Wireless Personal Communications
https://doi.org/10.1007/s11277-023-10389-1

A Deep Learning and Channel Sounding Based Data Authentication and QoS Enhancement Mechanism for Massive IoT Networks

Rajeev Kumar[1] · Gaurish Joshi[1] · Amit Kumar Singh Chauhan[1] · Arun Kumar Singh[1] · Ashish K. Rao[1]

Accepted: 21 March 2023

Abstract
The Internet of things has emerged as a technology that is affecting a lot of domains such as manufacturing and automation, smart traffic systems, security, disaster management, etc. Security and user authentication are challenging due to the large number of connected devices and the magnitude of data shared among the devices. Typically, some digital fingerprint in terms of the features of the data stream to be transmitted is embedded in the data streams, but they can be extracted in case the adversary analyses the data stream and records it for a long period with a sufficient number of samples. Moreover, large length stochastic features would inevitably increase the system computation overhead and latency at the gateway. While lesser overhead can be settled that would result in higher bit errors and chances of attacks. In this paper, a deep learning-based approach is used to detect possible attacks based on the statistical features embedded into the bitstream transmitted. Additionally, the channel state information has been utilized for enhancing the Quality of Service of the system. The performance metrics are the bit error rate, number of epochs for training, and mean square error of the deep learning model.

Keywords Bit error rate · Channel state information · Deep learning · Internet of things · Signal authentication

1 Introduction

Internet of things (IoT) can be thought of as the interconnectivity of several devices over the internet. There can be a great deal of diversity in the type of devices connected to the IoT network [1–3]. One of the major constraints of IoT networks is the computational and memory limitations of internet of things devices (IoT) since low-cost sensors may have less storage and computation power to implement complex encryption algorithms. Moreover, conventional security in terms of cryptographic algorithms is NOT completely

✉ Arun Kumar Singh
arun@reck.ac.in

[1] Department of Electronics Engineering, Rajkiya Engineering College, Kannauj, India

secure. Cryptography relies on the infeasibility of computers to perform a computational operation within a specific time due to its computational complexity. However, with the emergence of Quantum Computing, the future scenario can completely change with the "Hack now, decode later approach". It is infeasible to search for any intrusion detection system to find all possible loopholes while traversing the entire periphery of the network [4]. Additionally, in the case of IoT, there is a large diversity of devices with varying levels of memory and computational power, making complex cryptographic algorithms infeasible to be implemented (although the advanced cryptographic algorithms are NOT completely secure too [5]. There always remains a tradeoff between the level of security and computational power needed thereby constraining system performance [6]. The enormous number of such sensing devices keeps increasing with scaling up the IoT framework to a massive IoT framework. Massive IoT frameworks are typically used for diverse applications such as defense and security, climate monitoring, disaster management, etc. [7, 8]. Due to the scale of the massive IoT networks, they are prone to attacks from adversaries who may either extract the data, extract and manipulate the data, add jamming to the transmitted data stream or employ denial of service depending upon the type of attack planned [9]. The IoT security model aims at securing the network fundamentally at three levels:

1. Physical Level Security
2. Network Level Security
3. Application-Level Security

The physical level security often termed the bit level security aims at securing the data to be shared on the hardware level of the IoTD. However, this approach may not be suitable if the IoT network is extremely large with a large diversity of devices connected constrained to the limited memory and compute power [10]. The network-level security is often employed at the IoT gateway, where the gateway on analyzing the individual IoTD data streams decided upon the authenticity of the data received, and evaluates the possibility of attacks. This is challenging owing to the constraints of bandwidth, time, and computation capability of the gateway. The gateway also needs to estimate the possible IoTDs whose security may have been compromised i.e. it needs to make a selection among the IoTDs which can be analyzed for attacks [11]. The application-level security tries to detect and block malicious applications which try to access the IoT framework. However, these attacks are at the point of the end-user, before which the actual data may have been compromised [12]. Based on the review of existing literature in the field, the following major challenges, problems, and research gaps in the domain have been identified:

1. Most conventional intrusion detection systems (IDS) are reactive whereas, for large-scale networks, a proactive approach is needed to ensure security [13, 14].
2. Application layer security alone is **NOT** reliable and enhanced security measures at the network layer and physical layer need to be augmented, which has seen lesser impetus in existing work.
3. Proactive approaches to detect possible attacks use the channel state information (CSI) of the network. However, limited work has been done in estimating the time-varying CSI statistics. Outdated CSI can lead to false alarms regarding attacks [15].
4. Limited work is done on devising hybrid peak to average power ratio (PAPR) reduction techniques which can achieve very low values making traffic imperceptible to potential attackers [16–18].

5. Correlation analysis among using the CSI, associated channel scatter and the error rate has not been sufficiently highlighted and exemplified [19].
6. A combination of data imperceptibility leveraging CSI for scattering and error analysis has NOT been coupled with efforts to statistically recover corrupt data packets using equalization techniques [20].

The basic security model for IoT frameworks is depicted in Fig. 1a while the categories of IoTDs in the network is depicted in Fig. 1b.

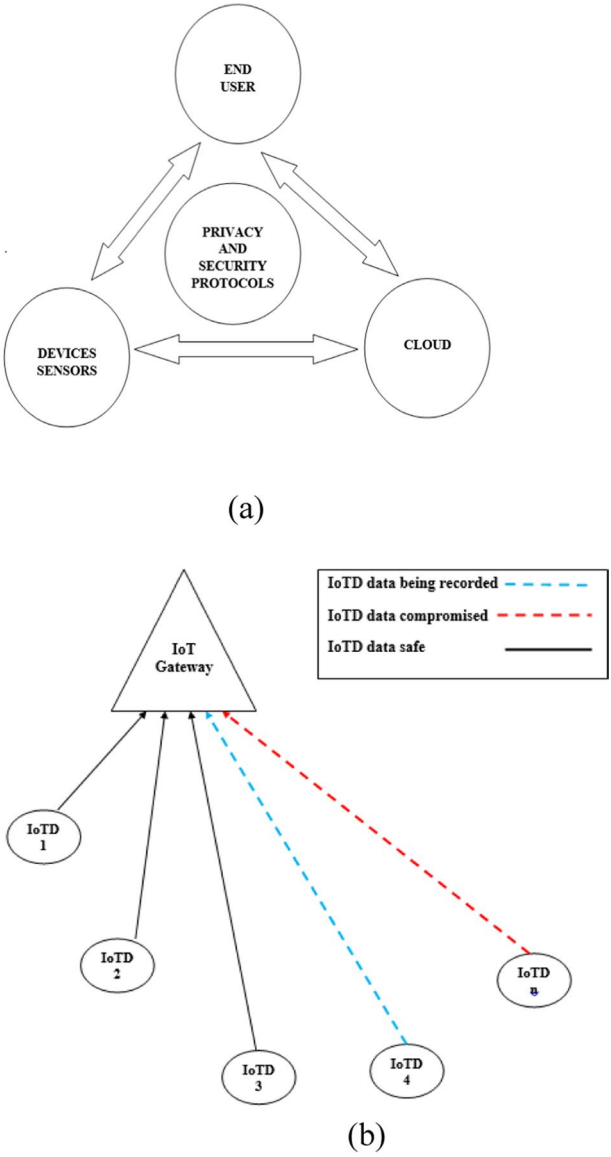


Fig. 1 **a** The IoT security model, **b** Categories of IoTDs in a network

With an increasing number of users, sensing nodes, and coverage areas, the internet of things can be scaled to design massive internet of things. In real-time applications, authenticating the data received is vital as the network can be prone to attacks from adversaries.

With limited memory and processing power at the disposal of IoT Devices (IoTDs), there exists a continued trade-off between the error rate (authentication metric), system overhead, computational complexity, and latency of the system. Hence an extremely meticulous system design with an appropriate choice of stochastic parameters and authentication scheme should be adopted. With the emergence of machine learning techniques, large and complex datasets can be analyzed in relatively much lesser time compared to conventional statistical techniques. This paper adopts a deep learning-based approach for signal authentication in massive IoT networks. Additionally, the quality of service of the network is a critical attribute of the system, which is typically evaluated in terms of the error rate and latency of the system. Thus, this research paper comes up with a proposed solution which tries to addess the problems identified in existing standard leiteratrue which can be summarized as:

The proposed work would work on combining the security attributes of both the physical and network layer in a proactive approach. For that purpose, the first step is to design a system which could extract the channel sense information at regular intervals of the system considering network parameters or network statistics **Quasi Stationary.** The channel state information (CSI) would be used to accomplish the following;

1. Detect possible ongoing attacks.
2. Avoiding future attacks.

This CSI base proactive approach would allow in higher attack and intrusion avoidance compared to conventional network based intrusion detection systems (NIDS). Moreover, to recover data, equalization techniques would also be employed. To increase the imperceptibility of the system, the peak to average power of transmitted data is also to be reduced using hybrid techniques thereby further reducing the chances of unauthorized intercepts. Finally, the CSI, error rate, scatter would be computed and correlated to reach a comprehensive conclusion. Additionally, utilizing the channel state information (CSI) of the system decide upon the choice of channels may help in improving the BER performance of the system [21]. The rest of the paper is organized as:

The difficulties in protecting IoT networks are discussed in Sect. 2, along with the system model for IoT authentication and the frequency selectivity of wireless channels. Deep learning and deep neural networks are discussed in Sect. 3 along with how they can be used to secure IoT networks. Also discussed is the value of channel state information (CSI). The acquired simulation findings and their importance are discussed in Sect. 4. The conclusions and key lessons of the suggested approach are presented in Sect. 5

2 System Model For Iot Signal Authentication and Extracting Channel State Information (CSI)

This section presents the signal authentication framework along with extracting the channel state information (CSI) and utilizing it.

2.1 IoT Device Authentication

There are several challenges corresponding to the authentication of IoTDs in a network, which primarily are:

IoT devices may have very limited processing power and memory, the enormity of the decisions and actions to be performed by the gateway makes it extremely constraining for the gateway to attain convergence of results in limited amounts of time, the IoT gateway doesn't always have information about the IoTDs, whose security may or may not have been compromised, adding large watermarks or digital fingerprints leads to computational overhead of the system which again adversely affects the gateways constrained computational and decision making capabilities, bandwidth limitations also do not allow simultaneous authentication of all IoTDs, deciding which of the IoTDs can be authenticated among all the IoTDs and finally deciding how to authenticate the IoTDs selected with least overhead and minimum bit error rate (BER). The different categories of IoTDs in a network are shown in the Fig. 2 whose data reaches the IoT gateway [22, 23]. Typically, the enormity of the decisions to be incurred by the gateway results in a tradeoff between the security and the quality of service parameters such as the bit error rate and the latency [24]. One of the most effective yet convenient techniques to secure IoTDs transmission and authentication is computing statistical features or parameters from the data stream and embedding it into the transmitted data. The set of features is often termed as the digital fingerprint. The bit stream containing the digital fingerprint is analyzed by the gateway, which extract the bit stream and decides whether the IoTD is compromised or not [25]. Typically, the attack would occur between the IoTD and the gateway which would manipulate the stochastic properties of the data stream. This can be sensed by the authentication mechanism at the gateway and the decision regarding possible attack can be taken [26]. The security framework is depicted in Fig. 2a.The frequency selective nature of wireless channels is depicted in Fig. 2b.

The limitations of the computational resources at the gateway invariable compel the gateway to forecast the data streams with higher chances of being compromised and then authenticating them at first. On the contrary, the adversaries would focus on targeting the data streams from IoTDs which are least possible to be picked up by the gateway for authentication. This leads to the formulation of a non-cooperative game at the gateway between the gateway terminal and adversaries recording the data streams. Thus, at the gateway terminal, the IoTDs whose data streams can be analyzed by the gateway under resource constraints are [27]:

$$s_G = T \in N : \sum_{i \in T} f_s \leq R \tag{1}$$

Here, s_G is the strategy at the IoT Gateway. T is the number of IoTDs to be analyzed at the gateway. N is the total number of IoTDs transmitting at a time to the gateway. f_s is the sampling frequency at which the data stream is sampled under resource constraints of 'R'.

R is the set of available resources.

The limitation on the gateway for the authentication of the IoTDs can be expressed in terms of the computational complexity notation 'O' as:

$$O\left(\frac{f_i}{n_i}\right) \leq O(C) \tag{2}$$

Here, f_i is the sampling frequency of the ith IoTD. n_i is the number of IoTDs authenticated?$O(C)$ is the total authentication complexity.

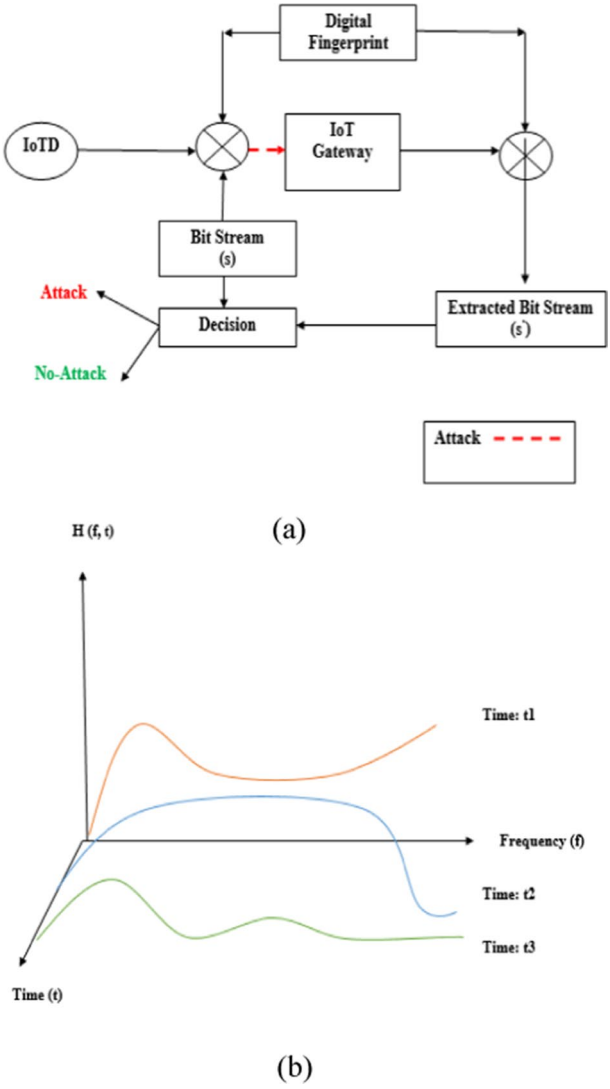


Fig. 2 **a** Framework for securing an IoT network at gateway, **b** Channel response of a frequency selective channel

A successful resource constrained sampling and authentication is possible only if the inequality in (2) is maintained [28].

2.2 Frequency Selective Nature of Wireless Channels

Practical wireless channels exhibit frequency selective nature in terms of the channel frequency response. The signals undergoing different fading effects create different BER and Outage patterns at the output. The fading pattern depends on the attenuation constant. The attenuation constant again depends on the material constants of the channel which are the permittivity, permeability, conductivity. It also depends on the frequency of transmission. Therefore the fading pattern would obviously vary with the frequency of transmission and

also on the nature of the channel as it keeps changing with changes in the channel characteristics. Mathematically, the attenuation constant is given by [28]:

$$\alpha = \frac{\omega\pi}{2}\sqrt{\frac{1}{\sigma + \omega\epsilon}^{2} - 1} \tag{3}$$

Here, α represents the attenuation constant. ω represents the angular frequency. μ represents the permeability of the medium. ϵ represents the permittivity of the medium. σ represents the conductivity of the medium.

Since the attenuation constant depends on the angular frequency ω, which in turns depends on the frequency as per:

$$\omega = 2\pi f \tag{4}$$

Here, f represents the frequency.

Hence, for multiple frequencies, the nature of the channel and hence the channel response would vary. This is typically important to gauge so as to find out suitable frequencies for transmission. This necessitates the evaluation of the channel state information and further selection of the frequencies for transmission which exhibit a satisfactory channel gain. The channel gain is computed as:

$$g_f = \frac{P_o}{P_i} \tag{5}$$

Here, g_f represents the channel gain for a particular frequency f. P_i represents the input power to the channel for the frequency. P_i represents the output power of the channel for the frequency.

3 Proposed Method

The main challenge faced by the IoT gateway is the decision regarding the authentication of IoTDs and the elated computational complexity [29]. One of the most effective approaches is adding digital fingerprints to the data stream to be transmitted so as to secure the transmission and subsequently use some framework to authenticate the data for:

- Non-compromised security
- Compromised security.

3.1 Watermarking Strategy

EquationsThe watermarking strategy adopted in this case is based on the statistical feature extraction of the parameters from the transmitted IoTDs.

Considering 'N' IoTDs transmitting to the gateway 'G', $IOTD_i$ transmits a data stream y_i at time 't' sampled at a sampling frequency of f_i.

This gateway and the adversary play a non-cooperative game where the gateway tries to identify the IoTDs to be authenticated wherein the adversary tries to mark IoDs which are less likely to be analyzed by the gateway and manipulated the data stream y_i to $y_i^{'}$.

The authentication mechanism at the gateway then needs to compare y_i and $y_i^{'}$ thereby deciding upon the status of attack or non-attack. The constraints which the gateway

faces are the large magnitude of simultaneous transmissions by IoTDs, noise and disturbance in the channel changing the nature of the bit streams transmitted, limitations of bandwidth and power. The computation of the following stochastic parameters is done in this case [30]:

$$mean\{y_i(t)\} = \mu_i \tag{6}$$

$$variance\{y_i(t)\} = \sigma_i^2 \tag{7}$$

$$standarddeviation\{y_i(t)\} = \sigma_i \tag{8}$$

$$Energy\{y_i(t)\} = E_i \tag{9}$$

$$Entropy\{y_i(t)\} = En_i \tag{10}$$

Additional parameters are correlation, skewness and kurtosis. The data stream comprising of the watermark is given by:

$$s_w(t) = s_i(t) + \gamma_i br_i(t) \forall t = 1 \ldots .n_i \tag{11}$$

where,

$$\gamma_i = \frac{Power(r_i)}{Power(s_i)} \tag{12}$$

Here, $s_w(t)$ is the embedded data stream $.s_i(t)$ is the IoTD bit stream. r_i is the random sequence generated for IOTDi.b is the hidden bit stream of + 1 or –1 for bipolar signaling.n_i denotes the number of samples.

In order to detect the attacks, the gateway computes:

$$\widehat{b_i} = \frac{\langle r_i, s_i \rangle n_i}{\gamma_i n_i} \tag{13}$$

Here, $\langle r_i, s_i \rangle$ denotes the correlation or inner product. $\widehat{b_i}$ which is the extracted watermarked bit-stream at the gateway can be expressed as the summation of the actual embedded bit stream $\widehat{b_i}$ and the received data stream at the gateway $\widehat{s_i}$, thus giving:

$$\widehat{b_i} = \widehat{s_i} + b_i \tag{14}$$

The decision regarding the bit extracted (for bipolar signaling is based on the following conditions),

{
If $(\widehat{b_i} > 0)$bit = 1
Else,bit = −1
}

If the gateway computes the received bit stream to be $\widehat{y_i}$ in place of y_i, an attack is detected. As the data to be analysed is extremely large and complex in a massive IoT system, machine learning can be used for the authentication purpose.

The Machine Learning (ML) enabled security framework is depicted in Fig. 3a while the mathematical model for a neural network is depicted in Fig. 3b.

The ML model is to be trained with the digital footprints (extracted features) of the data streams of IoTDs and the Random PN sequence data. Based on the extracted digital fingerprint values, the ML model decides whether the data stream arriving at the gateway is compromised or not. The probability of incorrect estimation is given by [31]:

For the Gateway,

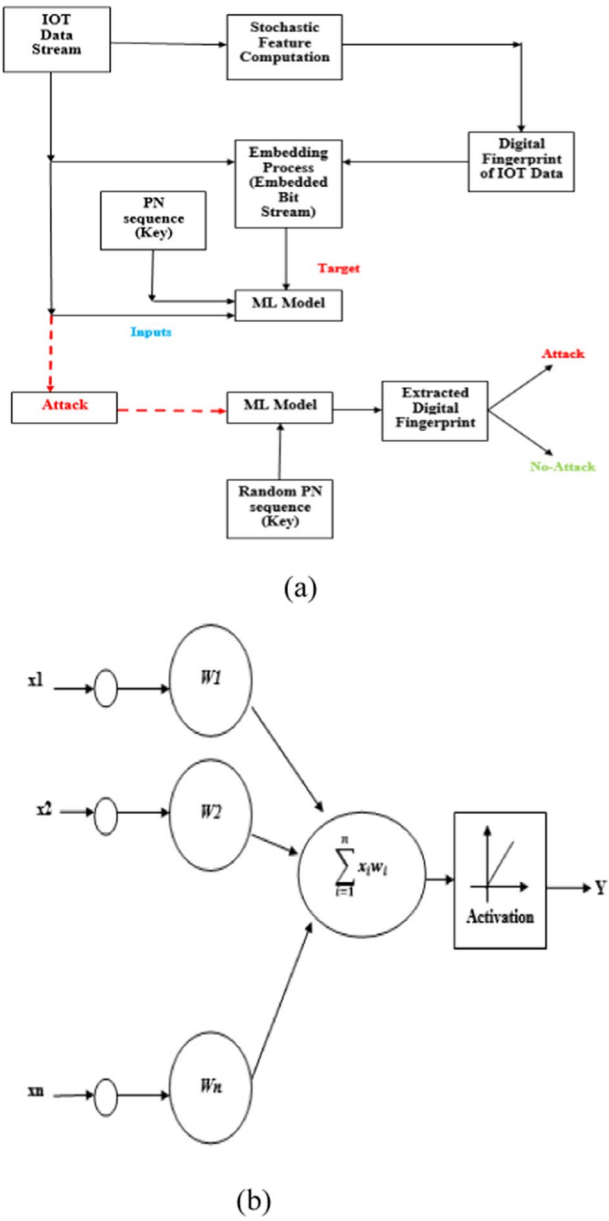


Fig. 3 **a** The proposed deep learning based authentication framework, **b** Model of a neural network

$$P_e = \Pr\{\widehat{b_i} = 0,\ for\ b_i = 1\} \leq P \tag{15}$$

Here, Pr denotes probability. $\widehat{b_i}$ is the estimated bit. b_i is the actual bit transmitted.P is a desired low probability.

Thus for the gateway, represents the probability of error of detecting a bit as bit '0', for a transmission of bit '1'.

A similar formulation can be developed for transmission of bit '0' and reception of bit '1'.

Considering a joint probability for simultaneous probability of error for gateway and attacker, we can write the probability of error for the attacker as:

$$P_e = \Pr\left\{\widehat{b_i} = 0, for b_i = 1\right\} \geq 1 - P \tag{16}$$

Thus, to jointly obtain low BER (probability of error) for gateway and high BER (probability of error) for attacker, the value of P should be as low as possible with P being bounded by:

$$0 \leq P \leq 1 \tag{17}$$

The probability of error as a function of the error function or Q function is given by:

$$P_e = \frac{1}{2} erfc\left(\frac{\gamma_i \sqrt{n_i}}{\sigma_i \sqrt{2}}\right) \tag{18}$$

Here, erfc denotes the error function.

For large values of γ_i, the probability of errors would reduce as larger values of arguments for the erfc function result in lower values and vice versa. However, large values of γ_i would also mean larger power consumption as the power of the random sequence generated would be more. This however, has a much more serious repercussion in terms of the security. Let is consider large values of γ_i such that,

$$P(r_i) \gg P(s_i) \tag{19}$$

This would mean more perceptibility of the inserted random bit stream, making the chances of successful attack higher. Thus, while larger values of γ_i would ensure lesser errors and more reliable data transfer, it would escalate the chances of successful data intercepts by adversaries. Lower values of γ_i would mean inherently higher value of errors making the data transfer more prone to errors [32]. Thus a trade off between the security and the reliability of data transfer exists in the system. One of the possible solutions to the problem is the use of large values of n_i, while this may allow the adversary to record more samples of the data received at the gateway thereby making more accurate estimated about the IoTD data stream. Moreover, the computation at the gateway would increase manifold owing to larger values of n_i. The proof for the aforesaid proposition can be ststes in brevity as [33]:

For a Gaussian random a variable Z with a distribution function $N\left(\frac{\mu_I}{\gamma_I^2 \sigma_I^2}\right)$, received signal at the IoT gateway can be given by:

$$z_i = \frac{1}{\gamma_i n_i} \sum_{i=1, i \epsilon Z^+}^{n} z_i(t) - \sum_{i=1, i \epsilon Z^-}^{n} z_i(t) = \frac{n_{i^+}}{\gamma_i n_i n_{i^+}} \sum_{i=1, i \epsilon Z^+}^{n} z_i(t) - \frac{n_{i^-}}{\gamma_i n_i n_{i^-}} \sum_{i=1, i \epsilon Z^-}^{n} z_i(t) \tag{20}$$

Assuming a fair or unbiased event $'A'$, with the random variable z exhibiting equi-probabile states of$0 or 1$, the Central Limit Theorem yields:

$$P_i^-\{z(i=0)\} = P_i^+\{z(i=1)\} \tag{21}$$

The combination of the Gaussian Random variables $z_i^- and z_i^+$) would result in:

$$z_i \sim N\left(\frac{\{n_{i^+} - n_{i^-}\}\mu_i}{\gamma_i n_i}\right) \sim \frac{1}{2} erfc\left(\frac{\gamma_i\sqrt{n_i}}{\sigma_i\sqrt{2}}\right) \tag{22}$$

In order to limit the computational complexity and latencies at the gateway, machine learning algorithms rendering low to moderate number of training epochs should be chosen. Off late, artificial intelligence and machine learning have evolved as computational tools which can be used for analysis of large and complex data sets for time critical applications. Artificial neural networks (ANNs) are mathematical models which can be to implement artificial intelligence and machine learning practically [34]. The mathematical model for the neural network is depicted in Fig. 3b. The output of the ANN is given by:

$$y = \sum_{i=1}^{n} f(w_i x_i + \varphi) \tag{23}$$

Here, y is the output. x is the input vector.w is the weight vector. φ is the bias. f is the activation function.n is the number of inputs.

The data in this case is time series in nature and thus neural networks which are recurrent in nature can be effective for the analysis.The back-propagation training algorithm can be used to train such a neural network given by [35]:

$$w_{k+1} = w_k - \left[J_k J_k^T + \mu I\right]^{-1} J_k^T e_k \tag{24}$$

Here, w_{k+1} is weight of next iteration, w_k is weight of present iteration. J_k is the Jacobian Matrix. J_k^T is Transpose of Jacobian Matrix. e_k is error of Present Iteration .μ is step size and I is an identity matrix.

As the data is large and complex time series in nature, hence a deep neural network with multiple hidden layers is expected to render lesser value of errors and high accuracy [36, 37]. In this case, the number of hidden layers taken is 50. The performance metric for the deep neural network are considered to be the number of iterations and mean square error (cost function) defined as:

$$mse = \frac{1}{n}\sum_{I=1}^{N}(X - X')^2 \tag{25}$$

Here, X denotes the actual output. X' denotes the predicted output.n denotes the number of samples predicted.

3.2 Utilizing the Channel State Information (CSI)

Figure 4 shows how channel sounding, which normally produces a temporally fluctuating pattern, can be used to extract the channel state information (CSI). A sampled representation of the channel frequency response which is obtained by the typical CSI is given by [38]:

$$CSI_t = \sum_{i=1}^{n} H(f, t - Ti) \tag{26}$$

Here, T is the time period for channel sounding. $i \in 1, 2 \ldots .. CSI_t$ is the time varying CSI. H is the channel frequency response.

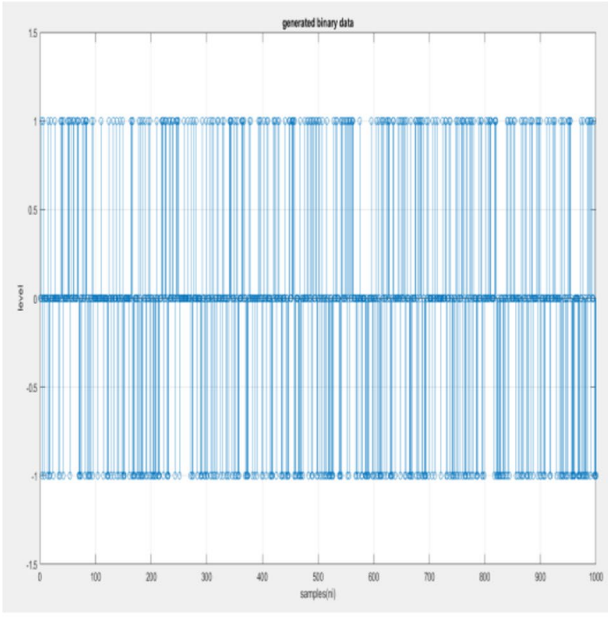


Fig. 4 **a** Bipolar data stream, **b** Extracted features

Samples of the channel response can be obtained as a vector as:

$$H(f,t) = H1, H2, H3 \ldots \ldots Hn \tag{27}$$

Here, $H(f,t)$ is the time dependent channel sounding information. f is the frequency metric. t is the time metric. H is the response at a particular time t.

Here, it can be shown that the channel response depends on both time and frequency. On channel sounding, a temporally variable pattern is often obtained [39]. Considering the bit error rate as one of the major Quality of Service (QoS) metrics for the system, the important decision to be made on channel sounding is the choice of carriers [40]. The carriers to be chosen at time 't' should exhibit a channel gain above a particular threshold based on the system requirements and the receiver noise sensitivity. Thus if a threshold value of 'T' is chosen, the all frequencies exhibiting a channel gain greater than 'T' at a particular time 't' would qualify to be used as frequencies for transmission given by the following condition.

$$if\ g_f(t) > T;\ use\ carrier\ for\ transmission\ else,\ discard\ carrier. \tag{28}$$

This would allow is selecting carriers which would satisfy the minimum channel gain requirements of the system. As the channel changes its nature continuously, hence continuously sampling the CSI is necessary which may be computationally expensive [40].There would clearly exist a trade off between the number of samples to be considered to estimate the CSI and the computational complexity of the system. More samples (higher sampling rate) would render a more accurate picture of the channel while consuming more computational resources.

4 Results and Discussion

The system has been simulated on MATLAB 2020a. The obtained results have been discussed subsequently. The results include the binary data stream for transmission and computed statistical features from the bit steam which are embedded into the bit stream in Fig. 4a, b respectively.

The number of bits used for the simulation are 10^6 per IoTD. Bipolar transmission scheme is considered in this case. Figure 4b depicts the bar graph of the computed feature values (digital fingerprints of the bit stream) to be embedded. The computed features are: Energy, Entropy, Correlation, Variance, Standard Deviation, Kurtosis, Skewness and Mean. Figure 5a depicts the Welch Power Specturm of the sequence, while Fig. 5b depicts the data stream under attack.The data stream exhibits a clear increase in power at the beginning of the attack. It can be observed that a sharp increase in the power of the samples takes place in case of inception of the attack. The attack renders an elevated yet variable power level corresponding to the jamming or adversarial power injection to sub-bands of the transmitted data stream.

The stochastic characteristics of the data vary in case of attacks which are the analyzed at the gateway using the relation $\hat{b_i} = \frac{\langle r_i, s_i \rangle n_i}{\gamma_i n_i}$. There exists a possibility of noise rendering a similar change in the power levels but in most cases would be distinguishable for AWGN conditions.Figure 6a depicts the training cost function or loss function up-to convergence. It can be observed that the number of iterations to convergence are 60 with a loss function

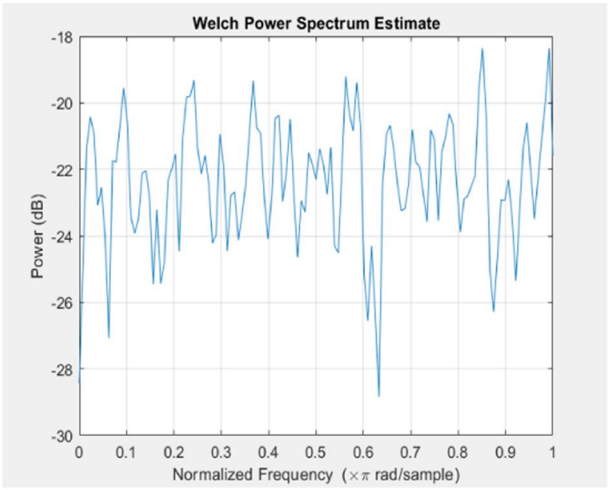
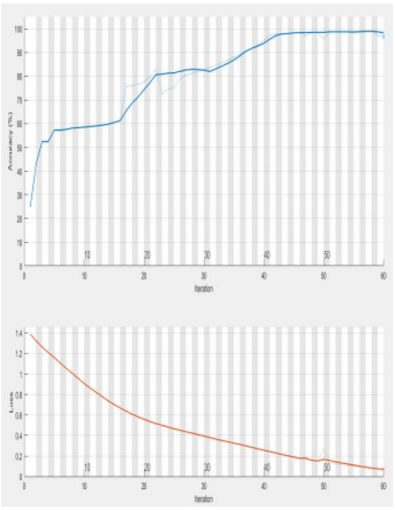


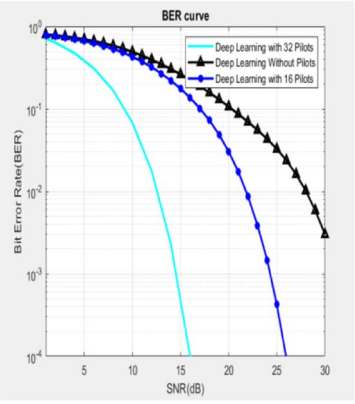
Fig. 5 **a** Welch power spectrum of data stream, **b** Data stream under adversarial attack

value stabilizing around 10^{-1}. The choice of training rule and deep neural architecture is critical to reduce the time complexity of the system.

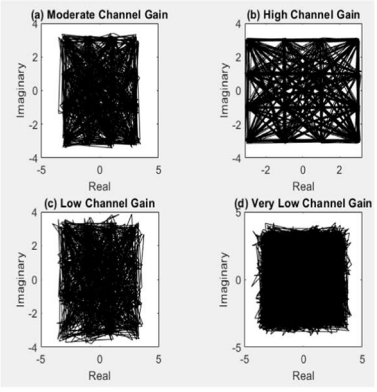
Figure 6b depicts the variation of the bit error rate (BER) of the system with respect to the SNR as the number of pilot bits are varied. The system is simulated for a channel gain threshold of 0.6 i.e. $T_{gain} = 0.6$. The value for the threshold could have been chosen higher but that would have left out more frequencies thereby limiting the usable spectrum. Thus the frequencies with a minimum channel gain of 0.6 are considered for data transmission and the rest are rejected for the particular channel sounding sample. Further, the BER performance of the system is evaluated with 16 and 32 pilot bits added to aid the deep learning mechanism. It can be seen from Fig. 6b that the addition of pilots results



(a)



(b)



(c)

Fig. 6 **a** Bipolar data stream, **b** Extracted features, **c** Channel scatter plot for varying channel gain

Table 1 Summary of results

S.no	Parameter	Value
1	Features computed	8
2	ANN topology	Deep neural network
3	Channel gain threshold	0.6 or 60%
4	Training epochs	60
5	MSE (objective function) at end of training	0.1
6	Pilots used	0, 16, 32
7	Minimum BER obtained	10^{-4} at SNR of 16 dB

in a steeper reduction of the BER. However, it increases the system overhead. Figure 6c depicts the scatter plot for the system for four different channel conditions which are high channel gain, moderate channel gain, low cahnnel gain and very low channel gain. It can be observed that a summary of the results obtained is tabulated in Table 1.

The proposed system employing the deep neural network reaches convergence of training in only 60 iterations with a loss function value of 0.1 for the system designed. The SNR requirement of 16 dB to reach a BER of 10^{-4} indicates relatively low power requirement. 16 and 32 pilot bits used in conjugation with the Deep Neural Network indicate low overhead.

5 Conclusion

Presently massive IoT systems are being used in several applications but one major problem which is being encountered is the security and authentication of such systems. This is due to the fact that the amount of data generated and shared in the IoT network makes is extremely challenging for the IoT gateway to authenticate the IoTDs, under constraints of resources. In this paper, a deep neural network based techniques has been proposed for the authentication of IoTDs to be employed at the IoT gateway. The system uses a deep neural network for authentication. Moreover, to enhance the reliability and quality of service of the system, a channel sounding and CSI based frequency selection mechanism is proposed. It has been shown that the proposed system attains a very low mean square error of training with low training epochs. The BER of the system reaches 10^{-4} with 16 pilot bits at an SNR value of 16 dB. Further directions of research could be computing and minimizing the latency of large netwoks which would further improve the quality of service (QoS) of the system.

Acknowledgements The authors would like to extend their gratitude towardsthe faculty members of Department of Electronics Engineering, Rajkiya Engineering College, Kannauj, India. The suggestions and constructive criticism has helped in polishing the paper and making it more comprehensible.

Author Contributions All authors contributed equally to prepare this work.

Funding The author(s) received no financial support for this article's research, authorship, and/or publication.

Date Availability All data generated or analyzed during this study are included in this published article.

Declarations

Conflict of interest The authors declare that there are no conflicts of interest.

Compliance with Ethical Standards All procedures performed in studies involving human participants were in accordance with the ethical standards.

Consent to Participate Not applicable.

Consent for Publication The Author transfers his copyrights to the publisher.

References

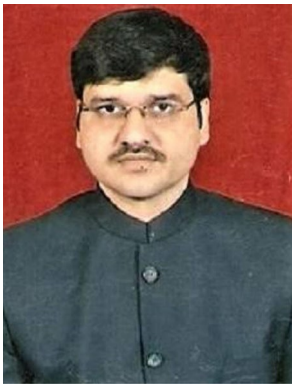
1. K. Zhao and L. Ge, A Survey on the Internet of Things Security, 2013 Ninth International Conference on Computational Intelligence and Security, IEEE 2013, pp. 663–667.
2. Q. Abbas, S.A. Hassan, H.K. Qureshi, K. Dev, and H. Jung, "A comprehensive survey on age of information in massive IoT networks," in *Computer Communications* , 2022.
3. Hossain, M. A., Hossain, A. R., & Ansari, N. (2022). Numerology-capable UAV-MEC for future generation massive IoT networks. *IEEE Internet of Things Journal, 9*(23), 23860–23868.
4. Q. Gou, L. Yan, Y. Liu and Y. Li, "Construction and Strategies in IoT Security System," 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, IEEE 2013, pp. 1129–1132
5. Lee, B. M., & Yang, H. (2022). Energy efficient scheduling and power control of massive MIMO in massive IoT networks. *Expert Systems with Applications, 200*, 116920.
6. Namvar, N., Saad, W., Bahadori, N., & Kelley, B. (2016, December). Jamming in the internet of things: A game-theoretic perspective. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.
7. Song, K., Wang, Q., Peng, L., Li, C., & Wu, X. (2021). Secrecy energy efficiency optimization for DF relaying IoT systems with passive eavesdropping terminal. *Journal of Physical Communications, 44*, 1–28.
8. Saravanan, V., Sreelatha, P., Atyam, N. R., Madiajagan, M., Saravanan, D., & Sultana, H. P. (2023). Design of deep learning model for radio resource allocation in 5G for massive iot device. *Sustainable Energy Technologies and Assessments, 56*, 103054.
9. Song, K., Yang, J. C., & Fang, B. X. (2011). Security model and key technologies for the Internet of things. *The Journal of China Universities of Posts and Telecommunications, 18*(2), 109–112.
10. Pecorella, T., Brilli, L., & Mucchi, L. (2016). The role of physical layer security in IoT: A novel perspective. *Journal of Inforamtion, MDPI, 7*(3), 1–17.
11. Kalkan, K., & Zeadally, S. (2018). Securing internet of things with software defined networking. *IEEE Communications Magazine, 56*(9), 186–192.
12. Sarrab, M., & Alnaeli, S. M. (2018, November). Critical aspects pertaining security of iot application level software systems. In 2018 IEEE 9th annual information technology, electronics and mobile communication conference (IEMCON) (pp. 960-964). IEEE.
13. 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.
14. Mohamad, F., Haroun, T., Haroun, M. F., & Gulliver, T. A. (2021). Secure OFDM with peak-to-average power ratio reduction using the spectral phase of chaotic signals. *Entropy, 23*(11), 1380.
15. Chen, Y., Zhang, T., Liu, Y., & Qiao, X. (2020). Physical layer security in noma-enabled cognitive radio networks with outdated channel state information. *IEEE Access, 8*, 159480–159492.
16. J. Shen Bo Liu; Yaya Mao; Rahat Ullah; Jianxin Ren; Jianye Zhao; Shuaidong Chen., "Enhancing the Reliability and Security of OFDM-PON Using Modified Lorenz Chaos Based on the Linear Properties of FFT," in Journal of Lightwave Technology, vol. 39, no. 13, pp. 4294–4299, July1, 2021.
17. Istiaque Ahmed, K., Tahir, M., Hadi Habaebi, M., Lun Lau, S., & Ahad, A. (2021). Machine learning for authentication and authorization in IoT: Taxonomy, challenges and future research direction. *Sensors, 21*(15), 5122ssssss.
18. Sadique, J. J., Ullah, S. E., Islam, M. R., Raad, R., Kouzani, A. Z., & Mahmud, M. A. P. (2021). Transceiver design for full-duplex uav based zero-padded ofdm system with physical layer security. *IEEE Access, 9*, 59432–59445.

19. 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.
20. J Zhao, B Liu, Y Mao, R Ullah, J Ren, S Chen, High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization”, OSA publications, vol.28, issue.14, pp.21236–21246.
21. Wang, H.-M., Bai, J., & Dong, L. (2020). Intelligent reflecting surfaces assisted secure transmission without eavesdropper’s CSI. *IEEE Signal Processing Letters, 27*, 1300–1304.
22. Bordel, B., Alcarria, R., Robles, T., & Iglesias, M. S. (2021). Data authentication and anonymization in iot scenarios and future 5G networks using chaotic digital watermarking. *IEEE Access, 9*, 22378–22398.
23. Ferdowsi, A., & Saad, W. (2018). Deep learning-based dynamic watermarking for secure signal authentication in the internet of things. *IEEE International Conference on Communications (ICC), 2018*, 1–6.
24. 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.
25. Moosavi, S. R., Gia, T. N., Rahmani, A. M., & Nigussie, E. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science, 52*, 452–459.
26. MNO Sadiku, Elements of Electromagnetics, 4th Edition, Oxford University Press.
27. 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.
28. PSF Sheron, KP Sridhar, S Baskar, “A decentralized scalable security framework for end to end authentication of future IoT communication”, Special Issue on Cross layer innovations in Internet of Things and Advanced Microprocessor Optimization methods for the Internet of Things, Wiley Online Library, vol. 31, no. 12, pp.1–12.
29. Eriksson, J., Ollila, E., & Koivunen, V. (2010). Essential statistics and tools for complex random variables. *IEEE Transactions on Signal Processing, 58*(10), 5400–5408.
30. Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. *Heliyon, 4*(11), e00938.
31. P. G. Madhavan, Recurrent neural network for time series prediction, Proceedings of the 15th annual international conference of the IEEE engineering in medicine and biology societ, (1993), pp. 250–251.
32. Conitzer, V., & Sandholm, T. (2008). New complexity results about nash equilibria. *Games of Economic Behaviour, 63*(2), 621–641.
33. Hu, J., Li, W., & Zhou, W. (2019). Central limit theorem for mutual information of large mimo systems with elliptically correlated channels. *IEEE Transactions on Information Theory, 65*(11), 7168–7180.
34. Reynaldi, A., Lukas, S., & Margaretha, H. (2012). Backpropagation and levenberg-marquardt algorithm for training finite element neural network. *Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation, 2012*, 89–94.
35. H. Sun, X. Chen, Q. Shi, M. Hong, X. Fu and N. D. Sidiropoulos, Learning to optimize: Training deep neural networks for wireless resource management, 2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2017, pp. 1–6.
36. Zhou, F., Zhou, H., Yang, Z., & Gu, L. (2021). IF2CNN: Towards non-stationary time series feature extraction by integrating iterative filtering and convolutional neural networks. *Expert Systems with Applications, 170*, 114527.
37. B. Neekzad, K. Sayrafian-Pour, J. Perez and J. S. Baras, Comparison of ray tracing simulations and millimeter wave channel sounding measurements, 2007 IEEE 18th international symposium on personal, indoor and mobile radio communications, (2007), pp. 1-5.
38. Talak, R., Karaman, S., & Modiano, E. (2020). Improving age of information in wireless networks with perfect channel state information. *IEEE/ACM Transactions on Networking, 28*(4), 1765–1778.
39. Katorin, Y. F., Makshanov, A. V., Danilin, G. V., Yemelyanov, V. A., & Ovcharenko, I. K. (2020). Improving the QoS multiservice networks: New methods, impact on the security of transmitted data. *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2020*, 341–344.
40. Earle, B., Al-Habashna, A., Wainer, G., Li, X., & Xue, G. (2021). Prediction of 5G new radio wireless channel path gains and delays using machine learning and CSI feedback. *Annual Modeling and Simulation Conference (ANNSIM), 2021*, 1–11.

Rajeev Kumar obtained his Bachelors in Technology from UIET, Kanpur and Masters in Technology from Intian Institute of Technology, Kanpur (IITK). His areas of interest are signal processing, wireless sensor networks, IoT and future generation wirelss networks. Presently he is an Assistant Professor in the Department of Electronics Engineering, Rajkiya Engineering College, Kannauj, India. rajeev@reck.ac.in

Gaurish Joshi obtained his Bachelors in Engineering from Z.H.C.E.T, AMU(Aligadh muslim university) Aligarh and Masters in Technology from Motilal Nehru National Institute of Technology, (MNIT) Allahabad. His areas of interest are image processing, data science, machine learning and wireless networks. Presently he is an Assistant Professor in the Department of Electronics Engineering, Rajkiya Engineering College, Kannauj, India. gaurishjoshi@reck.ac.in

Amit Kumar Singh Chauhan obtained his B. Tech. from BIET Jhansi and M. Tech. from Motilal Nehru National Institute of Technology, (MNNIT) Allahabad. His areas of interest are Semiconductor Devices, Embedded System, and IoT Systems. Presently he is an Assistant Professor in the Department of Electronics Engineering, Rajkiya Engineering College, Kannauj, India. amitchauhan@reck.ac.in



Arun Kumar Singh obtained his B.E in Electronics and Instrumentation Engineering from BIET Jhansi in year 1997, M.Tech. in Digital Electronics and Systems, and Ph.D. in the area of distributed systems (Adhoc networks) from Uttar Pradesh Technical University, Lucknow. Presently he is Dean (Academics/PGSR), CoE along with Head of the Electronics Engineering Department at Rajkiya Engineering College, Kannauj, U.P, and has more than 24 years of experience. Dr. Singh is a Fellow member of IE (I), IETE, a Senior member of IEEE, and life member of ISTE. He wrote several books on digital electronics and microcontrollers and got CMI Level 5 Award in Management and Leadership. He contributed research papers in several national and international conferences/journals and also delivered many lectures/keynote address; organised several FDP and workshop/training programs for students and teachers. As a Technologist/Engineer, his interests are: application of technology driven education paradigm, wireless communication, distributed systems, control systems, formal methods, and system modelling. Orcid Id: 0000–0002-7367–8619. arun@reck.ac.in

Ashish K. Rao received his B.Tech degree from Dr. APJ Abdul Kalam technical university, Lucknow, and M.Tech degree from BBD University Lucknow,UP, India. He is currently an Assistant Professor in the Department of Electronics Engineering in Rajkiya Engineering College Kannauj, UP, India. His research interests include Wireless Sensor Network, Cognitive Radio Communication. asis151rao@gmail.com