International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

A Channel State Information Based Secure Channel Allocation Mechanism for Wireless Networks

Ayush Nagar[1], Prof. Pankaj Raghuwanshi[2]

Abstract: IoT networks have a great potential in supporting time-critical data delivery among the Internet of Things (IoT) devices and for emerging applications such as smart cities and automation. Due to continued sharing of resources, IoT networks often come under security attacks, most common of which are eavesdropping attacks. In the case of eavesdropping attacks, deliberately designed random eavesdropping data is added to the channel. These eavesdropping along with noise result in packet losses and low throughput, degrading the overall performance of the cognitive network. In this work, a security aware eavesdropping rejection mechanism is proposed which detects suspicious signals in the channel frequency response and employs discrete equalization to recover transmitted data. The proposed approach uses a CSMA-CD/EH protocol for possible adversarial eavesdropping attacks. The energy harvesting information is used to mitigate the possible attacks on the network at the gateway. The packet intercept ratio at the gateway is computed in the case of conventional CSMA-CD and the proposed system. The results show that the proposed system outperforms the exiting systems in terms of the performance metrics.

Keywords:- Internet of Things (IoT), Eavesdropping Activity, Carrier Sense Multiple Access-Collision Detection (CSMA-CD), Energy Harvesting (EH), Packet Intercept.

I.Introduction

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network. IoT is becoming very popular these days to satisfy the needs of increasing number of users and increased bandwidth needed per user due to multimedia and big data applications. The radio frequency spectrum is a limited that is divided into spectrum bands and is used for multiple applications. Currently, spectrum bands have been apportioned to diverse services, for example, mobile, fixed, broadcast, fixed satellite, and mobile satellite services. Spectrum is allocated to users or service providers and most often requiring licenses for operation, a crucial issue confronting future wireless systems is to discover suitable carrier frequencies and bandwidths to take care of the anticipated demand for future services.

The software and the programming languages on which IoT works uses very common programming languages that programmers use and already know.

Firstly, because embedded systems have less storage and processing power, their language needs are different. The most commonly used operating systems for such embedded systems are Linux or UNIX-like OSs like Ubuntu Core or Android. IoT software encompasses a wide range of software and programming languages from general-purpose languages like C++ and Java to embedded-specific choices like Google's Go language. The IoT parameters or channel state information (CSI). The main attribute of Cognitive radio systems is the fact the fact that it utilizes the spare part of the spectrum that is not being utilized by present users and is lying fallow, another aspect of which is resource allocation among networks that utilize cognitive system design.

This paper presents an energy harvesting based approach for detection of eavesdropping activity for Cognitive Networks. It is been shown that through energy detection and equalization, the proposed system attains higher throughput compared to previous systems.

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

II. Characteristics of a Cognitive Radio

The major characteristics of cognitive radios are given as:

1) Cognitive ability: It is the ability of Cognitive Systems to sense or catch the data from the radio surroundings of the radio technology. It can be said that cognitive radio constantly observes nature, orients itself, makes plans, decides, and then acts

2) Reconfigurability: It is continuously adapting to the changes in the spectrum that change the properties of the channel. Thus it can be said that it is the utilization of the channel state information. (frequency, transmission power, modulation scheme, communication protocol) of radio.

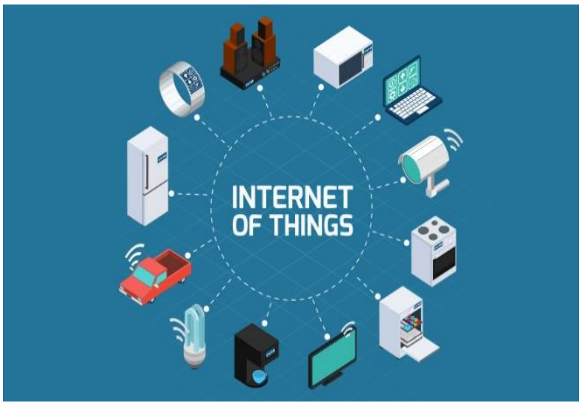

Fig.1 The IoT Framework

III. Adverserial Eavesdropping

Eavesdropping 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. This can be categorized in 3 cases:

1) Low eavesdropping
2) Moderate eavesdropping
3) High eavesdropping

The eavesdropping activity changes the channel response of system from an ideal nature to non-ideal natue. The eavesdropping activity can be gauged based on the channel state information (CSI) of the system. Howeber there are some challenges in utilizing the CSI. 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 eavesdropping 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)

IV. Proposed Algorithm based on CSMA-CD/EH.

Figure 2 depicts the IoT-energy harvesting technique at the hub/gateway of the network:

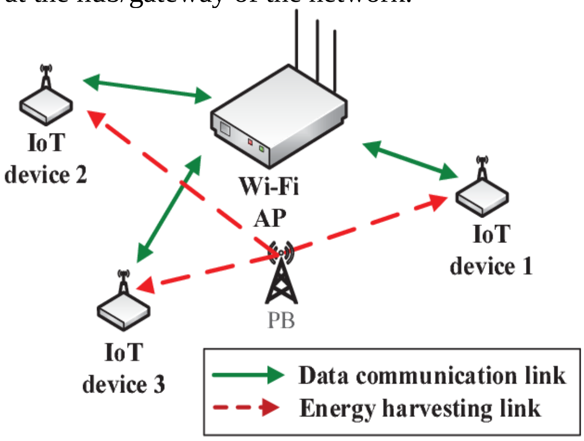

Fig.2 Energy Harvesting at Hub of IoT Network

The proposed technique with CSMA-CD/EH 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 eavesdropping mechanism.
Let the eavesdropping 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 eavesdropping action
The decision is to be based on:
Low Eavesdropping Activity: if sub-carrier gain<1.5*Ideal Subcarrier Gain
Moderate Eavesdropping Activity: if sub-carrier gain>1.5*Ideal Subcarrier Gain>2*Ideal Subcarrier
High Eavesdropping Activity: if sub-carrier gain>2*Ideal Subcarrier Gain

Step6. Generate signaling points for the system and obtain the scatter plot for:

- No Eavesdropping Action
- Low Eavesdropping Action
- Moderate Eavesdropping Action
- High Eavesdropping Action
  The scatter plots can be plotted for
  Re{x(n)}
  Img{x(n)}

Step7. Design a eavesdropping rejection mechanism using discrete frequency equalization
This can be done by designing a block with inverse response as that of the channel

Step8. Compute Packet Intercept for 3 cases:
1) Low Eavesdropping activity
2) Moderate Eavesdropping Activity
3) High Eavesdropping activity

$$H(freg) = f(freq)$$

Here,
$H(freg)$ represents the channel frequency response.
$f(freq)$ denotes a function of frequency.

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 following:

$h(t) = k(t); ideal\ collision\ condition$
$h(t) = k(t) + j(t); collision\ present$

The chances for a false alarm occur when there is collision present but the CSI suggest that collision is absent or vice versa. The chances of false alarm increase when there is actual addition of noise in the desired spectrum. It is noteworthy that such noise effects may lead to a false interpretation that there is collision 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. The effect can be summarized as follows:
Let the threshold for collision to be present by 'T'
If $h(t) > T; Collision\ presnet$
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 collision threat.

Results:

The results have been obtained using MATLAB. The various graphs obtained under the proposed system have been shown in the following section and the inferences are explained subsequently. A 500mx500m network with 1000 nodes has been chosen.

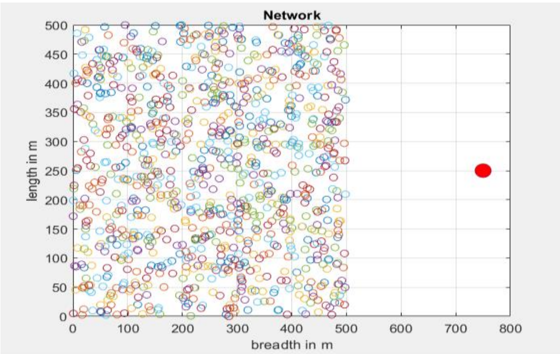

Fig.3 Network Design

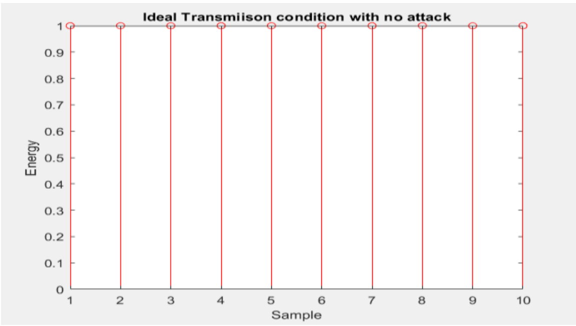

Fig.4 Ideal Transmission with No attack

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

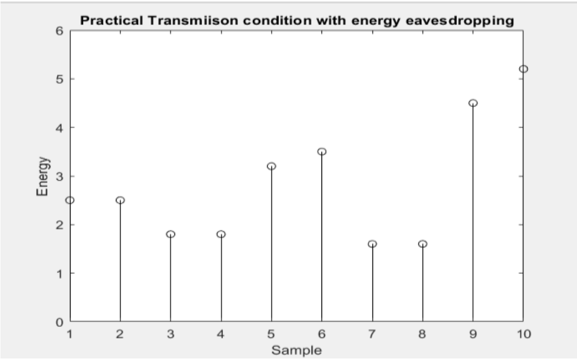

Fig.5 Practical Transmission with eavesdropping

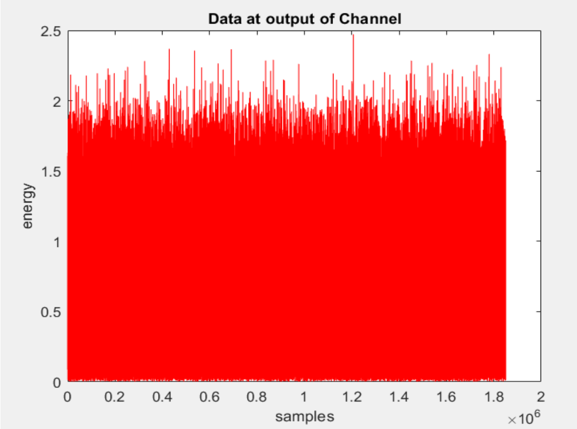

Fig.6 Packets at channel output

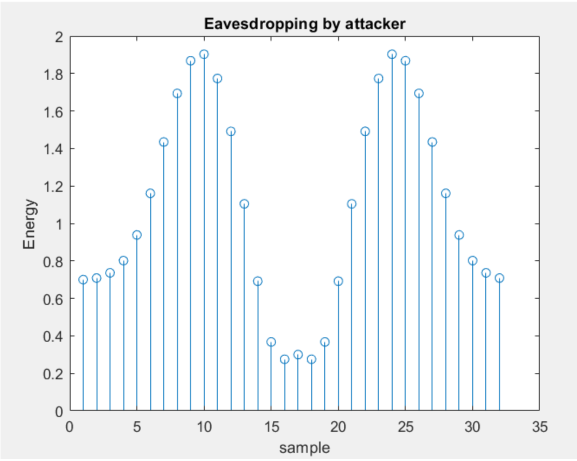

Fig.7 Condition of Eavesdropping

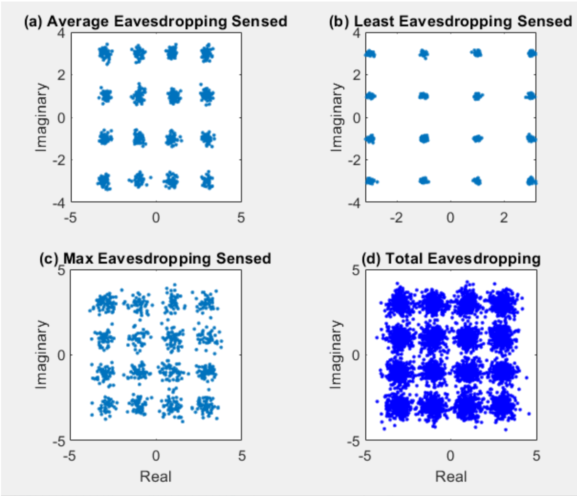

Fig.8 Energy Harvesting

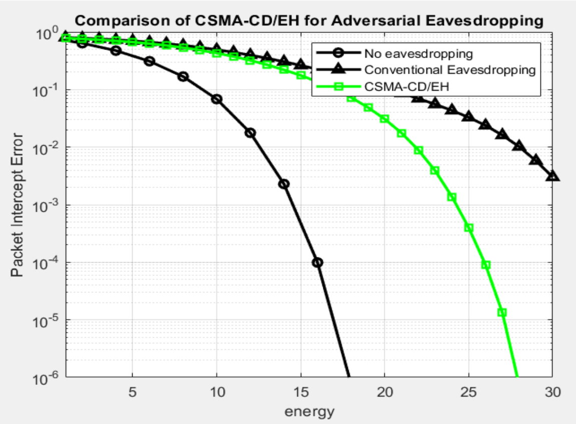

Fig.9 Packet Intercept

Conclusion: It can be concluded form the above discussions that IoT networks are being used for a wide variety of applications. The proposed approach uses a CSMA-CD/EH protocol for possible adversarial eavesdropping attacks. The energy harvesting information is used to mitigate the possible attacks on the network at the gateway. The packet intercept ratio at the gateway is computed in the case of conventional CSMA-CD and the proposed system. The results show that the proposed system outperforms the exiting systems in terms of the performance metrics.

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 2022
[2] Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani," NS-2 based simulation framework for cognitive radio sensor networks", SPRINGER 2021
[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 2020
[4] K. J. Prasanna Venkatesan ,V. Vijayarangan, "Secure and reliable routing in cognitive radio networks",SPRINGER 2019
[5] Keke Gai ,Meikang Qiu ,Hui Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data",IEEE 2018
[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