Design of Security Aware Cognitive Networks based on Energy Sensing based Spectrum Allotment

MohdSibtainul Fazal[1]
Student- PG
Electronics and Communication
Sagar Institute of Research & Technology (SIRT), Indore.

Dr.Nidhi Tiwari[2]
Associate Professor
Electronics and Communication
Sagar Institute of Research & Technology (SIRT), Indore.

Abstract: Cognitive radio networks (CRNs) are being widely used for Wide area networks. 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. For this purpose, the energy sensing pattern (ESP) is used. Channel Equalization is also used to revert the effects of actual noise and increase the throughput. The BER analysis for the different jamming conditions has also been performed. It has been shown that the proposed system achieves higher throughput compared to previous techniques for low, moderate and high jamming activity [1].

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 [2]-[3]. There are several techniques for the sensing purpose of the cognitive channel which are being discussed here. Only the frontlines are being discussed here which show the maximum promise in the accurate spectrum sensing [4].This technique is used for the energy detection mechanism and senses the energy of the channel at any given point of time [5]. The hypothesis that governs this technique is the following:

$$h(t) = k(t); ideal\ no\ jamming\ condition$$

$$h(t) = k(t) + j(t);\ jamming\ present$$

The chances for a false alarm occur when there is jamming present but the CSI suggest that jamming is absent or vice versa.

Effect of Noise on Probability of False Alarm (Security Threat)

The chances of false alarm increase when there is actual addition of noise in the desired spectrum [6]-[7]. It is noteworthy that such noise effects may lead to a false interpretation that there is jamming noise being injected in the signal spectrum and it is the act of eavesdropping by the adversary. This however is not true and leads to misleading and inaccurate results [8]. The effect can be summarized as follows:

Let the threshold for jamming to be present by 'T'

If $h(t) > T; Jamming\ present$

However,

If $h(t) + n(t) > T$ holds true;

Then there is a clear chance of false alarm often computed as the probability of false alarm of security threat [9]-[10].

II. Characteristics of a Cognitive Radio

The major problem that security aware cognitive channels face is the low throughput performance due to lost or corrupt data packets [11]. 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 [12-[13]:

- Cognitive radio networks are prone to attacks because of wireless nature of the channel
- Jamming attacks are the most common form of attacks in cognitive networks, since it is not easy to break high complexity encryption in time-critical situations [14].

Security aware networks can detect possible jamming attacks which can help in decoding data at receiving end with higher accuracy and high throughput

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 [15]. 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 [16]. 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) [17].

IV. Proposed Algorithm.

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.

Let the average received CSI (amplitude) of the channel be given by:

$$\rho = \frac{E\left[H_{i,j}H_{i,k}^{*}\right]}{\sigma_i^2}$$

For i =1,2,3……..,K
And
J ≠ k, 0 ≤j, k≤1,……N
Where * denotes the complex conjugate.
E stands for the expectation or average of the random variable
H1 and H2 represent the obtained energies
σ represents the standard deviation of the data from the mean
The jamming can be categorized by the observation of the relative deviation from the average value, given below in terms of R.

$$\bar{R} = \sum_{n=1}^{N} R_n P[\Gamma_n \leq \gamma_{i*,m} < \Gamma_{n+1}]$$

$$\bar{R} = \sum_{n=1}^{N} R_n (P[\gamma_{i*,m} < \Gamma_{n+1}] - P[\gamma_{i*,m} < \Gamma_{n+1}])$$

Here,
$R_n$denotes the relative strength of the nth sub carrier
P stands for the probability
$\gamma_{i*,m}$represents the intermediate strength between consecutive samples
$\Gamma_n$represents the previous sub carrier
Γ_{n+1}represents the subsequent sub carrier

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

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.

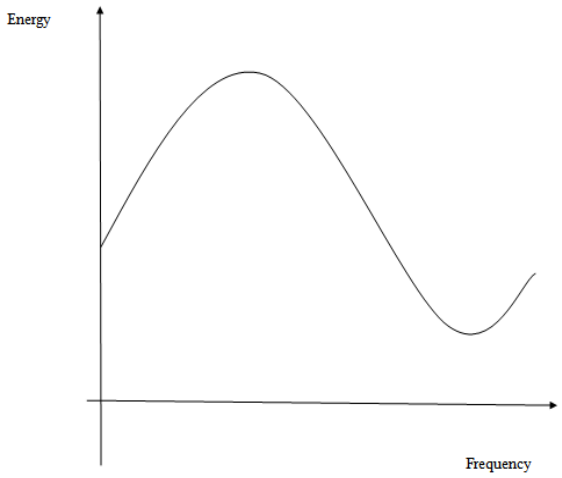

Fig.1Channel sub-carrier response

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.

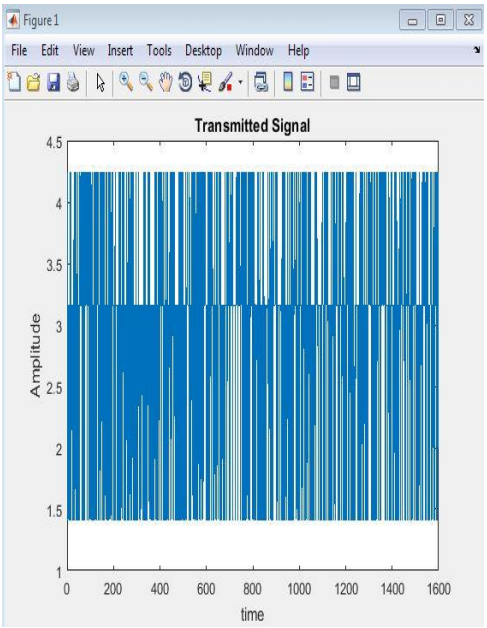

Fig.2 Transmitted binary signal

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

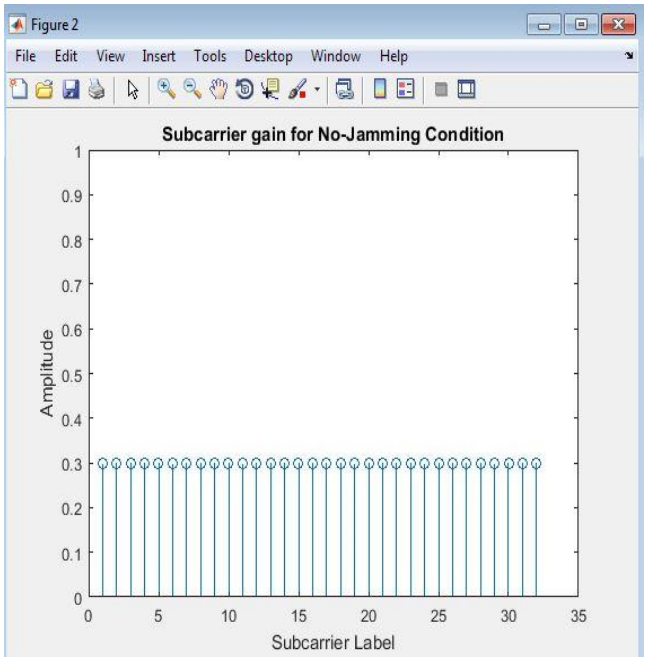

Fig.3 Subcarrier Gain for Non-Jamming Condition

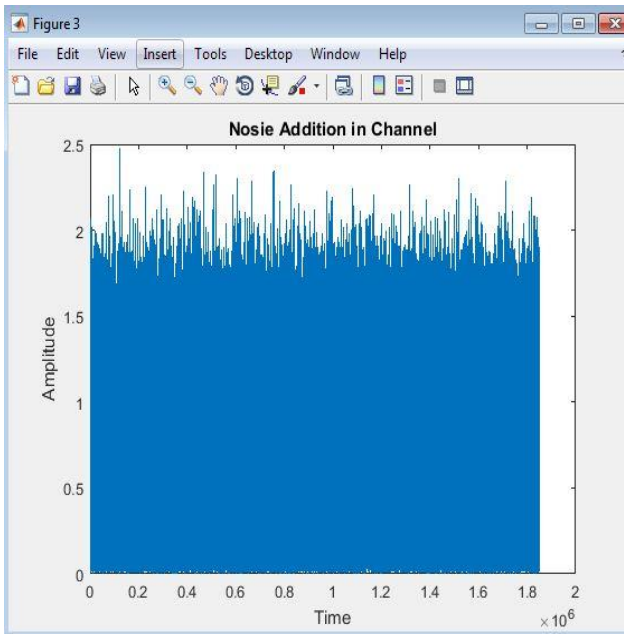

Fig.4 Addition of Noise in the Channel

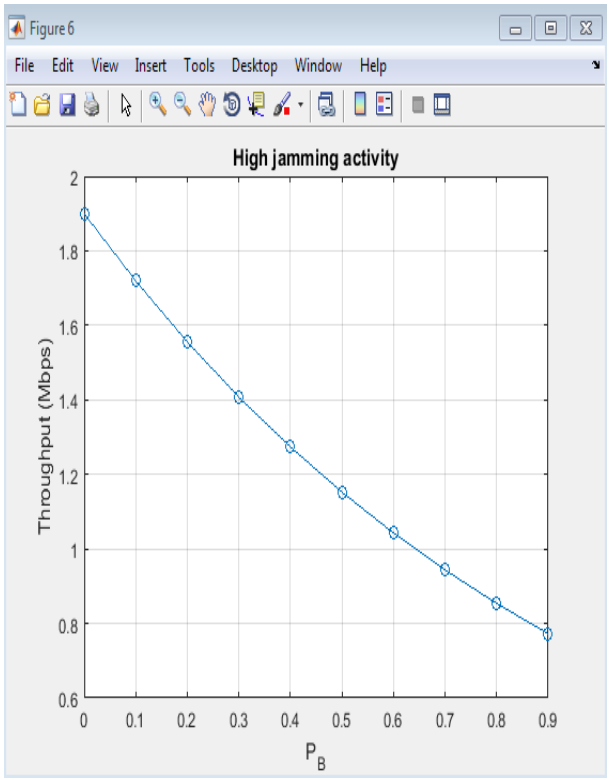

Fig.6 Throughput for High Jamming Conditions

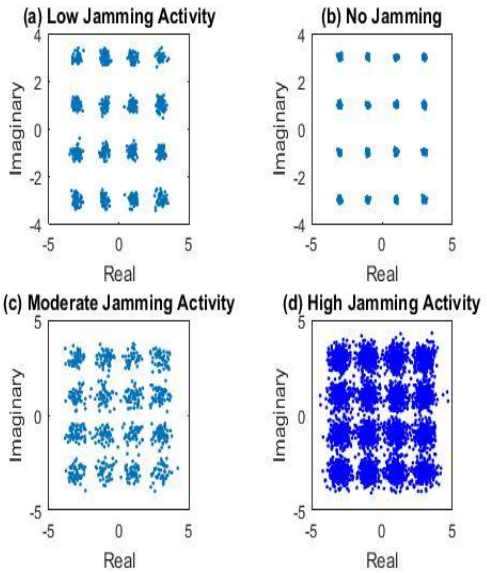

Fig.5 Scatter Plot for Different Jamming Conditions

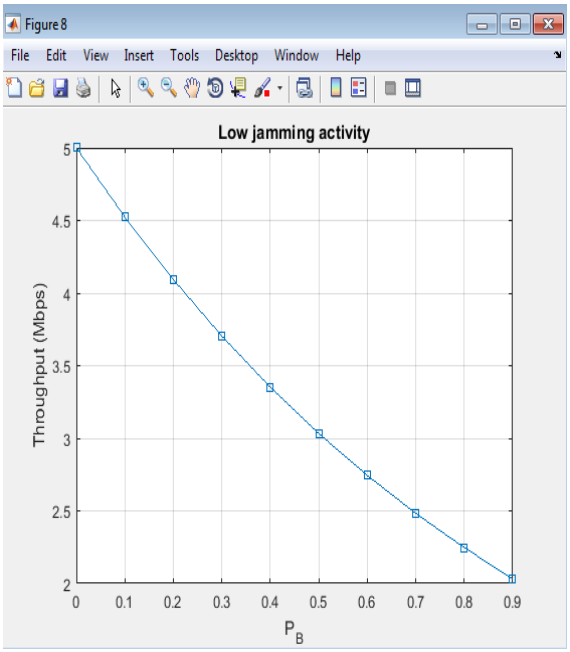

Fig.7 Throughput for Low Jamming Conditions

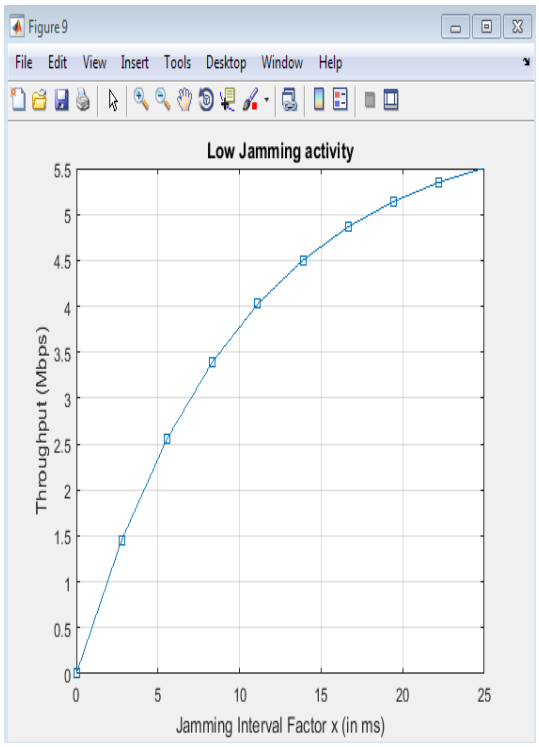

Fig.8 Throughput Analysis with respect to jamming interval (low jamming)

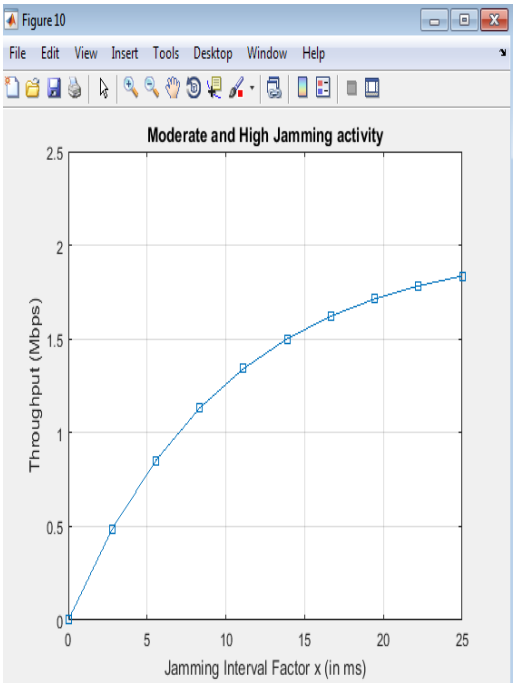

Fig.9 Throughput Analysis with respect to jamming interval (moderate and high jamming)

S.No	Parameter	Previous Work	Proposed Work
1.	Throughput (High Jamming Activity)	1.7 Mbps (max)	1.9 Mbps (max)
2.	Throughput (Moderate Jamming Activity)	1.9 Mbps (max)	2.0 Mbps (max)
3.	Throughput (Low Jamming Activity)	4.2 Mbps (max)	5 Mbps (max)
4.	Throughput with respect to jamming interval (Moderate and High Jamming Activity)	1.6 Mbps (max)	1.8 Mbps (max)
5.	Throughput with respect to jamming interval (Low Jamming Activity)	4.3 Mbps (max)	5.5 Mbps (max)

Table.1 Comparative Analysis with base paper

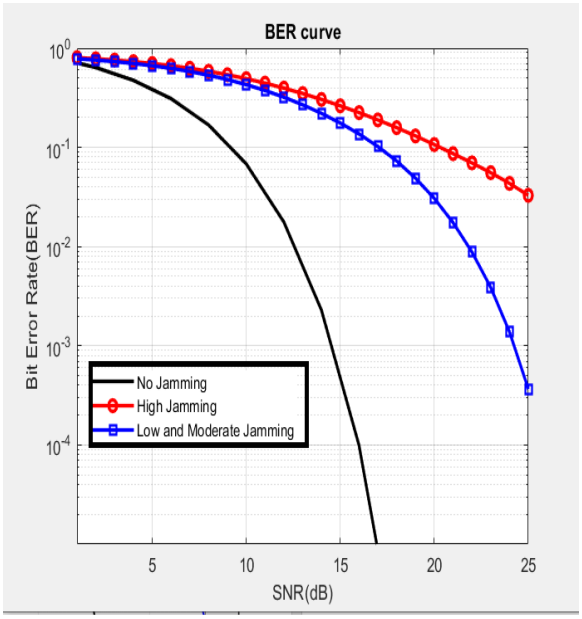

Fig. 11 BER Analysis of Proposed System

VI.Conclusion:

It can be concluded form the above discussions that the proposed system attains better throughput compared to the previously existing system. 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 activityThe results can be attributed to energy detection and subsequent discrete frequency equalization. The BER of the proposed system also complies with the throughput analysis of the system.

References

[1] HaythemBanySalameh, SufyanAlmajali , Moussa Ayyash, and Hany Elgala, "Security-aware Channel Assignment in IoT-basedCognitive Radio Networks for Time-Critical Applications", IEEE 2017

[2] K. J. PrasannaVenkatesan ,V. Vijayarangan, "Secure and reliable routing in cognitive radio networks",SPRINGER 2017

[3] KekeGai ,MeikangQiu ,Hui Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data",IEEE 2016

[4] JuRen ,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

[5] Rajesh K. Sharma ;,Danda B. Rawat," Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey",IEEE 2015

[6] MagedElkashlan ,Lifeng Wang ,Trung Q. Duong , George K. Karagiannidis ,ArumugamNallanathan, "On the Security of Cognitive Radio Networks",IEEE 2015

[7] ErolGelenbe," A Software Defined Self-Aware Network: The Cognitive Packet Network", IEEE 2014

[8] Mahmoud Khasawneh ,Anjali Agarwal," A survey on security in Cognitive Radio networks", IEEE 2014

[9] Yulong Zou, XianbinWang ,Weiming Shen," Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks",IEEE 2013

[10] Muhammad Faisal ,Amjad,Baber Aslam ,Cliff C. Zou, ," Reputation Aware Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks", IEEE 2013

[11] GianmarcoBaldini ,Taj Sturman ,Abdur Rahim Biswas ,RuedigerLeschhorn ,GyozoGodor ,Michael Street," Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead", IEEE 2012

[12] Alvaro Araujo ,JavierBlesa,ElenaRomero,Daniel Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems", SPRINGER 2012

[13] 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

[14] Ying-Chang Liang ,Kwang-Cheng Chen ,Geoffrey Ye Li ,Petri Mahonen, "Cognitive radio networking and communications: an overview", IEEE 2011

[15] GayathriVijay ,ElyesBdira ,Mohamed Ibnkahla, "Cognitive approaches in Wireless Sensor Networks: A survey", IEEE 2010

[16]SaziaParvin ,Song Han ,Biming Tian ,FarookhKadeer Hussain, "Trust-Based Authentication for Secure Communication in Cognitive Radio Networks", IEEE 2010

[17] T Qin, H Yu, C Leung, Z Shen, C Miao, "Towards a trust aware cognitive radio architecture" ACM 2009.