International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 08 | Aug - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Proactive Security Approach Against Illegal Intelligent Reflecting Surface (IIRS) Attacks

Zishan[1], Prof. Upvan Sharma[2]

Abstract: Illegal intelligent reflecting surfaces (I-IRSs), i.e., the illegal deployment and utilization of IRSs, impose serious harmful impacts on wireless networks. The existing I-IRS-based illegal jammer (IJ) requires channel state information (CSI) or extra power or both, and therefore, the I-IRS-based IJ seems to be difficult to implement in practical wireless networks. Due to continued sharing of resources, wireless 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 jamming and 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 chaos based FFH protocol for possible adversarial eavesdropping attacks. The error rate and average sum rate show that the proposed system outperforms the exiting systems in terms of the performance metrics.

Keywords:- Illegal Intelligent Reflecting Surface (IIRS), Jamming Attack, Packet Intercept. Error Rate, Sum Rate

I.Introduction

The emergence of Intelligent Reflecting Surfaces (IRS) has introduced innovative solutions for enhancing wireless communication by manipulating signals. However, this technology also opens the door to potential misuse. Illegal Intelligent Reflecting Surface (IIRS) based jamming attacks represent a concerning trend where these surfaces are exploited for disruptive purposes.

Intelligent Reflecting Surfaces are designed to improve signal strength and coverage by intelligently reflecting and redirecting wireless signals. These surfaces, typically composed of metamaterials, can adaptively adjust their properties to optimize signal transmission. 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.

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.

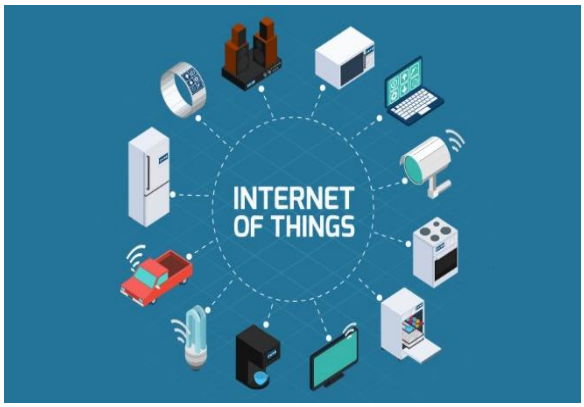

Fig.1 The IoT Framework

II. 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)

III. Proposed Algorithm

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

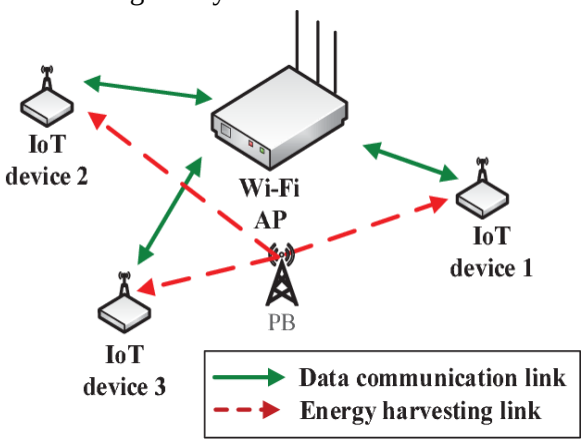

Fig.2 Energy Harvesting at Hub in a Wireless Networks

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)}

Step.7. Segregate the power levels for **Data and Artificial Noise.** Apply Power Access Control (PAC) Protocol. The number of frequencies changed is given by the **generation length (L).** However increasing L also increases BER of the system. Power Access Control means sending the data at low power level in between artificial noise. The time duration of artificial noise and actual signal is know only to Tx and Rx. Thus, only receiver can access the transmitted signal.
Step.8. Design a typical channel response of an ideal cognitive system.

Step.9 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

Step.10 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.

Jamming attacks on wireless networks involve the deliberate interference with the communication signals between devices, disrupting their ability to transmit or receive data. Perpetrators deploy various

techniques to generate interference, hindering the normal functioning of wireless networks and causing potential service disruptions. Jamming attacks often target specific frequencies or wireless protocols, exploiting vulnerabilities in the communication channels. Attackers may use radio frequency jammers to flood the targeted frequency bands or employ sophisticated techniques to disrupt specific wireless protocols, making it challenging for devices to maintain a reliable connection.

IV. 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.

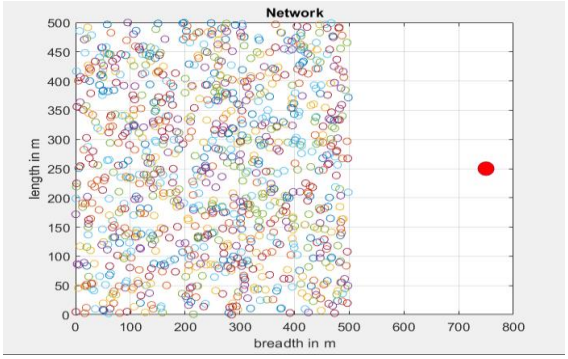

Fig.3 Network Design

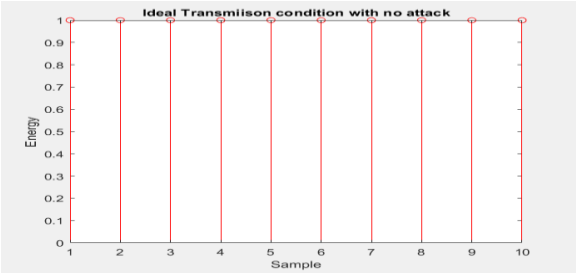

Fig.4 Ideal Transmission with No attack

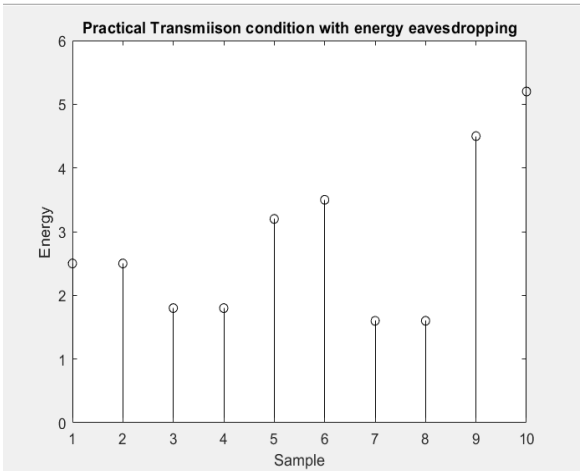

Fig.5 Practical Transmission with eavesdropping

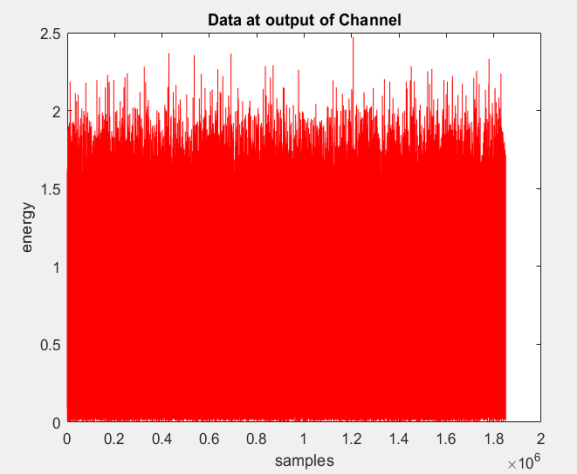

Fig.6 Packets at channel output

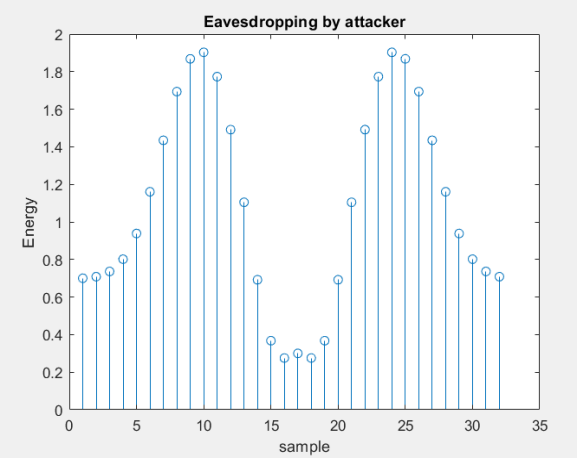

Fig.7 Condition of Eavesdropping

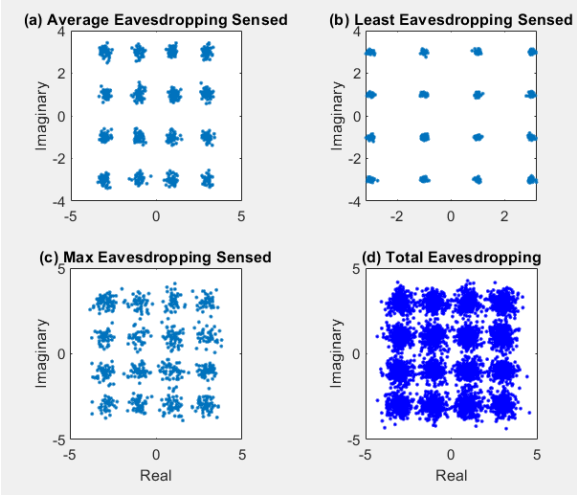

Fig.8 Energy Harvesting

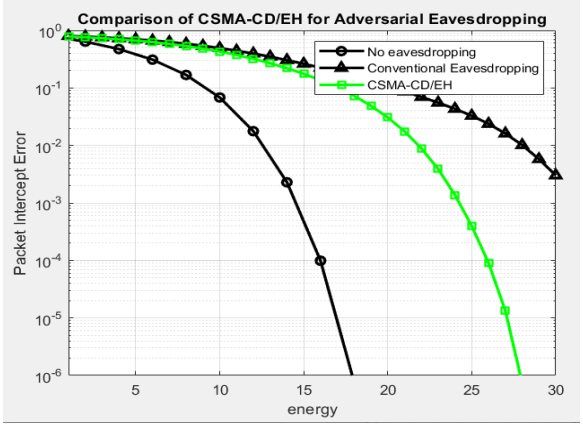

Fig.9 Packet Intercept

Conclusion: The proposed work presents a power access protocol for securing device to device networks. It has been discussed that with the increase in the data transfer capacity of stationary and predominantly handheld mobile devices, the data traffic of networks has increased manifold. The problem is more aggravating since the allocated bandwidth to networks is limited yet the bandwidth requirement of users is increasing by the day due to multimedia applications. The ease of cloud and bog data platforms is adding more data traffic to the already loaded network conditions

If FFH-Chaos is employed, the adversary is misled by generating artificial noise and it is injected into the actual data or bit stream. Due to the high signal strength of the artificial noise, it is difficult to detect the actual data stream with accuracy. The error rate and scatter have been computed to evaluate the performance of the system.

References

1. H. Huang, Y. Zhang, H. Zhang, C. Zhang and Z. Han, "Illegal Intelligent Reflecting Surface Based Active Channel Aging: When Jammer Can Attack Without Power and CSI," in IEEE Transactions on Vehicular Technology, vol. 72, no. 8, pp. 11018-11022, Aug. 2023.
2. F. T. Zahra, Y. S. Bostanci and M. Soyturk, "Real-Time Jamming Detection in Wireless IoT Networks," in IEEE Access, vol. 11, pp. 70425-70442, 2023.
3. H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, 2022, vol. 24, no. 2, pp. 767-809
4. J Singh, I Woungang, SK Dhurandher, K Khalid, “A jamming attack detection technique for opportunistic networks”, Internet of Things, 2022 – Elsevier, vol.17, 100464.
5. X. Cheng, J. Shi, M. Sha and L. Guo, "Launching Smart Selective Jamming Attacks in WirelessHART Networks," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, Vancouver, BC, Canada, 2021, pp. 1-10
6. E. Bout, V. Loscri and A. Gallais, "Energy and Distance evaluation for Jamming Attacks in wireless networks," 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Prague, Czech Republic, 2020, pp. 1-5
7. 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 2019
8. Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani,“ NS-2 based simulation framework for cognitive radio sensor networks”, SPRINGER 2018
9. 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
10. K. J. Prasanna Venkatesan ,V. Vijayarangan, "Secure and reliable routing in cognitive radio networks",SPRINGER 2017
11. Keke Gai ,Meikang Qiu ,Hui Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data",IEEE 2016
12. 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
13. Rajesh K. Sharma ;,Danda B. Rawat," Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey",IEEE 2015
14. Maged Elkashlan ,Lifeng Wang ,Trung Q. Duong , George K. Karagiannidis ,Arumugam Nallanathan, "On the Security of Cognitive Radio Networks",IEEE 2015
15. Erol Gelenbe," A Software Defined Self-Aware Network: The Cognitive Packet Network", IEEE 2014
16. Mahmoud Khasawneh ,Anjali Agarwal," A survey on security in Cognitive Radio networks", IEEE 2014
17. Yulong Zou, Xianbin Wang ,Weiming Shen," Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks",IEEE 2013
18. [12] Muhammad Faisal ,Amjad,Baber Aslam ,Cliff C. Zou, ," Reputation Aware Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks", IEEE 2013
19. 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\
20. Alvaro Araujo ,Javier Blesa,Elena Romero,Daniel Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems", SPRINGER 2012
21. 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
22. Ying-Chang Liang ,Kwang-Cheng Chen ,Geoffrey Ye Li ,Petri Mahonen, "Cognitive radio networking and communications: an overview", IEEE 2011
23. Gayathri Vijay ,Elyes Bdira ,Mohamed Ibnkahla, "Cognitive approaches in Wireless Sensor Networks: A survey", IEEE 2010