Analysis of Cognitive Radio Networks with Security Awareness Employing Channel Sensing

Prof. Anubhav Pandey[1] Deepak Dwivedi[2]
[1]Professor & Head of Dept. [2]Scholar
[1,2]Department of Electronics & Communication Engineering
[1,2]JNCT, Rewa M.P., India

Abstract— Cognitive radio networks (CRNs) have a great potential in supporting time-critical data delivery among the Internet of Things (IoT) devices and for emerging applications such as smart cities and automation. A wireless channel (radio) about which we have information is called a cognitive radio. However, Cognitive Radio Networks share common resources such as bandwidth or spectrum among several users or stations. Due to continued sharing of resources, cognitive networks often come under security attacks, most common of which are jamming attacks. In the case of jamming attacks, deliberately designed random jamming signals are added to the channel. These jamming signals along with noise result in packet losses and low throughput, degrading the overall performance of the cognitive network. In this work, a security aware jamming rejection mechanism is proposed which detects suspicious signals in the channel frequency response and employs discrete equalization to recover transmitted data. Moreover, this also reduces the effects of noise in the channel. The probability of false alarm has been analyzed with respect to the energy threshold. It has been shown that the probability of false alarm reduced with increase in the energy threshold. A comparative analysis of the proposed work and the previous work [3] shows that the proposed system outperforms the previous work in terms of throughput when analyzed with respect to jamming power and jamming interval. Thus it has been proven that the proposed methodology has been effective in mitigating the effects of the security threats arising out of the jamming activity by possible adversaries. An analysis of probability of false alarm with respect to the energy threshold for energy sensing has also been shown in which it can e clearly shown that as the threshold is lowered, the chances of false alarm increases and vice versa.

Keywords: Cognitive Radio Networks (CRNs), Internet of Things (IoT), Wireless Channel (Radio)

I. INTRODUCTION

A. Cognitive Networks

Cognitive networks are networks are the type of networks that show the attributes of leverage the channel state info for the use of resources like information measure and energy. the main challenge with cognitive systems comprising of cognitive networks is that the undeniable fact that finding the channel state info with high accuracy is usually very advanced in nature. The random nature of the medium or channel makes is very tough to assess truth nature of the channel that is usually time variant in nature. primarily the Cognitive feature networks are comprised of the subsequent activities:

1) Sense channel or radio surroundings
2) Obtain the channel state info (CSI)
3) Share spectral resources
4) Take selections concerning network security
5) Repeat the method of channel sensing.

The higher than mentioned ideas are exemplified victimization the subsequent diagram. The diagram shows a typical cognitive radio environment.

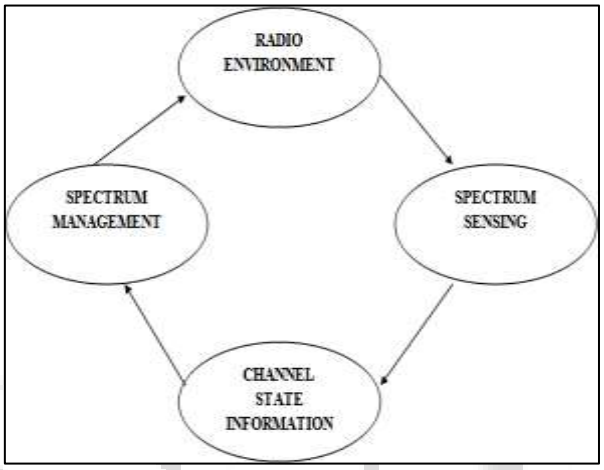


Fig. 1.1: Basic Functions of Cognitive Networks

B. Security Aware Cognitive Networks

Security aware cognitive networks are those cognitive networks which rely on the channel state information (CSI) for the detection of jamming attacks by possible adversaries. The channel state information is typically the frequency response of the channel. Based on the channel state information, the jamming activity can be categorized into 3 groups:

1) Low jamming activity
2) Moderate jamming activity
3) High jamming activity.

C. Advantages and Disadvantages of Cognitive Networks

1) Advantages

- Enhanced reliability of networks
- Lesser cost
- Advances network topologies simpler to implement
- Advanced Software Defined Radio (SDR)
- Better resource management

2) Disadvantages

- Dependency on SDR.
- Uncontrolled situations for system mutations.
- Concerns regarding regulation
- Enhanced adaptability
- Security threats

D. Objective

The main objective of the proposed work is to mitigate the effects of jamming and eavesdropping attacks by possible

adversaries. This can be done by sensing the channel which is wireless in nature often termed as radio. The distinction between the channel or radio being affected by attacks or not is to be decided based on the channel state information. This in turn needs the use of energy detection. The energy detection mechanism is to be used to find deviations in the average energy of the channel or radio depending on the baseline value. The mitigation of the problem can be done if sub-carriers affected by the jamming attacks are rejected completely termed as tone rejection. The throughput is to be enhanced in this case. The proposed work holds grounds if the throughput performance is better compared to existing systems.

II. LITERATURE REVIEW:

1) Haythem Bany et al. proposed a time critical approach based network. This network was cognitive in nature thereby sensing the channel and utilizing the channel state information (CSI). The applications of the proposed system could be found in Internet of Things (IoT) based applications. The authors proposed that security aware cognitive networks are those cognitive networks which rely on the channel state information (CSI) for the detection of jamming attacks by possible adversaries. The channel state information is typically the frequency response of the channel. Based on the channel state information, the jamming activity can be categorized into 3 groups i.e. low jamming activity, moderate jamming activity and high jamming activity.]
2) K. J. Prasanna et al. proposed a reliable and secure architecture for routing in cognitive networks. The approach used the channel state information or the frequency response of the channel to detect possibly malicious activity. The routes were dynamically adjusted based on the condition of the network. The main objective of the proposed work was to mitigate the effects of jamming and eavesdropping attacks by possible adversaries. This can be done by sensing the channel which is wireless in nature often termed as radio.
3) Keke Gai et al. the authors used the cloud platform to implement their approach. The use of big data analytics was also used for a mass storage system that was using the concept of cognitive networks and hence was security aware in nature. The major challenge in this approach was to limit the data usage due to the enormous data size based on cloud and the big data frameworks. The throughput of the system was the governing factor.
4) Ju Ren et al. proposed techniques based on collaborative resource sharing in cognitive networks. This technique is used for the energy detection mechanism and senses the energy of the channel at any given point of time. The hypothesis that governs this technique is the fact that jamming or attacks would definitely or invariably alter the spectral properties of the cognitive network. This would in turn make the attack or the eavesdropping perceptible.
5) Rajesh K. Sharma et al. presented a survey on the measures of security threats for cognitive networks as cognitive networks are prone to attacks as their functioning was governed by the channel state information. This can be done by sensing the channel which is wireless in nature often termed as radio. The distinction between the channel or radio being affected by attacks or not is to be decided based on the channel state information. This in turn needs the use of some effective detection mechanism.
6) Maged Elkashlan et al. proposed a technique to assure the security of cognitive networks. It was shown that the more the average deviation from the standard channel state energy, the more were the chances of attacks. Security aware cognitive networks are those cognitive networks which rely on the channel state information (CSI) for the detection of jamming attacks by possible adversaries. The idea was a more general and holistic development of a security mechanism.

III. PROBLEM FORMULATION:

A. Main Challenges in Cognitive Networks

Main Challenges faced in Spectrum Sensing in Cognitive Radio Systems:

- Wireless channels change randomly over time, therefore sensing wireless channelsbefore they change is tough.
- Determining jamming activity may be tough due to the addition of noise.
- Due to addition of noise in the transmitted signal, detection of spectrum holes may bepractically tough
- Due to dynamic spectrum allocation, there exists a chance of 'Spectrum Overlap' causing interference between users.
- Designing cognitive radio systems to perform error free in real time may be complexto design i.e. reduced throughput of the system. (bits/sec)

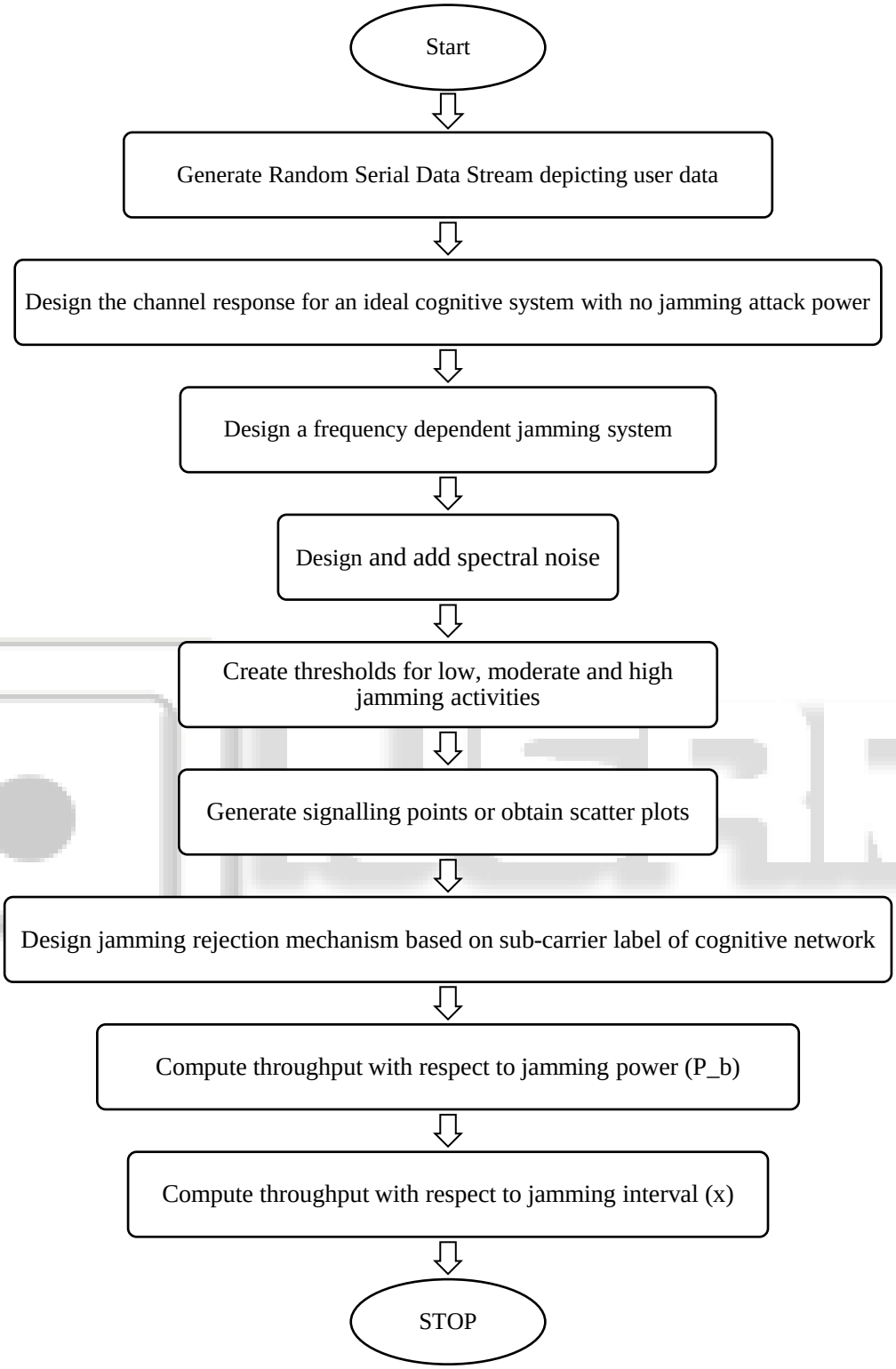
B. Challenges in Utilizing CSI for Enhanced Throughput and Probability of False Alarm

- The major problem that security aware cognitive channels face is the low throughputperformance due to lost or corrupt data packets. This primarily happens due to:
- Wireless nature of network
- Frequent sharing of spectrum by users
- Addition of noise in channel degradation
- Achieving high throughput and security at the same time

However, the need for spectrum sensing for security aware system s lie in the fact that:

- Cognitive radio networks are prone to attacks because of wireless nature of thechannel
- Jamming attacks are the most common form of attacks in cognitive networks, since itis not easy to break high complexity encryption in time-critical situations.
- Security aware networks can detect possible jamming attacks which can help indecoding data at receiving end with higher accuracy and high throughput.

IV. PROPOSED METHODOLOGY



V. RESULTS AND DISCUSSIONS

The results have been obtained using MATLAB. The various graphs obtained under the proposed system have been shown in the following section and the inferences are explained subsequently.

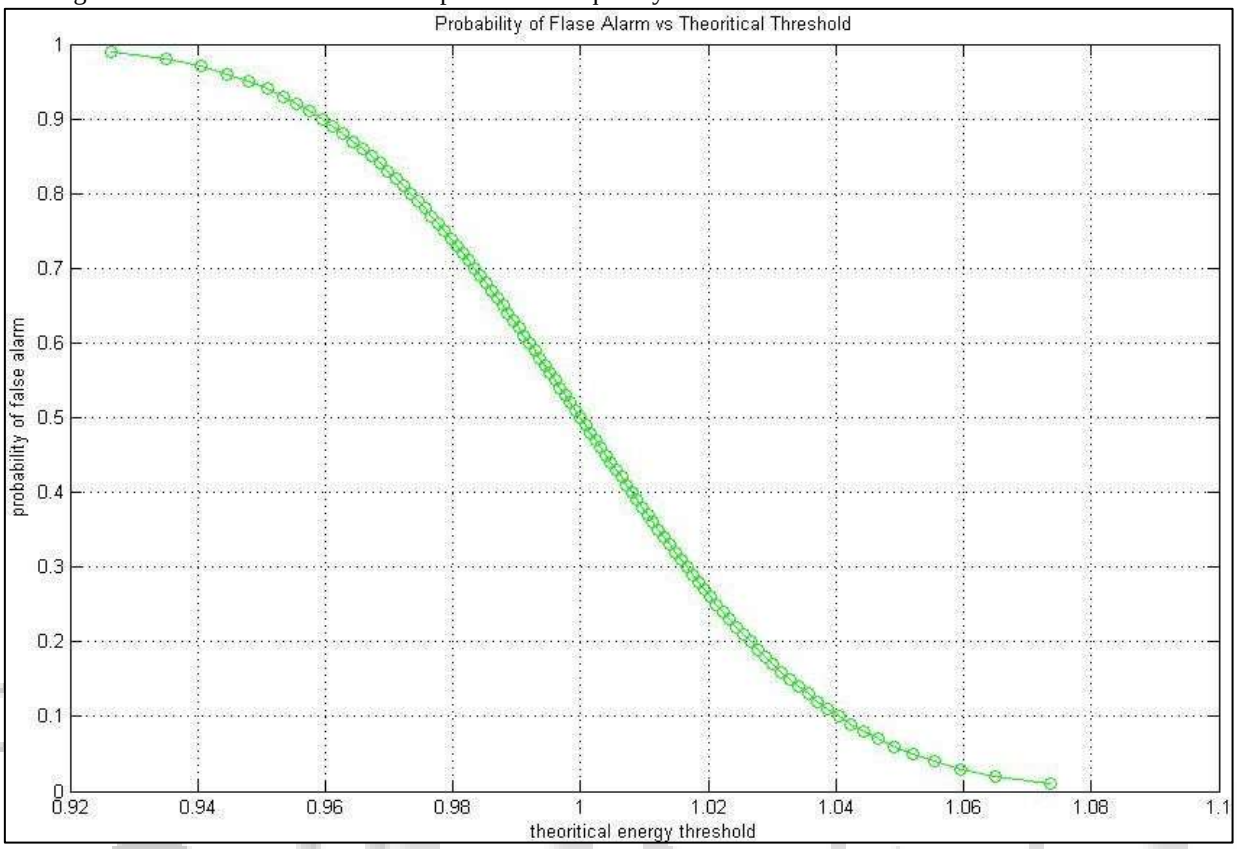


Fig. 5.1: Probability of False Alarm w.r.t. Energy Threshold

Fig.5.1 explains the probability of attaining a false alarm as the energy threshold for detecting a hole varies.

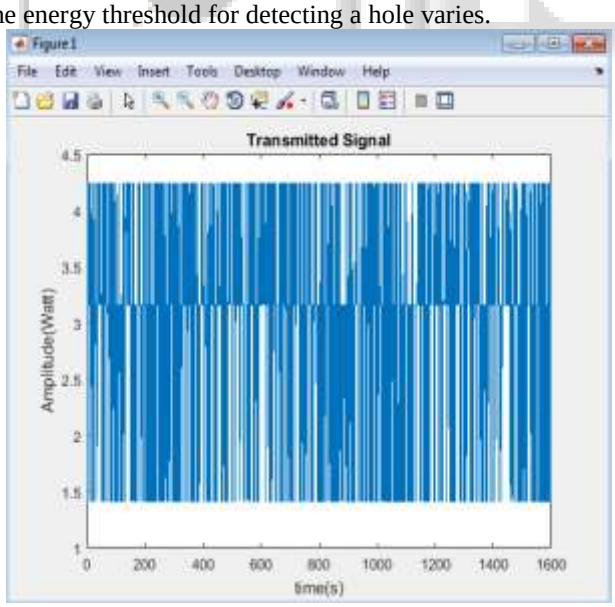


Fig. 5.2: Transmitted binary signal

Fig.5.2 depicts the binary discrete signal that is transmitted from the transmitting end of the Cognitive Network.

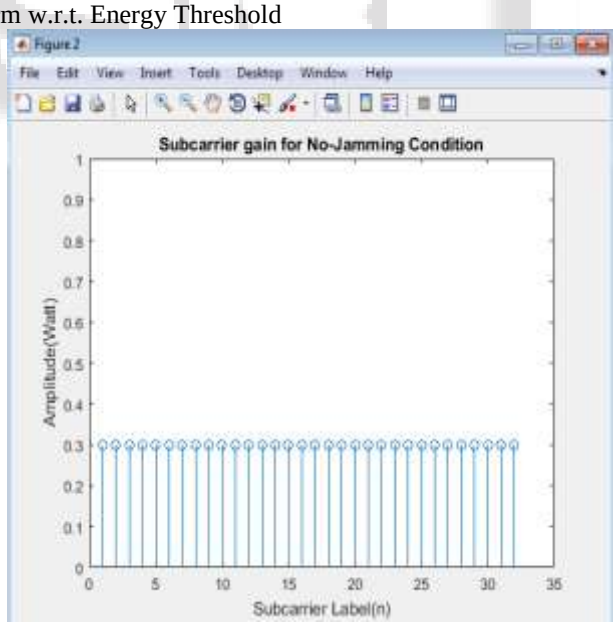


Fig. 5.3: Subcarrier Gain for Non-Jamming Condition

Fig.5.3 depicts an ideal flat channel i.e. a channel with an ideal channel gain characteristic.

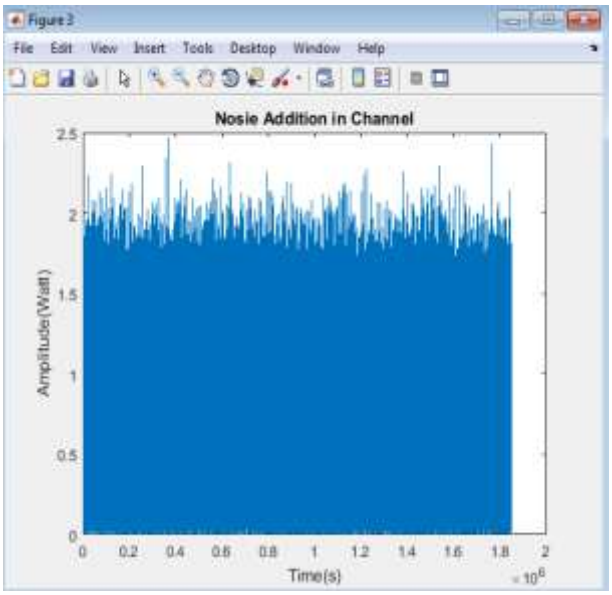


Fig. 5.4: Addition of Noise in the Channel

Fig.5.4 depicts the addition of noise in the channel which is completely random in nature.

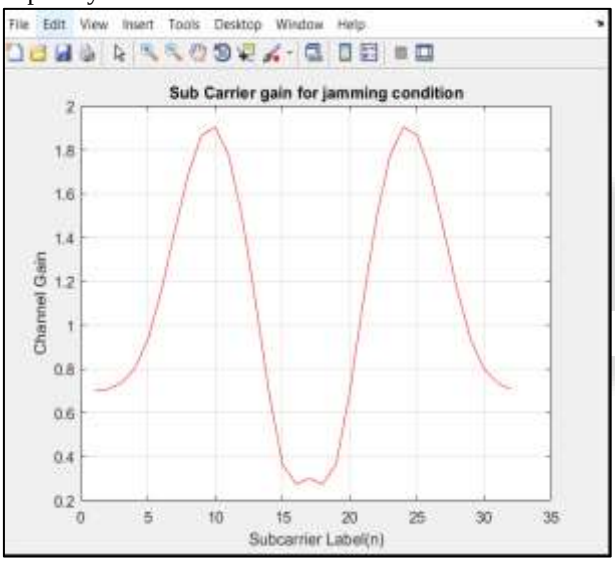


Fig. 5.5: Subcarrier Gain for Jamming Condition

Fig.5.5 depicts the subcarrier label of the network in terms of the channel gain of the system.

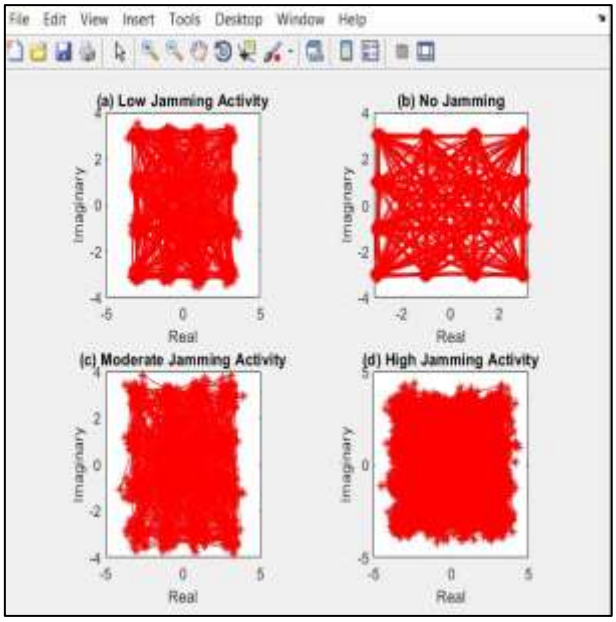


Fig. 5.6: Scatter Plot for Different Jamming Conditions

Fig.5.6 depicts the scatter plots for the various jamming conditions. It can be seen that the jamming conditions result in maximum scatter.

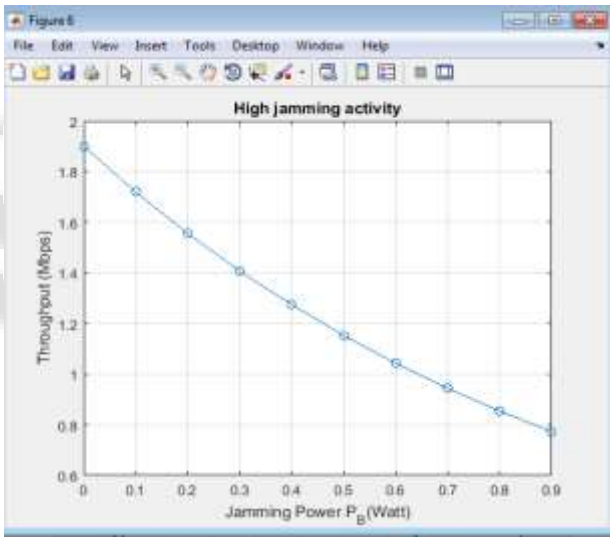


Fig. 5.7: Throughput for High Jamming Conditions

Fig.5.7 depicts the throughput for sensed high jamming activity in the channel corresponding to the cognitive radio network.

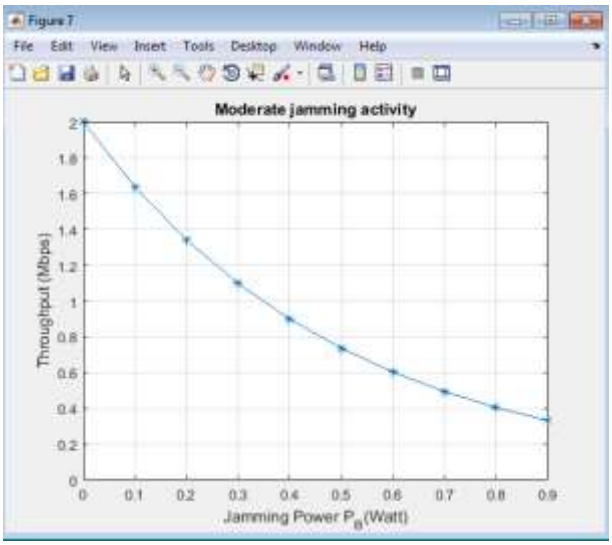


Fig. 5.8: Throughput for Moderate Jamming Conditions

Fig.5.9 depicts the throughput for sensed moderate jamming activity in the channel corresponding to the cognitive radio network.

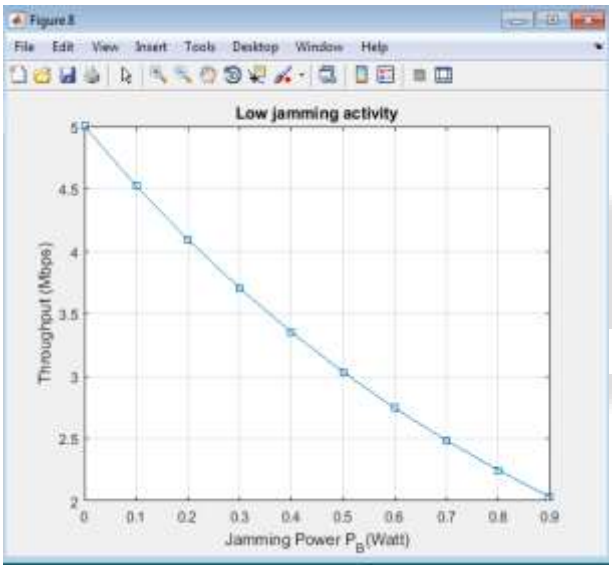


Fig.5.9 Throughput for Low Jamming Conditions

Fig.5.9 depicts the throughput for sensed low jamming activity in the channel corresponding to the cognitive radio network.

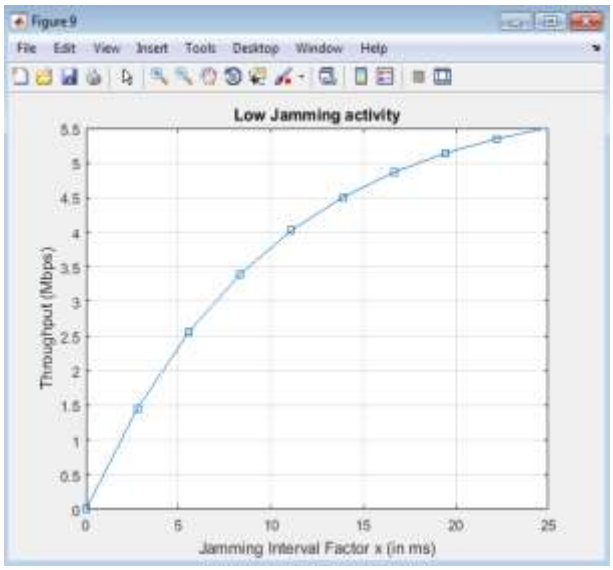


Fig. 5.10: Throughput Analysis with respect to jamming interval (low jamming)

Fig.5.10 depicts the throughput w.r.t. the jamming interval for the cognitive network under low jamming condition which can be utilized for transmission.

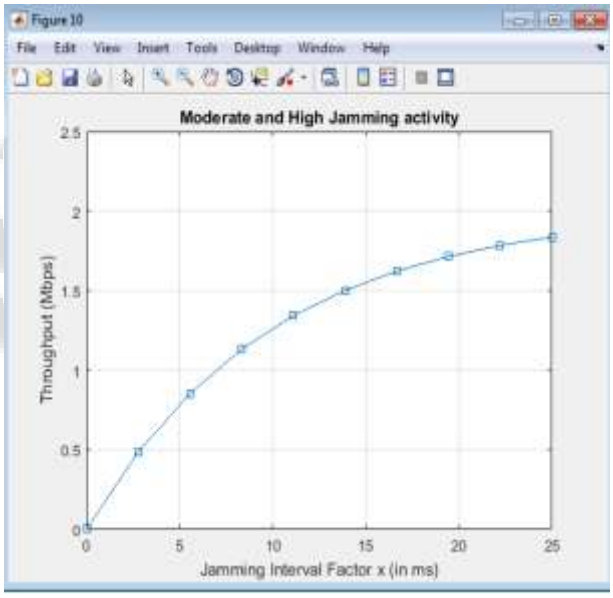


Fig.5.11 Throughput Analysis with respect to jamming interval (moderate and high jamming)

Fig.5.1 depicts the throughput w.r.t. the jamming interval for the cognitive network under moderate and high jamming condition which can not be utilized for transmission due to chances of low throughput and high errors.

VI. CONCLUSIONS

It can be concluded from previous discussions that cognitive radio has emerged as one of the key enablers in high data rate in wireless technology. Cognitive Radio is no more just an extension of Software Defined radio but in conjugation with Channel Sounding and OFDM, can lead to much higher data rates even at substantially low levels of Bit Error Rate (BER) or Probability of Error (Pe). In the present work, a novel technique for Throughput improvementhas been suggested which employs the use of the Channel State Information (CSI) using the data provided by energy detection. It has been

assumed here that the channel sounding information has taken into account the frequency selective nature of practical wireless channels, i.e. to say the channel impulse response in the time domain or the channel frequency response in the frequency domain has been sampled quicker than the channel changes over time. A multi carrier system has been considered in which there are several carriers with varying amount of sub-carrier gain in the practical channel. It is the very nature of a frequency selective practical wireless channel that it would attenuate or fade off different frequencies of a multi carrier communication scheme. In the present work, security awareness of the channel is implemented using the jamming activity in 3 cases:

- Low Jamming
- Moderate Jamming
- High Jamming

The attributes have been presented based on the scatter plots. The discrete channel equalization mechanism has been implemented using the real and imaginary parts of the signalling points often referred to as scatter plots.

Finally the throughput comparison with base paper has been presented. A comparative analysis of the proposed work and the previous work [3] shows that the proposed system outperforms the previous work in terms of throughput when analyzed with respect to jamming power and jamming interval. Thus it has been proven that the proposed methodology has been effective in mitigating the effects of the security threats arising out of the jamming activity by possible adversaries.

REFERENCES:

[1] Lei Xu , Arumugam Nallanathan ,Xiaofei Pan, Jian Yang ,Wenhe Liao, "Security-Aware Resource Allocation With Delay Constraint for NOMA-Based Cognitive Radio Network", IEEE 2018
[2] Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani," NS-2 based simulation framework for cognitive radio sensor networks", SPRINGER 2018
[3] Haythem Bany Salameh ,Sufyan Almajali ,Moussa Ayyash ,Hany Elgala, "Security-aware channel assignment in IoT-based cognitive radio networks for time-critical applications", IEEE 2017
[4] K. J. Prasanna Venkatesan ,V. Vijayarangan, "Secure and reliable routing in cognitive radio networks",SPRINGER 2017
[5] Keke Gai ,Meikang Qiu ,Hui Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data",IEEE 2016
[6] Ju Ren ,Yaoxue Zhang ,Qiang Ye , Kan Yang ; Kuan Zhang ,Xuemin Sherman Shen," Exploiting Secure and Energy-Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks", IEEE 2016
[7] Rajesh K. Sharma ;,Danda B. Rawat," Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey",IEEE 2015
[8] Maged Elkashlan ,Lifeng Wang ,Trung Q. Duong , George K. Karagiannidis ,Arumugam Nallanathan, "On the Security of Cognitive Radio Networks",IEEE 2015
[9] Erol Gelenbe," A Software Defined Self-Aware Network: The Cognitive Packet Network", IEEE 2014
[10] Mahmoud Khasawneh ,Anjali Agarwal," A survey on security in Cognitive Radio networks", IEEE 2014
[11] Yulong Zou, Xianbin Wang ,Weiming Shen," Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks",IEEE 2013
[12] Muhammad Faisal ,Amjad,Baber Aslam ,Cliff C. Zou, ," Reputation Aware Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks", IEEE 2013
[13] Gianmarco Baldini ,Taj Sturman ,Abdur Rahim Biswas ,Ruediger Leschhorn ,Gyozo Godor ,Michael Street," Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead", IEEE 2012
[14] Alvaro Araujo ,Javier Blesa,Elena Romero,Daniel Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems", SPRINGER 2012
[15] Yiyang Pei ,Ying-Chang Liang, Kah Chan Teh ,Kwok Hung Li, "Secure Communication in Multiantenna Cognitive Radio Networks With Imperfect Channel State Information", IEEE 2011
[16] Ying-Chang Liang ,Kwang-Cheng Chen ,Geoffrey Ye Li ,Petri Mahonen, "Cognitive radio networking and communications: an overview", IEEE 2011
[17] Gayathri Vijay ,Elyes Bdira ,Mohamed Ibnkahla, "Cognitive approaches in Wireless Sensor Networks: A survey", IEEE 2010
[18] Sazia Parvin ,Song Han ,Biming Tian ,Farookh Kadeer Hussain, "Trust-Based Authentication for Secure Communication in Cognitive Radio Networks", IEEE 2010
[19] T Qin, H Yu, C Leung, Z Shen, C Miao, "Towards a trust aware cognitive radio architecture" ACM 2009
[20] S Sanyal, R Bhadauria, C Ghosh, "Secure communication in cognitive radio networks", IEEE 2009

