



Defence against PUE attacks in ad hoc cognitive radio networks: a mean field game approach

Saim Bin Abdul Khaliq¹ · Muhammad Faisal Amjad¹ · Haider Abbas¹ · Narmeen Shafqat¹ · Hammad Afzal¹

Published online: 29 May 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract

Cognitive Radio (CR) is an emerging and promising communication technology geared towards improving vacant licensed band utilization, intended for unlicensed users. Security of Cognitive Radio Networks (CRN) is a highly challenging domain. At present, plenty of efforts are in place for defining new paradigms, techniques and technologies to secure radio spectrum. In a distributed cognitive radio ad-hoc network, despite dynamically changing topologies, lack of central administration, bandwidth-constraints and shared wireless connections, the nodes are capable of sensing the spectrum and selecting the appropriate channels for communication. These unique characteristics unlock new paths for attackers. Standard security techniques are not an effective shield against attacks on these networks e.g. Primary User Emulation (PUE) attacks. The paper presents a novel PUE attack detection technique based on energy detection and location verification. Next, a game model and a mean field game approach are introduced for the legitimate nodes of CRN to reach strategic defence decisions in the presence of multiple attackers. Simulation of the proposed technique shows a detection accuracy of 89% when the probability of false alarm is 0.09. This makes it 1.32 times more accurate than compared work. Furthermore, the proposed framework for defence is state considerate in making decisions.

Keywords Primary user emulation (PUE) attack · Game theory · Cognitive Radio Network (CRN)

1 Introduction

Due to rapid growth in wireless industry there is an immense scarcity of wireless spectrum availability. The core reason of this is the static allocation of spectrum for legacy systems. There are several cases mostly below 3 GHz, where numerous spectrum allocations are made for multiple frequency bands, resulting in a severe competition for reliable access to spectrum resources [1].

Contrary to this, large portions of spectrum are detected sporadically utilized. Mostly, the issue of underutilization or in-occupancy is present in licensed spectrum which is occupied by licensed transmitters.

To cater the scarcity or underutilization issue of spectrum there was a requirement of an approach in which unlicensed users are able to access the licensed spectrum when it is unoccupied by its rightful licensed users. This approach is termed as Dynamic Spectrum Access (DSA) [2]. CR nodes have capability of dynamic spectrum sensing to detect the unoccupied licensed band called white spaces. White spaces have no radio interference, only white Gaussian noise. Secondary CR nodes use these white spaces opportunistically without interfering primary users in the network [3]. DSA technology was also welcomed by Federal Communications Commission (FCC), enabling secondary users to access underutilized TV broadcasting spectrum.

✉ Muhammad Faisal Amjad
faisal@nust.edu.pk

Saim Bin Abdul Khaliq
saimkhaliq.msis14@students.mcs.edu.pk

Haider Abbas
haider@mcs.edu.pk

Narmeen Shafqat
narmeen_shafqat@mcs.edu.pk

Hammad Afzal
hammad.afzal@mcs.nust.edu.pk

1.1 Primary user emulation attack

The core problem behind spectrum sensing is precisely distinguishing Primary User (PU) signal from Secondary Users

¹ National University of Sciences and Technology, Islamabad, Pakistan

(SU) signals. In a CRN, PU has priority over all SUs in accessing the channel. The Network permits secondary user SU to use a specific band till the time primary user is not using it. Still, if the secondary user senses the presence of a primary user, it shifts instantly to another band to avoid interference to the primary user. Moreover, when a secondary user senses another secondary user on a common band, it employs specific techniques for spectrum sharing. Based on the described scenario there lies a potential for malicious SUs to mimic the signature of PUs and get priority over other SUs. This issue is addressed in literature as primary user emulation attack [4]. The advantage of the attack is that an attacker does not have to share resources with other secondary users and get access to full spectrum.

The attack motives are classified into selfish and malicious. In selfish attack, the attacker steals the precious spectrum resources. The attacker does so by averting the legit users contest to get the band by mimicking the characteristics of licensed user spectrum. This attack can be launched by multiple nodes desirous of making a dedicated communication link. On the other hand, the attacker with malicious motives tries to damage the DSA process triggering denial of service. Unlike the first, the attackers do not use the spectrum for their communication needs.

FCC recently used a centralized approach to control PUE problem. In the approach, there is a static master base station (BS) with access to online white-space database [5]. The BS is connected to mobile device users. In order to utilize the spectrum, the devices access the database via the fixed BS. Certain rules applied by FCC are followed and final channel selection decisions are made. A centralized collaborative spectrum sensing approach is also employed in IEEE 802.22 standard [6] in which all secondary users send sensing reports to a BS periodically.

There are problems with this approach. Firstly, it is not viable in certain situations like in military exercises, during disaster situations and in infrastructure less environments. Secondly, there is delay due to central linking overheads. Hence, there is requirement of establishing techniques to detect PUE attacks that do not rely on the above approaches.

There is a lot of research going on to address this issue. Most of the work also depends upon centralized approach where there is a central node or fusion centre where final decisions are made [7,8]. Most commonly discussed methods in the collaborative spectrum sensing concept are hard-combining and soft-combining approaches. In a hard-combining approach decisions are made locally at each node, and reports are sent to a centralized fusion centre, on the other hand, in soft-combining system raw sensing data is sent to the decisive fusion centre. There are some issues in considering centralized fusion centre. First, a network protocol is required to connect each SU to common receiver. Secondly, special relay routes are required for far away nodes

to reach a common receiver. Next, there is requirement of secure, dependable wireless broadcast channels to make the decision known to all secondary nodes. Moreover, linking problems and packet drops can degrade the performance of the whole network. The issue of false reporting is also there which impacts final decisions.

In this work, each node is equipped with a detection system to detect PUEA. This diminishes extra processing workload at a central level as detection is carried out locally. It also reduces communication overheads, as there is no cooperation between nodes besides routing protocols. It also serves to be best in the case where each node has to detect and defend individually without cooperation.

After detection of attacker, the utmost requirement is of a mechanism which enables a node to do its effective defence. Since the attack can be at individual or cluster level and resources (like, power and battery life) are limited, therefore best possible defence strategy is vital. Game theoretical approach is effective in this regard. It proves to be a valuable mathematical framework for analysing decision problems.

1.2 Contribution

To the best of our knowledge the mechanism proposed in this paper has not been used for handling PUE attacks. Moreover, Mean Field Game theory considering multiple PUE attackers in CRN environment is also not applied in the existing work. Specifically, we have made the following contributions in this work.

- Proposed a PUE detection mechanism to enable each node to detect the attacks without incurring additional overheads.
- Proposed a novel mean field game approach which enables the SUs to independently make defence decision (based on their remaining battery life) of whether or not to search for, and switch to a vacant channel.
- Unlike existing work, multiple PUE attackers are considered in the network and the proposed techniques can be implemented in a distributed manner.

The rest of the paper is organised as follows. Section 2 contains literature reviewed. PUEA detection techniques, effects on CRN, and existing papers are discussed in this section. The proposed scheme of PUEA detection is in section 3. The system model, energy detection, and location verification mechanisms are in Section 3. Proposed scheme for making defence decisions, game formulation, mean field game model, transition laws, states, players cost functions, and mean field game system are described in Section 4. The simulation results are discussed in Section 5. The conclusion is in Section 6.

2 Literature review

2.1 PUE detection techniques

An ideal detection scheme should be fast, accurate and efficient. Present research work in PUE detection categorize them into energy detection, location verification, analytical model based detection, feature detection, and received signal strength (RSS) detection techniques.

2.1.1 Energy detection

It is the most widely used technique for spectrum sensing in CRN. The implementation is simple and works by measuring the received signal power level. A typical energy detector cannot differentiate between PU and PUE attacker. The existing energy detectors implicitly presume a primary transmitter. It is considered a simple transmitter verification technique, because it can only recognize signals of other SUs. When it detects an unrecognizable signal, it assumes that the signal is a PU signal. The advantage of this technique is that no prior knowledge of PU signal is required.

2.1.2 Localization-based detection

This is the approach in which signal characteristics and known location of transmitter is used to differentiate the PU from attacker.

2.1.3 Feature detection

In [9] an energy detection technique is presented to identify the users in the frequency spectrum. Later, cyclostationary calculations are made to get the features of the user signal. This data is then used to detect PUE attackers via an artificial neural network. No extra hardware or time synchronization algorithms are needed in this approach.

2.1.4 RSS-based detection

In [10] received signal strength based detection technique is presented, in which PUE attacks are detected without using any location information. No dedicated sensor networks are assumed. Detailed study is done using Fentons approximation and Walds probability ratio test for CRN where PUE attackers are arbitrarily distributed.

2.1.5 Difference between techniques

Energy detection is the signal detection mechanism using a radiometer to specify the presence or absence of signal in the band. The conventional energy detector measures the energy associated with the received signal over a specific

time duration and bandwidth. The measured value is then compared with an appropriately selected threshold to determine the presence or the absence of the primary signal.

RSS based detected is a range based localization algorithm. It is used for determining the distance between nodes. Received Signal Strength Index (RSSI) is used to approximate the distance between the receiver and the transmitter using another value called Measured Power (MP). MP is a constant which indicates what's the expected RSSI at a distance of 1 meter to the transmitter. Combined with RSSI, it allows you to estimate the distance between the receiver and the transmitter. Compared with energy detection and RSS based detected, feature detection requires a priori information of the PUs to operate efficiently.

2.2 Effects of PUE attacks on CRN

The whole operation of a CRN can be jeopardised by attackers capable of emulating a PU and denying the use of spectrum to SUs in the CRN. A successful attack can result in wastage of bandwidth and degraded quality of service. Furthermore, it can also cause interference to the PU network, originate connection issues, and enforce denial of service.

This attack has the capability to target both the types of CRs such as learning radios and policy radios [43]. In the scenario of policy radios, the effect of the PUE attack cease to exist when the attackers leave the channel. The SUs claim the channel considering it idle. On the other hand, in learning radios, data about the PUs current and the past behaviors are gathered in order to know when the channel gets idle. The attackers perform this attack when the channel gets idle. There are various therapies to solve this PUE attack.

2.3 Defence techniques against PUE attacks

Sometimes the aim of the malicious nodes in the network is to disturb the communications of the legitimate CR nodes. Even if the detection system has exposed the malicious nodes, they can still continue transmission and interfere with secondary users. In such a scenario, there is a need of a defence system like, special RF-signal processing receivers at each node to recover the real signal. Different defence strategies can be applied at different layers to tackle PUE attacks.

- *Physical Layer*: Special practises e.g. source separation via signal design, and adaptive arrays smart antennas to handle the interference from PUE attackers can be used.
- *Link Layer*: Radio Resource Management (RRM) tactics e.g. spectrum scheduling, admission control etc. can be applied to uphold performance of CRN.
- *Network Layer*: To deal with detected PUE attackers in a CRN, a location-based cognitive routing strategy can be

applied. In this technique, the SUs matching the location of the attackers are neglected.

- *Cross-Layer Approach*: In this approach, mechanisms at different layers are jointly synchronized to defend PUE attacks. Attacks are characterised and best defending strategy is employed.

Several research papers have covered aspects, such as routing, quality of services, spectrum sensing etc. In addition, security is also a prime research focus, being a rock in the wide adoption of CR ad hoc networks. Limited computational ability, exhaustible batteries, vague physical network boundaries are some limitations which make typical security techniques ineffective in infrastructure-less environment. Some protocol vulnerabilities are discussed in [11]. User authentication schemes proposed for similar environments are discussed in [12–14]. Hence, there is an effective need of developing intrusion detection system (IDS) along with an effective defence mechanism for tackling active and passive attacks [15]. There are two research approaches geared towards securing networks: prevention approach and detection approach [16,17]. In this paper, IDS in ad hoc networks and PUE attack specific systems mechanisms are scrutinized.

Majority of the IDSs are signature based and use known attack patterns to compare signatures for intrusion detection. There are a number of performance parameters. In [18] [19] the number of detection libraries and signatures are the performance parameters. Large amount of detection and signature libraries ensure successful detection of a number of known attacks. However, this will reduce systems throughput because of increased computation. Moreover, limiting the databases will provide better performance but make the system weak. In short, there is always a case of finding the middle ground between performance and security strength [20].

In [21], Zhang and Lee presented the requirements needed for IDS to work in Mobile Ad-hoc Network (MANET) environment along with a detection and response mechanism. In their work, each node has an independent IDS agent for detection and reaction. Authentication is done as a reaction to the detection process. The nodes which fail to authenticate are rejected from the network.

In [22], a distributed design for IDS facilitated by mobile agents is presented. In this scheme, each node has a local intrusion detection system (LIDS). Each system can take actions locally and cooperatively with others by exchanging data. Data includes local intrusion alerts and security data detected through collaboration with other LIDS. This data collection is vital for investigating intrusions.

Ferraz et al. in [23] presented a Trust-based Exclusion Access-control Mechanism (TEAM). It provides a full-bodied and distributed access control mechanism based on trust models to provide security and cooperation modes in

the network. It segments the access control process into two settings: local and global. The duty of the local context is to inspect and inform the global context about mistrustful behaviour.

Ruiliang Chen and Jung-Min Park in [24], proposed two tests to detect PUE attacks. Distance Ratio Test (DRT) evaluating signal strength and, Distance Difference Test (DDT) evaluating signal phase difference. The approaches were based on trusted nodes termed Location Verifiers (LVs). The core problem in this was that the system can be dodged if attack is launched from the location of the PU transmitter. Tight synchronization is also a must between LVs.

The author in [25] presented a location based approach termed LocDef. It relied on Wireless Sensor Networks (WSN) to log RSS values. The logged measurements were then compared to known RSS measurement of the PU.

In [26,27] a location based approach is presented which employ TDOA and FDOA. Its a passive localization method which relies on the arrival time difference of the transmitted pulses. It does not require any previous knowledge of the pulse time. In the end the location estimation is computed. The downside of this is that many confining assumptions are made making it suitable for a specific type of CRN.

The author in [28] presented fingerprinting approach that is used to authenticate source. This gives better results but increases signal processing and sensing time. It also increases storage needs.

Hadi Otrok in [29], provided an intrusion detection system for cluster of nodes. Election for the head node (providing services of IDS) is done within the whole cluster to reduce the overheads. To increase their IDSs effectiveness they proposed a framework to stabilise the resource consumption among the cluster nodes. This increased the lifetime of the whole network. The approach is also able to catch and penalize a misbehaving leader by checking his behaviour. A cooperative game theoretical approach is introduced to model the interaction between nodes and limit the false-positives. A checking approach is also introduced to limit the performance overheads of checking nodes. To resolve the game, they found a Bayesian Nash Equilibrium to determine the detection strategy of leaders in a network.

Several researchers have applied mean field games and approximation methods to solving typical wireless network problems [30–33]. In [34] Y. Wang presented a system model, mean field game formulas, approximate approach of process, and the solution to the game for MANETs. In addition, the paper also includes updating function, and cost formulation. Moreover, an example to illustrate the derivation of defending strategy is also presented in the paper. The paper considers the scenario of a single attacker attacking the MANETs. This work can also be applied to vehicular ad-hoc networks.

There are Quality of Service (QoS) aware protocols that consider QoS parameters for path selection. This type of rout-

ing is achieved by comparing multiple intelligent methods. Among these, Genetic Algorithm (GA) is one of the most prevalent methods. A Fuzzy GA is employed for QoS routing [39]. The GA-based routing algorithm lead to the development of a heuristic methodology for MANETs. Cellular Automaton (CA) is capable of resolving various complex issues in MANET. The author in [40] presented a hybrid scheme which integrate GA with CA to improve efficiency. In the work, two QoS parameters are considered for routing; energy and delay. A set of routes that fulfill the delay constraints are selected based on CA routing algorithm and then GAs are used to find the best one.

In [41], a distributed and adaptive resource management approach was proposed in cloud-assisted CR vehicular networks. Furthermore, in the scenario of CR-based Internet of Things (IoT) networks [42], random access protocol is designed. In [42] the author presented a fair channel grouping scheme. The paper considered both the competition and the fairness between SUs, by modeling secondary random access as a multi-armed bandit problem.

The authors in [44] presented a reputation-aware collaborative spectrum sensing framework for ad hoc CRN. The scheme can detect malicious SUs reliably and make decisions under SSDF attack. The mechanism is designed for the scenarios where PU has a smaller transmission range as compared to the CRNs coverage area. In [45], a game theoretical framework is presented to make choice of channels to maximize channel utility in the presence of malicious induced-attacks.

The authors in [46] have proposed an unsupervised scheme to distinguish CRs from PUs irrespective of static and mobile users. In their work, K-means and graph theory work in-parallel to improve detection results.

3 Proposed scheme of detection

In this section, the proposed PUE attack detection technique is presented. It is the basis for the proposed defence technique against PUE attacks, presented in Sect. 4. (Table 1) lists the notations used in our proposed scheme.

3.1 System model

In the system model, there are N nodes of ad hoc cognitive radio network. Each node is equipped with an IDS. The primary user is a static base station (like. TV broadcasting tower). The system is under attack by M number of PUE attackers as shown in Fig.1.

3.1.1 Assumptions

Both malicious and legit secondary users are uniformly distributed over an area. A PU transmitting output power is

hundreds of watts and corresponding range is several tens of miles. Each CR node is assumed to be location aware and has a maximum transmitting power of few watts, having range of few hundred meters. The attackers are self-aware and have coordination i.e. at a given time only one attacker will launch an attack in a specific band. The attacking nodes are capable of varying their frequency, transmission power and modulation scheme.

3.2 Basic operation

Each node has a detection system comprising of following components; a signal processing box, energy detection box location verifier and decision box as shown in Fig. 2 whereas the overall proposed PUE attack detection scheme is shown in Fig. 3. Every secondary user cognitive radio in the network can detect the presence or absence of a user in a specific band. Consider the binary hypothesis testing model which is dependent on the state of primary user.

Hypothesis 0: \mathbf{H}_0 (signal is absent)

Hypothesis 1: \mathbf{H}_1 (signal is present)

$$\begin{cases} \mathbf{H}_0 : y(t) = \omega(t) \\ \mathbf{H}_1 : y(t) = h.x(t) + \omega(t) \end{cases} \quad (1)$$

Where, $y(t)$ is received signal, $x(t)$ is signal transmitted, $\omega(t)$ represents Additive White Gaussian Noise with zero mean and variance σ^2 , h is gain coefficient of channel. It is represented as $h_r + jh_i$, and is constant for each spectrum sensing period.

The Eq. (1) can also be revised as:

$$y(t) = b.x(t) + \omega(t) \quad (2)$$

Here b is 0 for \mathbf{H}_0 and 1 for \mathbf{H}_1 . After that, the signal sampling is done in observed interval t by signal pre-processing box to generate sampled energy vectors $e[n]$ (where $n = 1, 2, \dots, N_s$) and combined energy E_c . Here, energy vector is $e[n] = |y^2(n)|$. The combined energy is $E_c = \sum_1^{N_s} e[n]$. The average energy can be expressed as:

$$E = \frac{1}{N_s} \sum_1^{N_s} e[n]$$

Our proposed energy detection scheme is based on Urkowitz classic model [38]. The input signal $y(t)$ is passed via a Band Pass Filter with centre frequency f_o and bandwidth W , with transfer function

Table 1 Notations

H_0	Hypothesis for signal is absent
H_1	Hypothesis for signal is present
$y(t)$	Received signal
$x(t)$	Transmitted signal
$\omega(t)$	Additive White Gaussian Noise (AWGN) with zero mean and variance σ^2
h	Channel gain coefficient. Represented as $h_r + jh_i$
$e[n]$	Sampled energy vectors (where $n = 1, 2, \dots, N_s$)
s	Test statistics of energy detector
a_0, a_1, a_2	Three thresholds in threshing box
H_1	Hypothesis for a real PU signal
H_2	Hypothesis for a PUEA signal
P_{md}	Probability of miss detection
P_{fa}	Probability of false alarm
P_d	Probability of detection
N	Real Gaussian distribution
$s_j(t)$	State of attacking player n_j at time t
$a_j(t)$	Action of attacking player n_j at time t
$s_i(t)$	State of defending player n_i at time t
$a_i(t)$	Action of defending player n_i at time t
$\alpha_{E_j}, \alpha_{I_j}$	The energy and the information weights of attacker n_j
$\alpha_{E_i}, \alpha_{S_i}$	The energy and the security weights of defender n_i
$S^{(N)}(t)$	Mean state of defending players, The rate of existence of the states in CRN of N nodes at time t
$T_j(y x, a_j)$	State transition laws of attackers n_j
$T_i(y x, a_i)$	State transition laws of defenders n_i
$\theta(t)$	Limiting process which is used in calculation of $S^{(N)}(t)$
p_i	Defenders n_i security value as a result of successful defence
q_i	Defenders n_i security value as a result of unsuccessful defence
r_i	Rate of successful defence
Π_j	Attackers tactics
Π_i	Defenders tactics
T_{rev}	Matrix to reverse the function Φ

$$H(f) = \begin{cases} \frac{2}{\sqrt{N_o}}, & |f - f_o| \leq W \\ 0, & |f - f_o| > W \end{cases} \quad (3)$$

Where, N_o is the one-sided noise power spectral density, it is found helpful in computing false alarms and detection probabilities. This pre-filter reduces the noise and stabilizes the noise variance. The integrator’s output is directly proportional to the energy of the signal received.

On applying Neyman–Pearson criterion on the problem, the likelihood ratio for the hypothesis test can be expressed as [35].

$$\Lambda_{LR} = \frac{f_y|H_0(x)}{f_y|H_1(x)} \quad (4)$$

Here, probability density function (PDF) of the received signal y under hypothesis H is $f_y|H_0(x)$ The log likelihood

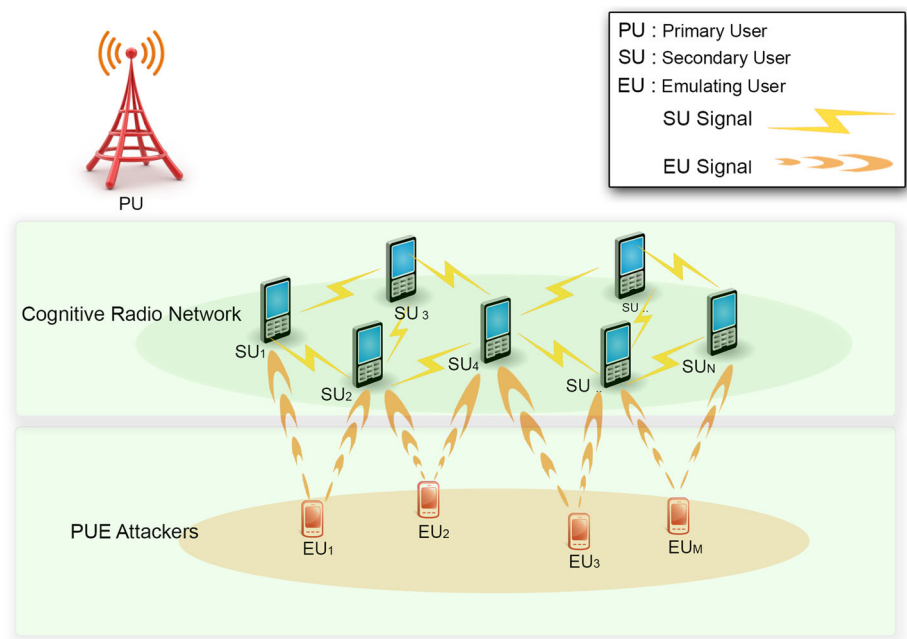
ratio (LLR) is given by $a + b \sum_1^{N_s} e[n]$ where N_s is the number of samples. The terms a and b are independent of signal $y(n)$. Log likelihood ratio is directly proportional to $\sum_1^{N_s} e[n]$ which is energy detector’s test statistic. This indicates that, when the receiver has knowledge of signal power, the energy detector is the best non-coherent detector for any type of Gaussian signal $s(n)$, with the uncorrelated noise [36] (Fig. 3).

After applying filter, energy sampling, squaring, and integrating of values, the statistics of detector can be written as:

$$\Lambda = \sum_1^{N_s} |y[n]|^2 = \sum_1^{N_s} |e_r(n)^2 + e_i(n)^2| \quad (5)$$

Here $e_r(n) = bh_r s_r(n) - bh_i s_i(n) + w_r(n)$ and $e_i(n) = bh_r s_i(n) - bh_i s_r(n) + w_i(n)$. Where, r and i are real and imaginary component.

Fig. 1 Cognitive radio network under PUE attack



Next, the combined energy is compared to three thresholds in a thresholding box to differentiate between a real PU and a PU emulating attacker. The thresholds are represented as a_0, a_1, a_2 . Where, $a_0 < a_1 < a_2$, and a_0 is the native threshold of an ordinary energy detector. If energy $E < a_0$ then there is no activity on the channel and no primary user or emulating attacker present. The thresholds a_1 and a_2 are designed to differentiate the primary from emulating user. If energy is between a_0 and a_1 , or greater than a_2 (i.e. $a_0 < E < a_1$ or $E > a_2$) then it's a PUE attacker. Else, if energy is between a_1 and a_2 (i.e. $a_1 < E < a_2$) it's considered a valid PU signal.

In a conventional energy detection algorithm, a trust-based mechanism is used to differentiate between secondary and primary users. A secondary user can recognize only other secondary users. Therefore, if a secondary user cannot recognize the signal, it's considered a PU's signal. This characteristic can be easily utilized by the attacking secondary users. A malicious secondary user can fabricate an unrecognizable signal by transmitting at a higher power than other nodes, pretending a PU and refuting spectrum resources to other SUs. The idea behind using the energy thresholds to discriminate between attacker and primary user is that it is very difficult for the malicious secondary user to mimic the transmission power of a legitimate primary user.

Despite the distributed architecture of the CR network, nodes share certain information and knowledge of channel characteristics. If a few SUs are allocated to measure the real PU received power and then share with other SUs, the fake PU detection probability can be increased.

After clarity by comparison with thresholds that there is an attack or not, the detection process ends and control goes

straight to the decision box. Else, the more detailed information in the sampled energy vector $e[n]$ is dispatched to the location verifying box.

Based on the proposed concept, the hypothesis test with H_0, H_1 and H_2 , where they signify absence of signal, presence of PU signal, and PUEA signal respectively, are represented as:

- H_0 : No signal ($E < a_0$)
- H_1 : Real PU signal ($a_1 < E < a_2$)
- H_2 : PUE attacker signal ($a_0 < E < a_1$) or ($E > a_2$)

Depending upon these criteria, the detection system can face the following threats:

- *Probability of Miss Detection (P_{md})*: It is the probability of the scenario in which an attacker is considered a primary user. From the attacker's perspective, it is the probability of a successful PUE attack.
- *Probability of False Alarm (P_{fa})*: It is the case when a legitimate primary user is considered an attacking user by the system.

In testing, the interest is in the probability of detection P_d and the probability of false alarm P_{fa} .

As there are a large number of samples, the central limit theorem (CLT) is applied. The main idea is to get clarity on the uncertainties of the whole population by looking at smaller samples. The theorem states that for K number of random values with finite mean and variance, they approach a normal distribution when there are a large number of samples. By

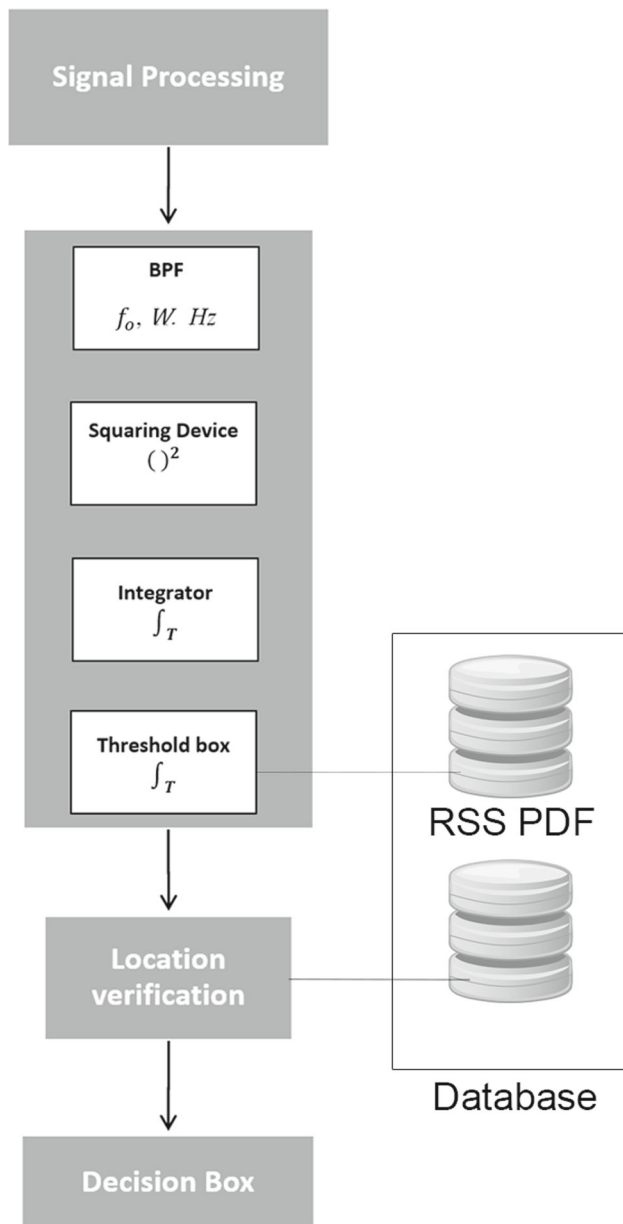


Fig. 2 Architecture of proposed PUE attack detector

applying CLT to the test statistics (5) the accurate approximation with a normal distribution for a big sample set is given as:

$$\Lambda = N \left(\sum_1^{N_s} \mathbf{E}[|y[n]|^2], \sum_1^{N_s} \mathbf{Var}[|y[n]|^2] \right) \quad (6)$$

For multiple signals the mean and variance can be given by:

$$\mathbf{E}[|y(n)|^2] = \begin{cases} 2\sigma_w^2 & : \mathbf{H}_0 \\ 2\sigma_w^2 + |h|^2 |s(n)|^2 & : S1 \\ 2\sigma_w^2 + |h|^2 |2\sigma_s^2|^2 & : S2 \end{cases} \quad (7)$$

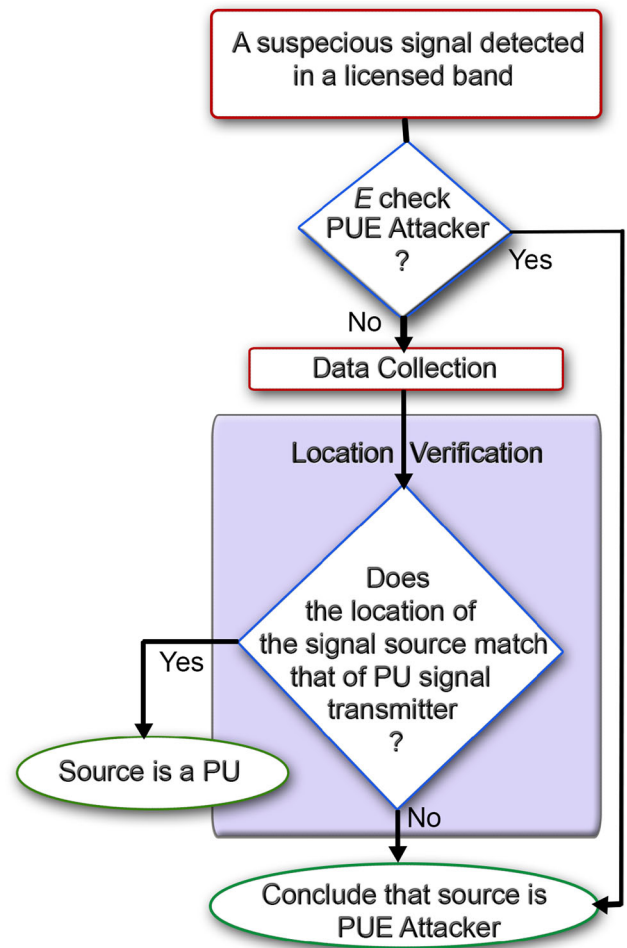


Fig. 3 PUE attack detection scheme

$$\mathbf{Var}[|y(n)|^2] = \begin{cases} (2\sigma_w^2)^2 & : \mathbf{H}_0 \\ 4\sigma_w^2 (\sigma_w^2 + |h|^2 |s(n)|^2) & : S1 \\ 4(\sigma_w^2 + |h|^2 \sigma_s^2)^2 & : S2 \end{cases} \quad (8)$$

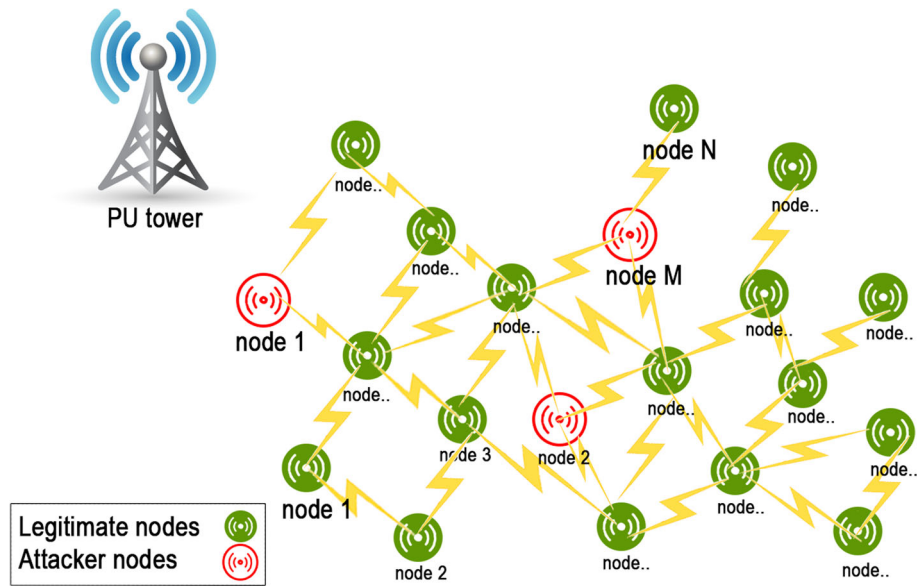
The distribution Λ can be given as:

$$\Lambda \sim \begin{cases} (K(2\sigma_w^2), K(2\sigma_w^2)^2) & : \mathbf{H}_0 \\ (K(2\sigma_w^2)(1-\gamma), K(2\sigma_w^2)^2(1-2\gamma)) & : S1 \text{ complex - PSK} \\ (K(2\sigma_w^2)(1-\gamma), K(2\sigma_w^2)^2(1-\gamma)^2) & : S2 \end{cases}$$

Using mean and variance in the above equation, the false alarm probability P_{fa} is approximated as:

$$P_{fa} \approx Q \left(\frac{a - N(2\sigma_w^2)}{\sqrt{N}(2\sigma_w^2)} \right) \quad (9)$$

Fig. 4 An N node CRN with M attackers



Here, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{u^2}{2}} du$ is the Gaussian-Q function. Likewise, detection probability P_d is given by:

$$P_d \approx Q\left(\frac{a - N(2\sigma_w^2)(1 + \gamma)}{\sqrt{N(1 + 2\gamma)}(2\sigma_w^2)}\right) \tag{10}$$

Consider, $P_d(a_1, a_2)$ and $P_{fa}(a_1, a_2)$ which represent the probabilities of primary user emulation attack detection and false alarm, respectively.

$$P_d(a_1, a_2) = P_r\{a_0 < E < a_1 | H_2\} + P_r\{E > a_2 | H_2\} \tag{11}$$

$$P_{fa}(a_1, a_2) = P_r\{E < a_1 | H_1\} + P_r\{E > a_2 | H_1\} \tag{12}$$

As stated above, each node in the network is location aware and maintains a database having the location figure prints of real PU and PUE attackers. This location authentication classifies the source of the processed signal from PU and attackers. The SU scan the energy vectors and approximate the source position by getting the top corresponding entry in the database.

In this scenario, if the approximated location of signal origin deviates the known location of the PU tower in the database then the signal source is considered an attacker regardless of the identical signal characteristics. The attacker may also try to dodge the location detection system by transmitting from the location of the PU tower. In that case, the energy detection system kicks in, and identify the attack. The reason of success in this scenario is that it is infeasible for the attacker to imitate both energy level and location of the PU because of its lower transmission power. Once, the source is branded as a PUE attacker its location and energy level is logged in database for future reference.

4 Proposed scheme for defence

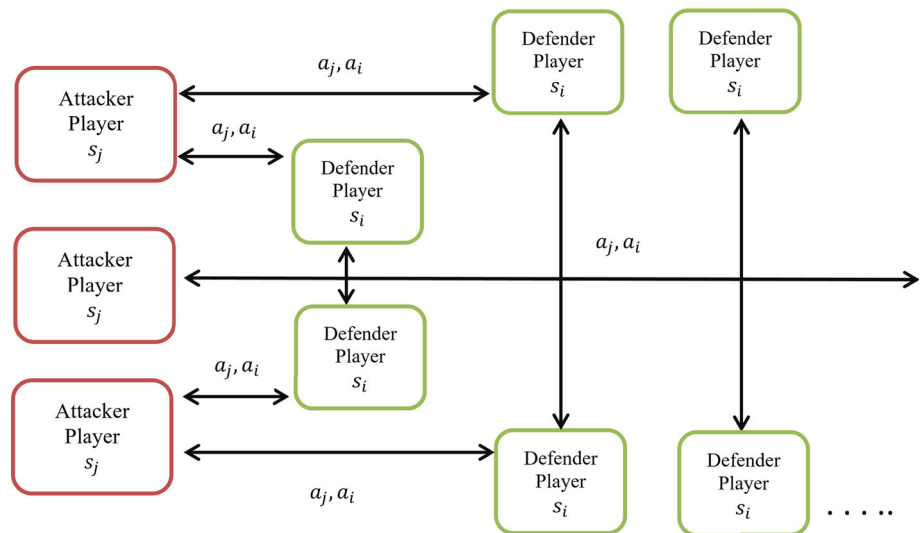
After proposing detection scheme, in this section a game theoretical approach is presented for enabling each node to make better strategic defence decisions. An (N+M) Mean Field game theory is introduced for catering the scenario of multiple attackers.

4.1 Game model and formulation

The Fig. 4 shows an N-node CRN and M attackers which can launch attacks on the nodes dynamically. The legitimate nodes of network are autonomous because of no centralized management. Like a real game there are some rewards in case of a successful attack by attacker (like, secret information). Similarly, attack statistic is given to the defending node in case of a successful defence strategy. Each node has to pay a cost in the form of power consumption for deploying a defence or attack strategy.

To model the case as an (N+M) Mean field game in Fig. 5 all legitimate nodes are considered as N defending players. In addition, the malice nodes which attack the network are M attacking players. The attacking players state space and action space are $S_j = \{1, \dots, K_j\}$ and $A_j = \{1, \dots, L_j\}$, respectively. Similarly, the defending player's state and action spaces are $S_i = \{1, \dots, K_i\}$ and $A_i = \{1, \dots, L_i\}$, respectively. At time $t \in \{0, 1, 2, 3, \dots\}$, the attacker $n_j, j \in (1, \dots, M)$ state is $s_j(t)$ and action is $a_j(t)$. Similarly, the state and action of a defending node $n_i, i \in (1, \dots, N)$, are denoted as $s_i(t)$ and $a_i(t)$ respectively. All the defence actions that can be applied by the defenders (e.g. RRM techniques, special location-based routing techniques etc.) to handle PUEA, are in their action sets.

Fig. 5 Mean field game model of CRN representing states and actions of attackers and defenders



To demonstrate the interaction between the attackers and the defenders the game is a non-cooperative game. We interpret that each defender has a value of security for a CRN. Consider that the value of a protected asset is 1 and loss of security value is -1 . It is also considered that the loss of a defending node is equal to a gain of the PUE attacking player.

4.2 Defining transition laws, states and cost functions

The states of the attacking players can be interpreted as an amalgam of energy and possessions (Like, knowledge). It is denoted in [33] as:

$$\alpha_{E_j} E_j + \alpha_{I_j} I_j \tag{13}$$

Here, α_{E_j} and α_{I_j} signify the energy and possession weights, respectively. Likewise, the state of defending player can be expressed as a amalgam of energy and security of functionality of system, respectively. Its denoted as:

$$\alpha_{E_i} E_i + \alpha_{S_i} S_i \tag{14}$$

Here, α_{E_i} and α_{S_i} symbolize the loads of the energy and the security, respectively. If $S^{(N)}(t)$ is mean state of defenders, then:

$$S^{(N)}(t) = \left(S_1^{(N)}(t), \dots, S_K^{(N)}(t) \right) \quad (t \geq 0) \tag{15}$$

State transition laws of attacker and defender players respectively are:

$$T_j(y|x, a_j) = P(s_j(t+1) = y | s_j(t) = x, a_j(t) = a_j) \tag{16}$$

Here, $x, y \in S_j$ and $a_j \in A_j$

$$T_i(y|x, a_i) = P(s_i(t+1) = y | s_i(t) = x, a_i(t) = a_i) \tag{17}$$

Here, $x, y \in S_i$ and $a_i \in A_i$.

4.2.1 Attacker player’s cost

The costs of the attacking players can be expressed by:

$$c_j(s_j(t), a_j(t), S^{(N)}(t)) = f_j(s_j(t), a_j(t)) - f(S^{(N)}(t)) \tag{18}$$

Here, $f_j(s_j(t), a_j(t))$ is the combined energy cost when attacker adopts various actions in different states. $f(S^{(N)}(t))$ is the payoff of the attacker which is as a result of strike. When a state has full energy, the attacking player can decide to attack the whole CRN. The energy cost is elevated in this case than the state of low energy. Attacking players will not attack in poor energy state.

4.2.2 Defender players cost

The cost of a defending player i can be expressed by:

$$c_i(s_i(t), a_i(t), s_j(t), a_j(t), S^{(N)}(t)) = g_i(s_i(t), a_i(t)) + g_{ij}(S^{(N)}(t), s_j(t), a_j(t)) \tag{19}$$

In the equation $g_{ij}(S^{(N)}(t), s_j(t), a_j(t))$ is the collective cost when the representative defender adopts different actions.

4.3 Mean field game formulation

The mean field game can be expressed as in [33]:

$$\theta(t + 1) = \Phi(x_j(t), \theta(t)) \tag{20}$$

Here, $\theta(t)$ is the limiting process which is used in calculation of $S^{(N)}(t)$. The aim is to reduce complexity. This is required because it is difficult to directly find $S^{(N)}(t)$ in ad-hoc environment. As shown before, $S^{(N)}(t)$ represents the mean state of all the defenders in dynamically changing topology and without central management. Therefore, limiting process $\theta(t)$ is the process which is used in calculation of $S^{(N)}(t)$. Here, the equation describes that the update of random process is done by the current state of attacker and the mean state of CRN.

4.3.1 Limiting function and updating rule

For the system description consider a matrix of size $n \times n$:

$$\begin{aligned} & \text{Transition}(s, \theta) \\ &= \begin{bmatrix} T(1|1), \hat{\pi}(1, s_j, \theta) & \cdots & T(n|1), \hat{\pi}(1, s_j, \theta) \\ \vdots & \ddots & \vdots \\ T(1|n), \hat{\pi}(n, s_j, \theta) & \cdots & T(n|n), \hat{\pi}(n, s_j, \theta) \end{bmatrix} \end{aligned} \tag{21}$$

The function Φ from (20) can be written as:

$$\Phi(s_i(t), \theta(t)) = \theta \text{Transition}(s, \theta) \tag{22}$$

To reduce complexity, suppose that each defending player has two states 0 and 1. This defines the limiting function as: $\theta(t)$ = Probability of first state, Probability of second state or

$$\theta(t) = \{\theta_0(t), \theta_1(t)\}.$$

For $\theta(t)$ the updating rule is given by $(\theta \in [0,1])$:

$$\Phi = s_j(\theta)^{1/2} + (1 - s_j)(\theta)^2 \tag{23}$$

When the attackers are in the state 0 or 1 the function Φ is transformed as:

$$\Phi = \begin{cases} (\theta)^2, & (s_j = 0) \\ (\theta)^{\frac{1}{2}}, & (s_j = 1) \end{cases}$$

4.3.2 Effect of mean field on the cost functions

Consider $(1 - r_i)q_i$ is attackers reward as a result of a successful PUE attack then the defending players respective security value will be $r_i p_i - (1 - r_i)q_i$. r_i is the rate of successful

defence while, q_i is loss of security value as a result of failed defence attempt. The updated cost functions on considering the effects of mean field to players is:

$$\begin{aligned} & c_j(s_j(t), a_j(t), \theta(t)) \\ &= f_j(s_j(t), a_j(t)) - \theta(t) \sum_{i=1}^N (1 - r_i) q_i \end{aligned} \tag{24}$$

$$\begin{aligned} & c_i(s_i(t), a_i(t), s_j(t), a_j(t), S^{(N)}(t)) \\ &= g_i(s_i(t), a_i(t)) + \theta(t) [r_i p_i - (1 - r_i) q_i] \end{aligned} \tag{25}$$

4.4 Mean field game solution

Here, dynamic programming method is employed. It is also considered an optimization method in various fields in which complex problems are broken down into alike sub problems. In ideal case a memory-based data structure is used to avoid re-computing the solution of same problems. In this section, dynamic programming is used to find the attacking players optimum strategy Π_j . Applying the mean field approximation approach to overcome the complexity, the mean field equation system can be given as in [33].

$$v(s_j, \theta) = \min_{a_j \in A_j} \{c_j(s_j, a_j, \theta) + \Delta\} \tag{26}$$

where, $\Delta = \rho \sum_{k \in S_j} T_j(k|s_j, a_j) v(k, \Phi(s_j, \theta))$. The defending players optimum strategy Π_j can also be achieved by:

$$w(s_i, s_j, \theta) = \min_{a_i \in A_i} \{c(s_i, a_i, s_j, \theta) + \Omega\} \tag{27}$$

$\Omega = \rho \sum_{j \in S, k \in S_j} T(j|s_i, a_i) T_j(k|s_j, \Pi_j) w(j, k, \Phi(s_j, \theta))$. In the end the function is revised as (23). The (26) and (27) are dynamic programming equations for the attacker and defender, respectively. Simulating dynamic programming equations and respective cost functions the optimum strategies are determined.

$$\Pi_j = \{P_{j1} + P_{j2} + P_{j3} \dots \dots \dots P_{jL}\}$$

$$\Pi_i = \{P_{i1} + P_{i2} + P_{i3} \dots \dots \dots P_{iL}\}$$

The strategies are probabilities. Having a strategy Π for each step in a game represents a player adopting a particular action L with probability P_L . Considering the optimum strategies, the state transition law can be updated as:

$$T_j((y|s_j), \Pi_j) = \sum_{s_j \in S_j, a_j \in A_j} P_j(a_j|s_j) T_j((y|s_j), a_j)$$

$$T_i((y|s_i), \Pi_i) = \sum_{s_i \in S_i, a_i \in A_i} P_i(a_i|s_i) T_i((y|s_i), a_i)$$

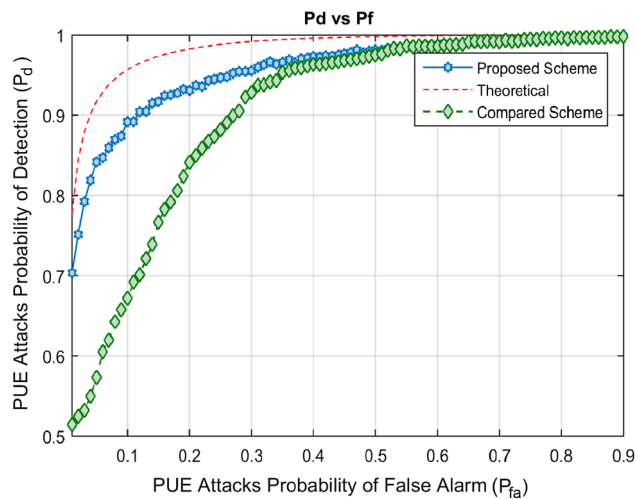


Fig. 6 Plot of probability of detection (P_d) versus probability of false alarm (P_{fa})

5 Simulation Results And Discussion

In this section, the simulation results of proposed scheme are presented. The proposed detection scheme is 1.32 times more accurate than Trong N. Les and Wen-Long Chins non-cooperative scheme. Next, an example is presented to demonstrate optimum attack and defence strategies by players in a CRN.

5.1 Simulation of attack detection

For simulation, consider a scenario in which there is a PUE attacker at location L. The SU are uniformly distributed in a region. PU is present in the network. Each SU can detect the PUE attacker on its own. Fig.6 demonstrates the working of the proposed detection system. The attack detection probability is presented in relation to the false alarm probability. In this, Monte Carlo method is applied. Monte Carlo method is used to solve problems having a probabilistic interpretation. The essential idea is using randomness to solve problems that might be deterministic in principle. We have employed this method in our simulation to get more realistic results. More samples lead to higher detection probability. The SNR is -5 dB. It can be observed that when probability of false alarms is 0.1, the PUE attack detection probability is 0.89. Comparing the results with Trong N. Le’s and Wen-Long Chin’s non-cooperative scheme [37], it can be observed that the proposed scheme is 1.32 times more accurate when $P_{fa} < 0.1$.

5.2 Attacking player’s strategies Π_j

To simplify the problem, consider that each PUE attacker has actions 0 and 1 representing Attack and Standby. The attacking player’s state transition matrices represent the probability

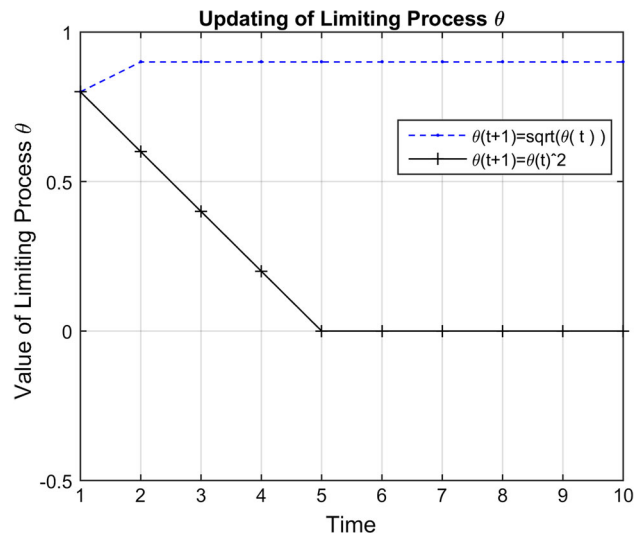


Fig. 7 Value of theta updating during the iteration. Its value close to 1 represents that most of the legit nodes of network are in defence state. When value is close to 0, it means most of the nodes are in negative defending states (i.e. most of them may be compromised). Their successful defending rate should be low and the attackers will get more rewards

of change of state from one to another. Consider the attacker has state 0, In the next step, it can retain the state and make an action 0 with the probability of 0.8, or change the state to 1 with probability 0.2.

The attacking players cost function is defined as $f_j(s_j, a_j) = (2 - s_j)(1 - a_j)$, $N = 20$, $r = 0.8$, and $q_i = 0.25$. In attacking players cost function, as θ reaches 1, it implies that majority of defending nodes are in defending state. If the attacker attacks while the defending nodes are in this state, then the rate of successful defence r would be greater and in turn the return $\sum_{i=1}^N (1 - r_i) q_i$ will be a lesser value. Hence, cost will be high. The value of θ in the iteration is shown in Fig. 7. In forming the initial values its assumed that most of the properties of nodes are made known. The supposition is principally realistic considering the network in focus. By known parameters or properties its meant that the initial states and related information are known. These parameters are used to initialize the cost and transition matrices. Here, its assumed that the state transition matrices of respective attacking player are:

$$T_j((y|x), a_j = 0) = \begin{bmatrix} 0.8 & 0.2 \\ 0.03 & 0.97 \end{bmatrix}$$

$$T_j((y|x), a_j = 1) = \begin{bmatrix} 0.9 & 0.1 \\ 0.02 & 0.98 \end{bmatrix}$$

The cost matrix for the attacking node is defined as:

$$C1 = \begin{bmatrix} c_j(0, 0, \theta) & c_j(0, 1, \theta) \\ c_j(1, 0, \theta) & c_j(1, 1, \theta) \end{bmatrix} = \begin{bmatrix} 2 - \theta & -\theta \\ 1 - \theta & 0 \end{bmatrix}$$

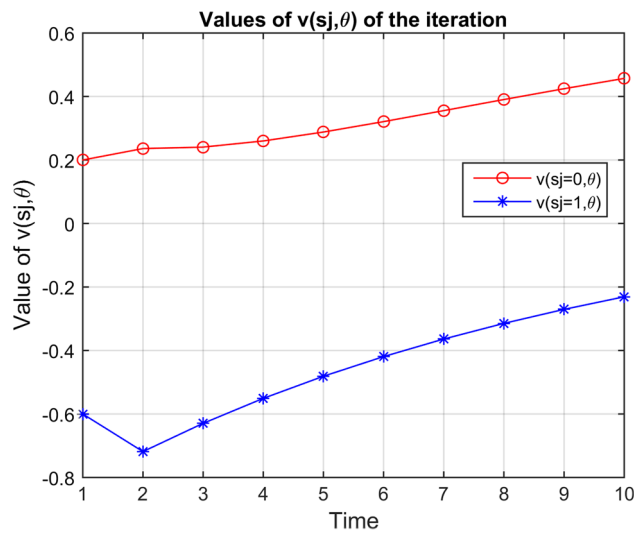


Fig. 8 Value of $v(s_j, \theta)$ from dynamic programming equation for attacking players (26)

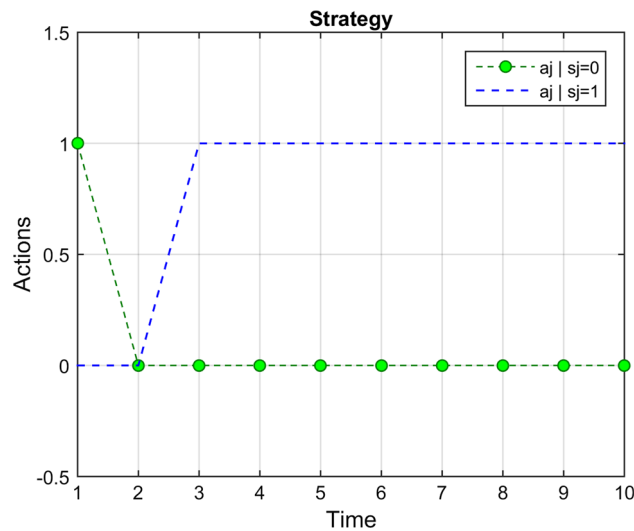


Fig. 9 Strategy of attacking players

It can be observed from the graphs that while the state of attacker is standby the values of v are very low (Figs. 8 and 9). The results also present that more strikes will not enhance the reward value provided the defending players successful detection. This is the point where the cost of attacking is more than the rewards. After the tenth step the simulation stops and the strategy is revealed.

When state $s_j = 0$:

$$\Pi_j^0 = [(a_j = 0 | s_j = 0) = 1, (a_j = 1 | s_j = 0) = 0]$$

When state $s_j = 1$:

$$\Pi_j^1 = [(a_j = 0 | s_j = 1) = 0, (a_j = 1 | s_j = 1) = 1]$$

Here, strategy $\Pi = 1$ means “no change”, and $\Pi = 0$ means “change”. After simulating the iteration, the state transition matrix will be updated as per equation above:

$$T_j = \begin{bmatrix} T_j(0|0), \Pi_j & T_j(1|0), \Pi_j \\ T_j(0|1), \Pi_j & T_j(1|1), \Pi_j \end{bmatrix} = \begin{bmatrix} 0.8 & 0.2 \\ 0.02 & 0.98 \end{bmatrix} \quad (28)$$

It can be concluded from this, that the optimum strategies of attacking players are the best actions compatible with their states.

5.3 Defending player’s strategies Π_j

As expressed earlier, the states of defending nodes are a combination of energy and security value. For simplicity, the state space is specified as $S_i = 0, 1$ and action space as $A_i = 0, 1$. Being in state $s_i = 0$ represents that the node has full energy and is considered secure. On the other hand, state $s_i = 1$ represents that the node is insecure. Likewise, action $a_i = 0$ means that the node is defending by applying defensive action against the emulating attacker, and $a_i = 1$ means node is doing nothing to defend. Considering the state transition matrices of defending player:

$$T = \begin{bmatrix} 0.7 & 0.3 \\ 0.03 & 0.97 \end{bmatrix}$$

$$T = \begin{bmatrix} 0.9 & 0.1 \\ 0.02 & 0.98 \end{bmatrix}$$

Considering $g_i(s_i, a_i) = (1.8 - s_i)(1 - a_i)$, $N = 20$, $r_i = 0.8$, $p_i = 1$, and $q_i = 1.5$ in (27) and forming the utility matrix in tactical form for defending nodes in a CRN.

States	Defence	No Defence
Attack	$g_i(s_i, 0) + \theta(t)[r_i p_i - (1 - r_i)q_i]$	$g_i(s_i(t), 1) + \theta(t)q_i$
Standby	$g_i(s_i, 0)$	0

The cost matrices for the defending nodes are:

$$C1 = \begin{bmatrix} c_i(0, 0, 0, \theta) & c_i(0, 1, 0, \theta) \\ c_i(1, 0, 0, \theta) & c_i(1, 1, 0, \theta) \end{bmatrix},$$

$$C2 = \begin{bmatrix} c_i(0, 0, 1, \theta) & c_i(0, 1, 1, \theta) \\ c_i(1, 0, 1, \theta) & c_i(1, 1, 1, \theta) \end{bmatrix}$$

Using the results of the tactical form of utility matrix the cost matrices are updated as:

$$C1 = \begin{bmatrix} 1.8 - 0.3\theta & 2.5\theta \\ 0.8 - 0.3\theta & 2.5\theta \end{bmatrix}$$

and,

$$C2 = \begin{bmatrix} 1.8 & 0 \\ 0.8 & 0 \end{bmatrix}$$

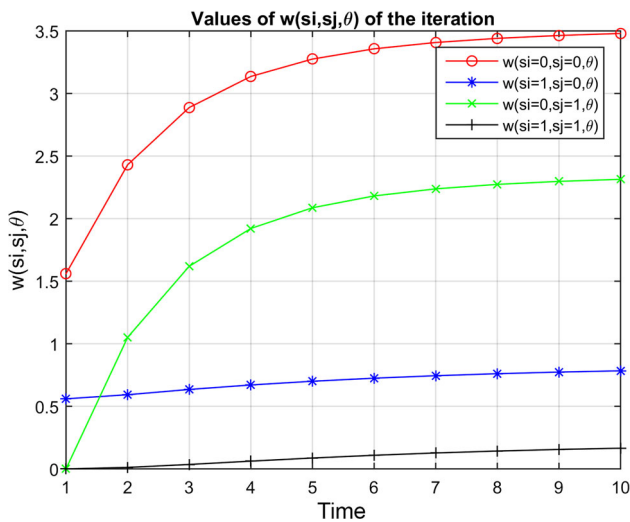


Fig. 10 Value of $w(s_i, s_j, \theta)$ from dynamic programming equation for defending players (27)

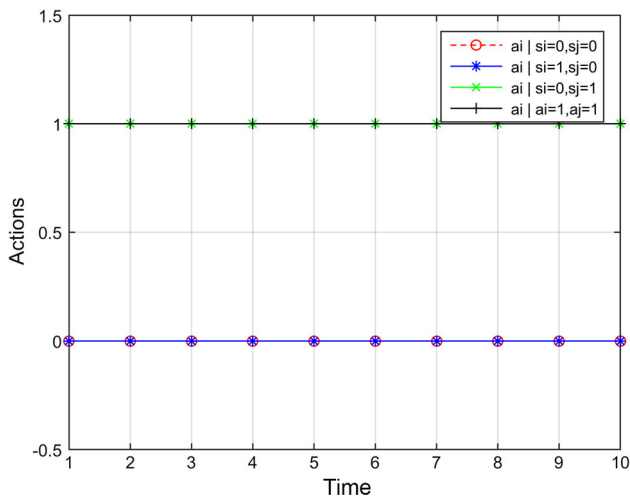


Fig. 11 Strategy of defending players. The defending players defend when the state of attacker is attacking (i.e. $s_j = 0$) and are on standby when attacker is not attacking (i.e. $s_j = 1$)

To form the optimum strategies of the legitimate secondary nodes of the cognitive radio network the $\theta = 0.8$ to start the iteration. It is updated like before. In the end of the iteration, the optimum strategy for respective defending player Π_i (Figs. 10 and 11):

$$\begin{aligned} \Pi_i^0 &= \begin{bmatrix} (a_i = 0 | s_i = 0, s_j = 0) = 0 \\ (a_i = 1 | s_i = 0, s_j = 0) = 1 \end{bmatrix}, \\ \Pi_i^1 &= \begin{bmatrix} (a_i = 0 | s_i = 1, s_j = 0) = 1 \\ (a_i = 1 | s_i = 1, s_j = 0) = 0 \end{bmatrix} \\ \Pi_i^2 &= \begin{bmatrix} (a_i = 0 | s_i = 0, s_j = 1) = 0 \\ (a_i = 1 | s_i = 0, s_j = 1) = 1 \end{bmatrix}, \\ \Pi_i^3 &= \begin{bmatrix} (a_i = 0 | s_i = 1, s_j = 1) = 0 \\ (a_i = 1 | s_i = 1, s_j = 1) = 1 \end{bmatrix} \end{aligned}$$

The state transition law considering the strategy of the respective defending players can be written as:

When state of attacker s_j is 0:

$$T = \begin{bmatrix} 0.9 & 0.1 \\ 0.03 & 0.97 \end{bmatrix}$$

When it is 1:

$$T = \begin{bmatrix} 0.9 & 0.1 \\ 0.02 & 0.98 \end{bmatrix}$$

The output shows that the optimum strategy matrices of the defending players are different for different states of attacking players. Applying the method in [31] and [32], the function Φ can be expressed as (23).

The matrix (21) in the current scenario can be written as:

$$\begin{aligned} Transition(s_j, \theta) &= \begin{bmatrix} T(0|0), \Pi(1, s_j, \theta) & T(1|0), \Pi(1, s_j, \theta) \\ T(0|1), \Pi(1, s_j, \theta) & T(1|1), \Pi(1, s_j, \theta) \end{bmatrix} \\ T_{rev}(s_j = 0, \theta) &= \begin{bmatrix} 0.9 & 0.1 \\ 0.03 & 0.97 \end{bmatrix} \\ T_{rev}(s_j = 1, \theta) &= \begin{bmatrix} 0.9 & 0.1 \\ 0.02 & 0.98 \end{bmatrix} \end{aligned}$$

For complete simulation of the scheme consider an ad-hoc CR network of N nodes. Each node in the network uses proposed approach for PUE attack detection. The number of nodes in the network can be changed. There are attacking nodes which want to attack the network. The attackers are intelligent and do the PUE attack when the legitimate PUs are not present. The SUs can detect the attackers actions. For demonstration in Fig. 12, the number of legit nodes in the simulation is 20. Each node in the system employs defence strategy when attacked. The defenders in this simulation do not apply proposed optimum strategy.

In Figs. 13 and 14, the number of legitimate nodes is increased to 40 and 100 respectively. The attackers launch PUE attacks optimally on randomly chosen nodes. Observing the 100–1000 steps of the simulation shows that the nodes do not always choose the defending action optimally. This can be explained as the decision-making process is dependent on the existing state of the defending nodes therefore, defending action is not the most feasible action all the time. It also represents that each node recognises its state (i.e. energy consumption and security) and considers it while making a decision to conserve network resources.

Now, to simulate network lifetime, some rules on parameters are placed. There is a network of 100 CR nodes. Its assumed that, each node has some energy value. When energy of CR node is less than 10%, its considered dead. If 75% of the nodes in the CRN are dead, the network is considered dead. The plot in Fig. 15 shows the lifetime comparison of

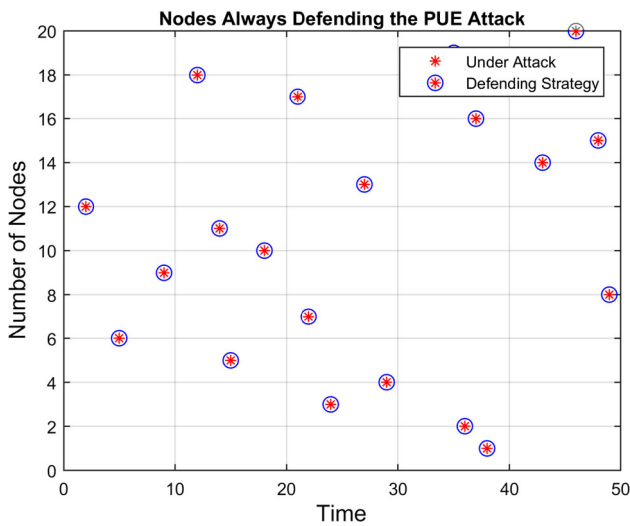


Fig. 12 All nodes defending the PUE Attack (standard defence scheme)

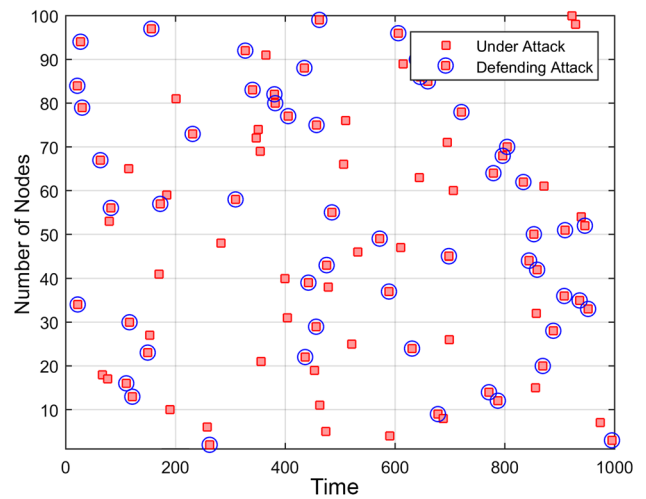


Fig. 14 CRN of 100 Nodes defending PUE attacks keeping their, and attackers states under consideration

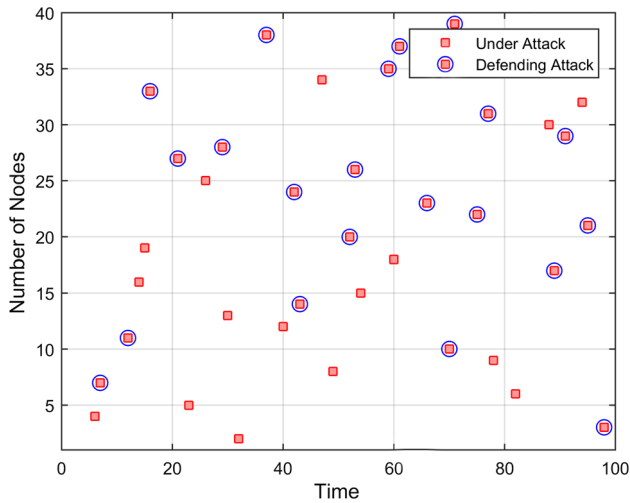


Fig. 13 CRN of 40 Nodes defending PUE attacks keeping their, and attackers states under consideration

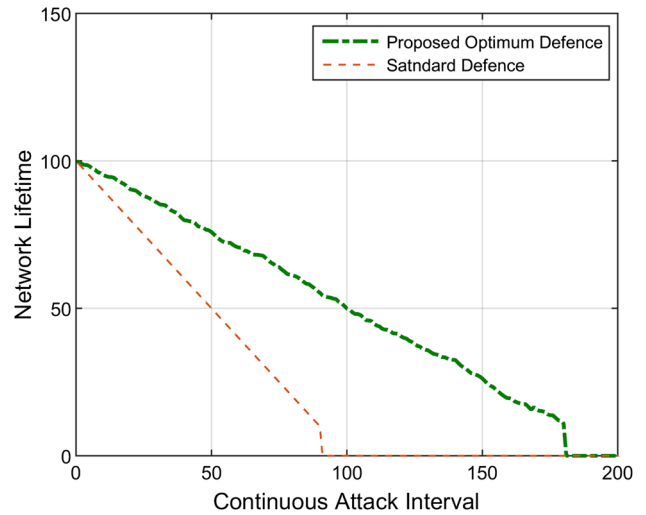


Fig. 15 Lifetime comparison of the proposed defence scheme with standard scheme

network under continuous PUE attack. It can be observed that lifetime of network employing proposed defence scheme is higher than standard defence scheme, in which nodes make state oblivious decisions.

Next, the cost of a respective defending player is compared adopting the two strategies against PUE attacks. In Fig. 16, the bar graph of defending costs applying smart defence and continuous defence strategy are shown in 50 steps. The later strategy is effective in the scenarios where security is utmost priority. It can be observed that the cost is lower when the player does state aware defence decision against attacks. In a nutshell, the results show that proposed defence scheme is 0.846 times more cost effective.

5.4 Simple statistical analysis

The proposed detection scheme’s simulation results show a detection accuracy of 89% when the probability of false alarms is 0.09. This makes it 1.32 times more accurate than compared work. The simulation results of the proposed defence scheme show the life time of the network is 91%, making it 1.16 times higher than standard defence. The costs comparison show that proposed defence scheme has cost of 43.7%, making it 0.846 times more cost effective than standard defence.

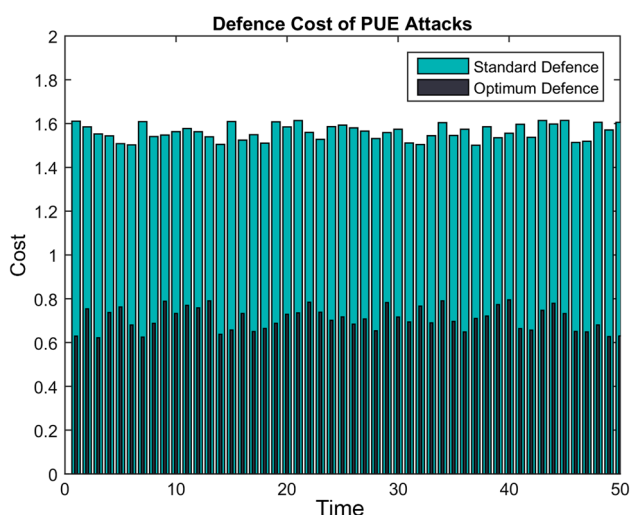


Fig. 16 Cost comparison between standard and optimum defence actions under PUE attacks

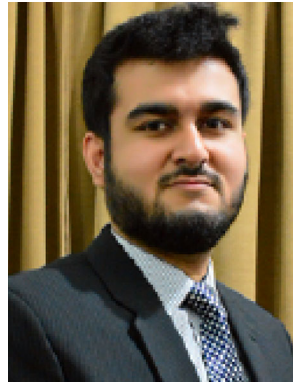
6 Conclusion and future work

This paper presents a complete security system to detect and smartly defend a CRN against PUE attacks. In the commencement of the paper a PUE detection approach was presented to spot attacking nodes. The approach reduces network overheads produced by data signing and other cryptographic techniques. The simulation results show that it is 1.32 times more accurate than compared work. The mechanism for energy detection and location verification is also presented in the paper. After spotting the attacker nodes, mean field game approach is used to enable each node to make defence decisions depending upon their states. The scenario of multiple attackers is also considered. As challenges in ad hoc CRN environment are mobility, lack of infrastructure and central administration. In the future work, we will implement this system on vehicular CR ad hoc networks and design test for mobility. Moreover, we will also try-out other game theoretic approaches in our scenario.

References

1. Federal Communications Commission (FCC), *FCC online table of frequency allocations*, August 31, (2016) [Online] <https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf>.
2. Zhao, Q., & Sadler, B. M. (2007). A survey of dynamic spectrum access. *IEEE Signal Processing Magazine*, 24(3), 7989.
3. Lien, S.-Y., Chen, K.-C., & Liang, Y.-C. (2014). Lin Y Cognitive radio resource management for future cellular networks. *IEEE Wireless Communication*, 21(1), 7079.
4. Marinho, J., Granjal, J., & Monteiro, E. (2015). A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP Journal on Information Security*, 114.
5. Spectrum Bridge. *White space overview*. [Online]: <http://spectrumbridge.com/tv-white-space/>.
6. WRAN WG on Broadband Wireless Access Standards, *IEEE 802.22* [Online]. www.ieee802.org/22.
7. Jana, S., Zeng, K., & Cheng, W. (2013). Trusted collaborative spectrum sensing for mobile cognitive radio networks. *IEEE Transactions on Information Forensics and Security*, 8(9), 1497–1507.
8. Wengui, S., & Yang, L. (2015). A jury-based trust management mechanism in distributed cognitive radio networks. *China Communications IEEE*, 12(7), 119–126.
9. Pu, D. (2012). Detecting primary user emulation attack in cognitive radio networks. In *Proc. IEEE global telecommunications conf*, Dec.
10. Jin, Z., Anand, S., & Subbalakshmi, K. P. (2009). Detecting primary user emulation attacks in dynamic spectrum access networks. In *Proc. IEEE Intl Conf. Commun. (ICC)*.
11. Akhunzada, A., Ahmed, E., Gani, A., Khan, M. K., Imran, M., & Guizani, S. (2015). Securing software defined networks: Taxonomy, requirements, and open issues. *IEEE Communications Magazine*, 53(4), 3644.
12. Kumari, S., Khan, M. K., & Atiquzzaman, M. (2015). User authentication schemes for wireless sensor networks: A review. *Ad Hoc Networks*, 27, 159–194.
13. Tai, W.-L., Chang, Y.-F., & Chen, Y.-C. (2016). A fast-handover-supported authentication protocol for vehicular ad hoc networks. *Journal of Information Hiding and Multimedia Signal Processing*, 7(5), 960–969.
14. Ngo, N. M., Unoki, M., Miyauchi, R., & Suzuki, Y. (2014). Data hiding scheme for amplitude modulation radio broadcasting systems. *Journal of Information Hiding and Multimedia Signal Processing*, 5(3), 324–341.
15. Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection and prevention approaches for network layer attacks. *IEEE Communications Surveys and Tutorials*, 15, 2027–2045.
16. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. *IEEE Transactions on Wireless Communications*, 11, 3847.
17. Albers, P., Camp, O., Percher, J. M., Jougla, B., Me, L., & Puttini, R. Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches. In *Proceedings of the 1st international workshop on wireless information systems*.
18. Snort Team. (2014). *SNORT User Manual*, 2.9.7 ed, Available online at: <https://www.snort.org/documents>.
19. Bro Team. *Bro documentation and manual*. Available online at: <https://www.bro.org/documentation>.
20. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2010). Mitigating routing misbehaviour in mobile ad hoc networks. In *Proceedings of the 6th international conference on mobile computing and networking*, Boston, MA, pp. 255–265.
21. Zhang, Y., & Lee, W. (2013). Intrusion detection in wireless ad hoc networks. In *ACM MOBICOM*, pp. 275–283.
22. Albers, P., Camp, O., Percher, J. M., Jougla, B., Me, L., & Puttini, R. (2012). Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches. In *Proceedings of the 1st international workshop on wireless information systems (WIS-2002)* (pp. 1–12).
23. Ferraz, L., et al. (2014). An accurate and precise malicious node exclusion mechanism for ad hoc networks. *Ad Hoc Networks*, Elsevier, pp. 1–14.
24. Chen, R., & Park, J.-M. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. In *First IEEE workshop on networking technologies for software defined radio networks (SDR)* (pp. 110–119). VA, September: Reston.
25. 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.

26. Huang, L., Xie, L., Yu, H., Wang, W., & Yao, Y. (2010). Anti-PUE attack based on joint position verification in cognitive radio networks. In *International conference on communications and mobile computing (CMC)*, Vol. 2, Shenzhen, China, pp. 169–173.
27. Zhao, C., Wang, W., Huang, L., & Yao, Y. (2009). Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio. In *5th International conference on wireless communications, networking and mobile computing (WiCom 09)*, Beijing, China, pp. 1–5.
28. Afolabi, O. R., Kim, K., & Ahmad, A. (2009). Secure spectrum sensing in cognitive radio networks using emitters electromagnetic signature. In *Proceedings of 18th international conference on computer communications and networks (ICCCN 2009)*, San Francisco, CA, pp. 1–5.
29. Otrók, H., et al. (2008). A game-theoretic intrusion detection model for mobile ad hoc networks. *Elsevier Computer Communications*, 31, 708–721.
30. Liang, X., & Xiao, Y. (2013). Game theory for network security. *IEEE Communication. Surveys Tutorials*, 15(1), 472486.
31. Meriaux, F., Varma, V., & Lasaulce, S. Mean field energy games in wireless networks. In *Proc. 2012 Asilomar conf. signals, systems, computers*.
32. Tembine, H., Vilanova, P., Assaad, M., & Debbah, M. Mean field stochastic games for SINR-based medium access control. In *Proc. 2011 intl ICST conf. performance evaluation methodologies tools*.
33. Huang, M. Y. Mean field stochastic games with discrete states and mixed players. In *Proc. 2012 GameNets*.
34. Wang, Y., Yu, F., Tang, H., & Huang, M. (2014). A mean field game theoretic approach for security enhancements in mobile ad hoc networks. *IEEE Transactions on Wireless Communications*, 13(3), 16161627.
35. Trees, H. L. V. (2001). *Detection, estimation, and modulation theory: Part I*. New Jersey, USA: Wiley-Inter science.
36. Tandra, R., & Sahai, A. (2008). SNR walls for signal detection. *IEEE Journal of Selected Topics in Signal Processing*, 2(1), 417.
37. Le, T. N., Chin, W.-L., & Lin, Y.-H. Non-cooperative and cooperative PUEA detection using physical layer in mobile OFDM-based cognitive radio networks. In *International conference on computing, networking and communications*, 24 March 2016.
38. Urkowitz, H. (1967). Energy detection of unknown deterministic signals. *Proceedings of the IEEE*, 55(4), 523–531.
39. Ayyasamy, A., & Venkatachalapathy, K. (2015). Context aware adaptive fuzzy based QoS routing scheme for streaming services over MANETs. *Wireless Networks*, 21(2), 421–30.
40. Ahmadi, M., Shojafar, M., Khademzadeh, A., Badie, K., & Tavoli, R. (2015). A hybrid algorithm for preserving energy and delay routing in mobile ad-hoc networks. *Wireless Personal Communications*, 85(4), 2485–505.
41. Cordeschi, N., Amendola, D., & Baccarelli, E. (2015). Distributed and adaptive resource management in cloud-assisted cognitive radio vehicular networks with hard reliability guarantees. *Vehicular Communications*, 2(1), 1–12.
42. Zhu, J., Song, Y., Jiang, D., & Song, H. (2016). Multi-armed bandit channel access scheme with cognitive radio technology in wireless sensor networks for the internet of things. *IEEE Access*, 4, 4609–4617.
43. Pei, Y., Liang, Y.-C., Zhang, L., The, K. C., & Li, K. H. (2010). Secure communication over MISO cognitive radio channels. *IEEE Transactions on Wireless Communications*, 9, 1494502.
44. Amjad, M. F., Aslam, B. & Zou, C. C. (2013). Reputation aware collaborative spectrum sensing for mobile cognitive radio networks. In *MILCOM 2013* (pp. 951–956). San Diego, CA, 18–20.
45. Mneimneh, S., & Bhunia, S. (2017). A game-theoretic and stochastic survivability mechanism against induced attacks in Cognitive Radio Networks. *Pervasive and Mobile Computing Archive*, 40(C), 577–592.
46. Hosseini, A., Abolhassani, B., & Hosseini, A. (2017). Secure cognitive radio communication for internet-of-things: Anti-PUE attack based on graph theory. *Journal of Computer and Communications*, 5, 27–39.



Saim Bin Abdul Khaliq is a graduate student in the Department of Information Security, National University of Sciences and Technology Pakistan. He received Engineering degree in Computer Engineering from National University of Sciences and Technology Pakistan in 2012. His research interests mainly focus on security in networks including cognitive radio and wireless sensor networks, game theory, malware dissection, and system's vulnerability exploitation.

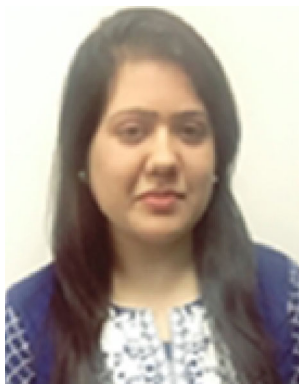


Muhammad Faisal Amjad is a senior member of the IEEE and an Assistant Professor in the Department of Information Security, National University of Sciences and Technology (NUST), Pakistan. He received his PhD degree in Computer Science from University of Central Florida USA in 2015. He is also associated with "Center of Data and Text Engineering and Mining (CoDTeEM)" at NUST. His current research focusses on the application of machine learning and game theoretic techniques in the domains of IoT and network security, digital forensics and malware analysis. He specializes in dynamic spectrum access and defense against security vulnerabilities in Cognitive Radio Networks as well as wireless sensor and ad hoc networks.



Haider Abbas received the M.S. degree in Engineering and Management of Information Systems and the Ph.D. degree in Information Security from the KTH Royal Institute of Technology, Stockholm, Sweden, in 2006 and 2010, respectively. His professional career consists of activities ranging from research and development and industry consultations (government and private), through multi-national research projects, research fellowships, doctoral studies advisory services, international journal editorships, conferences/workshops chair, invited/keynote speaker, technical program committee member, and reviewer for several international journals and conferences. He is currently a Cyber Security Professional, an Academician, a Researcher, and an

Industry Consultant who took professional trainings and certifications from the Massachusetts Institute of Technology, USA; Stockholm University, Sweden; the Stockholm School of Entrepreneurship, Sweden; IBM, USA; and the EC Council. He is also an Adjunct Faculty and Doctoral Studies Advisor at the Florida Institute of Technology, USA. In recognition of his services to the international research community and excellence in professional standing, he has been awarded one of the youngest Fellows of the Institution of Engineering and Technology, U.K.; a fellow of the British Computer Society, U.K.; and a fellow of the Institute of Science and Technology, U.K.



Narmeen Shafqat is a lecturer in the Department of Information Security, National University of Sciences and Technology (NUST), Pakistan. She received her MS degree in Information Security and BE degree in Electrical Telecommunication from NUST. She has acquired Cyber Executive Training from Sandia National Laboratories, USA. Her areas of research are Network Security, Cyber laws, and Cyber Risk/Vulnerability Assessment.



Hammad Afzal is currently heading “The Center of Data and Text Engineering and Mining” (CoD-TeEM) group at NUST. His primary interests are machine learning, text and data mining systems. He completed PhD from School of Computer Science, University of Manchester, UK in Dec, 2009 under supervision of Dr. Goran Nenadic in Text Mining Group. Before PhD, he completed MSc in Advanced Computing Sciences from University of Manchester, UK where he was awarded Pro-

gram Prize of the year from Department of Computation for acquiring highest grades in MSc courses. He has also been affiliated with Digital Enterprise Research Institute (DERI), National University of Ireland, Galway as a Research Assistant from July, 2009 to Dec, 2009.