International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 04, April-2015

Analysis and Simulation of Anti-Jamming Performance of Cognitive Radio Networks using Markov Models

V. Nithyakala[1], K. Mourougayane[2], J. Raja Paul Perinbam[3]
[1] PG Scholar, Department of ECE, KCG College of Technology, Chennai.
[2] SAMEER, Centre for Electromagnetics, Chennai
[3]Professor, KCG College of Technology, Chennai.

***Abstract* – Rapid growth of wireless devices highlights the importance of effective utilization of the spectrum. Cognitive radio (CR) is one of the growing technology to overcome the spectrum scarcity problem. Cognitive radio network(CRN) has more design challenges and –security threats as it allows dynamic spectrum sensing. Spectrum sharing policy among the licensed and unlicensed users, opens up the possibility of various security threats. Malicious attackers can launch the jamming attacks to prevent the efficient utilization of the spectrum opportunities. A Markov chain model helps to predict the behavior of open spectrum access in the unlicensed bands. In this paper, different types of jammers and their jammed region are identified based on the signal strength, packet sent ratio, packet delivered ratio. Markov theory based CRN transmission model is developed to compute the jamming probabilities and the throughput. Jamming strategy and anti-jamming performance of CRNs are analyzed using Markov model.**

Keywords - Cognitive radio (CR), Cognitive radio network (CRN), Primary user (PU), Secondary user (SU), Packet sent ratio (PSR), Packet delivered ratio (PDR), Jamming attack, Jammers.

I. INTRODUCTION

A. Brief History

Cognitive radio is an intelligent radio which enables the dynamic spectrum access by spectrum sensing, software and hardware reconfigurability and adaptation with the communicating environment. Spectrum sensing plays an important role as it helps to find the available spectrum that can be assigned to the secondary users to improve the spectrum utilization. A CRN is formed by the set of nodes with the CRs and relies on the opportunistic spectrum for its operation. CRN can be potentially used for many real time applications to alleviate congestion, to control the transmit power levels and to improve the quality of service. CRs classified as Secondary Users (SU) can sense the environment and occupy the vacant channels for their operation without causing interference to the Primary Users(PU).Wireless networks have already grown considerably and consequently the security and secrecy has become a critical issue. Jamming is one of the main threats to the CRN. Jamming the communication channel is one of the most efficient way of attacking the user communication and easy to implement. CRs are used in both licensed and un-licensed bands. In licensed bands, the frees spectrum can be used by CR opportunistically and the channel need to be vacated when primary user intends to use. In the un-licensed bands, CRs co-exists with the other primary / secondary users without causing interference. Jamming analysis and development of effective Anti-jamming techniques are important area of research and a challenge in the design of CR/CRNs. Markov chain is a random theory which illustrates the transition from one state to another, based only on the current state and not on the states preceded it. Markov Model can also be used in analyzing the vulnerabilities of jamming attacks in different operation states of CR.

B. Contribution

This paper is focused on analyzing the anti-jamming performance of CRN using Markov models[10]. Approaches for sensing the jamming activities, identifying the types of jammers are simulated. Throughput of the CRN is computed using the jamming probabilities derived from transmission model. Performance of the jammers and anti-jamming performance of the CRN[2][5][7][9] are analyzed with the help of simulations carried out using MATLAB.

II. JAMMING STRATEGY

Wireless networks are very much prone to the malicious attacks than the wired networks. Since the SUs of CRN are dynamically accessing the spectrum, it is very difficult to protect the network from adversaries. Jammers can also designed with the CR technology and can access the spectrum intelligently like CR nodes. Hence, ensuring security in CRN is a critical issue. Jamming attack can be executed in many forms like making the communication channel busy by sending the waste data, disturbing the SU communication, sending the interruption and forcing the receiver to receive the data. There are many type of jammers[1] like constant jammer, deceptive jammer, reactive jammer and random jammer. Jammers evolved with the low power, energy efficient and more coverage area.

Constant jammer continually emits the jamming signal with the high transmission power into the communication channel, until it's power drained off. Transmission medium would never be available for the communication. Deceptive jammers use the jamming data same like the original message to be transmitted and block the communication channel. It is difficult to differentiate between the original data and jamming data. This type of jammer can be used only for a limited amount of time. Random jammer's main intention is to preserve the battery power whenever possible. This type of jammer will be active for a predefined time and then it will go to the sleep mode. Reactive jammer is very effective and intelligent jammer designed to overcome the limitations of the other jammers. This jammer emits jamming signal only when there is a actual data transmitted through the channel, otherwise it will be in energy conservation mode. Another motive of the jammer is to hide from the jamming detection algorithms and continue the jamming process.

III. JAMMER TYPE AND JAMMED REGION DETECTION

To mitigate the jamming attacks in CRN, it is necessary to find the existence of jammers in CRN and its type and the jammed regions. A specific area in the network is selected for jamming attack. Jammers try to block the communication channel using an undesired signal. CSMA networks check for the idle channel to transfer the data. It will wait until the channel is freed and finally user gives up and hence the service is blocked. Also jammers try to block the RTS/CTS messages in order to prevent the communication between the pair of nodes. Authentication messages of the network can be altered by the attackers and access the network to launch their attacks. Efficient jamming attack can be made by power management of the jammers. Energy efficient jammers can continue their attack for more time.

There are some scenarios which resemble the presence of jammer like low Signal-to-noise ratio, battery running out of power. Parameters like signal strength, Packet delivered ratio and the carrier sensing time helps to detect the presence of jammers. Strength of the signal is compared with the Jammer may try to corrupt the transmitted packet. In this situation, packet delivered ratio helps to detect the jamming attack. PDR determines the number of packets delivered successfully to the destination. To implement the effective defense strategies, distinguishing the type of jammer is mandatory. Packet send ratio is the measure of the packets that are actually sent into the channel.

Jammer type[6] can be identified using signal strength, PDR and PSR. When the signal strength is low and PDR drop is high, it represents the jammed area. Based on the PDR, PSR parameters jammer type can be identified. Deceptive jammer prevents the packet sent into the communication channel and hence the PSR is zero. If the PSR and PDR is about 2%, it represents the constant jammer. Random jammer is active for certain period and it will be in sleep mode for the remaining time. Hence PSR is like 70% and PDR is about 20%. Reactive jammer is very effective and it completely blocks the actual data sent on the channel. So, PSR is 100% and PDR is 0%.

IV. SYSTEM DESIGN AND RESULTS

CRN Transmission model is constructed using Markov theory and the jamming probabilities, throughput are computed for the CRN with the parameters 100 channels, 10 jammers, jamming duration is 1ms and the number of jamming signals is 2. Markov transmission model consists of three states called spectrum sensing, channel switching and data transmission. Transition from one state to another in CRN transmission model can be predicted using the probability matrix of Markov theory[10].

Throughput of the Markov theory based transmission model[3] can be derived as,

$$R = \frac{(1-p_{jc})\,(1-p_{jd})\,(1-p_{js})T_d}{(1-p_{jc})T_s + (1-p_{jc})(1-p_{js})\,T_d + (p_{jd}+p_{js} - p_{jd}\,p_{js})\,T_c}$$

where T_C ,T_d , T_s is the channel switching slot duration, data transmission slot duration and the spectrum sensing slot duration. p_{jc}, p_{jd}, p_{js} is the probability of channel switching slot being jammed, probability of data transmission slot being jammed and the probability of sensing slot being jammed respectively.

Each jammer has the same capability of CRN nodes and with the equal amount of power. Instead of one jammer, more than one jammers and different type of jammers can be used. Jammers do not have idea about the channels being used by the CR users. It has to select the channels randomly and launch the attacks. Total number of channels can be used to send the jamming signals depend on the transmission slot length and the jamming signal duration. If the jamming signal duration is small, then more number of channels can be jammed and if it is more, then it block only less number of channels. Jamming parameter is the ratio of the multiplication of Jammer power and the number of jammers with the number of channels that can be jammed simultaneously. Jamming attack can be easily implemented in CRN. When a jamming signal enters into the PU sensing slot[8], it increases the signal-to-interference noise ratio greater than the sensing threshold. Hence CRN should vacate the channel and continue the time consuming channel switching process to find a new channel.

Jammed region[4] of the CRN can be identified using PDR and signal strength. If the signal strength is high and the PDR drop is low, the region is jammed by the jammers. Simulation result shows that if the PDR drop is below 50% and the signal strength is above 50% then it means that CRN is jammed. Jammed region is shown in the figure 1.

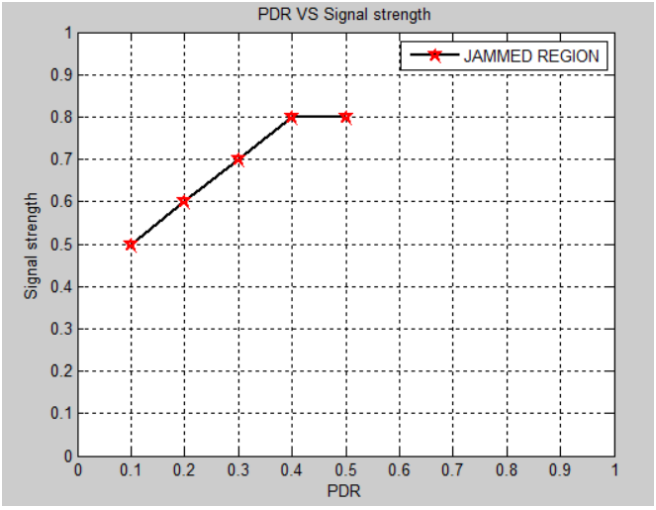

Figure 1. Jammed Region detection

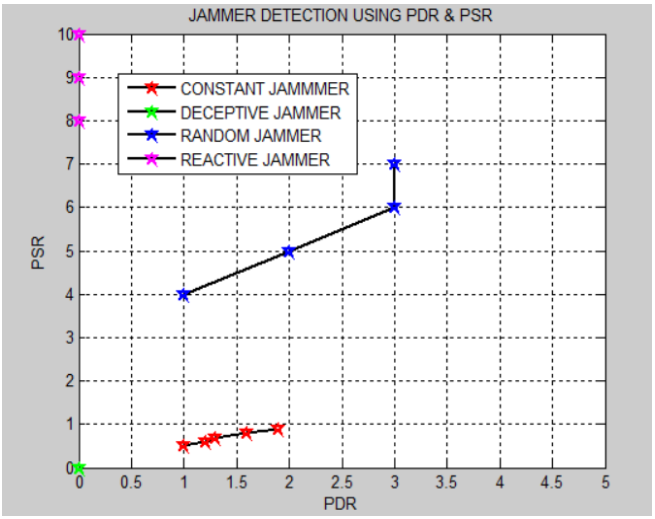

Figure 2. Jammer Type detection

The nature and type of jamming attack can be identified using PDR and PSR. Constant jammer when the PSR and PDR is zero. Deceptive jammer exists when the PSR is 1% and the PDR is up to 2%. Random jammer exists when the PSR is 70% and PDR is 16%. Reactive jammer exists when the PSR is 100% and the PDR is zero. As per the simulation results shown in figure 2, reactive jammer is more effective in jamming because it affects the actual data sent on the channel completely. Also it is very easy to detect the constant jammer and the reactive jammer. Deceptive jammer can be detected by checking the header of the packets sent. It is very difficult to detect the reactive jammer.

Figure 3 represents the performance of CRN for the number of channels. Throughput increases with the number of channels and it is saturated after certain limit. It is clear that obtaining 60% throughput itself is very difficult in the absence of any jammers.

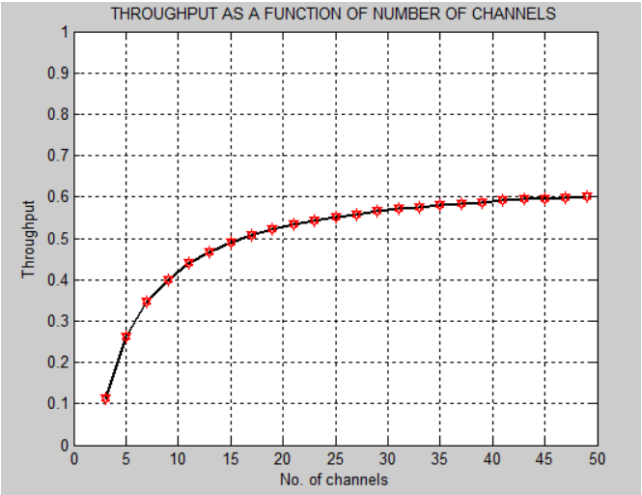

Figure 3. Throughput Vs Number of channels

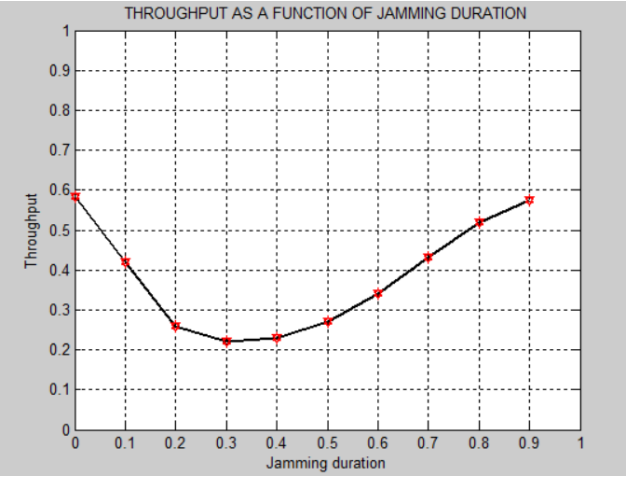

Figure 4. Throughput Vs Jamming signal duration

Figure 4 represents the effect of jamming signal duration on the performance of CRN. Simulation result shows that only 10% to 20% of the jamming signal duration affects the throughput severely and the remaining 30% to 80% of the jamming signal duration affects the performance slowly.

Figure 5 represents the effect of jamming parameter on the performance of CRN. Jamming parameter is the ratio of the multiplication of number of jammers and the power of the jammer with the number of channels that can be jammed simultaneously. Result shows that 10% to 20% of the jamming parameter affects the performance severely and up to 50% jamming parameter affects the performance slowly.

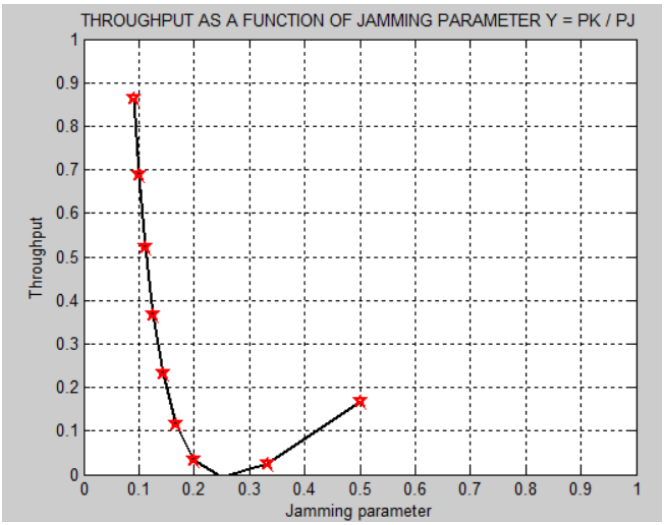

Figure 5 Throughput Vs Jamming Parameter

Figure 6 represents the effect of jamming parameter on the performance of CRN. Jamming parameter is the ratio of the multiplication of number of jammers and the power of the jammer with the number of channels that can be jammed simultaneously. Result shows that performance degrades when jamming parameter increase. Jamming parameter 0.05 affects the performance more than the jamming parameter 0.01.

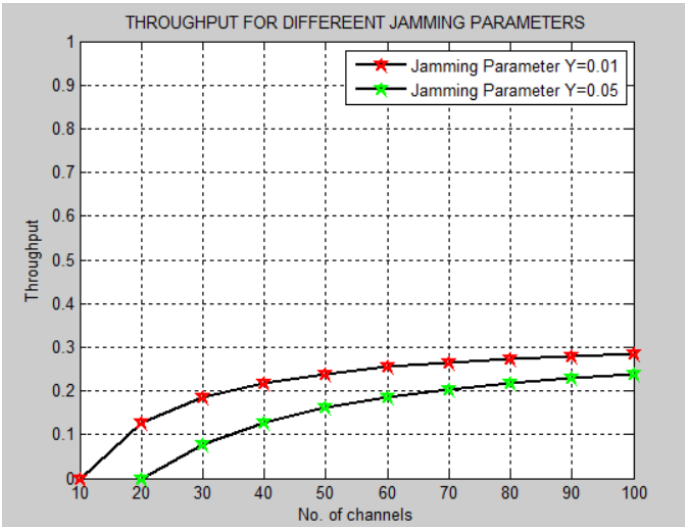

Figure 6. Throughput Vs Number of channels for different Jamming parameters

Figure 7, represents the effect of jammers on the performance of the CRN. Simulation result shows that the throughput of CRN decreases with the number of jammers.

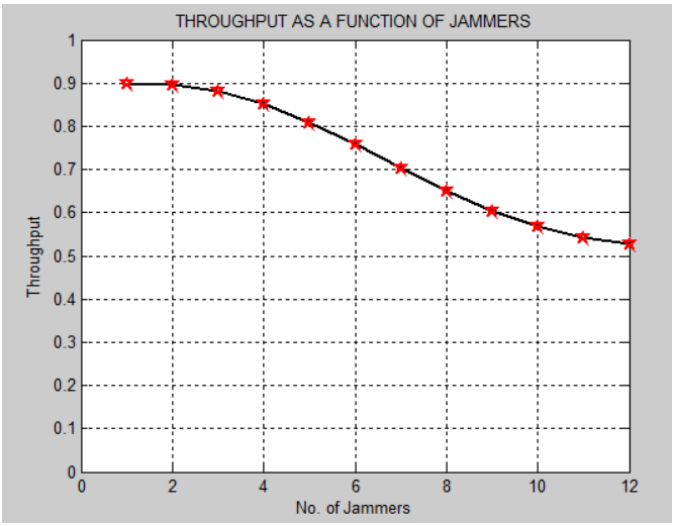

Figure 7. Throughput Vs Number of Jammers

Figure 8 represents the effect of jammers on the performance of the CRN. Simulation result shows that the throughput of CRN decreases with the number of jammers. The-advantage gained by increasing the number of white space channels in order to increase the anti-jamming capability of CRN is nullified by increasing the number of jammers.

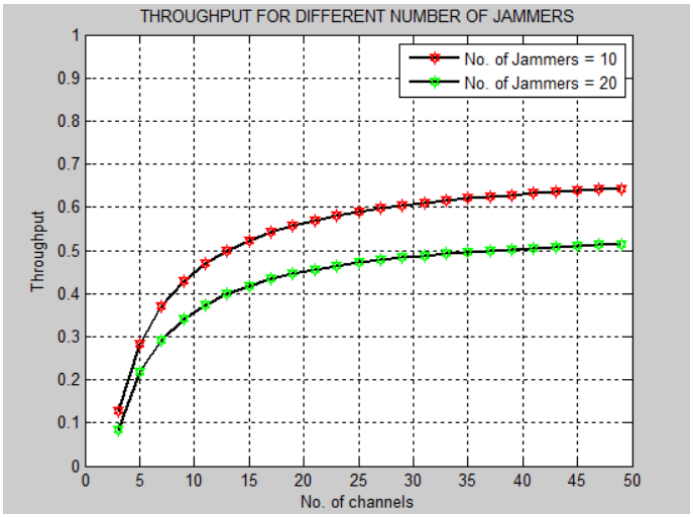

Figure 8. Throughput Vs Number of Channels for different number of Jammers

Figure 9 represents the effect of different type of jammers on the performance of CRN. Simulation result shows that reactive jammer severely affects the performance as it completely blocks the actual data sent on the communication channel.

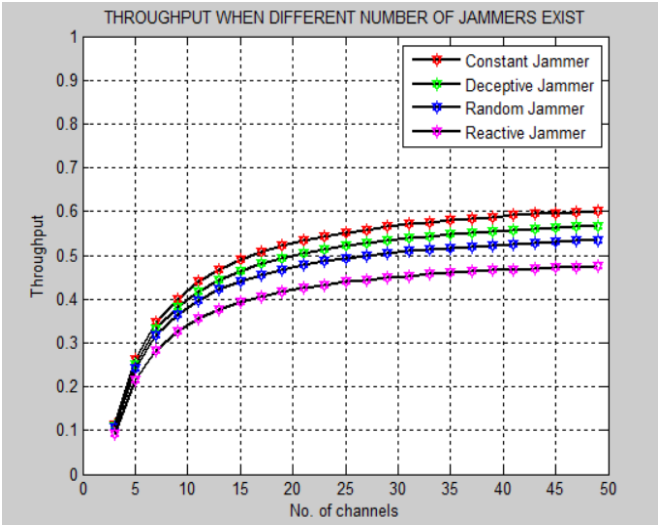

Figure 9. Throughput Vs Number of Channels for different Type of Jammers

V. CONCLUSION

In this paper, the anti-jamming performance of the CRN is analyzed with the help of the transmission model developed using Markov theory. Performance of the jammers and the anti-jamming performance of the CRN are analyzed based on the jamming probabilities and the throughput. To defend against the jamming attacks, jammed region and the type of jammer attacks in the CRN are found using the jamming detection algorithm. Effect of number of jammers, jamming duration, jamming strategy parameter, different jammers and the performance degradation are analyzed. All necessary simulations are done using MATLAB. It is clear that though CR helps to resolve the spectrum scarcity problem, it is more vulnerable for smart jamming attacks and opens up the way for many security threats. Implementing an effective anti-jamming mechanism and maintaining reliable performance is very challenging in CRN.

REFERENCES

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

[2]. Cadeau, W. and Li, X, "Anti-Jamming Performance of Cognitive Radio Networks under Multiple Uncoordinated Jammers in Fading Environment", Proceedings of the 46th Annual Conf. on Information Sciences and Systems (CISS), 2012.

[3]. Cadeau, W. and Li, X, "Jamming Probabilities and Throughput of Cognitive Radio Communications against a Wideband Jammer". The 47th Annual Conference on Information Sciences and Systems (CISS),2013, Johns Hopkins University.

[4]. H. Liu, W. Xu, Y. Chen and Z. Liu," Localizing Jammers in Wireless Networks". In Pervasive Computing and Communications, 2009. PerCom 2009, pages 1,2009.

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

[6]. Wang, Le, Wyglinski, Alexander M,"A Combined Approach for Distinguishing Different Types of Jamming Attacks against Wireless Networks," In the Proceedings of the Conference on Communications, Computers and Signal Processing Pacific Rim, pp.809-814, 23-26 IEEE, Aug. 2011.

[7]. W. Cadeau and X. Li, "Anti-jamming performance of cognitive radio networks under multiple uncoordinated jammers in fading environment," Proc. of the 46th Annual Conf. on Information Sciences & Systems (CISS), Princeton Univ., Princeton, NJ, March 2012.

[8]. Wednel Cadeau, Xiaohua Li, Chengyu Xiong (2014) 'Markov Model Based Jamming and Anti-Jamming Performance Analysis for Cognitive Radio Networks', Scientific Research, Communications and Network, Vol. 6,pp. 76-85.

[9]. X. Li and W. Cadeau, "Anti-jamming performance of cognitive radio networks," Proc. of the 45th Annual Conf. on Information Sciences & Systems (CISS), March 2011.

[10]. Yongle Wu, Beibei Wang, and K. J. Ray Liu , 'Optimal Defense Against Jamming Attacks in Cognitive Radio Networks using the Markov Decision Process Approach', IEEE Globecom 2010 proceedings,2010.

[11]. Yongle Wu, Beibei Wang, K. J. Ray Liu, and T. Charles Clancy ,'Anti-Jamming Games in Multi-Channel Cognitive Radio Networks',IEEE,Vol. 30,2012.