International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A CSI Based Security Aware Channel Assignment Mechanism for Software Defined Networks

Megha Jat
Asst. Professor (Computer Applications),
SAGE University, Indore, India

Abstract: Software Defined Networks (SDNs) 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. A wireless channel (radio) about which we have information is called a software defined radio. However, Software defined radio Networks 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 attacks. In the case of jamming attacks, deliberately designed random jamming signals are added to the channel. These jamming signals 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 rejection mechanism is proposed which detects suspicious signals in the channel frequency response and employs discrete equalization to recover transmitted data. Moreover, this also reduces the effects of noise in the channel. It has been shown that the proposed system achieves higher throughput compared to previous techniques for low, moderate and high jamming activity.

Keywords:- Software defined radio, Internet of Things (IoT), Jamming Activity, Energy Detection, Equalization, Throughput.

I.Introduction

A typical SDN generally has the capability of automatic fallback or handover. Handover may occur between two systems when the performance of once system starts to deteriorate compared to the other system [1]. The proposed approach aims at leveraging the handover mechanism for SDNs**.** In the proposed approach, a handover between a primary multiple access technique **(MA1)** and a secondary multiple access technique **(MA2)** is proposed with automatic fallback enabled receivers [2].

The condition for switching or handover is proposed to be the BER of the system based on different channel fading conditions [3].

The **SDN** would incorporate both:

1) Near and Far User cases
2) Fading conditions [4]

Moreover, for effective interference suppression, many MUD schemes also require an estimate of the covariance matrix of the received signal, which is typically the sample covariance matrix. The sample covariance matrix converges slowly, resulting in a poor estimate of the true covariance matrix when the number of samples of the received signal is relatively low [5].

Software defined radio (SDR) can be defined as a radio or radio frequency spectrum whose cognizance or knowledge is possessed by the user or service provider [6]. The tern cognizance or knowledge can be a little vague at times but the meaning of cognizance of a radio spectrum indicates towards the knowledge of its statistical parameters or channel state information (CSI) [7].

The main attribute of Software defined 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 [8].

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

II. Characteristics of Software Defined Radio

In the context of Software-Defined Networking (SDN), "handover" typically refers to the process of transferring the control of a network flow or connection from one network device to another. Handovers are crucial in scenarios where devices move or change their network attachment points, such as in mobility scenarios or when dealing with virtualized network functions. Handover mechanism include [11]-[12]:

Centralized Control: In an SDN architecture, the control plane is centralized in an SDN controller. The controller has a global view of the network and can make decisions about

how to manage handovers. When a device, like a mobile user or a virtual machine, moves from one part of the network to another, the SDN controller can dynamically update forwarding rules to ensure that the flow or connection is seamlessly handed over to the appropriate devices [13].

Dynamic Flow Management: SDN enables dynamic flow management, allowing the controller to modify flow entries in the switches or routers to redirect traffic as needed. This is particularly useful in scenarios where a device transitions between different access points or network segments [14].

Programmability through Northbound APIs: SDN controllers expose northbound APIs that allow higher-level applications to communicate with the controller. Applications responsible for mobility management or handover decision-making can use these APIs to instruct the controller on how to handle handovers [15]

Flow Prioritization: SDN allows for the prioritization of network flows. When a handover occurs, the controller can ensure that critical or real-time traffic is given priority during the transition to maintain quality of service [16].

Integration with Network Function Virtualization (NFV): In virtualized environments, SDN often works in conjunction with NFV. Virtualized network functions (VNFs) can be dynamically instantiated or migrated to different locations in response to changes in network conditions, and the SDN controller plays a role in managing this dynamic instantiation or migration [17].

By centralizing control and providing a programmable interface, SDN simplifies the management of handovers in networks, making them more efficient and adaptable to changing conditions [18].

This is particularly valuable in scenarios where seamless connectivity and mobility are critical, such as in mobile networks, IoT environments, or data center networks with virtualized [19]

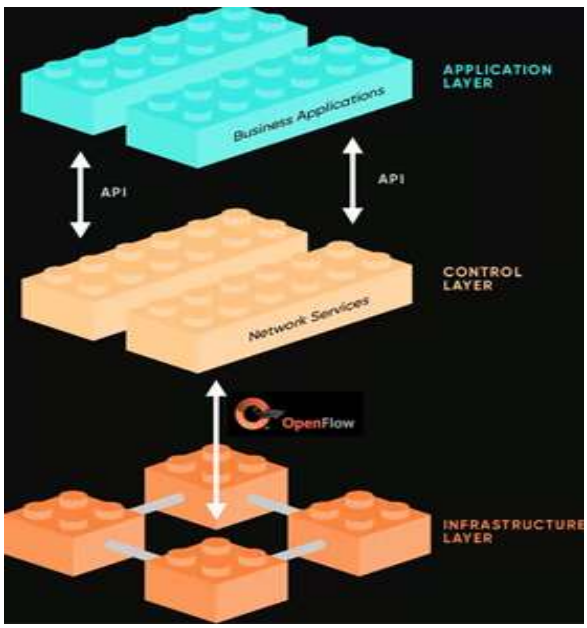

Fig.1 Architecture of SDN

III. Jamming Activity in Software defined radio Systems.

Jamminng attacks are the most common form of attack for software defined 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 [20]:

1) Low jamming activity
2) Moderate Jamming Activity
3) High Jamming Activity

The jamming activity changes the channel response of system from an ideal nature to non-ideal natue. The jamming activity can be gauged based on the channel state information (CSI) of the system. Howeber there are some challenges in utilizing the CSI [21]. Main Challenges faced in Spectrum Sensing in Software defined radio Systems [22]

1) Wireless channels change randomly over time, therefore sensing wireless channels before they change is tough [23].
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 software defined 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.

The proposed technique 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 jamming mechanism.

Let the jamming 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 jamming action
The decision is to be based on:
Low Jamming Activity: if sub-carrier gain<1.5*Ideal Subcarrier Gain
Moderate Jamming Activity: if sub-carrier gain>1.5*Ideal Subcarrier Gain>2*Ideal Subcarrier
High Jamming Activity: if sub-carrier gain>2*Ideal Subcarrier Gain

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

- No Jamming Action
- Low Jamming Action
- Moderate Jamming Action
- High Jamming Action

The scatter plots can be plotted for
Re{x(n)}
Img{x(n)}

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

Step8. Compute Throughput for 3 cases:
1) Low Jamming activity
2) Moderate Jamming Activity
3) High Jamming activity

The above figure depicts the channel frequency response of a typical wireless channel. It can be seen that it varies with the frequency i.e.

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

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

V. Results:

The experimental setup has been conducted for 1 million bits. The various graphs obtained under the proposed system have been shown in the following section and the inferences are explained subsequently.

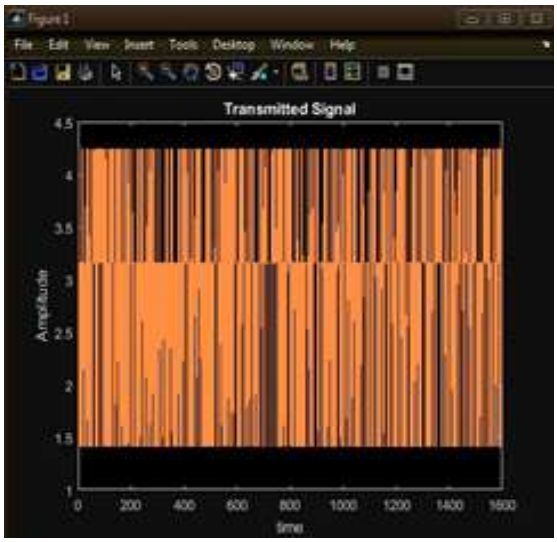

Fig.2 Transmitted binary signal

The above figure depicts the transmitted binary signal in the form of 1s and 0s.

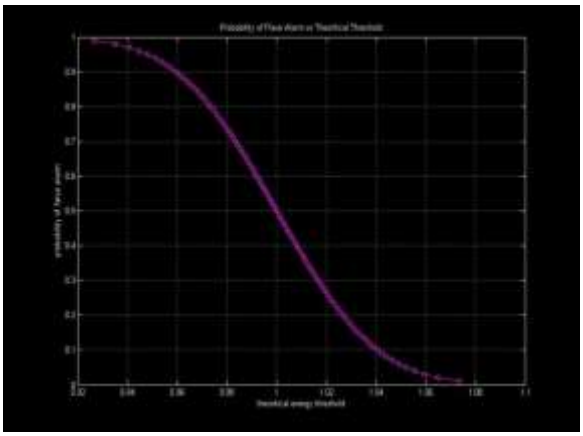

Fig.3 Probability of False Alarm

The above figure depicts the transmitted binary signal in the form of 1s and 0s.

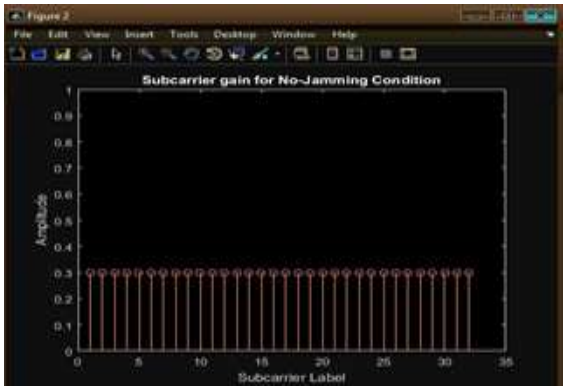

Fig.4 Subcarrier Gain for Non-Jamming Condition

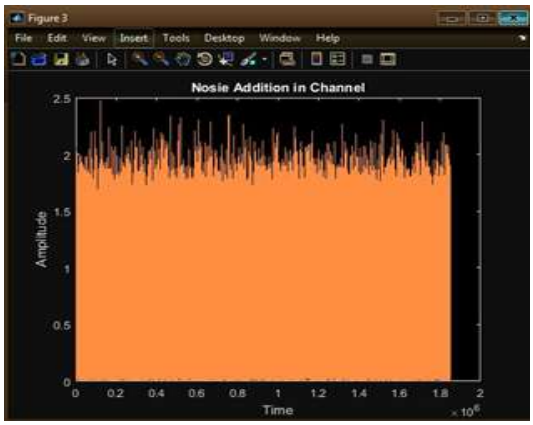

Fig.5 Addition of Noise in the Channel

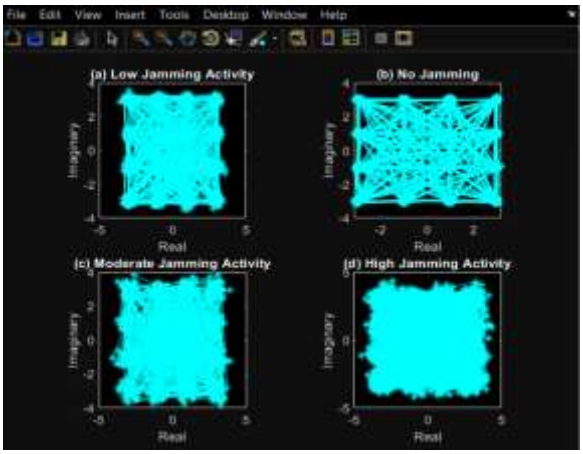

Fig.6 Scatter Plot for Different Jamming Conditions

Figure 5 depicts the addition of noise in the channel while figure 6 depicts the channel scatter.

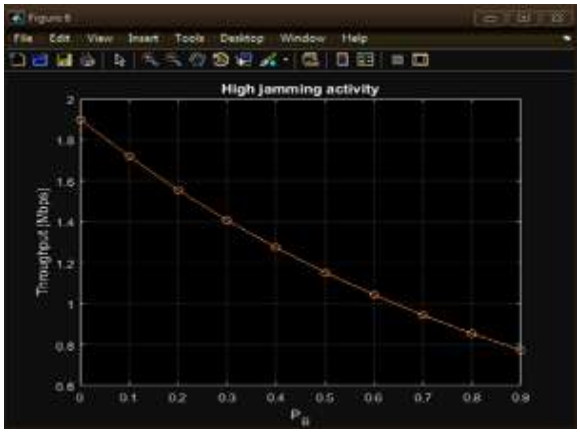

Fig.6 Throughput for High Jamming Conditions

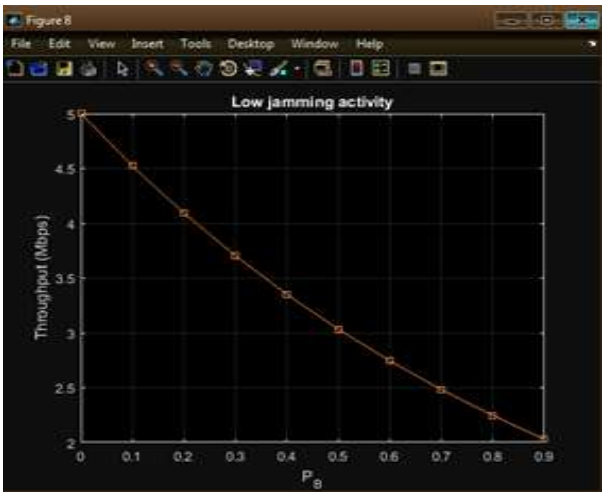

Fig.7 Throughput for Low Jamming Conditions

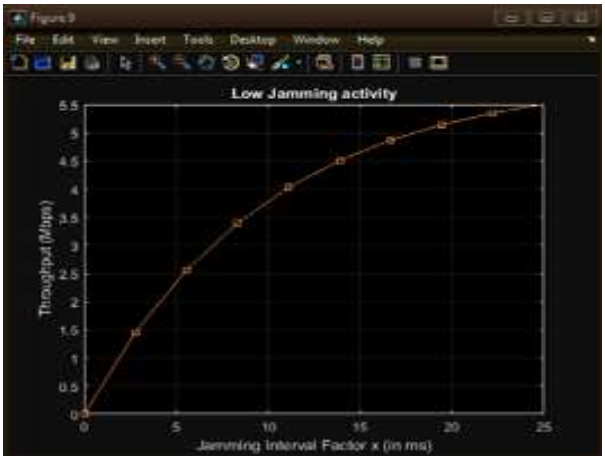

Fig.8 Throughput Analysis with respect to jamming interval (low jamming)

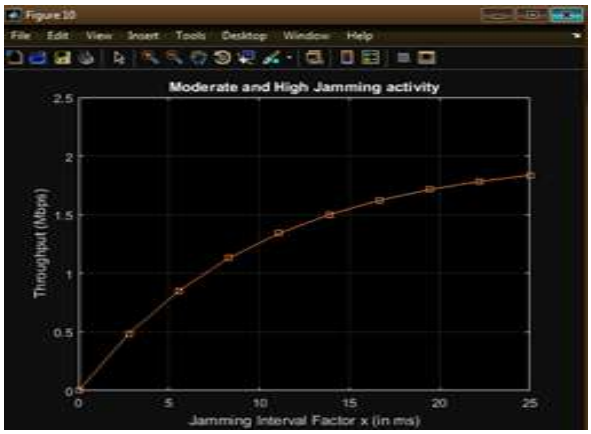

Fig.9 Throughput Analysis with respect to jamming interval (moderate and high jamming)

VI. Conclusion:

It can be concluded form the above discussions that the proposed system attains better throughput compared to the previous work (Security-aware Channel Assignment in IoT-based Software defined radio Networks for Time-Critical Applications. This has been achieved by using energy detection for software defined radio. The analysis has been

performed for 3 cases of jamming activity: Low jamming activity, Moderate jamming activity and High Jamming activity The results can be attributed to energy detection and subsequent discrete frequency equalization.

References

1. L. D. Manocchio, Y. Chen, S. Layeghy, D. Gwynne and M. Portmann, "P4-Secure: In-Band DDoS Detection in Software Defined Networks," in IEEE Transactions on Network and Service Management, 2025, vol. 22, no. 2, pp. 2120-2137
2. H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao and Q. Wu, "Deep Reinforcement Learning Based Intelligent Reflecting Surface for Secure Wireless Communications," *IEEE*, Feb. 2020.
3. K. St. Germain and F. Kragh, "Physical-Layer Authentication Using Channel State Information and Machine Learning," *IEEE*, Jun. 2020.
4. A. Senigagliesi, L. Baldi and E. Gambi, "Performance of Statistical and Machine Learning Techniques for Physical Layer Authentication," *arXiv*, 2020.
5. A. Albehadili *et al.*, "Machine Learning-Based PHY-Authentication for Mobile OFDM Transceivers," in *Proc. IEEE VTC 2020-Fall*, 2020.
6. G. Gao, N. Ni, D. Feng, X. Jing and Y. Cao, "Physical Layer Authentication Under Intelligent Spoofing in Wireless Sensor Networks," *Signal Processing*, vol. 166, 2020.
7. L. Liao *et al.*, "Multiuser Physical Layer Authentication in Internet of Things with Data Augmentation," *IEEE Internet of Things J.*, vol. 7, no. 3, pp. 2077–2088, Mar. 2020.
8. H. Fang, X. Wang, Z. Xiao and L. Hanzo, "Autonomous Collaborative Authentication with Privacy Preservation in 6G: From Homogeneity to Heterogeneity," *IEEE Network*, vol. 36, no. 6, pp. 28–36, Jul. 2022.
9. R. Xie *et al.*, "A Generalizable Model-and-Data Driven Approach for Open-Set RFF Authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4435–4450, Aug. 2021.
10. C. Li, C. She, N. Yang and T. Q. S. Quek, "Secure Transmission Rate of Short Packets with Queueing Delay Requirement," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 203–218, Jan. 2022.
11. X. Zeng, C. Wang and Z. Li, "CVCA: A Complex-Valued Classifiable Autoencoder for mmWave Massive MIMO Physical Layer Authentication," presented at *IEEE INFOCOM Workshops*, 2023
12. T Burton, K Rasmussen, "Private data exfiltration from cyber-physical systems using channel state information" ACM SIGSAC Conference on Computer and Communications Security, ACM 2021, PP.223-235.
13. AA Sharifi, M Sharifi, MJM Niya, "Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach", vol.70, issue.1, Elsevier 2020.
14. Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani," NS-2 based simulation framework for cognitive radio sensor networks", SPRINGER 2019/.
15. K. J. Prasanna Venkatesan ,V. Vijayarangan, "Secure and reliable routing in cognitive radio networks", SPRINGER 2018.
16. Ara and B. Kelley, "Physical Layer Security for 6G: Toward Achieving Intelligent Native Security at Layer-1," in IEEE Access, 2024, vol. 12, pp. 82800-82824.
17. K Gai ,Meikang Qiu ,Hui Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data",IEEE 2017.
18. 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.
19. R.K. Sharma ;,Danda B. Rawat," Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey",IEEE
20. A. Khamaiseh, I. Alsmadi, and A. Al-Alaj, "Deceiving Machine Learning-based Saturation Attack Detection Systems in SDN," in Proc. IEEE NFV-SDN, 2020.
21. M. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença Jr., "A GRU Deep Learning System Against Attacks in Software Defined Networks," J. Network and Computer Applications, vol. 177, p. 102942, 2021.
22. J. Bhayo et al., "A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN," IEEE Internet of Things J., vol. 9, no. 5, pp. 3612–3630, Mar. 2022.
23. K. G. Yalda, D. J. Hamad, N. Tapus and I. T. Okumus, "Security Issues in Software-Defined Networking (SDN) Environments," 2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2024, pp. 1-8