International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-06, Issue-01, Apr 2020

A Survey on Security Aware Channel Assignment in Cognitive Networks (CRNs)

[1]Mohd Sibtainul Fazal, [2]Dr. Nidhi Tiwari

[1]Student- PG, [2]Associate Professor, Electronics and Communication, Sagar Institute of Research & Technology (SIRT), Indore, India.

Abstract: This paper presents a survey on Security Aware Channel Assignment for Cognitive Radio Networks (CRNs). Cognitive networks are networks are the sort of networks which show the attributes of leveraging the channel state information for the utilization of resources such as bandwidth and energy. The major challenge with cognitive systems comprising of cognitive networks is the fact that finding the channel state information with high accuracy is often extremely complex in nature. Moreover, securing such a network against attacks is even more challenging. This paper focuses on contemporary contributions in the field.

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

I. INTRODUCTION

Cognitive networks are networks are the sort of networks which show the attributes of leveraging the channel state information for the utilization of resources such as bandwidth and energy [1]. The major challenge with cognitive systems comprising of cognitive networks is the fact that finding the channel state information with high accuracy is often extremely complex in nature. The random nature of the medium or channel makes is extremely difficult to **assess** the true nature of the channel which is often time variant in nature. Basically the cognitive networks are comprised of the following activities:

1)Sense channel or radio environment
2)Obtain the channel state information(CSI)
3)Share spectral resources
4) Take decisions regarding network security
5)Repeat the process of channel sensing.

The above mentioned concepts have been exemplified using the following diagram. The diagram shows a typical cognitive radio environment.

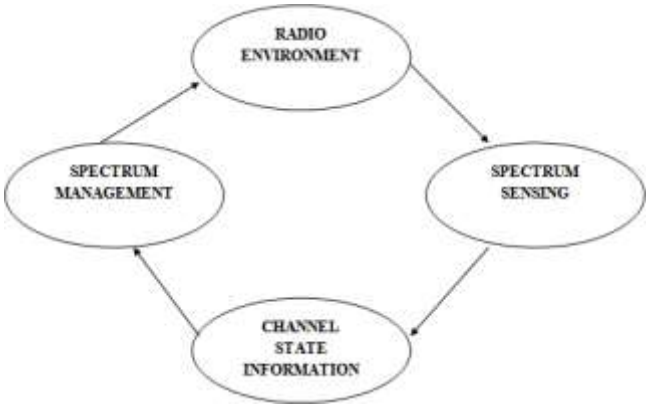

Figure 1.1 Basic Functions of Cognitive Networks

II. SECURITY AWARENESS IN 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.

III. LITERATURE REVIEW

A cognitive network structure that was aware of the attacks possibly made by adversaries. It was a (non-orthogonal multiple access) based cognitive network architecture. The major challenge as shown by the authors in the work was that cognitive systems comprising is the fact that finding the channel state information with high accuracy is often extremely complex in nature. The random nature of the medium or channel makes is extremely difficult to assess the true nature of the channel which is often time variant in nature. Here the performance metrics were the throughput and the BER of the system [1].

A cognitive network based on security metrics using network simulator (NS-2) module design, The packet delay, frame transfer rate and the throughput were analyzed. It was shown that additional overhead was indeed needed in case of jamming attacks. This happens due to the missing data packets. The energy spectrum sensing technique was cited as a possible successor to the proposed technique [2].

A time critical approach based network was designed. This network was cognitive in nature thereby sensing the

 DOI : 10.35291/2454-9150.2020.0291

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. 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 [3].

A reliable and secure architecture for routing in cognitive networks was proposed. 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 [4].

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 [5].

Collaborative resource sharing in cognitive networks was proposed. 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 to attacks [6].

One of the major challenges 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 [7].

A technique to assure the security of cognitive networks was designed. 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 [8].

A software defined self aware cognitive network wherein the concept of software defined radio was proposed for the security enhancement of cognitive systems. Leveraging the pre-defined values of the channel state enabled the detection of attacks This would allow the network design to be immune towards attacks in cognitive networks by leveraging the channel response or the channel gain of the system [9].

Different channel sensing techniques such as energy sensing, cyclostationarity sensing, matched filter sensing and wavelet sensing were surveyed. The effect of noise on false alarm was also discussed. It was shown 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. Moreover, the system performance is evaluated in terms of throughput [10].

IV. CHALLENGES IN SPECTRUM SENSING

Main Challenges faced in Spectrum Sensing in Cognitive Radio Systems [11-[12]:

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)

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

- Random nature of wireless 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 systems lie in the fact that:Cognitive radio networks are prone to attacks because of wireless nature of the channel [14]. Security aware networks can detect possible jamming attacks which can help in decoding data at receiving end with higher accuracy and highthroughput [15]-[16].

The probability of false alarms is also a serious challenge given by:

 DOI : 10.35291/2454-9150.2020.0291

$$Prob(FA) = Prob\left(\frac{H}{N.H.}\right) + Prob(\frac{N.H.}{H})$$

Here,

Prob. denotes probability

FA denotes false alarm

H denotes spectrum hole

N.H. denotes spectrum non-hole

Thus the probability of false alarm hinders the possibility of finding out spectrum holes effectively [17].

V. CONCLUSION

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 Networks face basically two types of attacks which are data extraction and jamming. It is necessary to sense the channel to in order to obtain the channel state information and decide the frequencies or spectrum which is safe for data transmission. The final aim is to obtain high throughput for the system.

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.

 DOI : 10.35291/2454-9150.2020.0291