Mirza Anas Beg,2021, 9:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

ANN Based Efficient and Secure Authentication Key Agreement Protocolfor WSNs in IOT

M. Tech. Scholar Mirza Anas Beg, Prof. Zuber Farooqui
Department of Computer Science and Engineering,
All Saints' College of Technology,Bhopal,MP,India

Abstract-The Internet of Things (IoT) based on a large number of wide range of interconnected heterogeneous units general applications, including healthcare systems, Energy management, environmental monitoring, household and Business automation. Although the Internet of Things is considered activation Different service technologies, it also improves a lot of security and privacy. This thesis focuses on development security Data source agreement with identity verification and privacy Preservation scheme. The aim of the scheme is to realize device authentication in the security approaches is more energy-consuming. 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 IoT environment. The MATLAB software has been used to show simulation performance. This simulation performance compare the system while attack taking and after mitigation.

Keywords: ANN, Secure authentication, IOT, Protocol, WSN

I. INTRODUCTION

The Internet of Things (IoT) is a modern computing model that refers to interconnected material devices or IoT devices containing sensors, actuators, and networking so that these IoT devices can link, communicate and share data. With the risein the number of IoT devices, several security concerns have been found, especially in sharing of sensitive data.

Authentication is one of these reliability concerns. In the IoT world, authentication is a major challenge due to complexity of protocols, devices, or topologies. IoT systems interacting with each other need to be trustworthy in order to prevent various forms of security negligence attacks. Authentication is also the cornerstone of access management and transparency.

The Internet of Things (IoT) consists of knots with minimal resources, which, regardless of time or place, are widely dispersed in the IoT environment.

IoT is now used for a wide range of purposes, including hospitals, intelligent homes, intelligent manufacturing, and intelligent cities. Furthermore, a hypertext net age can be used between different handheld terminals, but most (if not all) of our applications, thanks to the advent and marketing of the fifth-generation (5G) cellular network, is also possible.

Link information between objects or exchange information. By 2022, it is expect that 43 billion devices will be related to IoT around globe, and the numbers of such systems are probable to amplify exponentially with marketing of 5 G networks. The massive Internet of Thingsnetwork can deal with approximately 1 million items per square

kilometer, depending on the 5 G Vision Specifications from the Radio Communications Department of International Telecommunication Union (ITU-R).

The advancement of Internet of Things or broad Internet of Things holds good promise but these systems are exposed to a range of vulnerability due to the extended attack surface. To safeguard user privacy in the IoT environment, protective features such as data protection, virtual network security, service compatibility, or data privacy must also be make available.

In the complex construction, safe user authentication or key exchange systems using encryption technologies must meet these IoT protection rations. The network of things faces different challenges with user nodes or sensor nodes communicating with each other. The user authentication system has to ensure the following protection or practical specifications to recover safety of the IoT system.

However, most of these IoT devices follow wireless connectivity, which opens the door to various security challenges associated with wireless sensor networks .The difficulty of securing nodes in a system is always a problem in wireless networks. In the case of IoT, when a device instigates a connection (whether it is data processing or data collection), it is possible to attack attackers through manipulation or fake tools.

This will not only allow an attacker to access important communication data, but will also change the location of your device. For example, the lack of authentication of the local network of the human body used in medical and healthcare applications on the Internet of Things will cause enemies to attack in the form of unscrupulous devices.

Potential, which may issue incorrect instructions to patients 'equipment, detrimental to their health [4]. In general, these devices are vulnerable to various safety attacks such as emulation and update attacks. This urgently requires security systems that need to verify the authenticity of equipment prior to data collection and data compilation operations [5,6].

In addition, these IoT devices have incomplete memory or dispensation power [7], which leads to knowledge resource consumption, which also makes these secure cryptographic protocols should be lightweight protocols to reduce headaches. computational and extend its lifespan [8].

Different network environments have different authentication models. The tool verification mechanism presented in this journal is lightweight or dynamic. It uses symmetric basic protocols and asymmetric cryptography to achieve authentication and mutual agreement. These protocols are designed to be used to validate IoT devices and network access gateways.

II.LITERATURE REVIEW

Muhammad Naveed Aman et.al.2019[1] The Internet of Things (IoT) engulfs a large number of interconnected heterogeneous devices from a wide range of pervasive application areas including health-care systems, energy management, environmental monitoring, and home and commercial automation. Although IoT is considered an enabling technology for a variety of services, it also raises many security and privacy concerns. This paper focuses on developing secure protocols for data provenance with authentication and privacy preservation in IoT systems. Protocols for two scenarios are presented, one when an IoT device is directly connected to a wireless gateway and the other when an IoT device is indirectly connected to the wireless gateway through multiple hops of other IoT devices.

The proposed protocols use Physically Unclonable Functions along with wireless link fingerprints derived from the wireless channel characteristics between two communicating entities. This results in protocols which are not only efficient in terms of computational complexity and energy requirements but are also safe against various types of attacks including physical and cloning attacks.

Experimental results show that in comparison to existing protocols, the proposed protocols are upto 100% more accurate in detecting attacks on data provenance and can save upto 83.8% and 73.5% energy consumption for the IoT devices in terms of CPU and radio energy, respectively.

In 2020 Hakjun Leea et al. [1] the authors proposed the user authentication schemes and proposed an updated method to correct and

enhance the protection. A random Oracle, BAN logic, methods were used for formal and informal security analyses for security of the proposed scheme to be tested. The results of study show that the proposed system is safe, can withstand a large number of known attacks, and comply with all safety criteria.

Also, the Author conducts a benchmarking study based on the hardware features of mobile devices and sensors and other related solutions in the real world of the Internet of Things. The findings of the study show the compatibility of the solution with very low-cost IoT products. The approach planned in this study is therefore useful for IoT user authentication.

Timothy Malche et.al(2020) Internet of Things (IoT) security requires the security of connected objects and networks. The Internet of Things is increasingly a collection of so -called unique objects. These objects have the ability to send data automatically through the network. Most of the growth of IoT connectivity comes from computing devices and integrated metering systems that are used for machine-to-machine (M2M) communication, home automation and home automation in-vehicle communication, sharp grids and usable tools. Since it is to connect all physical objects to the Internet, the idea is not always evaluated in product design.

IoT products cannot choose secure security. Therefore, security is one of the most important priorities in the Internet of Things. This research proposes an IoT architecture that is related to device security. The main purpose of this research is to ensure that the real device uploads the data and limits the fake data generated by the device trying to become a real device. This research offers a powerful authentication technology based on secret keys that can protect the identity of IoT devices in a network.

The authentication and authentication technologies presented in this article can ensure that the right equipment transmits and receives the right data at the right location and for the right purpose.

III.PROPOSED METHODOLOGY

The aim of the scheme is to realize device authentication in the security approaches is more energy-consuming as well as having time constraints. 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 IoT security systems to make adjustments in changing environments as per requirements.

The purpose of this protocol is to use the public key to be used in the next step of communication connecting devices to achieve device verification and secure key placement. In addition, there are other security objectives that can be achieved, such as counteracting layer attacks (such as simulation attacks), and attack recovery (while preserving integrity and capability).

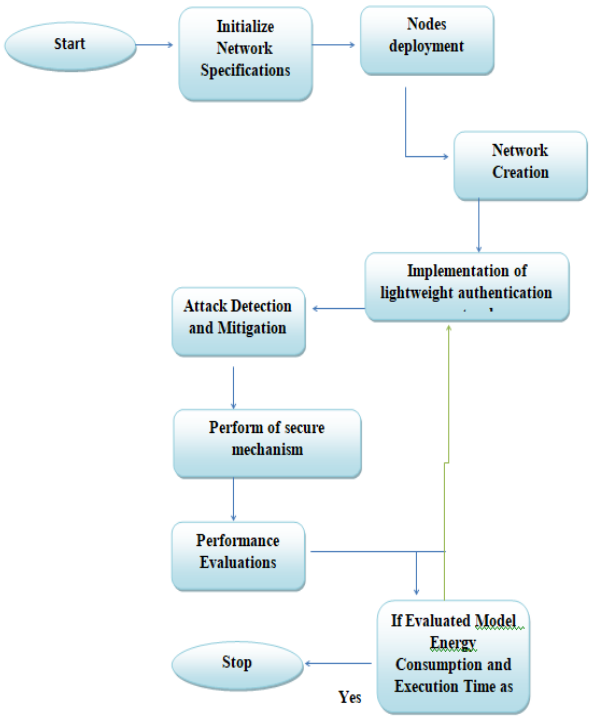

Fig 1. Proposed Flow Diagram.

Figure 5.1 shows simulation based on a network of 30 nodes. Throughout the entire network used as an administrator, it monitors malicious activity in the network. The simulation was done using MATLAB software.

This section discusses the use of symmetric core protocols and ECC encryption for device authentication and machine learning-based

International Journal of Science, Engineering and Technology

An Open Access Journal

technologies to detect and protect malicious activity. Whatever the worthy application of the WSN, it is most vulnerable to attacks by hackers, such as Man-in-the-middle attacks (MITM).

In the event of an MITM attack, an unsolicited third party will log in as a legitimate user in a short period of time. The attacker or attacker behaves like a proxy user and manipulates the data according to their needs.

In the ancient literature, MITM was abbreviated in various ways, such as MIM. MITM Attack MITM is a malicious attack that secretly listens to the conversations of two legitimate users of the attacker.

When necessary, the attacker pretends to be a legitimate user and attacks data or information for manipulation. Often, during a MITM attack there will be new discussions or transfers. Without reliable security, two legitimate users will not know the authenticity of the data. This work mainly examines the MITM Intrusion Detection System (MITM-IDS) based neural network study.

The whole process tries to create attack-resistant MITM-IDS to ensure non-attack communication when unclean points are detected.

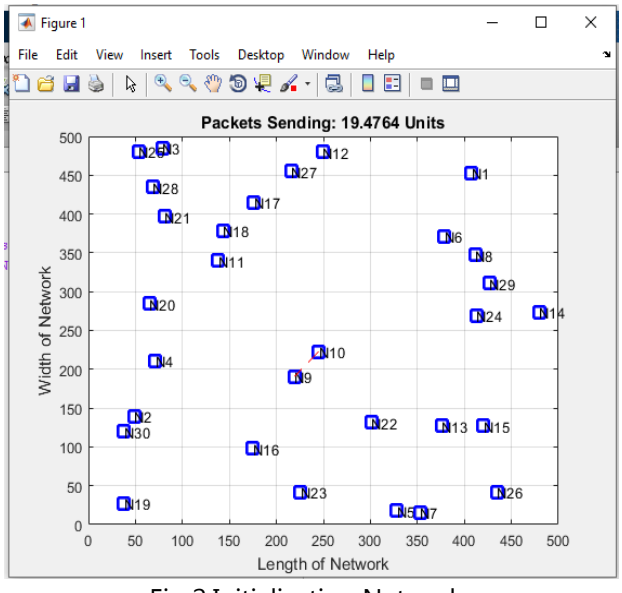

Fig 2.Initialization Network.

Data from the public node is sent to the source routing node in the region to execute the route request, and the source node adds the information of the selected route to the source routing header in it. In a data packet.

In addition, in the data transmission process, the transmission point between the intermediary points follows the relay path and progresses according to the source path information in the packet head, and no connection to the source routing node, which can reduce the energy consumption of the system.

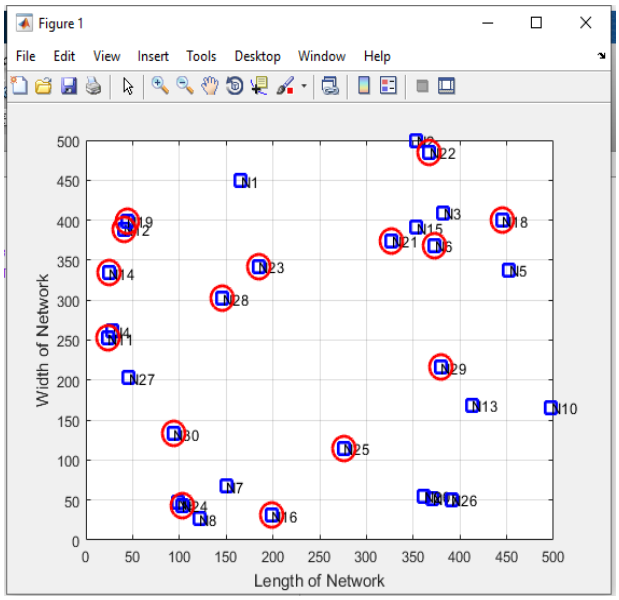

Fig 3. Device Registration.

The configuration of the zone depends entirely on the energy efficiency between the source routing node and the public node. To extend the life of the network, the energy efficiency determines which of the resource node areas is more suitable for the public domain. Zone creation is accomplished through a process of controlling message exchange between the source routing node and the public node.

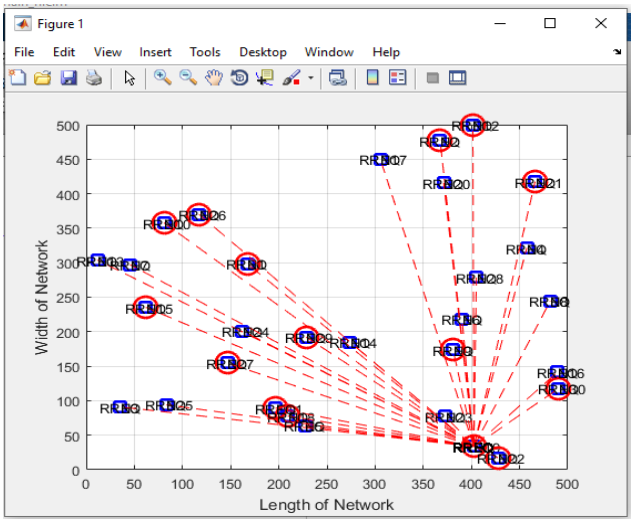

Fig 4. Route request packet (RREQ) is broadcasted from a source node to other nodes in the network.

International Journal of Science, Engineering and Technology

An Open Access Journal

The possibility of sending different messages through RREQ is a process in which a request path packet (RREQ) is sent from a source node to another point in the network. The default record field in the source transport package contains all the paths from the source to the destination as it travels.

The data packet comes with a source data transmission function that allows an intermediate hop between the source node and the target node to include the network address in the data packet (RREP), while the data packet follows the path from the target to the source. In this way, a route is created and the source node can use the path to send data packets to the destination of the source path.

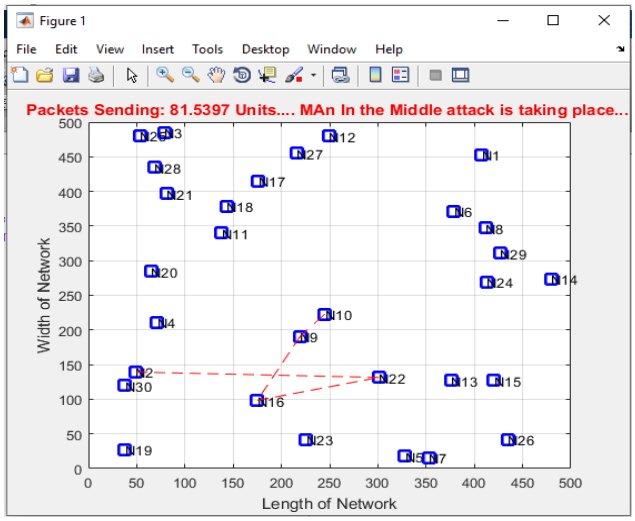

Fig 5. MIM attack taking place.

Fig 5.4 showing,A middleman attack is an attack that occurs when a point is incorrectly entered into the network and positioned in the middle of the data stream there are two sensors and router node.

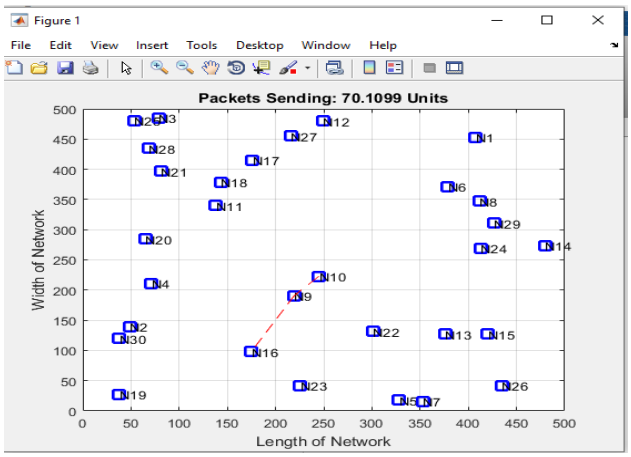

Fig 6.Searching Path and Reroute.

And finally, the malicious node forwards the configured data packet to the target node, blocking its path to the wrong path and creating a wrong neighbor between the target points in the process.

The next step is to capture the data packet so that you can find the modified application data and insert it into the target node. When the dirty spot cannot withstand interesting traffic, it will store the package and repeat the capture process.

MITM attacks will focus primarily on data entry between clients and servers for other malicious activities. However, MITM attacks can use more attacks.

Thus, we define that MITM attackers are able to establish an independent relationship with the victim and convince them that their conversation is still being made through personal contact. Attackers have the ability to block, transmit data packets, and even inject new data packets.

MITM attacks are primarily focused on importing data between clients and servers for other malicious activities. However, we believe that MITM attacks could be more numerous. Thus, the MITM attacker is able to establish an independent relationship with the victim and convince them that their conversation is still being done through personal communication. Attackers have the ability to block, transmit and even inject new packets.

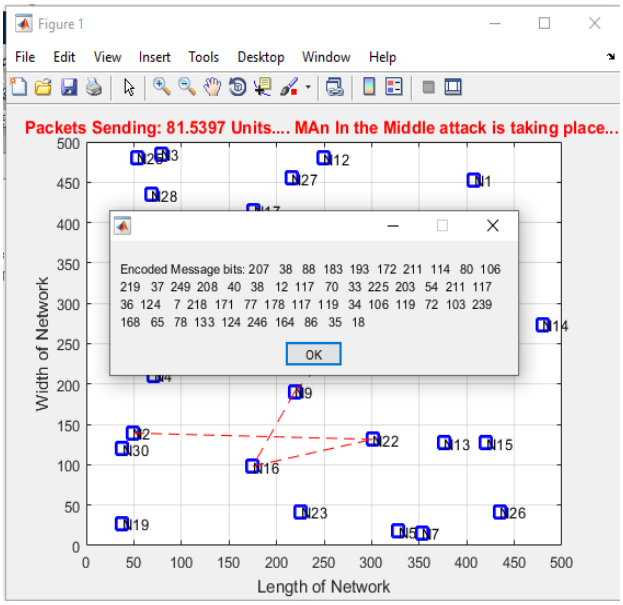

Fig 7. Elliptic Curve Cryptography (ECC) Message Bits.

International Journal of Science, Engineering and Technology

An Open Access Journal

Elliptic Curve Cryptography (ECC) is a type of public key cryptography. The user or device participating in the communication usually has a key, a public key and a private key and a series of functions associated with these keys to perform encryption operations.

Only private users know the private key, and the public key is shared with all users participating in the connection. In a symmetric account, the data is erased and locked by a common shared key, so there is a basic exchange problem. Secure sharing of key communication keys is a big problem because it is not always possible to share keys.

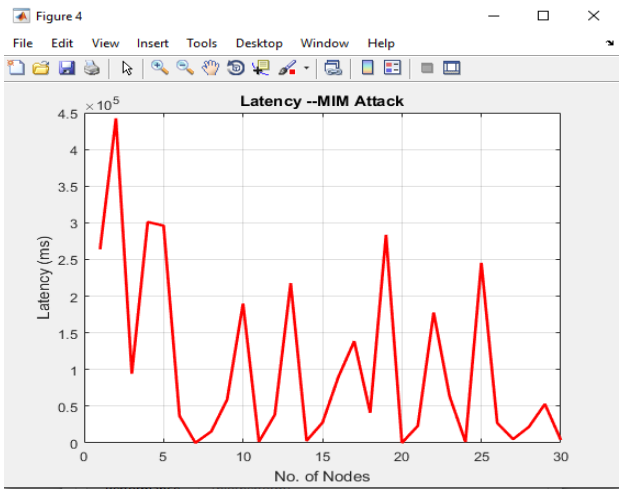

Fig 8. Latency MIM attack.

Figure 5.6 shows the network latency, which measures the time it takes for some data to reach the network's destination. It is usually measured by the delay back and forth - the time it takes for the message to reach its destination and return again.

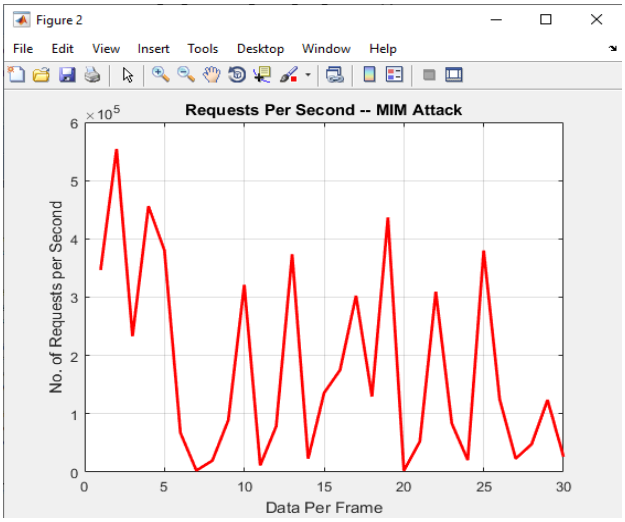

Fig 9. Number of request per secondMIM attack.

Fig 5.7 showing the number of attack per second with each data frame where y axis showing the number of data per second and x axis showing the data frame.

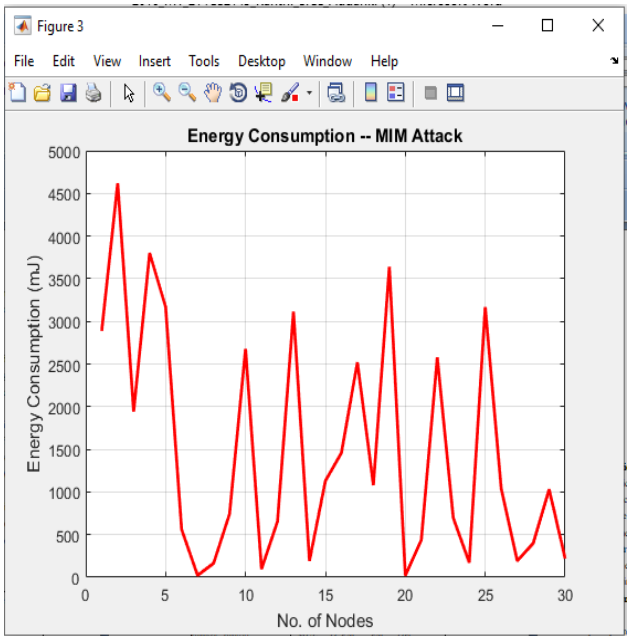

Fig10. Energy consumption while MIM attack.

Fig 5.8showing energy consumption while MIM attacks in Wireless networks, most of the energy is consumed in the process of data transmission.

In the fig y axis showing the amount of energy consumption during packet transmission and y axis showing the no of node.

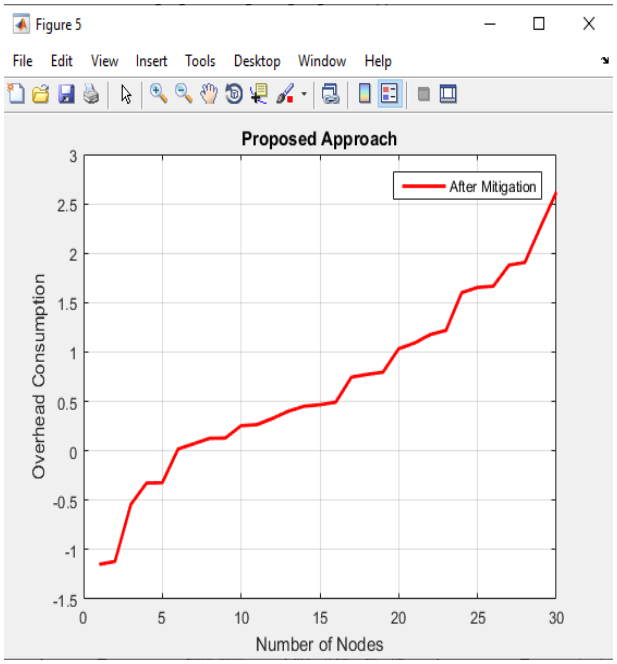

Fig 11. Overhead consumption.

International Journal of Science, Engineering and Technology

An Open Access Journal

Fig. 5.9overhead consumption showing the total number of packets to be transferred or conveyed from one node to another It contains overhead of routing procedure, routing table and packet preparation in a sensor node.

In fig y axis showing the overhead consumption and x axis showing the number of node.

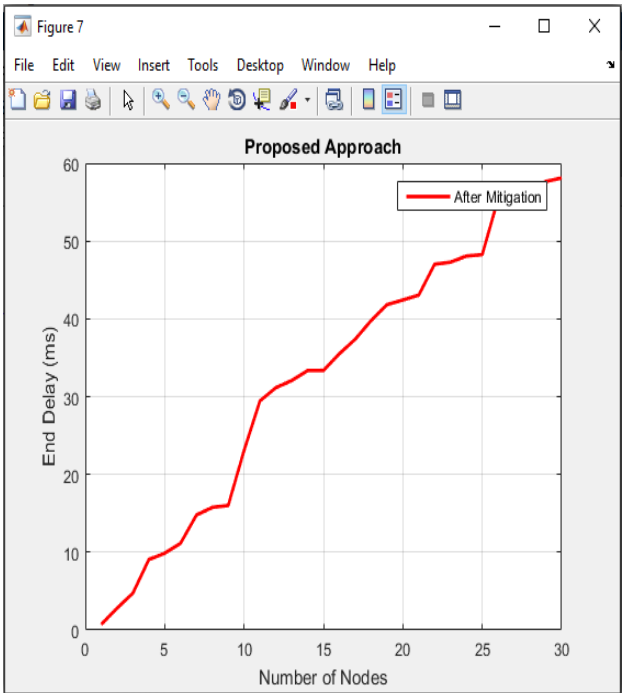

Fig 12. End Delay.

Delay refers to the amount of time it takes for first bit to travel over a link among sender and receiver.

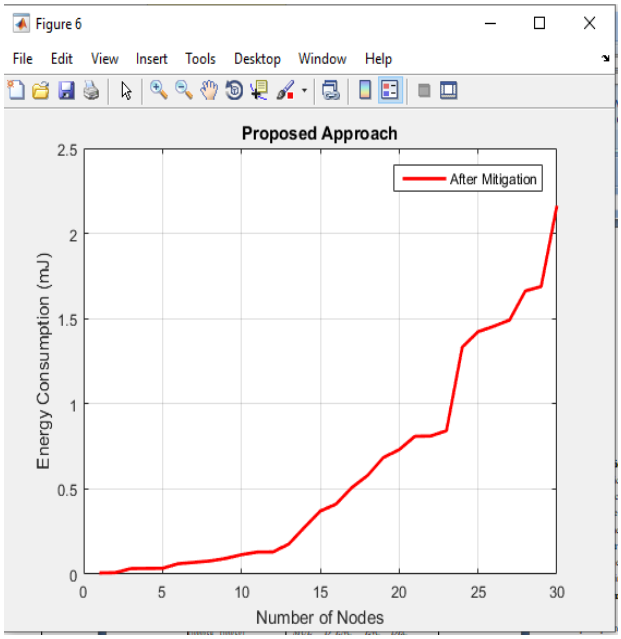

Fig 13. Proposed SystemEnergy Consumption.

Figure 5.11 shows the energy consumption provided for the system.As the coverage area increases, the energy consumption also increases, mainly due to the distance between the member and the single CH.

The energy balance is determined by the energy consumption of the equipment and the transmission power of the wireless sensor network. In the figure, the y axis shows the energy consumption, and the x axis shows the number of nodes.

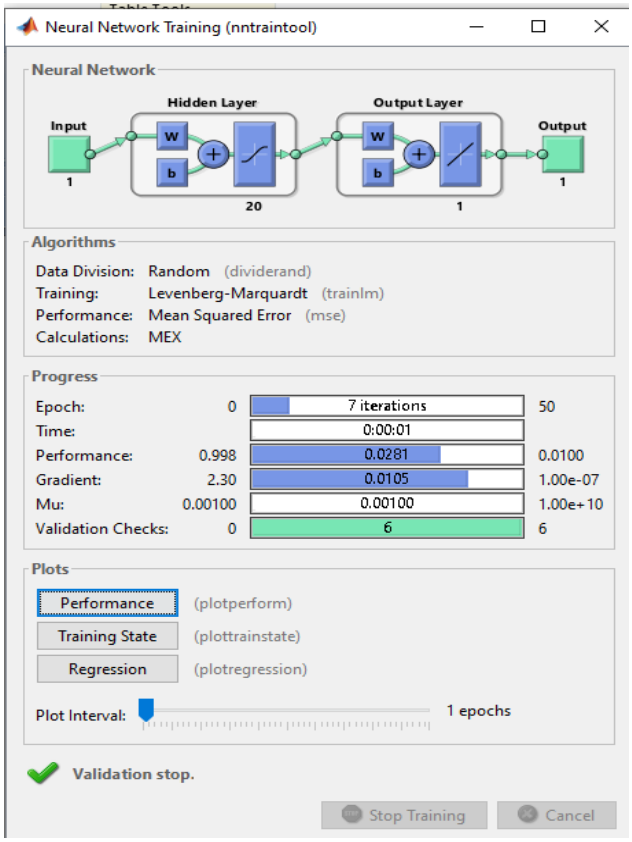

Fig 14. Neural network training.

Neural networks are made up of different barriers or cells. The component is responsible for storing information about network activities. The neural network maintains two states, such as the latent state and the cell state.

These two states work through the three functions of forget, access and output. Analysis of these cells helps to understand the cell cycle behavior. Input transmission helps the last cell in the network.

The extraction function selects only the information needed for the cell. Forget to delete unnecessary information in the cell.

Table 1. Comparison table.

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

IV.CONCLUSION

In this paper, we focus mainly on the challenges of the Internet. Then, we solved the validation problem in the perception layer of the Internet of Things. We have noticed that existing verification methods are still under attack, and some of them will overtake the head of the device.

We propose a validation mechanism based on a symmetric base agreement, which uses ECC at the registration process and performs a symmetric base configuration at the end of the protocol validation process. Then, use this key between devices to perform data collection tasks. We can see that the strengthening of cooperation has been achieved.

Based on the analysis of the performance, because the key to using the cryptography ECC is small, compared to the existing method, this method is also light and easy to use. But in the security survey, we found that the protocol may be vulnerable to attacks by people in the middle.

Therefore, at the end of the authentication process of the protocol, an asymmetric key agreement-based authentication mechanism is implemented, which uses an elliptic curve-enabled encryption scheme during the registration partition and assigns a symmetric key.

This key can be used for data collection tasks between devices. We can see that the verification of both parties can be performed by this method. Based on the analysis of the performance, the proposed method is only light compared to the existing methods, but we can make exchanges in terms of safety and lightness.

In the future, we hope to build a collaborative architecture that allows devices to use the same type of lightweight authentication model for access to a variety of cloud network services.

An interesting fundamental question that arises from our research and analysis is whether a lack of adequate stability and light objectives can explain the recurring errors that can occur in old verification principles, and build a more effective and robust approach to future work, The importance of light verification projects.

REFERENCES

[1] M. H. Rehmani and A.-S. K. Pathan, Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications. CRC Press, 2016.

[2] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.

[3] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, pp. 393–422, 2002.

[4] Sazonov and M. R. Neuman, Wearable Sensors: Fundamentals, implementation and applications. Elsevier, 2014.

[5] Blilat, A. Bouayad, N. el houda CHAOUI, and M. Ghazi, "Wireless sensor network: Security challenges," in Network Security and Systems (JNS2), 2012 National Days of. IEEE, 2012, pp. 68–72.

[6] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013, pp. 663–667.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[8] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," Sony Corporation, pp. 7–10, 2008.

[9] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: State of the art," in Robots and Sensor Clouds. Springer, 2016, pp. 55–75.

[10] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012, pp. 257–260.

[11] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. IEEE, 2012, pp. 1282–1285.

[12] Y. R. Shi and T. Hou, "Internet of things key technologies and architectures research in information processing," in Applied Mechanics and Materials, vol. 347. Trans Tech Publ, 2013, pp. 2511–2515.

[13] Hakjun Leea, Dongwoo Kanga, Jihyeon Ryub, Dongho Wonc, Hyoungshick Kimc, Youngsook Lee "A three-factor anonymous user authentication scheme for Internet of Things environments" ELSEVIER 2020.

[14] Anca Jurcut, Tiberiu Niculcea, Pasika Ranaweera, Nhien-An Le-Khac "Security Considerations for Internet of Things: A Survey" SN Computer Science 2020.

[15] Chi-Tung Chen, Cheng-Chi LeeID, Iuon-Chang Li "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments" PLOSE ONE 2020.

[16] Liang Xiao, He Xu, Feng Zhu, Ruchuan Wang, and Peng Li "SKINNY-Based RFID Lightweight Authentication Protocol" MDPI 2020.

[17] Evangelina Lara, Leocundo Aguilar, Mauricio A. Sanchez, and Jesús A. García "Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things"MDPI 2020.

[18] Afrah Albalawi, Amal Almrshed, Arwa Badhib, Suhair Alshehri "A Survey on Authentication Techniques for the Internet of Things" IEEE 2019.

[19] Seul-Ki Choi, Ju-Seong Ko, Jin Kwak "A Study on IoT Device Authentication Protocol for High Speed and Lightweight" IEEE 2019.

[20] Zaheer Abbas, Syed Muhammad Sajjad, Hassan Jalil Hadi "Light Weight Secure Authentication for Accessing IoT Application Resources" IEEE 2019.

[21] Data Provenance for IoT with Light Weight Authentication and Privacy Preservation Muhammad Naveed Aman, Mohammed Haroon Basheer, Student Member, IEEE Biplab Sikdar, Senior Member, IEEE 2327-4662 (c) 2019 IEEE.