Evaluating the effect of jammers on Cognitive Radio Networks using Markov Models

V.Nithyakala
PG Scholar, Department of ECE, KCG College of Technology, Chennai.
Email: nithy2984@gmail.com

Abstract – Cognitive radio (CR) is a promising technology to resolve the spectrum shortage problem faced by the wireless systems. The inherent capability of the CRs to take their decisions based on their view of the environment and to learn from the experience makes their operation susceptible to a variety of malicious attacks. Jammers can stop the communication between nodes by attacking physical, network or Medium access layer. Multiple layers can be attacked simultaneously. In a Cognitive radio network (CRN), attackers launch jamming attacks to disturb efficient spectrum utilization. The main objective of this paper is to mitigate the jamming attacks in cognitive radio networks. Existence of jammer, jammer type and location of jammer in CRN should be identified. Effect of jammer on the performance of the CRN is checked using markov theory based transmission model.

Keywords - Cognitive radio (CR), Cognitive radio network (CRN), Primary user (PU), Secondary user (SU), Jamming, Jammers.

I. INTRODUCTION

A. Brief History

Radio frequency spectrum is a very limited natural resource to enable wireless communication. To communicate on certain frequency bands, licenses are required. It has been observed that most of the allocated spectrum is not effectively utilized and it opens up the opportunity to identify and exploit the spectrum holes. If any secondary user can access a spectrum hole then the spectrum utilization is improved considerably. CR is a fully configurable radio device that can adapt itself to the communication requirements of its user, to the radio frequency (RF) environment in which it is operating. It has to scan and identify the unused spectrum resources exist in the licensed bands without interfering with the primary user. Radio-scene analysis, channel identification, dynamic spectrum management and transmit power control are the major tasks of CRs.

Cognitive cycle comprises of the steps: sensing, understanding, deciding and adapting. It is a continuous process. Cognitive cycle helps CR to sense the spectrum, identify the portion of the spectrum available, and to select the best available channel, co-ordinate the spectrum access with other users and to vacate the channel when PU reclaims the spectrum. Figure 1 illustrates the way by which unique features of a CR conceptually interact with the radio environment.

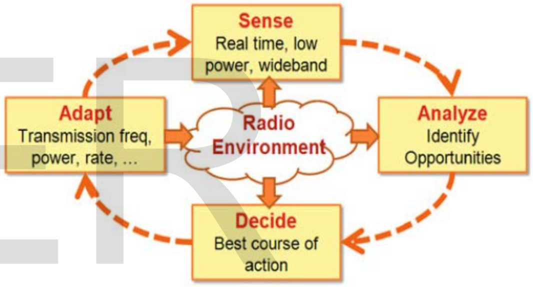


Figure 1 Cognitive cycle

Cognitive capability and Reconfigurability are the two main characteristics of CR. Cognitive capability allow CR to continually monitor the dynamically changing radio environment to take decision regarding the transmission plans. Reconfigurability is CR's ability to retune the parameters of transceiver based on the analysis of the surrounding radio environment.CR transceiver should be very flexible to exploit the emerging spectral opportunities.

CR can be extended to CRN which requires a software adaptable network to actually implement the basic network functionalities. CRN consists of a set of software defined radios (SDR) to incorporate the multiple sources of information to dynamically adopt the transmission parameters and channel access method for better performance. CRN can either be centralized infrastructure-based or distributed Adhoc network. CRN is not licensed to operate in a predefined band. The main functionalities are spectrum sensing, spectrum management, spectrum mobility and spectrum sharing.

Spectrum sensing refers to the ability of a CR to measure the electromagnetic activities, due to the radio transmissions over different spectrum bands. The sensed information helps CR to reach accurate conclusion regarding the radio environment. Spectrum sensing should be fast enough to track the temporal variations of the radio environment. Spectrum access decision defines the transceiver parameters based on the spectrum sensing and analysis information. Spectrum mobility allows CR to dynamically utilize the available spectral opportunities. Hence spectrum mobility associated with the handoff guarantees the transition to new frequency band without breaking the communication between the two communicating CR terminals and improves the performance.

CR should take efficient spectrum sensing, spectrum accessing decision while using the unutilized spectrum bands. Also these decisions should consider the time varying activities of the PUs. Coordination mechanism used by CRN should be defined explicitly or implicitly to improve the spectrum utilization. CR networking and opportunistic spectrum access can be used in many different applications like cognitive mesh networks, public safety networks, battlefield military networks, disaster relief and emergency networks.

Wireless networks are more prone to higher rate of attacks than the wired networks. Any attacker who gains access to the network is the serious threat to the highly confidential data. In CRN, SUs do not have their own spectrum and hence the opportunistic spectrum access cannot be protected from adversaries. Also distributed network structures it to difficult to implement security measures. As CRNs capable of utilizing the spectrum efficiently and intelligently, the same technologies can also be used by attackers to launch complicated and unpredictable attacks with greater damage. Jamming attack is the major threat to CRN, where several malicious attackers intend to interrupt the communication of SU. Nowadays jammers have evolved into low power, energy efficient and are capable of high coverage region.

B. Contribution

Main objective of this paper is to mitigate the jamming attacks on CRN. Existence of jammer, jammer type and the exact location of the jammer in CRN are identified. Effect of jammers on the performance of CRN is analyzed using the transmission model prepared using Markov theory. All necessary simulations are carried out using the software Matrix Laboratory (MATLAB).

I. TYPES OF JAMMERS

Various jamming attacks can be launched to disrupt the wireless communication. Constant jammer injects the high power jamming signal to the channel regularly, until the jammer is dried out of power. Once the jammer power is utilized completely, actual service can begin. Deceptive jammer resembles constant jammer in its activities, but it uses different jamming signal to interrupt the communication. This jammer uses the actual valid message to jam the network. It is very tough to differentiate the actual message and the jamming signal. Energy of this jammer is the drawback and hence its usage is limited.

To conserve the power whenever possible, random jammer is designed to be active for some time and to be in sleep mode for the remaining time. This jammer transmits the random signal (noise signal or any other signal) to occupy the medium for a defined time and make it available for the remaining time alternatively to increase the lifetime of the jammer. Reactive jammer is an intelligent jammer and it eliminates the limitations of all jammers. This jammer is active only when the actual message is sent through the channel, otherwise it will be in energy conservation mode. This jammer saves more power of the jammer. It sends the jamming message to collide with the actual message. So, the legitimate message is dropped on collision.

These four jammers act externally to the network according to the command from the attacker. In some cases, internal users of the network act selfishly to block the other users. This type of attack is called as selective jamming attacks. They selectively jam the networks, by altering some important messages. Also they can jam the services and functions of the networks.

III. JAMMER DETECTION STRATEGIES

To defend from the jammers, it is essential to first detect the existence of jammer. There are many detection methods like signal strength detection, carrier sensing time detection and Packet delivery ration detection (PDR) detection. Signal strength distribution might be affected by the presence of a jammer.

Comparing the signal strength with the predefined threshold value and classifying the shape of the window of a signal samples are two approaches to detect the jamming attacks using signal strength.

Carrier sensing time can be used as a mean to detect whether a device is jammed or not. This measurement is suitable when the jammer is non-reactive/non-random and the MAC protocol determines the availability of the channel by comparing the noise level with the fixed threshold. Jammers may not only prevent a node from sending packets, but may also corrupt the packets during transmission. PDR can be measured either by sender/receiver. Unlike the other two measurements, PDR should be measured during a specified window of time, where a particular amount of traffic is expected.

To mitigate the jamming attacks in the network, distinguishing the different type of jamming attacks is necessary. If the received signal is lower than the threshold set up by the MAC layer, the channel is considered as idle. Network nodes can receive and interpret the signal only if the signal strength is greater than the threshold. To evaluate the efficiency of transmission and reception, two metrics are used. They are Packet Send Ratio (PSR) and PDR. PSR is the ratio of the frames that are actually sent to the channel compared to the number frames intended to be sent. PDR is the ratio of the frames reached the destination compared to the number of frames actually sent from the source. If the PDR drop of any network is high and high level signal strength then it is clear that channel is jammed. After coming to the conclusion that the network is jammed, it is desirable to map out the regions that are jammed. This map information helps network services to influence routing, power management.

IV. SYSTEM MODEL

Markov chain is a mathematical system which undergoes transition from one state to another. It is a random process. Next state depends only on the current state and not on the states preceding it. Markov model of CR transmission consists of three states called spectrum sensing, data transmission and channel switching. Transmission model starts with the spectrum sensing state. Spectrum sensing helps to find out the channel for secondary access. Data transmission starts once the channel is available. If channel is not available, channel switching process will be initiated. This model always starts from spectrum sensing whether the model is jammed or not.

Consider a CR system where a pair of CR transmitter and receiver is conducting transmission at unit throughput. A group of jammers tries to jam the CRN transmission and reduce the throughput. Signal-to-noise-and-interference ratio (SINR) measures the signal and jamming levels. For successful data transmission the SINR should be greater than the minimum workable SINR, otherwise it is jammed. For a spectrum sensing slot, if SINR is larger than the minimum detectable SINR means that the channel is occupied by primary users. Markov transmission model is used to determine the jamming probabilities and throughput of the CRN. For high throughput, spectrum sensing duration should be less than data transmission and channel switching duration.

A jammer with the channel sensing, transmission capability as CR decides to jam the CR transmission. Jammer is not aware of the secret keys and channels used by the CRs Hence jammer may select the channels randomly to launch their attacks. Jammer can attack more than one channel simultaneously. When a jamming signal enters into the sensing slot, then the SINR of this slot becomes greater than the sensing threshold. Hence CRs should vacate the channel and do the channel switching procedure which is time consuming to get a new channel. There may be more than one jammer. Each jammer has the same power as the CRN node. Jamming strategies are defined by the parameters called jamming duration and the number of channels that can be jammed simultaneously. Over all jamming power is low, if the jamming duration is small and the jammers can attack more channels simultaneously.

This paper focuses on improving the anti-jamming performance of CRN. CRs can achieve better anti-jamming capability due to the flexible physical and MAC layer functions. But CRN is more susceptible for jamming attacks. In CRN, there is a necessity to vacate the channel during negative spectrum sensing result, which allows a jammer to conduct jamming attack very easily and at low cost. The conventional physical layer anti-jamming technique like spreading is not every effective and the upper layer anti-jamming techniques like channel surfing and spatial retreats are very costly. Channel switching amount CR nodes is very time consuming, since the spectrum white space channels are time varying and need to be detected in real time.

Average throughput of CRN can be calculated from the transition probabilities of the three states of markov transmission model.

To mitigate jamming attacks in CRN, jamming signal strength and the number of channels that can be jammed can be varied. One way is to mitigate the jamming attacks and to get better throughput, number of white space channels should be increased. Though the number channels are increased, throughput increases up to certain limit and after that it remains constant. Another way is to increase spectrum sensing threshold and by reducing the spectrum sensing slot length. When increasing these parameters, interference to the PUs increases and throughput decreases.

In a CRN, four type of jammers called constant jammer, deceptive jammer, random jammer and reactive jammer are introduced an its effect on the performance is analyzed. As per the simulations, it is clear that reactive jammer severely affects the performance of CRN.

V. SIMULATION RESULTS

CRN with 50 modes is constructed as shown in figure 2 with all capabilities of CR. Jammer is placed in some nodes and the effect of the jammers on the performance of CRN is analyzed. Different jammers like constant, deceptive, random and reactive jammers placed and verified its effects.

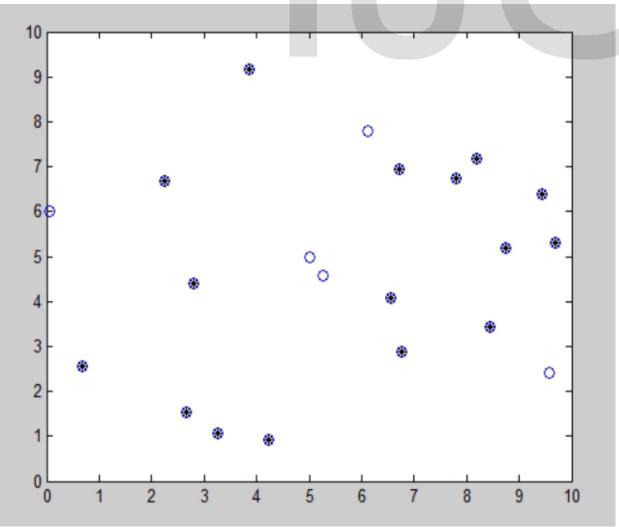
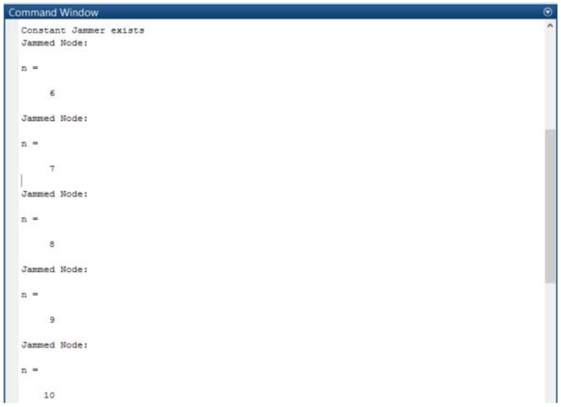


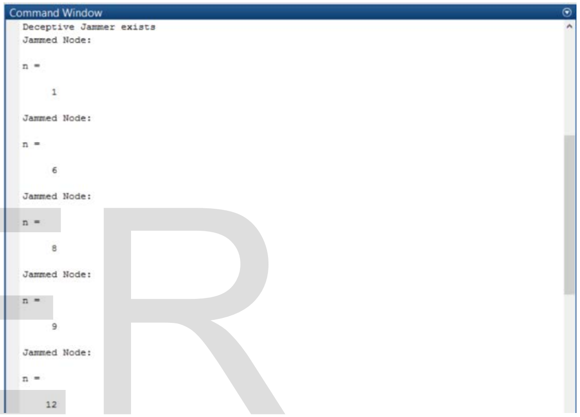
Figure 2. CRN with 20 nodes

Based on the metrics PSR and PDR, type of the jammer and the jammed nodes are identified. Results are shown in figures 3, 4, 5 and 6.



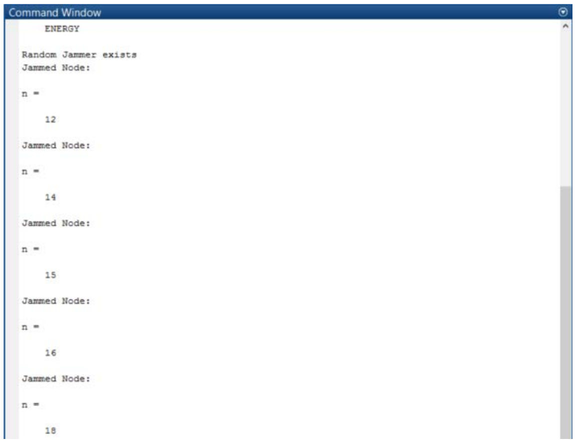
```
Constant Jammer exists
Jammed Node:

n =

     6

Jammed Node:

n =

     7

Jammed Node:

n =

     8

Jammed Node:

n =

     9

Jammed Node:

n =

    10
```

Figure 3. Constant jammer detection



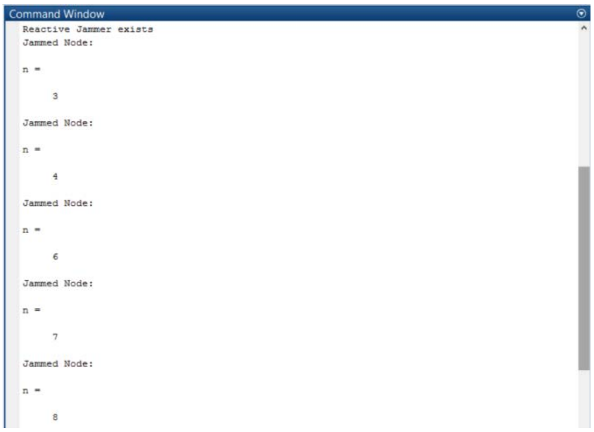
```
Deceptive Jammer exists
Jammed Node:

n =

     1

Jammed Node:

n =

     6

Jammed Node:

n =

     8

Jammed Node:

n =

     9

Jammed Node:

n =

    12
```

Figure 4. Deceptive jammer detection



```
    ENERGY

Random Jammer exists
Jammed Node:

n =

    12

Jammed Node:

n =

    14

Jammed Node:

n =

    15

Jammed Node:

n =

    16

Jammed Node:

n =

    18
```

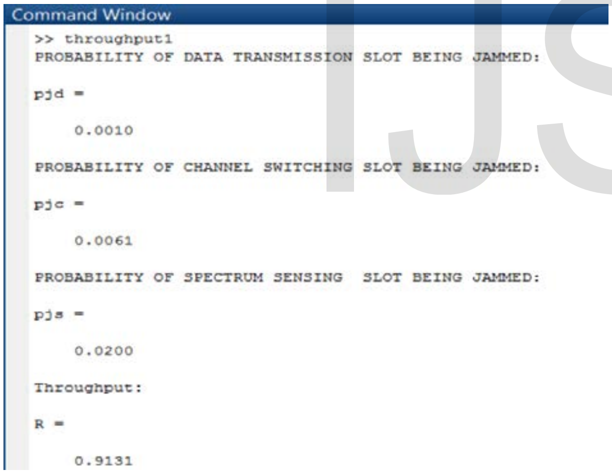
Figure 5. Random jammer detection



```
Reactive Jammer exists
Jammed Node:

n =

     3

Jammed Node:

n =

     4

Jammed Node:

n =

     6

Jammed Node:

n =

     7

Jammed Node:

n =

     8
```

Figure 6. Reactive jammer detection

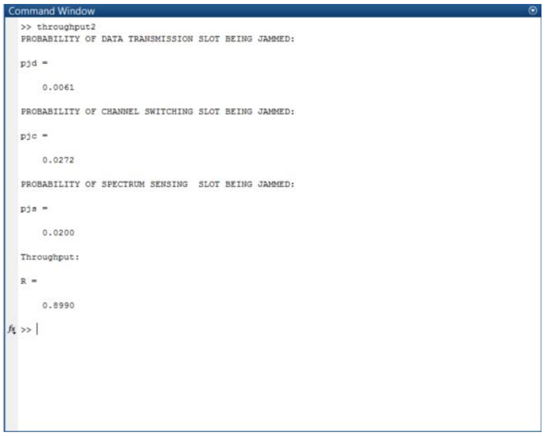
Markov theory based CRN transmission model is constructed with the parameters: 100 channels, 10 jammers, data transmission slot duration 5 ms (milliseconds), channel switching slot duration 10 ms, spectrum sensing slot duration 0.25 ms, jamming duration is 1 ms and the number of jamming signals is 2. Throughput is calculated based on the transition probabilities shown in figure 7.



```
>> throughput1
PROBABILITY OF DATA TRANSMISSION SLOT BEING JAMMED:

pjd =

    0.0010

PROBABILITY OF CHANNEL SWITCHING SLOT BEING JAMMED:

pjc =

    0.0061

PROBABILITY OF SPECTRUM SENSING  SLOT BEING JAMMED:

pjs =

    0.0200

Throughput:

R =

    0.9131
```

Figure 7. Jamming probabilities and Throughput.

When jamming duration decreases to 0.5 ms, probability of data transmission being jammed (pjd) and probability of channel switching being jammed (pjc) increases and hence throughput decreases as shown in figure 8.



```
>> throughput2
PROBABILITY OF DATA TRANSMISSION SLOT BEING JAMMED:

pjd =

    0.0061

PROBABILITY OF CHANNEL SWITCHING SLOT BEING JAMMED:

pjc =

    0.0272

PROBABILITY OF SPECTRUM SENSING  SLOT BEING JAMMED:

pjs =

    0.0200

Throughput:

R =

    0.8990

>> |
```

Figure 8. Jamming probabilities and Throughput.

Throughput increases with the number of channels up to certain limit (800 channels), after that throughput is not getting increased. It remains constant as shown in figure 9.

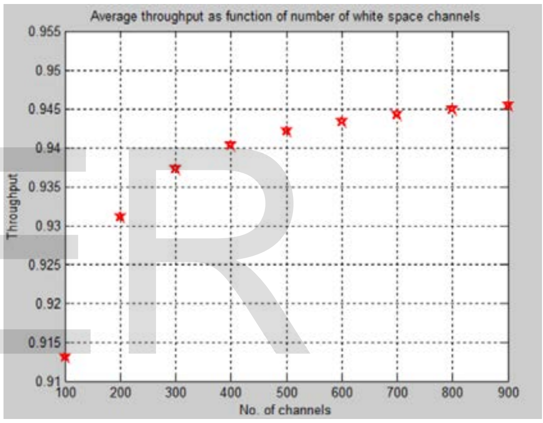


Figure 9. No. of channels Vs Throughput

When relative jamming duration increases up to 0.4 ms, accordingly throughput increases slowly. After that throughput decreases and remains constant for every 0.1 ms increase of jamming duration.

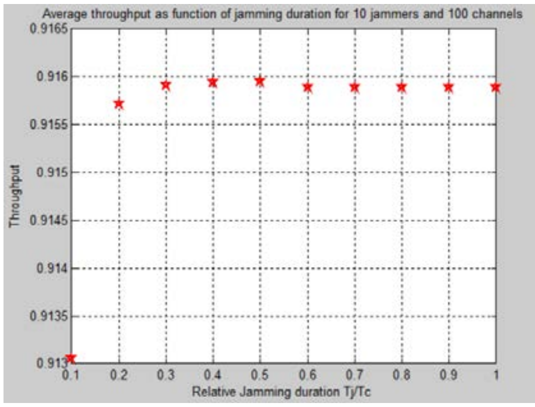


Figure 10. Jamming duration Vs Throughput

V. CONCLUSION

In this paper the degradation of CRN performance due to the presence of jammers is analyzed and the existence of jammer, type of the jammer and the jammed region are identified. All necessary simulations are done and it shows that to improve the performance if we increase the number channels, after some extent throughput is saturated. Jamming duration change also affects the throughput up to certain point after that there is no change in throughput.

REFERENCES

[1] A.Mummoorthy and S.Suresh Kumar (2012), 'A Detailed Study on Evolution of Recent Jammers in Wireless Sensor Networks', *International Journal of Engineering Research and Development*, Vol. 4,No. 6.

[2] Anthony Busson (2012) 'Markov chains, Markov Processes, Queuing Theory and Application to Communication Networks'.

[3] Beibei Wang and K. J. Ray Liu (2011) 'Advances in Cognitive Radio Networks: A Survey', *IEEE Journal of selected topics in signal processing*, Vol. 5, No. 1.

[4] Diana Alejandra Sánchez-Salas, José Luis Cuevas-Ruíz (2010) 'Wireless Channel Model with Markov Chains Using MATLAB'.

[5] Feng Wang, Student Member, *IEEE*, 'Cognitive Radio Networks and Security: A Survey'.

[6] Le Wang, Alexander M. Wyglinski, 'A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks'.

[7] Hongbo Liu, Wenyuan Xu, Yingying Chen, Zhenhua Liu,'Localizing Jammers in Wireless Networks'.

[8] Qian Wang, Kui Ren, and Peng Ning (2011) 'Anti-jamming Communication in Cognitive Radio Networks with Unknown Channel Statistics', *19th IEEE International Conference on Network Protocols.*

[9] Qihang Peng, Pamela C. Cosman, and Laurence B. Milstein (2011) 'Spoofing or Jamming: Performance Analysis of a Tactical Cognitive Radio Adversary', *IEEE Journal on selected areas in communications*, Vol. 29, No. 4.

1. [10] Roberto Di Pietro y 'Jamming Mitigation in Cognitive Radio Networks'.

[11] Sisi Liu, Loukas Lazos, and Marwan Krunz (2012) 'Thwarting Control-Channel Jamming Attacks from Inside Jammers', *IEEE transactions on mobile computing*, Vol. 11, No. 9.

2. [12] Shameek Bhattacharjee a, Shamik Sengupta b, Mainak Chatterjee (2013) 'Vulnerabilities in cognitive radio networks: A survey',*Computer Communications.Elsevier*.Vol 36.pp 1387–1398.

3. [13] T. Charles Clancy,Nathan Goergen,'Security in Cognitive Radio Networks:Threats and Mitigation'.

4. [14] Vamsi Krishna Tumuluru, Ping Wang, and Dusit Niyato, 'Performance Analysis of Cognitive Radio Spectrum Access with Prioritized Traffic'.