ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

Leveraging CSI and Recursive Decoding to Enhance QoS of IoT Networks

Vaidehi Bakshi*
Department of Computer Science and Engineering, Rabindranath Tagore University, Raisen, India
**Corresponding Author: Vaidehi Bakshi*
Email of corresponding Author: vaidehibakshi35@gmail.com

***Abstract*— Internet of Things (IoT) is finding its applications in several domains such as large scale automation, precision agriculture, smart healthcare, intelligent traffic systems etc. IoT networks are replacing conventional networks by connecting different types of devices in the wireless medium. However, due to the wireless nature of the medium, IoT networks often face the challenge of degrading Quality of Service (QoS). The resulting consequence happens to be increased error rates and degraded sum secrecy rates for the network. As IoT networks utilize the ISM band for data transmission, hence the limitation of bandwidth becomes a serious constraint in achieving high data rates while keeping the Bit Error Rate (BER) low. To address the aforesaid challenges, this paper presents a combination of channel sensing and recursive error detection to alleviate the problem of data reliability and securing the data transmission against adversarial attacks. The channel sensing information is leveraged to utilize the section of the bandwidth suitable for transmission while the recursive error detection algorithm further damps bit errors at the receiving end. The evaluation metrics computed are the error rate, secrecy rate and throughput of the network, which can be seen to outperform existing benchmark approaches in the domain.**

***Index Terms*—Internet of Things (IoT), Channel Sensing, Recursive Decoding, Quality of Service (QoS), Error Rate.**

I. Introduction

Web 3.0 has become synonymous with connected devises and pervasive networks. It can be viewed as an interconnected system of smart devices connected over the internet.

The data transmission being wireless in IoT networks has some substantial advantages which are:

- Ease of mobility.
- No cabling cost.
- Ease in up-scaling or down-scaling the network.

However, there are associated challenges pertaining the security of the network as the data travels in free space without any guided media [2]. This makes the data easier to access to possible adversaries. Adversaries or potential attackers often try to attack the data, implementing different security attacks [3]. There are various types of attacks which IoT networks encounter such as man in the middle attack, impersonation attacks, denial of service attacks, jamming attacks etc. One of the fundamental and inherent constraints of IoT networks is the limited memory and processing power corresponding to the wide diversity among IoT devices (IoTDs) [4]. This often makes the implementation of complex encryption algorithms infeasible on all IoTDs due to the constraints of memory and processing power. Moreover, due to the emergence of machine learning and quantum computing applications, "save now and decrypt later" approaches can open up a completely new area of security threats [4]. Hence, rather than completely relying on encryption algorithms alone, it is logical to migrate towards a proactive approach wherein the data transmission in IoT networks can be done in such a manner that it would sense the channel for potential attacks and avoid spectral bands which are most prone to attacks. This would serve as an attack avoidance mechanism rather than just an attack detection or encoded version of the data trying to thwart security attacks

The paper is divided in to the following sections: Section I presents the need for proactive network security measures as against conventional reactive intrusion detection systems (IDS). Section II presents the important recent contributions in literature review. Section III discusses the research framework for the paper. Section IV discusses in detail the obtained experimental results and it implications. Section V concludes the significance and findings of the paper and potential directions of future enhancement.

II. Related Work

This section presents the salient feature of contemporary research work carried out in the domain of research.

Germain et al. [5] proposed an approach leveraging the channel state information (CSI) and recurrent neural networks to implement physical layer authentication. In this approach, the channel state information (CSI) and the stochastic parameters of the CSI are used to train a recurrent neural network (RNN) for data authentication in the network. Chen et al. [6] proposed implementing physical layer security employing outdate channel state information (CSI) for cognitive networks using non-orthogonal multiple access (NOMA) as the multiplexing technique. This approach doesn't sense the channel iteratively to obtain repeated values of the CSI. While this approach may lead to lesser computational complexity, but would be less impactful in case the CSI doesn't exhibit rapid stochastic changes. Ferdowsi et al. [7] proposed the use of deep learning for signal authentication in IoT networks. The long short term memory (LSTM) framework has been proposed in this approach which is trained using the stochastic parameters of the data to be transmitted. The stochastic parameters are used as a watermark

ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

on the signal to be transmitted and are analysed by the LSTM at the IoT gateway. Burton et al. [8] proposed a data exfiltration method for IoT networks along with possible methods to avoid such attacks using the channel state information (CSI). Data exfiltration is a technique to extract data from a network without authorization as well as cognizance of the network or device(s) in the network. It is shown in the paper that if the channel is sensed for a long enough time, then the stochastic parameters can be extracted. It is also proposed that such attacks can be avoided by continuously changing the transmission bandwidth of the system which shown pseudo random patterns. Li et al. [9] proposed deep learning for feature extraction and subsequent intrusion detection in large scale IoT networks typically deployed in smart city projects for large scale automation. In this approach the stochastic features are computed the deep neural network and subsequently matched with features of the data stream without attacks to sense the possibility of attacks. Pecorella et al. [10] discussed the importance of physical layer security in IoT networks. The paper shows that while security patches can be incorporated at network layer and application layer too, they can be bypassed with lesser difficulty as compared to physical layer security where bit level security ensures the highest security typically for memory and processing power constrained IoT networks. Typical mechanisms can be frequency hopping and code division multiple access [11].

An analysis of the recent literature in the domain indicates that obtaining the dynamic CSI is critically important to leverage contextual information pertaining to potential attacks and can serve as a tool to attack avoidance, as opposed to simply identifying intrusions or designing authentication mechanisms [12]. This paves the path for the research framework in the paper.

III. Research Framework

In this paper, two major challenges are addressed:

Mitigating potential attacks under variable channel conditions [13]-[14]:

Enhancing reliability and QoS of the system even under noisy and random channel conditions.

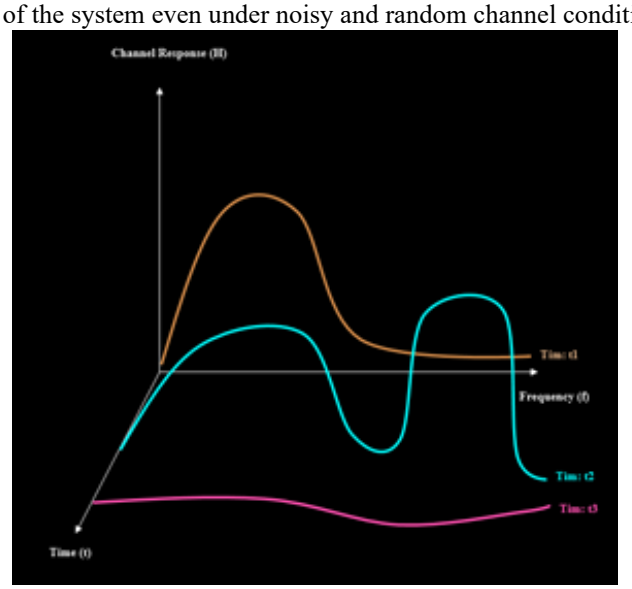

Fig.1. Depiction of Typical CSI

Figure 1 depicts a typical CSI for a random and noisy channel which is challenging to estimate due to the random temporal attributes of the channel [15]. Effective channel sensing is necessary in this case to estimate the behavior of the channel even under random noisy nature [16]. To estimate potential jamming attacks on IoT networks, the concept of cognitive networks is proposed to be leveraged [17]. Cognitive networks are a sub-class of wireless networks where the cognizance (awareness or information) regarding the network is extracted through a channel sensing mechanism [18]. The cognitive cycle typically has the following steps [19]-[20]:

1) Sense channel.
2) Obtain channel state information.
3) Manage spectrum.
4) Repeat steps 1-3.

It is necessary to sense the channel conditions continuously or recursively as the channel's response and hence the channel state information (CSI) keeps changing [21]. The channel response is often evaluated based on the sensed energy for each frequency. For instance, the channel response of any frequency f is computed as [22]:

$$H(f) = O(f) / I(f) \quad (1)$$

Here,

H(f) is the channel response for frequency f.

ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

O(f) & I(f) represent the channel output and input respectively measure w.r.t. the frequency metric.

To estimate the complete channel response (CSI) or H(f,t), the channel is to be sensed periodically, every Ts seconds for all the frequencies in the bandwidth under interest. For instance, the channel sensing iterated over every Ts seconds to updated the CSI [23].

$$CSI(t) = \Sigma_{(i=1 \text{ to } n)} H(f, t - Ts \cdot i),\ i \in \{1, 2, \ldots.\} \quad (2)$$

Here,

Ts represents the sampling time to sense the channel to be sensed.

Based on the sensed response, the equalization mechanism can be designed. The equalization has to be performed every Ts seconds as the channel sensing has to be repeated periodically to estimate the updated channel response. The advantage of such an approach would be an updated version of the CSI but having a major constraint of enhanced complexity of the system [24]-[25].

Thus, the proposed algorithm aims at continuously estimating the channel state response to evaluate the jamming activity and avoiding the bandwidth section which is prone to moderate and high jamming activity. The algorithm for estimating the CSI to proactively evade attacks is presented next:

Algorithm 1:

Start:

{

Step.1: Generate binary dummy packets for channel sensing as:

$$XD = randn(N, SP) \quad (3)$$

Step.2 Generate random frequency response of channel as:

$$HChan(f, t) = FFT(rand(H)) \quad (4)$$

Step.3: Ping channel using XD every Ts to estimate channel response as:

for (t = TS to nTS)

Compute:

$$\Sigma_{(t=TS \text{ to } nTS)} [FFT(XD) \cdot FFT(rand(H))]t \quad (5)$$

Step.4: Estimate CSI as:

$$CSI(t) = \Sigma_{(i=1 \text{ to } n)} H(f, t - Ts \cdot i),\ i \in \{1, 2, \ldots.\} \quad (6)$$

Step.5: Apply Equalization as:

$$K(H(f,t)) = \text{argmin } (1/n) \Sigma\, e(f,t)^2,\ \forall\ t \in [TS, nTS] \quad (7)$$

Step.6: Implement proactive network security as:

for (Bi = B1….Bn)

if (y(f,t) ≫ mean(Σ (t=TS to nTS) [FFT(XD).FFT(rand(H))]t * K(H(f,t))))

{

Discard Bi

}

else

{

Utilize Bi : i ∈ [1,n] for data transmission.

}

}

Stop.

Here,

XD are the dummy packets.

N denotes number of packets.

SP denotes bits per packet.

HChan(f,t) denotes temporal frequency dependent channel.

FFT denotes the Fast Fourier Transform for time to frequency translation.

K denotes the equalization constant

$e(f,t)^2$ denotes error in channel estimation over the period t.

Bi : i ∈ [1,n] denote spectral bands available for data transmission over the IoT network.

The main idea in this case is to proactively sense the CSI using the sensing mechanism and estimate the product $\Sigma_{(t=TS \text{ to } nTS)} [FFT(XD).FFT(rand(H))]t * K(H(f,t))$ which is nothing but the channel response to the input XD in frequency domain.

The same analysis could have been done in time domain as well rending the same result. In case the above result exceeds the mean value of TS, it would be treated as spurious activity potentially by adversaries [27]. In such as case the part of Bi needs to be discarded to ensure system security. The next step is developing a recursive decoding mechanism for error detection and correction. In this case, the transmitter is used to generate two parity streams P1 and P2 along with the data stream I. The

ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

party stream P2 happens to be the interleaved version of P1.

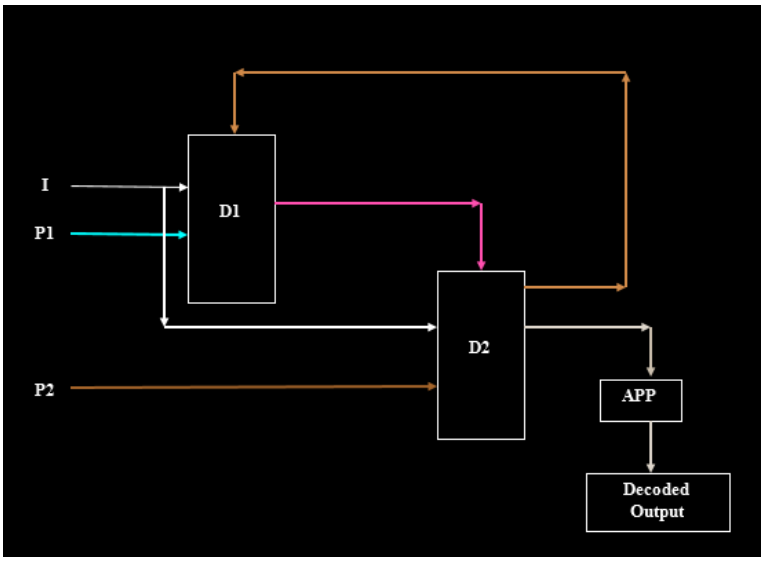

Fig.2. Architecture for Recursive Error Detection and Correction

Figure 2 depicts the recursive error detection and correction mechanism which works very effectively in the BER-Waterfall region.

The recursive decoding algorithm employed in this approach is presented next:

Algorithm 2:

Start:

{

Step.1: Apply P1 and I to the first decoder of the model D1 while applying P2 and I to the second decoder D2.

Step.2: Apply YD2 as XD1 and vice versa.

Step.3: Define maximum iterations, Imax

Step.4: Apply recursive decoding as:

(for i=1:Imax)

{

Estimate YD1 and YD2

}

Step.5: Based on the aposteriori probability,

Estimate final output as:

Maximize (Prob(Y, YD1, YD2) ∈ [0,1]) (8)

Step.6: Computer BER of the system based on:

BER = (1/N) Σ (i=1 to N) [Yi ≠ Xi] (9)

Here,

YD2 denotes output of D2

XD1 denotes input of D1

Yi & Xi denote the actual transmitted and received bits.

}

Stop.

The simulation results are presented next:

IV. Experimental Results

The experimental parameters in the proposed study are presented in table I. The network data simulation has been performed on a PC with 11th Generation Intel i7 Processor with 16GB DDR4 RAM and 2TB SSD.

Table. I. Simulation Parameters

S.No.	Parameter	Value
1.	No. of bits in simulation	10^8
2.	Packet Size	1600 bytes
3.	Pilot Bits	16
4.	Sub-carriers	32

ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

5.	Channel	Gaussian
6.	SNR Range	0-30 dB
7.	Ideal Sub-Carrier Gain	0.3

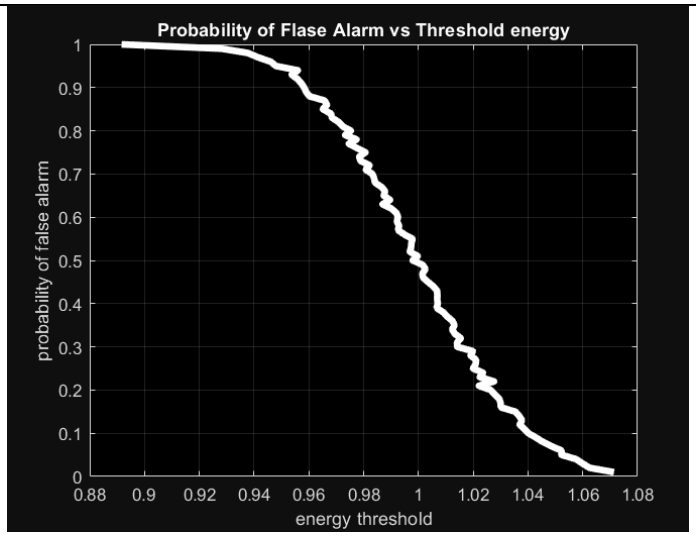

Fig.3. Probability of false alarm

Figure 3 depicts the probability of false alarm with respect to the variations in the energy threshold. It can be clearly observed that as the energy threshold increases, the probability of false alarm keeps plummeting. This supports the theoretical standpoint as noise is typically weak in nature compared to the signal strength. Thus, noise, deceiving the receiver completely would be extremely uncommon with the increase in the energy threshold for the detection of signals.

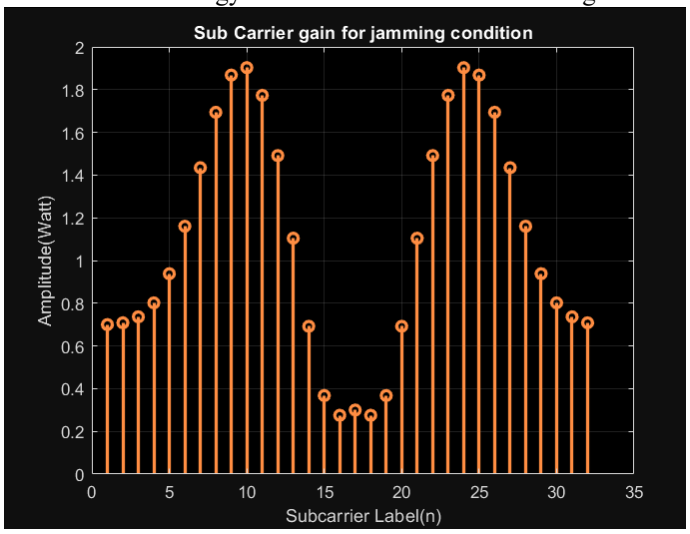

Fig.4. IoT channel under adversarial attacks

Figure 4 is depicts the adversarial attack on the IoT channel. The magnitude response can be used to estimate the term Σ (t=TS to nTS) [FFT(XD).FFT(rand(H))]t * K(H(f,t)) as defined earlier.

ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

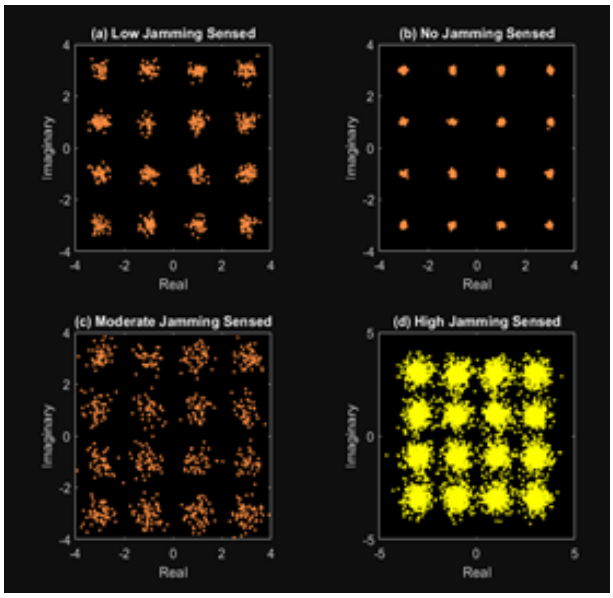

Fig.5. IoT Channel Scatter

Figure 5 depicts IoT channel scatter. The scatter here is considered based on the complex valued signaling points of the bit or packet stream given by:

$$Xb = Re(X) + j \cdot Img(y) \quad (10)$$

Here,

Xb denotes the binary bit X.

Re{ } denotes the real part.

Img{ } denotes the imaginary part.

j is the imaginary number $\sqrt{-1}$

The scatter varies with the magnitude of adversarial activity. Lower activity results in lesser scatter.

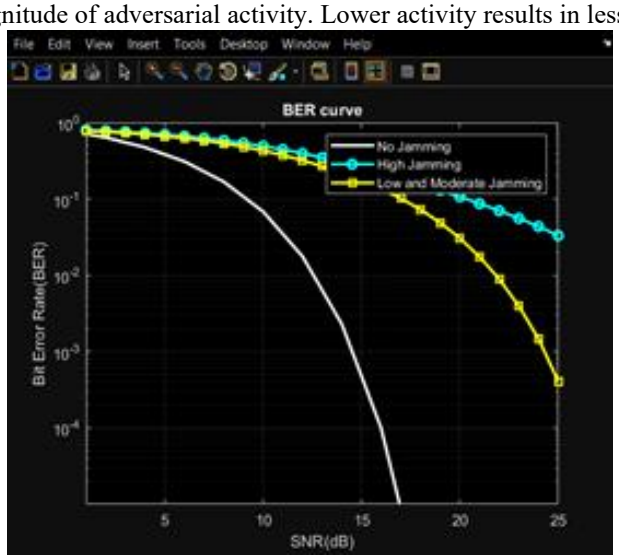

Fig.6. BER under adversarial activity

Figure 6 depicts the BER metric of the system under adversarial conditions. It can be observed that the error rate bears correspondence with the adversarial activity. Higher error rates correspond to higher adversarial activity. However, in the absence of channel sensing based IoT bandwidth allocation Bi = B1….Bn, higher error rates are observed as opposed to CSI leveraged bandwidth allocation. Another evaluation metric for the analysis of the system happens to be throughput of the system. In this case, the jamming conditions would affect the throughput of the system. Moreover, the jamming interval (frequency) between jamming activities would also impact the throughput. The throughput as a function of the jamming interval is also depicted subsequently

ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

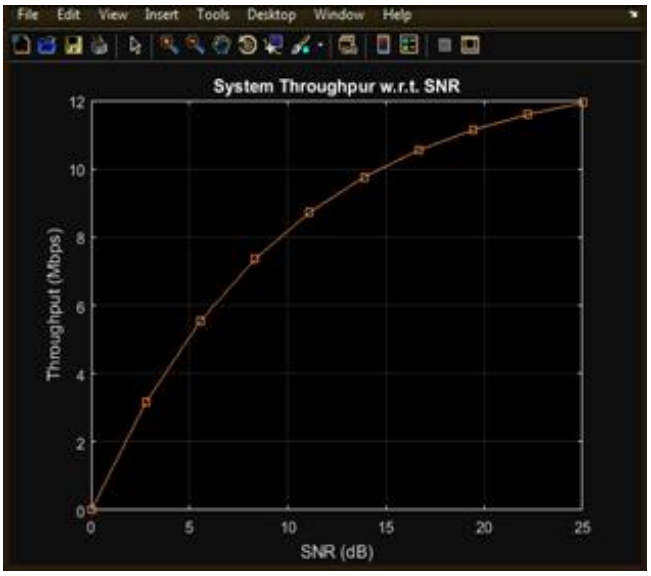

Fig.7 (a). Throughput as a function of SNR and 7 (b) Sum Secrecy Rate under Different Jamming Conditions.

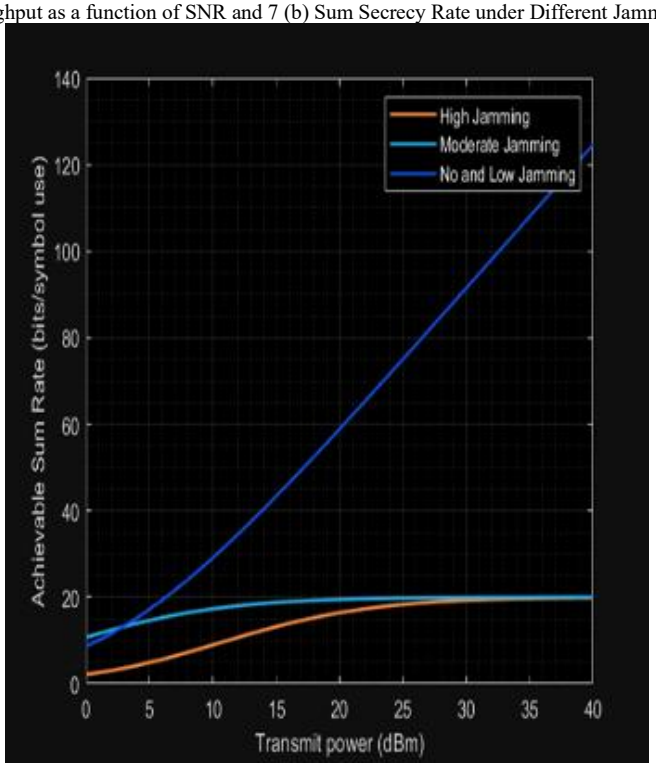

Fig.7 (a). Throughput as a function of SNR and 7 (b) Sum Secrecy Rate under Different Jamming Conditions.

Figure 7 (a) depicts the variation of the throughput with respect to the SNR of the system. It can be observed that as the system SNR increases, the throughput of the system also increases. This is in clear compliance with the system BER as a function of the SNR of the system. Figure 7 (b) presents the sum secrecy rate (typically measured in bits/s/Hz) for the proposed system. It can be clearly observed that the sum secrecy rate for the proposed system is the highest for the low and no jamming activity. This again is in clear coherence with the scatter and BER plots of the system.

ISSN (ONLINE): 2456-5717
ISSN (PRINT): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 12, Issue 10, October 2026

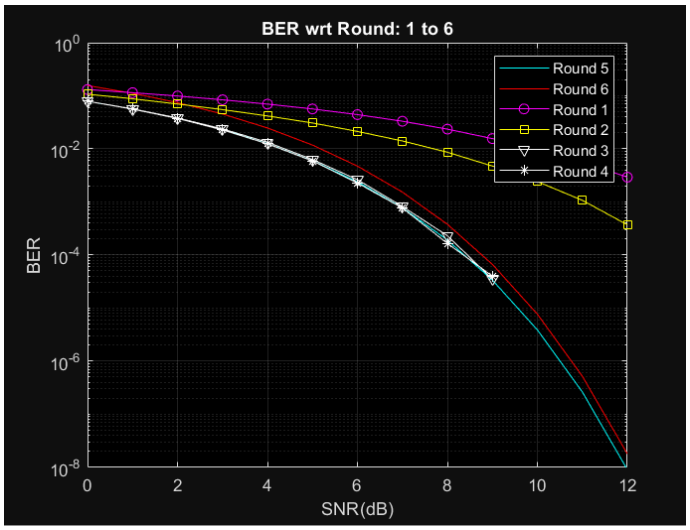

Fig.8 Obtained BER after recursive decoding

Figure 8 depicts the BER after the error detection and correction is carried out after equalization. It can be observed that increase in the decoding iterations reduces the system BER but also increase the computational complexity of the system resulting in latency. Hence, for time critical IoT applications, the maximum iterations must be set meticulously.

The tabulation of experimental parameters is presented next.

TABLE II. THROUGHPUT AND BER ANALYSIS

S.No	SNR	Throughput (MB/s)	BER vs. Iterations
1	5	5.2	10^{-2} at iteration 1
2	10	8.0	10^{-3} at iteration 2
3	15	10.0	10^{-4} at iteration 3
4	20	11.2	10^{-4} at iteration=4
5	25	12.0	10^{-5} at iteration 5 & 6

It can be observed that as the SNR increases, the throughput increases to 12Mbps after which it saturates. The BER continuously keeps dropping in the waterfall region as the iterations increase. The maximum iterations are limited to 6 as soon as the BER reaches the order of 10^{-5}, typically around the Shannon's limit.

TABLE III. BER ANALYSIS UNDER DIFFERENT JAMMING CONDITIONS

SNR (dB)	BER	Condition
5	$>10^{-1}$	No Jamming
10	$<10^{-1}$	No Jamming
15	10^{-3}	No Jamming
20	10^{-4}	No Jamming
25	10^{-5} - 10^{-6}	No Jamming
5	$>10^{-1}$	Low and Moderate Jamming
10	$>10^{-1}$	Low and Moderate Jamming
15	10^{-1}	Low and Moderate Jamming
20	10^{-2}	Low and Moderate Jamming
25	$<10^{-3}$	Low and Moderate Jamming
5	$>10^{-1}$	High Jamming
10	$>10^{-1}$	High Jamming
15	$>10^{-1}$	High Jamming
20	10^{-1}	High Jamming
25	10^{-1} - 10^{-2}	High Jamming

The BER analysis of the proposed system renders the following information:

1) The BER of the high jamming activity is the highest and reduces extremely slowly. This implies that the bandwidth chunk experiencing high jamming activity should be avoided for data transmission, else the reliability of the system in terms of accuracy, error and throughput performance of would be poor. On the contrary, the low jamming activity spectrum can be utilized with caution and iterative channel sensing as the error rate reduces significantly. The moderate jamming condition can

be avoided or in case, the receiver is extremely sensitive can be utilized if the other sections of the bandwidth are occupied. The no jamming condition is an ideal condition which assumes no jamming. It is more of a theoretical yardstick to evaluate the performance of the system under different jamming conditions. A comparative analysis in terms of performance parameters is presented in table IV.

TABLE IV. COMPARATIVE RESULTS

S.No.	Reference	Evaluation Metric	Value
1.	[21]	BER	10^{-4}
2.	[22]	BER	10^{-5}
3.	[23]	BER	10^{-3}
4.	PROPOSED	BER	10^{-6}
5.	[24]	Sum Secrecy	77 bits/s/Hz
6.	PROPOSED	Sum Secrecy	120 bits/s/Hz
7.	[25]	Throughput	5×10^{6} bps
8.	PROPOSED	Throughput	12×10^{6} bps

Table IV presents the comparative analysis of the proposed work with contemporary research in the domain in terms of three fundamental metrics namely sum secrecy rate, throughput and attack detection error%. It can be observed that the proposed work outperforms Huang et al. [22] in terms of sum secrecy rate, Zhara et al. [23] in terms of maximum throughput and Miranda et al. [24] in terms of attack detection error percentage. These parameters present a holistic picture of the efficacy of the system as he sum secrecy rate and attack detection error % indicate the accuracy of the system while the throughput indicates the data transfer efficiency of the system.

V. CONCLUSION

This paper presents a proactive security mechanism for wireless networks based on channel sensing and estimation of CSI. For this purpose, leveraging the Channel State Information (CSI) based approach has been proposed. It is a proactive approach rather than a reactive approach t thwart potential attacks. Channel Equalization is also used to revert the effects of jamming attacks and distortions in the channel. The evaluation metrics for the designed system would be the scatter plot and the bit error rate. It is expected that the error rate would show a much steeper fall employing jamming rejection compared to employing all channels for data transmission. The proposed work tries to design a proactive cognitive approach to evade possible jamming attacks. Equalization is proposed to reduce the error rate of the system. A comparative performance analysis in terms of sum secrecy rate, throughput and attack detection error% clearly indicates superior proactive security for the proposed approach w.r.t. baseline models. Further the recursive decoding algorithm limits the error rates below 10^{-5} in the error-waterfall region enhancing the system QoS.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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
[11] 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.
[12] 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.
[13] 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.

[14] 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
[15] 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.
[16] 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.
[17] 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.
[18] 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.
[19] 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
[20] 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.
[21] 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.
[22] S. Zhao, J. Wen, S. Mumtaz, S. Garg and B. J. Choi, "Spatially Coupled Codes via Partial and Recursive Superposition for Industrial IoT With High Trustworthiness," in IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6143-6153, Sept. 2020.
[23] I. 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
[24] 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.
[25] 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.
[26] 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, IEEE 2022, vol. 15, pp. 2602-2615.
[27] M. M. Ali, S. J. Hashim, M. A. Chaudhary, G. Ferré, F. Z. Rokhani and Z. Ahmad, "A Reviewing Approach to Analyze the Advancements of Error Detection and Correction Codes in Channel Coding With Emphasis on LPWAN and IoT Systems," in IEEE Access, vol. 11, pp. 127077-127097, 2023.