Machine Learning for Intrusion Detection for Massive IoT Networks

Pritibala Mali[1], Prof. Pankaj Raghuwanshi[2]

Abstract: Wide area networks such as fog and internet of things often encounter network level security. There would exist 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 appropriate choice of stochastic parameters and authentication scheme should be adopted. In this proposed work, an acceleration learning based LSTM network has been proposed to detect attacks in IoT networks. It can be observed from the obtained results that the proposed system attains better performance compared to previously existing system. The performance enhancement can be attributed to additional features computed and the LSTM with acceleration used to train and further detect errors.

Keywords: Internet of Things (IoT), Network Level Security, Neural Networks, Deep Learning, Accuracy, Gateway Utility.

I. INTRODUCTION

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network.

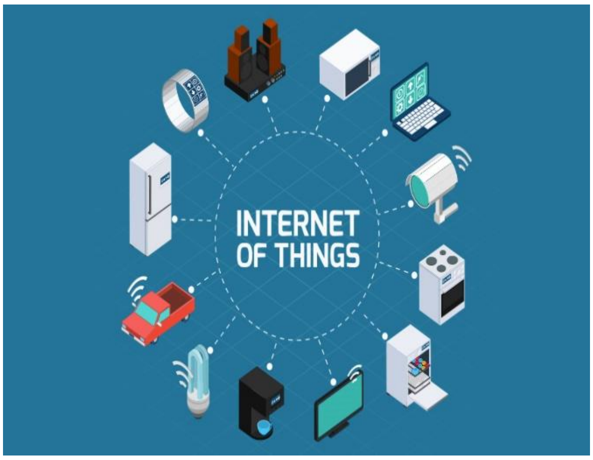


Fig. 1 Conceptual Framework for IoT

In There are 3 primary security paradigms in IoT networks:

1) Application Layer Security
2) Network Layer Security
3) Physical Later Security

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business. Protecting IoT objects necessitates a general security framework - which is a challenging task indeed - covering all IoT assets and their corresponding possible attacks in more details. Therefore, it is absolutely essential to identify all attacks against security or privacy of IoT assets, which is the first step towards developing such framework. Having said that, IoT ecosystem, without doubt, is very complex and confusing, especially when it comes to precisely defining its main assets. Literature, however, has shown several IoT threat models based on IoT assets, none of which has introduced a comprehensive IoT attack model along with compromised security goals for such a highly intricate system. 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. All kinds of traffic that comes to and goes from the network is sensed for any sort of malicious activity or intrusion.

II. THHE IOT SECURITY MODEL

Network and cyber security techniques and methodologies have been developed and utilized for some time. Not only are IoT systems vulnerable to most if not all of the existing manner of threats, but also that they pose new security concerns due to several factors. Here, we briefly summarize three main challenges for IoT systems: Limited Device Capability: IoT devices and systems have entered areas that have traditionally been the domain of physical control devices. Such devices are often required to be simple and efficient for dedicated functionalities.

As a result, they are designed/equipped/deployed with limited computing and networking capability. Converting these to IoT systems requires significant thought, planning and design, but the rush to market can short circuit this process and imposes severe security risks to the systems.

• Gigantic Scale and Volume: The sheer scale of IoT deployments creates very tempting attack targets for cyber criminals. Discovering and exploiting vulnerability can quickly create a massive army of attackers with which to perpetrate further attacks.

• Vulnerable Environments: IoT devices tend to be placed in unprotected environments easier for attacks to access, comparing to firewall-protected networks. Perhaps most concerning is that low-cost devices are less likely to be patched and maintained in the same manner as traditional physical devices might be, creating an economic disincentive to maintain the software that operates IoT devices.

In light of these concerns, considerable thought and effort has been expended to better understand and define the challenges posed by this emerging paradigm, with the hopes that these efforts will result in a more standardized way of considering and addressing the issues that are presented by IoT. The IoT security model is depicted in figure 2.

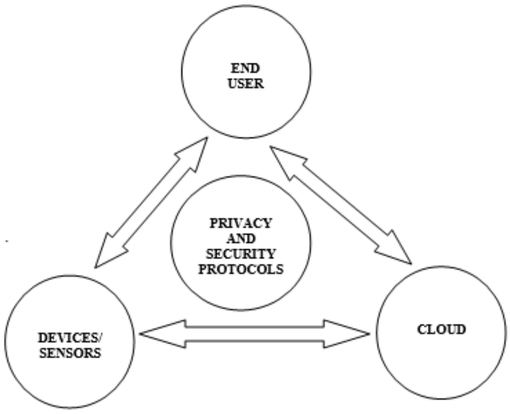


Fig.2 The IoT Security Model

This laudable goal may prove to be challenging given the wide variety of IoT-enabled devices and systems that continue to proliferate rapidly. This challenge is exacerbated by our increased reliance upon these IoT systems and the threats posed by the aforementioned factors. Given this, it is clear that security deployment for IoT must be given careful consideration**.**

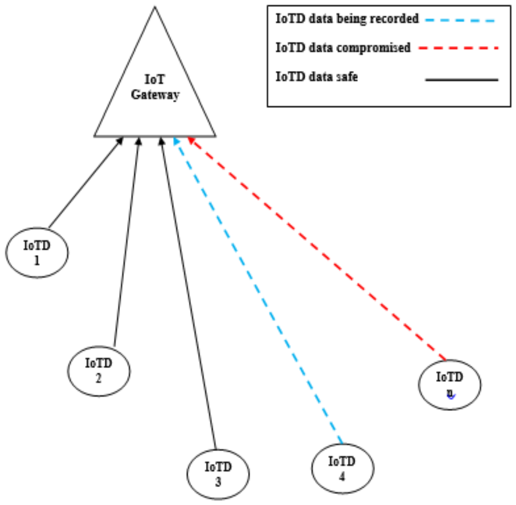


Fig.3 System Authentication Model

The basic challenges in front of the IoT gateway are:

1) Which of the IoTDs can be authenticated among all the IoTDs.

2) How to authenticate the IoTDs selected with least overhead and minimum bit error rate (BER)

Typically, some digital fingerprint in terms of the features of the data stream to be transmitted is embedded onto the individual IoTDs data, but it can be extracted in case the attack analyses the data stream and records it for a long period with sufficient number of samples to extract the possibly used stochastic features of the data stream generated by the IoTD.

Moreover, large length stochastic features would inevitably and invariably increase the system computation overhead and latency at the gateway. While lesser overhead can be settled for, but that would result in higher bit errors. Thus there would exist a continued tradeoff between the error rate (authentication metric), system overhead, computational complexity and latency of the system. Hence an extremely meticulous system design with appropriate choice of stochastic parameters and authentication scheme should be adopted.

III. PROPOSED METHODOLOGY

As discussed earlier, the main challenge faced by the IoT gateway is the decision regarding the authentication of IoTDs and the elated computational complexity. 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:

1) Non-compromise on security

2) Compromised security.

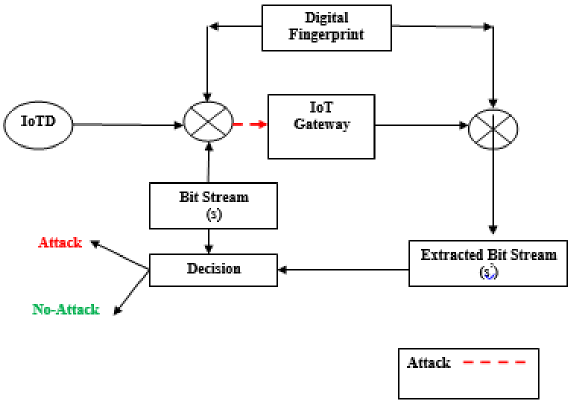


Fig.4 (a) Security Framework for Massive IoT Systems

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:

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:

$$\boldsymbol{w_i(t) = y_i(t) + \beta_i b p_i(t) \forall t = 1 \ldots . n_i}$$

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

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

b is the hidden bit stream in the embedded bit stream which can take values of +1 or -1

n_i is the number of samples or frame length of the original bit stream used to hide a single bit.
The IOT Gateway correlates the embedded bit from IOTDi and the PN Sequence to extract the watermarked bit. Mathematically, the gateway computes:

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

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

Above expressions can be simplified to obtain:

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

Two conditions can exist on evaluation of $\boldsymbol{\widehat{b_\iota}}$**,** which are:
{
If ($\widehat{b_\iota} > 0$)
Extracted bit = 1
elseif ($\widehat{b_\iota} < 0$)
Extracted bit = - 1
}
Here,
$\langle w_i, p_i\rangle n_i$ denotes the inner product of n_i samples (time metric) of w_i *and* p_i
$p_i(t)$ *and* $y_i(t)$ represent independent stochastic variables at time 't'
The stochastic parameters of $y_i(t)$ are given by:

$$\boldsymbol{mean\,\{y_i(t)\} = \mu_i}$$
$$\boldsymbol{variance\,\{y_i(t)\} = \sigma_i^2}$$
$$\boldsymbol{standard\ deviation\,\{y_i(t)\} = \sigma_i}$$
$$\boldsymbol{Energy\,\{y_i(t)\} = E_i}$$
$$\boldsymbol{Entropy\,\{y_i(t)\} = En_i}$$

In case, based on the computation of the stochastic parameters listed above, the gateway computes the received bit stream to be $\widehat{y_\iota(t)}$ in place of $y_i(t)$, it will trigger an alarm indicating a possible attack. The LSTM is designed for detection of the attack. The LSTM primarily has 3 gates:
1) Input gate: This gate collects the presents inputs and also considers the past outputs as the inputs.
2) Output gate: This gate combines all cell states and produces the output.
3) Forget gate: This is an extremely important feature of the LSTM which received a cell state value governing the amount of data to be remembered and forgotten.

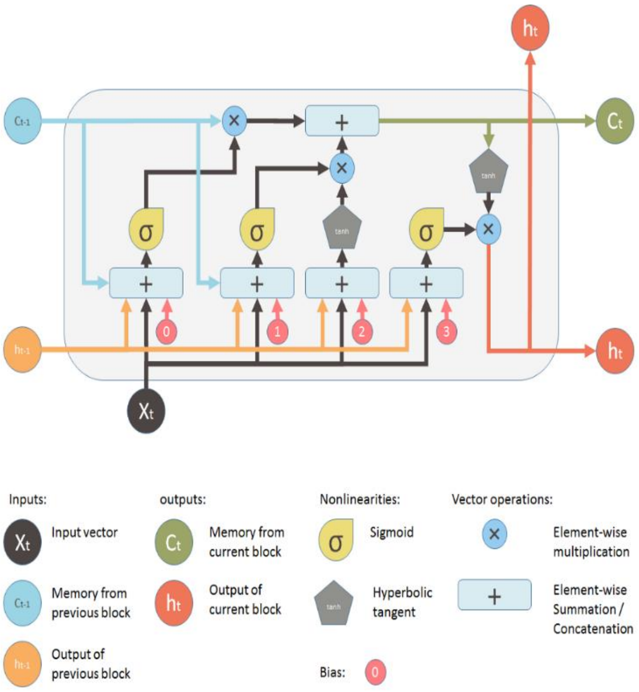


Fig.4 (b) The structure of LSTM

IV. SIMULATION RESULTS

The simulations have been run on Matlab.

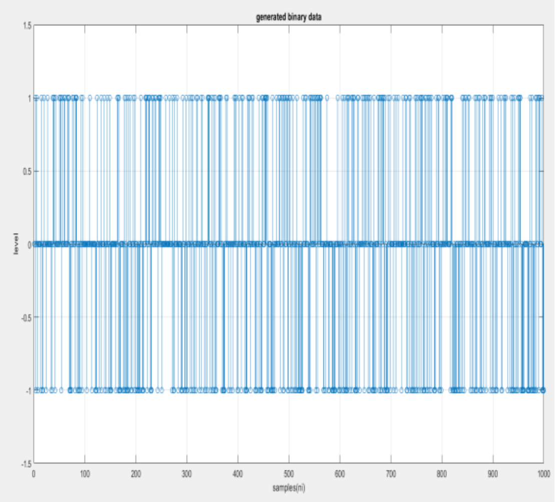


Fig. 5 Binary data transmitted by IoTDs

Fig.5 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.

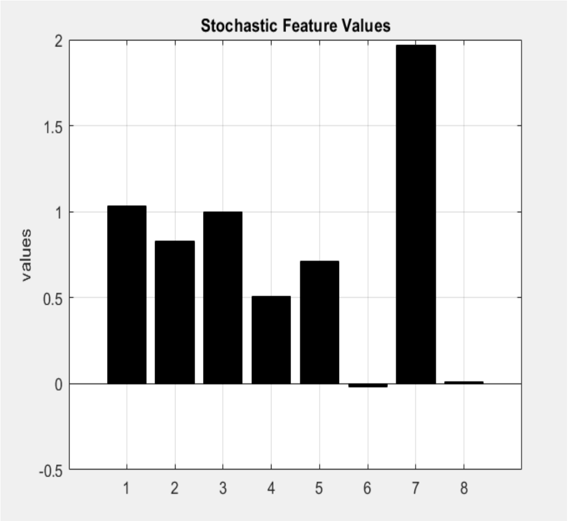


Fig. 6 Stochastic Feature Vales of data stream

Figure 6 depicts the stochastic feature values of the data stream which are:
Energy, Entropy, Correlation, Variance, Standard Deviation, Kurtosis, Skewness, Mean.
These feature comprise the digital fingerprint of the data stream.

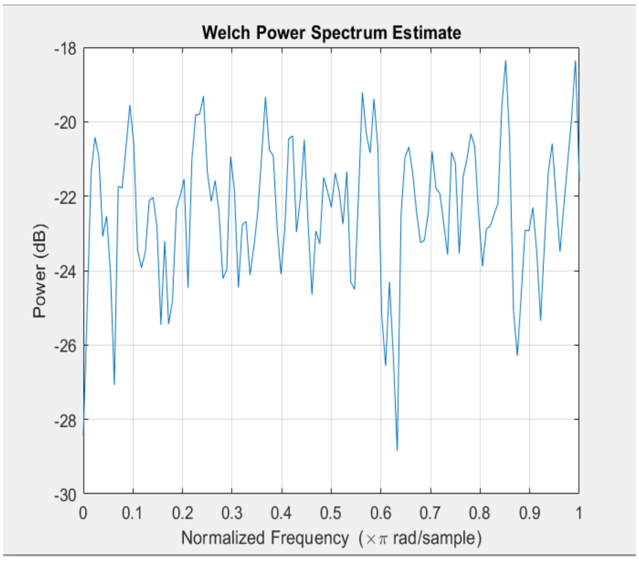


Fig. 7 PSD of data stream

Figure 7 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.

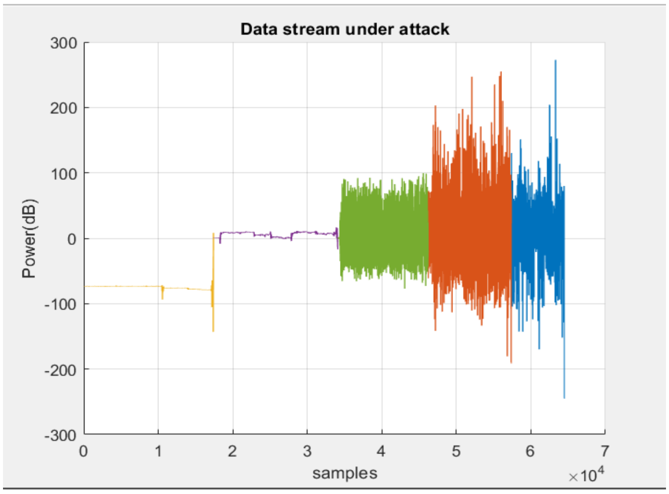
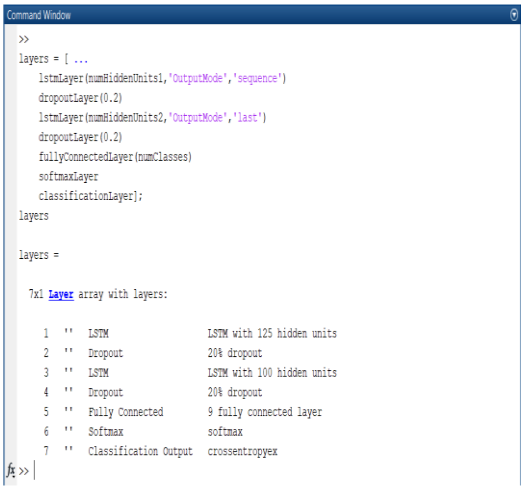


Fig. 8 Data Stream Under Attack

It can be observed 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.9 LSTM Parameters

Figure 9 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.

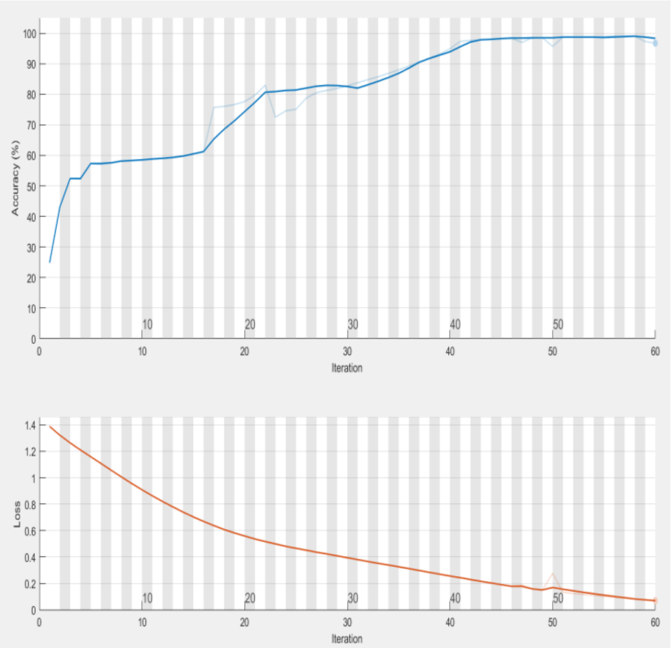


Fig. 10 Accuracy and Loss Curves of LSTM model

It can be observed from figure 10 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%.

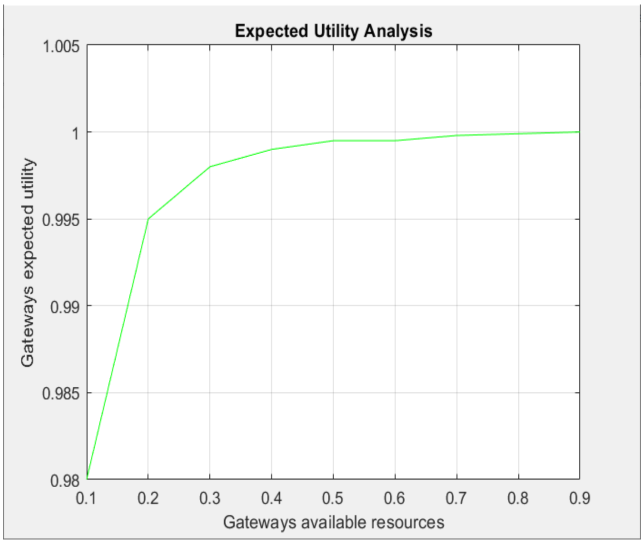


Fig. 11 Utility Analysis of Gateway Under attack

It can be observed from figure 11 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.

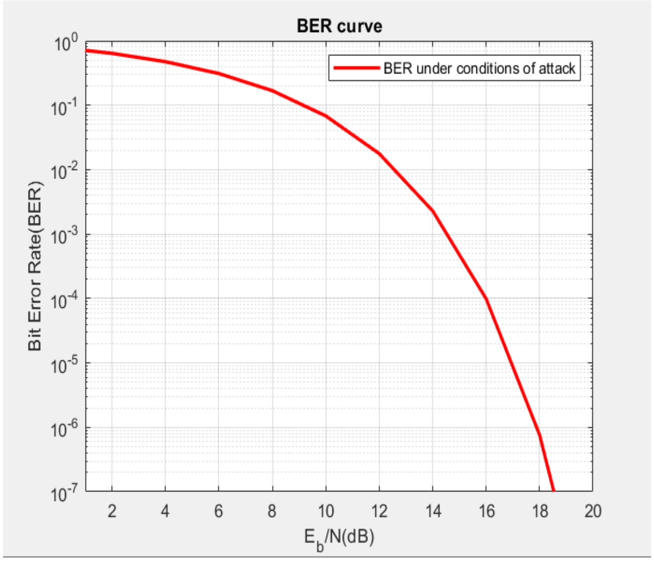


Fig. 12 BER performance of system

The figure 12 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 Eb

Conclusion: It can be concluded from the previous discussions that increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business. 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. It can be observed that the proposed system attains better performance compared to previously existing system. The performance enhancement can be attributed to additional features computed and the LSTM with acceleration used to train and further detect errors.

References

[1] Aidin Ferdowsi and Walid Saad, “Deep Learning for Signal Authentication and
Security in Massive Internet of Things Systems”, IEEE 2021

[2] Francesco Restuccia, Member, IEEE, Salvatore D’Oro, Member, IEEE, and Tommaso Melodia, Fellow, IEEE., “Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking”, IEEE 2020

[3] Liang Xiao∗, Xiaoyue Wan∗ , Xiaozhen Lu∗ ,Yanyong Zhang , Di Wu, “IoT Security Techniques Based on Machine Learning”, IEEE 2019

[4] Marwa Mamdouh; Mohamed A. I. Elrukhsi; Ahmed Khattabi , and Qi Shi, “Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey”, IEEE 2018

[5] Longzhi Yang, Jie Li, Gerhard Fehringer, Phoebe Barraclough, Graham Sexton, “Intrusion Detection System by Fuzzy Interpolation”, IEEE 2017

[6] Reeta Devi , Rakesh Kumar Jha , Akhil Gupta, Sanjeev Jain, Preetam Kumar, “Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network”, ELSEVIER 2017

[7] Sivakami Raja, Saravanan Ramaiah, “An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection”, Springer 2017

[8] Shahram Jamali, Reza Fotohi, “DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system”, SPRINGER 2017

[9] N. Pandeeswari & Ganesh Kumar, “Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN”, SPRINGER 2016

[10] B. M. Aslahi-Shahri,R. Rahmani ,M. Chizari, A. Maralani, M. Eslami, M. J. Golkar, A. Ebrahimi, “A hybrid method consisting of GA and SVM for intrusion detection system”,SPRINGER 2016

[11] Nitin Naik , Ren Diao , Qiang Shen, “Application of dynamic fuzzy rule interpolation for intrusion detection: D-FRI-Snort”, IEEE 2016

[12] Przemysław Kudłacik , Piotr Porwik, Tomasz Wesołowski, “Fuzzy approach for intrusion detection based on user’s commands”, SPRINGER 2016

[13] Nitin Naik, “Fuzzy Inference Based Intrusion Detection System: FI-Snort”, IEEE 2015

[14] Asry Faidhul Ashaari Pinem , Erwin Budi Setiawan, “Implementation of classification and regression Tree (CART) and fuzzy logic algorithm for intrusion detection system”, IEEE 2015

[15] Yogita Danane , Thaksen Parvat, “ntrusion detection system using fuzzy genetic algorithm”, IEEE 2015

[16] Snehal G. Kene , Deepti P. Theng, “A review on intrusion detection techniques for cloud computing and security challenges”, IEEE 2015

[17] Sergei Dotcenko ; Andrei Vladyko ; Ivan Letenko, “A fuzzy logic-based information security management for software-defined networks”, IEEE 2014

[18] Alka Chaudhary ; V.N. Tiwari ; Anil Kumar, “Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks”, IEEE 2014

[19] Alka Chaudhary ; Vivekananda Tiwari; Anil Kumar, “A novel intrusion detection system for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks”, IEEE 2014

[20] Biswajit Panja ; Olugbenga Ogunyanwo ; Priyanka Meharia, “Training of intelligent intrusion detection system using neuro fuzzy”, IEEE 2014

[21] P. Jongsuebsuk , N. Wattanapongsakorn , C. Charnsripinyo, “Real-time intrusion detection with fuzzy genetic algorithm”, IEEE 2013

[22] Ali Feizollah, Shahaboddin Shamshirband, Nor Badrul Anuar, Rosli Salleh, Miss Laiha Mat Kiah, “Anomaly Detection Using Cooperative Fuzzy Logic Controller”, SPRINGER 2013

[23] P.Arun Raj Kumar, S.Selvakumar, “Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems”, ELSEVIER 2013

[24] Sannasi Ganapathy , Kanagasabai Kulothungan, Sannasy Muthuraj kumar, , Muthusamy Vijayalakshmi, Palanichamy Yogesh , Arputharaj Kannan , “Intelligent feature selection and classification techniques for intrusion detection in networks: a survey”, SPRINGER 2013

[25] Monita Wahengbam ; Ningrinla Marchang, “Intrusion Detection in MANET using fuzzy logic”, IEEE 2012

[26] Krasimira Kapitanova, Sang H.Son, Kyoung-Don Kang, “Using fuzzy logic for robust event detection in wireless sensor networks”, Elsevier 2012

[27] Khalid Alsubhi Issam Aib Raouf Boutaba, “ FuzMet: a fuzzy - logic based alert prioritization engine for intrusion detection systems” , Wiley Online Library 2012

[28] K Kapitanova, SH Son, KD Kang, “Using fuzzy logic for robust event detection in wireless sensor networks”, IEEE 2012

[29] O Linda, M Manic, T Vollmer, “Fuzzy logic based anomaly detection for embedded network security cyber sensor”, IEEE 2011

[30] A Chauhan, G Mishra, G Kumar, “Survey on data mining techniques in intrusion detection”, Citeseer 2011