IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 5, Ser. II (Sep. – Oct. 2020), PP 40-48
www.iosrjournals.org

"Cognitive Radio Networks" Game theoretic approach to mitigate security attacks

Khumjila Quinker M.Tech,
CSE Scholar MUR1801364
Computer Science & Engineering Mewar University , Gangrar Chittorgargh-312901, India.

Mr. Ankit Navalakha, Shiv Kumar (Assit. Prof.)
Computer Science & Engineering Mewar University , Gangrar Chittorgargh-312901, India.

Abstract:- *The Spectrum utilization demand due to large number of growth of wireless users that has led to spectrum shortage problem and that is expected to increase more and more by years. Thus, the technology that identified the spectrum shortage is known as Cognitive Radio. It solves the spectrum shortage problem by allowing unauthorized users to consume the spectral resources when Primary Users (PU) is not active. Its main function of Cognitive Radio Networks (CRNs) is Spectrum sensing and also to identified the unused licensed spectrum bands and also to protect the transmissions of primary users (PUs). In Cognitive Radio Networks, the jamming attack is one of the major threats, where several malicious attackers intend to stop the communications of secondary users by giving disturbance. In this project, evolutionary game has been used to applied in order to minimise the attack.*

Keywords: *Spectrum, Cognitive Radio, Cognitive Radio Networks, jamming attack*

Date of Submission: 07-10-2020 Date of Acceptance: 22-10-2020

I. Introduction

Cognitive radio network is one of the network technologies which gives the facility to reutilize or utilize the unused bandwidth network. Supposed there is a television band and there are two users, i.e. Primary Users (PUs) or licensed users and the Secondary Users (SUs) or unlicensed users. The primary user is the main user and also the owner of the bandwidth .Supposed television has owned one band with dedicatedly for the television channel, however frequencies it has reserved that much frequency is not used by the television . So that the unused frequency can be use by the Secondary users (SUs) .These days devices (mobile, ipad, computer, laptop, etc.) are increasing day by day, so if per person has at least 3 devices that connects to wireless network however that can be used limited frequency only as the frequency cannot be increased. So if unused frequency started using, it will utilize the bandwidth or the frequency as well as the best utilization of the resources.

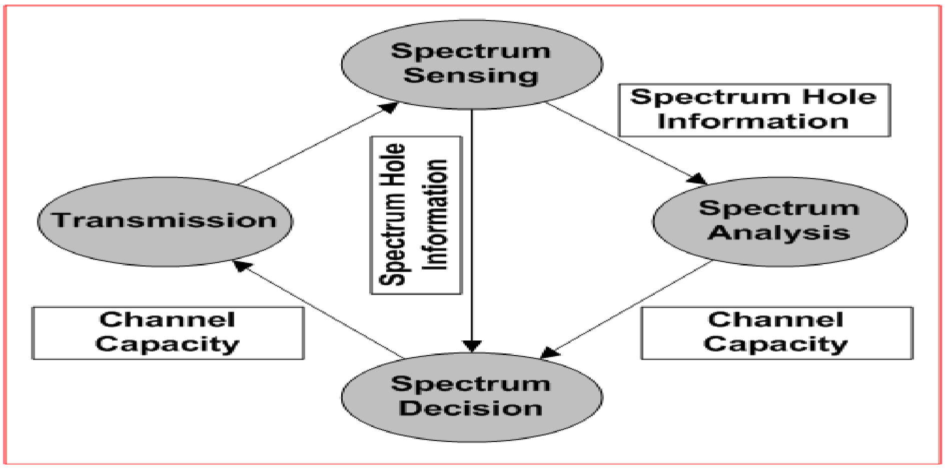

Figure (1): Cognitive Radio Network Architecture

From the above figure it is clearly showing that first we have to sense the spectrum whether the channel is free or busy, if the channel is busy then primary user or licence user is active using the spectrum.

1.1 GAME THEORY

Game theory is a mathematical tool which is used to study various interact among multiple decision makers .We can predict the result also we can calculate the probability properly using game theoretic approach. The importance of studying cognitive radio networks in a game theoretic framework is multifold. Game theory is the formal study of conflict and cooperation. Game theoretic concepts apply whenever the actions of several agents are interdependent. These agents may be individuals, groups, firms or any combination of these. It deals with the study of decision making in which there were players. A player is the one who makes decision in game. The concept of game theory provides a language to formulate structure, analyses and understand strategic scenarios

Generally there are two types of Game theories, they are:-

1. **Co-operative Game Theory:** It is a game with computation between group of layers due to possibility of external enforcement of cooperative behaviour.
2. **Non-cooperative Game Theory:** It is a game with competitive between individual players and in which only self-enforcing aliases are possible due to the absence of external means to enforce cooperative behaviour.

1.2 SECURITY ATTACKS IN COGNITIVE RADIO NETWORKS:

In wireless communication the number of technologies has been developed and there is always a common issue in this field i.e. 'Security' due to its open medium of communication. There are various types of attacks:

Primary User Emulation Attack (PUEA) is one of the major threats to the spectrum sensing, which decreases the spectrum access probability**.** In PUEA malicious users will be treated as the primary users in absence of the primary users however in actual scenario or in actual environment when the primary users is not present at that time the malicious users will behave as a primary users. So, when a signal is recognized which is detected when secondary user is active, it assumed that the signal is that of a secondary user only, otherwise it concludes that the signal is of a primary user.

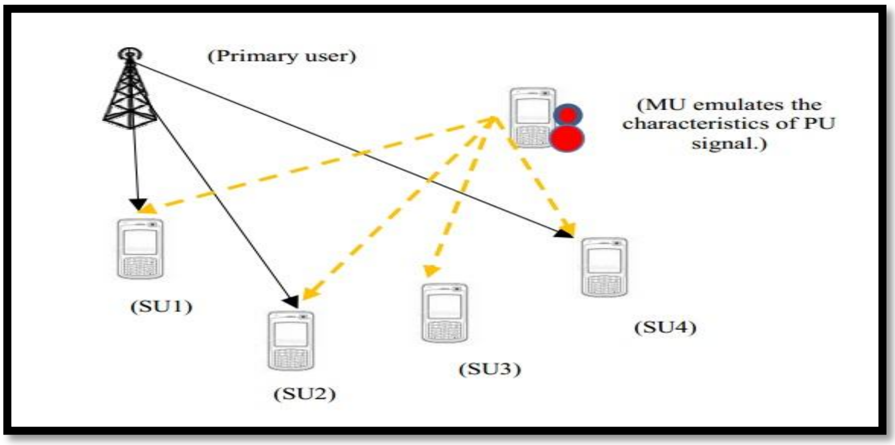

Figure (2): Illustration of PUEA launching scenario

Spectrum Sensing Data Falsification (SSDF) Attack: The attacks in which attackers send false local spectrum sensing results to a data collector, causing the data collector to make a wrong spectrum sensing decision is known as Spectrum Sensing Data Falsification(SSDF). In SSDF attack, there are two users, such as- Primary User and Secondary Users. According to rule, Secondary users (SUs) only remain active when Primary User (PUs) is inactive. So, secondary users detects the channels before using the channel whether primary users is active or not. If Primary user is inactive, secondary users will use the channel. While secondary users can be formed into two type of malicious users, such as- First malicious secondary users will do the malicious activity, however the second malicious secondary users will keep on interfering the channel. Malicious users are also nothing but secondary users however malicious users will use only for own benefits. In SSDF attack secondary users always give feedback to fusion centre that is nothing but centralized one machine, this machine will give everything class monitor every

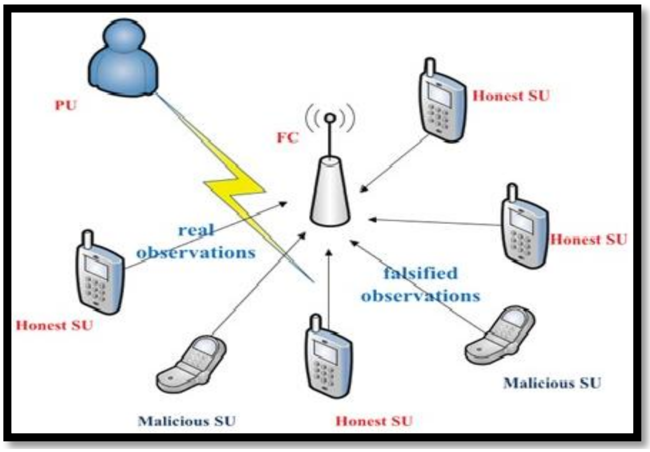

Figure (3): scenario of SSDF attack

Jamming attack: The main purpose of the jamming attack in network is to deny the service by using high usage of bandwidth. In jamming attack, the attacker send false information frequently to interfere the legitimate users in communication network session from sending or receiving data. The major attack that jammer can performed is jamming the dedicated channel that is being used to exchange sensing information between Cognitive Radio. While jamming attack can identified into four types, such as- Constant Jammer, Deception Jammer, Random Jammer and Reactive Jammer.

II. Literature Survey

This literature survey is regarding the project work that I had learned and had applied for it to complete the project work**.**

"Primary User Emulation Attack in Cognitive Radio Networks: According to Deepa Das and Susmita Das, Department of Electrical Engineering, NIT, Rourkela, India, it is one of the most causes for the spectrum sensing that reduces the spectrum accessibility. Also, CR has types of Access Point (AP) along with different kinds of unique behaviour. Such as- Misbehaving Access Point, Selfish AP, Cheat AP and Malicious AP. The dynamic spectrum access environment between PU and SUs is, PU always uses the authorized frequency band but SUs can utilize the spectrum only when PU is not active. When the attacker creates similar types of signal between PU and SUs, such as to create a mistake in frequency band of PU and to confuse the SU, also to make SUs identify the attacker as PU, and unoccupied the spectrum band immediately. Such an attack is known as PUEA.

"Security Challenges in Cognitive Radio Networks": According to Hanen Idoudi, Kevin Daimi, and Mustafa Saed, Cognitive radio is a technology to overcome the shortage of the unlicensed spectrum bands. It is also allowed the unlicensed users to use licensed bands while safeguarding the priority of primary licensed users. Also, CRNs are of two types- Primary Users (PUs) and Secondary Users (SUs). PUs has access priority to the spectrum and also allowed SUs to used spectrum band or channel when not active. Whereas SUs have to cater for the highest priority of PUs by detecting their presence and terminating their communications immediately to avoid any interference with PUs.

"A Credibility based Defence SSDF Attacks Scheme for the Expulsion of Malicious Users in Cognitive Radio": According to Hong Du, Shuang Fu and Hongna Chu, in SSDF, the malicious user always sends the results in contrast with the actual data. In order to eliminate the impact of malicious users to collaborative detection performance, a defence attack scheme based on credibility is proposed.

Spectrum Sensing Data Falsification (SSDF), also known as the Byzantine Attack , that takes place when an attacker sends false local spectrum sensing results to its neighbours or to the fusion center, causing the receiver to make a wrong spectrum-sensing decision. It also targets centralized as well as distributed CRNs. While in the centralized CRN, the fusion center can lessen the effect of false information by comparing the data received from all CRs and devising some smart techniques to know which CR might be lying.

" Survey of Security Issues in Cognitive Radio Networks": According to Wassim El-Hajj1, Haidar Safa1, Mohsen Guizani Computer Science Department, American University of Beirut, Lebanon Computer Science Department, Western Michigan University, USA, Cognitive Radio (CR) is a technology to solve the insufficiency of spectrum by allowing secondary users users without causing interference to their communication.

"Cognitive Radio Network Modeling Using Game Theoretic Approach for Effective Resource Allocation": According to KOUSIKA,DIVYA BHARTI.S, INDUMATHI, AJAY.V.P UG scholar, Dept. of ECE, KPR Institute of Engineering & Technology Arasur, Coimbatore, TamilNadu, India, Assistant Professor, KPR Institute of Engineering & Technology, Arasur, Coimbatore, Tamil Nadu, India, Game theory is the formal study of conflict and cooperation. Its concepts are applied whenever the actions of several agents are interdependent.

"Jamming Attack Detection Technique in Cognitive Radio Networks": According to Jebamalar Leavline, M.Dinesh, D. Asir Antony Gnana Singh**,** Department of Electronics and Communication Engineering Bharathidasan Institute of Technology, Anna University, Tiruchirappalli, India. Department of Computer Science and Engineering Bharathidasan Institute of Technology, Anna University, Tiruchirappalli 620024, India, In jamming attack, the (jammer) attacker maliciously sends or receives data to obstruct genuine users in a session. There exist four types of jammers: Constant Jammer, Deceptive Jammer, Random Jammer, and Reactive Jammer.

"Game theory for cognitive radio networks": According to Beibei Wang , Yongle Wu, K.J. Ray Liu Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA, Cognitive radio technology, a revolutionary communication paradigm that can utilize the existing wireless spectrum resources more efficiently, has been receiving growing attention in recent years. As network users need to adapt their operating parameters to the dynamic environment, which may pursue different goals, traditional spectrum sharing approaches based on a fully cooperative, static, and centralized network environment are no longer applicable. Instead, game theory has been recognized as an important tool in studying, modelling, and analyzing the cognitive interaction process.

"Game Theory in Operations Research": According to Nicol´ as E. Stier-MosesColumbia University, Graduate School of Business (United States), the most important tool used to address decision-making in the presence of competition in loosely integrated systems is Game Theory and the associated equilibrium concepts. The differentiating factor of the Operations Research and Computer Science communities was a focus on computation, which led to the name Algorithmic Game Theory directions of research central to our community where this trend has been significant include transportation.

"Mitigating SSDF Attack using K-Medoids Clustering in Cognitive Radio Networks ": According to Sikhamoni Nath, Ningrinla Marchang, Amar Taggu, NERIST, Nirjuli, The decision of the Fusion Center plays a vital role. Attackers may try to manipulate the decision-making of the Fusion Center (FC) for selfish reasons or to interfere with the primary user transmission. In an SSDF attack, malicious users try to manipulate the FC by sending false sensing reports.

"Cognitive Radio and its Functionalities" : According to Aishwarya Mishra, Tirtha Majumder, Rajiv Kumar Mishra, S. S. Singh School of Electronics Engineering KIIT University Bhubaneswar, Odisha, India , Cognitive Radio is an emerging technology that offers optimal use of spectrum. It is regarded as the best technology for reliable communication and data application in wireless networks.

"Spectrum Sensing in Cognitive Radio Applications": According to Vatsala Sharma, Dr. Sunil Joshi, Department of Electronics & Communication Engineering, College of Technology And Engineering, CTAE, MPUAT, Udaipur, Rajasthan, India. Cognitive radio is a promising technology to meet the requirements of efficient usage of limited available frequency spectrum for next generation technology and demand for high data transmission.

"Spectrum Sensing in Cognitive Radio Applications": According to Adrian Popescu Dept. of Communications and Computer Systems School of Computing Blekinge Institute of Technology 371 79 Karlskrona, Sweden, Cognitive Radio Networks (CRNs) are emerging as a solution to increase the spectrum utilization by using unused or less used spectrum in radio environments. The basic idea is to allow unlicensed users access to licensed spectrum, under the condition that the interference perceived by the licensed users is minimal.

III. Problem statement:

The main purpose of the CR is to realize dynamic access to the idle spectrum in order to have communication. However, implementation of a cognitive radio is a challenging task. A typical cognitive radio scenario consists of SUs that co-exist with the PUs. PU has a priority to use the spectrum as they have legacy rights for the spectrum access. SU opportunistically access the spectrum when they find that PU is not using the spectrum or underlay access to the spectrum, when both PU and SU co-exist, with strict constraint over non-interference among the users. The main issues of CR are as under-

Spectrum Sensing - Spectrum sensing is the important function of the CR is to sense the radio environment in order to detect the idle channels (or spectrum hole) and use these idle channels for its communication.

Spectrum Management - Spectrum management helps in finding the best idle channels or hole for the transmission of SU among large number of available spectrum holes.

Spectrum Mobility - Spectrum mobility is the process of switching the spectrum band during data transmission due to arrival of PU on that band.

Spectrum Sharing - Spectrum sharing is an important functionality of CR as it coordinates the traffic between secondary and primary users. It is a challenging task as it requires high degree of cooperation, understanding and coordination between primary and secondary users.

IV. Objectives:

In this project work, the main objective is to increase the utilization of CRN. I will use the game theoretic approach for my project work.

- Detect security attack in CRN.
- Prevent the CRN from security attack.
- Performance analysis after using the game theoretic approach.

V. Proposed Algorithm:

I consider a CRN with one normal SU and one jammer. I assume that the spectrum band is divided into three channels –channel 1, channel 2 , channel 3 and the system is time slotted. I propose a game where players are jammer and the normal SU. Normal SU will be present either in channel 2 or channel 3 and jammer will be present either in channel 1 or channel 2.According to my assumption the channel 2 has the higher bandwidth than other two channels. So, my proposed game will be used to decide whether channel 2 can be chosen by the normal SU or jammer for the next time slot.Also the aim of the game is to maximize the utility of the SU (by choosing Channel-2 as frequently as possible) even though jammer could be present in many instances.Such an opportunistic usage of Channel 2 based on a probability calculation, will lead to a higher bandwidth availability for the normal SU since using channel 2 gives higher payoff due a the availability of a larger bandwidth in channel 2. There are two possible actions—Present and absent. According to the actions, the utility functions for both the players are as follows:

1. When Jammer and normal SU Both are present:

U(Normal SU)=(1-Pj)*B-Cs*Pj

U(Jammer)=B*Pj

2. When jammer present and SU absent:

U(Normal SU)=0

U(Jammer)=B*Pj

3. When SU present and Jammer absent:

U(Normal SU)= B*(1-Pj)-Cs*Pj

U(Jammer)=0

4. When SU present and Jammer absent:

U(Normal SU)=0

U(Jammer)=0

Algorithm:

1. Initially, both normal SU and Jammer might be present in channel 2 a with a probability of 50%.

2. At each time slot t

- Each player n_i selects the action e ∈{Present, Absent} with probability pj(e, t)
- Each player computes the utility U(e, t) for the selection of action e at time slot t.

3. Each user i approximates the average utility for action e within the past T time slots
(including slot t),which can be expressed as $U_i(e)$; each user i also approximates the average utility of the mixed actions (all the actions) U_i in the past T slots. If there are less than T − 1 slots in the past, all slots need to be considered.

The probability of user n_i selecting the action e ∈{Present, Absent} for the next time slot can be computed as
$Pi(e,(t+1))=Pi(e,t)+ \eta_{j*}[U_i(e)-U_i]*P_i(e,t)$

Afterwards we vary the number of time slots and the probability of the presence of jammer to analyse the percentage of choosing Channel 2 for both the players, using the proposed algorithm.

		Normal SU	
		Present	Absent
Jam mer	Present	$B*P_j,(1-P_j)*B-Cs*P_j$	$B*P_j$,0
	Absent	$(1-P_j)*B-Cs*P_j$	0,0

Two player game

VI. Software / Platform:

MATLAB is a high-level language and interactive environment for numerical computation, visualization, and programming. Using MATLAB, we can analyze data, develop algorithms, and create models and applications.

The language, tools, and built-in math functions enable you to explore multiple approaches and reach a solution faster than with spreadsheets or traditional programming languages, such as C/C++ or Java. We can use MATLAB for a range of applications, including signal processing and communications, image and video processing, control systems, test and measurement, computational finance, and computational biology. More than a million engineers and scientists in industry and academia use MATLAB, the language of technical computing.

VII. Result and Analysis:

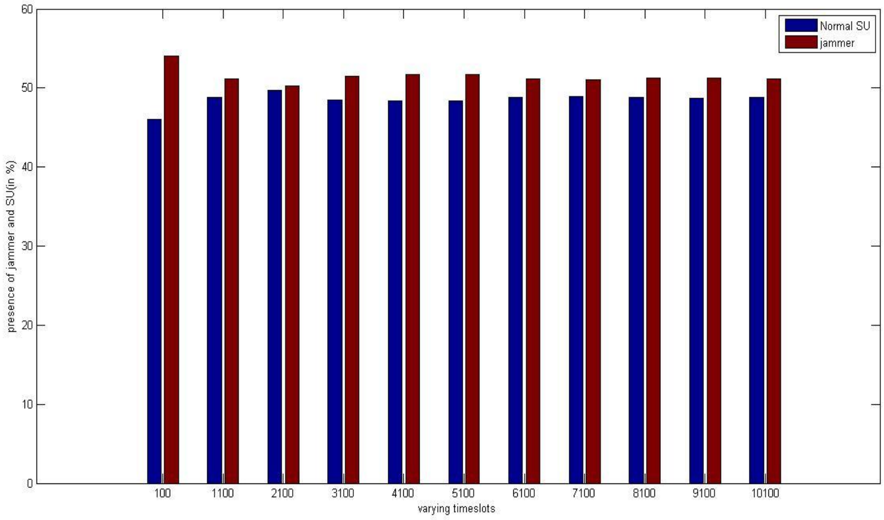

Figure 11:varying time slot, fixed probability presence of jammer (0.6) after one iteration

Figure 11 shows the presence of normal SU and jammer in channel 2 when the probability of presence of jammer is 0.6. I plotted the graph after one iteration with varying time slots from 100 to 10100.Here the 'blue' and 'red' bars indicate the occupancy of the channel by a Normal SU and a Jammer respectively. If the probability of presence of jammer in channel 2 is 0.6 then 60% of the time the jammer may be present in channel 2. So, the normal SU should get at most 40% chance to utilize the channel 2. But, for the evolutionary game, which i proposed, the utilization of channel 2 has increased.

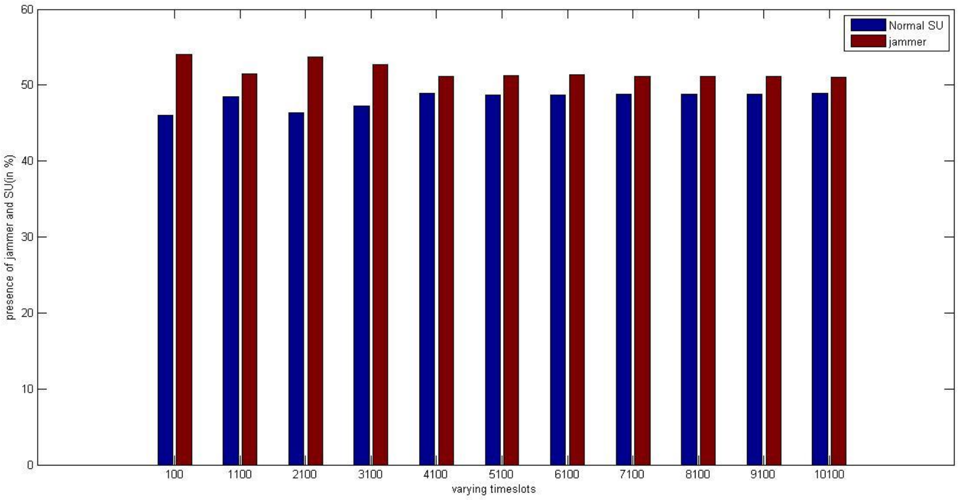

Figure 12: varying time slot, fixed probability presence of jammer (0.6) after 100 iterations

Here, i have followed the same procedure as described in Figure 11 for 100 iterations to analyze the result and i got approximately same result.

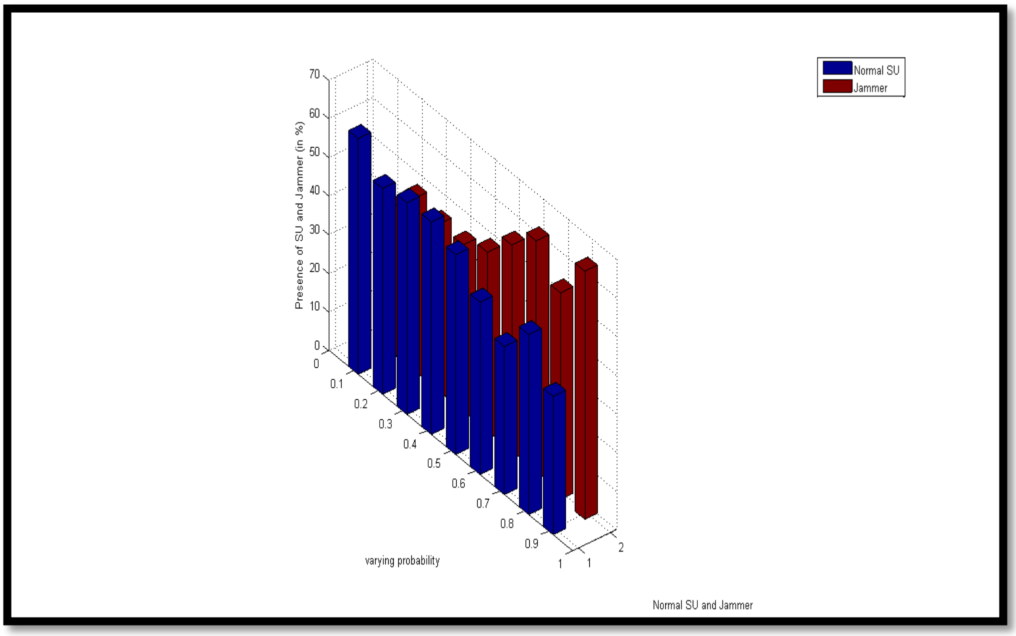

Figure 13 : Fixed time slot, varying probability of presence of jammer (after 1 iteration)

I have observed the result with fixed time slot and varying probabilities of the jammer being present (from 0.1 to 0.9).The graph clearly indicates that when the probability of presence of jammer increases, the scope of channel 2 being chosen by the normal SU decreases, which is an expected behaviour. However, because of my proposed algorithm, the normal SU still manages to use the common channel as much as possible.

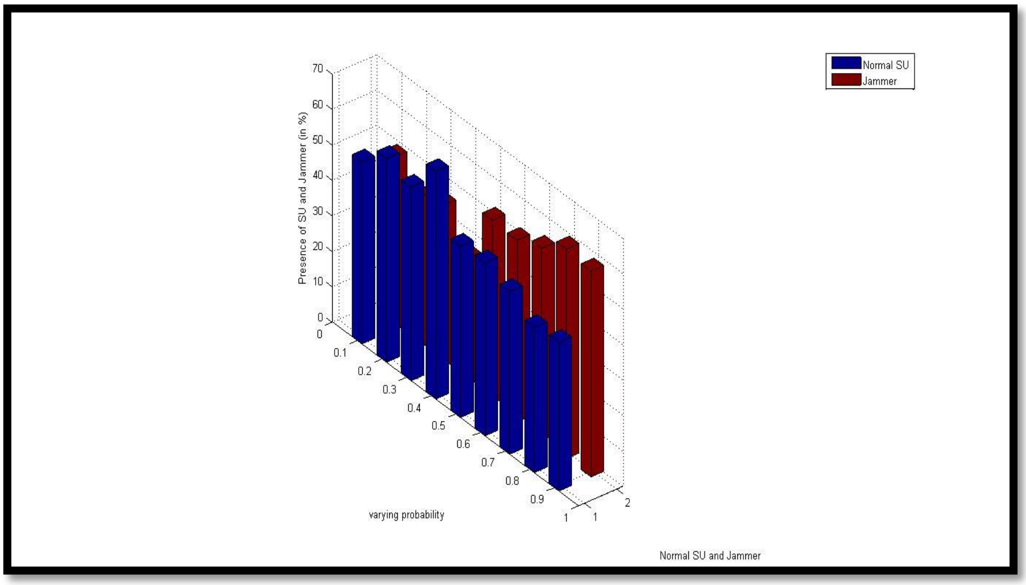

Figure 14 : Fixed time slot, varying probability presence of jammer (after 100 iteration)

To analyze the result more precisely i used the same procedure like Figure 13 for 100 iterations and i got the result as shown in Figure 14.It has shown approximately same result as Figure 13.

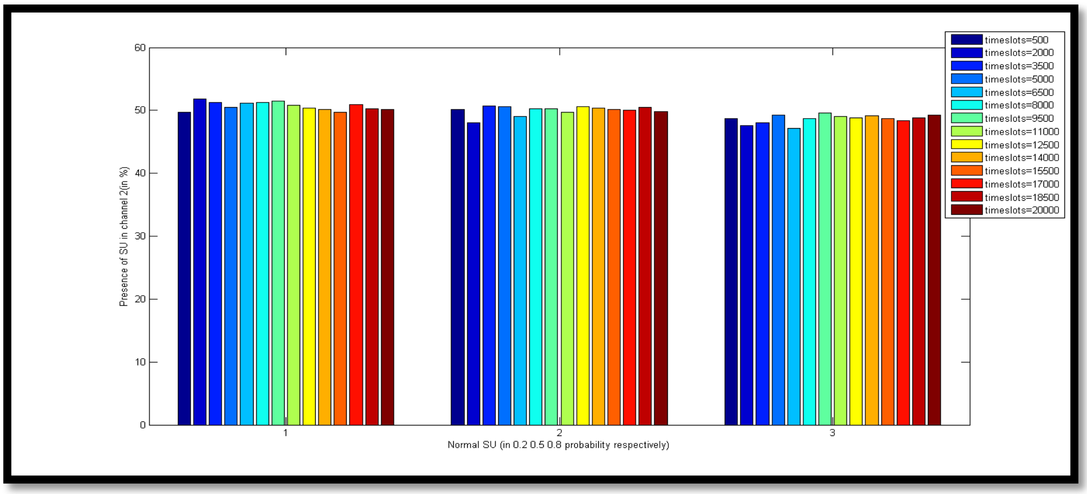

Figure 15: varying timeslots and varying probability

Next, the simulation was run to see the channel 2 occupancy by the normal SU for varying probabilities of the jammer being present (0.2, 0.5 and 0.8) and varying time slots (from 500 to 20000). As is evident from Figure 15, the normal SU manages to use the contending channel at least 50% of the times, irrespective of the different probabilities of the jammer being present. Also, the algorithm seems to converge around 9500 time slots. This indicates that for our proposed algorithm to run successfully, 10,000 time slots are sufficient.

II. Conclusion

A secure CRN is needed to utilize the spectrum. For that, an evolutionary game theoretic approach will be implemented so that in spite of presence of attacker the utilization of the network will increase. In this project, i proposed a an idea based on evolutionary game theory, which helps a SU to decide which channel to use when it is presented with two channels and one channel being intermittently jammed by a malicious user.

Future work

My setup had some limitations due to which i could not attain the best possible result. So, my suggestion for the future work is to overcome those limitations mentioned below:

1) For simplicity i am assuming only one SU. Further study is required to examine the presence of more SUs.

2) Only three channels were assumed. This can be further extended to include higher number of channels.

References

[1]. “Primary User Emulation Attack in Cognitive Radio Networks: A Survey”byDeepa Das and Susmita Das, Department of Electrical Engineering, NIT, Rourkela, India, JUNE 2013

[2]. “CODES: A Collaborative Detection Strategy for SSDF Attacks in Cognitive Radio Networks” byAmarTagguNERIST,Nirjuli, IndiaNERIST,Nirjuli, India Ningrinla Marchang NERIST Nirjuli, India , AUGUST 2015

[3]. A Credibility based Defense SSDF Attacks Scheme for the Expulsion of Malicious Users in Cognitive Radio” By-Hong Du, ShuangFu and HongnaChu, 2015

[4]. “Can Clustering be Used to Detect Intrusion During Spectrum Sensing in Cognitive Radio Networks?” by KennongRina, ShikhamoniNath, NingrinlaMarchang, Member, IEEE, and Amar Taggu, Member, IEEE 2016

[5]. “Dogfight in Spectrum: Combating Primary User Emulation Attacks in NOVEMBER 2010

[6]. “Open Research Issues in Multi-Hop Cognitive Radio Networks ShamikSengupta, John Jay College of Criminal Justice”- K. P. Subbalakshmi, Stevens Institute of Technology, APRIL 2013

[7]. “Cognitive Radio Networking and Communications: An Overview” by Ying-Chang LiangFellow, IEEE, Kwang-Cheng Chen, Fellow, IEEE, Geoffrey Ye Li, Fellow, IEEE, and Petri Mähönen, Senior Member, IEEE.SEPTEMBER2011

[8]. “An Effective Emitter-Source Localisation-based PUEA Detection Mechanism in Cognitive Radio Networks”- Dikita Salam NERIST, Nirjuli Arunachal Pradesh, India, Amar Taggu, NingrinlaMarchang NERIST, Nirjuli Arunachal Pradesh, India.SEPTEMBER2016

[9]. “Performance of Cooperative Spectrum Sensing with Censoring of Cognitive Radios in Rayleigh Fading Channel” by SrinivasNallagonda Dept. of Electronics & Communication Engineering National Institute of Technology, Durgapur Durgapur - 713209, India.JANUARY 2012

[10]. **“**Security Challenges in Cognitive Radio Networks” by HanenIdoud , Kevin Daimi, and Mustafa Saed.JULY 2014

[11]. “ A Stochastic Game Model for Jamming in Multi-Channel Cognitive Radio Systems” byQuanyan Zhu, Husheng Li, Zhu Han and Tamer Bas.AUGUST 2014

[12]. “Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks” by Z. Jin, S. Anand and K. P. Subbalakshmi Department of Electrical and Computer Engineering Stevens Institute of Technology, New Jersey, USA. 2009

[13]. “Survey of Security Issues in Cognitive Radio Networks” byWassim El-Hajj, Computer Science Department, American University of Beirut, Lebanon HaidarSafa, Mohsen Guizan, Computer Science Department, Western Michigan University, USA .APRIL 2015

[14]. "Attack and Surveillance Strategies for Selfish Primary User Emulator in Cognitive Radio Network". Nhan Nguyen-Thanh, Philippe Ciblat, Anh T. Pham, and Van-Tam Nguyen, Department of Communications and Electronics, Telecom ParisTech, France, 2014

[15]. "Game theory for cognitive radio networks: An overview" by Beibei Wang *, Yongle Wu, K.J. Ray Liu Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USAOCTOBER, 2010

[16]. "A Zero-Sum Game based Approach for Primary User Emulation Attack in Cognitive Radio Network" by Dong Hao,Kouichi Sakurai, Graduate School of Information Science and Electrical Engineering, Kyushu University.June 2013

[17]. "Introduction to Evolutionary Game Theory" by Marco TomassiniUniversity of Lausanne Lausanne, Switzerland.JULY 2014

[18]. "Repeated zero-sum games with budget" -TroelsBjerreSørensen University of Warwick CV4 7AL, United Kingdom.

[19]. "Game-theoretic Distributed Spectrum Sharing for Wireless Cognitive Networks with Heterogeneous QoS" by Tao Jin, ChunxiaoChigan, and ZhiTian Department of Electrical and Computer Engineering Michigan Technological University, Houghton, MI 49931 USA.