Defence Against PUE Attack in CRN: A Game Theoretic Approach

by

NS Saim Bin Abdul Khaliq

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfilment of the requirements for the degree of MS in Information Security

June 2017

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-constrains 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. This thesis 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.

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Dedication

“In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my mother, sister, and teachers who supported me each step of the way.

Acknowledgments

All praises to Allah for the strengths and His blessing in completing this thesis.

I would like to convey my gratitude to my supervisor, Major. Muhammad Faisal Amjad, PhD, for his supervision and constant support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis works are major contributions to the success of this research. Also, I would thank my committee members; Lecturer Narmeen Shafqat, and Lecturer Waleed Bin Shahid for their support and knowledge regarding this topic.

Last, but not the least, I am highly thankful to my mother (Mrs. Nabila Abdul Khaliq), and sister (Aisha Abdul Khaliq). They have always stood by my dreams and aspirations and have been a great source of inspiration for me. I would like to thank them for all their care, love and support through my times of stress and excitement.

Table of Contents

Page

Chapter

List of Figures

Chapter 1

Introduction

1.1 Overview

Wireless spectrum is the equitable demand of our contemporary society. Whether it is national defence, surveillance, health care services, monetary transactions, or entertainment industry they all require consistent access to wireless spectrum. 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 inoccupancy 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]. Cognitive Radio (CR) nodes have the 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.

The core problem behind spectrum sensing is precisely distinguishing Primary User (PU) signal from Secondary Users (SU) signals. In a CRN, PU has priority over all SUs in accessing the channel. The Network permits secondary user to use a specific band till the time primary user PU is not using it. Still, if the SU senses the presence of a PU, it shifts instantly to another band to avoid interference to the PU. Moreover, when a SU senses another SU on a common band, it employs specific techniques for spectrum sharing. Based on the described scenario there lies a possibility 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 (PUEA) [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 as malicious and selfish.

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.

1.2 Motivation and Problem Statement

The unique characteristics of CR networks which enhance their popularity in industry also make them vulnerable to a new breed of attacks which open new research areas for researchers. The fundamental issue in spectrum sensing is to precisely differentiate between a primary user and secondary user. There is a possibility for malice SU to mimic the signature of PU and dodge the system into believing that it’s a licensed primary user.

Hence, there is a need for an effective detection scheme. After detection of attacker, the utmost requirement is of a mechanism which enables a node to do its effective defence.

Game theory can provide a better mathematical framework for analysing theses security issues in the network.

1.3 Objectives

The main objectives of thesis are: -

- To propose a PUE detection mechanism to enable each node to detect the attacks.
- To present a game model showing attacking and defending players.
- Apply a dynamic mean field game theoretical approach to enable each node to make defence decisions against attacks.

1.4 Thesis 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.

The main contributions of this work are as follows.

- We propose a PUE detection mechanism to enable each node to detect the attacks without incurring additional overheads.
- Next, we have 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, we have considered multiple PUE attackers in the network and our proposed techniques can be implemented in a distributed manner.

1.5 Thesis Organization

The thesis is structured as follows:

- Chapter 2 contains the literature reviewed in the thesis. The general working of CR networks, security issues in the networks, the attacks susceptible to such networks, primary user emulation attack, PUE detection techniques and existing game theoretical approaches applied on the network are covered in the chapter.

- Chapter 3 contains the proposed scheme for PUEA detection, details of CR Network under consideration, system model for detection system, energy detection and location verification mechanisms. The simulation results representing the working of the scheme are covered in chapter 5.

- Chapter 4 covers the anticipated scheme for defence, system description, mean field game model, transition laws, states, attacking and defending players cost functions, and mean field game equation system.

- Chapter 5 contains an example representing the working of the theoretical system, players adopting the best strategies. The optimum tactic parameters are also discussed here. The simulation results involving defence actions, life time of network, and defence costs are discussed in detail.

- Chapter 6 marks the end of the document. The conclusion and future work areas are revealed in this chapter.

Chapter 2

Attacks on Cognitive Radio Networks

2.1 Introduction

This chapter contains the literature reviewed in the thesis. The general working of CR networks is discussed in the beginning. Next, security issues in the networks and the attacks susceptible to such networks are presented. The primary user emulation attacks and PUE detection techniques are also discussed. Existing game theoretical approaches applied on similar networks are also covered here. Furthermore, a brief introduction to mean field game theory is give in the end of this chapter.

2.2 Cognitive Radio Networks

Joseph Mitola and Gerald Maguire presented cognitive radios to the world in 1999 [1]. It was introduced as an extension of Software Defined Radios (SDR) geared to improve the performance by using cognition cycle Figure 2.1. Joseph Mitola, in [2] declared that CR is a focused and goal oriented system. The radios are autonomously aware of the surrounding environment, can oversee multiple services, gather data, deduce results, make plans, and best of all learn from past mistakes.

In a nutshell, a cognitive radio is a redefined SDR with additional sensors. The fundamental features that set it apart from others are radio environment awareness and learning capability to optimise performance [3].

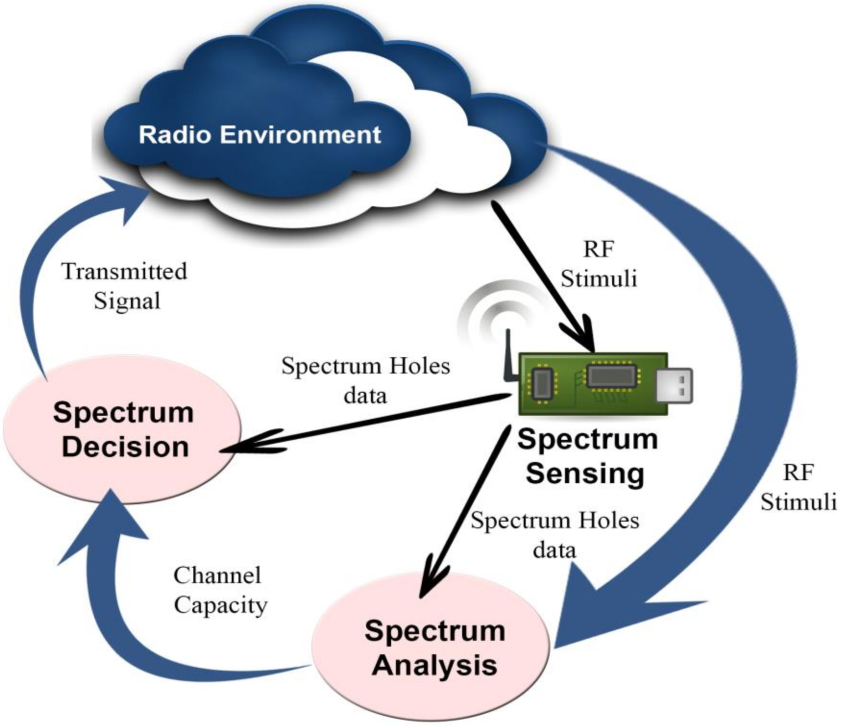

Figure 2.1: Cognitive cycle

2.3 Security of Cognitive Radio Ad-hoc Networks

Cognitive Radio is a smart technology which is developed to optimise the consumption of the licenced band by giving chance to unlicensed users. In a distributed cognitive radio ad hoc network each node can act as an autonomous unit. They can self-organize and establish a communication link in a resource constrained environment. Additionally, the nodes can also do spectrum sensing and select the right channel for communication. Due to shared wireless spectrum and lack of centralized management, this type of network is susceptible not only to characteristics based security channels like, black hole, denial of service, resource exhausting, confidentiality breach and interference etc. It is also vulnerable to a new breed of attack threats. Unlike most of the research work, here the attacks are categorized based on the layer they target.

2.3.1 Physical Layer Threats, Countermeasures and Verdict

2.3.1.1 Primary User Emulation Attack

The main tricky thing behind spectrum sensing is precisely distinguishing PU's signal from SUs signals. In a CRN, PU has priority over all SUs in accessing the channel. The Network permits secondary user to use a specific band till the time primary user PU is not using it. Still, if the SU senses the presence of a PU, it shifts instantly to another band to avoid interference to the PU. Moreover, when a SU senses another SU on a common band, it employs specific techniques for spectrum sharing. Based on the described scenario there lies a possibility 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 (PUEA) [4]. The later section will cover more detail about the attack.

2.3.1.2 Objective Function Attack

Few vital features of the CRN include its ability to stay aware of its environment, learning from past mistakes and make smart decisions in choosing the right transmission perimeters. The cognitive engine is the heart of the cognitive radio in control of selecting radio parameters as per the external environment. Maintaining energy consumption, data rate and security levels are the requirements which are responsible for need of adjustments in transmission of radio parameters. Bandwidth, working frequency, modulation scheme, channel protocol, coding rate, frame size and encryption algorithm used are all included in radio parameters. The attacker can affect the working of the cognitive engine by creating a false external environment for the radio by altering the perimeters it can control. A point worth noting here is that this type of attack is only susceptible to online learning radios.

T. Charles Clancy and Nathan Goergen in [5] presented an attack in which a cognitive engine has an objective function: $\mathit{function} = \mathrm{w}_1 R + \mathrm{w}_2 S$ where, w_1 and w_2 are the weights of rate of transmission (R) and security (S). Every time when the cognitive engine uses a high security level setting, the attacker launches a jamming attack and reduces transmission rate. As a result of this, the objective function reduces. To avoid this situation, the cognitive engine is restricted from enhancing the security level. In this way, the attacker is successful in controlling the cognitive engine into using the lower security setting.

In [6], a defence against Objective function attacks is presented in which all updatable parameters are assigned a fixed threshold value. The decision for establishing a communication link is done in comparison with threshold values. Getting help from some suitable IDS is also suggested in this work.

To improve the working of this concept using adaptive threshold values will be better instead of standard fixed ones. Getting support from an IDS is a very generic defence measure making it suitable for a very specific kind of attacks.

2.3.1.3 Jamming

Consider a malicious node transmitting on a channel. A legitimate node wants to use the same channel but is forced to stop. Due to this, the device will be under denial of service due to jamming. This attack can be targeted at physical or mac layer level. To avoid this attack at physical layer, the devices should be capable of differentiating between standard levels and non-standard levels of noise. Frequency hopping is considered a decent solution to jamming attack.

2.3.2 Link Layer Threats, Countermeasures and Verdict

2.3.2.1 Byzantine attack

Byzantine or Spectrum Sensing Data Falsification attack is an attack in which a malicious node does false reporting to its neighbours. The aim of attacker is to affect the spectrum sensing decisions by sending altered locally generated spectrum sensing reports [7]. The attack is effective on both distributed as well as centralized CRNs. The attack is more damaging for the distributed network because the false reports can be spread more swiftly, and there are no means of centralized control or fusion centre. In a centralized environment, the effect of attack can be reduced by adopting smart procedures like analysing and comparing locational data.

Ruiliang Chen and Jung-Min Park in [8], presented a data fusion method named Weighted Sequential Ratio Test. Research work consists of two steps. The foremost is reputation maintenance and the subsequent is actual hypothesis test. In the first, each node holds a reputation value equal to zero. The value is incremented with every true local report. The second step is a modified Sequential Probability Ratio Test (SPRT). This technique works like standard trust-based data fusion techniques in wireless sensor networks and shows decent performance.

2.3.2.2 Control Channel Overload (DoS Attack)

In Control Channel Overload DoS Attack, the malicious node creates forged control frames on link layer. The aim of the attacker is to overload the control channel as the channel can hold only a specific amount of parallel communications. This results in collision and destroys the network performance. As in a centralized CRN all the control channel packets are validated at the fusion centre therefore, this attack is only a threat for a distributed CRN. It limits the throughput close to zero.

Defence against Control Channel Overload attack can be done by employing a trust based approach in which a mistrustful device is monitored and authenticated by neighbouring devices. The neighbours analyse opinions and make a final decision on the behaviour of the node.

2.3.3 Network Layer Threats, Countermeasures and Verdict

2.3.3.1 Sinkhole Attacks

In this attack, the malicious CR node claims that its path is the best path to a particular destination. This attracts the neighbouring nodes into using the path for packet forwarding. In this position, a malicious node can also launch a selective forwarding attack in which it can breach integrity or drop packets.

Detection of a sinkhole attack is tough as it targets the design flaws of routing protocol and topology of CR network. CRNs with geographic routing protocols are considered immune to these types of attacks. Geographic routing protocols work by employing communications at local level to develop an on-demand network architecture. Hence, this avoids a sinkhole by linking paths with the actual physical locations.

2.3.3.2 HELLO Flood Attacks

An attack in which a broadcast message is sent by malicious device to every device in the network with a significant high-power level is called HELLO flood attack. The idea is to transmit with a convincing power level, luring the legitimate nodes into thinking that the transmitter is a neighbour. This will reassure even the most distant nodes into considering that the advertised path is the best. As a result of this all packet sent to this path will be lost. Moreover, any node discovering the true intensions of the attacker will be left alone without neighbours.

The routing attacks such as this can be dealt with in general by applying a safe protocol for routing, like Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [9]. It provides solid protection against DoS attacks by using a one-way hash function. It avoids the malicious use of network resources. SEAD is inspired by Destination-Sequences Distance-Vector protocol (DSDV) and delivers decent protection.

Cross layered solutions are also presented and are effective to provide protection against network layer attacks. In these channel scheduling choices are made by taking input from spectrum management and routing algorithm.

2.3.4 Transport Layer Threats, Countermeasures and Verdict

The transport layer is also under threat of attacks in CRN. Ad-hoc networks are the prime targets. Lion Attack is a well-known attack on CRNs which targets the transport layer.

2.3.4.1 Lion Attacks

The lion attack is initiated via a primary user emulation attack and its targeted at transport layers TCP connection. That is why it is also termed in literature as a cross layer attack. The attack starts by emulating a licenced user and deteriorating TCP performance by enforces the SUs into making frequency handoffs. As the protocol is not aware of the handoffs it will keep sending packets without acknowledgements. The segments will timeout and TCP will retransmit with bigger timeout. This results in delay and loss of packets. If in any case the attacker has access to messages it can guess the attacked frequency band and use it as licenced user and cause network starvation.

To tackle this attack Juan Hernandez Serrano, Olga León in [10] proposed a cross-layer data sharing approach. This approach makes the TCP more aware about the physical layer’s link with transport layer. This enables the devices in the network to freeze TCP controls during handoffs.

2.4 Primary User Emulation Attack (PUEA)

The attack is defined in the section above. The advantage of PUE attack is that the attacker does not have to share resources with other secondary users and get access to full spectrum.

The attack motives are classified as malicious and selfish. 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.

To counter PUE attack the cryptographic verification of licenced user seems a good idea. But, this cannot be executed because in order to implement this some changes had to be made to the primary user node. This is a violation of FFC’s policies.

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 [11]. 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 FFC are followed and final channel selection decisions are made. A centralized collaborative spectrum sensing approach is also employed in IEEE 802.22 standard [12] 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.

A lot of researchers are working 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 [13][14]. 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 effect final decisions.

2.4.1 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.

2.4.1.1 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.

2.4.1.2 Localization-Based Detection

This is the approach in which signal characteristics and known location of transmitter are used to differentiate the PU from attacker. Ruiliang Chen and Jung-Min Park in [15], 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 [16] 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 [17] [18] a location based approach is presented which employ TDOA and FDOA. It’s 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.

2.4.1.3 Feature Detection

In [19] 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. This gives better results but increases signal processing and sensing time. It also increases storage needs.

2.4.1.4 RSS-based Detection

In [20] 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 by applying Fenton's approximation and Wald's probability ratio test for CRN where PU emulating attackers are arbitrarily distributed.

2.4.2 PUE Attack Effects on CRN

Attackers denying others nodes access to spectrum can affect the whole idea of implementing a CRN. A successful attack can result in wastage of bandwidth, degrade quality of service. Furthermore, it can also cause interference to the PU network, originate connection issues, and enforce denial of service.

2.4.3 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 practices 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.

2.5 Intrusion Detection in Similar Networks

There are several studies covering varies 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. Hence, there is an effective need of developing intrusion detection system (IDS) along with an effective defence mechanism for tackling active and passive attacks [21]. There are two research approaches geared towards securing networks: prevention approach and detection approach [22], [23].

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 [24] [25] 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 system’s 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 [26].

In [27], Zhang and Lee presented the requirements needed for IDS to work in 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 [28], a distributed design for detection system facilitated by mobile agents is presented. In this scheme, each node has local based 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.

L Ferraz et al, in [29] presented a Trust-based Exclusion Access-control Mechanism (TEAM). It provides full-bodied, distributed access control mechanism built on trust models to provide security and collaboration 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.

2.6 Game Theory for Security in Networks

The preliminary concept of game theory was presented in 1944 in the book [30] by John Von Neumann and Oskar Morgenstern. It was initially used in economics for studying interactions between business companies. Later, this concept made its way to other fields.

Next, in 1953, John Nash contributed to this field and presented the renowned Nash equilibrium in [31]. Bayesian games and improvements were made to John Nash’s work later in 1960’s. Evolutionary game theory was introduced in 1970s which paved a way to game theory’s future in biology.

Game theory over the years has emerged as a valuable tool to provide mathematical models and framework to study security related decision making in networks. It is relevant for both wired and wireless networks. It is ideal for modelling a competition between players having different objectives [32].

Hadi Otrok in [33], 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.

2.6.1 Mean Field Game Theory:

Mean Field Game theory grabbed the attention of the world when it first came out in March, 2006 [34]. It is designed to study the scenarios having large population of players which have little effect on the complete game. Although, the players can influence the whole system by combining their efforts [35].

The key elements of a game are:

- Players
- Set of actions/strategies open to players
- Payoffs (as a result of adopted actions)
- Utility functions of players

Several researchers have applied mean field games and approximation methods to solving typical wireless network problems [36] [37] [38]. In [39] 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.

2.7 Conclusion

In this chapter, literature reviewed in the research was covered. The working of CR networks was presented in the preliminary part. Security issues of the CRN and attacks on networks were discussed in length. The primary user emulation attack is also defined along with PUE detection and defence approaches. Moreover, existing mean field game theoretical approaches applied on the network are covered in the chapter.

Chapter 3

Proposed Scheme for Attack Detection

3.1 Introduction

In this chapter, we present our proposed PUE attack detection technique which is the basis for the proposed defence technique against PUE attacks, presented in Chapter 4.

3.2 System Description

In our system model, there are N nodes of ad hoc cognitive radio network. Each node is equipped with a detection system. 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 3.1.

Assumptions:

- Both malicious and legitimate 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.

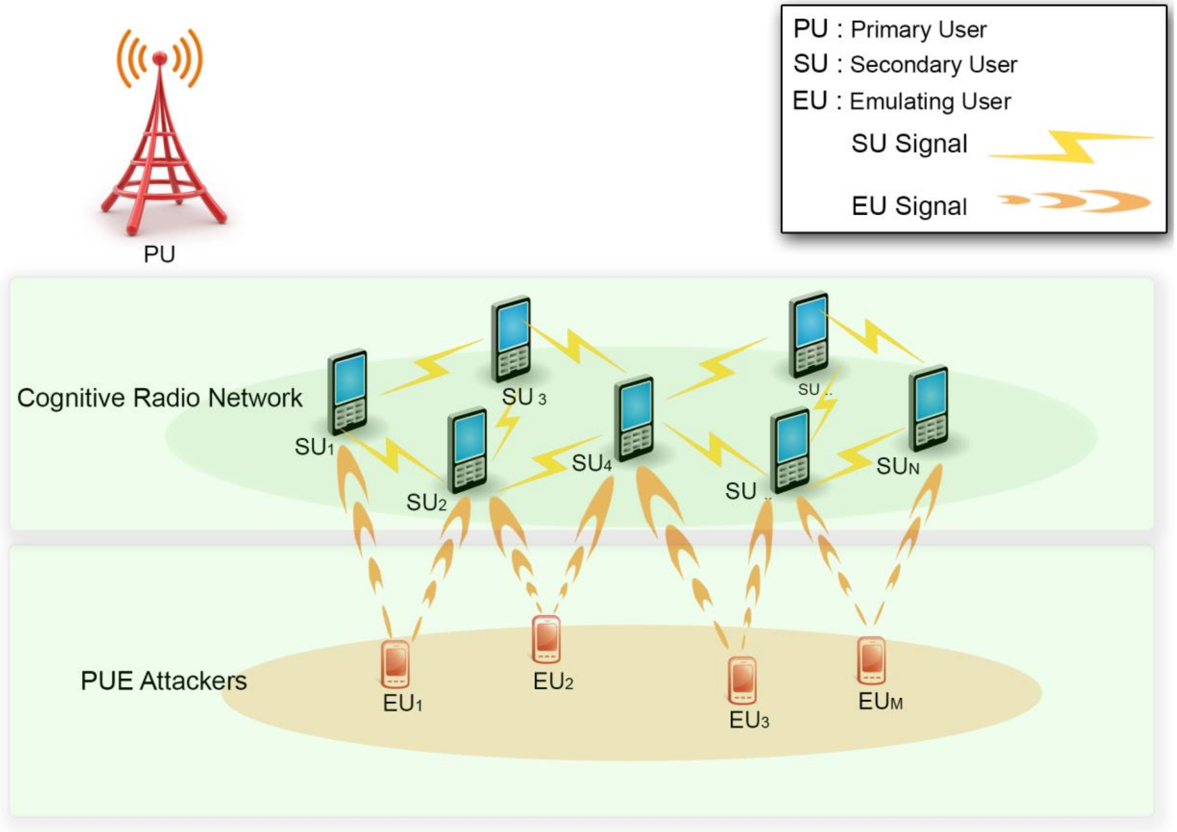

Figure 3.1: Cognitive radio network under PUE attack

3.3 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 3.2. 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**:** $\boldsymbol{H_0}$ (signal is absent)

Hypothesis 1**:** $\boldsymbol{H_1}$ (signal is present)

$$\begin{cases} H_0 : y(t) = \omega(t) \\ H_1 : y(t) = h.x(t) + \omega(t) \end{cases} \qquad (1.1)$$

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

The equation (1.1) can also be revised as:

$$y(t) = bh.x(t) + \omega(t) \qquad (1.2)$$

Here b is 0 for H_0 and 1 for 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, …,* N_s*).* The combined energy is E_c. Here, energy vector e[n] = |y^2(n)|, and combined energy 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 [40]. The input signal *y(t)* is passed via a Band Pass Filter with centre frequency f_o and bandwidth *W*, with transfer function.

$$H(f) = \begin{cases} \frac{2}{\sqrt{N_o}}, & |f - f_o| \leq W \\ 0, & |f - f_o| > W \end{cases} \qquad (1.3)$$

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.

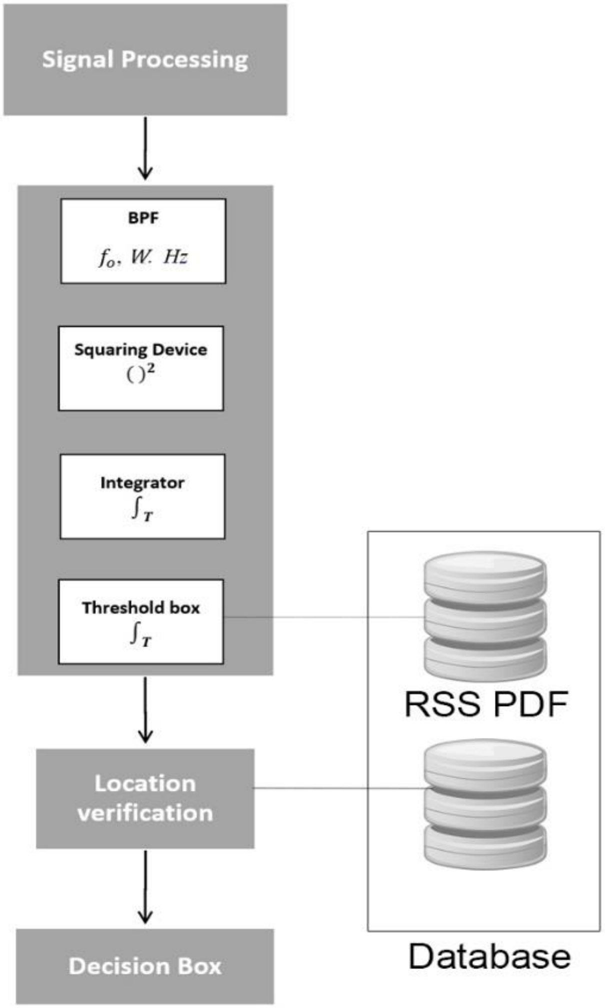

Figure 3.2: Architecture of proposed detection system

On applying Neyman-Pearson criterion on the problem, the likelihood ratio for the hypothesis test can be expressed as [34].

$$\Lambda_{LR} = \frac{f_y|H_0(x)}{f_y|H_1(\mathrm{x})} \tag{1.4}$$

Here, probability density function (PDF) of the signal received y under hypothesis H is $f_y|H_0(\mathrm{x})$ 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 [35]. After applying filter, energy sampling, squaring, and integrating of values, the statistics of detector can be written as:

$$\Lambda = \sum_1^{N_s} |y[n]|^2 = \sum_1^{N_s} |e_r(n)^2 + e_i(n)^2| \tag{1.5}$$

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.

Next, the combined energy is compared to three thresholds in threshing 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 exists. 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 its PUE attacker. Else, if energy is between a_1 and a_2 (i.e. $a_1 < E < a_2$) its considered a PU signal.

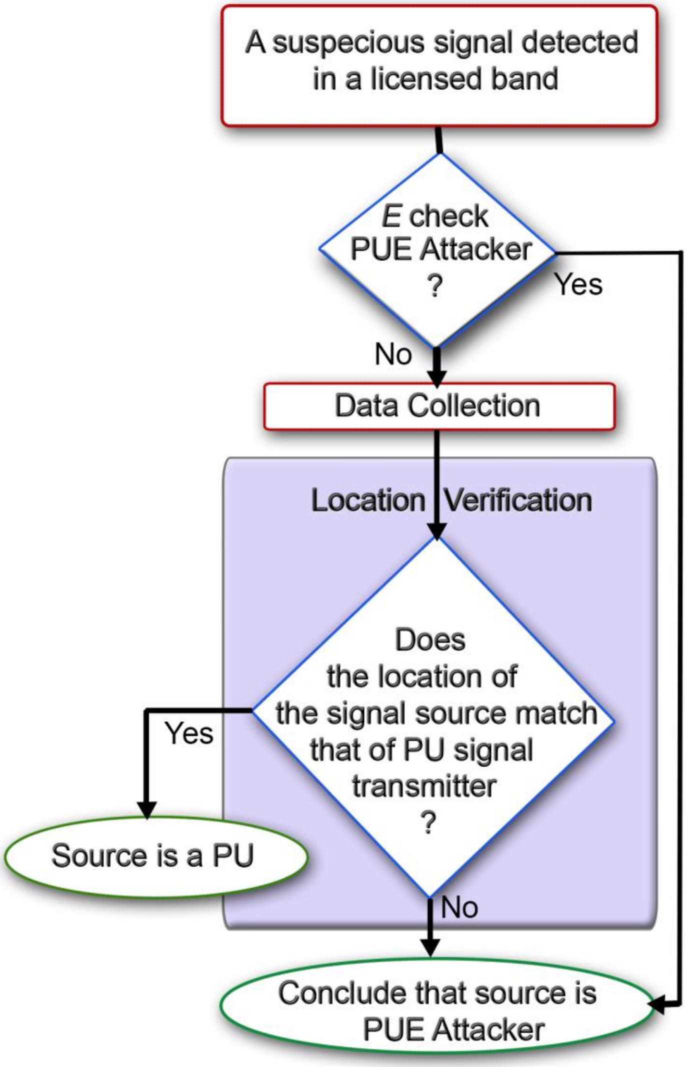

Figure 3.3: Flow chart of detection scheme

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, its considered a PUs signal. This characteristic can be easily utilized by the attacking secondary users. A malicious secondary user can fabricate an unrecognisable signal by transmitting at a higher power than other nodes, pretending a PU and refute 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 legit primary user.

Despite the distributed architecture of the CR network, nodes share certain information and knowledge of channel characteristics. If few SU 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 decision box. Else, the more detailed information in sampled energy vector e[n] is dispatched to the location verifying box.

Based on our concept we can represent hypothesis test with $\mathbf{H_0}$, $\mathbb{H}_1$ & $\mathbb{H}_2$, where they signify absence of signal, presence of PU signal, and PUEA signal respectively.

$$\begin{cases} \mathbf{H_0}: & \text{No signal} & (E < a_0) \\ \mathbb{H}_1: & \text{Real PU signal} & (a_1 < \mathrm{E} < a_2) \\ \mathbb{H}_2: & \text{PUE attacker signal} & (a_0 < \mathrm{E} < a_1)\text{or}(\mathrm{E} > a_2) \end{cases} \tag{1.6}$$

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

Probability of Misdetection (P_{md})

It is the probability of the scenario in which an attacker is considered primary user. From attacker's perspective, it is the probability of a successful PUE attack.

Probability of False Alarm *(P_{fa}):*

When malicious users are considered primary users. From attacker's perspective, it is the probability of a successful PUE attack. In our case, we are only interested in probability of detection P_d and probability of false alarm P_{fa}.

As there are large number of samples, we use central limit theorem (CLT). The main idea is to get clarity on 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 values approach a normal distribution when there are large number of samples. By applying CLT, to the test statistics (1.5) we can get the accurate approximation with a normal distribution for a large number of samples:

$$\Lambda \sim \mathcal{N}\left(\sum_1^{N_s} \mathbb{E}[|y[n]|^2], \sum_1^{N_s} \mathbb{V}ar[|y[n]|^2]\right) \tag{1.7}$$

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

$$\mathbb{E}[|y(n)|^2] = \begin{cases} 2\sigma_w^2 & : \mathbf{H_0} \\ 2\sigma_w^2 + |\boldsymbol{h}|^2\ |s(n)|^2 & : \mathbf{S1} \\ 2\sigma_w^2 + |\boldsymbol{h}|^2\ |2\sigma_s^2|^2 & : \mathbf{S2} \end{cases} \tag{1.8}$$

$$\mathbb{V}\mathrm{ar}[|y(n)|^2] = \begin{cases} (2\sigma_w^2)^2 & : \mathbf{H_0} \\ 4\sigma_w^2(\sigma_w^2 + |\boldsymbol{h}|^2\ |s(n)|^2) & : \mathbf{S1} \\ 4(\sigma_w^2 + |\boldsymbol{h}|^2\ \sigma_s^2)^2 & : \mathbf{S2} \end{cases} \tag{1.9}$$

The distribution Λ can be given as:

$$\Lambda \sim \begin{cases} (K(2\sigma_w^2), K(2\sigma_w^2)^2) & : \mathbf{H_0} \\ (K(2\sigma_w^2)(1-\gamma), K(2\sigma_w^2)^2(1-2\gamma) & : \boldsymbol{S1}\ complex - PSK \\ (K(2\sigma_w^2)(1-\gamma), K(2\sigma_w^2)^2(1-\gamma)^2) & : \boldsymbol{S2} \end{cases} \tag{1.10}$$

Using mean and variance in (1.10), the false alarm probability $P_{fa}$is approximated as:

$$P_{fa} \approx Q\left(\frac{a-N(2\sigma_w^2)}{\sqrt{N}(2\sigma_w^2)}\right) \qquad (1.11)$$

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

$$P_d \approx Q\left(\frac{a-N(2\sigma_w^2)(1+\gamma)}{\sqrt{N(1+2\gamma\ )(2\sigma_w^2)}}\right) \qquad (1.12)$$

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.

$$P_d(a_1, a_2) = P_r\{a_0 < E < a_1|\mathbb{H}_2\} + P_r\{E > a_2|\mathbb{H}_2 \qquad (1.13)$$

$$P_{fa}(a_1, a_2) = P_r\{E < a_1|\mathbb{H}_1\} + P_r\{E > a_2|\mathbb{H}_1\} \qquad (1.14)$$

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

In our 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 will kick in, and identify the attack. The reason of success in this scenario is that it is unfeasible 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.

3.4 Conclusion

To sum it up, in this chapter, we presented the proposed scheme for PUEA detection, details of CR Network under consideration, system model for detection system, energy detection, and location verification mechanisms. The simulation results representing the working and effectiveness of the scheme are covered in chapter 5.

Chapter 4

Proposed Scheme for Defence

4.1 Introduction

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

4.2 Game Model & Formulation

The Figure 4.1 illustrates an N-node CRN and M attackers which can attack the nodes dynamically. The nodes of network are independent 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 information will be 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 6 we consider all legitimate nodes 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 players' 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,….,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,….N), are denoted as $s_i(t)$ and $a_i(t)$ respectively.

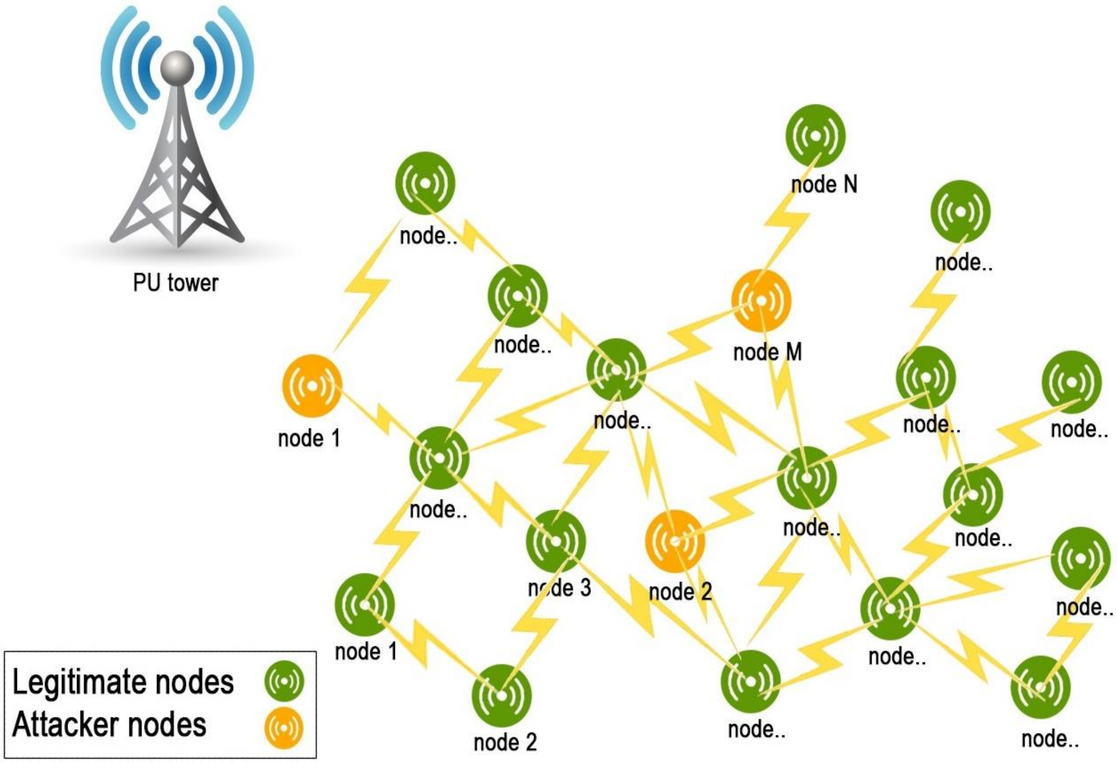

Figure 4.1: An N node CRN with M attackers.

To demonstrate the interaction between the attackers and the defenders the game is a non-zero sum, non-cooperative game. It is defined that the defending player has a security value 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.

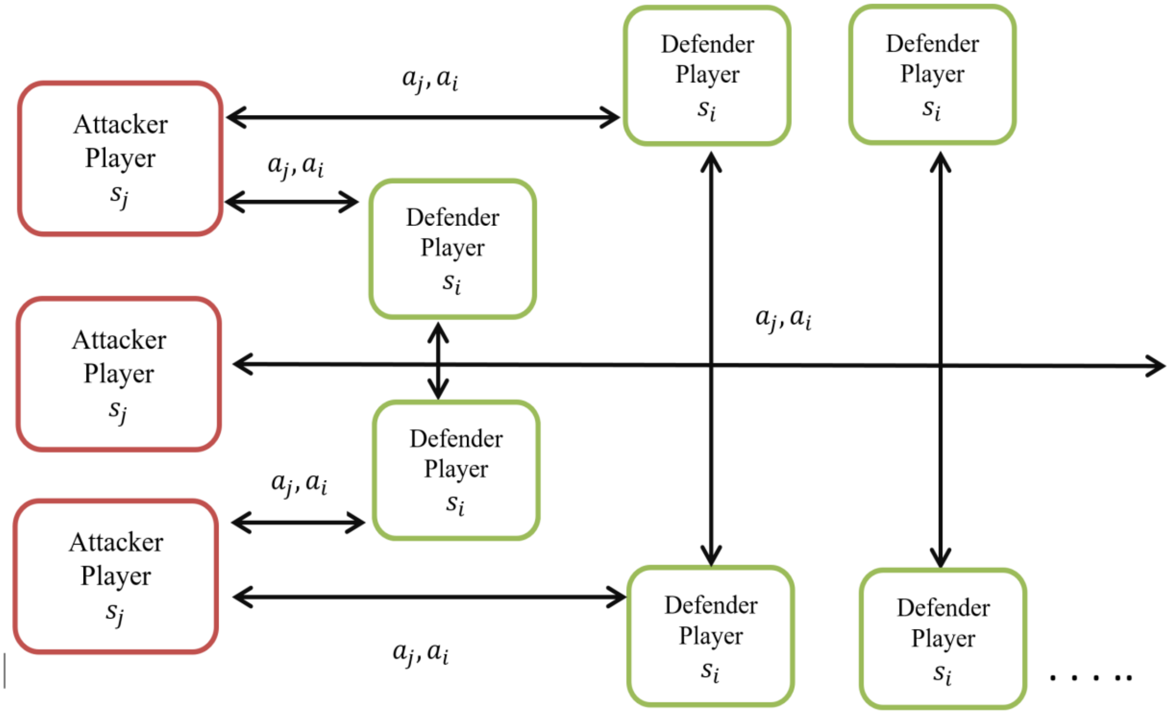

Figure 4.2: Mean Field Game model of our CRN representing states and actions of attackers and defenders.

4.3 Defining Transition Laws, States and Cost Functions

The state of the attacking players can be defined as a combination of energy and possessions (Like, information). It is denoted in [33] as:

$$\alpha_{E_j} E_j + \alpha_{I_j} I_j \tag{2.1}$$

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

$$\alpha_{E_i} E_i + \alpha_{S_i} S_i \tag{2.2}$$

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

$$S^{(N)}(t) = (\mathrm{S}_1^{(\mathrm{N})}(t), \cdot \quad \cdot \quad \cdot, \mathrm{S}_\mathrm{K}^{(\mathrm{N})}(t)) \ (\mathrm{t} \geq 0) \tag{2.3}$$

State transition laws of attacker and defender players respectively are:

$$T_j(y|x, a_j) = P(s_j(t+1) = y|s_j(t) = x, a_j(t) = a_j) \tag{2.4}$$

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

$$T_i(y|x, a_i) = P(s_i(t+1) = y|s_i(t) = x, a_i(t) = a_i) \tag{2.5}$$

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

4.3.1 Attacker Player’s Cost

The costs of the attacking players can be expressed by:

$$c_j\left(s_j(t),\ a_j(t), S^{(N)}(t)\right) = f_j\left(s_j(t),\ a_j(t)\right) - f(S^{(N)}(t)) \tag{2.6}$$

Here, $f_j\left(s_j(t),\ a_j(t)\right)$ is the combined energy cost when attacking player adopts different actions under different states. $f(S^{(N)}(t))$ is the payoff of the attacker player which comes from attacking. When a state has full energy, the attacking player can decide to attack the whole CRN. The energy cost is much higher in this case than the state of poor energy. The attacking players mostly will not attack in poor energy state.

4.3.2 Defender Player's Cost

The cost of a representative defending player i can be expressed as:

$$c_i\left(s_i(t), a_i(t), s_j(t), a_j(t), S^{(N)}(t)\right) = g_i\left(s_i(t), a_i(t)\right) + g_{ij}(S^{(N)}(t), s_j(t),\ a_j(t)) \quad (2.7)$$

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.

4.4 Mean Field Game Formulation

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

$$\theta(t+1) = \phi(s_j(t), \theta(t)) \quad (2.8)$$

Here, θ(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 θ(t) is used. Here, the equation describes that the update of random process is done by the current state of attacker and the mean state of CRN.

4.4.1 Limiting function and Updating Rule

For the system description consider a matrix of size n x n:

$$Transition(x,\theta) = \begin{bmatrix} T(1|1), \hat{\pi}(1, s_j, \theta)) & \cdots & T(n|1), \hat{\pi}(1, s_j, \theta)) \\ \vdots & \ddots & \vdots \\ T(1|n), \hat{\pi}(n, s_j, \theta)) & \cdots & T(n|n), \hat{\pi}(n, s_j, \theta)) \end{bmatrix} \qquad (2.9)$$

The function ϕ from (2.8) can be written as:

$$\phi(s_i(t)\ ,\theta(t)) = \theta\, Transition(s,\theta) \qquad (2.10)$$

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

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

For θ(t) the updating rule will be ($\theta\epsilon[0,1]$):

$$\Phi = s_j(\theta)^{1/2} + (1 - s_j)(\theta)^2 \qquad (2.11)$$

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

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

4.5 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. It is given by [33]:

$$\mathrm{v}(s_j,\theta) = \min_{a_j \in A_j} \{c_j\ (s_j, a_j, \theta)\ + \Delta\}\ , \qquad (2.14)$$

where, $\Delta = \rho \sum_{k \in S\mathrm{j}} T\mathrm{j}\ (k\ |s_j, a_j\ )\ v\ (k, \phi(s_j, \theta))$. The defending player's optimum strategy π_i can also be achieved by:

$$\mathrm{w}(s_i,\ s_j,\ \theta) = \min_{a_i \in A_i} \{\mathrm{c}\ (s_i, a_i, s_j, \theta)\ +\ \Omega\} \qquad (2.15)$$

$\Omega\ = \rho \sum_{j \in S, k \in S\mathrm{j}} T(j\ |xi, ui\ ) T\mathrm{j}\ (k\ |s_j, \hat{}\pi_j) w\ \left(j, k, \phi\ (s_j, \theta)\right)$. In the end the function ϕ is revised as (2.11). Using dynamic programming equations and respective cost functions the optimum strategies are determined.

$$\pi_j = \{P_{j1} +\ P_{j2} +\ P_{j3} \ldots \ldots \ldots P_{jL}\}$$

$$\pi_i = \{P_{i1} +\ P_{i2} +\ P_{i3} \ldots \ldots \ldots P_{iL}\}$$

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.

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

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

4.6 Conclusion

To summarise this, we have covered the anticipated scheme for defence. The chapter covers the system description, mean field game model, transition laws, states, attacking and defending players cost functions, and mean field game solution.

Chapter 5

Simulation Results and Discussion

5.1 Introduction

In this chapter, the simulation results of proposed scheme are presented. Our 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.

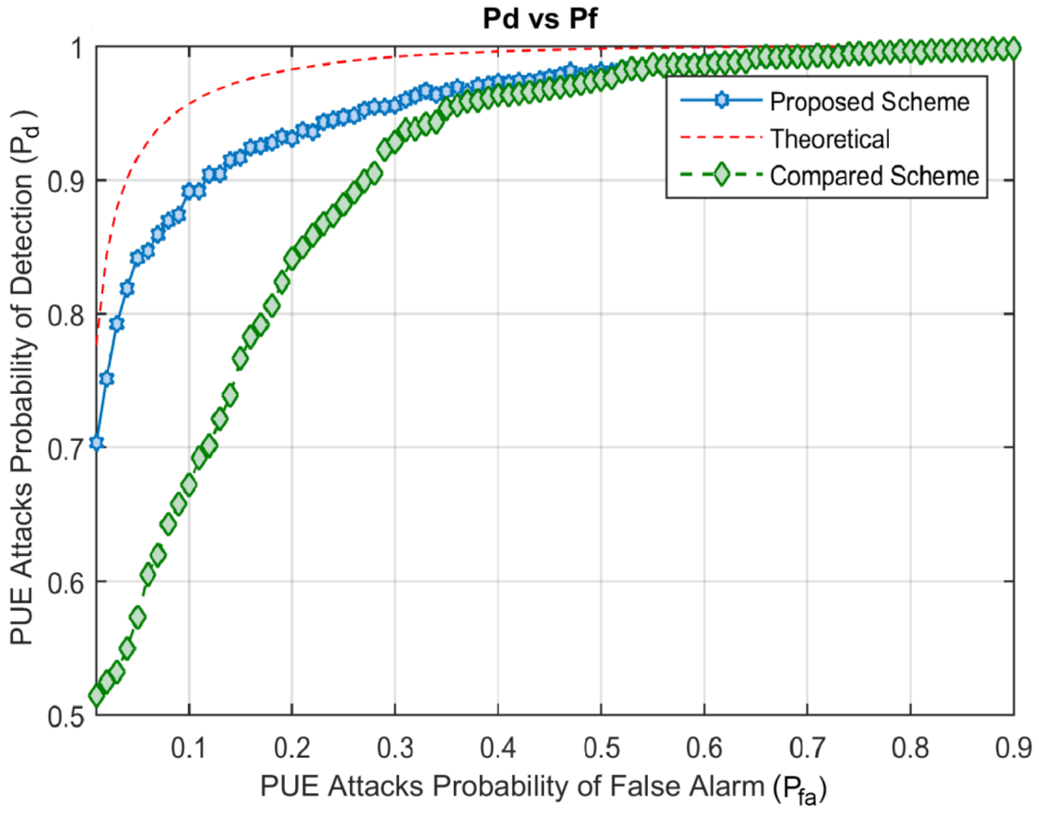

Figure 5.1. Plot of Probability of Detection (P_d) vs Probability of False Alarm (P_{fa}).

5.2 Simulation of Attack Detection

For simulation, we make 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. Figure 5.1 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 used. More samples lead to higher detection probability. The SNR is -5dB. 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 [41], we can observe that the proposed scheme is 1.32 times more accurate when P_{fa} <= 0:1.

5.3 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 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 can be 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 γ 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 8. 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:

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

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

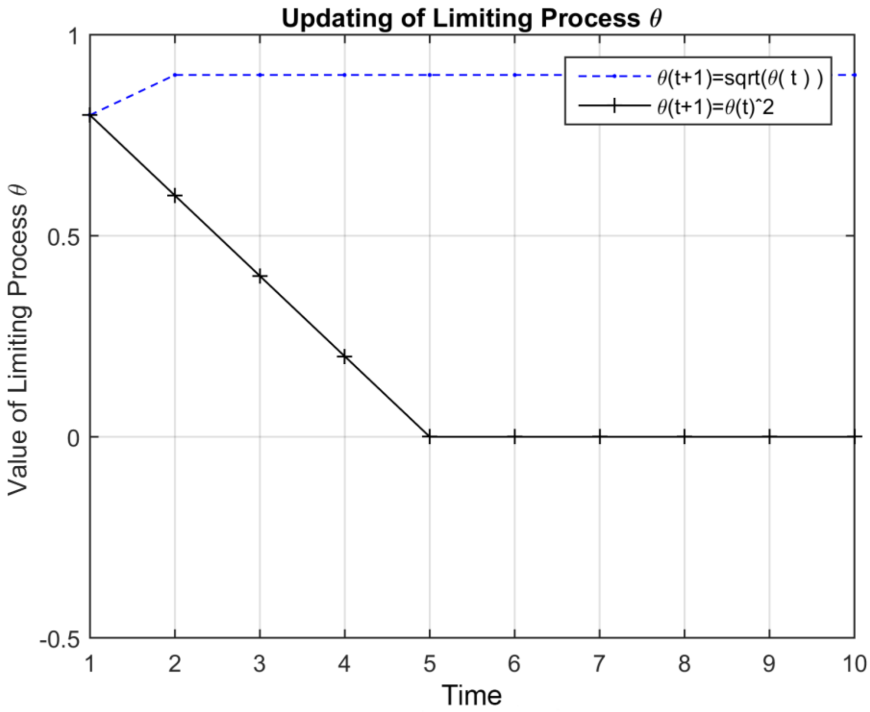

Figure 5.2: Value of theta updating during the iteration. Its value close to 1 represents that most of the legit nodes of network are in defence state.

The cost matrix for the attacking node is defined as:

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

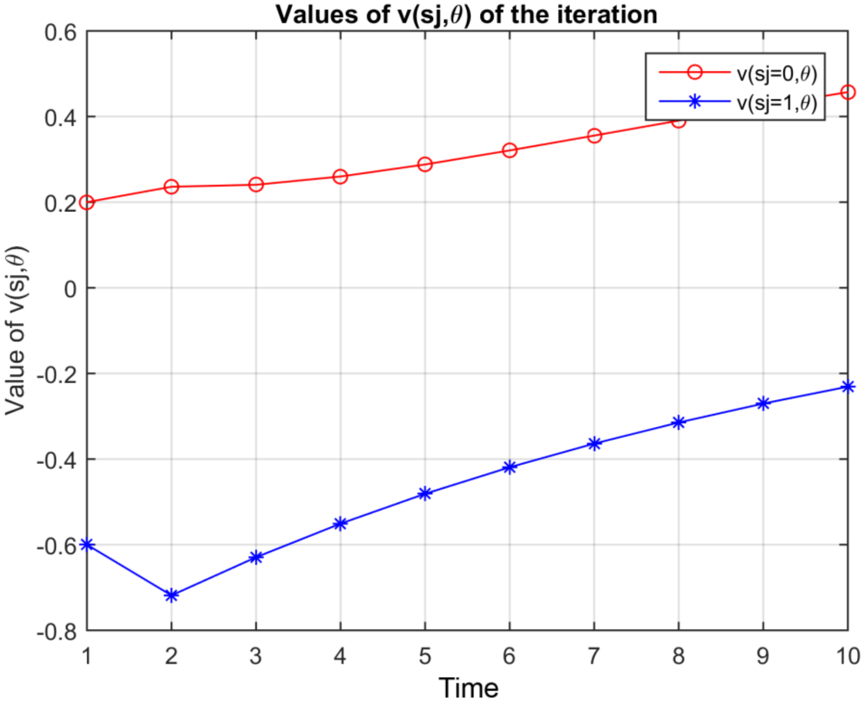

Figure 5.3: Value of v from dynamic programming equation for attacking players.

It can be observed from the graphs in Figure 5.2 and 5.3 that when the state of the attacking player is standby the value of *v* is below zero. The results also present that more attacks 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 π is revealed.

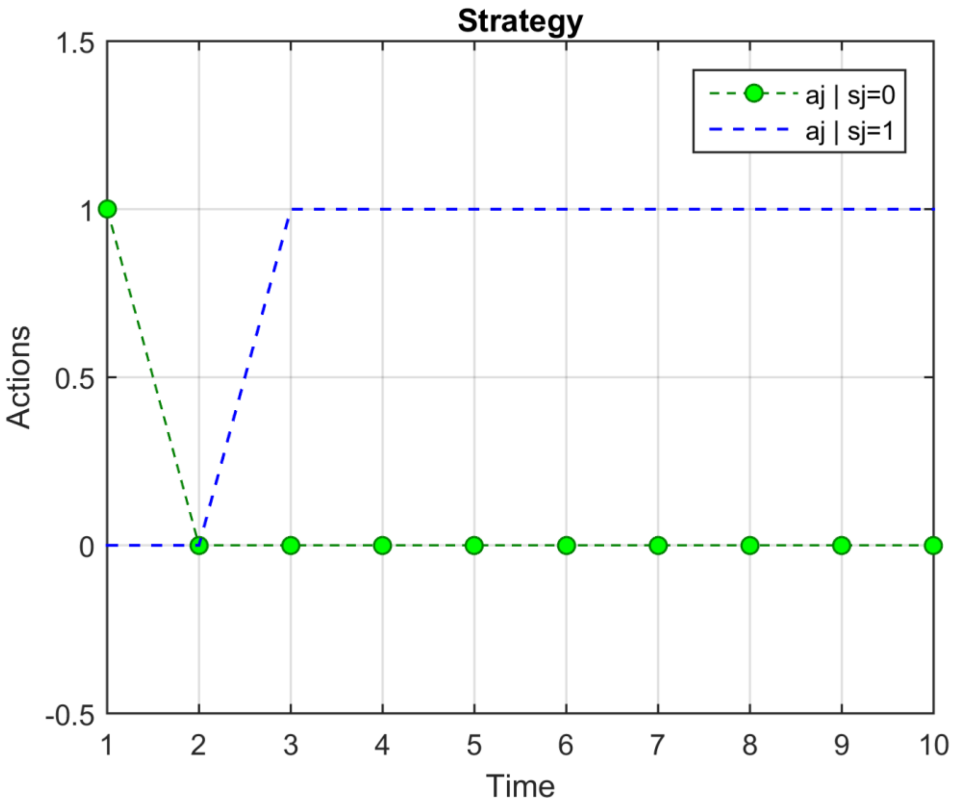

Figure 5.4: Strategy of attacking players.

When state $s_j = 0$:

$$\pi_0^0 = [p\left(a_j = 0 \middle| s_j = 0\ \right) = 1, \qquad p\left(a_j = 1 \middle| s_j = 0\ \right) = 0]$$

When $s_j = 1$

$$\pi_0^1 = [p\left(a_j = 0 \middle| s_j = 1\ \right) = 1, \qquad \alpha\left(a_j = 1 \middle| s_j = 1\ \right) = 1]$$

After simulating the iteration, the state transition matrix will be updated as per equation above:

$$T_j = \begin{bmatrix} T_j(0|0), \pi_j & T_j(1|0), \pi_j \\ T_j(0|1), \pi_j & T_j(1|1), \pi_j \end{bmatrix} = \begin{bmatrix} 0.8 & 0.2 \\ 0.02 & 0.98 \end{bmatrix} \tag{2.16}$$

5.4 Defending Player’s Strategies π_i

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:

$$\mathrm{T} = \begin{bmatrix} 0.7 & 0.2 \\ 0.03 & 0.97 \end{bmatrix}$$

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

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 (2.15) and forming the utility matrix in tactical form for defending nodes in a CRN.

$$\begin{array}{ccc} \textbf{States} & \textbf{Defence} & \textbf{No Defence} \\ \textbf{\textit{Attack}} & g_i(s_i, 0) + \theta(t)[r_i p_i \; - \; (1 - r_i) q_i] & g_i(s_i(t), 1) + \theta(t) q_i \\ \textbf{\textit{Standby}} & g_i(s_i, 0) & 0 \end{array} \tag{2.17}$$

The cost matrices for the defending nodes are:

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

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

Using the results of the tactical form of utility matrix we get the cost matrices as:

$$C1=\begin{bmatrix} 1.8 \; - \; 0.3\theta & 2.5\theta \\ 0.8 \; - \; 0.3\theta & 2.5\theta \end{bmatrix} \text{ and, } C2=\begin{bmatrix} 1.8 & 0 \\ 0.8 & 0 \end{bmatrix}$$

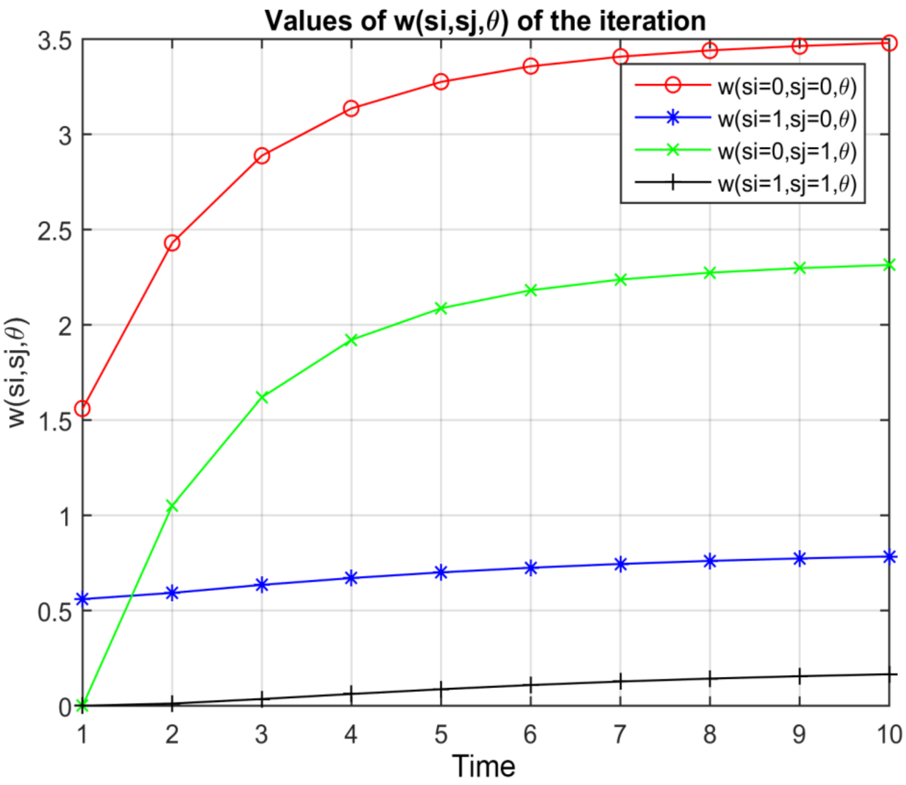

Figure 5.5: Value of w(s_i, s_j, θ) from dynamic programming equation for defending players

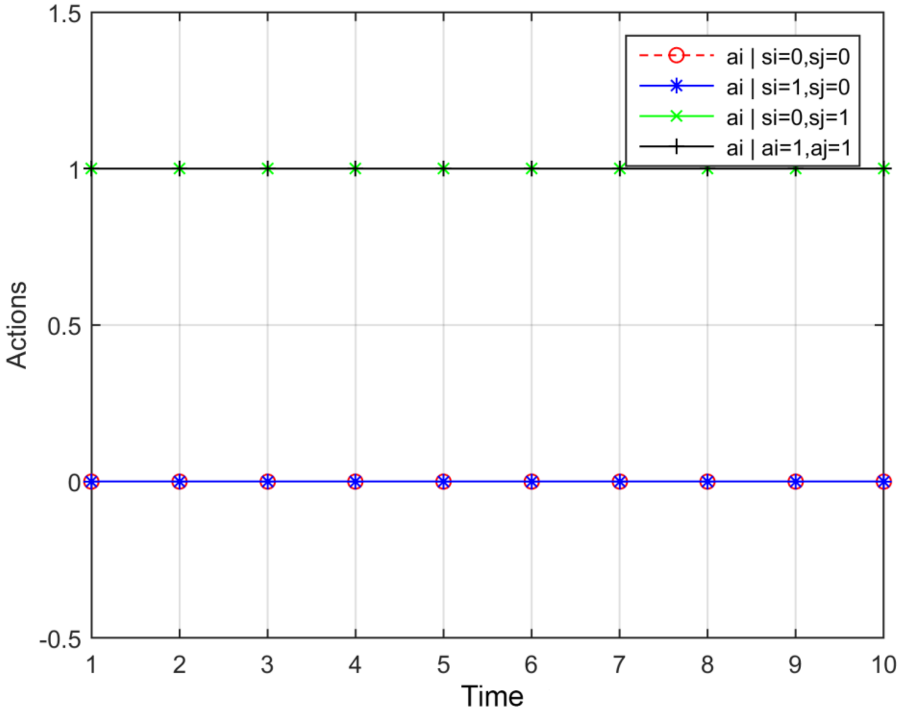

Figure 5.6: Strategy of defending players.

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 we get the optimum strategy for respective defending player π_i.

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

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

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

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

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

When state of attacker s_j is 0;

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

When it is 1;

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

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 (2.12). The matrix (2.11) in our current scenario can be written as:

$$Transition(s_j,\theta) = \begin{bmatrix} T(0|0), \hat{\pi}(1, s_j, \theta)) & T(1|0), \hat{\pi}(1, s_j, \theta)) \\ T(0|1), \hat{\pi}(1, s_j, \theta)) & T(1|1), \hat{\pi}(1, s_j, \theta)) \end{bmatrix} \qquad (2.14)$$

$$T_{rev}(s_j = 0, \theta) = \begin{bmatrix} 0.9 & 0.1 \\ 0.03 & 0.97 \end{bmatrix}$$

$$T_{rev}\ (s_j = 0, \theta) = \begin{bmatrix} 0.9 & 0.1 \\ 0.02 & 0.98 \end{bmatrix}$$

For complete simulation of the scheme we consider an ad-hoc CR network of N nodes. Each node in the network uses our 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 Figure 5.7, 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 Figure 5.8 and 5.9, 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.

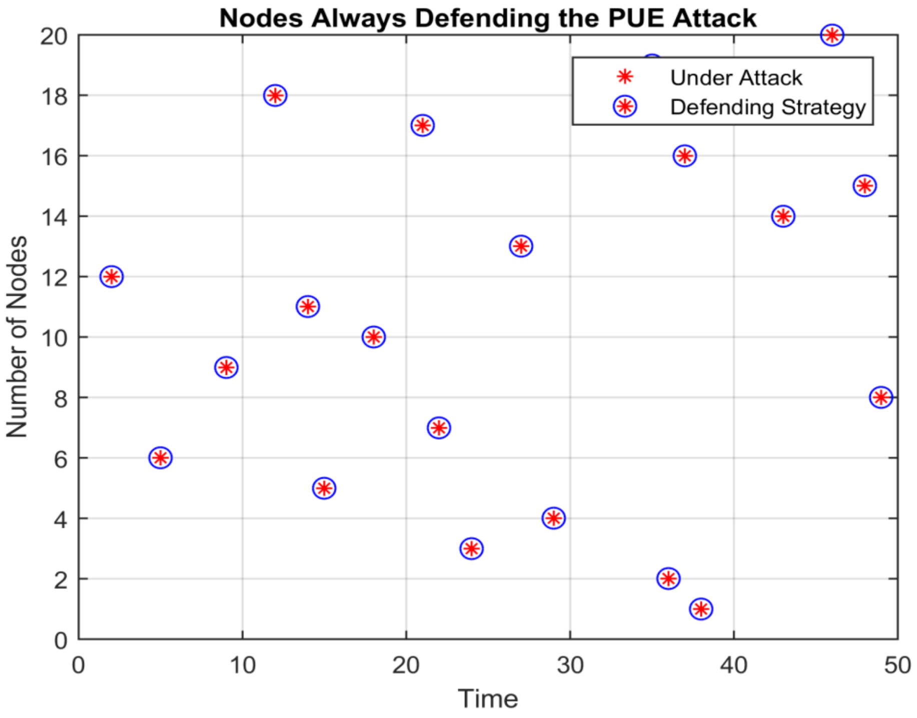

Figure 5.7: All nodes defending with optimum strategy

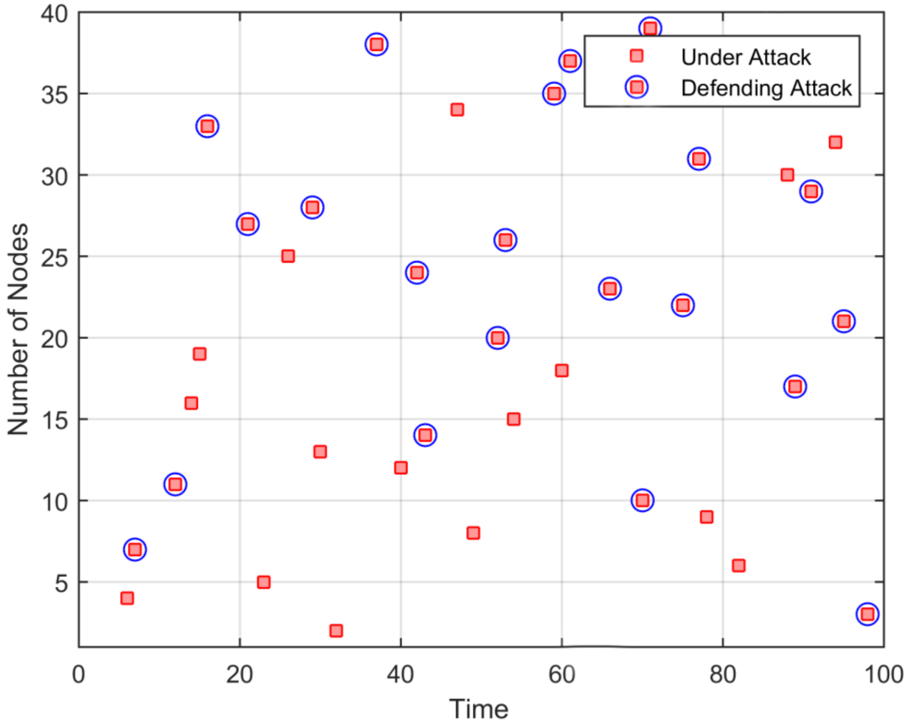

Figure 5.8: Nodes defending PUE attacks keeping their state under consideration.

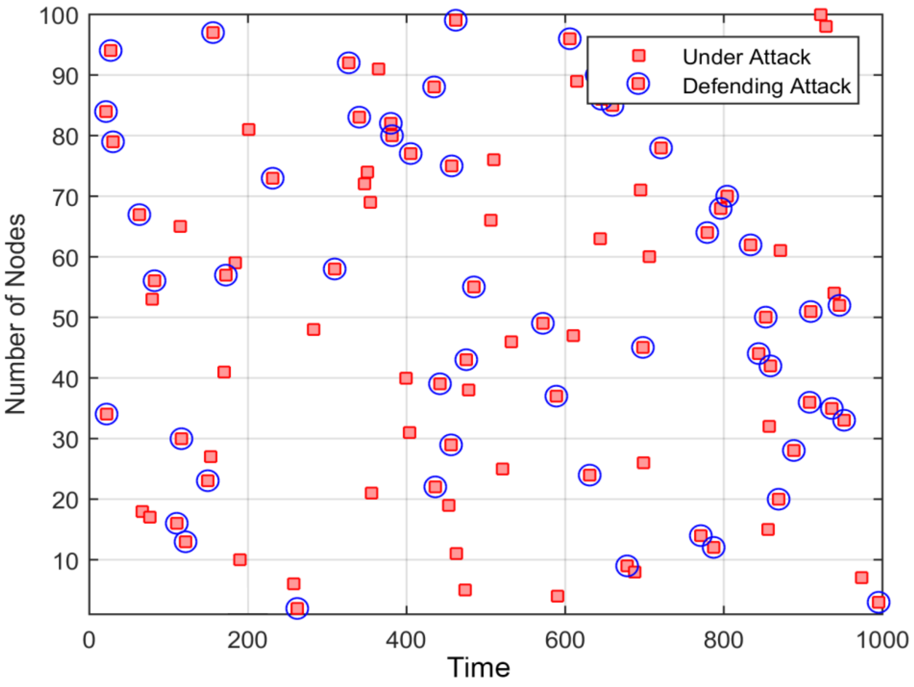

Figure 5.9: CRN of 100 Nodes defending PUE attacks keeping their, and attacker's states under consideration.

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 Figure 5.10 shows the lifetime comparison of 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 Figure 5.11, 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.

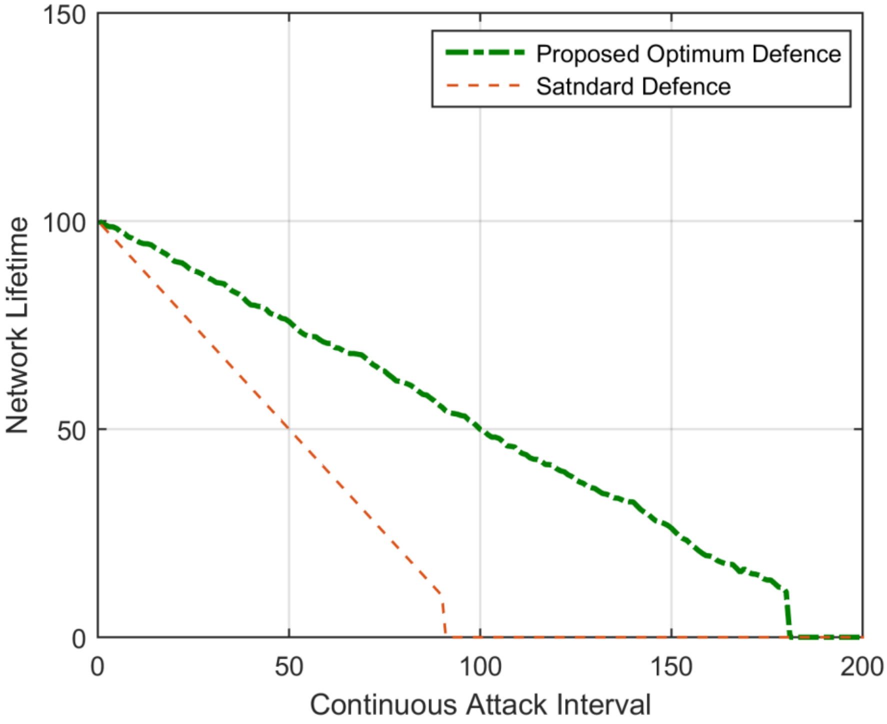

Figure 5.10: Lifetime comparison of the proposed defence scheme with standard scheme.

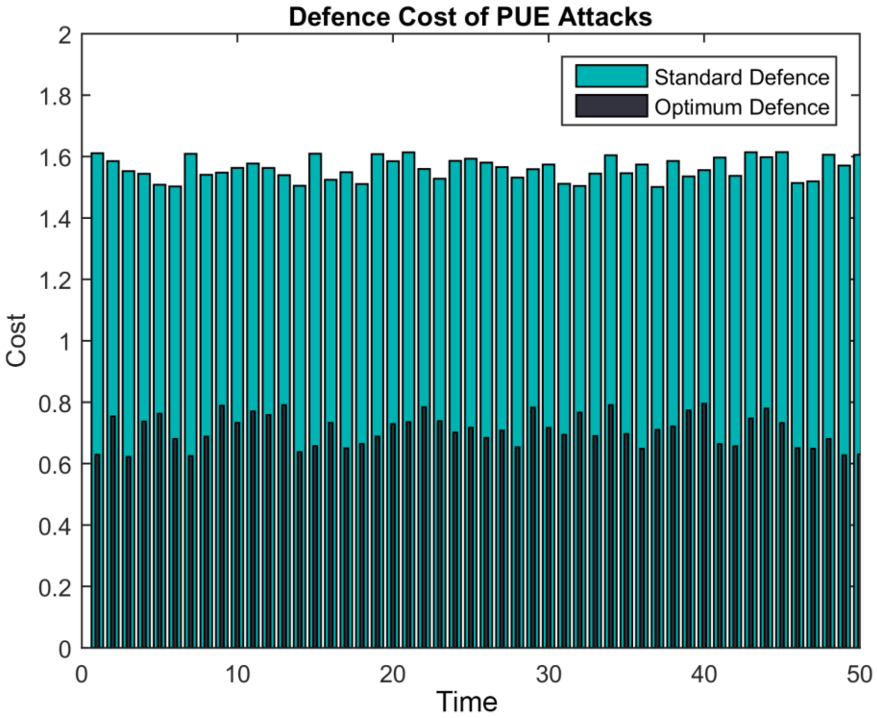

Figure 5.11: Cost comparison between standard and optimum defence actions under PUE Attacks.

5.4 Conclusion

In summary, an example representing the working of the theoretical system and players adopting the best strategies is presented in this chapter. The optimum tactic parameters are also discussed here. Moreover, the simulation results involving defence actions, lifetime of network, and defence costs are compared, and discussed in length.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

This thesis presents a complete security system to detect and smartly defend a CRN against PUE attacks. In the commencement of the document, a PUE detection approach was presented to spot attacking nodes. The approach reduces network overheads produced by data signing and other cryptographic techniques. The mechanism for energy detection and location verification is also presented in the research work.

After spotting the attacker nodes mean field game approach is used to enable each node to make strategic defence decisions depending upon the states of the node and attacker. The scenario of multiple attackers is also considered.

The simulations are in the culminating chapter. The results show that the proposed detection system is 1.32 times more accurate than compared work. An example to demonstrate the adoption of optimum strategies of attackers and defenders is also in this work. Furthermore, simulations of nodes doing defence, network lifetime comparison under continuous PUE attack, and defence cost comparison are also in this thesis.

In short, the proposed scheme is used to enable each individual node to make better strategic defence decisions against multiple PUE attackers. The scheme also considers energy consumption along with the security to make intelligent decisions.

6.2 Future Work

In the future work, we will implement this system on vehicular CR ad hoc networks, formulate equations of mobility, design tests, and simulate results. Creation of more utility functions is also our aim in the future. A different updating rule for limiting process and comparison results will also be in our work.

We will also implement the proposed game approach to handle routing problems in ad hoc environment. Moreover, our upcoming goal would be to present a game approach to cater security and other complex parameters in different network settings like. CR-VANETS, and CR-FANETS. Last but not the least, our work will hold scenarios to tackle various categories of attacks on the network.

Notations

$\mathbf{H_0}$	Hypothesis for signal is absent
$\mathbf{H_1}$	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 $n = 1, 2, \ldots, N_s$)
Λ	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_j
$S^{(N)}(t)$	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	Defender's n_i security value as a result of successful defence
q_i	Defender's n_i security value as a result of unsuccessful defence

r_i	Rate of successful defence
Π_j	Attackers strategies
Π_i	Defenders strategies
T_{rev}	Matrix to reverse the function Φ

References

[1] M. III and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[2] J. Mitola III, *Cognitive Radio*. Licentiate dissertation, The Royal Institute of Technology, Stockholm, Sweden, Sept. 1999.

[3] F. K. Jondral, “Software-defined radio-basics and evolution to cognitive radio,” *EURASIP Journal on Wireless Communications and Networking*, vol. 3, pp. 275–283, 2005.

[4] Z. Marinho J, Granjal J, Monteiro E, “A survey on security attacks and countermeasures with primary user detection in cognitive radio networks”. *EURASIP Journal on Information Security*: 1–14, 2015

[5] T. Charles Clancy and Nathan Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), Singapore, May, 2008, pp.1-8.

[6] Olga León, Juan Hernández-Serrano and Miguel Soriano, Securing Cognitive Radio Networks, International Journal of Communication Systems, Vol.23, No.5, 2010, pp.633-652.

[7] Chetan Mathur and Koduvayur Subbalakshmi, Security Issues in Cognitive Radio Networks, Cognitive Networks: Towards Self-Aware Networks, Wiley, New York, 2007, pp.284-293.

[8] Ruiliang Chen, Jung-Min Park, Y. Thomas Hou and Jeffrey H. Reed, Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks, IEEE Communications Magazine, Vol.46, No.4, 2008, pp.50-55.

[9] Yih-Chun Hu, David B. Johnson and Adrian Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, NY, June, 2002.

[10] Juan Hernandez-Serrano, Olga León and Miguel Soriano, Modeling the Lion Attack in Cognitive Radio Networks, EURASIP Journal on Wireless Communications and Networking, Vol.2011, Article ID 242304, 10 pages, 2011.

[11] Spectrum Bridge, "White space overview." [Online]: http://spectrumbridge.com/tv-white-space/

[12] WRAN WG on Broadband Wireless Access Standards, IEEE 802.22 [Online]. www.ieee802.org/22.

[13] Shraboni Jana, Kai Zeng, Wei Cheng "Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks", IEEE Transactions on Information Forensics and Security, vol. 8, Issue.9: 1497 – 1507, 2013

[14] Su Wengui, Liao Yang, "A jury-based trust management mechanism in distributed cognitive radio networks," China Communications IEEE, vol.12, Issue.7: 119 – 126, 2015

[15] Ruiliang Chen and Jung-Min Park, Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks, *First IEEE Workshop on Networking Technologies*

for Software Defined Radio Networks (SDR), Reston, VA, September, , pp.110-119. 2006.

[16] Ruiliang Chen, Jung-Min Park and Jeffrey H. Reed, Defense against Primary User Emulation Attacks in Cognitive Radio Networks, *IEEE Journal on Selected Areas in Communications, Vol.26, No.1*, pp.25-37, 2008

[17] Lianfen Huang, Liang Xie, Han Yu, Wumei Wang and Yan Yao, Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks, *International Conference on Communications and Mobile Computing (CMC), Vol.2, Shenzhen, China*, pp.169-173, April, 2010,

[18] Caidan Zhao, Wumei Wang, Lianfen Huang and Yan Yao, Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio, *5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom '09), Beijing, China,* , pp.1-5, September, 2009

[19] D. Pu., "Detecting Primary User Emulation Attack in Cognitive Radio Networks," Proc. IEEE Global Telecommunications Conf, Dec. 2012.

[20] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Proc. IEEE Int'l Conf.Commun. (ICC), 2009.

[21] Adnan Nadeem, and Michael P. Howarth," A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE communications surveys & tutorials. pp. 2027-2045, 2013.

[22] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” IEEE Trans. Wireless Commun., vol. 11, pp. 38–47, Feb. 2004.

[23] P. Albers, O. Camp, 1. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems.

[24] Snort Team, SNORT User Manual, 2.9.7 ed, 2014, Available online at: https://www.snort.org/documents.

[25] Bro Team, Bro Documentation and Manual. Available online at: https://www.bro.org/documentation.

[26] S. Marti, T. 1. Giuli, K. Lai, and M. Baker, "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., August 2010

[27] Y. Zhang and W. Lee, “Intrusion detection in wireless ad hoc networks,” in ACM MOBICOM, pp. 275–283,2013.

[28] P. Albers, O. Camp, 1. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1- 12, April 2012.

[29] L. Ferraz, et-al., "An accurate and precise malicious node exclusion mechanism for ad hoc networks," Ad Hoc Networks, Elsevier. pp.l- 1 4, March. 2014.

[30] O. Morgenstern and J. Von Neumann, Theory of Games and Economic Behavior. Princeton University Press, third ed., May 1944.

[31] J. Nash, “Two person cooperative games,” Econometrica, vol. 21, pp. 128–140,Jan 1953.

[32] X. Liang and Y. Xiao, “Game theory for network security,” IEEE Communication. Surveys Tuts., vol. 15, no. 1, pp. 472–486, 2013.

[33] Otrok, H., et al., “A game-theoretic intrusion detection model for mobile ad hoc networks,” Elsevier Computer Communications, 31.

[34] M. Huang, R. P. Malham, and P. E. Caines, “Large population stochastic dynamic games: closed-loop mckean-vlasov systems and the nash certainty equivalence principle,” Communications in Information and Systems, vol. 6, pp. 221–252, Mar 2006.

[35] S. L. Nguyen and M. Huang, “Mean field lqg games with mass behavior responsive to a major player,” in Proc. 51st Int’l Conf. Decision and Control (CDC), pp. 5792–5797, Dec 2012.

[36] F. Meriaux, V. Varma, and S. Lasaulce, “Mean field energy games in wireless networks,” in Proc. 2012 Asilomar Conf. Signals, Systems., Computers.

[37] H. Tembine, P. Vilanova, M. Assaad, and M. Debbah, “Mean field stochastic games for SINR-based medium access control,” in Proc. 2011 Int’l ICST Conf. Performance Evaluation Methodologies Tools.

[38] M. Y. Huang, “Mean field stochastic games with discrete states and mixed players,” in Proc. 2012 GameNets.

[39] Y. Wang, F. Yu, H. Tang, and M. Huang, “A mean field game theoretic approach for security enhancements in mobile ad hoc networks,” IEEE Trans. Wireless Communication., vol. 13, no. 3, pp. 1616–1627, 2014.

[40] H. Urkowitz ”Energy detection of unknown deterministic signals”. Proceedings of the IEEE Volume: 55, Issue:4, April 1967

[41] Trong Nghia Le, Wen-Long Chin, and Ya-Hsuan Lin, ”Noncooperative and cooperative PUEA detection using physical layer in mobile OFDM-based cognitive radio networks”. International Conference on Computing, Networking and Communications, 24 March, 2016.