**Journal of Information Systems Engineering and Management**
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Securing the Internet of Things (IoT) against possible intrusions based on Channel State Information (CSI) and Peak to Average Power (PAPR) Reduction

Navashish Kaur[1], Dr. Dinesh Kumar[2]
*Department of Computer Science and Engineering[1,2]*
*GZSCCET, MRSPTU Bathinda, Punjab, India[1,2]*
*Corresponding Author: Navashish Kaur, navashish@gmail.com*

**ARTICLE INFO**

Received: 09 Nov 2024
Revised: 27 Dec 2024
Accepted: 13 Jan 2025

**ABSTRACT**

Conventional computer networks are being replaced with more pervasive networks such as the Internet of Things (IoT) and fog computing networks. Pervasive networks lay a constraint on the amount of processing power and memory for the diverse type of connected devices. This leads to investigating security measures which can be applied to the pervasive network structure so that it secures the network at multiple levels of the OSI model. This paper presents a proactive approach which combines leveraging the channel state information (CSI) as well as minimizing the PAPR of the system so as to enhance the security in both aspects of security aware channel assignment as well as introducing imperceptibility in data transmission over the security aware channel assignment protocol. The effectiveness of leveraging security aware channel assignment is evaluated in terms of the BER and sum secrecy rate of the system while the imperceptibility is evaluated in terms of the PAPR or crest factor value. The paper also combines MIMO-equalization so as to enhance the spectral efficiency of the system. A comparison with existing work in the domain clearly demonstrates the improvement of the proposed approach in terms of the performance metrics.

**Keywords:** Internet of Things (IoT), Channel State Information (CSI), PAPR, MIMO, Spectral Efficiency, Sum Secrecy Rate

## 1. Introduction

Modern wireless networks such as IoT, fog and edge computing face several security challenges due to increasing data traffic, constraints of processing power and memory and evolving cyber attacks [1]. Hence, it is necessary to design proactive security frameworks which can enhance the security of pervasive wireless networks as opposed to conventional intrusion detection systems (IDS) and network intrusion detection systems (NIDS) which are typically rely on rule based approaches [2] To attains satisfactory Quality of Service (QoS), the bit error rate and outage should be low, while for seamless data transfer, the system spectral efficiency and sum secrecy rate should be high. The imperceptibility of the system can be increased through reducing the Peak to Average Power Ratio (PAPR) of the system.

The Internet of Things (IoT) is witnessing a staggering increase due to large scale automation and evolution of AI systems. Figure 1 depicts the forecast of IoT revenue till 2033 in billion USD.

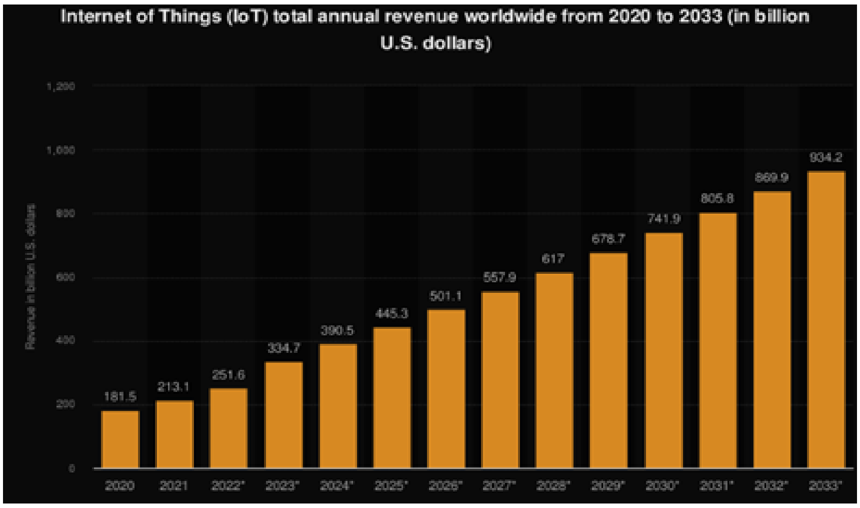

Fig.1 Forecast of rise of IoT Market Revenue by 2033

(Source: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/)

The continued increase of the IoT industry and IoT applications also has its fair share of challenges [3]. The Internet of Things (IoT) has revolutionized industries by connecting billions of devices to networks, enabling automation, efficiency, and real-time monitoring. However, this rapid expansion has also introduced significant security risks [4]. Intrusion Detection Systems (IDS) play a critical role in identifying and mitigating cyber threats in IoT networks. Despite their importance, IDS implementation in IoT environments faces several limitations and challenges that hinder their effectiveness. The major aspects are presented next [5]:

**Resource Constraints:** One of the primary challenges in securing IoT networks through IDS is the resource-constrained nature of IoT devices. Many IoT devices operate with limited processing power, memory, and battery life, making it difficult to deploy traditional IDS solutions [6]. These limitations prevent IoT devices from performing complex anomaly detection or real-time traffic analysis, leaving them vulnerable to cyber threats [7].

**High Volume of Data and Traffic:** IoT networks generate vast amounts of data due to continuous device communication. Monitoring and analyzing this data in real time using IDS can overwhelm computational resources, leading to performance degradation [8]. The sheer volume of network traffic makes it difficult to differentiate between normal and malicious activities, increasing the risk of false positives and false negatives in threat detection [9].

**Lack of Standardization:** The IoT ecosystem comprises a wide variety of devices, manufacturers, and communication protocols, many of which lack standardized security frameworks [10]. This diversity makes it difficult for IDS to apply uniform security policies or detect anomalies consistently across different devices. Without standardization, IDS implementations remain fragmented, limiting their ability to provide comprehensive security coverage.

**Scalability Issues:** As IoT networks continue to expand, IDS must scale accordingly to monitor a growing number of connected devices. Traditional IDS solutions designed for enterprise networks struggle to adapt to the dynamic and heterogeneous nature of IoT environments. The challenge lies in developing scalable IDS architectures that can efficiently analyze large-scale IoT deployments without compromising detection accuracy or network performance [11]

**Evasion Techniques by Attackers:** Adversaries continuously develop sophisticated evasion techniques to bypass IDS mechanisms. Attackers may use encrypted traffic, obfuscation methods, or low-rate attacks to avoid detection. Since many IoT IDS solutions rely on signature-based detection, they may fail to identify new or zero-day attacks that do not match predefined attack patterns. Enhancing IDS with advanced threat intelligence and machine learning techniques is necessary but adds complexity and computational overhead [12].

**Privacy and Legal Concerns:** Deploying IDS in IoT networks often involves monitoring sensitive data generated by smart devices, raising privacy and legal concerns. Some IDS implementations require deep packet inspection, which can violate user privacy by analyzing personal or confidential information. Additionally, different regions have varying data protection laws, making it challenging to implement IDS solutions that comply with global security and privacy regulations [13].

## 2. Security Issues in IoT Networks.

Computer Networks are migrating from the wired to the wireless domain due to the following reasons [14]:

1. Ease of mobility: easy to mode the connected devices.
2. Scalability: Adding or removing devices, avoiding cabling cost.

However, due to the lack of guided media like LAN cables etc., chances of attacks on the network also increase. The IoT framework typically has copious amounts of data being generated and collected at the IoT-WAN gateways [15].

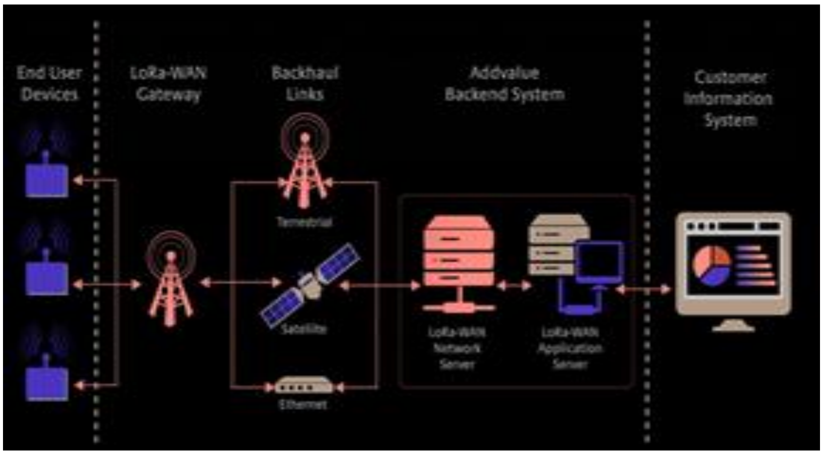

Fig.2 The IoT-WAN Interconnection

With wide area networks coming under the purview of the IoT framework, the WAN-IoT interface is depicted in figure 2.

As concurrent execution applications are becoming popular for live streaming, cloud and fog applications, the necessity for wide area networks with low latency and high bandwidth efficiency has become mandatory [16]. This doorway of high efficiency and low latency networks is based on the fact that the IoT paradigm is all inclusive of the diverse types of devices which an be connected over a wide area network. The challenge for such massive networks would certainly remain the security aspect of the network, which eavesdropping and jamming being the major concerns [17].

### *2.1 Cognitive IoT Networks*

One of the most recent IoT sub-classes is the cognitive IoT Networks which are typically termed as CINs. Such network rely on the fact that the channel state information (CSI) value for time bound IoT transmission is available for the network designer whose choice of data transmission in the network would decide the latency and the throughput of the system [18]. One of the most common approaches which adversarial techniques employ is jamming subparts of the specturm where the possible data transmission is to occur. Thus for the jamming power to be used for a specturm of bandwidth 'W', the jamming power average would be computed as [19]:

$$\boldsymbol{P_J = \frac{1}{N}\sum_{i=1}^{N} B_i S_i} \qquad \textbf{(1)}$$

Here,

$P_J$ is the mean jamming power.

N is the total number of transmission sub-bands

B is the sub-band bandwidth

S is the allocation per subband

As the mean would be much less than a particular sub-band energy for jamming, hence it is necessary to conceptrate the jamming power to a specific bandwidth section as [20]:

$$\boldsymbol{P_{J-mean} \ll P_{J-S}} \qquad \textbf{(2)}$$

Here,

$P_{J-mean}$ is the mean jamming power across the entire bandwidth

$P_{J-S}$ is the sub-band jamming

Fundamentally, there can be two basic appraoches for securing the WAN-IoT framework which are:

1) A NIDS appraoch based on intrusion detetcion.
2) A proactive approach based on secure assignment of bandwidth.

### *2.2 Attributes of Conitive IoT*

While typical IDS or NIDS is more of a reactive appraoch, the second is more of a proactive approach. In such a security aware process, a dummy packet is sent from transmitting end to the receiving end to sense the channel [21]

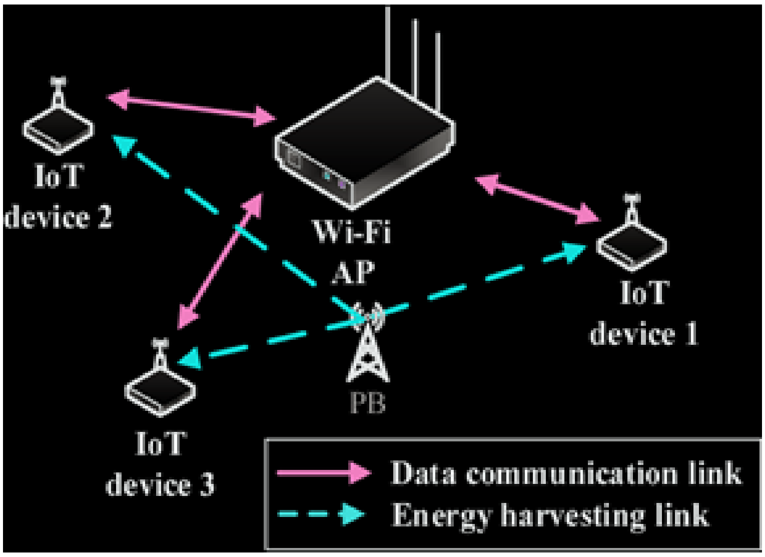

Fig.3 Energy Harvesting at Hub of IoT Network

The possibility of attack is evaluated. The bandwidth with least possibility of attack is chosen for data transmission. It is a proactive approach to avoid jamming attacks in the network. Equalization is typically performed to reduce error rates and increase throughput [22]. Figure 3 depicts the IoT-energy harvesting technique at the hub/gateway of the network. One major challenge however remains the fading nature of the channels typically exhibiting a Rayleigh distribution. Energy harvesting is an innovative approach that allows IoT devices to collect and utilize energy from ambient sources such as solar power, radio frequency (RF) signals, thermal gradients, and vibration. By harvesting energy from the environment, IoT devices can reduce dependency on batteries and extend their operational lifespan. This technique is particularly beneficial for remote or hard-to-reach locations where battery replacement is difficult. However, efficient energy management strategies are necessary to optimize harvested energy utilization and ensure seamless network performance. The typical urban environment for an IoT-WAN network is depicted in figure 4.

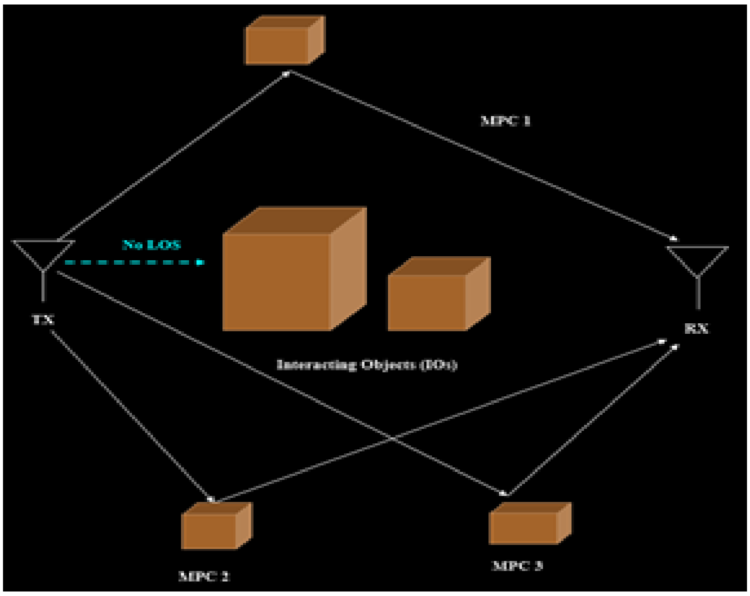

Fig.4 Rayleigh Model

The urban environment in terms of a Rayleigh model typically lacks a clear line of sight (LOS) path while containing multiple reflected paths of data transfer [23]. This results in the waxing and weaning of the IoT strength at the receiving end depicted in figure 5.

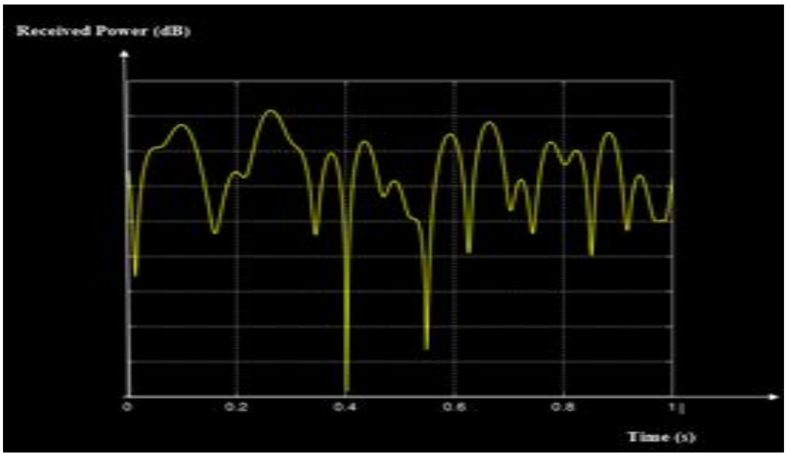

Fig.5 Received waxing and weaning pattern

Figure 5 depicts the waxing and weaning pattern signal patterns for a typical IoT network hub or gateway. Security aware channel assignment in such a case needs to be implemented through estimation of the CSI of the networks [24].

## 3. Proposed Security Framework

The proposed security framework combines the following approaches to come up with a novel and holistic approach for securing IoT networks:

1. Estimating the CSI for security aware channel assignment.
2. Increasing imperceptibility through reduction of PAPR
3. Combining MIMO-Equalization to enhance spectral efficiency and sum secrecy rate.

Each of the approaches are presented next:

### 3.1 Estimating CSI for Security Aware Channel Assignment

Security aware channel assignment requires correct estimation of CSI. The research framework proposed in this work tries to design a proactive security mechanism rather than a reactive security or authentication mechanism [25].

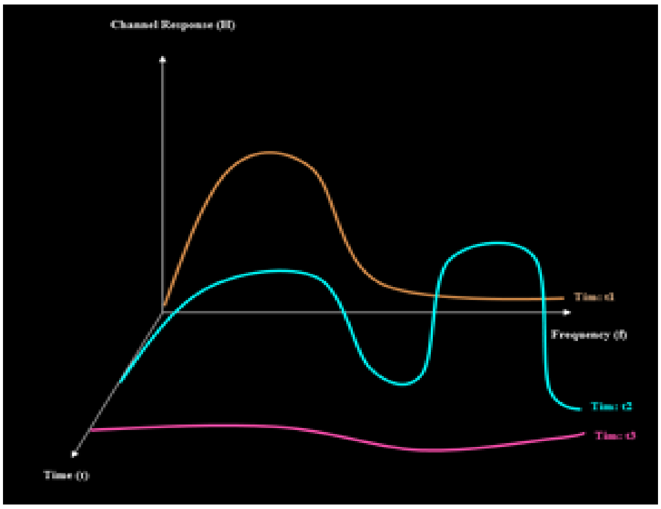

Fig.6. Time varying CSI

The conceptualization of the time varying CSI of the channel is depicted in figure 6. The cognitive radio network (CRN) framework is proposed in this approach which collects the information regarding the channel continuously to possess cognizance or information regarding the transmission channel. The approach proposed in this paper is based on the following considerations, which can be assumed without loss of generality. The attackers have limited jamming power $P_j$ as hence would attack only sections of the entire transmission bandwidth $B_{tr}$. If the channel can be sensed iteratively every $T_s$ seconds, then the time varying channel sense information (CSI) can be obtained which can be used to thwart security attacks [26]. In this case, the channel can be sensed through the following algorithm:

***Algorithm for Security Aware Channel Assignment:***

***Step.1 :*** *Initialize iteration counter i to 1.*

***Step.2*** *Transmit dummy data $x'$ through the channel $h(t)$.*

***Step.3:*** *Obtain the output of the ideal channel as:*

$$\boldsymbol{y(t) = \int_{t_i}^{t_f} x(t)h(t-\delta)dt} \qquad \textbf{(3)}$$

*Here,*

*$y(t)$ denotes the output of the channel.*

*$h(t-\delta)$ is the time varying channel response with a delay of $\delta$.*

*$t_i$ and $t_i$ are the initial and final time stamps for data transmission.*

***Step.3:*** *Compare the actual channel output $y'(t)$ and compute the correlation among $y(t)$ and $y'(t)$.*

***Step. 4:*** *Estimate the actual channel response $h(t)$ iteratively by sensing the channel every $T_s$ seconds rendering the channel state information (CSI).*

***Step.5:*** *Estimate the magnitude of jamming and categorize it into 4 categories:*

*a) No jamming.*
*b) Low jamming.*
*c) Moderate Jamming.*
*d) High Jamming.*

***Step.6:*** *Avoid the spectral*

*regions of moderate and high jamming attack and utilize no or low jamming attack regions.*

***Step.7:*** *Based on step 4 above, design a feedback based adaptive equalizer to nullify the effects of the noise and disturbance in the channel as:*

$$E_{Periodic} = \frac{1}{h(t)} \qquad (4)$$

***Step.8:*** *Compute the bit error rate, scatter and throughput of the system.*

To mitigate security risks, a security-aware channel assignment approach can be employed to dynamically allocate communication channels based on real-time threat detection and energy efficiency. This strategy involves continuously monitoring the network for potential intrusions and assigning channels that minimize interference and enhance security. For example, frequency hopping techniques can be used to prevent attackers from intercepting data by frequently switching between channels. Additionally, machine learning-based algorithms can analyze network traffic patterns and predict secure channel allocations, ensuring robust protection against cyber threats [27].

### *3.2 Increasing Imperceptibility*

While security aware channel assignment is effective in thwarting several jamming attacks, a more holistic approach is employing imperceptibility so as to avoid most attacks from adversaries [28]. As IoT and wireless networks are vulnerable to various security threats, including eavesdropping, jamming, and unauthorized interception. High PAPR signals are more susceptible to detection by adversaries using advanced radio frequency (RF) surveillance techniques. Attackers can identify and localize wireless transmissions with high peak power, making it easier to disrupt or manipulate communications. In contrast, reducing PAPR helps minimize the visibility of transmitted signals, making them blend more effectively with background noise, thereby reducing the likelihood of detection and targeted attacks [29].

The proposed approach employs the Selective Mapping (SLM) bases chaotic approach to increase imperceptivity. The essence of the SLM approach is its chaotic behaviour and no loss of information unlike clipping. The selective mapping (SLM) technique aims to exploit differences in the signal crest factor by using shift vectors represented as complex values. The PAPR is defined as:

$$CF \text{ or } PAPR = \frac{Peak\ Power\ \{x(t)\}}{Average\ Power\ \{x(t)\}} \qquad (5)$$

The shift vectors alter the temporal characteristics of the signal or data stream. The crest factor varies with the incorporation of the vectors in the sample set. (b1, b2..........................bn). Each vector addition yields a distinct crest factor, hence altering the PAPR. In the SLM approach, the shift vector b that minimizes the crest factor value is identified among all versions of the signal X [30]. The selective mapping relies on reduction of the PAPR based on different phasor products. Integrating PAPR reduction strategies inside network-level security frameworks might operate as a preemptive approach to mitigate security vulnerabilities [31]. Reducing PAPR decreases power consumption, mitigates the likelihood of signal distortion, and enhances the network's resilience against external interference, including jamming or interception. Consequently, communication systems enhance their resilience, thereby augmenting the efficiency and security of the network architecture [32].

To further reduce the PAPR from the SLM, a windowing based approach with an inverted sync function is employed. The PAPR reduction approach is presented next:

***Step.1:*** *Generate random binary data stream **X** emulating an actual data transmission environment.*

***Step.2:*** *Convert the data from serial to parallel employing the transpose operation.*

$$Y = X^T \qquad (6)$$

*Here,*

*T denotes the transpose operation.*

***Step.3:*** *Compute the Fast Fourier Transform of the parallel data.*

$$\boldsymbol{ZZ = FFT(Y)} \qquad \textit{(7)}$$

***Step.4:*** *Add different phase or delay vectors to the data stream to generate multiple shifts and hence multiple copies of the data stream with different PAPR values.*

$$\boldsymbol{S_{delay} = [\, S_1, S_2 \dots \dots \dots S_n]} \qquad \textit{(8)}$$

***Step.5:*** *The addition of $S_{delay}$ would result in the generation of multiple copies of the data signal Y expressed as:*

$$\boldsymbol{Y_{composite} = [\, Y_1, Y_2 \dots \dots \dots Y_n]} \qquad \textit{(9)}$$

***Step.6:*** *From $\boldsymbol{Y_{composite}}$ search the copy of the data stream which has the least PAPR i.e.*

$$\boldsymbol{for\ i = 1{:}\,n}$$

$\boldsymbol{find\ (min([\, Y_1, Y_2 \dots \dots \dots Y_n]))}$

***Step.7:*** *Decide the threshold (T) for the residual peaks of the data stream as:*

$$\boldsymbol{T = mean\{max(X)\, , mean(X)} \qquad \textit{(10)}$$

***Step.8:*** *Apply the windowing function*

$$\boldsymbol{Sync_{inv} = \frac{1}{sin\,(\pi z)/\pi z}} \qquad \textit{(11)}$$

***Step.9****: Compute the CCDF of the PAPR.*

### *3.3 MIMO-Equalization*

To enhance the spectral efficiency and sum secrecy rate, the MIMO equalisation is employed. To support these conditions, effective multiple access techniques are required, which can use the available bandwidth efficiently to render high data transmission capacity and throughput [33]. Moreover, modern networks are now transforming into IoT networks which are essentially different types of devices connected over the internet, wirelessly. Typically, network parameters are controlled automatically through medium access control (MAC) protocols. Medium access control means the control and management of network resources such as [34]:
Bandwidth.

1. Power
2. Shared devices
3. Data etc.

The single input single output systems capacity can be defined by [35]:

$$\boldsymbol{C = Blog_2(1 + \frac{S}{N})} \qquad \textbf{(12)}$$

Here,

C is channel capacity

B is bandwidth

S is signal power

N is noise power

The challenge arrives in increasing the channel capacity because:

1) B is generally limited
2) S can’t be increased beyond a limit due to SAR value restrictions or battery life

3) N can't be pre-determined.

Hence the MIMO systems are to be resorted to whose capacity is given by [36]:

$$\boldsymbol{C = kBlpg_2(1 + \frac{h_{ij}^2 S}{N})} \qquad \textbf{(13)}$$

Here,

C is channel capacity

B is bandwidth

S is signal power

N is noise power

k is a constants

h is the channel matrix

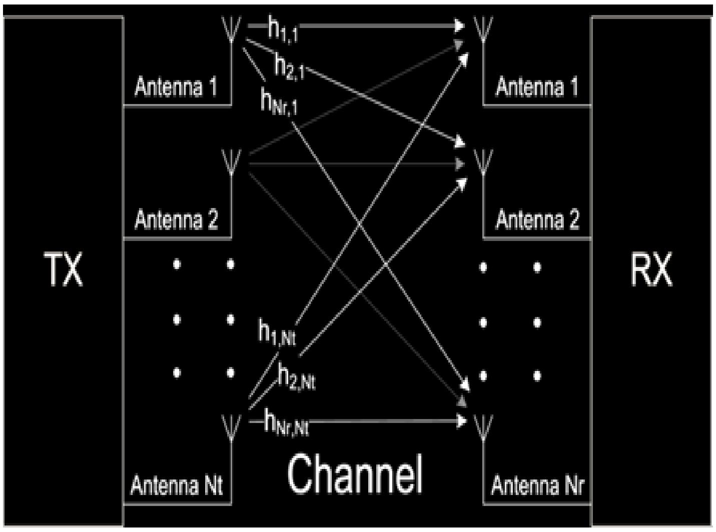

Fig.7 The MIMO System

The channel impulse response (IR) of a wireless channel can be modelled as a sum of impulse responses given by [37]:

$$\boldsymbol{himp(t) = \sum_{i=1}^{k} \delta_i(t)} \qquad \textbf{(14)}$$

Here,

$himp(t)$ denotes Channel IR(time variant).

$\delta$ denotes impulse function.

The frequency translation of channel IR into the f domain is given by:

$$\boldsymbol{H(f) = \int_{-\infty}^{\infty} himp(t) e^{-j\omega t}\, dt} \qquad \textbf{(15)}$$

Here,

$H(f)$ denotes the frequency response of the channel.

The space time block coding (STBC) algorithm is employed to implement MMO. The STBC based approach is one of the most effective techniques to employ MIMO encoding for practical wireless channels. STBC is a specific form of spatial coding that employs multiple transmit antennas to encode data in a manner that improves error performance without requiring additional bandwidth. STBC operates by encoding the data symbols across multiple antennas and time slots in a structured manner, creating a code matrix that optimizes the use of spatial and temporal resources. The fundamental idea is to introduce redundancy and diversity in the transmitted signals, so that even if one or more signal paths experience deep fades, the receiver can still recover the original data from the unaffected paths. It is a technique in which we re-arrange the data in the form of a matrix with [38]:

the number of columns = the number of transmitters and,

The number of rows = the number of time slots needed to transmit the entire bit stream i.e.

C=i, where C = no. of columns and I is number of Transmitters

R=t, where R= no. of rows and t is number of time slots

This step is often referred to as MIMO encoding. MIMO allows for more parallel paths for data transfer thereby increasing the spectral efficiency significantly which can lead to increased throughput and sum secrecy rate.

## 4. Experimental Results

The system has been simulated on MATLAB for $10^6$ bits. The libraries used in work are:

Wireless Networks Toolbox

MIMO Toolbox

Deep Learning Toolbox

Communications Toolbox

The results are presented subsequently.

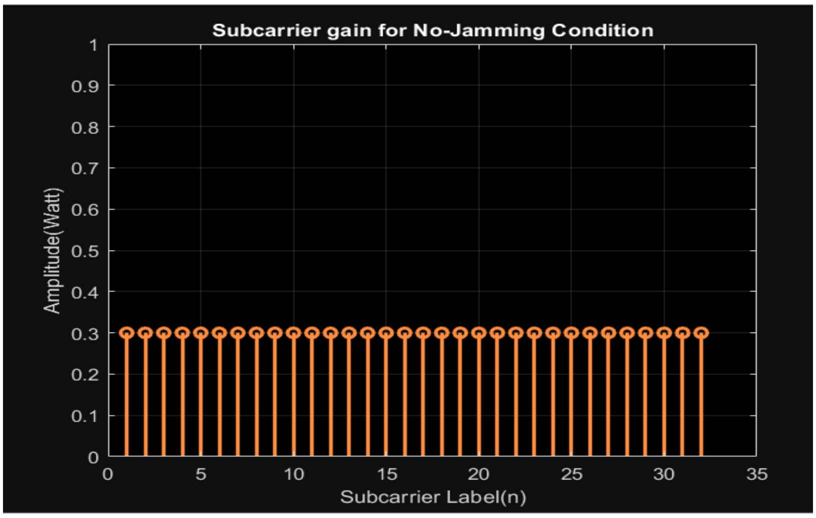

Fig.8 Sub carrier gain (no jamming condition)

Figure 8 depicts the sub-carrier gain for the no jamming condition. It can be observed that the sub-carrier gain remains almost constant for the no jamming condition (ideal case). Thus the energy sensing pattern would yield a constant curve for the sensed channel energy.

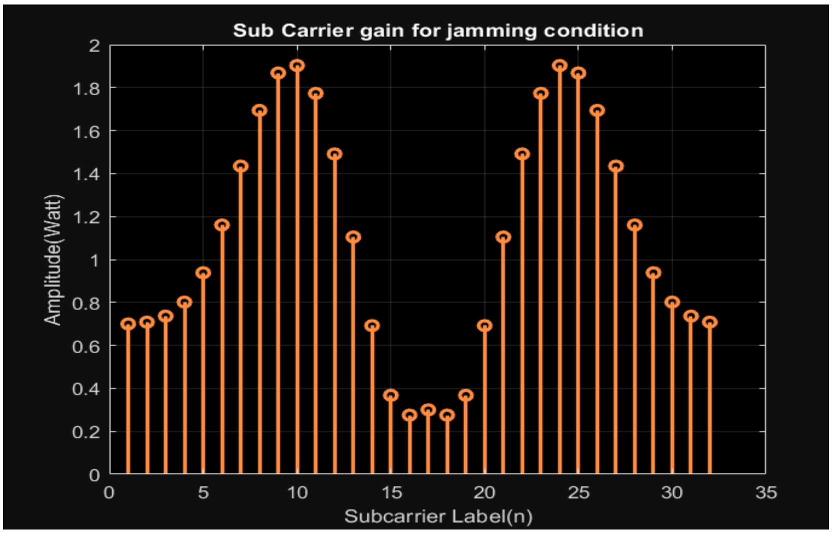

Fig.9. Sub carrier gain under jamming conditions.

The subcarrier gain can be seen to vary based on the jamming condition. The jamming condition can be categorized in four cases:

1) No jamming (with subcarrier energy at receiving end equal or less than transmitted magnitude)

2) Low jamming (with the subcarrier energy less than 1.5 times of transmitted magnitude)

3) Moderate jamming (with the carrier energy between 1.5 to 2 times of transmitted magnitude).

4) High Jamming (with the subcarrier energy more than 2 times of transmitted magnitude).

The effect of the jamming can be seen on the scatter plot as well as the error rate of the system. The bit error rate or the packet error rate of the system is evaluated in this case to evaluate the performance of the system. A clear correlation among the scatter plot and the error rate can be observed.

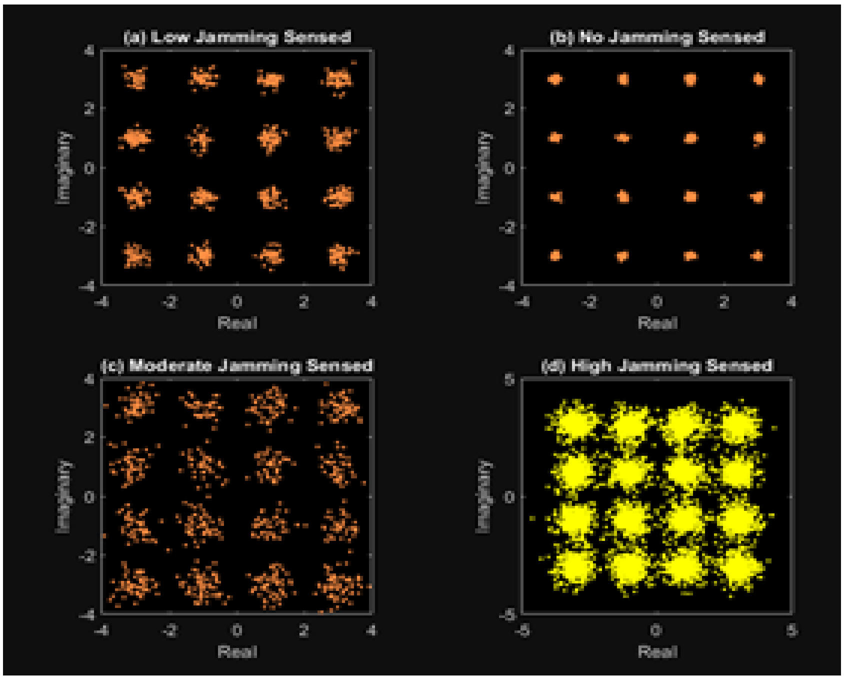

Fig.10. Sub carrier gain under jamming conditions.

The scatter under the different conditions can be observed in figure 10. It can be seen that as the jamming impact increases, the scatter in the data packets increases thereby complying with the theoretical observations. As the Scatter is one of the parameters to evaluate the quality of service (QoS), another extremely important metric happens to be the bit error rate (BER) of the system. The BER of the proposed system under different channel scatter and jamming conditions is depicted subsequently.

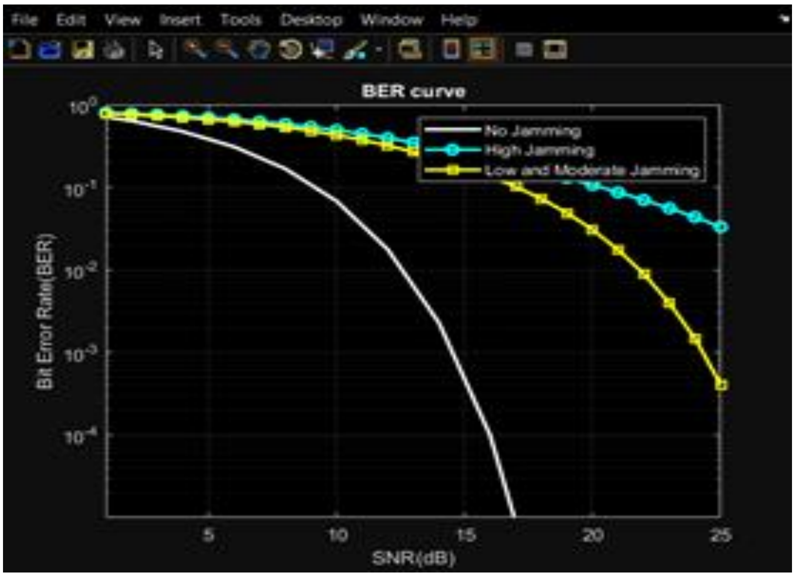

Fig.12. Comparative BER analysis under varying jamming conditions.

Figure 12 depicts the comparative BER analysis for the different cases. The comparative BER analysis of the system under different conditions has been evaluated and plotted against each other for the ease of analysis.

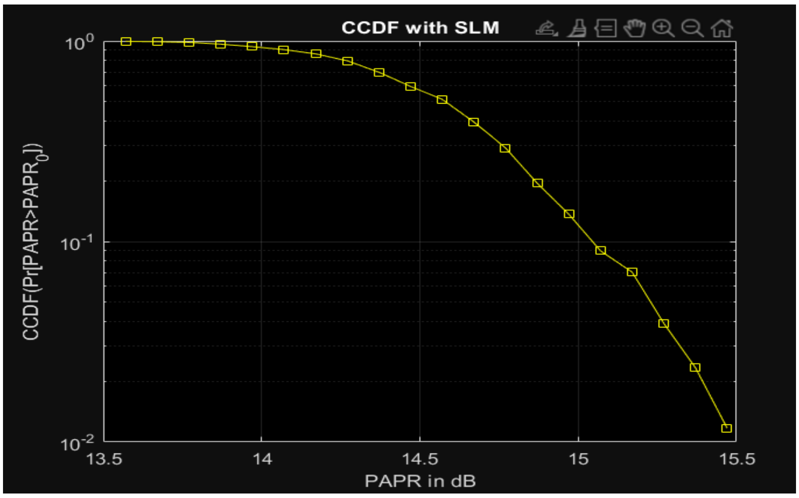

Fig.13. CCDF of PAPR for conventional SLM

Figure 13 depicts PAPR value for conventional SLM. It can be observed that it reaches 15dB.

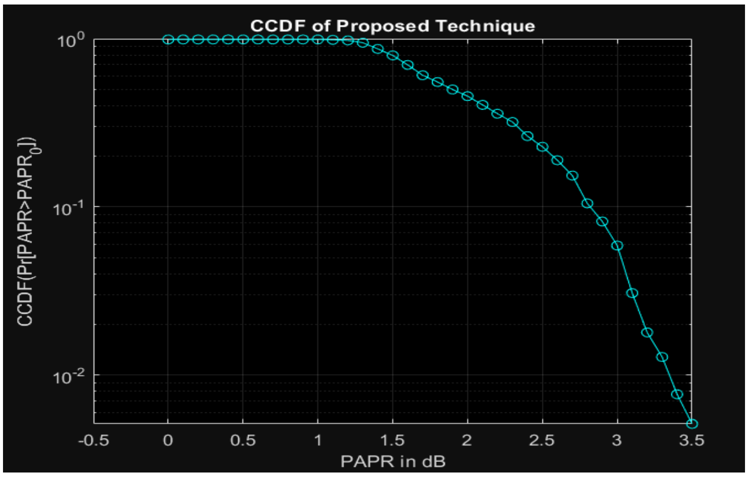

Fig.14. CCDF of PAPR for modified SLM approach.

Figure 14 depicts PAPR value for modified SLM approach. It can be observed that it reaches 3.5dB.

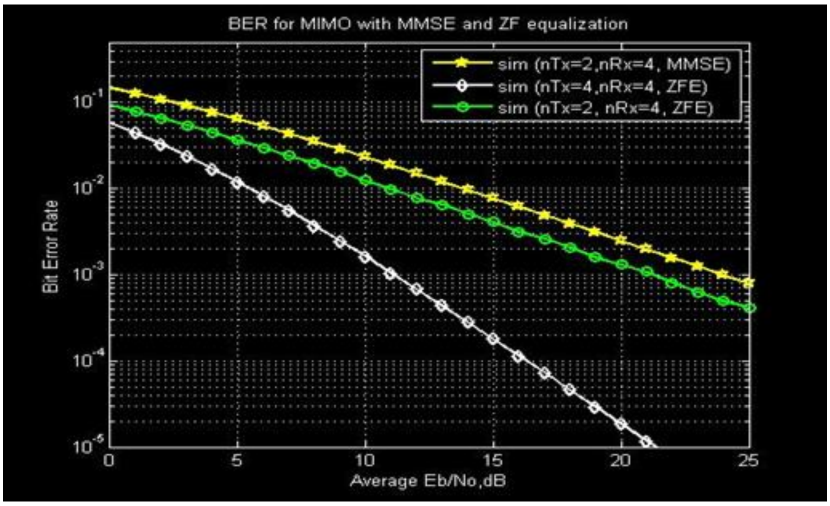

Fig.15 BER for MIMO with MMSE and ZFE Equalization.

Figure 15 depicts a comparative BER analysis for the different MIMO structures and equalization techniques. It can be clearly observed from the above graphs that ZFE performs better compared to MMSE in terms of equalization and the BER falls earlier for ZFE. Moreover, as the number of transmitters increases, the BER has an earlier fall indicating the enhanced channel capacity of the system.

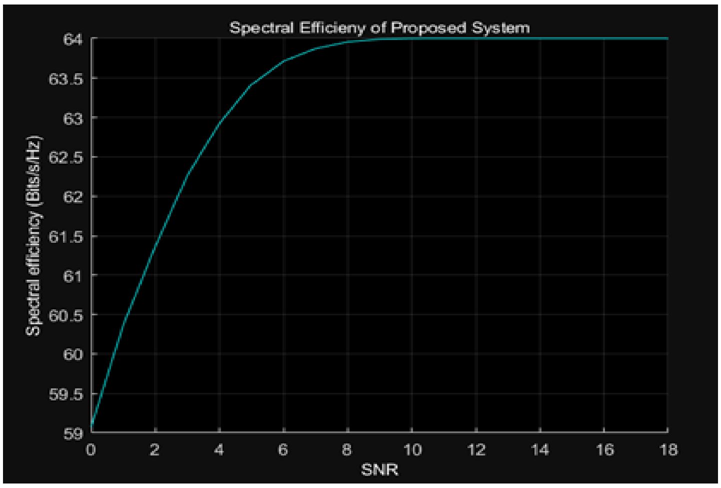

Fig.16 Obtained Spectral Efficiency

Figure 15 depicts a obtained spectral efficiency for the system. It can be observed that the spectral efficiency saturates after a certain point of increasing the SNR indicating the fact that the IoT channel saturates in data transfer capability.

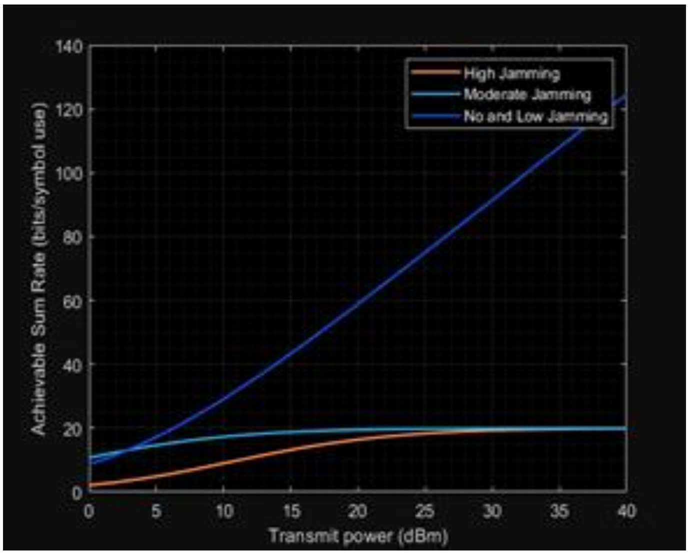

Fig.17 Spectral Efficiency

Figure 17 depicts the obtained sum secrecy rate for CSI based security aware channel assignment. It can be observed that low and no jamming bandwidth sections render maximum sum secrecy.

Table 1.

Comparison with Existing Frameworks

| S.No. | Reference | Parameter | Value |
|---|---|---|---|
| 1. | Huang et al. [39] | Sum Secrecy Rate | 70bits/s/Hz |
| **2.** | **(Proposed Work)** | **Sum Secrecy Rate** | **122bits/s/Hz** |
| 3. | Zahra et al. [40] | Max. Throughput | 5000bytes/s |
| **4.** | **(Proposed Work)** | **Max. Throughput** | **12000bytes/s** |
| 5. | Miranda et al. [41] | Attack Detection Error % | 14.36% |
| **6.** | **Proposed Work** | **Attack Detection Error %** | **1.1%** |
| 7. | Padave et al. [42] | PAPR | 10dB. |
| **8.** | **Proposed Work** | **PAPR** | **3.5dB.** |
| 9. | Lee et al. [43] | MIMO Bit Error Rate | $10^{-2}$ at SNR of 20dB |
| **10.** | **Proposed Work** | **MIMO Bit Error Rate** | **$10^{-3}$ at SNR of 20dB and $10^{-4}$ at SNR of 23dB** |

Table 1 presents a comparative analysis of the obtained results stacked up against existing approaches in the domain. It can be observed that the proposed work outperform existing approaches in terms of sum secrecy, throughput, PAPR as well as MIMO BER values. Thus the proposed approach not only ensures proactive security for IoT and pervasive wireless networks but also support satisfactory QoS metrics such as throughput and spectral efficiency.

## 5. Conclusion

It can be concluded that modern pervasive networks such as the IoT are replacing conventional networks. While rule based IDS and NIDS have been used conventionally, with more sophisticated attack, proactive mechanisms for securing networks is needed. While IDS/NIDS plays a crucial role in securing IoT networks, its effectiveness is hindered by resource constraints, high data volumes, lack of standardization, scalability challenges, evasion techniques, and privacy concerns. Addressing these challenges requires a combination of innovative security solutions, adaptive proactive mechanisms, and collaborative efforts between industry and regulatory bodies. Only through continuous advancements in security frameworks can IoT networks be effectively protected against evolving cyber threats.

This paper combines the idea of leveraging the CSI for security aware channel assignment of the available bandwidth along with PAPR reduction for increased imperceptibility of data transfer. MIMO-Equalization is also employed to enhance the spectral efficiency and sum secrecy rate of the system. It has been shown that the proposed system outperforms exiting approaches in terms of the evaluation metrics such as BER, PAPR, spectral efficiency and sum secrecy rate.

### Conflict of Interest

The authors declare no potential conflict of interest.

## References

[1] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi and M. Qiu, "Adversarial Attacks Against Network Intrusion Detection in IoT Systems," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10327-10335, 1 July1, 2021.

[2] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021.

[3] S. Singh, A. S. M. S. Hosen and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," in IEEE Access, vol. 9, pp. 13938-13959, 2021.

[4] SM Tahsien, H Karimipour, P Spachos, “Machine learning based solutions for security of Internet of Things (IoT): A survey”, Journal of Network and Computer Applications Elsevier 2020, vol.161, 102630.

[5] A. Ferdowsi and W. Saad, "Deep Learning-Based Dynamic Watermarking for Secure Signal Authentication in the Internet of Things," 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-6

[6] J. H. Anajemba, T. Yue, C. Iwendi, P. Chatterjee, D. Ngabo and W. S. Alnumay, "A Secure Multiuser Privacy Technique for Wireless IoT Networks Using Stochastic Privacy Optimization," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2566-2577, 15 Feb.15, 2022

[7] M. Mahmoud, M. Kasem, A. Abdallah and H. S. Kang, "AE-LSTM: Autoencoder with LSTM-Based Intrusion Detection in IoT," 2022 International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 2022, pp. 1-6.

[8] K. Kalkan and S. Zeadally, "Securing Internet of Things with Software Defined Networking," in IEEE Communications Magazine, vol. 56, no. 9, pp. 186-192, Sept. 2018.

[9] M. Sarrab and S. M. Alnaeli, "Critical Aspects Pertaining Security of IoT Application Level Software Systems," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 960-964.

[10] 15. B. Bordel, R. Alcarria, T. Robles and M. S. Iglesias, "Data Authentication and Anonymization in IoT Scenarios and Future 5G Networks Using Chaotic Digital Watermarking," in IEEE Access, vol. 9, pp. 22378-22398, 2021.

[11] M. El-hajj, M. Chamoun, A. Fadlallah and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)," 2017 1st Cyber Security in Networking Conference (CSNet), 2017, pp. 1-3.

[12] K. S. Germain and F. Kragh, "Mobile Physical-Layer Authentication Using Channel State Information and Conditional Recurrent Neural Networks," 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), 2021, pp. 1-6.

[13] Y. Chen, T. Zhang, Y. Liu and X. Qiao, "Physical Layer Security in NOMA-Enabled Cognitive Radio Networks With Outdated Channel State Information," in IEEE Access, vol. 8, pp. 159480-159492, 2020.

[14] A. Ferdowsi and W. Saad, "Deep Learning for Signal Authentication and Security in Massive Internet-of-

Things Systems," in IEEE Transactions on Communications, vol. 67, no. 2, pp. 1371-1387, Feb. 2019.

[15] T Burton, K Rasmussen, “Private Data Exfiltration from Cyber-Physical Systems Using Channel State Information”, in Proceedings of Private Data Exfiltration from Cyber- Physical Systems Using Channel State Information, ACM 2021, pp.223-235.

[16] D Li, L Deng, M Lee, H Wang, “IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning”, International Journal of Information Management, Elsevier 2019, vol.49, pp. 533-545.

[17] T Pecorella, L Brilli, L Mucchi, “The role of physical layer security in IoT: A novel perspective”, Journal of Inforamtion, MDPI 2016, vol. 7, no. 3, pp.1-17

[18] SR Moosavi, TN Gia, AM Rahmani, E Nigussie, “SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways”, Procedia Computer Science, Elsevier 2015, vol. 52, pp. 452-459.

[19] S. Sathyadevan, Vejesh V, R. Doss and L. Pan, "Portguard - an authentication tool for securing ports in an IoT gateway," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 624- 629.

[20] A. Olutayo, J. Cheng and J. F. Holzman, "A New Statistical Channel Model for Emerging Wireless Communication Systems," in IEEE Open Journal of the Communications Society, vol. 1, pp. 916-926, 2020.

[21] A. Albaseer, B. S. Ciftler and M. M. Abdallah, "Performance Evaluation of Physical Attacks against E2E Autoencoder over Rayleigh Fading Channel," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 177-182

[22] E. Björnson and L. Sanguinetti, "Rayleigh Fading Modeling and Channel Hardening for Reconfigurable Intelligent Surfaces," in IEEE Wireless Communications Letters, vol. 10, no. 4, pp. 830-834, April 2021.

[23] S. Yousefi, H. Narui, S. Dayal, S. Ermon and S. Valaee, "A Survey on Behavior Recognition Using WiFi Channel State Information," in IEEE Communications Magazine, vol. 55, no. 10, pp. 98-104, Oct. 2017.

[24] C. Studer, S. Medjkouh, E. Gonultaş, T. Goldstein and O. Tirkkonen, "Channel Charting: Locating Users Within the Radio Environment Using Channel State Information," in IEEE Access, vol. 6, pp. 47682-47698, 2018.

[25] A. Saci, A. Al-Dweik, A. Shami and Y. Iraqi, "One-Shot Blind Channel Estimation for OFDM Systems Over Frequency-Selective Fading Channels," in IEEE Transactions on Communications, vol. 65, no. 12, pp. 5445-5458, Dec. 2017.

[26] W. Ma, C. Qi and G. Y. Li, "High-Resolution Channel Estimation for Frequency-Selective mmWave Massive MIMO Systems," in IEEE Transactions on Wireless Communications, vol. 19, no. 5, pp. 3517-3529, May 2020

[27] P. Singh, E. Sharma, K. Vasudevan and R. Budhiraja, "CFO and Channel Estimation for Frequency Selective MIMO-FBMC/OQAM Systems," in IEEE Wireless Communications Letters, vol. 7, no. 5, pp. 844-847, Oct. 2018.

[28] K. Venugopal, N. González-Prelcic and R. W. Heath, "Optimality of Frequency Flat Precoding in Frequency Selective Millimeter Wave Channels," in IEEE Wireless Communications Letters, vol. 6, no. 3, pp. 330-333, June 2017.

[29] A. Kumar, N. Gaur and A. Nanthaamornphong, "Optimizing PAPR, BER, and PSD Efficiency: Using Phase Factors Generated by Bacteria Foraging Algorithm for PTS and SLM Methods," in IEEE Access, 2024, vol. 12, pp. 54964-54977

[30] P. Singh, E. Sharma, K. Vasudevan and R. Budhiraja, "CFO and Channel Estimation for Frequency Selective MIMO-FBMC/OQAM Systems," in IEEE Wireless Communications Letters, vol. 7, no. 5, pp. 844-847, Oct. 2018.

[31] R. Zayani, J. -B. Doré, B. Miscopein and D. Demmer, "Local PAPR-Aware Precoding for Energy-Efficient Cell-Free Massive MIMO-OFDM Systems," in IEEE Transactions on Green Communications and Networking, 2023, vol. 7, no. 3, pp. 1267-1284.

[32] M Bharti, “Analysis of PAPR suppression scheme for next generation wireless system”, International Journal of System Assurance Engineering and Management, Springer 2023, vol.14, pp. 818–826.

[33] J. -M. Kang, "MIMO-LoRa for High-Data-Rate IoT: Concept and Precoding Design," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 10368-10369, 15 June15, 2022.

[34] Y. Yuan et al., "NOMA for Next-Generation Massive IoT: Performance Potential and Technology Directions," in IEEE Communications Magazine, vol. 59, no. 7, pp. 115-121, July 2021

[35] N. T. Nguyen, K. Lee and H. DaiIEEE, "Application of Deep Learning to Sphere Decoding for Large MIMO Systems," in IEEE Transactions on Wireless Communications, vol. 20, no. 10, pp. 6787-6803, Oct. 2021.

[36] M. B. Mashhadi and D. Gündüz, "Pruning the Pilots: Deep Learning-Based Pilot Design and Channel Estimation for MIMO-OFDM Systems," in IEEE Transactions on Wireless Communications, vol. 20, no. 10, pp. 6315-6328, Oct. 202.

[37] H. He, C. Wen, S. Jin and G. Y. Li, "Model-Driven Deep Learning for MIMO Detection," in IEEE Transactions on Signal Processing, vol. 68, pp. 1702-1715, 2020.

[38] Y. Wang, J. Wang, W. Zhang, J. Yang and G. Gui, "Deep Learning-Based Cooperative Automatic Modulation Classification Method for MIMO Systems," in IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4575-4579, April 2020.

[39] 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.

[40] 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.

[41] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg and K. Kaur, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, IEE 2022, vol. 15, pp. 2602-2615.

[42] S. Padave, N. A. Natraj and G. G. Hallur, "Qualitative Analysis on Implementation of Security Aspects for Web 3.0," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 1352-1356.

[43] S. Lee and D. Sim, "Deep Learning-Based Channel Estimation Method for MIMO Systems in Spatially Correlated Channels," in IEEE Access, 2024, vol. 12, pp. 79082-79090.