. Let s denote the time slots in a channel M where $(s-1)$ slots are used for accumulating sensed information. A single time is used for processing sensed information. SU broadcasts the information to the FC in its allocated time slots.

1.6 Methodology

Detecting PU signals instigates with the observation of received signal power. As free space propagation loss is not ideal for shorter distance, log-normal fading propagation is used to evaluate the received signal power (p_r).

$$p_\mathrm{r} = p_\mathrm{t} + L - 10\eta \log_{10} \frac{d}{d_o} + I \tag{1}$$

where p_t is the transmit power, L is the path loss, η is the exponent for path loss, d_o is the reference distance, d is the distance between transmitter and receiver and I is

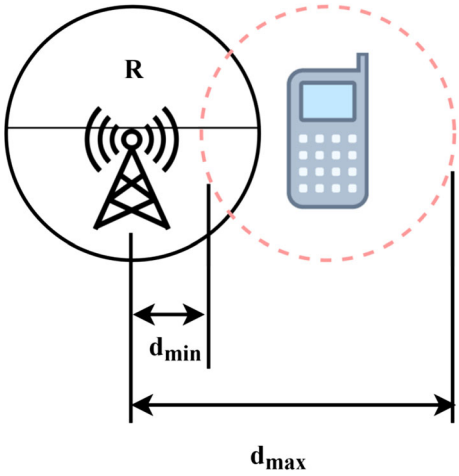

Fig. 3 Distance estimation

a random integer. With the received power, the distance between the transmitting PU and SU is estimated as:

$$d^* = 10^{p_t - p_r}/\eta \tag{2}$$

The above distance is estimated and analyzed with two cases of the received power with respect to the position of the PU. The estimated d^* differs from d due to L observed in transmission. The SU shares the sensing information with the FC for further processing; FC decides the reliability the PU. Let $\mathbb{C}_i$ represent the sensing ability of a SU i to transmit a information through broadcast to its receiver pair. The probability of SU to detect a channel M to communicate at a slot (ρ_d) is estimated using Eq. (3):

$$\rho_d = 1 - \left[\rho(\rho_r|\mathbb{C}_i = 1)\right] \tag{3}$$

Here, $\mathbb{C}_i = 1$ if a PU is presented within the communication range (R) of an SU. With ρ_d, the ρ_r for each $\emptyset_t$ is estimated for the minimum and maximum distance in R of the transmitter.

Now, chances of selecting a transmitter are assessed by the reward-based learning process. In Fig. 3, the minimum and maximum distance $\left(d_{\min} \text{ and } d_{\max}\right)$ within and outside the range of the transmitter is illustrated. The minimum and maximum distance varies the rate of interference in the p_r. The minimum and maximum distance factors are estimated for approximating the detection factor. The detection of malicious users is instigated with their signal strength-based distance that is different for legitimate and mimic users. The learning process operates on this distance to enumerate CS to classify the uniqueness of the signal. The channel occupancy and the time interval of communication are evaluated based on the learning approximated distance factor.

Let d_f be the fixed distance estimated in a conventional manner by knowing the position PU. The difference $|d_f - d^*|$ must be less than the threshold d_{th} for a PU to

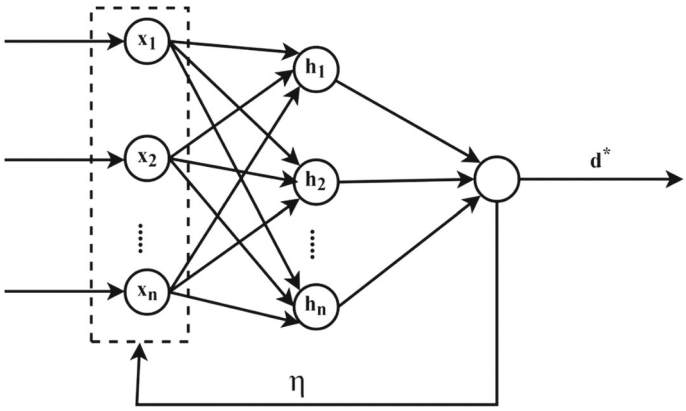

Fig. 4 Learning process

be legitimate. Contrarily, the case is valid for PU with direct communication with SU, whereas a PU with lesser transmission or varying distance (due to mobility) does not fit this condition. This results in increasing misdetection probability, decreasing the rate of reliability. To avoid misdetection, the FC employs an adaptive learning technique to differentiate the following cases:

(i) Legitimate PU
(ii) PU with less communication
(iii) PU is malicious

The learning process is represented in Fig. 4.

The learning technique is fed with a series of distance inputs $\{x_1, x_2, \ldots x_n\}$ that is processed for L and η at the hidden layers $\{h_1, h_2, \ldots h_n\}$. The final output of the learning process is the d^* and η. The η is accounted at the time of processing the next set of distance inputs. The near to precise distance is estimated with the received p_r considering η that has been experienced in the previous learning iterate.

Case 1 If $|d_f - d^*| < d_{th}$, i.e., the difference between fixed distance and observed distance is less than the threshold distance, then the PU is said to be legitimate. On the other hand, the minimum and maximum distance constraints are verified for proper PU estimation. If $d_{min} \leq d_{th} < d_{th}$, then the SU is present in line of sight (LOS) with the PU, and therefore, interference is nearly 0, and hence, error η is computed using Eq. (4):

$$\eta = \left| p_r(d) - p_r\left(d^*\right) \right| \tag{4}$$

The error in distance variation is now more accurately analyzed to get awareness of the actual SU and illegitimate user using the allocation channel. To verify the η

with respect to the density $\emptyset$ of N neighbors for p_r, a normalization error matrix is constructed such that

$$\eta(N,d) = p_i \begin{bmatrix} L_{11}/d_{11} \cdots L_{N1}/d_{N1} \\ \vdots \\ L_{1N}/d_{1N} \cdots L_{NN}/d_{NN} \end{bmatrix} \tag{5}$$

Equation (5) is satisfied when two or more SUs share the same R of a PU. The simple expression of Eq. (5) is expressed for a set of x iterates as:

$$\left.\begin{aligned} \eta(N,d_o) &= p_i\left(L_1/d_0\right) \\ \eta(N,d_1) &= p_i\left(L_0/d_1\right) \\ &\vdots \\ \eta(N,d_n) &= p_i\left(L_{i-1}/d_n\right) \end{aligned}\right\} \tag{6}$$

The FC verifies $|p_r(d) - p_r(d^*)|$ with each of the obtained $\eta(N,d)$. The difference in d_f and d^* between $[d_{\min}, d_{\max}]$ is always less than d_{th} for all the N iterates of the learning process (Fig. 4).

Case 2 The PU is legitimate, but the number of communication through the PU is less.

The learning process concludes that $|d_f - d^*| \geq d_{th}$ as the PUs spectrum is not sensed in at most intervals. Therefore, the cyclostationary feature of the signal is analyzed as the above condition misdetects a legitimate PU as malicious. As the communication interval is sparse, the unused spectrum is influenced by the noise of the neighbors in the sane L. The error reduction feature of the detection minimizes η and L in the least sensed PU spectrum. The error reduction is performed using a signal mean function that is estimated over a time t. The communication through the PU is analyzed in this time and is prolonged for a time period of $(t+s)$. This is analyzed to observe if there are any changes in the communication with the time factor. The observed variation is correlated with the signal strength, time factor and detection approximations to verify the presence of any malicious users. The mean $m(t)$ of a signal $s(t)$ is estimated using Eq. (7) as:

$$m(t) = m(t+s) \tag{7}$$

And the autocorrelation function $c(t)$ is represented as:

$$c(t) = c(t+s_0, \eta) \tag{8}$$

To determine the reliability of the signal from the PU, spectral correlation function $\Delta\mathbb{C}(f)$ is estimated as:

$$\Delta\mathbb{C}(f) = \prod_{s=1}^{\infty} \cdot \prod_{\Delta t=1}^{\infty} \frac{1}{\Delta t} \int_{\Delta t/2}^{-\Delta t/2} \frac{1}{s} \varphi\left(s, f + \frac{\gamma}{2}\right) \varphi\left(s, f - \frac{\gamma}{2}\right) \mathrm{d}t \tag{9}$$

where $\varphi(s, f)$ is the Fourier transform in $(s - s_1), (s_1 - s_2), \ldots, (s_{n-1} - s_n)$ time slots and γ is the set of all Fourier transform functions which are given as:

$$\varphi(s, f) = \int_{t-\frac{s}{2}}^{t+\frac{s}{2}} \varphi(t + \frac{s}{2}) e^{-2\pi f} . \varphi\left(t - \frac{s}{2}\right) . e^{-2\pi f} \mathrm{d}t \tag{10}$$

$$\varphi(s, f) = \int_{t-\frac{s}{2}}^{t+\frac{s}{2}} e^{-2\pi f} \left[\varphi\left(t + \frac{s}{2}\right) \cdot \varphi\left(t - \frac{s}{2}\right)\right] \mathrm{d}t \tag{11}$$

As the time slot for that particular PU communication is of prolonged time, i.e., $0 < t \leq s, s \to \infty$, interference is observed, and hence, $\gamma \neq 0$. This minimizes the p_r that is precisely estimated using a normalization. The normalization of Eqs. (9) and (11) is represented as:

$$\mathbb{C}(f)(d_m)(f) = \frac{\Delta\mathbb{C}(f)}{\sqrt{\left[\Delta\mathbb{C}\left(f + \frac{\gamma}{2}\right) \cdot \Delta\mathbb{C}\left(f - \frac{\gamma}{2}\right)\right]}} \tag{12}$$

The adverse channel effects are removed by normalizing the signal of a least used PU. Now, the error matrix is estimated as:

$$\eta(N, d) = p_\mathrm{r} \begin{bmatrix} \gamma_{11}/d_{11} \ldots\ldots \gamma_{11}/d_{(N-x)1} \\ \vdots \\ \gamma_{1(N-x)}/d_{1(N-x)} \ldots\ldots \gamma_{(N-x)(N-x)}/d_{(N-x)(N-x)} \end{bmatrix} \tag{13}$$

where $(n - x) \in [s, \infty]$ and $(N - x) < N$.

The learning process for Case 2 is illustrated as shown in Fig. 5.

The output of the learning process is assessed at (s + 1) slots at which the communication occurs. The γ obtained in this phase is less than η of a regular PU. Despite normalization and feature detection, if $\gamma > \eta$, then the PU is malicious.

Case 3 If the PU is malicious.

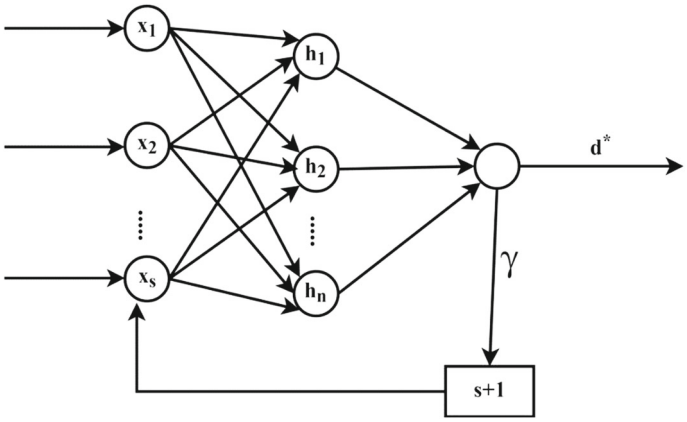

Fig. 5 Learning process when $|d_f - d^*| \geq d_{th}$

Analysis 3 Excluding the Cases 1 and 2, the PUs that are detected are classified as attackers. The exceptions of Case 1 and Case 2 are discussed here. From Case 1, if that $|d_f - d^*| > d_{th}$, then the PU is malicious; the η is estimated as

$$\eta(N, d) = p_r + \sigma\left(\frac{L}{d}\right) \tag{14}$$

where σ is the variance error observed in the PU communication. The error observed in this case is high due to inconsistent data handling and CS observations. The rate of learning is instantaneous to detect the malicious user to prevent additional impact on other channels. The detection process is first assessed using the distance factor. The successive process of detection confirms the detection of malicious users occupying the channel. Unlike the previous cases, matrix normalization is not required for all N neighbors; if any of the neighbor senses the η, then the PU is declared as malicious. To further verify the proof of identification, $|p_r(d) - p_r(d^*)| > \eta(N, D)$ is considered. The malicious user distance (d_m) is estimated using Eq. (15) from Eq. (2):

$$d_m = 10^{(p_t - p_r)/\eta + \sigma} \tag{15}$$

Hence, in this case, the signal received is feeble with errors. Therefore, as per Case 2, the cyclostationary mean of the signal $s(t)$ is given as in Eq. (16):

$$m(t) = m(t + s + \sigma) \tag{16}$$

And autocorrelation function is represented as:

$$c(t) = c(t + s, (\eta + \sigma)) \tag{17}$$

The normalization $\mathbb{C}(f)$ is expected to be:

$$\mathbb{C}(f)(d_{\mathrm{m}}) = \frac{\Delta \mathbb{C}(f,\sigma)}{\sqrt{\Delta \mathbb{C}(f+\sigma)\cdot \Delta \mathbb{C}(f-\sigma)}} \tag{18}$$

$$\mathbb{C}(f)(d_{\mathrm{m}}) = \frac{\Delta \mathbb{C}(f,\sigma)}{\sqrt{\Delta \mathbb{C}[(f+\sigma)\cdot (f-\sigma)]}} \tag{19}$$

where $\Delta \mathbb{C}(f,\sigma)$ represents the spectral correlation with respect to error variance. Both the additive $(f+\sigma)$ and nonadditive variations $(f-\sigma)$ are addressed for normalization with respect to the autocorrelation function represented in Eq. (17), provided the function is determined for the cyclostationary mean of the signal observed between t and $(s+t)$ period for the CS. Equation (19) determines the normalization of sensing function with error, where $\gamma \neq 0$ and $|d_{\mathrm{f}} - d^*| > d_{\mathrm{th}}$.

The transmitting PU that satisfies Case 1 and Case 2 of the learning process is classified as legitimate, and hence, the SU shares the spectrum of the PUs. Contrarily, if the exception cases of 1 and 2 are met, then the PU is illegitimate, and therefore, the FC announces the SU to evade spectrum access of that particular PU. The efficiency of the system is designed as a joint optimization with respect to malicious detection and throughput optimization. The throughput of the SUs is enhanced by detecting malicious SUs by analyzing the error which is distance based on CS. The rate of channel utilization and occupancy of the legitimate users are definite to improve communication rate of the SUs. More precisely, the distance variation as estimated in the learning process confines improper signal strength evaluations to improve the rate of detection.

2 Results and Discussion

The performance of the proposed ALAD is analyzed through simulations performed in network simulator. In this simulation, there are 300 SUs distributed in a region of 2000 m × 2000 m with a communication range of 150 m. There are 10 PUs placed that covers an interference range of 500 m with eight channels operating at a frequency rate of 6 MHz. The path loss factor L is set as one for indoor users and two for outdoor users. The performance of the proposed RL-CSS is analyzed using a comparative analysis with the existing P-CSS [10], ANN-SDR and GABC [8] for the metrics: SU throughput, signal classification time [2], misdetection probability and detection probability. Concentrating the rate of detection based on received signal strength correlating the false alarm is introduced in ALAD. ALAD classifies the PU signals to differentiate legitimate and illegitimate users based on thorough learning process. The lag in the existing methods mentioned above is addressed in the proposed method using cyclostationary analysis. The variations in measurements are presented in the form of analysis, and results are illustrated below. A detailed description of the experimental setup is presented in Table 1.

Table 1 Experimental parameter and values

Experimental parameter	Value
Network region	2000 m × 2000 m
SU	300
Frequency	6 MHz
PU	10
Radio range	150 m
Interference range	500 m
Path loss factor	1/2

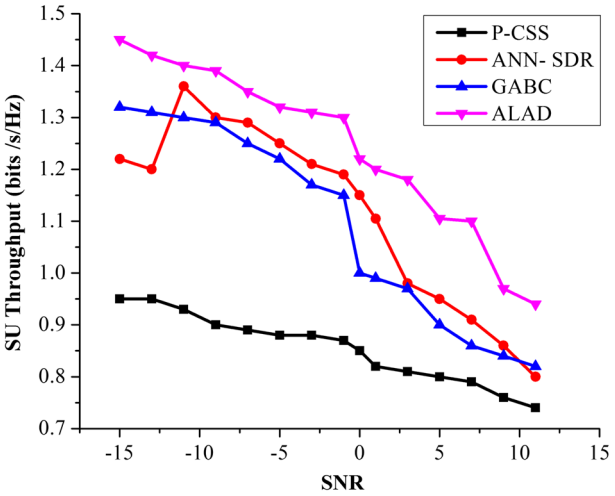

Fig. 6 SNR versus SU throughput

2.1 SU Throughput Analysis

Figure 6 illustrates the comparison of SU throughput between the existing and proposed methods. In the proposed ALAD, the reliability of the PU is classified through two learning cases. This aid SU to detect illegitimate PU more precisely that prevents the SU from accessing their spectrum. This improves the communication rate of SU, retaining higher throughput. Besides, different from the existing methods, the low signal SU is independently identified through a constraint-based learning (Case 2) due to which it is efficiently identified amid the presence of PUEA. The least possible radio resource is also utilized by the SU for communication that adds up SU throughput.

2.2 Signal Classification Time

The conventional signal classification is facilitated by analyzing the L in the received power. In the proposed ALAD, the specific analysis of the signal in Case 2 helps to improve the rate of differentiation. Both least used signal and unknown signal

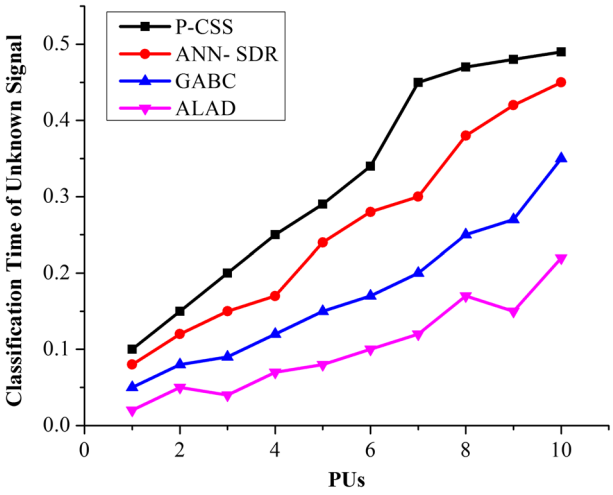

Fig. 7 PUs versus classification time of unknown signal

satisfying $|d_{\mathrm{f}} - d^*| < d_{\mathrm{th}}$(legitimate PU) or $(n - x) \in [s, \infty]$ and $(N - x) < N$ for Eq. (13) (low communication PU) are distinguished through assessment in s and (s-1) intervals. Therefore, both the cases aid ease of signal detection consuming lesser time through appropriate learning instances (Cases 1 and 2). The comparative analysis of the signal classification time is portrayed in Fig. 7.

2.3 Misdetection Probability Analysis

In Fig. 8, the misdetection probability is compared between the existing and proposed methods with respect to false alarm. In ALAD, the learning process is recursive considering the error in the previous output for analyzing the legitimacy of PUs. Case 2 of the learning process analyzes the signal in communication time slots with the L factor in communication. The low signal user is also differentiated from the malicious CR, minimizing the rate of misdetection. The learning Case 1 identifies the legitimacy and Case 2 differentiates the users. Therefore, the chances of misdetection are less; the users in d_{m} are identified as malicious if $|d_{\mathrm{f}} - d^*| < d_{\mathrm{th}}$ for the first iterate. Therefore, the ALAD shows up some misdetection. Obviously, it is less compared to the existing methods, where low signal PU is classified as malicious.

Figure 9 illustrates the comparison of misdetection probability with respect to signal-to-noise (SNR) ratio. The misdetection probability in the proposed method is less (comparatively) due to the classification induced by the learning process. The variation in misdetection occurs as it analyzes the cyclostationary features of a signal for distinguishing from the illegitimate PU signal. The above graph is accounted for one iterate of the learning process; the consecutive learning minimizes the misdetection probability of the proposed ALAD. In addition to the feature classification, distance-based verification minimizes the rate of misdetection. Table 2 presents the SU throughput observed in the corresponding misdetection of the adversary.

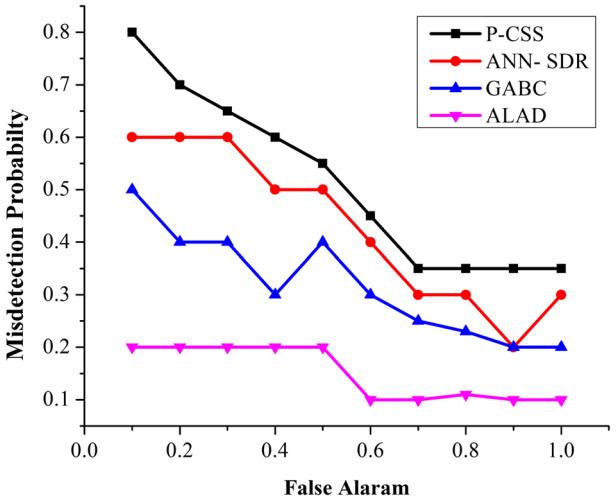

Fig. 8 False alarm versus misdetection probability

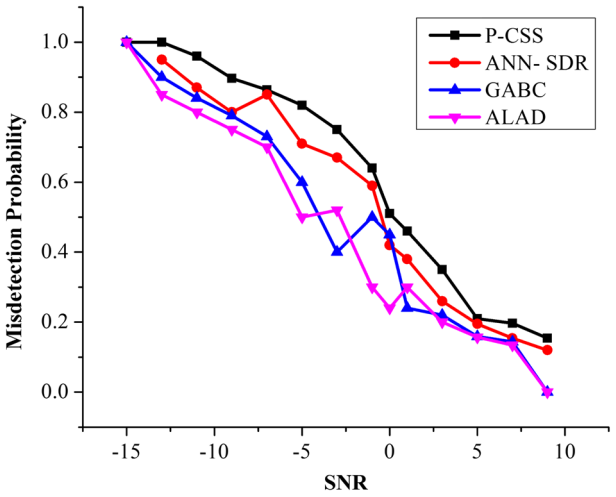

Fig. 9 SNR versus misdetection probability

2.4 Detection Probability

Figure 10 illustrates the detection probability comparison of the existing methods with the proposed ALAD. As mentioned in Fig. 9, the number of iterates minimizes the rate of misdetection for the observed SNR. The rate of path loss L and γ are estimated separately for both legitimate and malicious users. To improve the detection precision, the received signal is analyzed for $\eta(N, d_o)$ to $\eta(N, d_n)$ if the transmitted is legitimate, and for illegitimate users, both $\mathbb{C}(f)(d_{\mathrm{m}})$ and γ are estimated to verify its consistency. Based on the analysis and feature detection in Cases 2 and 3, the user is identified more precisely (in spite of low communication), achieving a higher detection rate in

Table 2 SU throughput and misdetection analysis values

SNR	SU throughput (bits/s/Hz)	Misdetection
− 15	1.45	1
− 10	1.4	0.79
− 5	1.34	0.58
0	1.23	0.28
5	1.11	0.2
10	0.97	0.18

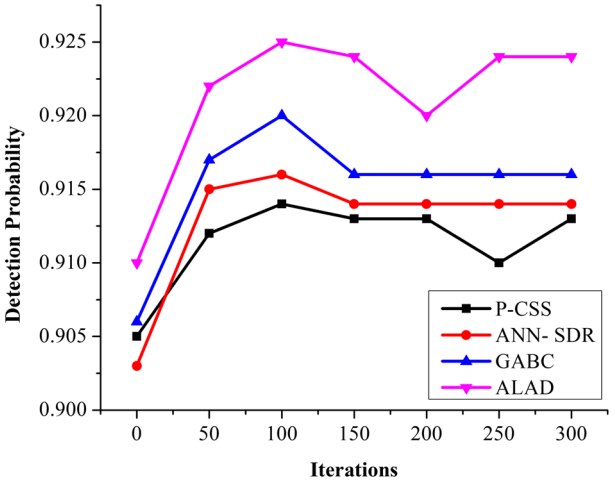

Fig. 10 Malicious SU versus network throughput

Table 3 Experimental data values of the existing and proposed methods

Metric	P-CSS	ANN-SDR	GABC	ALAD
SU throughput (bits/s/Hz)	0.74	0.8	0.82	0.94
Unknown signal classification time	0.49	0.45	0.35	0.22
Misdetection	0.35	0.3	0.2	0.1

the proposed ALAD. Table 3 presents the experimental data values observed for the existing P-CSS, ANN-SDR and GABC and proposed ALAD in order.

In Table 3, the observed analysis is presented. The analysis varies with respect to SNR for throughput, PU density for classification time and false alarm for misdetection correspondingly. The variations are observed from t to $(s + t)$ accounting σ and η for all the iterations of CS process.

3 Conclusion

This manuscript proposes an adaptive learning-based attack detection in cognitive radio networks. The adaptive learning is responsible for detecting and distinguishing legitimate and malicious transmitters by analyzing their signals. The learning method adopts both distance and cyclostationary feature-based analyses for differentiating legitimate users from malicious transmitters. The learning method is reliable for identifying legitimate users through constraint based on communication slots. Experimental results illustrate the consistency of the proposed ALAD by improving SU throughput and detection by 16.31% and 9.67% and minimizing signal classification time and misdetection by 48.53% and 18.3% correspondingly. In the future process of attack detection, self-decision-making opportunistic methods are planned to be incorporated. This improves the rate of detecting a various class of attacks with predetermined unknown signal classification, reducing the time of detection.

References

1. A. Abrardo, M. Barni, K. Kallas, B. Tondi, A game-theoretic framework for optimum decision fusion in the presence of by zantines. IEEE Trans. Inf. Forensics Secur. **11**(6), 1333–1345 (2016)
2. S. Baskar, S. Periyanayagi, P.M. Shakeel, V.S. Dhulipala, An energy persistent range-dependent regulated transmission communication model for vehicular network applications. Comput. Netw. **152**, 144–153 (2019)
3. K.M. Borle, B. Chen, W.K. Du, Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation. IEEE Trans. Inf. Forensics Secur. **10**(10), 2225–2235 (2015)
4. R.L. Chen, J.M. Park, Y.T. Hou, Toward secure distributed spectrum sensing in cognitive radio networks. IEEE Commun. Mag. **46**(4), 50–55 (2008)
5. D. Das, S. Das, Intelligent resource allocation scheme for the cognitive radio network in the presence of primary user emulation attack. IET Commun. **11**(15), 2370–2379 (2017)
6. X. Dong, Y. Gong, J. Ma, Y. Guo, Protecting operation-time privacy of primary users in downlink cognitive two-tier networks. IEEE Trans. Veh. Technol. **67**(7), 6561–6572 (2018)
7. T. Duc-Tuyen, N. Nguyen-Thanh, P. Maille, P. Ciblat, and V. T. Nguyen, Mitigating selfish primary user emulation attacks in multi-channel cognitive radio networks: a surveillance game, in *Proceedings of IEEE Globecom* (2016)
8. S. M. Elghamrawy, Security in cognitive radio network: defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm. Future Gener. Comput. Syst. (2018). https://doi.org/10.1016/j.future.2018.08.022
9. S. Fu, G. Zhang, L. Yang, Spectrum sensing defending against PUE attack based on fractal dimension. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-1427-x
10. M. Ghaznavi, A. Jamshidi, Defence against primary user emulation attack using statistical properties of the cognitive radio received power. IET Commun. **11**(9), 1535–1542 (2017)
11. Q.M. Jiang, H.-F. Chen, L. Xie, K. Wang, On detecting primary user emulation attack using channel impulse response in the cognitive radio network. Front. Inf. Technol. Electron. Eng. **18**(10), 1665–1676 (2017)
12. M. Karimi, S.M.S. Sadough, Efficient transmission strategy for cognitive radio systems under primary user emulation attack. IEEE Syst. J. **12**(4), 3767–3774 (2018)
13. S.B.A. Khaliq, M.F. Amjad, H. Abbas, N. Shafqat, H. Afzal, Defence against PUE attacks in ad hoc cognitive radio networks: a mean field game approach. Telecommun. Syst. **70**(1), 123–140 (2019)
14. S.C. Lin, C.Y. Wen, W.A. Sethares, Two-tier device-based authentication protocol against PUEA attacks for IoT applications. IEEE Trans. Signal Inf. Process. Netw. **4**(1), 33–47 (2018)
15. M.H. Ling, K.-L.A. Yau, G.S. Poh, Trust and reputation management in cognitive radio networks: a survey. Secur. Commun. Netw. **7**(11), 2160–2179 (2013)

16. S. Madbushi, R. Raut, M.S.S. Rukmini, Trust establishment in chaotic cognitive environment to improve attack detection accuracy under primary user emulation. Iran. J. Sci. Technol. Trans. Electr. Eng. **42**(3), 291–297 (2018)
17. M.A. Mirza, M. Ahmad, M.A. Habib, N. Mahmood, C.M.N. Faisal, U. Ahmad, CDCSS: cluster-based distributed cooperative spectrum sensing model against primary user emulation (PUE) cyber attacks. J. Supercomput. **74**(10), 5082–5098 (2018)
18. S.K.S.L. Preeth, R. Dhanalakshmi, R. Kumar, P.M. Shakeel, An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system. J. Ambient Intell. Humaniz. Comput. (2018). https://doi.org/10.1007/s12652-018-1154-z
19. D. Pu, B. Aygun, A.M. Wyglinski, Primary user emulation detection algorithm based on distributed sensor networks. Int. J. Wirel. Inf. Netw. **24**(4), 344–355 (2017)
20. S. Shrivastava, A. Rajesh, P. Bora, Defense against primary user emulation attacks from the secondary user throughput perspective. AEU Int. J. Electron. Commun. **84**, 131–143 (2018)
21. D.T. Ta, N. Nguyen-Thanh, P. Maille, V.-T. Nguyen, Strategic surveillance against primary user emulation attacks in cognitive radio networks. IEEE Trans. Cognit. Commun. Netw. **4**(3), 582–596 (2018)
22. N.N. Thanh, P. Ciblat, A. Pham, V.-T. Nguyen, Surveillance strategies against primary user emulation attack in cognitive radio networks. IEEE Trans. Wirel. Commun. **14**(9), 4981–4993 (2015)
23. N.L. Venkataraman, R. Kumar, P.M. Shakeel, Ant lion optimized bufferless routing in the design of low power application specific network on chip. Circuits Syst. Signal Process. **122**, 122 (2019). https://doi.org/10.1007/s00034-019-01065-6
24. R. Yu, Y. Zhang, Y. Liu, S. Gjessing, M. Guizani, Securing cognitive radio networks against primary user emulation attacks. IEEE Netw. **29**(4), 68–74 (2015)