Anurag Khare, 2022, 10:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Machine Learning and ECC Algorithm Based Intrusion Detection and Mitigation

M. Tech. Scholar Anurag Khare, Asst. Prof. Shivraj Singh
Department of Electronics and Communication,
Technocrats Institute of Technology,
Bhopal, India
anuragkhare1982@gmail.com, 86. shivraj@gmail.com

Abstract- Machine learning techniques are being widely used to develop an intrusion detection system (IDS) for detecting and classifying cyber attacks at the network-level and the host-level in a timely and automatic manner. However, many challenges arise since malicious attacks are continually changing and are occurring in very large volumes requiring a scalable solution. There are different malware datasets available publicly for further research by cyber security community. In the proposed approach elliptic curve, the cryptography approach used for more security with fewer key sizes with protocol enhancements to perform an efficient authentication process. The other solutions ML model using back propagation neural contributed in this work to detect the attack or for optimization of network and to reduce the overhead consumption as well as increase the network lifetime. Proposed system provides a secure network using the lightweight authentication protocol to mitigate the effect of the attack in the network environment. The MATLAB software has been used to show simulation performance. This simulation performance compare the system while attack taking and after mitigation.

Keywords- Machine Learning and ECC Algorithm, Intrusion Detection System, ANN.

I. INTRODUCTION

Currently, there are more than 25 billion devices connected to the Internet worldwide, three times as many human beings [1–3]. The Internet of Things (IoT) is based on interconnected smart devices, and different services are used to integrate them into a single network.

This allows the smart devices to gather sensitive information and carry out important functions, and these devices connect and communicate with each other at high speeds and make decisions according to indicator information.

The IoT environment uses cloud services as a backend for processing information and maintaining remote control. Client users use mobile applications or web services to access data and control the devices. The IoT infrastructure uses large numbers of sensors to extract significant information, and this information is analyzed by artificial intelligence algorithms [4, 5]. Intrusion detection systems (IDSs) are the technical, regulatory, and administrative means used to prevent unauthorized use, abuse, and recovery of electronic Information and communication systems and the information they contain, aimed at ensuring

The availability and continuity of the work of the Information systems and enhancing the protection, confidentiality, and privacy of personal data by taking all measures. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security [6–4].

II. MOTIVATION

Security from Wireless Channel Characteristics- The use of wireless channel characteristics to derive

security primitives has gained interest over the last decade. The theory behind these techniques is as follows: consider two communicating parties, Alice and Bob that encounter an intrinsically symmetric wireless channel. Then, if Alice and Bob transmit identical signals, they will receive identical signals, given they use identical transceivers and antennas in [4]–[5].

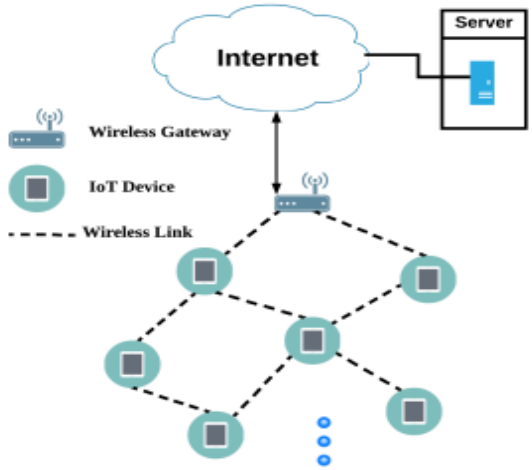

Fig 1. Network model.

Similarly, the authors of quantify the effects of small-scale fading on secret-key agreement in an office space and an anechoic chamber. They propose a technique to generate a secret key only when the wireless channel has high variation. Other works that exploit the entropy of the shared wireless channel state include secure pairing proximity based authentication, intrusion detection and detecting spoofing and Sybil attacks.

Deriving data provenance from wireless channel characteristics has been proposed in [6]. The authors propose the extraction of wireless fingerprints from the received signal strength indicator (RSSI) for body area networks. The proposed technique computes a Pearson correlation coefficient of the wireless fingerprints derived individually at the transmitter and the receiver. However, this technique depends on long wireless fingerprints which increase the communication overhead.

Furthermore, the authors do not present a complete protocol to use with the wireless fingerprints and the proposed protocol does not support privacy preservation. Similarly, in [7], the authors use the same technique as to generate the wireless fingerprints and present a protocol for establishing data provenance in multi-hop IoT networks. However, this technique suffers from a serious key leakage problem. [10]

III. METHODOLOGY

- **Step 1:** Initialize the network with network specifications
- **Step 2:** network nodes location evaluations and coverage area evaluation.
- **Step 3:** Design the Secure network using the lightweight authentication protocol to mitigate the effect of the attack in the network environment.
- **Step 4:** Perform Attack implementation to evaluate network performance.
- **Step 5:** Perform a supervised ML model using back propagation neural to perform the optimization process.
- **Step 6:** Evaluate the performance of the network to achieve enhanced network life and security in the network.

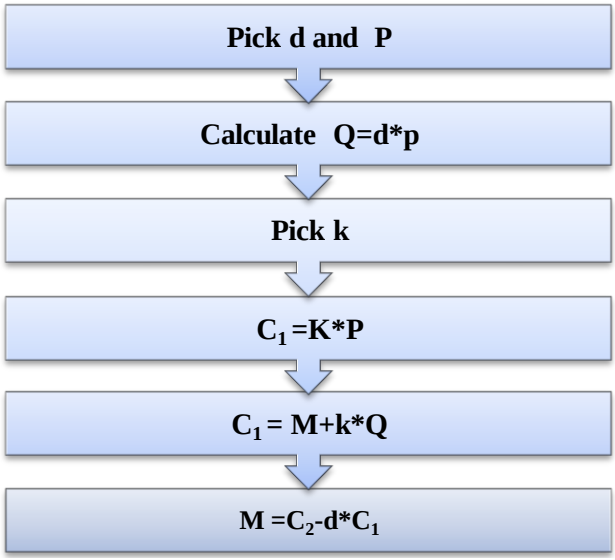

Fig 2. ECC Algorithm Flow.

1. ECC:

A public key encryption technique based on the algebraic structure of elliptic curves over finite fields that can be used to create faster, smaller, and more efficient cryptographic keys .The size of the key of elliptic curves is size of field over which elliptic curve is defined. This is not necessarily exactly the size of the private key. For example, Curve 255 is a 255-bit elliptic curve or 252-bit private keys, though they are usually encoded as 256-bit values with four fixed

bits. Public keys are 256-bit values, but only contain 255 bits of information since the last bit is always 0. High-level description of the algorithm is given below and depicted in Fig 2.

The equation of an elliptic curve:

$$Y^{3=}x^{3+}ax+b$$

2. Key generation:
Using following equation, we can produce public key

$$Q=d*p$$

(12) d – the random number selected within range (1 to n-1); private key.
P – The point on curve;
Q – The public key.

3. Encryption:
Let "m" be message that should be sent. We have to represent this message on the curve. Consider "m" has the point "M" on curve "E". Randomly choose "k" from [1 – (n-1)]. We need to produce two cipher texts (C1 and C2) and send them.

$$C_{1=}K*P$$

We can get the original message using this function:

$$M=C_2-d*C_1$$

IV. IMPLEMENT WORK

The aim of the scheme is to achieve device authentication in the security and attack mitigation as well as energy-consuming as well as having time constraints approaches. In the proposed approach variants of the elliptic curve, the cryptography approach can be implemented to provide more security with fewer key sizes and with protocol enhancements to perform an efficient authentication process.

Also, the other solutions can be contributed to using machine learning models where it can be used to detect the attacks and enabling network security systems to make adjustments in changing environments as per the requirements. The aim of the protocol is to achieve device authentication and secure key establishment with the common key to be used in the next stage of communication between the devices.

Besides, there are other security goals to be achieved such as the resistance against the perception layer attacks such as impersonation attack, replay attacks while preserving the integrity, availability. The proposed protocols can likely be deployed in the below scenario of wireless and cloud body area network. Fig 3 shows a proposed Deployment Scenario.

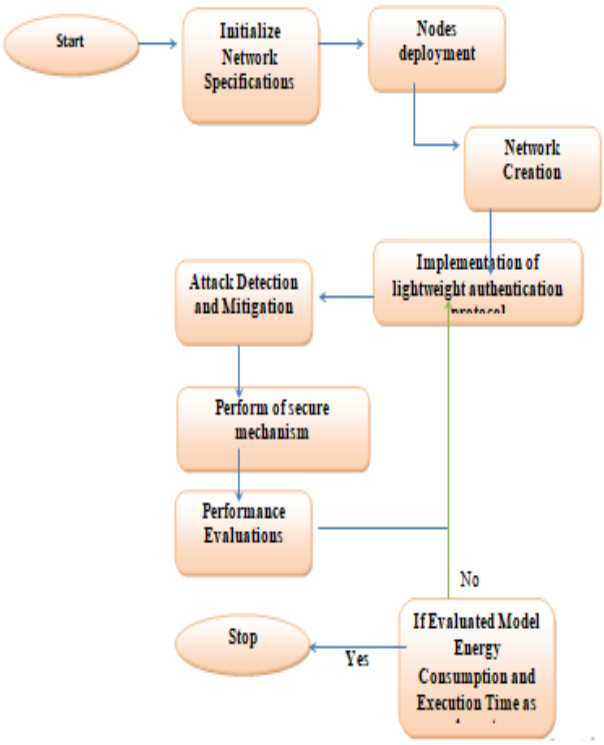

Fig 3. Proposed Flow Diagram.

Authenticated before they send any medication information to the patients. Our assumed device in the proposed protocol can be the patient's device or staff device and the gateway in our protocol is the server shown the Fig 1. After the authentication is performed, using the session key both the entities can exchange valid information with each other with less energy in computation and proposed protocols are supposed to be lightweight.

V. SIMULATION RESULT

A 30-node based network, in the total network used as administrator which monitors the malicious activities over the network. The simulation has been done with MATLAB software. In this thesis discuss about the Device Authentication using Symmetric Key Negotiation with ECC encryption and machine learning based techniques apply for the detection

International Journal of Science, Engineering and Technology

An Open Access Journal

and the protection from malicious activities .Regardless of all decent applications of WSN its most vulnerable to intruder attacks such as Man in Middle attack (MITM) In case of MITM attack an uninvited third party penetrates the conversation as a legitimate user.

The intruder or attacker acts like proxy user and manipulates the data as his/her needs. In the past literature the MITM is abbreviated in various ways such as MIM, MitM or MIM etc, MITM attack MITM is a type of eavesdropping attack where the attackers secretly listen the conversation between two legitimate users.

At the of need, the attacker pretends as a legitimate user and hack the data or information for manipulation. Normally, during MITM attack, conversations or transfer of information. Without proper security, both of legitimate users will never come to know about the authenticity of data .

This paper primarily focuses on MITM intrusion detection system (MITM-IDS) based on neural network learning. The whole process tries to develop an attack-tolerant MITM-IDS that ensures attack free communications with detection of malicious node.

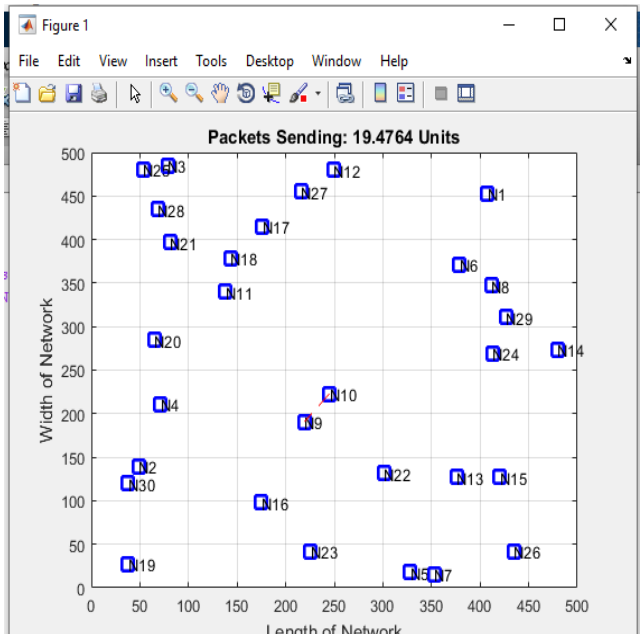

Fig 4. Initialization network.

The data from the common node is sent to the source routing node in the region to perform the path request, and the source routing node encapsulates the selected path information into the source routing header of the packet. Moreover, in the process of data transmission, the intermediate nodes along the path perform relay forwarding according to the source routing path information in the packet header without any communication to the source routing node, which can reduce the system energy consumption.

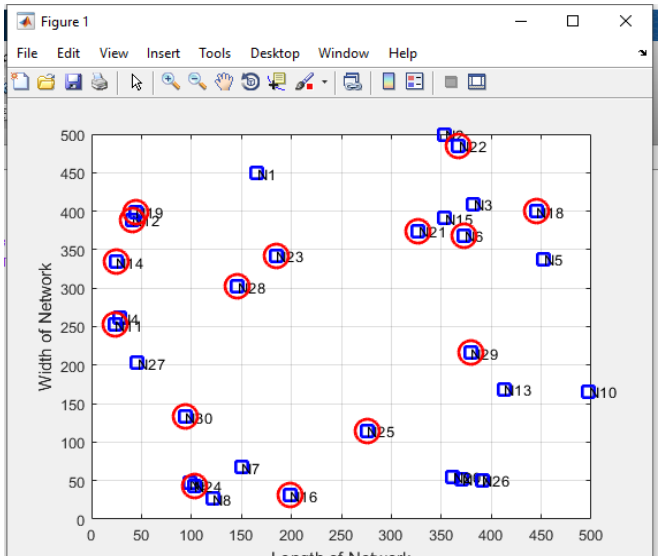

Fig 5. Device Registration.

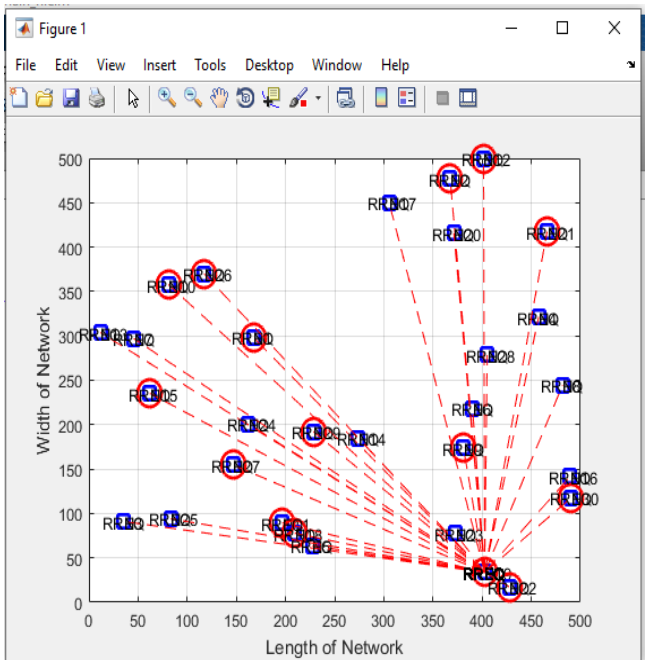

Fig 6. route request packet (RREQ) is broadcasted from a source node to other nodes in the network.

Man in the Middle -attack occurs when a node is maliciously entered into the network and positioned in the middle of a data stream of two (2) sensors or a sensor and a router node, capturing as much traffic circulating on the intercepted network as possible.

International Journal of Science, Engineering and Technology

An Open Access Journal

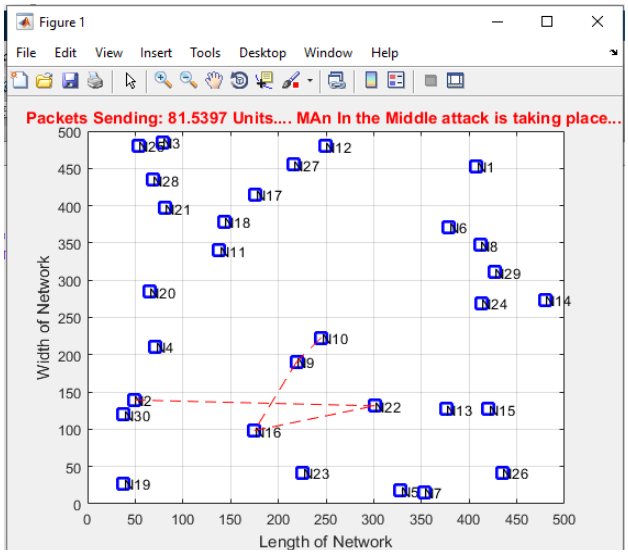

Fig 7. MIM attack taking place.

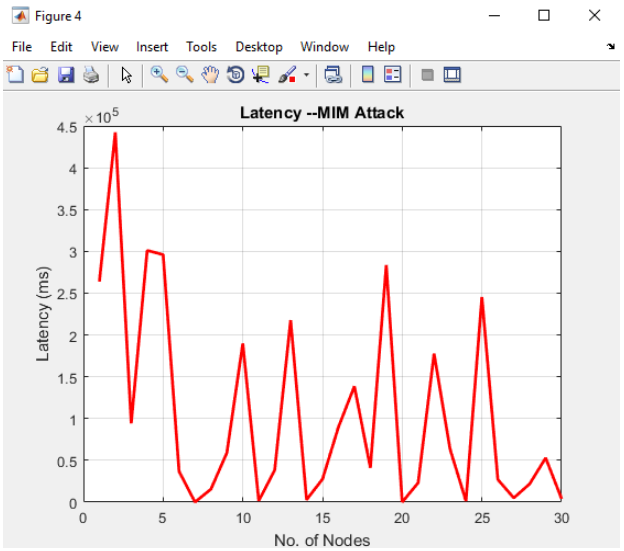

Fig 10. Latency MIM attack.

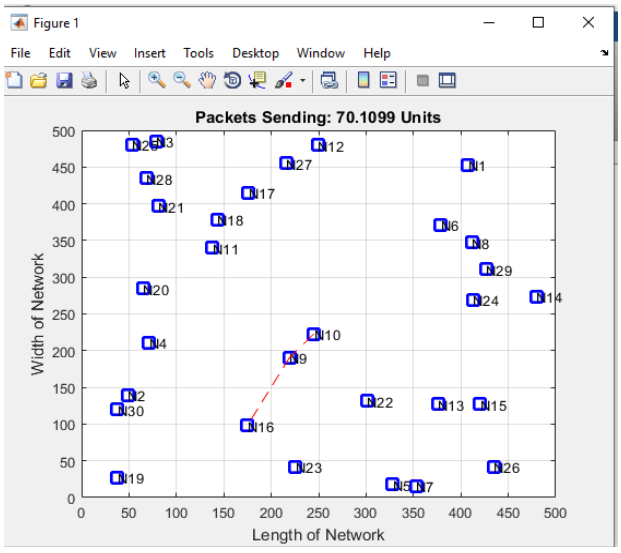

Fig 8 searching path and reroute.

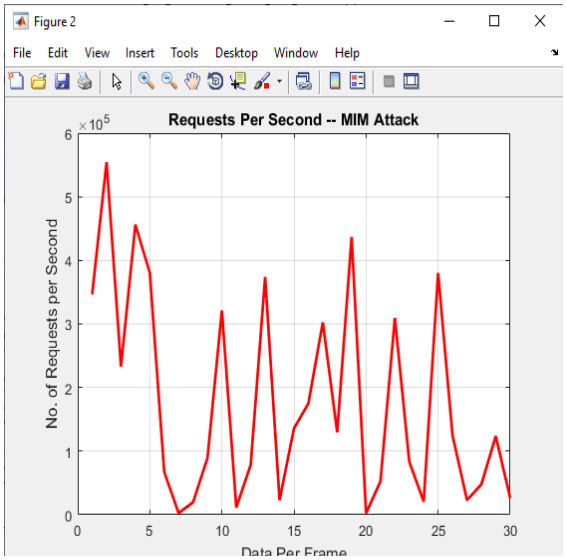

Fig 11. number of request per second MIM attack.

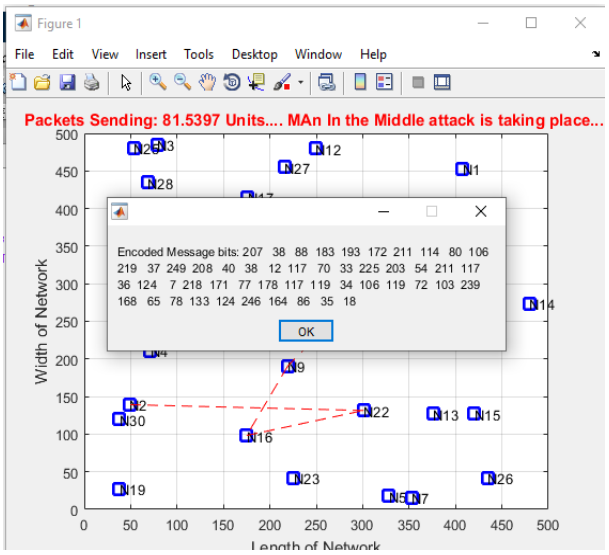

Fig 9. Elliptic Curve Cryptography (ECC) Message Bits.

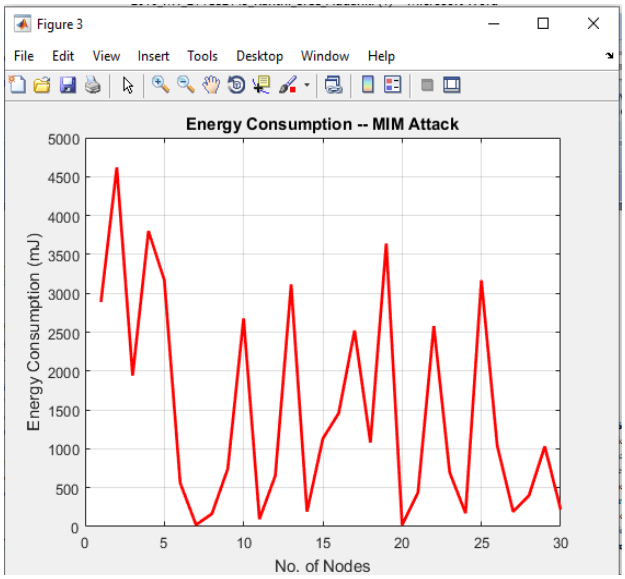

Fig 12. Energy consumption while MIM attack

International Journal of Science, Engineering and Technology

An Open Access Journal

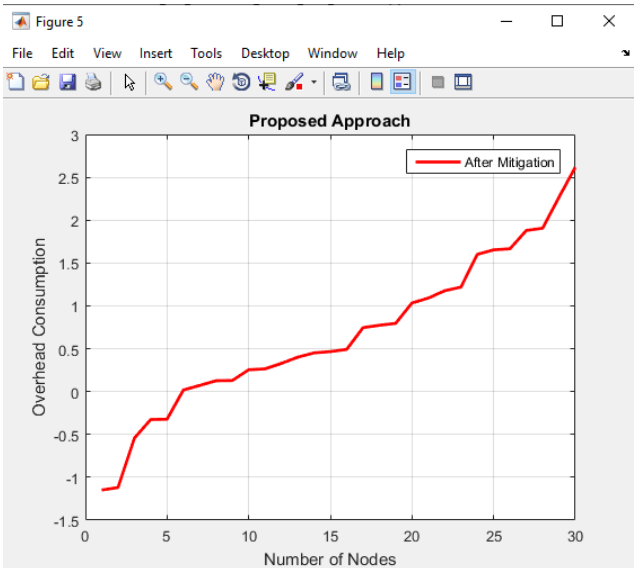

Fig 13. Overhead consumption.

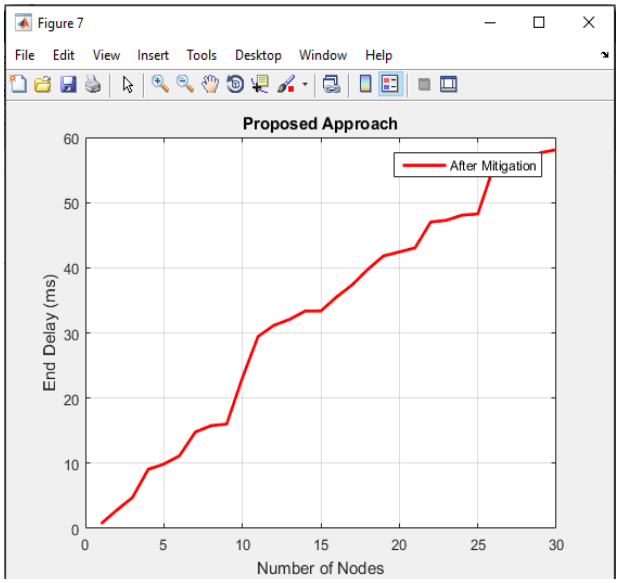

Fig 14. End Delay.

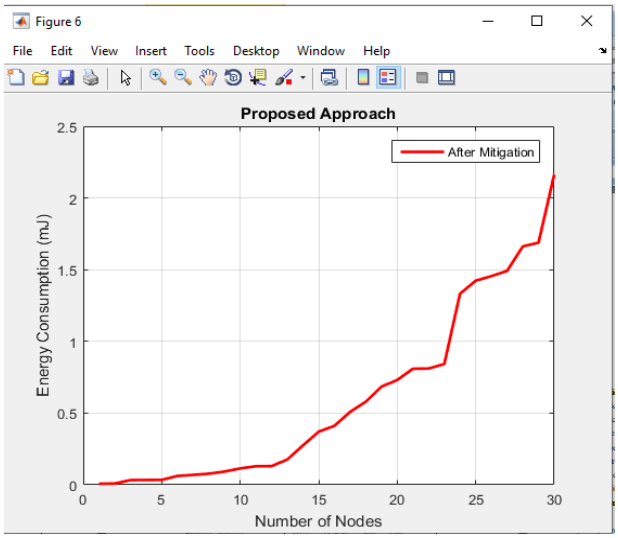

Fig 15. proposed system energy consumption.

The neural network contains different blocks or cells. The cells are responsible for storing of information about the network activities. The neural network maintains two states like hidden state and cell state. These two states getting operated through three functions like forget, input and output.

These operations on these cells help to identify manipulated behavior of cells. The input operation adds recent information into the cells. The output operation selects only required information from the cells. The forget operation removes the unnecessary information from the cells.

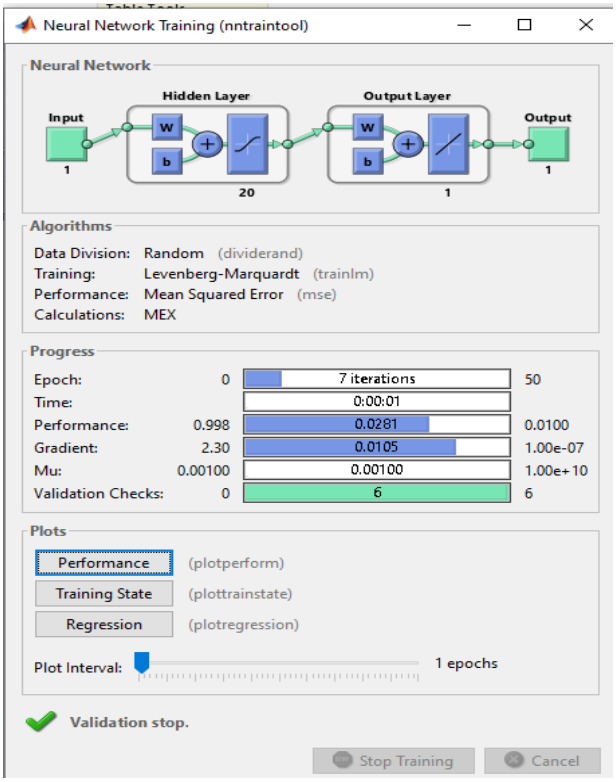

Fig 16. Neural Network training.

VI. CONCLUSION

We proposed a symmetric key negotiation based authentication mechanism which uses ECC in the registration phase and a symmetric key establishment is performed at the end of authentication phase of the protocol. This key is then used between the devices for data collection tasks.

We can observe that mutual authentication is achieved. Based on the performance analysis, the proposed method is also lightweight compared to the existing methods due to the smaller key size used by the ECC cryptography.

But in security analysis, we observed that the protocol can be subjected to man-in-the-middle attacks. Hence, an asymmetric key negotiation based authentication mechanism which uses Elliptic Curve Integrated Encryption Scheme in the registration phase and a symmetric key establishment is performed at the end of authentication phase of the protocol.

This key can be used between the devices for data collection tasks. We can observe that mutual authentication is achieved in this method. Based on the performance analysis, the proposed method is also lightweight compared to the existing methods but we can observe a tradeoff between security and lightweight factor. This direction to improve these methods with certain level of standards which aims at light weight nature and security within the network.

Table 1. Comparison table.

	Energy Consumption M/J	End Delay (M/S)	Overhead Consumption	Latency(S)	Overhead Consumption	Number of Request Per Second
With MIM Attack	4.5 M/J	80(M/S)	3.5	4.5(S)		5.5
After Mitigatio	2.2 M/J	60(M/S)	2.5		2.51	

REFERENCES

[1] Feifei Wang, Guoai Xu, and Lize Gu "A Secure and Efficient ECC-Based Anonymous Authentication Protocol" Hindawi 2019.

[2] SungJin Yu, KiSung Park, and YoungHo Park "A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment" MDPI 2019.

[3] Hong K, Kim Y, Choi H, Park J. SDN-Assisted slow HTTP DDos attack defense method. IEEE Commun Lett 2017;22(4):688–91.

[4] Tsai SC, Liu IH, Lu CT, Chang CH, Li JS. Defending cloud computing environment against the challenge of DDos attacks based on software defined network. Advances in intelligent information hiding and multimedia signal processing (pp. 285–292). Cham: Springer; 2017.

[5] Kholidy HA, Baiardi F. CIDS: a framework for intrusion detection in cloud systems. In: 2012 ninth international conference on information Technology-new generations (pp. 379–385). IEEE; 2012.

[6] Modi CN, Patel DR, Patel A, Muttukrishnan R. Bayesian classifier and snort based network intrusion detection system in cloud computing. In: 2012 third international conference on computing, communication and networking technologies (ICCCNT'12) (pp. 1–7). IEEE; 2012.

[7] Manish Kumar; Ashish Kumar Singh Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) Year: 2020 DOI: 10.1109/ IEEE Tirunelveli, India

[8] Ajay Shah; Sophine Clachar; Manfred Minimair; Davis Cook Building Multiclass Classification Baselines for Anomaly-based Network Intrusion Detection Systems 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA) Year: 2020

[9] Sungwoong Yeom; Kyungbaek Kim Improving Performance of Collaborative Source-Side DDoS Attack Detection 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS) Year: 2020 DOI: 10.23919/: IEEE Daegu, Korea (South)

[10] Hodong Kim; Changhee Hahn; Junbeom Hur Real-time Detection of Cache Side-channel Attack Using Non-cache Hardware Events 2021 International Conference on Information Networking (ICOIN) Year: 2021 DOI: 10.1109/ IEEE Jeju Island, Korea (South)