iJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 7 Issue 10 October 2019

Jamming Rejection Mechanism for Security Aware Cognitive Networks using Energy Detection

Nilesh
Department of Electronics and Communication,
UEC, Ujjain (India)

Prof. GirishKumar Tiwari
Department of Electronics and Communication,
UEC, Ujjain (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. It has been shown that the proposed system achieves higher throughput compared to previous techniques for low, moderate and high jamming activity.

Keywords:- Cognitive Radio, Internet of Things (IoT), Jamming Activity, Energy Detection, Equalization, Throughput.

I.Introduction

A Wireless Channel is also called a Radio. The term cognitive is derived from the word Cognizance meaning knowledge or awareness. A radio whose knowledge is

possessed by us is called a Cognitive Radio. Cognitive radio is becoming very popular these days to satisfy the needs of increasing number of users and increased bandwidth needed per user due to multimedia and big data applications. The radio frequency spectrum is a limited that is divided into spectrum bands and is used for multiple applications. Currently, spectrum bands have been apportioned to diverse services, for example, mobile, fixed, broadcast, fixed satellite, and mobile satellite services. Spectrum is allocated to users or service providers and most often requiring licenses for operation, a crucial issue confronting future wireless systems is to discover suitable carrier frequencies and bandwidths to take care of the anticipated demand for future services.

Cognitive Radio (CR) can be defined as a radio or radio frequency spectrum whose cognizance or knowledge is possessed by the user or service provider. The tern cognizance or knowledge can be a little vague at times but the meaning of cognizance of a radio spectrum indicates towards the knowledge of its statistical parameters or channel state information (CSI). The main attribute of Cognitive radio systems is the fact the fact that it utilizes the spare part of the spectrum that is not being utilized by present users and is lying fallow, another aspect of which is resource allocation among networks that utilize cognitive system design.

This paper presents an energy detection based approach for detection of jamming activity for Cognitive Networks. It is been shown that through energy detection and equalization, the proposed system attains higher throughput compared to previous systems.

II. Characteristics of a Cognitive Radio

The major characteristics of cognitive radios are given as:

1) Cognitive ability: It is the ability of Cognitive Systems to sense or catch the data from the radio surroundings of the radio technology. It can be said that cognitive radio constantly observes nature, orients itself, makes plans, decides, and then acts

2) Reconfigurability: It is continuously adapting to the changes in the spectrum that change the properties of the channel. Thus it can be said that it is the utilization of the channel state information. (frequency, transmission power, modulation scheme, communication protocol) of radio.

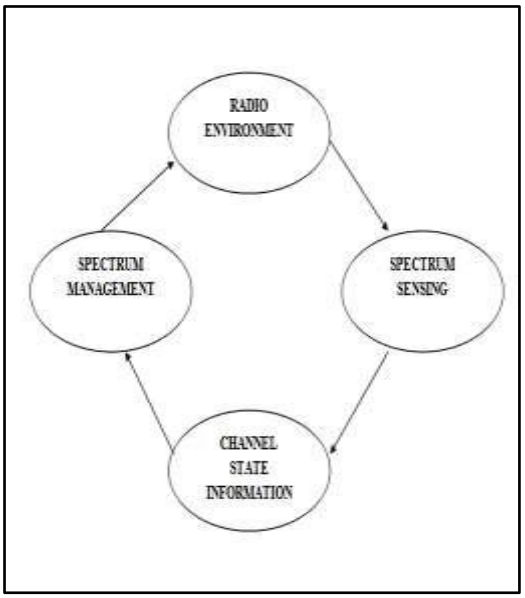

Fig.1 Basic Functions of Cognitive Radio

III. Jamming Activity in Cognitive Radio Systems.

Jamminng attacks are the most common form of attack for cognitive radio mehanisms where the attacker tries to jam the spectrum in order to deny access with high accuracy. This can be categorized in 3 cases:

1) Low jamming activity
2) Moderate Jamming Activity
3) High Jamming Activity

The jamming activity changes the channel response of system from an ideal nature to non-ideal natue. The jamming activity can be gauged based on the channel state information (CSI) of the system. Howeber there are some challenges in utilizing the CSI. Main Challenges faced in Spectrum Sensing in Cognitive Radio Systems:

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

IV. Proposed Algorithm.

The proposed technique can be explained using the following algorithm:

Step1. Generate a random serial data set that is to be transmitted in the form of 0s and 1s.
Let it be given by:
x(n)=random (n); where n is the number of bits are completely random

Step2. Design a typical channel response of an ideal cognitive system.
Let the channel response in time domain be h(t) in the frequency domain, let the channel response be H(f)
H(f)=F.T. {h(n)}
F.T. denotes the Fourier Transform

Step3. Design frequency dependent jamming mechanism.
Let the jamming power be:
Pjam=f(frequency or subcarrier)
here, different frequencies are used for different users in the network, which are also called sub-carriers

Step4. Design and add spectral noise
Design a time domain noise signal n(t)
Add it to the signal in the channel to get
X=S+N

Step5. Detect low, moderate and high jamming action
The decision is to be based on:
Low Jamming Activity: if sub-carrier gain<1.5*Ideal Subcarrier Gain
Moderate Jamming Activity: if sub-carrier gain>1.5*Ideal Subcarrier Gain>2*Ideal Subcarrier
High Jamming Activity: if sub-carrier gain>2*Ideal Subcarrier Gain

Step6. Generate signaling points for the system and obtain the scatter plot for:

- No Jamming Action
- Low Jamming Action
- Moderate Jamming Action
- High Jamming Action

The scatter plots can be plotted for
Re{x(n)}
Img{x(n)}

Step7. Design a jamming rejection mechanism using discrete frequency equalization
This can be done by designing a block with inverse

response as that of the channel

Step8. Compute Throughput for 3 cases:

1) Low Jamming activity
2) Moderate Jamming Activity
3) High Jamming activity

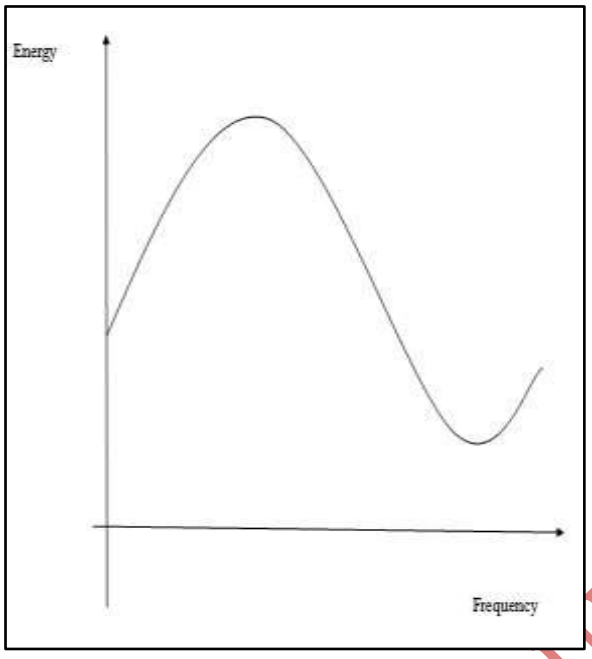

Fig.2 Channel sub-carrier response

The above figure depicts the channel frequency response of a typical wireless channel. It can be seen that it varies with the frequency i.e.

$$H(freg) = f(freq)$$

Here,
$H(freg)$ represents the channel frequency response.
$f(freq)$ denotes a function of frequency.

Results:

The results have been obtained using MATLAB2017a. The various graphs obtained under the proposed system have been shown in the following section and the inferences are explained subsequently.

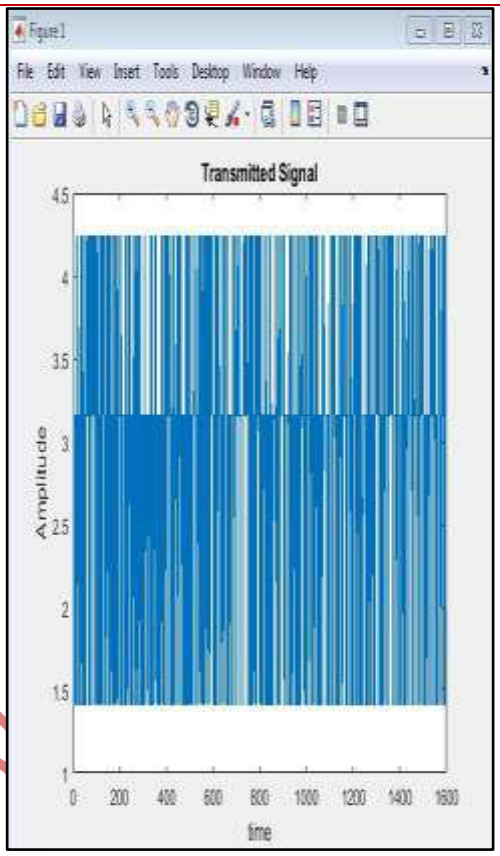

Fig.3 Transmitted binary signal

The above figure depicts the transmitted binary signal in the form of 1s and 0s.

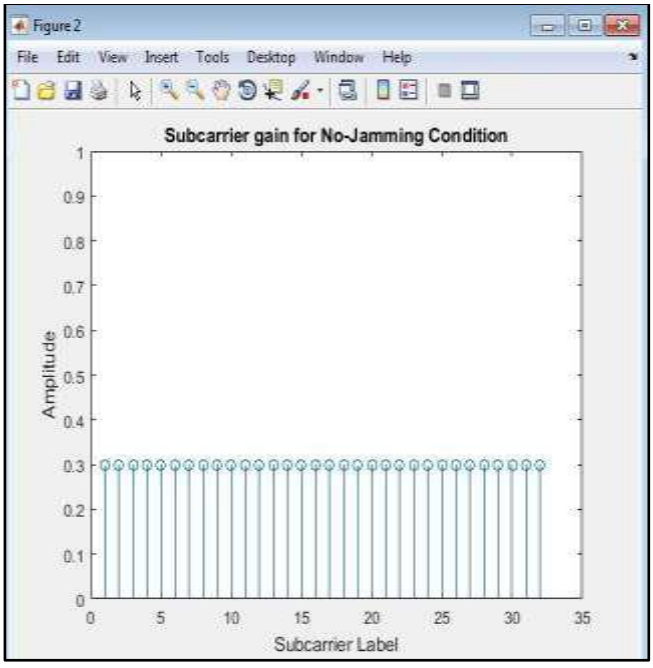

Fig.4 Subcarrier Gain for Non-Jamming Condition

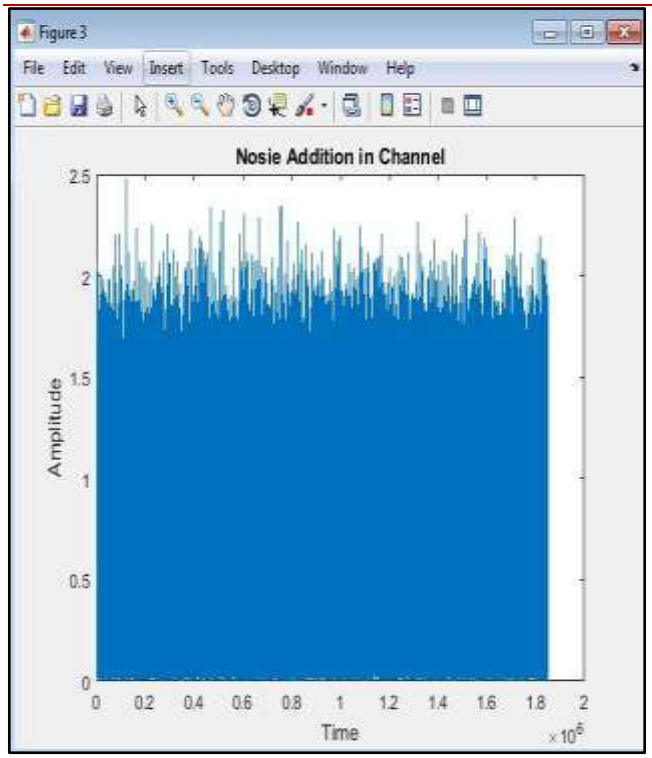

Fig.4 Addition of Noise in the Channel

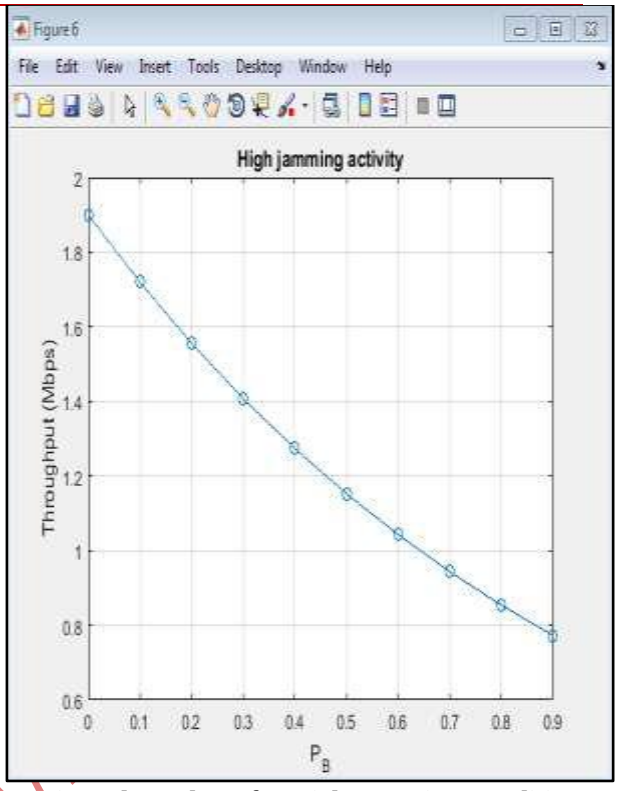

Fig.6 Throughput for High Jamming Conditions

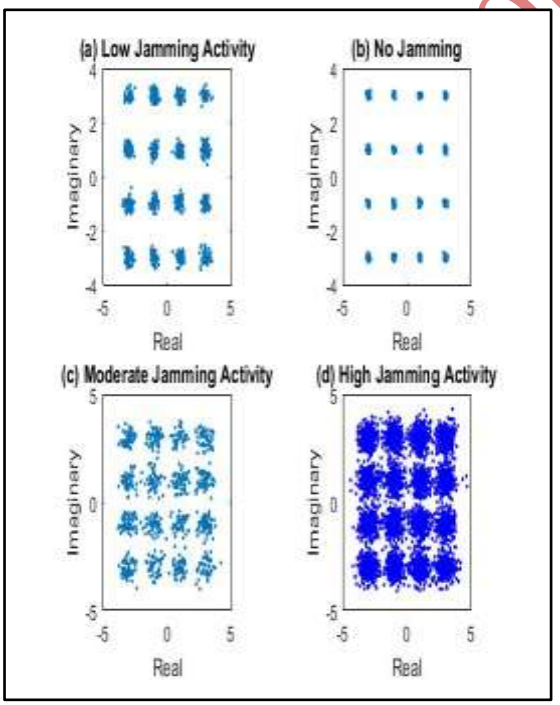

Fig.5 Scatter Plot for Different Jamming Conditions

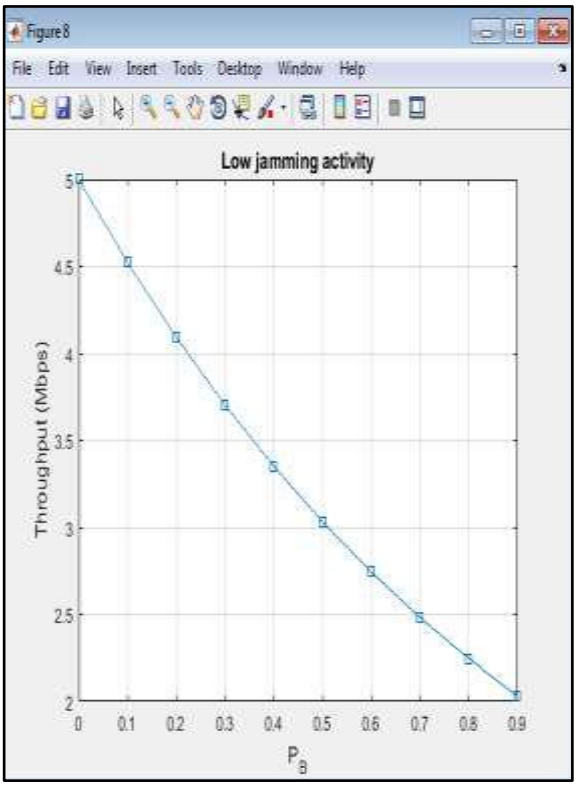

Fig.7 Throughput for Low Jamming Conditions

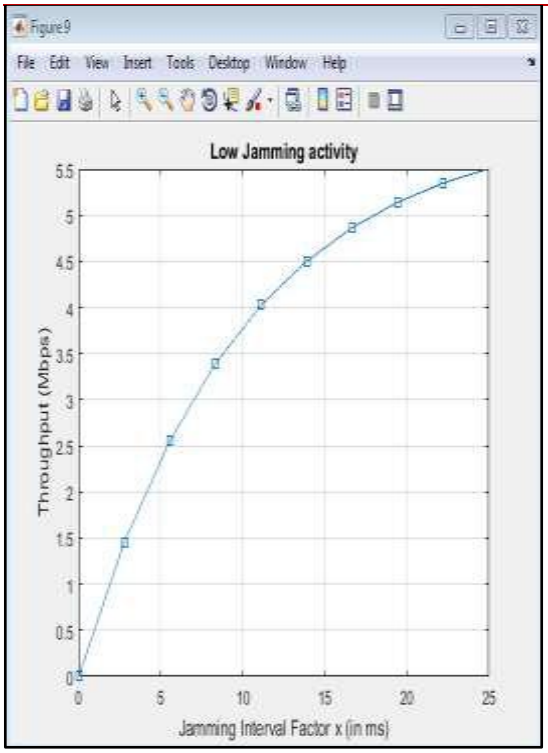

Fig.8 Throughput Analysis with respect to jamming interval (low jamming)

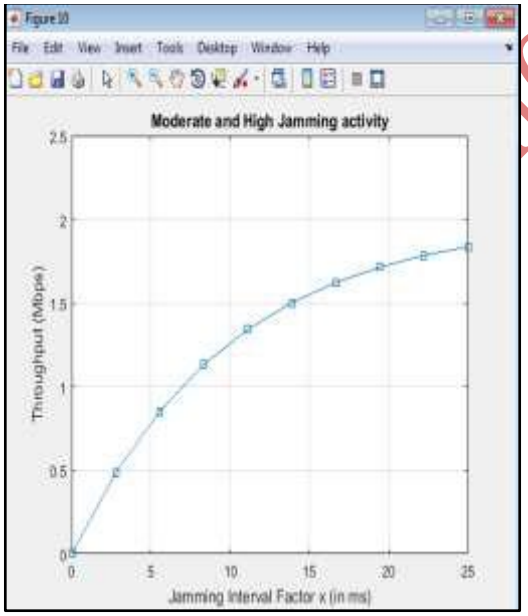

Fig.9 Throughput Analysis with respect to jamming interval (moderate and high jamming)

Parameter	Base Paper	Proposed Work
Throughput (High Jamming)	1.7 MBPS (max)	1.9 MBPS (max)
Throughput (Moderate Jamming)	1.9 MBPS (max)	2 MBPS (max)
Throughput (Low Jamming)	4.2 MBPS (max)	5 MBPS (max)
Throughput w.r.t. Jamming Interval (Moderate &High Jamming)	1.6 MBPS (max)	1.8 MBPS (max)
Throughput w.r.t. Jamming Interval (Low Jamming)	4.3 MBPS (max)	5.5 MBPS (max)

Fig.10 Comparative Analysis with base paper

VI. Conclusion:

It can be concluded form the above discussions that the proposed system attains better throughput compared to the previous work (Security-aware Channel Assignment in IoT-based Cognitive Radio Networks for Time-Critical Applications, by Haythem Bany Salameh et al, IEEE 2017). This has been achieved by using energy detection for cognitive radio. The analysis has been performed for 3 cases of jamming activity: Low jamming activity, Moderate jamming activity and High Jamming activity The results can be attributed to energy detection and subsequent discrete frequency equalization.

References

[1] Haythem Bany Salameh, Sufyan Almajali , Moussa Ayyash, and Hany Elgala, "Security-aware Channel Assignment in IoT-basedCognitive Radio Networks for Time-Critical Applications", IEEE 2017

[2] K.M. Apampa, G. Wills, and D. Argles, "Towards security goals in summative e-assessment security," in the International Conference for Internet Technology and Secured Transactions, (ICITST), London, Nov. 2009

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE 2014

[4] P. Rawat, K. Singh, and J. Bonnin, "Cognitive radio for M2M and internet of things: A survey," Computer Communications, vol. 94, pp 1-29, 2016.

[5] H. Bany Salameh, H. Kasasbeh, and B. Harb, "A

batch-based mac design with simultaneous assignment decisions for improved throughput in guard-band-constrained cognitive networks," IEEE Transactions on Communications, vol. 64, no. 3, pp. 1143–1152, March 2016.

[6] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," International Journal of Ad Hoc and Ubiquitous Computing, IEEE 2014.

[7] R. Muraleedharan and L. A. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system," in Wireless Sensing and Processing, May 2006.

[8] W. Xu, T. Wood, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in Proceedings of the 2004 ACM workshop on Wireless security, 2004, pp. 80–89.

[9] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating Energy-efficient jamming in IEEE 802.15.4-based wireless networks," in the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Jun. 2007.

[10] S.K. Jain and K. Garg, "A hybrid model of defense techniques against base station jamming attack in wireless sensor networks," in the First International Conférence on Computationnel Intelligence, Communication Systems and Networks, 2009.

