Survivability of Cognitive Radio Networks under Denial of Service Attack: A Game Theoretic Approach

by

NS Saba Afzal

Supervisor

Dr. Muhammad Imran

A thesis submitted to the faculty of Electrical Engineering Department Military College of Signals, National University of Sciences and Technology, Rawalpindi as part of the requirements for the degree of MS in Electrical Engineering

AUGUST 2018

Abstract

Spectrum is the essence of communication system. Wireless communication is inaccessible without Spectrum bands.CRNs provide the promising solution for the scarcity of wireless spectrum bands by presenting the idea of efficient utilization of vacant spectrum bands. The survivability of cognitive user under antagonistic conditions is a most challenging task. The survivability will become hard bitten with the actualization of “learning" and “smartness" features of the CRs. Denial of service attack is one of the most destructive type of attacks which creates devastation in the lifeblood of wireless communication system. It prevents the legitimate user to utilize the vacant spectrum band and prevents it from being able to communicate effectively. This thesis presents an adaptive mechanism for potent dynamic spectrum access (DSA) in the presence of DoS attack. Assuming both attacker and SU as rational players, and considering the notion of channel payoff, the optimal strategy is entrenched by presenting a scenario as zero-sum game which conclude to Nash equilibrium. We present linear programming algorithm to solve the mixed strategy Nash Equilibria.

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.

Acknowledgements

All praises to Almighty Allah who showed His blessings and gave me strength to complete my work.

This dissertation would not have been completed without the support and guidance of my advisors. I would like to special thanks to ***Major Muhammad Faisal Amjad,*** Phd. I am extremely fortunate to have such a generous advisor, whose continuous support and encouragement helped me to complete my research work. He opened new doors to the wireless communication research for me which have become the significant component of this thesis. He always made time for me, had long and useful discussions with me, and gave me invaluable advices. My sincere gratitude to my supervisor, ***Muhammad Imran***, PhD for serving as a mentor and kept me motivated during my research work. I would like to thank all my committee members **Col. Adil Masood**, PhD and **Col. Abdul Ghafoor**, PhD. Their valuable and insightful reviews have indeed helped me to improve the quality of my work.

Last but not the least, deepest thanks go to my mother and all my friends for their love, care and encouragement.

Dedication

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

I dedicate this research work to my mother and all the teachers in my life who have supported me at

every stage of life.

Table of Contents

List of Figures

List of Acronyms

Analog to digital convertor	A/D
Cognitive Radio	CR
Cognitive Radio Network	CRN
Denial of Service	DoS
Dynamic Spectrum Access	DSA
Federal Communications Commission	FCC
Game Theory	GT
Internet of things	IoT
Packet Delivery Ratio	PDR
Primary User	PU
Primary User Emulation Attack	PUEA
Radio Frequency	RF
Software Defined Radio	SDR
Spectrum Sensing Data Falsification	SSDF
Secondary User	SU

Chapter 1

INTRODUCTION

1.1 Overview

The wireless technology brought the great revolution in the field of communication, TV broadcasting and data networking. Electromagnetic radio spectrum is the backbone of wireless network. Wireless communication network allows user to feel free from traditional cord telephone network, which bound the user's presence in a specific area during communication. Wireless technology revolution provides global, easy and cheap mobile computing communication anywhere at any time. Next generation wireless applications require high transmission rate and faster speed, demands for more efficient spectrum. The evolution of IoT and software defined networks (SDNs), and moreover, the rapid usage of this technology, researchers predicted that more than 10 billion communication devices will be in use by 2020, and these devices would be more than 100 billion by 2025 [1]. Wireless communications and other applications cannot work without the electromagnetic radio spectrum band. These spectrum bands are divided and distributed according to the fixed spectrum assignment policy. The use of smart phones, tablets and other multimedia services create great demand for wireless broadband and digital networks. Due to fixed spectrum assignment policy and increasing people's demand for the latest wireless technologies beget spectrum scarcity and urge a need for more radio spectrum deployment. Spectrum has finite and limited frequencies. So user need to pay high amount for small portion of spectrum. Resource distribution is an important and difficult task in a wireless system. There is a need to utilize the available spectrum intelligently and efficiently. Wireless spectrum deployment is not an easy task. From decades, researchers are trying to improve the performance of wireless network in terms of cost, power consumption, availability, security, throughput, quality of service etc. Different technologies and methodologies have been proposed to cater the spectrum scarcity issues. It becomes difficult task in the presence of an attacker.

1.2 Benefits of CR Technology

The implementation of Cognitive radio technology in wireless network provides new paradigm to wireless technology. It makes the network self-reliant by reducing the power wastage, giving the capability to minimize the packet loss and increase the spectrum utilization. It allows the network to deal with the high degree of buffer management.

1.3 Motivation and Problem Statement

Secure and efficient network is the requisition of current users. The dynamic manner and open access philosophy in CRNs replenish unique vulnerabilities in the wireless spectrum band. SU want to utilize the spectrum band efficiently in the absence of PUs. In the contention over the vacant spectrum, SU does not have any methods to recognize that either the interruption observed on a band has done on purpose or unintentional. A secure and an efficient communication network should possess confidentiality, privacy, data integrity, authentication and service availability. In the presence of an attacker secure network features cannot be attained. There is a need to forge a mechanism for the secure and efficient communication over the CRN even in the presence of an attacker.

Heterogeneous wireless channels are available to SUs. This means each channel has different parameters e.g., bandwidth, signal to noise ratio, carrier frequency, delay spread etc. Each user tries to get maximum resources. So, every SU tries to get the higher quality channel. In the presence of Dos attack, wireless network compromise on the main security features i.e., service availability and data integrity.

Game theory provides adequate solution to access the spectrum band in the presence of attacker.

1.4 Objectives

The main objectives of research are as follow:

- Provide a secure communication network and maximize SU gain in the presence of an attacker
- To represent the interactions among attacker and defender as a game
- Mathematically analyze the network condition in the presence of Dos Attack

- Find the efficient ways to maximize the system throughput in the presence of an attacker.

1.5 Thesis Contribution

The main contributions of this research work are as follows:

- We propose a game-theoretic framework for developing choices of SU to select heterogeneous channels.
- Zero Sum game has been proposed to model the scenario because attacker and SU both are competing for same wireless resources. So the gain of one player results in the loss of other player.
- Channel utilities have modeled in terms of positive and negative payoffs
- We have proposed an optimize solution for cognitive user
- Linear programming algorithm has been utilized to find the mixed strategy Nash Equilibria
- Analysis and simulation results show that the acquired CRN strategies can provide adequate performance.

1.6 Thesis Organization

The thesis is structured as follows:

- Chapter 1 contains brief overview related to thesis introduction.
- Chapter 2 contains the literature reviewed in the thesis. The general working of CR networks.
- Chapter 3 contains security issues in the networks, different types of attacks and its countermeasures.
- Chapter 4 explains the basis of GT. Different types of GT and its application.
- Chapter 5 presents the system model and problem formulation. Proposed solution has been explained in detail in this chapter.
- Chapter 6 represents the simulation results. Different attacking and defending strategies present different results.
- Chapter 7 explains the conclusion and future work.

Chapter 2

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. Then its architecture design and functions has been explained.

2.2 Cognitive Radio Networks

Researchers and developers used the term "Cognition" which means "I know, perceive or to recognize". This word is used for the process of thinking. Mitola brought the "cognition" in wireless communication and introduced the phrase "Cognitive Radio" in 1999 [2]. Cognitive radios provide vicissitude to wireless engineering. Joseph Mitola presents the cognition cycle as:

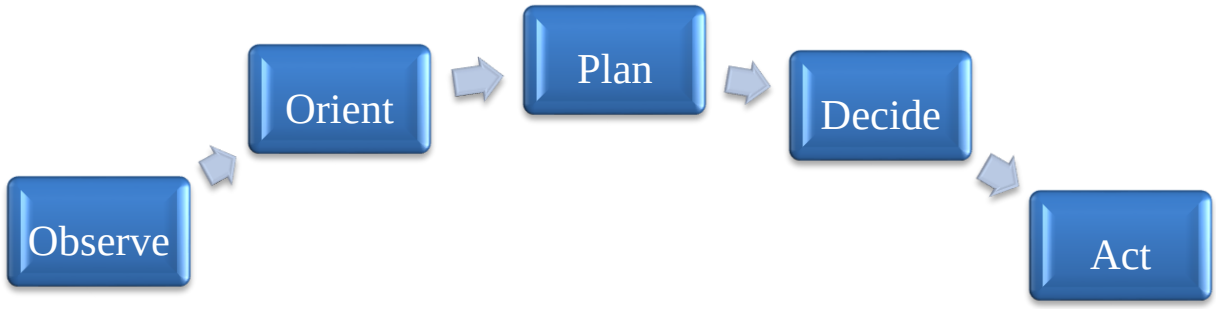

Figure 2.1: Cognition Cycle

Figure 2.1 represents the cognition cycle which explains the basic working model of CRN. CRs observe the environment and take decisions according to best available resources. CRNs is considered as a high potential technology which grant the promising solution for the scarcity of wireless spectrum bands by presenting the idea of efficient utilization of vacant spectrum bands. It aims to provide the efficient and secure communication anytime and anywhere needed by keeping the productive and effective use of radio spectrum. It allows the unlicensed user to temporary access the vacant licensed spectrum band without creating any interference to the legitimate PUs. Thus, we can summarize the objectives of CR in two points

- Potent communication at anywhere at anytime
- Efficient utilization of wireless spectrum

CRN becomes vulnerable to many security attacks due to its dynamic access and openness. Future CRs propose the compact devices having the nanotechnology feature. Large-scale deployment of CRNs is not an easy task. The new technology incorporate new hardware (Nano components incorporated) with SDR, MAC, SS, routing, policy definition, self-organizing, adaptive control mechanisms, learning and monitoring. The latest technology opens entirely new dimensions and challenges in wireless technology world. The Development and familiarization of recent technology needs suitable and strict security measures and policies. Therefore, security of cognitive wireless networks is a necessary task.

2.3 Cognitive Radio Network Architecture

The radios that use software to configure and modify the different parameters of radio network are knows as Software Defined Radio. This concept was first introduced by Joseph Mitola. Versatility is the most persuasive feature of the SDR. In radio communication system components are implemented in hardware like mixers, filters, amplifiers, modulators/demodulators, detectors, etc. While, SDR is a programmable radios in which radio communication systems and parameters are changed and programmed through software. SDR provides the basic platform for the deployment of cognitive radios. CR is an evolution of SDR. It is the combination of

- Cognitive engine
- SDR

CRs can perform functions without SDR, anyhow SDR provides more flexibility in performing different operations.

2.3.1 Cognitive Radio Engine

Cognitive engine is called as the brain of CR as it provides intelligent means for the efficient use of the spectrum. Intelligence is the silent feature of CR. It analyze the environment and then take decisions according to it. To build a cognitive engine, different methods and technologies such as artificial intelligence, neural networks, genetic algorithms and case-based reasoning have been discussed in [3]. In addition to this, cognitive engines based on incomplete information of channel states and environments, a multi-antenna system cognitive engine, and the robust training problem in cognitive engines have been widely studied and discussed. However, these researches were focused at particular applications with maximum related to link adaptation and WRM. Figure 2.2 represents the basic components of CR engine.

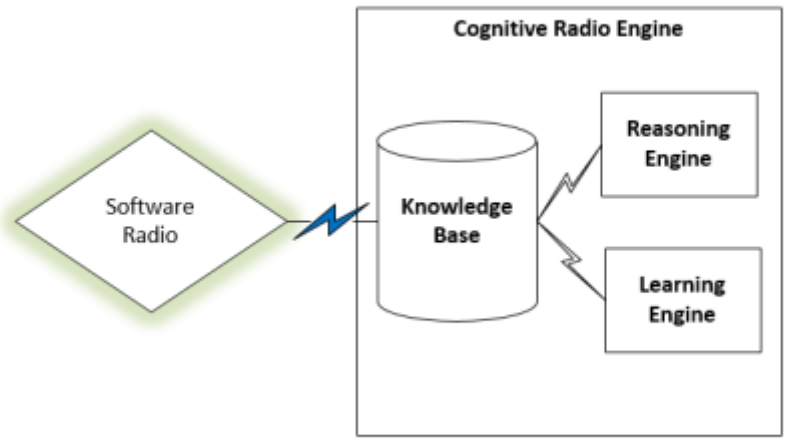

Figure 2.2: Cognitive Radio Engine

Cognitive engine contains

- Database
- Reasoning Engine
- Learning Engine

Figure 2.2 shows that database of cognitive engine stores important sensing information and maintain history about the spectrum. Reasoning engine gives logical support and assist in taking the decisions. If there are multiple vacant channels, the CE calls upon reasoning engine for selecting the maximum vacant bandwidth depending upon the knowledge base rules and policies. Hence, the transmission and communication rates can be increased by the system. The CE can configure radio system parameters like waveform modulation, protocol, coding rate, operating frequency, frame length and networking etc. Then learner comes and plays its role in learning new cases and develop new knowledge.

2.3.2 SDR

It is an exceptionally device use for wireless communications which can configure, typically capable of incorporating a multiple number of communications waveforms by processing graphs of different radio components.

SDR and CR system technologies together are expected to give flexibility, efficacy and provide adaptability to overall spectrum use. These technologies can be either combined or deployed

separately and can be implemented in systems of any radio communication service. Any wireless network which uses SDR or CR technologies should operate according to the provisions of the Radio Regulations.

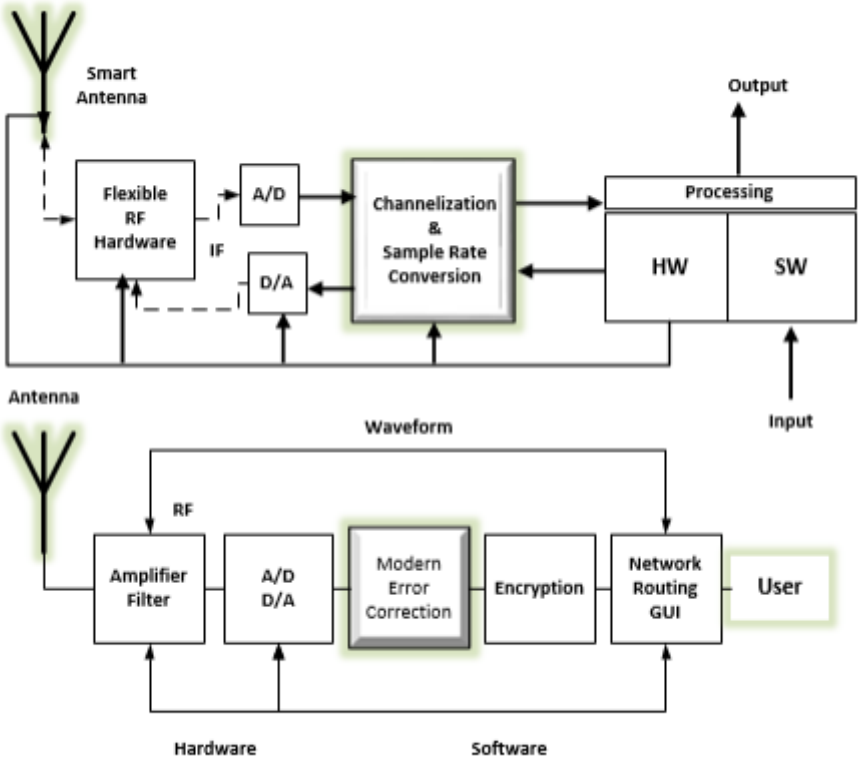

Figure 2.3: Software Define Radio

Figure 2.3 represents the basic structure of SDR. Figure 2.3 shows that SDR provides basic platform for the implementation of CRN. In SDR traditional components like mixers, filters, amplifiers etc. are replaced and operate by means of software.

2.4 Cognitive Radio Functions

CR is a smart radio technology characterized by the FCC as 'A radio that can change its transmitter parameters in light of collaboration with the surroundings in which it works. CR has two main characteristics

- cognitive capability
- re-configurability

2.4.1 Cognitive Capability

Observation is the first step for cognition in CRN for the execution of cognitive engine. CR capability means cognitive user sense the available spectrum and make decisions according to the spectrum capability, PU presence, traffic load, network congestion etc. This whole process is shown in figure 2.4. The Cognitive cycle works on five different junctures i.e., sensing, awareness, learning, adaptation and response, shown in figure 2.4. This is a continuous process in CRs.

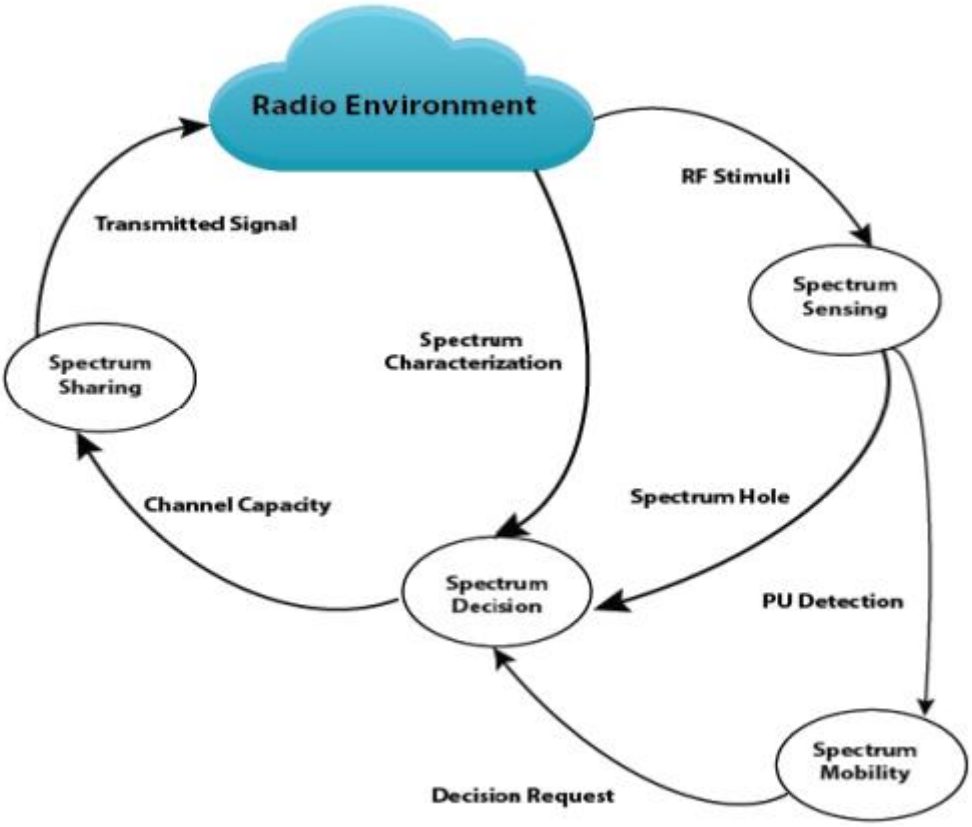

Figure 2.4: Cognitive Cycle

CRs first sense the environment, take the awareness about the spectrum availability, learn from the environment, monitors its own performance and change parameters accordingly. This whole process is also called as Dynamic Spectrum Management. Spectrum management choose the best available channel.

2.4.2 Reconfigurability

Reconfigurability means CR is such a tremendous technology which can change its parameters according to the environment in which it operates. It observes the environment and resources,

learn, make plans and adapt the changes. RF hardware has a capability to tune any portion of the frequency band.

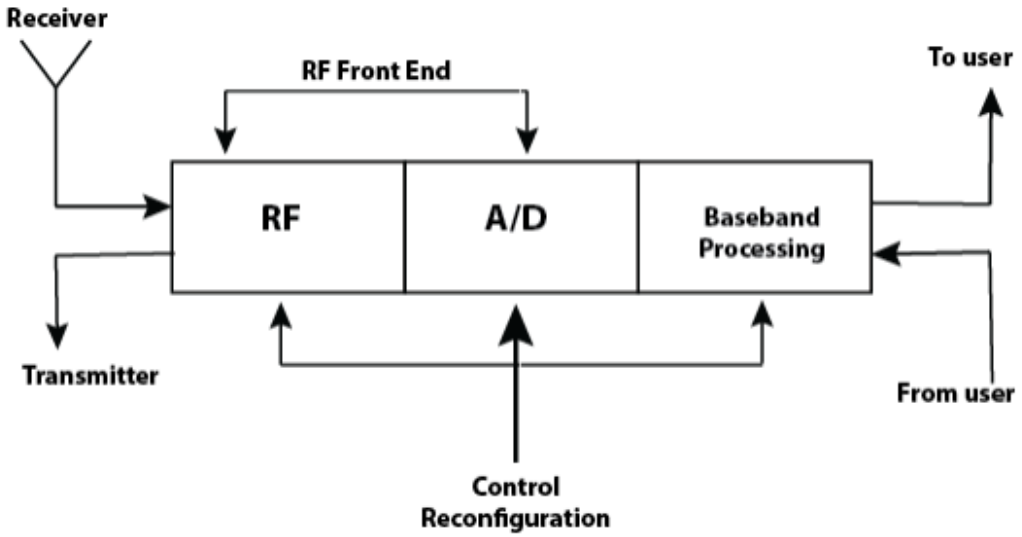

Figure 2.5: Cognitive Radio Transceiver

2.4.2.1 Adaptive Frequency Agility

CRN has the ability to change its frequency on which it operates depending upon the requirements. This method is useful to avoid transmission in occupied channels. This capacity more often than not consolidates with a strategy to progressively choose the suitable operating frequency according to the detected signals from different transmitters [4]. The change in frequency has been done to achieve various purposes like to mitigate jamming effects, to avoid interference to other users and to utilize wireless resources in a better way. Adaptive Frequency Agility is usually merged with Listen Before Talk (LBT) to make sure that signal should be transmitted in a free channel.

2.4.2.2 Adaptive Modulation/coding

Adaptive modulation is the feature that allow the radio system to modify the modulations scheme depending upon the specifications of the transmission channel and other output specifications of the user. These modulation techniques can modify transmission characteristics of a signal and waveforms patterns to give better opportunities for spectrum access and provide efficient use of spectrum while working around other users ‘signals that are present in the same environment. A CR choose the appropriate modulation type with a specific transmission system to allow interoperability between systems.

2.4.2.3 Transmit power control

Transmit power control enables a device to dynamically change between several transmission power levels during the data transmission process. It permits the transmission power at the acceptable limits when required but reduces the transmitter power to a minimum level to allow greater sharing of spectrum when higher power operation is not required.

2.5 Cognitive Radio Users

There are two types of users present in CRN. These users are termed as

- Primary User
- Secondary User

The licensed user is a PU who is considered as legitimate user. It has priority over SU to use the wireless spectrum bands. A SU has lower priority than PU.

2.6 Cognitive Radio Network Types

CRN can be divided into two types depending upon infrastructure classification

2.6.1 Centralized Cognitive Network

In Centralized CRN, whole network is divided into different cells. figure 2.6 represents the centralized CRN. In figure each cell is controlled and managed by a secondary base station. SU and medium access is managed by these secondary base stations. SU are synchronized with these base stations. SUs perform spectrum sensing and send reports to these base stations.

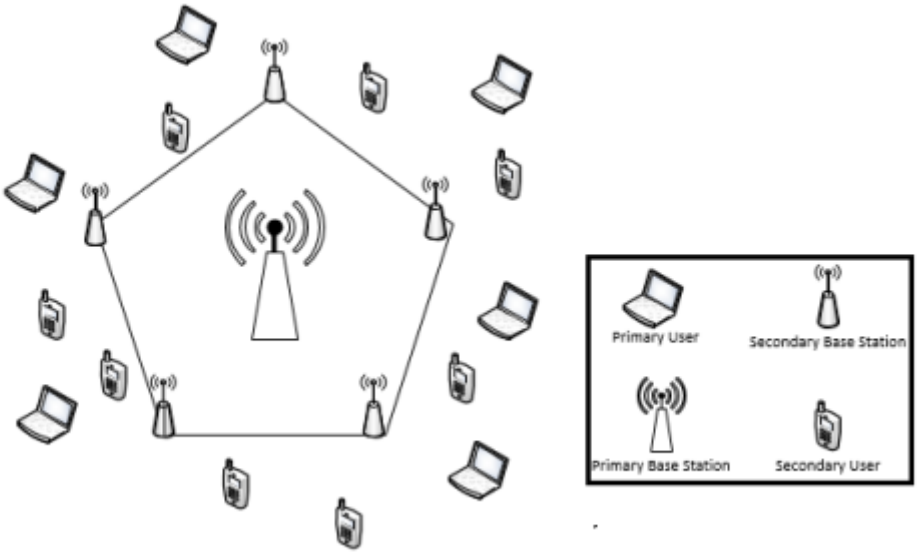

Figure 2.6: Centralized Cognitive Radio Network

2.6.2 Decentralized Cognitive Network

Figure 2.7 represents the decentralized CRN. In decentralized networks, SUs communicate with each other without any central entity collaboration. Secondary nodes either communicate directly if they are present in the vicinity of each other or use multiple hops to send information if the receiving node is present out of the communication range. Due to the lack of infrastructure and centralized station, these networks are also termed as ad-hoc networks. SUs take decision either on the bases of personal observation or by using different collaborative schemes.

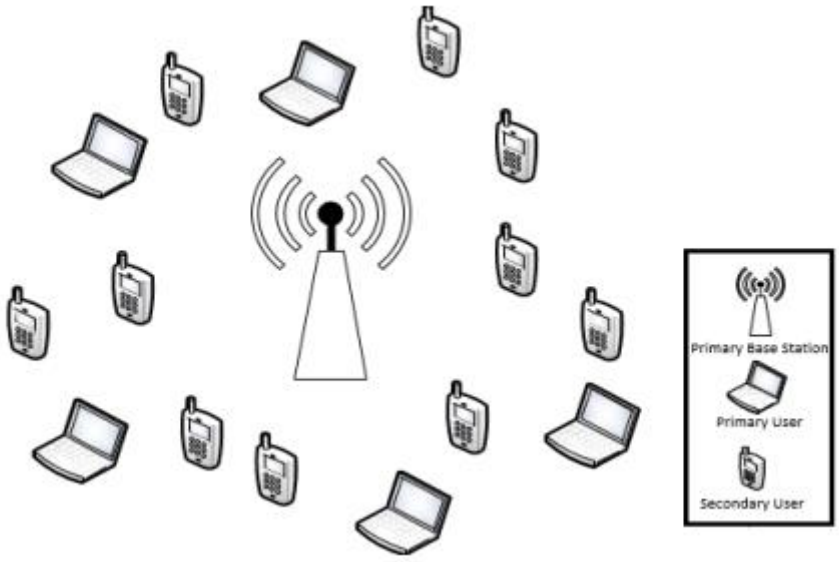

Figure 2.7: Decentralized Cognitive Radio Network

2.7 Conclusion

In this chapter, literature reviewed related to CRN was covered. The architecture design and working of CR networks was presented in detail in this chapter.

Chapter 3

ATTACKS ON COGNITIVE RADIO NETWORKS & COUNTERMEASURES

3.1 Introduction

Cognitive network implementation opens new challenges and security threats. In this chapter we will give detailed overview related to security threats of CRN. All functionalities of CRN such as spectrum sensing, spectrum management, and spectrum sharing and spectrum mobility are potentially vulnerable to attack [5]. The normal working of CRN can be destroyed and muddled by the malicious attackers when they send the reverse report of their observations (i.e., reduce the protection of PUs or degrade spectrum usage performance). While, attackers with rapacious or selfish purpose may report the PU activity correctly to get exclusive access of the wireless spectrum. Both malicious and greedy attackers have the similar aims of creating DoS attacks to SU [6]. In Figure 3.1, we encapsulate the major objectives of attackers against normal CR operations.

Motivations	Attack Goals	Attack Strategy	Attack Consequences
Greedy	Maximize the communication performance of the attacker	Make the SUs believe that spectrum is busy by Inducing false alarms	A decrease in spectrum usage
Malicious	Disrupt the performance of PUs and SUs	Make the SUs believe that vacant portion of spectrum is busy	A decrease in spectrum usage efficiency and degrade SUs' performance.
		Make SUs to believe that busy portion of spectrum is vacant	A decrease in protection of the PUs against interference caused by SUs transmission

Figure 3.1: Attacks Characterization

There are different types of attacks targeting the weaknesses on different layers of wireless network. These attacks are categorized on the basis of different layers on which they attack. Attacks which target the physical layer, come under the category of physical layer attacks. Same is the case with the other layers. Various securing methods have been proposed to mitigate the attacks on different layers [7].

3.2 Physical Layer Attacks & its Countermeasures

Physical layer carry out Spectrum sensing, Channel estimation and data transmission. Spectrum sensing is done to find the vacant channels for the smooth transmission of data without creating any interference to the PUs. Channel estimation has been done after spectrum sensing to estimate the channel quality. The data is transferred on the vacant channel which is estimated with the best quality. The security on higher layers have been done by using different authentication and encrypted methods. This layer is vulnerable to various attacks. Attackers launch many attacks on each layer of wireless network but they commonly attacks more on physical layer. At the physical layer primary user emulation attack (PUE), learning attack, eavesdropping attack, objective function attacks can occur. All these attacks have their own hindrance objectives and consequences [8].

3.2.1 Primary User Emulation Attack (PUE)

In this type of an attack, malicious user emulate the sensing report. An attacker mimics the PU behavior and sends the transmission signals in the licensed spectrum band to achieve the priority during spectrum sensing period. PUE attack is shown in figure 3.2 .This creates problem during spectrum sensing by SU and make it realize the presence of PU, so SU vacates the channel due to wrong sensing report. As SU always give priority to PU so wrong sensing report leads to spectrum wastage. Because of PUEA, In spite of the fact that spectrum is not utilize, SU is unable to utilize the vacant spectrum. The goal of an attacker is to stop legitimate SU from using spectrum band. It does not create any interference to PUs.

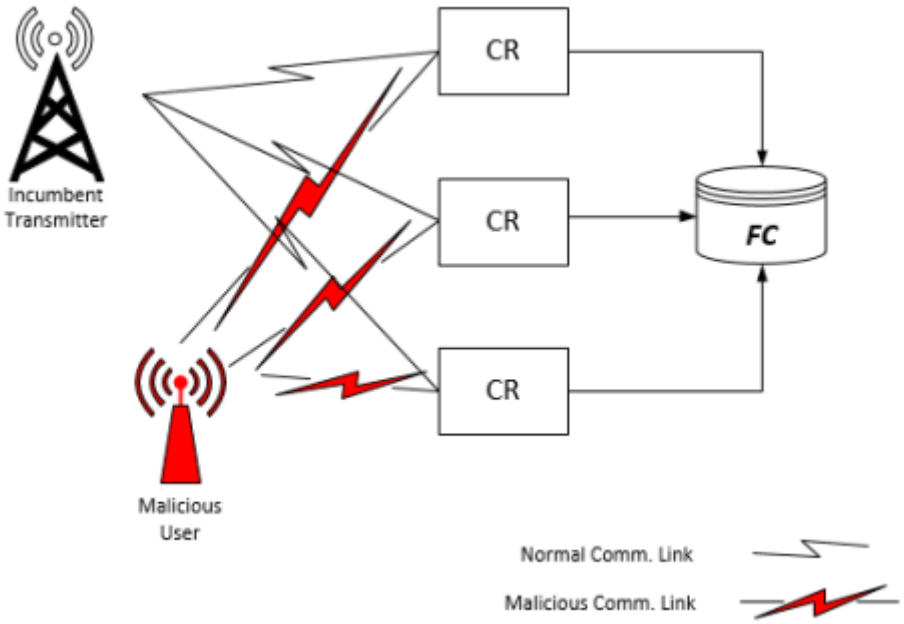

Figure 3.2: Primary User Emulation Attack

Figure 3.2 shows that when a selfish attacker finds any vacant spectrum, it prevents SU from using that vacant band by imitating the signal characteristics of PU. Depending upon the aim of the attacker, a PU emulation attack can be categorized as "Selfish PUE Attack" and "Malicious PUE Attack".

- **Selfish PUEA**: Attacker wishes to maximize its own spectrum usage and occupy the band, make it busy for others users.
- **Malicious PUEA**: Attacker creates hindrance for SU and does not allow others to use vacant spectrum bands .In this way spectrum resources go waste.

PUEA can be divided into three different categories depend upon the consequences achieve by an attacker.

- **Denial PUEA**: An attacker emits counterfeit signals in the absence of PUs. Thus making other users to believe the presence of PU. This is a short term attack, where the radios are denied immediate use of the available channels.
- **Induce PUEA**: A malicious user present in the locality of a secondary can mask the primary signal by increasing the noise. It may also transmit a low power masking signals if close to the SU to create interference. With a higher noise floor i.e., less Signal to Noise Ratio (SNR), a SU will mistakenly assume that a PU is not present and try to

use the spectrum. This is a violation of spectrum regulations because it creates interference in the transmission of PU. As a result of it the radio may be banned.

- **Coordinated PUEA**: In a coordinated manner multiple intruder node launch attacks on different multiple channels simultaneously to muddle as many networks nodes as possible. After detecting the current channel to be occupied, the secondary will try to choose another from the set of vacant channels. Even after switching the SU is unable to find a suitable channel if multiple vacant channels are being attacked. In the context of ontological CRs, such coordinated PUEA attacks on candidate channels will degenerate the learning phase by associating a few channels to be statistically non-usable. Although, in reality, the spectrum may be available, the radios will be reluctant to use the candidate channels after a few learning periods, thus limiting their learning capabilities.

Proposed Solution for PUEA can be categorized according to different mitigation approaches

- Reputation based approach
- Data mining based approach
- Artificial Intelligence based approach

In Reputation type of approach suspicion levels are assign to cognitive nodes. The node is marked as malicious if mistrust level of any node is greater from specific threshold level. This reputation-based method needs threshold values so to fulfill that requirement base station should have the previous knowledge about the attacker behavior to set the threshold values. Without prior knowledge base station cannot detect the malicious node. Researchers provided many passive approaches to strategically defend against PUE attack [14]. A dogfight in spectrum has been explained in [15] to present the defense mechanism against the PU emulation attack. Authors have considered the case of two opponents i.e., one is SU (defender) and other one is an attacker. Both fight for the vacant spectrum band. When the channel statistics are unknown to both the defender and attacker, the dogfight game is blind. The blind dogfight with complete and partial information about the different channels status has been presented by the authors. The channels' rewards are being analyzed in this paper.

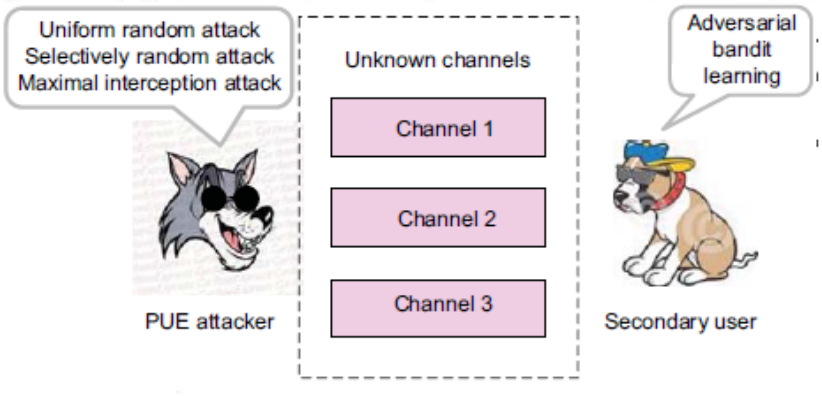

Figure 3.3: Blind Dog Fight in Spectrum

A Bayesian game has been formulated to analyze the emulation attacks in DSA [16]. A proactive detection scheme has been proposed in [17] to detect PUE attacks. A PUE attack in CRN has been defended by Differential game technique in [3].

3.2.2 Jamming Attack

Jamming attack occurs on physical and Mac layers. It is the simplest way to disrupt the wireless transmission. The purpose of jamming attack is to stop the legitimate user from using spectrum bands. It is one of the worst attacks in CRs. In jamming attacks, an attacker send the data packets on different channels and obstruct the legitimate user from using spectrum band. Jamming can be done by using one jammer or by the coordination of multiple jammers. There are two main goals of jamming. First is to prevent the communications of secondary and PU. Second is to stop the SU from using vacant bands.

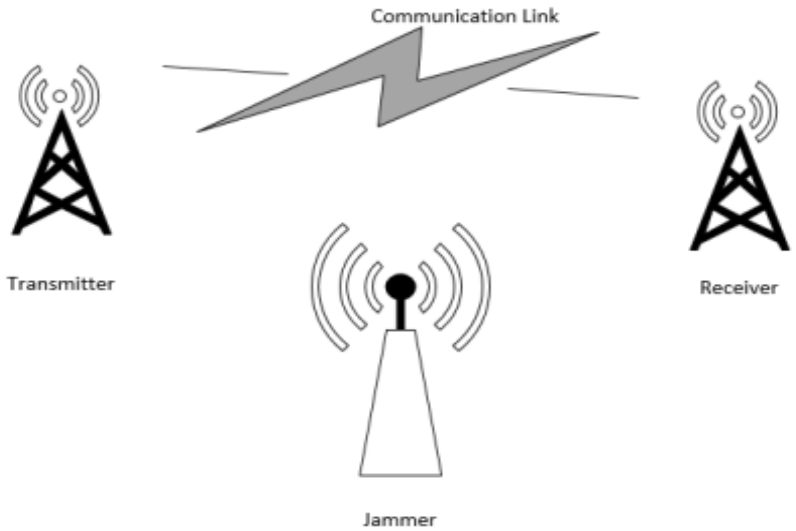

Figure 3.4: Jammer prevents transmission between TX & RX

In figure 3.4, jamming can cause network degradation which sometimes results in DoS scenario. The condition becomes more unfavorable when attackers jam dedicated channels. There are several types of jammers. Static jammer, Deception Jammer, Random jammer and Reactive Jammer are few of them. Static jammers continuously send jamming signals to jam a specific channel. Random jammer jams the channels on different time intervals. The jamming techniques may be categorized into three different types [9]

- **Broad Band attack**: A broad band attack attempts to jam the whole spectrum, thus it utilizes the most energy to jam the entire spectrum
- **Partial Band attack**: A partial band attack only interrupt a portion of the radio frequency's channel
- **Narrow Band attack**: A narrow band attack only jam the specific frequency of the band

The exchange of security keys between the nodes can create common control problems. The confidentiality and integrity of the transactions can be provided by the authentication among the nodes. By using the cloud application we can reduce or eliminate the jamming problem, hidden terminal problem, exchange of keys between the nodes and malicious user acts. The security to cloud still remains an open problem. In [18] , authors concluded that anti jamming is a crucial task. To mitigate the jamming attacks, CRN needs to use more channels and improve sensing capability of PU.

According to authors view, Channel hopping may not be the secure solution to mitigate intelligent jamming attacks. Reliability of Control channels cannot be fully guaranteed in adhoc CRNs [19]. They have presented a jamming resilient Control Channel (JRCC) game to show the interactions between SU and attacker. Control channel allocation with variable learning rates can be done by using JRCC algorithm in a competitive environment. This is a scalable algorithm which can be applied to multiple users.

In literature lots of work has been done to mitigate jamming Attacks. CR devices continuously looking for vacant spectrum bands due to which they reconfigure their parameter such as frequency, routing protocols, multiple times. Due to this dynamic nature of CR, fixed strategy jammer may not be effective for long period of time. So Attackers try to change their strategy to gain the maximum success by jamming different channels according to CR behavior. These types of jammers are known as cognitive jammer who change their parameters and adapt the best attacking strategy. A novel and efficient solution has been proposed in [20] to mitigate

such jamming effects. Distributed algorithms that are powerful against malicious behavior (jamming attack) has been proposed in [21]. Coordinated and uncoordinated jamming attacks has been considered. In a coordinated jamming attacks, jammers coordinate to attack on non-overlapping channels to maximize their gain. Different algorithms such as

- **CDJ** (Coordination in presence of Distinguishable Jammers), when jammers cooperate with each other and SUs can identify jammers.
- **CNJ** (Coordination in presence of Non-distinguishable Jammers), in the presence cooperative jammers when SU cannot identify correctly that whether collision is due to the presence of jammer or SU.
- **CUJ** (Co-ordination in presence of uncoordinated and non-distinguishable jammers), when jammers do not cooperate.

These algorithms have been proposed to achieve high confidence with constant regret. The proposed algorithms decrease the regret in a multi-player attackers. Regret is known as the difference between best achievable aggregate throughput when all the SUs cooperate with prior knowledge of network parameters and aggregate throughput achieved when they do not have any prior knowledge. Prior knowledge of network includes channel statistic, number of SUs and number of jammers etc.

Authors gave a realistic Universal Software Radio Peripheral (USRP) based experimental setup and evince the effectiveness of algorithms. In centralized system various algorithms have been proposed considering the Dynamic Spectrum Access in the presence of jammers [22]. The common observation is that the conventional jamming avoidance techniques such as frequency hopping or direct sequence spread spectrum may not be fruitful and efficient in CR Networks, as they require control channel link between SU's transmitter and receiver. In addition, the channels over which SU transmits its data may change dynamically with time. The novel Jammer Inference-based Jamming Defense (jDefender) algorithm in [23] identifies the SU acting as jammers based on their channel access information. However, the channel allocation must be done using the central database and it is not possible in the decentralized network.

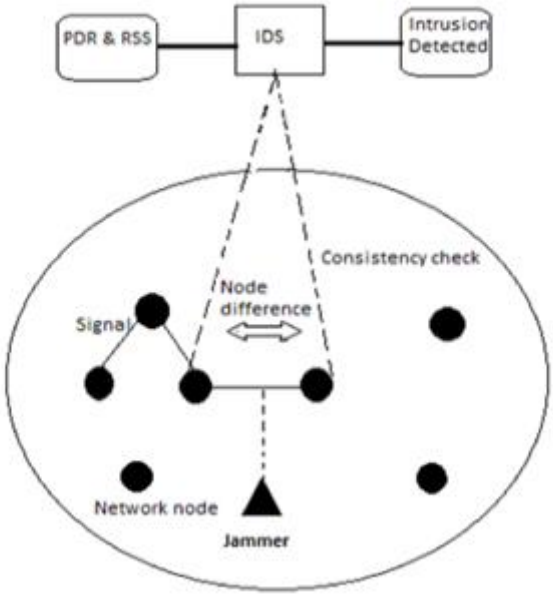

Figure 3.5: Consistency Check to defend Jamming Attack

The Intrusion Detection System (IDS) of consistency checks provides the defending mechanism against jamming attacks. Figure 3.5 shows the IDS performing consistency checks to recognize possible jamming attacks within the network. Theoretically, the node can be jammed when PDR is low and the node distance is small. The node has become victim to a network failure when there exists a low PDR and the large node distance [9].

3.2.3 Eavesdropping

Malicious user hark/intercept the transmission of legitimate user. In this type of attack, an attacker becomes passive. It does not directly affect the performance of cognitive network. Attacker just collects the information about the available channel which provides assistance and basis to achieve other attack's purposes.

3.2.4 Learning Attack

In learning attack, attacker tries to provide false sensing report to the learning radio. If a learning radio acquire wrong objective about the transmission scheme, radio use it all the ways till to the learning of correct ideas. Several methods have been proposed to mitigate the learning attack [24].Over the period of time learning results should be evaluated. Another way to avoid learning attack is to form a group of SUs. The purpose of making a group is to learn the environment by SUs collectively. It makes difficult for an attacker to launch a learning attack.

3.2.5 Objective Function Attack

In this type of attack, an attacker deliberately modify data to restrain CR from adapting changes. CRN has unique feature which provides the capability to sense the environment and change the radio parameters (i.e., power, bandwidth, center frequency, modulation type, data rate, frame size, routing protocols etc.), according to the situation. The three basic goals of wireless communication is high data rate, low energy consumption and secure communication. Cognitive engine controls different radio parameters and manipulate the objective function by using different input parameters. After calculation it observes which combination of input parameters gives better results so that with minimum power usage it can maximize its data rate. The purpose of learning attack is to exploit feature of CRs. An attacker launch objective function attack at the time of calculation of parameters to manipulate the calculated results. In this way attacker can transmute the results to make the situation favorable in his interest and restrict CR to use low security level, so that attacker can easily hack the system. An attacker may launch jamming attack to decrease the overall objective function, whenever a cognitive engine tries to use high security level. So cognitive engine tries to use low security level in order to achieve high objective function. This type of attack puts great impact on on-line learning radios and do not affect the off-line learning radios.

There are not very effective methods to safe guard CRs from the objective function attack. The simple proposed solution to avoid such attack is to set the threshold values for different radio parameters. If parameters show any significant deviation from the threshold values then avoid the communication [8].

3.3 Link Layer Attacks & its Countermeasures

The data link layer is the second layer of the OSI-model, responsible for transferring the data between adjacent nodes of a network. It provides the functional and procedural ways to transmit the data between network nodes on a point to point link. It is responsible for the local transmission of data transmission among devices on the same local area network. “Logical Link Control (LLC)” and “Media Access Control (MAC)” are the two sublayers of data link layer. In a CCRN, every CR node senses the spectrum band repeatedly and sends the measuring results to the Fusion center. After collecting the data, FC takes the final decision about the presence and absence of the legitimate user. FC does not consider the presence of malicious entity,who can manipulate the report, while taking the decision and assume that all the reports

sending by the legitimate users are honest. This assumption can make CRN vulnerable to several attacks by malicious entities.

3.3.1 Denial of Service Attack

DoS attack is one of the worst attacks in CRs and wireless network. CRN is exposed to such attacks due to its openness and dynamic nature of access. In this type of attack attackers prevent the legitimate user from accessing spectrum band by reducing the Channel utilization and by copying the MAC control frames. Attackers make the frequency channels inaccessible to legitimate users and it can affect multiple hops of CRN.

3.3.2 Channel Jamming Attack

Control channels expedite the communication among CR users. Attacker finds it the most effective and powerful method to destroy the whole network system by just causing a single point failure in a network. The purpose of jamming with common control channel is to insert a powerful signal in the control channel, due to which receivers are unable to receive the authentic control messages results in whole network degradation. To avoid the control channel jamming attacks, researchers made it possible to avoid the Common control channel for the exchange of control messages among the SUs. In [25] the authors use a different mode of operation of the SUs in order to prevent the requirement of using a dedicated Common Control Channel. They proposed a Tunable Transmitter - Fixed Receiver (TT-FR) mod, which allows the SUs to send data on any channel, but confine them to receive only on one fixed channel which is known to all their neighbors. Since all SUs know about the channel use for control messages transmission to another user, there is no need for a dedicated control channel. The purpose of this work is to find the TT-FR allocation that accommodate the maximum number of SUs. This approach is vulnerable to the hidden node and deafness problems and may decrease the level of connectivity because of the availibility of limited channels. Furthermore, the use of only one receiving channel bournes the maximum performance of the SUs and the network as a whole. In [26], S. Debroy and M. Chatterjee speculate that the SUs interchange control messages in the vacant channels and propose a heuristic method for the channel allocation. All channels are available for transmission, which in results maximize the channel utility and increase the overall throughput of the network.

3.3.3 Byzantine Attack

In SSDF attack, attacker modify spectrum sensing data report which cause a SU to take wrong

decisions. Figure 3.6 represents the SSDF attack. In this type of attack, an attacker represent the false information in the sensing report. It shows the vacant spectrum is occupied by the PU to willingly waste the spectrum resources and it shows the vacant band by hiding the presence of PU to create collision among the legitimate user/PU and SU. So during free time slot cognitive user is unable to use the spectrum due to this attack.

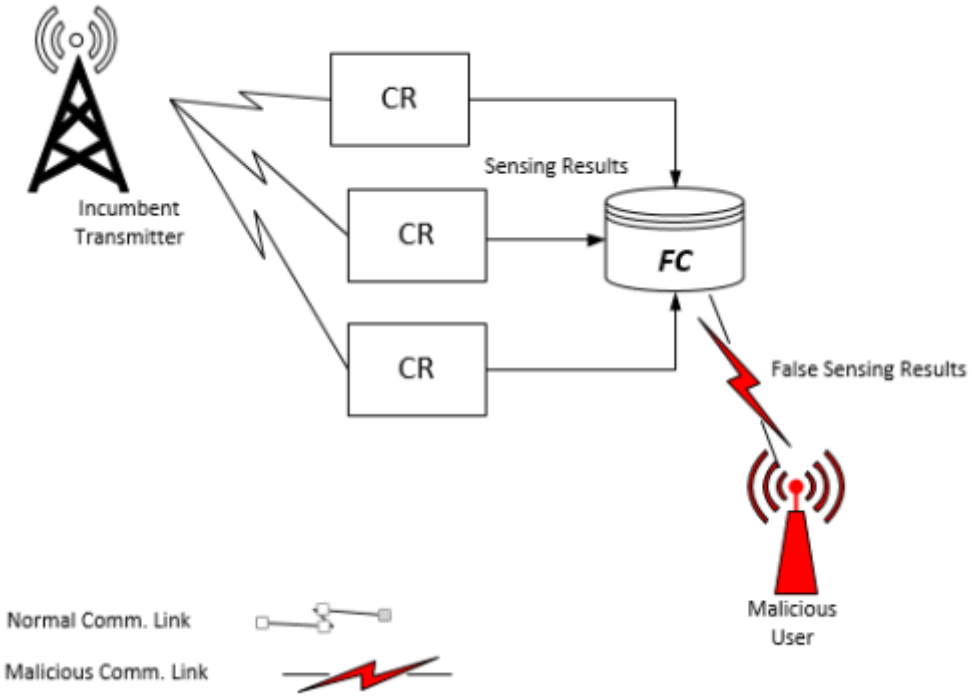

Figure 3.6: Byzantine Attack

So, attacker basically reverse the original sensing report in Byzantine attack. Thus, inducing incorrect decisions by SUs for spectral usage. This attack may come under the category of decision attack, as it destroys the decision process of a SU. Byzantine attack can be launched in three different categories:

- **Denial SSDF Attack**: An attacker declares vacant spectrum band (advertise 0) as occupied band (advertise 1) making legitimate user to believe the presence of PU. In this way spectrum resources go waste because SU interpret it as occupied spectrum band, which limits the channel access and make SU unable to use it according to the spectrum assignment policies. This is a short term attack.
- **Induce SSDF Attack**: An attacker divulges occupied spectrum band (advertise 1) as vacant (advertise 0) spectrum band. This can cause interference to PU.Because SU

assume it as vacant band and try to access that vacant band. Repeated interference to PUs may cause temporary and permanent expel of cognitive user from the CRN. This is a long term attack.

- **Sybil SSDF Attack**: The nodes having multiple unique fake identities are termed a Sybil nodes. These counterfeit nodes induce false report about channel state which leads to wrong decisions by legitimate cognitive users. This type of attack imposture the presence of sensing nodes, while in reality there are no such nodes exists thus creating an obscure situation for a legitimate user. A counterfeit Sybil node can countermand the honest and legitimate cognitive users and thus reduce the channel utilization for cognitive user and degrade the network performance. In [27], researchers presented a method to recognize the Byzantines. They have proposed to learn the behavior of attackers and estimate the false alarm probabilities and detection. They used probabilities to design the fusion rule. With time which converge to their true values of probabilities. Repetitive Trust Management (RTM) and Adversary detection methods have been proposed in [28] to counter the byzantine attack in Delay Tolerant Networks. In [29], researchers suggest a simple and robust secure cooperative spectrum sensing scheme combining hard decision for Opportunistic Spectrum Access (OSA) networks. Based on the previous sensing data records and the assistance of trusted OSA nodes, the proposed method efficaciously alleviate spectrum sensing data falsification attacks by prohibiting misbehaving OSA nodes from the process of cooperation. Weighted combining methods were proposed to decrease the possible impact from data falsification in cooperative spectrum sensing.

3.4 Network Layer Attacks & its Countermeasures

Network layer involves the transmission of data packets from source to destination, when both source and destination are present on different networks. The routing of data packets becomes more complicated in the case of CRs due to the requirement of immediate depart of SU to vacate channel on the arrival of PU.

3.4.1 Sinkhole Attack

In a Sinkhole Attack, an attacker node proclaims itself as having the best and shortest route to a particular destination. An attacker exploits the characteristics of multi hop routing in CRN by advertising itself as a best routing node to attract a network traffic. It forms a trust base to

launch the attack. It usually use high power to send received packets directly to the base station, showing it as a single hop from the base station[10].

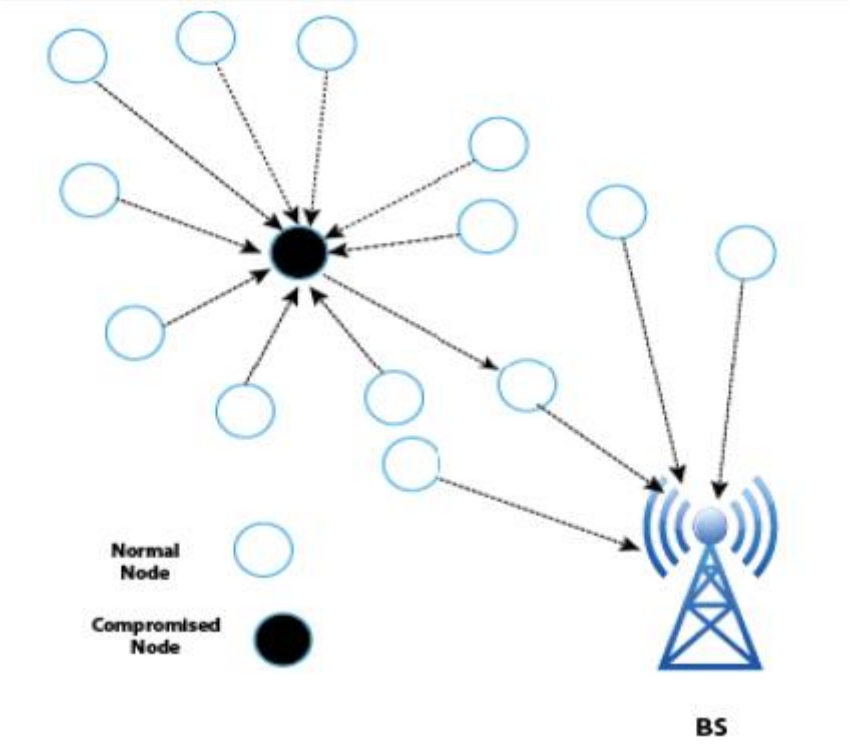

Figure 3.7: Sink Hole Attack

Sinkhole attack is used to launch others types of attacks such as selective forwarding attack, acknowledge spoofing attack etc. Usually mesh and infrastructure based architectures are degraded by such type of attack. Attacker receives all packets after advertising it as a best route and then do selective forwarding attack. The selective forwarding attack by an attacker can be carried out by forwarding, dropping, or modifying received packets from particular nodes [11]. Link layer authentication and encryption are used to avoid sinkhole attack from outside the network. It becomes difficult for an attacker to come in the network due to proper authentication mechanism. Hence attacker becomes helpless to launch sink hole attack [13]. Geographic routing protocols have been proposed to tackle this type of attack [30].

3.4.2 Sybil Attack

An attacker produce large number of feigned identities and sends packets to destroy the trust system of CRN. In a cognitive network where SUs hankering for vacant channels, intruder makes fictitious identities and try to get vacant spectrum bands. In this way they reduce the vacant spectrum availibility for legitimate SUs.

3.4.3 Hello Flood Attack

Malicious attacker broadcasts the message to all nodes of the CRN. It broadcasts the message with such a high power that the receiving nodes believe that broadcast message is send by their neighboring node. And in reality it is not present in their neighbor and may locate at a greater distance. Attacker sends packets to the network nodes, make them believe that it is their nearest neighboring node and can be used it for data transmission. So, because of false assumption of neighboring node even the far off node send their data packets to intruder node to transmit it to specific destination. Since all network nodes transmit their packets towards intruder node. So nodes may find themselves with no neighbors to forward packets and hence packets sent from the network nodes would be lost. Hello flood attack can be defended by using verification methods to check the bi-directionality of links before making routing links.

3.4.4 Ripple Attack

This type of attack is identical to PUE attack. Attacker exploits the dynamic nature of CRs. SU switch between different channels during communication to vacate the channel on the arrival of PU. Attackers take the advantage of this channel mobility and route the false information about hoping and due to which other nodes switch their channels. In this type of attack, intruder spread false information hop by hop and create an uncertainty and addle situation in a network [12].

3.4.5 Wormhole Attack

In this attack, an attacker gets packet from one portion of the network and sends them to another location with low latency rate and replays them into the CRN. FCC disallow any modification to PU. A wormhole attack is carried out by multiple hopes nodes, i.e., usually present at a distance of one or two hops from base station and nearer to the attacker. This type of attack may bring about the division of network. [12] .This network division results in the route disclosure which can provide information about CRN and accord assistance to carry out other attacks [13]. Researchers presented the efficient solution for reply and wormhole attack in [31]. They have introduced an authentication scheme to provide secure verification of the spectrum information.

3.5 Conclusion

In this chapter, literature reviewed in the research was discussed. Security issues of the CRN i.e., different attacks and its countermeasures on networks were discussed in detail.

Chapter 4

GAME THEORY

4.1 Introduction

This chapter covers the basic knowledge of game theory and related work .Ronald Fisher used game theoretic methods to study animal behavior in 1930's. His work precede the name "game theory" and laid its foundation. Later, it was applied in economics. John Maynard Smith gave its wide application in biology and presented his book Evolution and the Theory of Games. John Maynard Smith's concept of evolutionary stable system is important at whatever point the best thing for a creature or plant to do relies upon what others are doing. So, Game theory was developed broadly in the 1950s by many scholars.

Game theory was later applied to biology in the 1970s, although similar developments go back at least as far as the 1930s. Game theory is the branch of applied mathematics which has wide range applications in economics, political science, psychology, evolutionary biology, philosophy and in computer science. The mathematicians John von Neumann and John Nash revolutionized the field of economics by putting the foundation of GT. Psychologists name the theory of social situations, which economics call as game theory. It provides strategic decisions in case of competitive situations. GT has become an umbrella term due to its wide rang applications and behavioral relations.

4.2 Game theory Elements

The application of GT needs following particulars:

- Player
- Strategy
- Payoff

4.2.1 Player

A participant who takes decisions during game is termed as player.

4.2.2 Strategy

A decision which player takes is called as strategy.

The basic principle or significance of a game is the interdependence of player strategies. There are two different types of strategic interdependence:

- sequential
- simultaneous

In the sequential strategies the players move in sequence, each player has knowledge about the other player's previous actions. Players anticipate future decisions after analyzing previous outcomes. While in the simultaneous moves the players take decisions and act at the same time, ignoring others actions. In this type of actions, each player must be aware that there are other players who have similar knowledge. So they are also selects strategy which gives best result. The strategies can also be classified into following five categories on the basis of the outcome. These strategies are represented in figure 4.1.

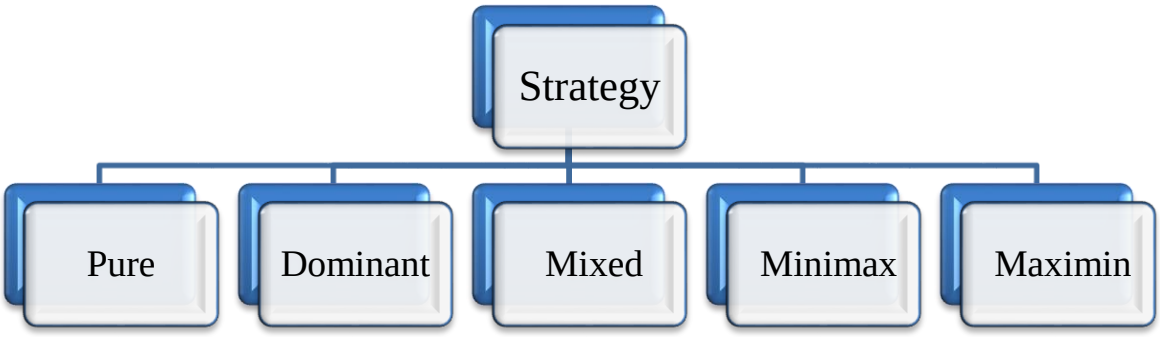

Figure 4.1: Classification of Strategy.

4.2.2.1 Pure Strategy

A pure strategy provides a complete definition of how a player will play a game. In particular, it determines the move a player will make for any situation he or she could face. A player's strategy set is the set of pure strategies available to that player.

4.2.2.2 Dominant Strategy

A strategy which pays best payoff to the player regardless of what strategy other player choose is termed as dominant strategy.

4.2.2.3 Mixed Strategy

Players randomize by certain probabilities over a set of deterministic strategies. Players randomly select pure strategy and assign certain probability to it.

4.2.2.4 Minimax Strategy

In this type of strategy players try to minimize their maximum loss.

4.2.2.5 Maximin Strategy

In this strategy players try to maximize their minimum gain.

4.2.3 Payoff

The outcome or result obtains by a player after applying specific strategy.

Game theory is defined as the process of demonstrating the logical interactions among players in competitive environment and which provides the suitable outcomes. It is the study of conflict and cooperation among players. It provides the mathematical tool for modeling the competition among the opposite players.

4.3 Game Theory Types

GT provides solution for different types of problems. There are several types of games. Some are cooperative games and some are non-cooperative games. Figure 4.2 shows different types of game.

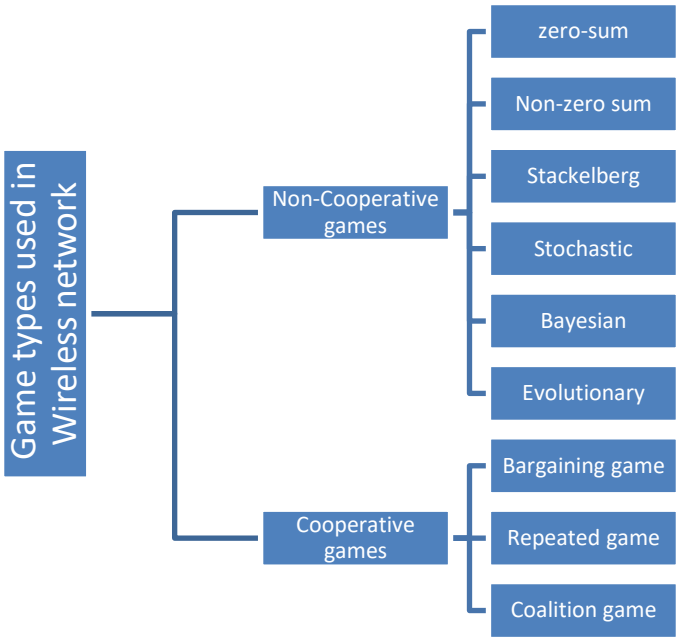

Figure 4.2: Types of game

4.3.1 Non-Cooperative Games

There is no element of cooperation among players in non-cooperative games. This type of games deals with the competitive situations where players have conflicting goals and there is no negotiation or deal among players.

4.3.1.1 Zero Sum Game

The concept of GT is used to analyze the interactions among cognitive users. Zero sum game is the type of non-cooperative game which typify the game of pure conflict and perfect competition. In zero-sum game, the payoff of one player is the negative payoff of another player, which means the gain of one player is equal to the loss of other player. So, the net sum equal to zero.

If one player endeavors to maximize its gain, then the other player tries to minimize its loss. Payoff sum for both players would be equal to zero. Mathematically it is expressed in equation 1.

$$U(A_i, B_j) = 0 \quad \forall (i.j) \in N \tag{1}$$

$$\boldsymbol{U(A_i, B_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} (\alpha_{ij}, \beta_{ij})} \quad \forall (i,j) \in N \tag{2}$$

We can represent the payoffs of the zero-sum game in a form of payoff matrix. This is shown in figure 4.3.

B_j / A_i	B_1	B_2	B_3	…	B_n
A_1	α_{11}, β_{11}	α_{12}, β_{12}	α_{13}, β_{13}	…	α_{1n}, β_{1n}
A_2	α_{21}, β_{21}	α_{22}, β_{22}	α_{23}, β_{23}	…	α_{2n}, β_{2n}
A_3	α_{31}, β_{31}	α_{32}, β_{32}	α_{33}, β_{33}	…	α_{3n}, β_{3n}
⋮	…	…	…	…	…
A_m	α_{m1}, β_{m1}	α_{m2}, β_{m2}	α_{m3}, β_{m3}	…	α_{mn}, β_{mn}

Figure 4.3: Payoff Matrix

A row player has set of strategies,$Ai = [A1, A2, \dots, Am]$, where $i = 1,2,3, \dots, m$, which represents the channel selected by an attacker.

A column player has set of strategies, $Bj = [B1, B2, \dots Bn]$, where $j = 1,2,3, \dots n$,these strategies represent the channel selected by a user.

SU and an attacker act as players. We assume that SU and attacker have an equal opportunity to access the vacant channel. Both select channel simultaneously and they can access only one channel at a time. Attacker and SU both have equal number of available channels, i.e., $m = n = C$. Which means they both have equal number strategies available. The payoff of a row player and a column player is represented as αij and βij respectively. According to zero sum game the gain of one player is equal to the loss of another player. Sum of the gain of both players must be equal to zero as written in equation (3-4).

$$\boldsymbol{\alpha_{ij} + \beta_{ij} = 0} \quad \forall (i, j) \in N \qquad (3)$$

$$\boldsymbol{\alpha_{ij} = -\beta_{ij}} \qquad (4)$$

The utility of a SU for selecting any channel i is as follow

$$\boldsymbol{us\ (Ai, Bj\ )} = \begin{cases} \boldsymbol{\beta ij \ \leq \ 0 \ \forall \ i \ = \ j} \\ \boldsymbol{\beta ij \ > \ 0 \ \forall \ i \ \neq \ j} \end{cases} \qquad (5)$$

The utility or payoff for the attacker would be

$$\boldsymbol{ua\ (Ai, Bj\ )} = \begin{cases} \boldsymbol{\alpha ij \ > \ 0 \ \forall \ i \ = \ j} \\ \boldsymbol{\alpha ij \ \leq \ 0 \ \forall \ i \ \neq \ j} \end{cases} \qquad (6)$$

4.3.1.2 Non Zero Sum Game

In non-zero sum game the winning of one player does not necessarily equal to the loss of other player. It may be turn to win-win situation or lose-lose situation.

4.3.1.3 Stackelberg Game

It is a sequential game. In this type of game one player moves first and the other players moves after him. Figure 4.4 represents the stacklberg game, where leader moves first and then follower take decision according to leader's move.

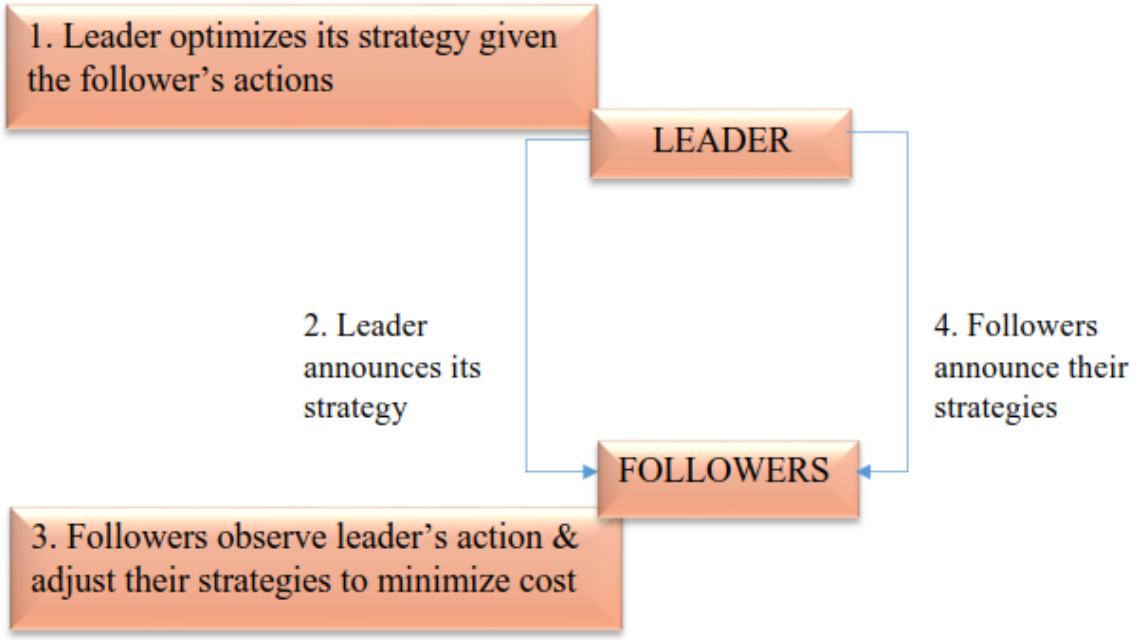

Figure 4.4: Stackelberg Game

4.3.1.4 Stochastic Game

This is a sequential game in which player play game with probabilistic transitions. The game start with some initial state. Players adopt specific strategy and receive payoff according to it at the given state. Then game forward to next state and in which probabilities are selected based on the previous state and players' strategies. So this is a dynamic game with finite and infinite number of stages.

4.3.1.5 Bayesian

A game of incomplete information. In this game players do not have complete information about other players' strategies or payoffs. Such games are known as Bayesian games because of the use of Bayesian analysis in predicting the outcome.

4.3.1.6 Evolutionary Game

Evolutionary game theory started slightly after other games have been developed [43]. John Maynard Smith proposed this type of game in context of biology to formalize the evolutionary stable strategies in 1973. In evolutionary game theory players select their strategies through a trial-and-error process .players learn over time that some strategies work better than others and thus they adopt the best strategies.

4.3.2 Cooperative Games

Cooperative games includes following categories

- Bargaining game
- Repeated game
- Coalition game

4.3.2.1 Bargaining game

It is a dynamic game with complete information. This game converges when players reach to any agreement state. Researchers have presented the Nash bargaining method to stabilize the information transmission efficiency of source to destination nodes and the residual harvested energy of relays in wireless powered relay networks in [44].

4.3.2.2 Repeated game

It is a type of an extensive game where players take decisions during the game and hence can affect the other player's decision. It can be finite or infinite game. Players play game multiple times where each decision is taken after observing the previous outcomes of the game [45].
In wireless network, repeated game has been used to model the cooperation between network nodes. Thus increasing the network performance and reducing the network disruption [46].

4.3.2.3 Coalition game

There are set of players who form groups to accomplish corporation for themselves. This game defines how each group of players can do better for itself.

4.4 Game Theory Applications

There are also different types of games and each have different applications in different fields. Lots of solutions has been proposed by using game theory in different fields. Here we focused to highlight the work related to zero sum game mostly. For example zero-sum games with incomplete information and large Zero sum games. Q-learning designs for the zero-sum game has been discussed in [32] . By using a model-free approach they achieved a solution for the game. Autopilot design for the F-16 plane is performed that shows better results of a method. Daskalakis has proposed no-regret algorithm in [33]. This zero-sum game theoretic algorithm obtains regret when applying against opponent. Quadratic improvement can be achieved on convergence rate to game value by applying this algorithm. The lower bound for all distributed dynamics is optimal when payoff matrix information is unknown to both players. But if players

know about their payoffs then they can compute minimax strategies individually. In [34] Bopardikar have proposed two algorithms after studying larger zero-sum games. Players have large number of options in this game. They gave Sampled Security Policy algorithm to compute optimal policies. Sorin have worked on repeated zero-sum games in [35]. They elaborated current advancement in these games especially together with differential games. They first described models of repeated games and differential games. Then they explained problems related to these models. Li and Cruz have studied deception and model zero sum game to resolve the conflicting situation [36]. To describe deception authors made relationship between knowledge and strategies. Repeated games with incomplete information is modeled as zero sum game in [37].

Matching penny is a perfect example of 2 player zero sum game. In this game players flip their coins secretly and then compare them. One player wins if coins match (c,d) and other lose his penny. While second player wins if coins do not match (a,b). So both players have conflicting goals and each of them tries to maximize their own gain. The figure 4.5 represents the whole scenario.

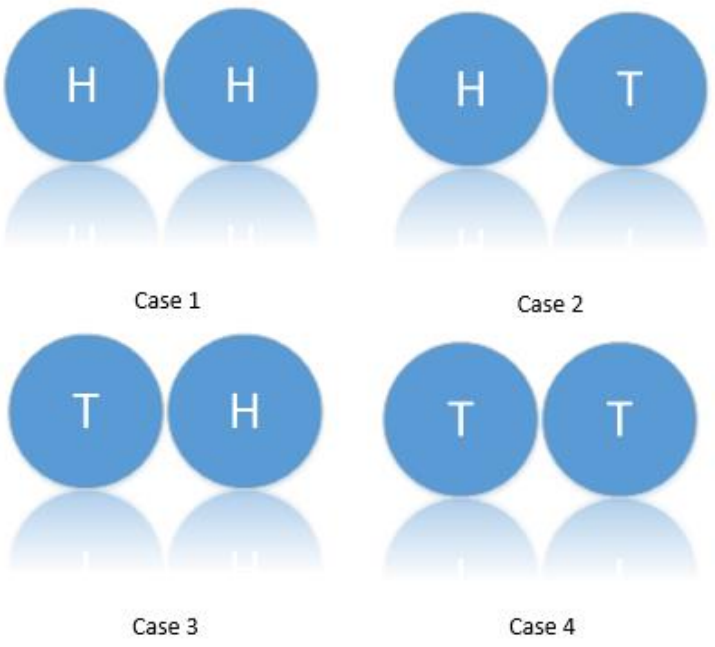

Figure 4.5: Matching Penny

Three persons matching pennies game has been described in [38]. Players have perfect information about payoffs. In this paper authors rejected the hypothesis of playing mixed

strategy. Researchers have concluded that players did not use Bayesian learning to obtain mixed strategy Nash Equilibrium. Mixed extension of matching pennies have studied in [39]. Authors represented the Nash equilibrium as finitely moments for polynomial games. Sirbu in [40] has presented the zero sum game as stochastic differential game. A unique solution came when players choose strategies after observing previous state. Pham and Zhang represented 2-player zero sum stochastic and differential game. They have considered a non-Markovian structure. The value of game is a random process which has been obtained by viscosity solution in [41]. Stochastic Differential Equation has been studied in [42] by Hernandez-Hernandez. Game has been described between controller and stopper. Controller is minimizer while stopper is maximizer in this game. Optimal strategies are not unique in this game in which controller has first move advantage.

4.5 Conclusion

In this chapter, we presented the GT .GT's basic terminologies and its applications has been presented in this chapter. Research work by different authors has been summarized in this chapter.

Chapter 5

PROPOSED METHOD TO DEFEND AGAINST DOS ATTACK

5.1 Introduction

This chapter comprises the proposed solution to defend against DoS attack. In the preliminary part we have presented the system model and assumptions. Then we have discussed the methods and algorithm to solve the problem.

5.2 System Model

Game theory is an appropriate model to formulate the scenario between an attacker and defender. Since it deals with the study of decision making of the players, where the best course of a player's action depends upon the decisions made by others. We use game theoretic representation to devise the problem between user and an attacker where heterogeneous wireless channels are available for use. Zero sum game is used to present the conflict among user and attacker. The aim of malicious attacker is to disrupt the transmission by jamming different channels and thus achieve its goal by limiting the access of SU from wireless channels. Whenever a SU tries to access the best quality channel, attacker tries to jam it by sending its transmission signals.

5.3 Assumptions

- There is no interference created by either player while PU is using channel.
- The following scenario is presenting while PU is in idle state.
- We have set of vacant wireless channels i.e., $K = 1,2,3, \ldots . k$
- Attacker and SU both have the complete information about vacant channels.
- Attacker and SU both have access to vacant channels.
- Channel utilities are fixed and are not change during transmission.
- Channels are heterogeneous and players have knowledge about it.
- Players take decisions simultaneously and select only one channel at a time.
- If both players selects same channel, then attacker gets the priority and user gets loss.
- There is no secret agreement among players.
- Players are rational.
- Number of players are not infinite.

- Number of strategies are finite.
- Same set of strategies are available for both players.
- Every player selects its own strategy and expecting the worst damage from opponent.

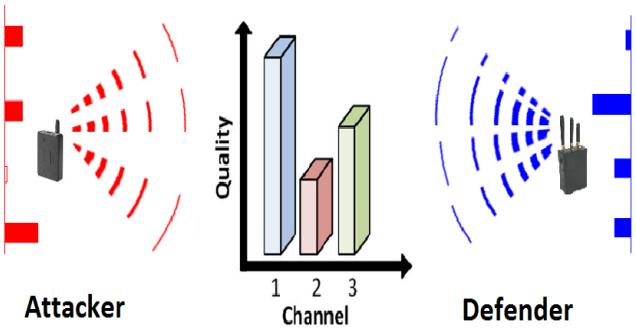

Figure 5.1: System Model

5.4 Problem Formulation

In wireless communication, the probability to create interference in network get increases by malicious users or attackers. The purpose of an attacker is to launch such attacks which can create obstruction or interference to legitimate users by using its minimum resources. The factor which is most important in game theory is to identify adequate solution for games in pervasive form.

In this thesis, the attacker and defender situation while accessing the CR channels is modeled as zero-sum game for two players. In such game, the winning of one player is equal to the loss of another player. We consider two players, i.e., SU and an attacker. Both are rational players. They are interested only in maximizing their own payoffs.

Both players i.e. attacker and defender, don't know about opponent actions or strategies. But both players know that each player who is involved in game adopt such strategy which gives maximum payoff. The attacker wishes to restrict SU by attacking on the same channel which SU try to access.

Payoffs are set by assuming the channel quality. Channel quality can be measured by setting different parameters as a scale, channel bandwidth, SNR, available time period etc. However here we assume that channel having high quality means it has higher bandwidth and available

for transmission for greater period. And thus, assign higher payoff to the attacker or defender on the successful access of that channel. Both attacker and defender try to access channel simultaneously and select one channel at a time. In our system model, we assign preference to an attacker. If an attacker and SU both access same channel at a same time then attacker gets success and gain positive payoff and SU is in loss and gain negative payoff.

5.5 Proposed Solution

According to our problem formulation, game theory proposed following solution. We used mixed strategy Nash Equilibria for solving this game problem. There is no pure strategy exists in our solution.

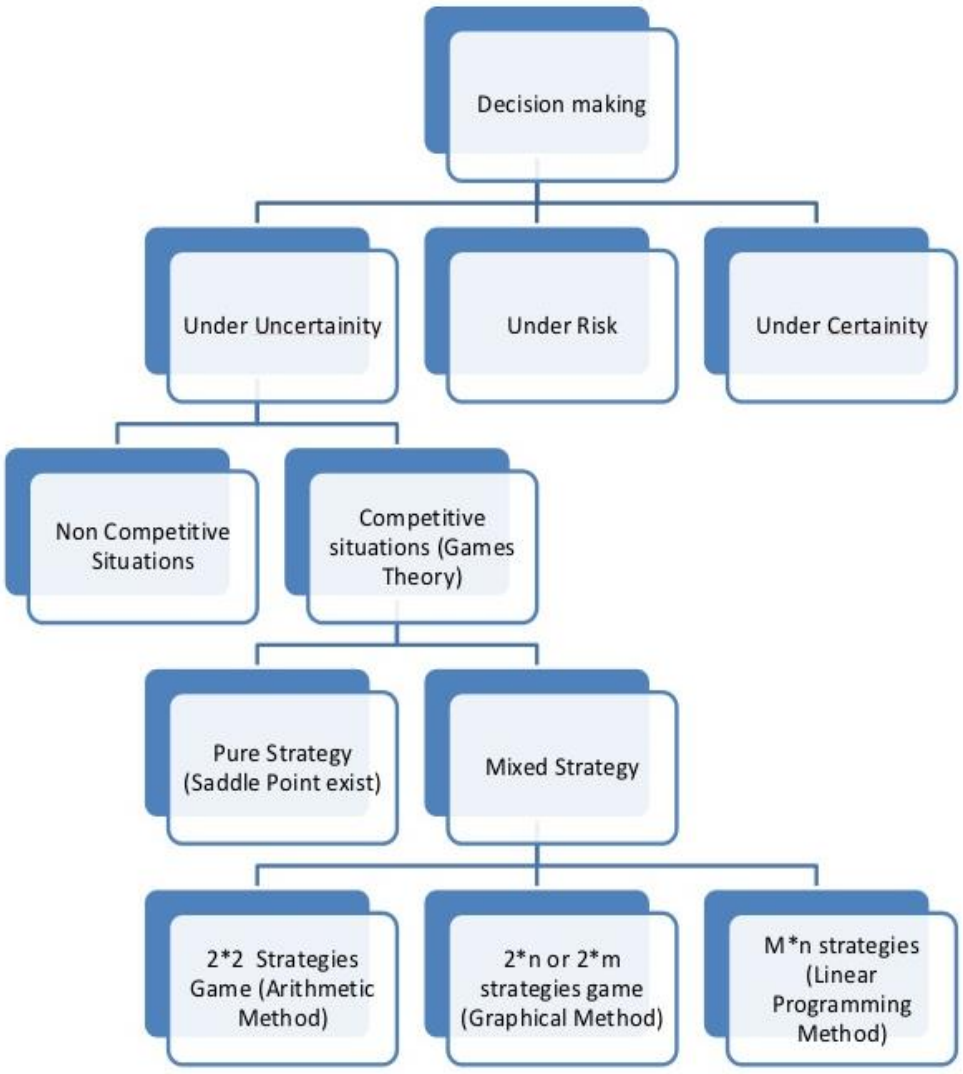

Figure 5.2: Game Solution

In the absence of saddle point, players must choose the strategy randomly i.e., players need to adopt mixed strategy to solve the game. In our case, there exists a mixed strategy and it has no pure strategy Nash Equilibrium.

Nash in 1951 has proposed that every game having finite number of players has a Nash Equilibria.

NASH's Theorem: Any game having a finite number of players each of which having finite set of strategies has a mixed strategy Nash equilibrium. According to this theorem, players either try to maximize their minimum expected payoff or minimize their maximum expected loss.

1. The expected payoff to the row player will be at least v if the row player plays his or her specific mixed strategy, no matter what mixed strategy the column player chooses.
2. The expected payoff to the row player will be at most v if the column player plays his or her specific mixed strategy, no matter what strategy the row player plays.

It is also named as ***Security strategy***. The security strategies are termed as saddle point. A saddle point is often mention as an equilibrium point because the players have no incitement to change their strategies (because there is no regret).
For a general two-player zero sum game

$$\max_{i \le m} \min_{j \le n} \alpha_{ij} \le \min_{j \le n} \max_{i \le m} \alpha_{ij} \qquad (7)$$

If both values are equal then we can write like this,

$$\max_{i \le m} \min_{j \le n} \alpha_{ij} = \min_{j \le n} \max_{i \le m} \alpha_{ij} = v \qquad (8)$$

Value of the game is represented as ***"v"***. In this scenario optimal strategies exist for both players.

Mixed Strategy:

As per requirement, attacker always attempts to choose the set of strategies with the non-zero probabilities i.e.,$p_i = \{p_1, p_2 \cdots, p_m\} \in \mathbb{R}$ to maximize its minimum gain. These probabilities must be like

$$\sum_{i=1}^{m} p_i = 1 \quad (\forall \ \ m \in C) \qquad (9)$$

$$0 \le p_i \le 1 \qquad (10)$$

Thus, an attacker tries to maximize his minimum expected gain.
Similarly, the defender would choose the set of strategies with the non-zero probabilities say $q_j = \{q_1, q_2 \cdots, q_n\} \in \mathbb{R}$ that minimizes his maximum expected loss.

$$\sum_{j=1}^{n} q_j = 1 \quad (\forall \ n \in C) \tag{11}$$

$$0 \leq q_j \leq 1 \tag{12}$$

When game's payoffs are shown in matrix form, it is called as normal form representation of game. The above table represent the normal form representation of a game. Equation 13 and equation 14 represents the expected utility for attacker and SU.

$$u_a(p) = \sum_{i=1}^{m} \left(p_i * \left(\sum_{j=1}^{n} \alpha_{ij} \right) \right) \quad \forall \quad i = 1,2, \dots, m \quad j = 1,2, \dots n \tag{13}$$

$$u_s(q) = \sum_{j=1}^{n} \left(q_j * \left(\sum_{i=1}^{m} \beta_{ij} \right) \right) \quad \forall \quad i = 1,2, \dots, m \quad j = 1,2, \dots n \tag{14}$$

Game without a saddle point can be solved by

- Arithmetic method
- Graphical method
- Algebraic method (Linear Programming Method)

We use linear programming method to get the optimize results of an attacker and SU zero-sum game for mxn matrix scenario.

5.5.1 Arithmetic Method:

This method is used to solve the game of 2* 2 matrix.
We will solve our game by using this method when we assume that we have only two channels. For this scenario the payoff matrix is represented in figure 5.3.

		DEFENDER	
		B_1	B_2
ATTACKER	A_1	α_{11}, β_{11}	α_{12}, β_{12}
	A_2	α_{21}, β_{21}	α_{22}, β_{22}

Figure 5.3: Payoff Matrix for 2 players Zero Sum game

Example: Mathematically we express the players' strategy in matrix form. Players have two strategies i.e., they have choice to select two channels. We assign 10 MBs/s data rate for lower quality channel and 20 MBs/s for higher quality channel to model the game. Let's assume channel 1 has lower quality while channel 2 has higher quality.

Both attacker and user selects one channel at a time. If an attacker and user both select same channels simultaneously, then attacker gets success and it stops legitimate user to use that channel. Hence, attacker gains payoff equal to that channel data rate. SU gets negative payoff equal to that which attacker gains. So, it is in the favor of user to select channel other than which attacker selects.

		Defender's Payoff	
		Ch1	*Ch2*
Attacker's Payoff	*Ch1*	-10 10	20 -20
	Ch2	10 -10	-20 20

Figure 5.4: Payoff Matrix for Attacker & SU

In figure 5.4, negative payoff of a user represents that channel is being attacked and attacker has snatched the resources. Negative payoff for an attack represents that attacker could not launch a successful attack.

Expected utility calculation of an attacker:

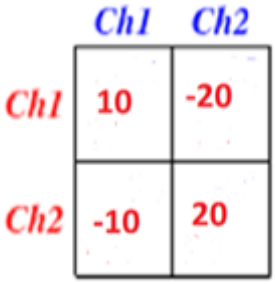

Figure 5.5: Payoff Matrix for Attacker

In a zero sum game payoff of one player is negative of payoff of other's player .So, we can represent figure 5.4 in a simple form as figure 5.5. Figure 5.5 represents the attacker's payoff matrix. There is no saddle point exists in this case, so we cannot use pure strategy. We will apply mixed strategy to fine equilibrium point.

Let's p1 represents the proportion of times that an attacker attacks on channel 1. Let us try to choose p1 so that attacker wins the same amount on the average whether SU selects 'channel1' or 'channel 2'.

Then attacker's average winnings when SU choose 'channel 1' is

$$10(p1) + (-10)(1 - p1)\ (15)$$

And attacker's average winnings when SU selects 'channel 2' is

$$-20p1 + 20(1 - p1)\ (16)$$

Attacker should selects p1 so that

$$p1(10) + (-10)(1 - p1) = (-20)p1 + (1 - p1)(20) \qquad (17)$$

$$10p1 - 10 + 10p1 = -20p1 + 20 - 20p1$$

$$20p1 - 10 = -40p1 + 20$$

$$60p1 = 30$$

$$p1 = 30/60$$

$$\boldsymbol{p1 = 1/2}$$

Hence, Attacker should choose ‘channel1’ with probability 1/2, and ‘channel 2’ with probability 1/2.

Expected payoff for an attacker can be calculated by using equation (13). We find the results as:

On average, attacker wins

$$ua\,(p) \;=\; (1/2)\,10 \;+\; (1/2)(-10) \;+\; (1/2)(-20) \;+\; (1/2)(20)$$

$$ua\,(p) \;=\; 0$$

Expected Payoff for an attacker is zero.

No matter what SU selects. Such a strategy that gives the same average winnings no matter what the opponent does is called an equalizing strategy.

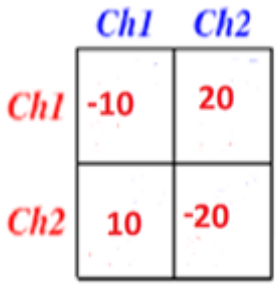

Figure 5.6: Payoff Matrix for SU

Figure 5.6 represents the SU’s payoff matrix. This figure shows results that are negative of the payoffs of figure 5.5.

Probability with which SU tries to access channel1 is

$$q1 = 2/3$$

Probability with which SU access channel2 is

$$q2 = 1/3$$

Expected Payoff for SU at equilibrium can be found by using equation (14)

We get the result at equilibrium as:

$$us\,(q) \;=\; (2/3)(-10) \;+\; (1/3)(20) \;+\; (2/3)\,(10) \;+\; (1/3)\,(-20)$$

$$us\,(q) \;=\; 0$$

5.5.2 Algebraic Method

Linear programming method has been proposed to solve the game in case of more than two channels. Simplex algorithm has been presented in this thesis. This algorithm as shown in figure 5.7, is capable of solving complex problems and give optimize solution.

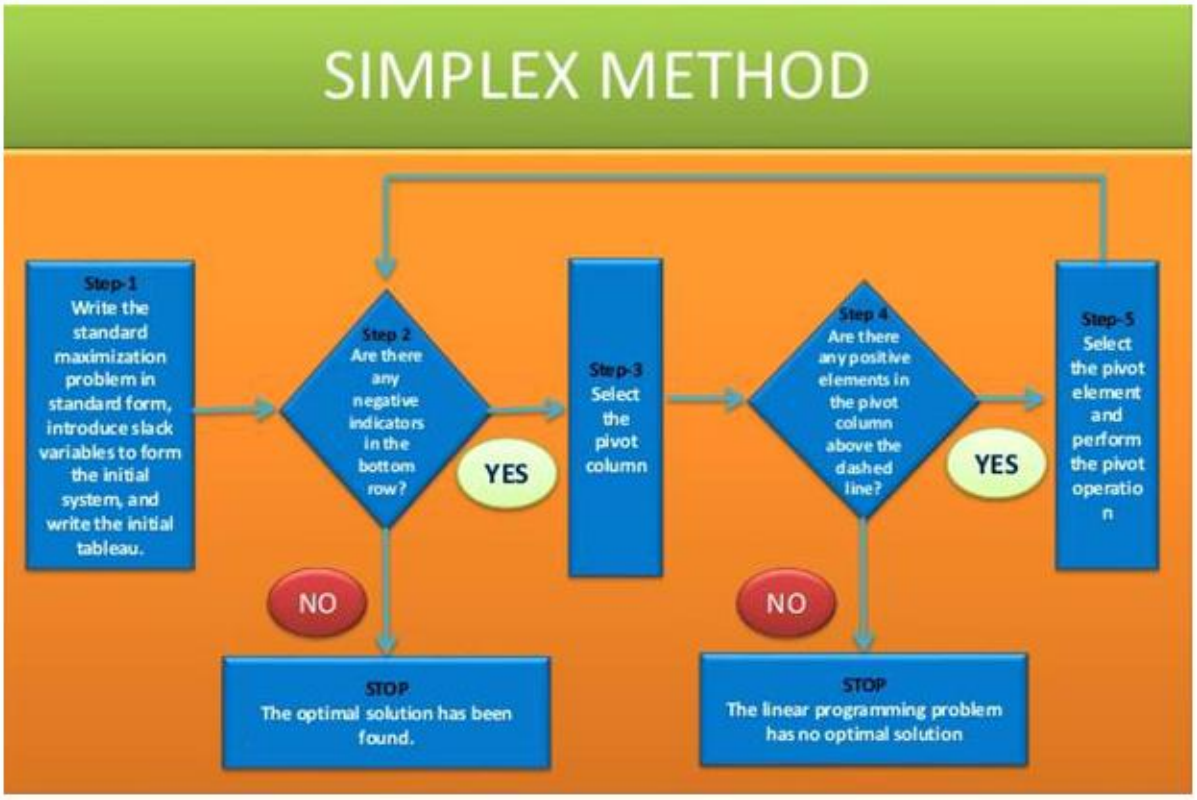

Figure 5.7: Simplex Algorithm for Standard Maximization problem

5.6 Conclusion

In this chapter we have first presented the problem formulation. Next we described the assumptions taken while solving the problem. In the end of the chapter, we have explained the simplex algorithm which was used to solve the game. Simulation results which was attained by using the above knowledge describes in the next chapter.

Chapter 6

SIMULATION RESULTS AND DISCUSSION

6.1 Introduction

In this chapter, the simulation results of proposed scheme are presented. Our proposed detection scheme gives optimize solution. Different cases has been taken to present the simulation results which verify the best defending strategies.

6.2 Simulations with One Vacant Channel

Case 1: This is a case when attacker and defender has only one channel to access. Same channel is occupied by attacker and user. If SU tries to access better quality channel all the time, in that case it would be easy for an attacker to guess the channel. In this way attacker get success all the time. So, this condition is not favorable for SU. Figure 6.1 represents Attacker and SU's payoffs.SU is deprived of high quality channel all the time and attacker gets success all time.

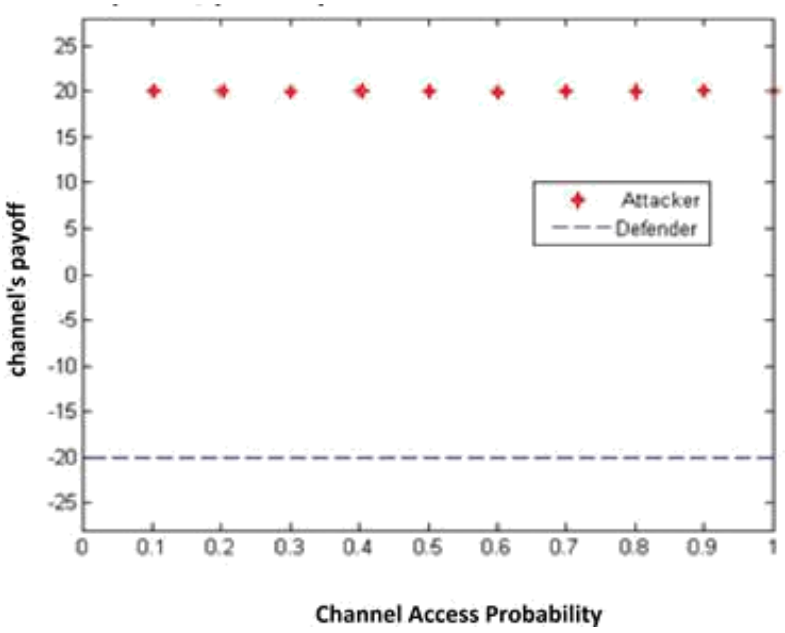

Figure 6.1: Attacker & SU Access Same Channel

Case 2: In this case, attacker attacks on channel with different probabilities because it does not sure about the presence of SU. If defender use high quality channel but attacker does not know

about SUs activity. Attacker tries to guess which channel is used by user mostly. So, attacker randomly select high quality channel with different probabilities.

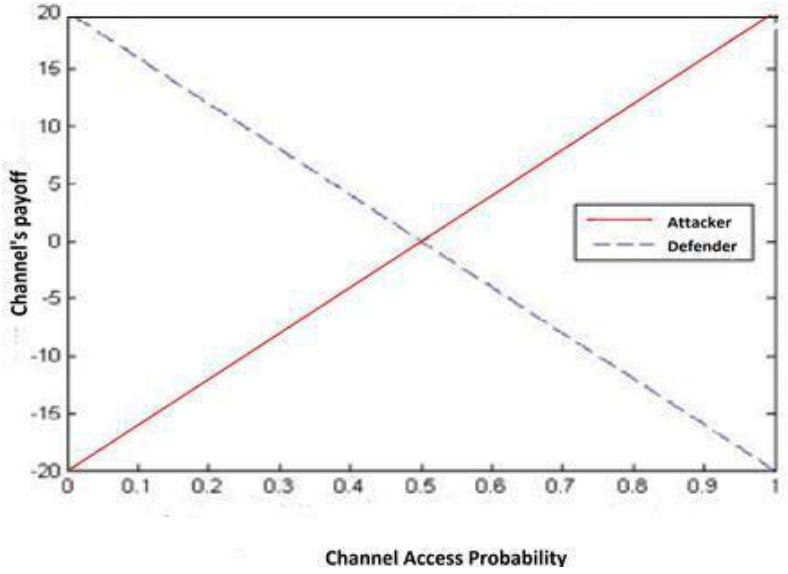

Figure 6.2: Channel Access with Different Probabilities

Figure 6.2 shows that initially when attacker selects high quality channel with lower probability, it gets no success and it gains lowest pay off. At equilibrium point attacker try to maximize its payoff and defender try to minimize its loss and attacker selects higher and lower quality channels with equal probabilities, as a result both get zero payoffs. When attacker increase its probability to attack on higher quality channel, it gets success and gain higher payoff results in defender's loss.in this way attacker gets user's activity knowledge that user is using higher quality channel. Same is the case goes if user selects lower quality channel.

Both the above graphs show that, if user does not adopt any strategy while accessing channel, then there is a chance of being attacked by the attacker on vacant channels. Using same vacant channel results in constant channel attack in long run.

6.3 Simulations with more than one Vacant Channel

In this case we consider 10 or 12 vacant channels which are available for communication. As per our assumption despite of the availibity of multiple vacant channels both players can only selects one channel at a time. Channels are categorized with increasing utility from channel 1 to channel n.

Case 1: By increasing number of channels attacker's payoff get decrease. Attacker does not have infinite resources to jam the whole communication network. So, it becomes difficult for

an attacker to actualize enormous interference if it has limited resources. So, SU can minimize its loss if it has multiple channels to access.

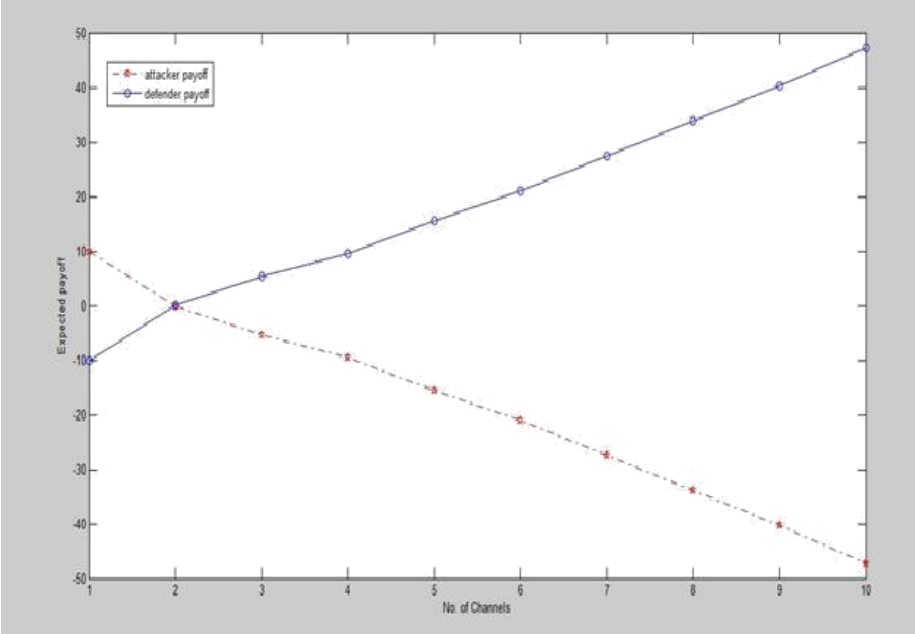

Figure 6.3: Attacker & SUs' Payoff when multiple channels are available

If we increase the number of channels then defender has more chance to avoid the attack. This case is shown in figure 6.3.So defender can increase its payoff if number of multiple channels are available to it.

Case 2a: In Random channel selection strategy, an attacker has chosen channel randomly (with equal probability). The figure 6.4 shows the simulation results after calculating the user's payoff in the presence of attacker. In figure 6.4, SU try to defend against attacker's random strategy. There is a great fluctuation in SUs payoffs if SU and attacker both select channels randomly. Simulation results prove that SU attain highest payoff by selecting either greedy or optimal strategy.

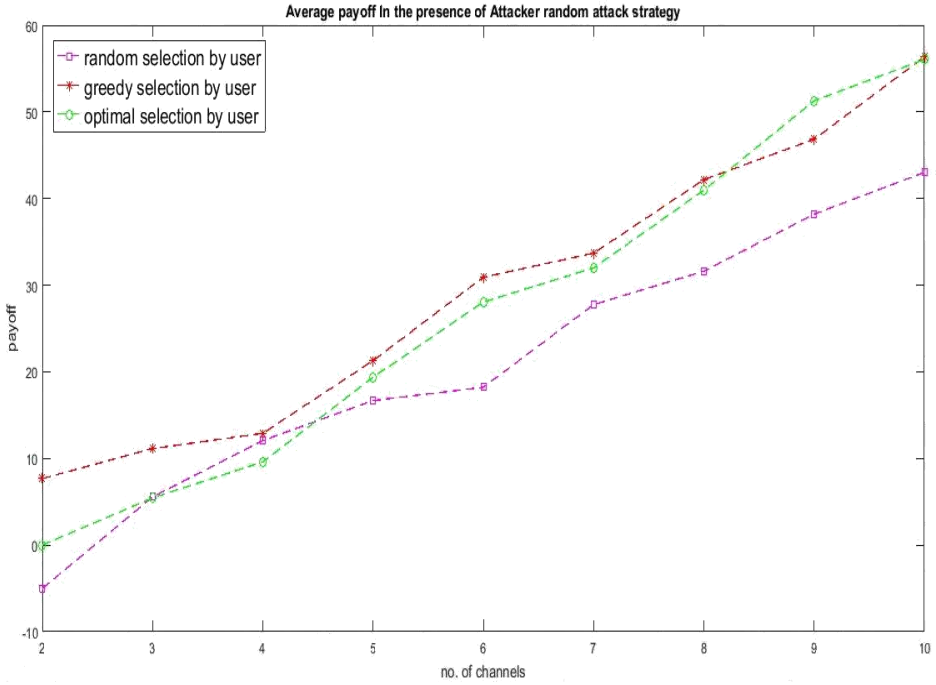

Figure 6.4: SUs payoff in the presence of Random Attack

Case 2b: The probability of selecting a higher utility channel is greater when an attacker attacks on a channel in avaricious mod. If attacker selects greedy strategy to attack on channels then SU apply defending strategy to get the maximum gain. In figure 6.5 ,Simulation results represent the payoffs for both the SU and the attacker. If we increase the number of vacant channels, then in long run SU gets more chances to avoid attack.

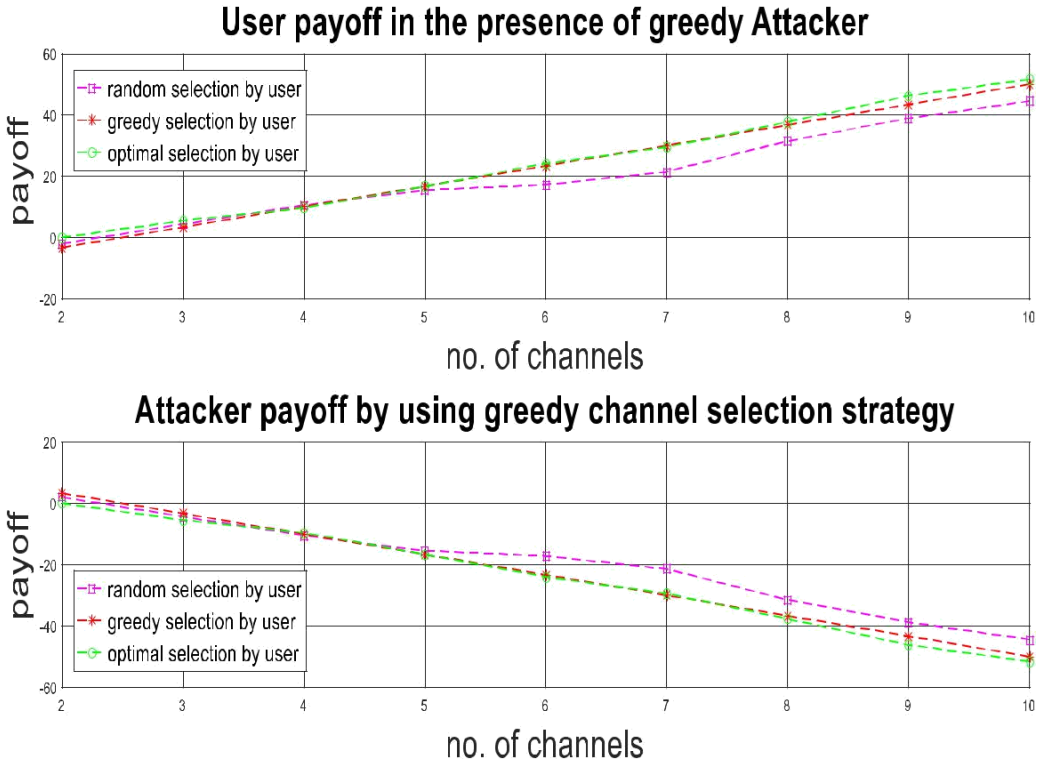

Figure 6.5: SU's payoff in the presence of Attacker's Greedy Strategy

Case 2c: Attacker and SU both selects optimal strategy to access channel. In figure 6.6, both players use linear programming method to find the best suitable results to access the channel.SU again gets the maximum payoff if he selects channel by using optimal strategy.

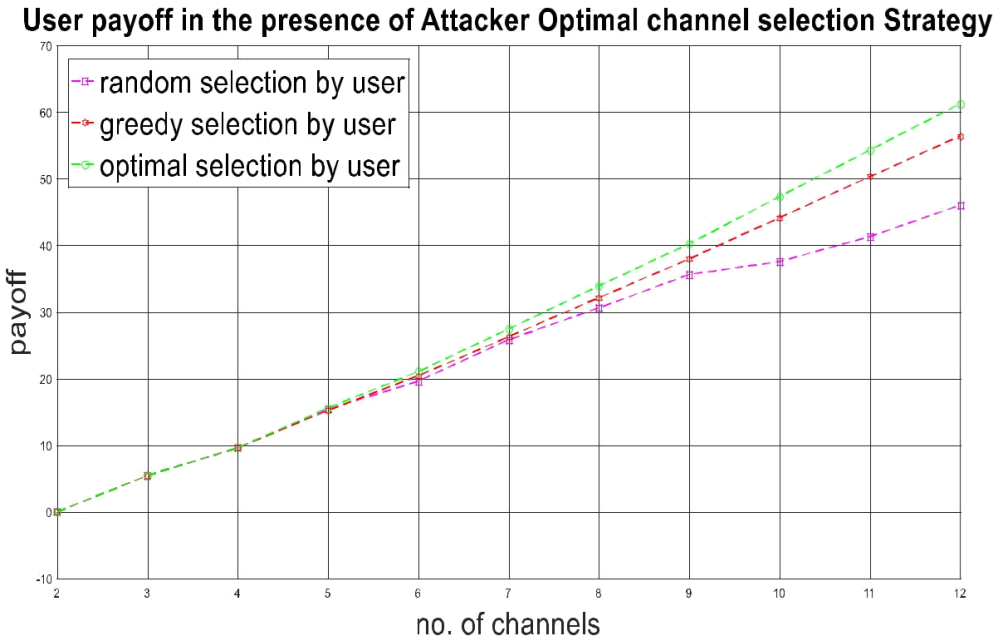

Figure 6.6: SU's payoff in the presence of Attacker's Optimal Strategy

Figure 6.6, represents that we get linear increase in the all the results, if both SU and attacker adopt optimal strategy.

6.4 Conclusion

This chapter concludes different cases, representing the working of the theoretical system and players adopting the best strategies is presented in this chapter. The optimum solution by using simplex algorithm are also discussed here. Different scenarios has been discussed and comparisons show that linear programming algorithm shows the best results in all cases. Number of fluctuations are greater in case of attacker's random strategy. While, greedy strategy adopting by players at different instances also does not ensure the ultimate success in channel's access. So here, we can conclude that the best suitable strategy in the presence of DoS attack is the optimal strategy which is obtained by applying linear programming algorithm and SU can defend against attack if greater number of vacant channels are available.

Chapter 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

In this thesis, we present a game theoretical model to analyze the attacker's behavior to jam the cognitive channels and derive a solution for CR user. The attacker and SU both have conflicting goals so we use zero-sum game to model the competitive situation in a mathematical frame work and show the significance of channel diversity to tackle the attacks. We describe a solution of the game for the known and fixed channel payoffs to the both players. We derive mixed strategy Nash Equilibria as a suitable solution for this scenario. We present the method of linear programming to solve the mixed strategy Nash Equilibria. Simulation results are shown by using MATLAB as a tool to present the demonstration of suggested solution.

7.2 Future Work

Here in this thesis, we just avoid or defend against Dos attack by using different strategies. Future work will also look into the case that the attacker can simultaneously exploit multiple channels while the defender can also simultaneously defend against several vulnerabilities. Furthermore the zero sum game can be extended for the case of multiple attackers attacking the network channels simultaneously. This work can also be extended in the direction of identifying the attacker's presence and mitigate the attacks instead of avoiding it.

REFERENCES

1. Lee, W.-Y. and I.F. Akyildiz, *Spectrum-aware mobility management in cognitive radio cellular networks.* IEEE Transactions on Mobile Computing, 2012. 11(4): p. 529-542.

2. Mitola, J. and G.Q. Maguire, *Cognitive radio: making software radios more personal.* IEEE personal communications, 1999. 6(4): p. 13-18.

3. Hao, D. and K. Sakurai. *A differential game approach to mitigating primary user emulation attacks in cognitive radio networks*. in *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on*. 2012. IEEE.

4. Chen, K.-C., et al. *Cognitive radio network architecture: part I--general structure*. in *Proceedings of the 2nd international conference on Ubiquitous information management and communication*. 2008. ACM.

5. Armi, N., et al., *Malicious User Attack in Cognitive Radio Networks.* Telkomnika, 2017. 15(3).

6. Xin, C. and M. Song, *Detection of PUE attacks in cognitive radio networks based on signal activity pattern.* IEEE transactions on mobile computing, 2014. 13(5): p. 1022-1034.

7. Akram, M.W., et al. *A review: Security challenges in cognitive radio networks*. in *Automation and Computing (ICAC), 2017 23rd International Conference on*. 2017. IEEE.

8. Bhattacharjee, S., R. Rajkumari, and N. Marchang, *Cognitive Radio Networks Security Threats and Attacks: A Review.* Journal of Computer Applications, ICICT, 2014: p. 16-19.

9. Rizvi, S., N. Showan, and J. Mitchell, *Analyzing the Integration of Cognitive Radio and Cloud Computing for Secure Networking.* Procedia Computer Science, 2015. 61: p. 206-212.

10. Sejaphala, L.C. and M. Velempini. *Detection algorithm of sinkhole attack in software-defined wireless sensor cognitive radio networks*. in *Wireless Summit (GWS), 2017 Global*. 2017. IEEE.

11. Kibirige, G.W. and C. Sanga, *A Survey on Detection of Sinkhole Attack in Wireless Sensor Network.* arXiv preprint arXiv:1505.01941, 2015.

12. Rehman, A. and D. Prakash, *Study of Attacks and their Defence Methods in CRN: A Survey.* 2018.

13. Hlavacek, D. and J.M. Chang, *A layered approach to cognitive radio network security: A survey*. Computer Networks, 2014. 75: p. 414-436.

14. Jiang, C., et al., *Renewal-theoretical dynamic spectrum access in cognitive radio network with unknown primary behavior*. IEEE Journal on Selected Areas in Communications, 2013. 31(3): p. 406-416.

15. Li, H. and Z. Han, *Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems—Part II: Unknown channel statistics.* IEEE Transactions on Wireless Communications, 2011. 10(1): p. 274-283.

16. Thomas, R.W., et al. *A Bayesian game analysis of emulation attacks in dynamic spectrum access networks*. in *New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on*. 2010. IEEE.

17. Chen, R., J.-M. Park, and K. Bian. *Robust distributed spectrum sensing in cognitive radio networks*. in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. 2008. IEEE.

18. Li, X. and W. Cadeau. *Anti-jamming performance of cognitive radio networks*. in *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*. 2011. IEEE.

19. Lo, B.F. and I.F. Akyildiz. *Multiagent jamming-resilient control channel game for cognitive radio ad hoc networks*. in *Communications (ICC), 2012 IEEE International Conference on*. 2012. IEEE.

20. Di Pietro, R. and G. Oligeri, *Jamming mitigation in cognitive radio networks.* IEEE Network, 2013. 27(3): p. 10-15.

21. Sawant, S., et al., *Learning to Coordinate in a Decentralized Cognitive Radio Network in Presence of Jammers.* arXiv preprint arXiv:1803.06810, 2018.

22. Attar, A., et al., *A survey of security challenges in cognitive radio networks: Solutions and future research directions.* Proceedings of the IEEE, 2012. 100(12): p. 3172-3186.

23. Zhu, H., et al., *You can jam but you cannot hide: Defending against jamming attacks for geo-location database driven spectrum sharing.* IEEE Journal on Selected Areas in Communications, 2016. 34(10): p. 2723-2737.

24. Shu, Z., Y. Qian, and S. Ci, *On physical layer security for cognitive radio networks.* IEEE Network, 2013. 27(3): p. 28-33.

25. Almasaeid, H.M. and A.E. Kamal. *Receiver-based channel allocation for wireless cognitive radio mesh networks*. in *New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on*. 2010. IEEE.

26. Debroy, S. and M. Chatterjee. *Intra-cell channel allocation scheme in IEEE 802.22 networks*. in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*. 2010. IEEE.

27. Vempaty, A., et al. *Adaptive learning of Byzantines' behavior in cooperative spectrum sensing*. in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*. 2011. IEEE.

28. Baburaj, C.A. and D.K. Alagarsamy, *REPETITIVE TRUST MANAGEMENT AND ADVERSARY DETECTION FOR DELAY TOLERANT NETWORKS.* Journal of Theoretical & Applied Information Technology, 2014. 61(3).

29. Zeng, K., Q. Peng, and Y. Tang, *Mitigating spectrum sensing data falsification attacks in hard-decision combining cooperative spectrum sensing.* Science China Information Sciences, 2014. 57(4): p. 1-9.

30. Karlof, C. and D. Wagner, *Secure routing in wireless sensor networks: Attacks and countermeasures.* Ad hoc networks, 2003. 1(2-3): p. 293-315.

31. Salem, F.M., M.H. Ibrahim, and I. El-wahab, *Secure authentication scheme preventing wormhole attacks in cognitive radio networks.* Asian Journal of Computer Science and Information Technology, 2012. 2: p. 52-55.

32. Al-Tamimi, A., F.L. Lewis, and M. Abu-Khalaf, *Model-free Q-learning designs for linear discrete-time zero-sum games with application to H-infinity control.* Automatica, 2007. 43(3): p. 473-481.

33.Daskalakis, C., A. Deckelbaum, and A. Kim, *Near-optimal no-regret algorithms for zero-sum games.* Games and Economic Behavior, 2015. 92: p. 327-348.

34. Bopardikar, S.D., et al., *Randomized sampling for large zero-sum games.* Automatica, 2013. 49(5): p. 1184-1194.

35. Sorin, S., *Zero-sum repeated games: recent advances and new links with differential games.* Dynamic Games and Applications, 2011. 1(1): p. 172-207.

36. Li, D. and J.B. Cruz Jr, *Information, decision-making and deception in games.* Decision Support Systems, 2009. 47(4): p. 518-527.

37. Gensbittel, F., *Extensions of the cav (u) theorem for repeated games with incomplete information on one side.* Mathematics of Operations Research, 2014. 40(1): p. 80-104.

38. McCabe, K.A., A. Mukherji, and D.E. Runkle, *An experimental study of information and mixed-strategy play in the three-person matching-pennies game.* Economic Theory, 2000. 15(2): p. 421-462.

39. Stein, N.D., A. Ozdaglar, and P.A. Parrilo, *Structure of extreme correlated equilibria: a zero-sum example and its implications.* International Journal of Game Theory, 2011. 40(4): p. 749-767.

40.Sirbu, M., *On martingale problems with continuous-time mixing and values of zero-sum games without the Isaacs condition.* SIAM Journal on Control and Optimization, 2014. 52(5): p. 2877-2890.

41. Pham, T. and J. Zhang, *Two person zero-sum game in weak formulation and path dependent Bellman--Isaacs equation.* SIAM Journal on Control and Optimization, 2014. 52(4): p. 2090-2121.

42. Hernandez-Hernandez, D., R.S. Simon, and M. Zervos, *A zero-sum game between a singular stochastic controller and a discretionary stopper*. The Annals of Applied Probability, 2015. 25(1): p. 46-80.

43. Weibull, J.W., *Evolutionary game theory*. 1997: MIT press.

44. Zheng, Z., et al. *Resource allocation in wireless powered relay networks through a nash bargaining game*. in *Communications (ICC), 2016 IEEE International Conference on*. 2016. IEEE.

45. Charilas, D.E. and A.D. Panagopoulos, *A survey on game theory applications in wireless networks.* Computer Networks, 2010. 54(18): p. 3421-3430.

46. Hoang, D.T., et al., *Applications of repeated games in wireless networks: A survey.* IEEE Communications Surveys & Tutorials, 2015. 17(4): p. 2102-2135.