International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

A Review on Security Aware Spectrum Assignment for Cognitive IoT Networks under Conditions of Cyber Attacks

Apurve Kothari[1] Prof. Ashish Tiwari[2]

Abstract: The internet of thins (IoT) framework has helped in design of high speed connected networks which include Wide Area Networks (WANs). Cognitive Radio can be considered to be one of the key enablers of high speed data transfer with evolving generation of wireless networks. Cognitive networks find their applications in military and defence as well with the advent of internet of things and its allied applications in military warfare. Cognitive Radio Networks often 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 and eavesdropping attacks. In this paper, the basics of cognitive IoT networks have been presented with the focus of security aware cognitive IoT networks. Previous work in the allied domain has been discussed along with their salient features.

Keywords: Wide Area Network (WAN), Internet of Things (IoT), cognitive radio network (CRN), security aware spectrum assignment, cyber-attacks, false alarm, and throughput.

I. INRRODUCTION

Internet of things or IoT is the connection of multiple devices termed as things over internet. A cognitive radio network is a form of network of cognitive radio nodes that are interlinked with each other. It results in a broad cognitive radio network that is powerful and very efficient for radio communication. The performance of the communication is drastically enhanced of that area where the network is created. In such a scenario an individual cognitive radio unit can communicate with many other cognitive radio stations and there will exchange of information in a broad range of area. And in some other instances, many cognitive radio units form a single radio unit and operate as a big network. This gives a wider range of region to operate upon and also enhances the performance and flexibility of the network and also the communication. The flexibility and intelligent working of the cognitive radio makes it very beneficial for the spectrum sensing process. The Cognitive Radio is a new form of radio technology that is gaining momentum in radio technology space. Much technological advancement has been taking place in this domain and following next to the software defined Radio, we have the cognitive radio technology. The CR is the major impetus towards an efficient and robust radio network framework that can benefit in radio communication. For using the radio spectrum band in a more effective and beneficial manner, the concept of cognitive radio has become prominent. This is a form of technology that sues many layers and levels of processing and the cognition of the radio is able to look upon and detect the available frequency bands and search for the best available communication efficacy. Similarly CR is capable of selecting the band of frequency and also the modulation type and the power metrics that are required and are the best fit for the specific conditions of an area and its regulatory policies. A cognitive radio is based on the cognition concept. It is a type of radio that is cognizant or aware of the surrounding environment and its internal and external state. It is capable of evaluating the situation by the help of its knowledge of various communication elements. It can take decisions based on its knowledge and capability. Basically it can look at the parameters of channel, can select the frequency, can detect spectrum availability and type of modulation etc. for effective communication.

The basic functioning of the cognitive radio framework can be understood using the following figure. In many cases, it can be modified manually to work and operate in a certain way or manner. It may

look after the regulatory policies and the presence of the licensed users and the access of the channel and channel state as well. It works in sync to ensure improved radio communication and proper use of the channel bandwidth available. It is also inter-related closely to software defined radio.

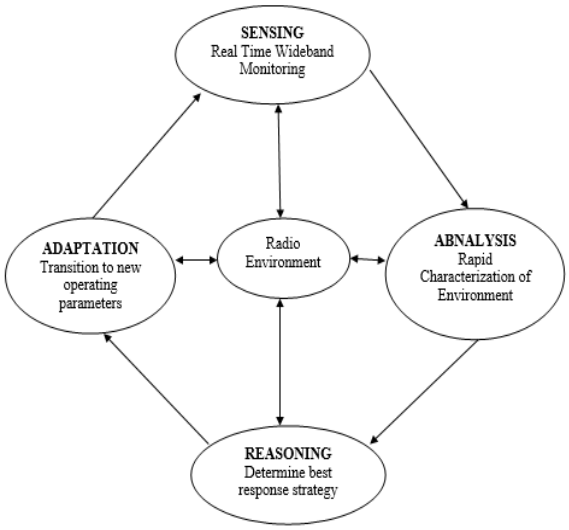

Fig. 1. Cognitive IoT Cycle.

II. SECURITY AWARE CHANNEL ASSIGNMENT IN THE PRESENCE OF CYBER ATTACKS

The cognitive radio framework tries in 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. 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. Security aware channel assignment means the assignment of frequencies to users which have lesser chances of security attacks. The major challenges in security aware channel assignment are:

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

1) Wireless nature of network
2) Frequent sharing of spectrum by users
3) Addition of noise in channel degradation
4) 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:

1) Cognitive radio networks are prone to attacks because of wireless nature of the channel
2) 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.
3) Security aware networks can detect possible jamming attacks which can help in decoding data at receiving end with higher accuracy and high throughput.

The spectrum is the most vital resource for increasingly large networks. As already a huge portion of the primary spectrum has been already reserved and assigned, it becomes an uphill task to find spectrum frequency bands for new services. Also there are regulations on the use of spectrum and its access by licensed users and unlicensed users cannot access them. For using the radio spectrum band in a more effective and beneficial manner, the concept of cognitive radio has become prominent. This is a form of technology that sues many layers and levels of processing and the cognition of the radio is able to look upon and detect the available frequency bands and search for the best available communication efficacy.

Thus sensing the spectrum is critically important for the CRN. The graphical illustration of the same if given below.

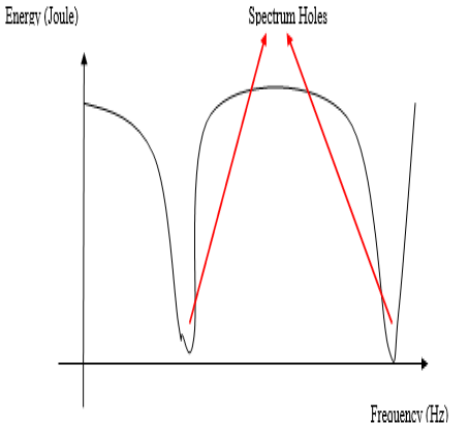

Fig.2 Energy Detection

. The sensing mechanism can be mathematically described as:

$$E_{sensed} = x(f) \quad (1)$$

Here,
E_{sensed} is the sensed energy
x(f) is the frequency dependent energy variation of the signal
However, the situation becomes challenging if there is addition of noise in the channel resulting in higher energy in the spectrum holes thereby leading to false detection of holes or even non-detection of holes. This is termed as false alarm. The false alarm is computed in terms of a probability. The dependent variable is a function of energy threshold chosen for detection of false alarm. The false alarm probability is given by

$$: Prob(FA) = Prob\left(\frac{H}{N.H.}\right) + Prob(\frac{N.H.}{H}) \quad (2)$$

Here,
Prob denotes probability
FA denotes false alarm
H denotes spectrum hole
N.H. denotes spectrum non-hole

The probability of false alarm is critically affected by noise effects. The threshold detected for noise can be instrumental in the false alarm rate. [5] The challenge associated with avoiding false alarm rate can be somewhat circumvented using other spectrum hole detection techniques such as cyclostationarity detection in which the channel is sensed with respect to repeated or reflected data.[7]. Alternative detection techniques can prove to sense the channel more accurately in case energy detection fails. [9]. The noise added false alarm is given by:

$$Prob(FA/N) = Prob\left(\frac{H/N}{N.H.}\right) + Prob(\frac{N.H./N}{H}) \quad (3)$$

Here,
Prob denotes probability
N denotes noise
FA/N denotes false alarm when noise addition occurs
H/N denotes spectrum hole when noise addition occurs
N.H./N denotes spectrum non-hole when noise addition occurs

III PREVIOUS WORK

This section presents the previous approaches adopted for channel assignment for cognitive radio networks along with their salient features.

In the year 2019, Haythem A. Bany Salameh et al. in [1] proposed a integration of cognitive radio (CR) technology with the future Internet-of-Things (IoT) for secure architecture is expected to allow effective massive IoT deployment by providing huge spectrum opportunities to the IoT devices. Several communication protocols have been proposed for the CR networks while ignoring the adjacent channel interference (ACI) problem by assuming sharp filters at the transmit and receive chains of each CR device. However, in practice, such an assumption is not feasible for low-cost hardware-constrained CR-capable IoT (CR-IoT) devices. Specifically, when a large number of CR-IoT devices are operating in the same vicinity, guard-band channels (GBs) are needed to mitigate the ACI problem, introducing GB adds constraints on the efficient use of spectrum and protocol design. In this paper, we develop a channel assignment mechanism for the hardware-constrained

CR-IoT networks under time-varying channel conditions with GB-awareness.

In the year 2018, Syed Hashim Raza et al. in [2] Simulated the 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.

In the year 2017, Haythem Bany et al. in [3] proposed a time critical approach based network. This network was cognitive in nature thereby sensing the 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 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 i.e. low jamming activity, moderate jamming activity and high jamming activity.
In the year 2017, K. J. Prasanna et al. in [4] proposed a reliable and secure architecture for routing in cognitive networks. 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.

In the year 2016, Keke Gai et al. in [5] the authors used the cloud platform to implement their approach. 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.

In the year 2016, Ju Ren et al. in [6] proposed techniques based on collaborative resource sharing in cognitive networks. 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.
In the year 2016, Rajesh K. Sharma et al. in [7] presented a survey on the measures 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.

In the year 2015, Maged Elkashlan et al. in [8] proposed a technique to assure the security of cognitive networks. 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.

In the year 2014, Erol Gelenbe et al. in [9] proposed 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.

In the year 2014, Mahmoud Khasawneh et al. in [10] presented a survey on the security of cognitive

networks. Different channel sensing techniques such as energy sensing, cyclo0-sttionarity 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.

IV. HARDWARE CONSTRAINTS IN NETWORKS

Cognitive IoT Networks are typically hardware constrained. In IoT networks such as WANs, data is shared among different devices (wirelessly) over internet. So the information does not travel through guided media (secure media). The information travels in free space. So it is possible to be attacked by attackers. Particularly in IoTs, if the data shared is critical data, attack on such data can cause serious issues such as:

1) Extraction of Data by Unauthorized users.
2) Data Modification
3) Denial of Service (DOS)
4) Data Corruption

So, securing the data transmission is necessary. However, this is a serious problem in securing the data transfer in IoTs due to the following reasons:

1) The data in conventional IoT networks which connect primarily devices such as mobiles and computers use complex encryption mechanisms such as AEC, TLS etc. for securing the data from attackers.
   Ex: In Whatsapp or gmail the data is encrypted using complex encryption algorithms such as AES, SHA, TLS algorithms etc. These algorithms need sufficient memory and processing power (processor) for implementation. Mobile phones or computers generally have sufficient memory and processing power.

2) However, in case of IoTs, the data is typically collected from sensors and connected devices which have very less memory and processing power. So implementing such complex encryption algorithms is not feasible.

Therefore, it is necessary to design mechanisms which would **NOT** include complex encryption techniques.

Conclusion: It can be concluded fro the previous discussions that security awareness in spectrum assignment is a critical aspect for cognitive IoT networks catering to defence and military applications or situations which deal with confidential and classified data. Various approaches pertaining to security in cognitive networks have been presented with their salient features. The probability of false alarm has also been investigated for ideal and practical channel conditions. It has been shown that hardware constraints poses a serous challenge in real time critical cognitive IoT networks. The paper presents the conventional and contemporary techniques to mitigate the issue of cyber attacks pertaining to such hardware constrained cognitive IoT Networks.

References

[1] Haythem A. Bany Salameh1, Saham Al-Masri, Elhadj Benkhelifa, And Jaime Lloret, “Spectrum Assignment in Hardware-Constrained Cognitive Radio IoT Networks Under Varying Channel-Quality Conditions”, IEEE 2021

[2] Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani,“ NS-2 based simulation framework for cognitive radio sensor networks”, SPRINGER 2020

[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 2019

[4] K. J. Prasanna Venkatesan ,V. Vijayarangan, “Secure and reliable routing in cognitive radio networks”,SPRINGER 2018

[5] Keke Gai ,Meikang Qiu ,Hui Zhao, “Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data”,IEEE 2017

[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

[18]Sazia Parvin ,Song Han ,Biming Tian ,Farookh Kadeer Hussain, "Trust-Based Authentication for Secure Communication in Cognitive Radio Networks", IEEE 2010

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

[20] S Sanyal, R Bhadauria, C Ghosh, "Secure communication in cognitive radio networks", IEEE 2009