Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Deep Learning Approach for Identifying Intrusion and Data Authentication for Pervasive Networks

Dr. Bharti Bhattad[1], Poonam Chaurasia[2]

[1]Associate Professor, Computer Science and Engineering, Acropolis Institute of Technology and Research, India, bhartibhattad@acropolis.in
[2]Assistant Professor, Computer Science and Engineering, Malawa Institute of Technology, India, poonam@mitjndore.co.in

As newer wireless technologies such as IoT, fog networks and edge computing are gaining more popularity, securing such networks also has become a primary objective for network designers. With copious amounts of data being shared among diverse types of devices, analysing the network traffic to identify anomalies or potential threats have become even more challenging. Moreover, as technologies such as quantum computing and quantum machine learning keep improving, the potential and methodologies of implementing attacks would also become more sophisticated in future. This necessitates the development of security mechanisms which can thwart sophisticated attacks on networks and render reliable authentication of user data. This paper presents a machine learning based approach for randomizing the data transmission as well as authenticating data through stochastic parameters. Thus, the approach employs both authentication as well as imperceptibility to the data transmission mechanism to secure wireless networks. A comparative analysis in terms of error rate and sum secrecy rate w.r.t. existing work indicates the improved performance of the deep learning approach compared to existing work in the domain.

Keywords: Networks Security, Intrusion Detection, Data Authentication, Data Imperceptibility, Deep Learning, Error Rate, Sum Secrecy Rate.

1. Introduction

The internet of things can be considered to be a pervasive and diverse connection of interconnected devices over the internet [1]. Several types of devices are connected over the internet which may possess highly varying hardware and software properties such as memory and data processing capability. The internet of things framework needs to be monitored and secured against attacks as the mode of data transmission is wireless thereby making the chances of possible attacks more compared to wired networks [2].

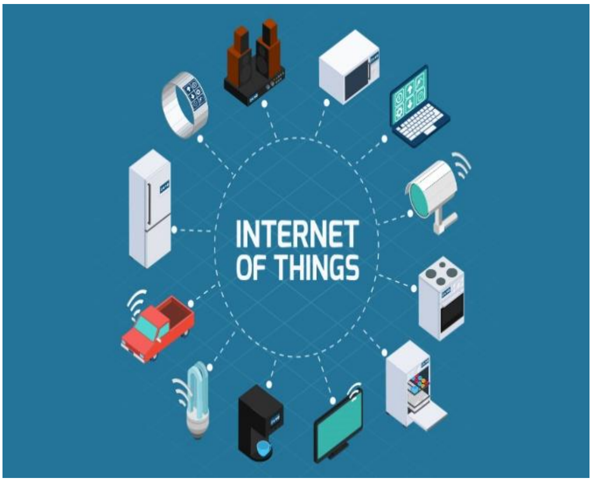


Fig. 1 Conceptual Framework for IoT

In There are 3 primary security paradigms in IoT networks [3]:

1) Application Layer Security

2) Network Layer Security

3) Physical Later Security

To secure the IoT framework, its often advisable to design a Network intrusion detection systems (in short NIDS) are systems designed to gauge and analyze the intrusions targeted towards networks. These systems are placed at specific places within the network to monitor every type of traffic that passes through the network [4]. All kinds of traffic that comes to and goes from the network is sensed for any sort of malicious activity or intrusion. The security model to design an intrusion mechanism based on machine learning is being explored off late as copious amounts of data need to be processed by the IoT gateway in real time [5]. Several approaches have been employed previously for data authentication and intrusion detection in wireless networks. A brief summary of existing work is presented in able 1.

Table 1. Previous work

S.No.	Authors	Approach
1.	A. Ferdowsi et al. [6]	Authenticating IoTDs in a massive IoT network through a game theoretic approach and digital data watermarking, analysing cases of attack and non-attacks and training an LSTM model.
2.	Anajemba et al. [7]	Securing a multi user detection (MUD) data transfer framework for IoT networks employing swarm intelligence based stochastic optimization.
3.	Mahmoud et al. [8]	Intrusion detection of IoT networks through IoD stochastic analysis using AE-LSTM: Autoencoder with LSTM.
4.	Nanjappan et al. [9]	Employing Deep Learning models such as LSTM and GRU for securing IoT networks through stochastic analysis of data streams at IoT gateway.
5.	Hu et al. [10]	Employing cooperative jamming for physical layer security in IoT networks. Analysis of spreading factor on error rates received done.

6.	Mahmoud et al. [11]	Employing deep reinforcement learning (DRL) to secure for bandwidth constrained IoT networks with sporadic malicious behaviour.
7.	Lin et al. [12]	A GAN- deep reinforcement learning based approach for securing IoT and Edge computing networks through cognitive energy harvesting protocol
8.	Ding [13]	Intrusion detection in IoT networks through data augmentation and generative adversarial networks (GAN). Cosine similarity index employed to optimized loss function for fictitious malicious data employed to train network.
9.	Rahmen et al. [14]	Network Intrusion Detection Systems (NIDS) designed for IoT network based on GANs to mitigate the effect of imbalanced datasets as malicious activity is infrequent and sporadic, reducing the dependency on real-world data.
10.	Trigui et al. [15]	Securing wireless networks under different fading conditions with phase noise using reconfigurable intelligent surface (RIS) assisted communications.
11.	Jameel et al. [16]	Securing wireless networks employing channel state information (CSI) though reduction of physical layer outage.
12.	Burton et al. [17]	Securing wireless networks under IIRS jamming attacks of employing channel state information (CSI).

It can be observed from previous work that multiple approaches employing machine learning and deep learning have been explored to secure IoT and Edge computing based pervasive networks. One of the challenges which most NIDS face is the imbalanced datasets through recording the IoTD behaviour. This is due to the fact that malicious activity often occurs sporadically and is much more infrequent compared to non-malicious activity. In such cases GANs have been promising, although accuracy in such cases dips due to training models with non-actual data. Additionally, deep learning model such as LSTM have shown promising results in case the IoTD data has been recorded for a significant amount of samples to aid pattern recognition of stochastic features. This is a more practical approach, which however may incur computational overhead. Thus, an optimization for a deep learning model is critical to strike a balance between computational complexity and system performance. This analysis serves as the underpinning for the proposed model, discussed next.

2. THHE IOT SECURITY MODEL

The networks security model to be designed for IoT security needs to cater to the needs of the system at three levels [18]:

1) End User

2) IoTDs

3) Cloud/Fog Server

The IoT security model is depicted in figure 2.

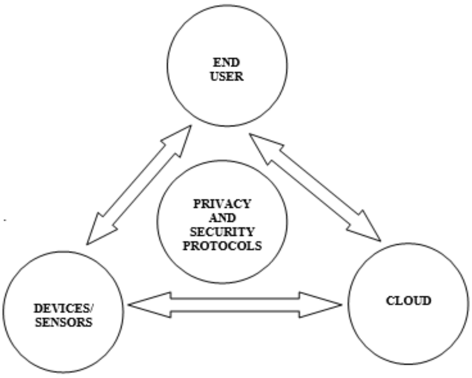


Fig.2 The IoT Security Model

The security mechanism depicted in figure 2 illustrates the various levels at which the IoT security mechanism needs to work. While end users may be catered to with application level security, the devices and cloud connection needs to be secured through network level or physical level security [19].

Figure 3 depicts the authentication mechanism for an IoT network at the gateway. One of the major challenges which such a gateway encounters in deciding how to authenticate a large number of IoT devices with the least amount of overhead and latency. This is challenging keeping in mind the enormity of the data being collected at the gateway [20].

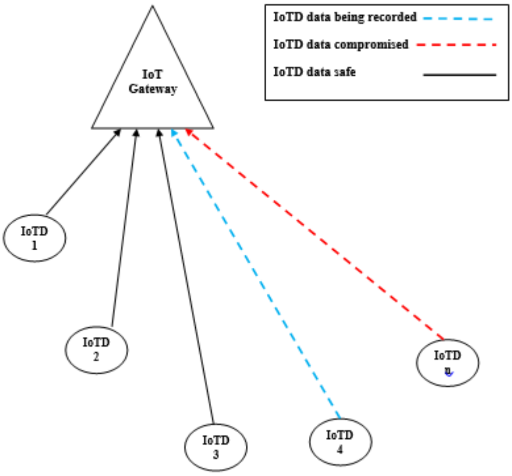


Fig.3 System Authentication Model

The proposed system authentication model is depicted in figure 3.

3. PROPOSED METHODOLOGY

The methodology developed in this paper aims at authenticating the IoT devices based on its stochastic features which would be different in cases of attack or non-attack. Figure 4 depicts such a scenario [21].

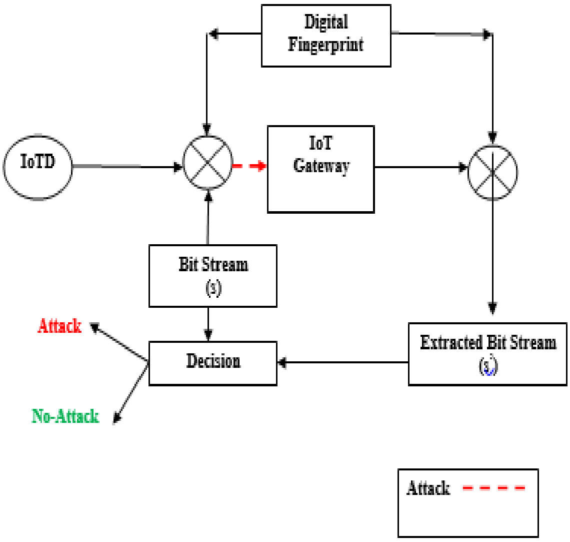


Fig.4 Security Framework for Massive IoT Systems

The mathematical formulation for such an authentication scenario is presented next:

Let there be ‘N’ IoTDs which are connected to the gateway ‘G’.

Let an IOTD_i generate a bit stream y_i at a given time ‘t’ with a sampling frequency f_i.

This data stream then reaches the gateway ‘G’ which estimating the status of the IOTDs and controlling them.

The attacker typically records the samples of the IOTDs and tries to manipulate the data to generate a stream y_i'

The responsibility of the gateway ‘G’ is to compare both y_i and y_i' and take the informed decision based on the comparison. The decision becomes non-trivial with the following constraints [22]:

1) Extremely large number of IOTDs transmitting simultaneously,

2) Changes in stochastic parameters of the bit stream while travelling from the IOTD to the gateway due to channel effects.

3) Resemblance of y_i and y_i'.

4) Constraints of computational power and latency.

Let the embedded (watermarked) IOTD data stream be given by:

$$w_i(t) = y_i(t) + \beta_i bp_i(t) \forall t = 1 \dots . n_i$$

Here,

$w_i(t)$ is the embedded data stream

p_i is a pseudo-noise or pseudo-noise sequence taking values of +1 or -1 for IOTDi

$\beta_i = \frac{\text{Power (PN Data Stream)}}{\text{Power (Original Data Stream)}}$

b takes values in the range $[-1, +1]$

n_i denotes the bits in the sequence

The role of the gateway/hub is to estimate:

$\widehat{b_\imath} = \frac{\langle w_i, p_i \rangle n_i}{\beta_i n_i}$

$\widehat{b_\imath} = \frac{\langle y_i, p_i \rangle n_i}{\beta_i n_i} + \frac{\beta_i b_i \langle p_i, p_i \rangle n_i}{\beta_i n_i}$

Above expressions can be simplified to obtain:

$\boldsymbol{\widehat{b_\imath} = \widehat{y_\imath} + b_i}$

Two conditions can exist on evaluation of $\boldsymbol{\widehat{b_\imath}}$, which are:

{

If $(\boldsymbol{\widehat{b_\imath} > 0})$

Extracted bit = 1

elseif $(\boldsymbol{\widehat{b_\imath} < 0})$

Extracted bit = - 1

}

Here,

$\boldsymbol{\langle w_i, p_i \rangle n_i}$ denotes the inner product of $\boldsymbol{n_i}$ samples (time metric) of $\boldsymbol{w_i \text{ and } p_i}$

$\boldsymbol{p_i(t) \text{ and } y_i(t)}$ denote the variables (stochastic) which care recorded at the gateway as a function of time ‘t’.

The stochastic parameters should be chosen such that the computation doesn’t include large overheads. Hence the parameters to be extracted from $\boldsymbol{y_i(t)}$ are [23]:

$\boldsymbol{mean\ \{y_i(t)\} = \mu_i}$

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

$\boldsymbol{standard\ deviation\ \{y_i(t)\} = \sigma_i}$

$\boldsymbol{Energy}\ \{\boldsymbol{y_i}(t)\} = E_i$

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

In this case, let the time dependent recorded variable at the receiving end be $\widehat{y_\imath(t)}$ while the one transmitted be $y_i(t)$.

In case the variability among $\widehat{y_1(t)}$ and $y_i(t)$ is high, the machine learning model picks up the changes and triggers an alarm indicating a potential attack. In order to train such a network, an apt model which can analyse large time series data needs to be employed. This ideally suits a long short term memory (LSTM) based neural network depicted in figure 5.

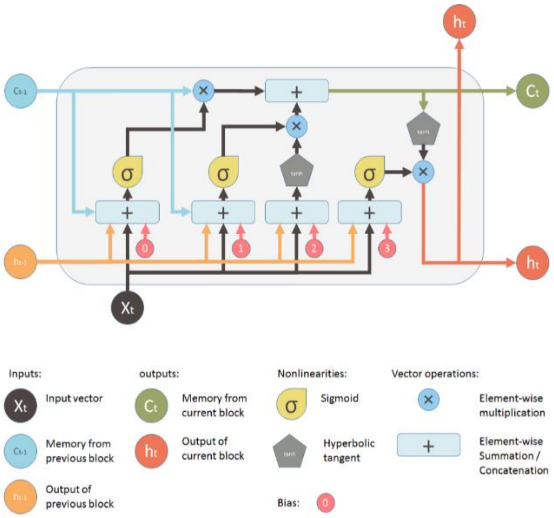


Fig.5 The structure of LSTM

The major benefit of using an LSTM model is the fact that it has a forget gate apart from the input and output gates [24]. The forget gate allows the older data to be stored in the long term memory while considering the latest data samples to be stored in the short term memory. Thus pattern recognition becomes more effective in case adversarial patterns change over time [25].

To create imperceptibility in data transmission of the network (to evade potential attacks), a frequency happening based approach can be adopted. In this approach, a pseudo random (PN) generator is proposed to spread out the data transmission bandwidth to masquerade the transmission process. Applying the spreading process in the present context is mathematically explained as [26]:

Assume two frequencies to be used for jamming.

$$\mathrm{Jm1} = e^{j\pi 12(\mathrm{rand\_int}(\mathrm{Lj.m,1})}$$

$$\mathrm{Jm0} = e^{j\pi 10(\mathrm{rand\_int}(\mathrm{Lj.m,1})}$$

Subsequent to frequency hopping, the obtained signal can be formulated as:

$$Y'(t) = g(\mathrm{ser\ data}, \mathrm{Jm1}, \mathrm{Jm0})$$

Here,

Jm1, Jm0 depict the spreading frequencies;

L_j denotes the PN sequence used for jamming;

n denotes the number of bits used for the present simulation;

rand_int denotes the random numbers generated.

Considering AWGN conditions in the channel, the following formulation holds [27]:

$N = K_0/2$

Here,

K denotes the strength of the Power Spectral Density (PSD)

N_0 represents value of PSD.

Thus hopping the transmission frequencies allows for quick change in transmission bandwidth and renders imperceptibility to adversaries [28].

4. SIMULATION RESULTS

The simulation has been carried out for 10 million bits with binary transmission over fading channels.

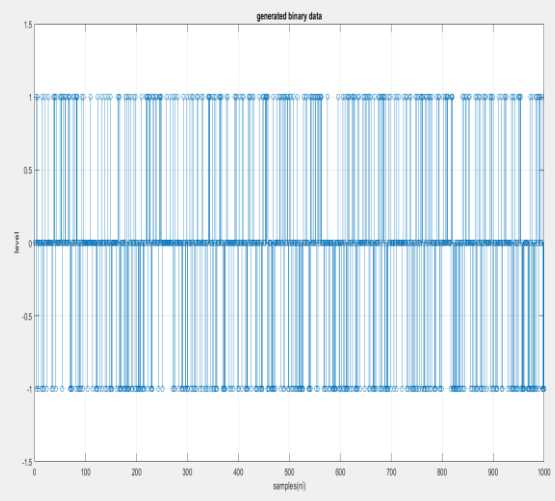


Fig. 6 Binary data transmitted by IoTDs

Fig.6 depicts the serial binary data stream generated by the IOTDs. It can be seen that two polarities correspond to the logic levels 0 and 1 respectively.

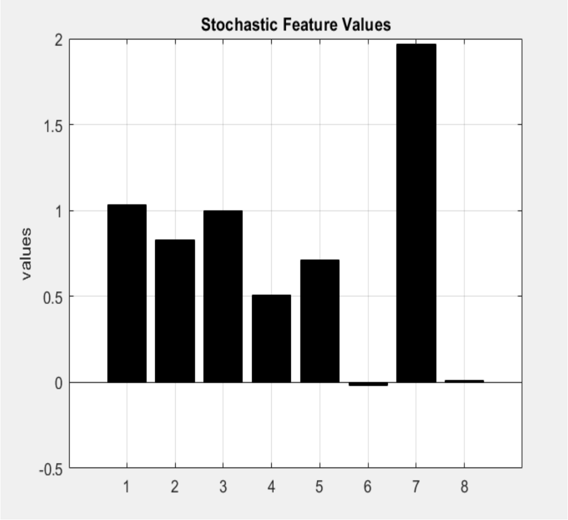


Fig.7 Stochastic Feature Vales of data stream

Figure 7 depicts the stochastic feature which serve as the digital fingerprints of the data stream.

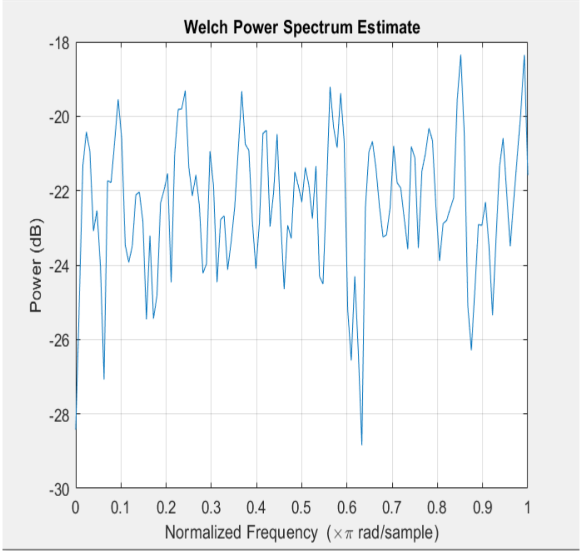


Fig.8 PSD of data stream

Figure 8 depicts the normalized power spectral density (PSD) of the data steam rendering information regarding the different frequency components of the data stream. It can be seen that the data stream depicts an almost random psd corresponding to random generated data.

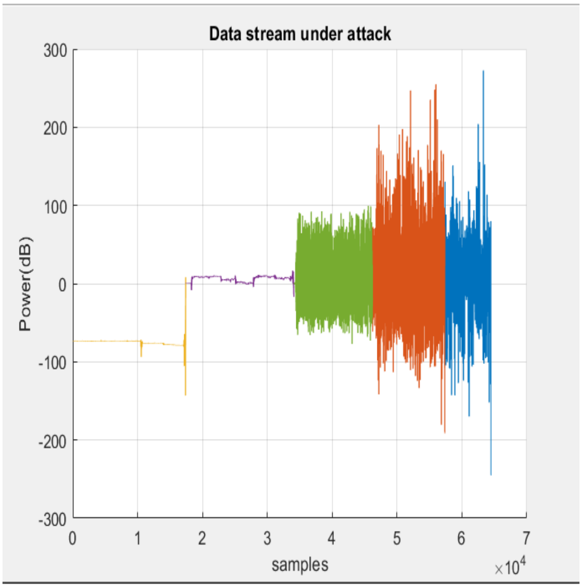
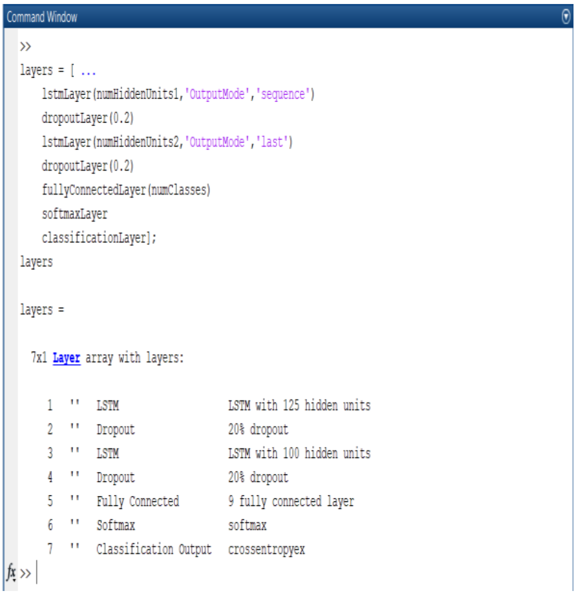


Fig. 9 Data Stream Under Attack

It can be observed from figure 9 that the power spectrum varies significantly in case of the attacks. The magnitude of attacks has been increased gradually after intervals of time (sample numbers). The beginning of the attack has been demarcated. The LSTM is further trained with the data, features and key (PN sequence values) for detection of attack.



```
>>
layers = [ ...
    lstmLayer(numHiddenUnits1,'OutputMode','sequence')
    dropoutLayer(0.2)
    lstmLayer(numHiddenUnits2,'OutputMode','last')
    dropoutLayer(0.2)
    fullyConnectedLayer(numClasses)
    softmaxLayer
    classificationLayer];
layers

layers =

  7x1 Layer array with layers:

     1   ''   LSTM                    LSTM with 125 hidden units
     2   ''   Dropout                 20% dropout
     3   ''   LSTM                    LSTM with 100 hidden units
     4   ''   Dropout                 20% dropout
     5   ''   Fully Connected         9 fully connected layer
     6   ''   Softmax                 softmax
     7   ''   Classification Output   crossentropyex
fx >>
```

Fig.10 LSTM Parameters

Figure 10 depicts the LSTM parameters for the experiment with the hidden units, drop out, fully connected and softmax layers' details being depicted. The system is designed with 125 hidden units.

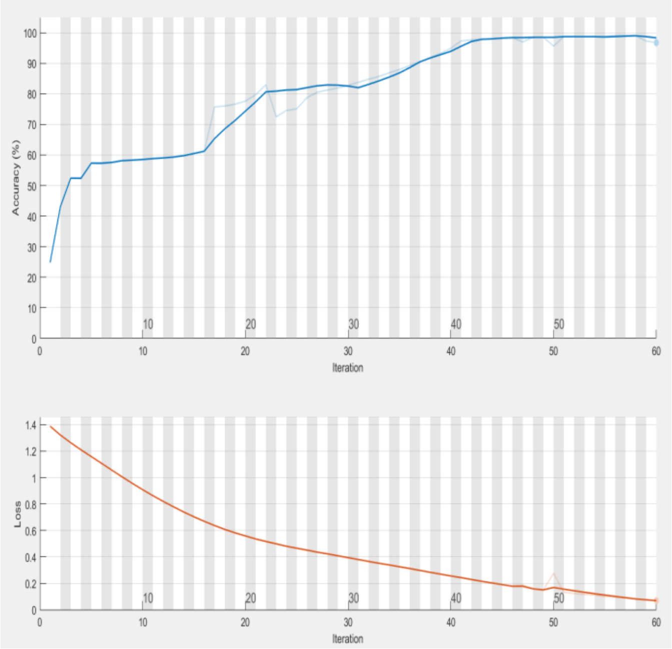


Fig. 11 Accuracy and Loss Curves of LSTM model

It can be observed from figure 11 that the loss of the LSTM network keeps decreasing as the number of iterations of the LSTM network increases. The accuracy of classification of the system is 96%.

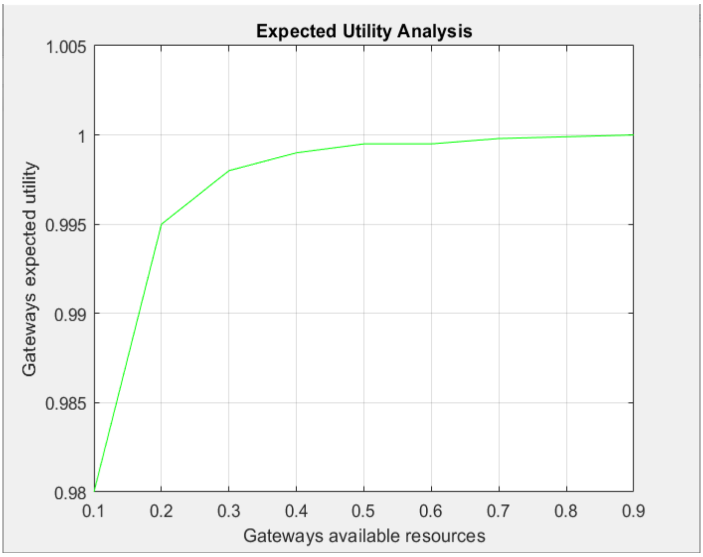


Fig. 12 Utility Analysis of Gateway Under attack

It can be observed from figure 12 that the gateways expected utility monotonically increases with the increase in the gateways resources. The resources also affect the computational time and latency of the system.

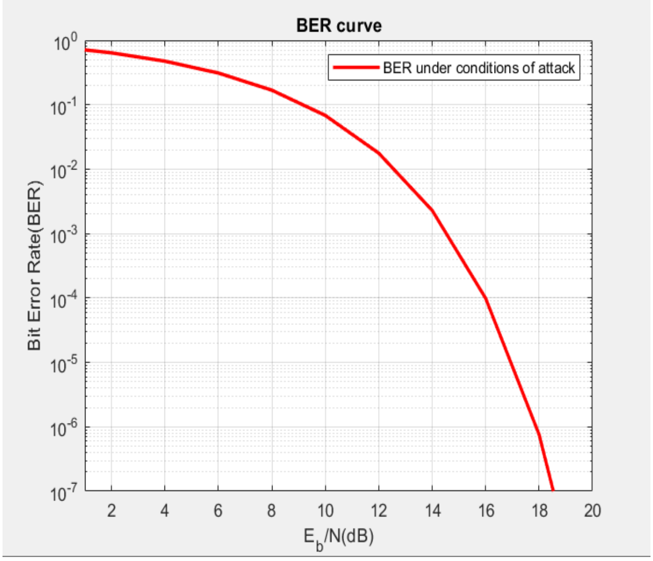


Fig. 13 BER performance of system

The figure 13 depicts the BER performance of the proposed system. It can be seen that the performance of the system improves with increasing the signal strength as compared to noise effects. Due to discrete data samples, the signal strength is denoted as energy per bit or $E_{b.}$

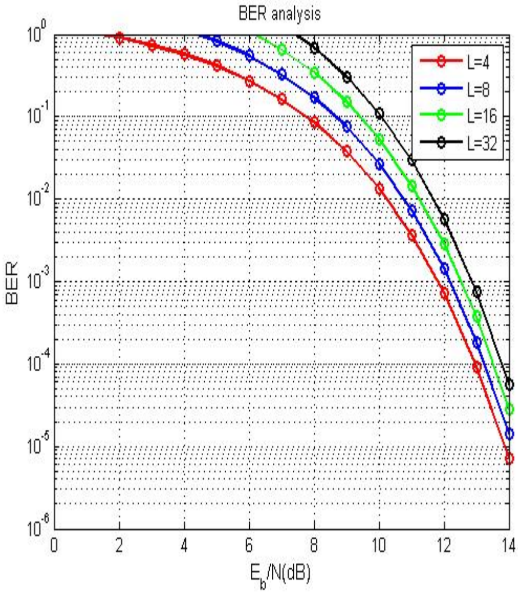


Fig.14 Error Rate Performance w.r.t. length of PN code factor

Figure 14 depicts the variation in the error rate as function of both SNR and the spreading factor ‘L’. It can be clearly observed that the increase in the spreading factor results in an upward shift in the error rate indicating higher chances of bit errors. This can be seen as a trade-off between security and the quality of service of the network.

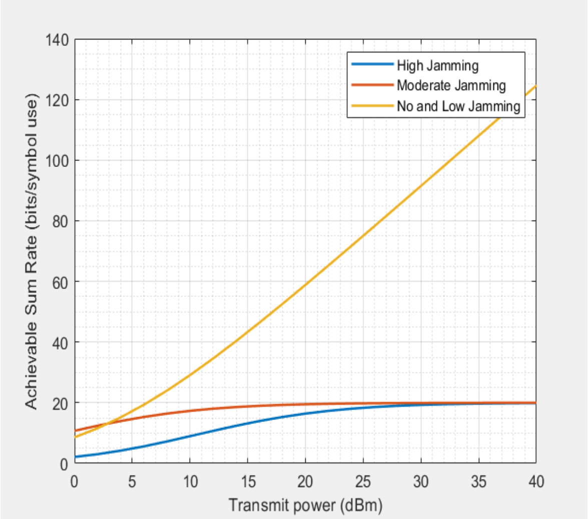


Fig.15 Sum Secrecy Rate

Figure 15 depicts the sum secrecy rate of the proposed system

The error performance and sum secrecy can be compared to existing contemporary research methodologies in the domain based on the error rate and the sum secrecy rate.

Table 2 Comparison with Exiting Work

Authors	Approach	Metric	Value
Trigui et al. [16]	RIS assisted communication	Error Outage	10^{-4}
Jameel et al. [17]	Physical layer security using CSI	BER	10^{-4}
Burton et al. [18]	Security against IIRS jammer using CSI	Sum Secrecy Rate	70 bits/symbol use
Proposed Approach	Deep Learning Based Channel Estimation and Data Authenticating	BER Sum Secrecy	BER of $10^{-6} - 10^{-7}$ Sum Secrecy Rate of 120 bits/symbol use

The appraoch presented in this paper incorporates both deep learning and stochastic feature extraction from the random data stream of IoTDs. While a two way appraoch may incur increased overhead, it can be observeed that the proposed appraoch attains extremely low error rates and outages in the range of 10^(-6)-10^(-7). The trained deep learing model attains an error detection accuracy of 96% while the sum secrecy rate is 120 bits/symbol use, which can be further translated to Bit/s/Hz for the available network bandwdth. A comparative analysis with existing work clearly indicates improved performance both in terms of error detection as well as sum serecy rate with respect to contemporary appraoches.

5. Conclusion:

It can be concluded from the previous discussions that IoT and large scale of the automated processes in the industries makes IoT a leveraging solution quite conspicuously. Protecting IoT networks is challenging due to the largeness of the data and hardware complexity. The proposed technique designs a dynamic watermarking technique and LSTM to detect attacks on IoT networks. Additionally a frequency hopping technique to spread out the transmission bandwidth of the network has also been proposed to ensure a double layer of security to the network. The LSTM model is shown to achieve an accuracy of 96% at convergence with a BER of 10^(-7). Additionally the BER under FFH spreading also reaches 10^(-6)-10^(-7). The sum secrecy rate attains a normalized values of 120 bits/symbol use. Thus, it can be concluded that the proposed approach is capable of both accurately authenticating devices on a large network along with attaining significantly low error rates while hopping transmission bandwidth to evade adversarial attacks.

References

1. S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," in IEEE Access, vol. 8, pp. 188082-188134, 2020.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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
7. 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
8. 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.
9. M Nanjappan, K Pradeep, G Natesan, A Samydurai, “DeepLG SecNet: utilizing deep LSTM and GRU with secure network for enhanced intrusion detection in IoT environments” Cluster Computing, Springer 2024.
10. L. Hu et al., "Cooperative Jamming for Physical Layer Security Enhancement in Internet of

Things," in IEEE Internet of Things Journal, 2018, vol. 5, no. 1, pp. 219-228.

11. H. Moudoud and S. Cherkaoui, "Empowering Security and Trust in 5G and Beyond: A Deep Reinforcement Learning Approach," in IEEE Open Journal of the Communications Society, 2023, vol. 4, pp. 2410-2420.
12. R. Lin, H. Qiu, J. Wang, Z. Zhang, L. Wu and F. Shu, "Physical-Layer Security Enhancement in Energy-Harvesting-Based Cognitive Internet of Things: A GAN-Powered Deep Reinforcement Learning Approach," in IEEE Internet of Things Journal, 2024, vol. 11, no. 3, pp. 4899-4913.
13. H. Ding, Y. Sun, N. Huang, Z. Shen and X. Cui, "TMG-GAN: Generative Adversarial Networks-Based Imbalanced Learning for Network Intrusion Detection," in IEEE Transactions on Information Forensics and Security, 2024, vol. 19, pp. 1156-1167
14. S Rahman, S Pal, S Mittal, T Chawla, C Karmakar, “SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security”, Internet of Things, Elsevier 2024, vol 26, 101212.
15. I. Trigui, W. Ajib, W. -P. Zhu and M. D. Renzo, "Performance Evaluation and Diversity Analysis of RIS-Assisted Communications Over Generalized Fading Channels in the Presence of Phase Noise," in IEEE Open Journal of the Communications Society, vol. 3, pp. 593-607, 2022,.
16. F. Jameel, S. Wyne and I. Krikidis, "Secrecy Outage for Wireless Sensor Networks," in IEEE Communications Letters, vol. 21, no. 7, pp. 1565-1568
17. T Burton, K Rasmussen, “Private data exfiltration from cyber-physical systems using channel state information” ACM SIGSAC Conference on Computer and Communications Security, ACM 2021, PP.223-235.
18. F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in IEEE Communications Surveys & Tutorials, 2020, vol. 22, no. 3, pp. 1686-1721.
19. M. Bagaa, T. Taleb, J. B. Bernabe and A. Skarmeta, "A Machine Learning Security Framework for IoT Systems," in IEEE Access, vol. 8, pp. 114066-114077, 2020.
20. M Kokila, S Reddy, “Authentication, Access Control and Scalability models in Internet of Things Security-A Review”. Cyber Security and Applications, Elsevier 2024, vol.3, 10005.7
21. Aidin Ferdowsi and Walid Saad, “Deep Learning for Signal Authentication and Security in Massive Internet of Things Systems”, IEEE Transactions on Communications,2010, vol. 67, no. 2, pp. 1371-1387.
22. Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," in IEEE Access, vol. 9, pp. 161546-161554, 2021
23. V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha and G. Srivastava, "Federated-Learning-Based Anomaly Detection for IoT Security Attacks," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545-2554, 15 Feb.15, 2022
24. G Qiao, T Ma, S Liu, M Bilal, “A frequency hopping pattern inspired bionic underwater acoustic communication”, Physical Communication, Elsevier 2021, vol.46, 101288.
25. Y. Li, Y. Zuo, H. Song and Z. Lv, "Deep Learning in Security of Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22133-22146, 15 Nov.15, 2022.
26. A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021.
27. R. Krishna Vanakamamidi, L. Ramalingam, N. Abirami, S. Priyanka, C. S. Kumar and S. Murugan, "IoT Security Based on Machine Learning," 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon), Singapore, Singapore, 2023, pp. 683-687
28. F. Zhu, C. Zhang, Z. Zheng and A. Farouk, "Practical Network Coding Technologies and Softwarization in Wireless Networks," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5211-5218, 1 April1, 2021.