INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Wireless Sensor Node Authentication and Data Security Framework Using Machine Learning

K Nirmala[1*], **D V Subba Rao**[2]

1 Research Scholar, Department of Computer Science and Engineering, S.V. University, Tirupati, Andhra Pradesh, India
2 Professor, Department of Computer Science and Engineering, S.V. University, Tirupati, Andhra Pradesh, India

OPEN ACCESS

Received: 17-02-2023
Accepted: 18-07-2023
Published: 30-09-2023

Citation: Nirmala K, Rao DVS (2023) Wireless Sensor Node Authentication and Data Security Framework Using Machine Learning. Indian Journal of Science and Technology 16(37): 3064-3072. https://doi.org/10.17485/IJST/v16i37.295

* **Corresponding author**.

nirmalagiddaluru26@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To implement Wireless Sensor Node Authentication and Data Security Framework Using Machine Learning. **Methods:** The study is centered on a Generative Adversarial Networks (GAN) learning technique which explains about authenticity of secured wireless sensor network. This method is developed using two main components like Generator (G) network which produces false data for confusing the attacker and Discriminator (D) network which consists of multiple layers that can efficiently differentiate between real and fake data for interpretation at the end node (Rx) for providing secure communication. Unauthenticated sensor nodes can be detected with higher accuracy, throughput and low end-to end delay using machine learning based framework. In this work, Probability of False Detection, Reliability and Uniqueness, Delay and throughput are evaluated to determine the performance of presented approach. **Findings**: Simulation results reveal that the proposed IFAs antennas can provide isolation with a mutual coupling reduction of 18 dB with respect to the transmission coefficients and can also obtain sufficient bandwidth by the proposed antenna array for the 5G mobile terminals applications. **Novelty**: GANs algorithm is used for the first time to resolve WSN middleware having security issues.

Keywords: WSN; Sensor Nodes; Authentication Mechanism; Machine Learning

1 Introduction

A group of sensor nodes are connected to each other in a network through wireless Communication is called Wireless Sensor Network (WSN). Sensor nodes are distributed spatially in WSN that are controlled mutually in some conditions [(1)]. Wireless sensor networks have attracted an extraordinary amount of attention from the scientific community over the course of the last several years. A typical wireless sensor network is made up of thousands of sensor nodes that are scattered around an area of interest at random or according to a defined statistical distribution [(2)]. Sensor nodes are present in adversarial environment such that the attackers can easily enter into the

network for capturing data from physical nodes. In most of the cases, the sensors may façade in any of the present node where every single sensor represents multiple sensor identities within the network [3].

With the rapid development of sensor technology, wireless sensor networks (WSNs) composed of a large number of low-cost, high-performance and plug and play sensor nodes have occupied more and more application scenarios in society, such as medical and health, environmental monitoring, business activities, and national defense security. However, a WSN is a distributed network exposed in an open environment. Each node is independent of the other, and the lack of a central node and monitoring node makes it vulnerable to malicious attacks, and it is difficult to prevent. Denial of Service (DoS) attack is one of them [4]. WSNs are typically deployed in potentially untrusted environments. Therefore, it is imperative to address the security challenges before they can be implemented.

At the present time, wireless sensor networks have become one of the hottest research areas due to their wide range of real-time applications like critical military surveillance, battlefields, building security monitoring, forest fire monitoring, and healthcare. The design of these applications assumes that all the nodes involved are cooperative and trustworthy. However, this is not the case in real-world deployments, where nodes are exposed to different types of attacks and intrusions that can downright damage the proper functioning of the network and degrades system performance. Faults that interrupt the communication services of the network, especially in sensor networks, can compromise the entire network. The detection of the faults, and subsequently their correct identification are the only ways to work towards any actions concerning the recovery of the network. R Unfortunately, ensuring the security of this type of network against various malicious attacks activities is a difficult task, especially when the nodes are made up of inexpensive electronic devices with limited hardware capabilities [5].

All cybersecurity problems, in particular attacks, prevention and mitigation are therefore very necessary to create a safe and secure framework. WSNs are vulnerable to a number of attack methods that could pose essential security threats. These attacks may be linked to two major categories: active and passive. In the category of passive attacks, attackers normally are disguised (camouflaged) and either damage the network components or use the connection to gather useful information. Passive attacks can also be classified into types of eavesdropping, disruption of nodes, malfunction of the node, node interrupt and monitoring of traffic. Whereas an attacker affects the roles and activities of the target network in the active attacks group. The effect can be the actual target of the intruder and can also be identified by means of protection mechanisms (intrusion detection). For example, as a result of such attacks, network services can be interrupted. Flooding, Denial-of-Service (DoS), Blackhole, Wormhole, Sinkhole and Sybil types are some of the active attack [6].

Authentication of identity for sensor node has to be performed in turn to prevent attacks. Such activities are practiced for public key cryptography in conventional internet. The ability of resource constrained with this storage cost sensor node is not efficient for generation of digital signatures. Present working models sort out the issue by forming secured pair wise keys through pre-distribution methods of random key. Nevertheless, this simplification is not totally secured and energy efficient. The traditional security mechanisms are authentication, symmetric key encryption & decryption and public key infrastructure (PKI) having built in cryptography. The major challenge is to deploy the techniques of above mechanisms or their modified incarnations in a sensor network with due regard to the WSN's being is characterized with constrained memory, power (sensor life) and processing capability. On the top of all this, the wireless sensors need very secure communication in wake of they being in open field and being based simply on broadcasting technology [7].

Due to the limited power in wireless sensor networks, options to rely on the security of ordinary protocols embodied in encryption and key management are futile due to the nature of communication between sensors and the ever-changing network topology [8]. The research gap due to these ineffective techniques and methodologies lead to various malicious attacks and data loss in WSN which is a challenge for the research community to diagnose and design fault tolerant sensor network that is highly robust. These limitations are needed to be overcome. In order to overcome these issues, we need an effective and accurate system which provides better security to the WSN. On the other hand, Machine learning algorithms are one of the better solutions for providing security services in this type of network by including monitoring and decision intelligence [9].

In this study, the current working system is enhanced for identification of radio sensor nodes basing on their fundamental signatures impulsively depending on communication signal that leads to complete analysis of Physical Unclonable Functions (PUF) features of radios for improved security of physical layers. The theoretical enhancement of RF-PUF is represented for an asymmetric IoT network [10]. Any additional hardware at the constrained resource of IoT node is not required for RF-PUF operation. PUF implementation at Tx node does not require on-chip or off-chip circuitry for RF-PUF. Process variability and component tolerance factors are inherent variations developed in proposed scheme at each transistor. A framework basing on machine learning techniques is designed in this study which reduces the non-idealities such as data variability accounts and variability in channel at receiver end [11].

At the time of data transmission, the data packets are highly prone to attacks. To overcome these drawbacks a powerful method is required that not only provides security but it should improve the efficiency of currently working network system.

This study presents a new technique based on machine learning which generates fake data for providing secured path for communication among sensor nodes by misleading the attacker. In proposed technique generation of fake data packets is not supported in order to reduce consumption of power and it avoids end to end delay by promoting throughput rate [12].

1.1 Literature Survey

Yu et al. [13] describes Service Attack Improvement in Wireless Sensor Network Based on Machine Learning. Different kinds of different layers in the occurrence WSN. These two types of machine learning techniques, neural network (NN), detect a Support Vector Machine (SVM), a media access control (MAC.) layer attacks. Authors have compared two methods. It has an access channel wireless sensor node, MAC. Protective layer is essential. Use scenario probability WSN. Wireless network simulator, Vanderbilt plow error simulation.

Chiristian Miranda, Georges Kaddoum, Elias Bou-Harb, Sahil Garg, Kuljeet kaur et al., [14] describes A collaborative security framework for software-defined wireless sensor network. A software-defined security framework is described that combines intrusion prevention in conjunction with a collaborative anomaly detection system. Initially, an IPS-based authentication process is designed to provide a lightweight intrusion prevention scheme in the data plane. Subsequently, a collaborative anomaly detection system is leveraged with the aim of supplying a cost-effective intrusion detection solution near the data plane. The performance of the proposed model is evaluated under different security scenarios as well as compared with other methods, where the model's high security and reduction of false alarms are demonstrated.

Abhishek Pandey, Lokendra Kumar Tiwari et al., [15] describes Novel Security Framework for Wireless Sensor Networks. Each individual sensor node acts as a part of the overall infrastructure. All nodes are connected in multi-hop mesh topology. In this flexible mesh architecture, we easily add new nodes and scale up to achieve control and monitoring over larger region. From the results it is observed that, if threshold value is too high then the number of suspected malicious node is minimum which decreases the reliability of a wireless sensor network. Therefore, for efficient wireless sensor network, we require optimum threshold value which varies in limited range and may be decided on case to case basis.

Swaminathan Ramesh, Calpakkam Yaashuwanth, Bala Anand Muthukrishnan et al., [16] describes Machine learning approach for secure communication in wireless video sensor networks against denial-of-service attacks. A secure framework is built along with encryption and decoding to protect from denial-of-service attack. Acknowledgement-based flooding attack has been focused with the help of support vector machine algorithm. The messages are encoded in from the source node and coded again during transmission phase to obtain the original message. Defending the traditional methodologies, the proposed work provides excellent QoS when compared and tested with other protocols. The results obtained ensure its efficiency when support vector machine technique is combined with encryption scheme.

Shruthi N, Seema Kousar et al., [17] describes Authentication of node in Wireless Integrated Sensor Networks using Certificate Authority. An efficient and secure framework is described which provides authentication to a roaming sensor node. And it allows a sensor node to move across multiple WSNs to solve the issues of Authentication. Encryption and Decryption techniques are provided to secure the data while transmitting data from one node to another. In propose work key management techniques are used to provide authentication by using Virtual Certificate Authority.

2 Wireless Sensor Node Authentication Framework Using Machine Learning

In this section, Wireless Sensor Node Authentication Framework Using Machine Learning is presented to overcome the problems of earlier approaches and to provide accurate and effective results to provide significant security to wireless sensor nodes. Low cost authentication devices within IoT node is the main focus of this work. It has remarkable difference from one node to another. During manufacturing and fabricating stages the device components have to be strictly controlled to reduce the difference between standard deviation and the count of correctly identified devices is reduced. Intriguingly, it leads to fabrication cost growth ultimately. Therefore, embracement of non-idealities becomes less expensive which does not affect the overall performance of framework and the usage of RF-PUF is justifiable. Thereafter, a scheme called Generative Adversarial Networks (GAN) for WSN is suggested for development of an intelligent security system. Traditional middleware is enhancement for its security and various kinds of characteristics of sensor nodes are handled effectively to generate reliable data. GANs algorithm is used for the first time to resolve WSN middleware having security issues. Furthermore, in WSN middleware, GAN is applied as it has ability to filter the unwanted data and anomaly detection in it. The process of machine learning based WSN node authentication and data security framework is shown in Figure 1.

2.1 Radio frequency-PUF

The manufacture variability of Tx(s) may lead to formation of PUF properties. The sub system Rx performance is identified for every node that draw out many features from the signals received. Due to inherent variations of local oscillator (LO) having ideal carrier frequency has its unique frequency for every transmitter. Device identification can be easily attained by using offset as a primary feature. In this research work standard receiver consists of carrier synchronizing module for compensation of LO offset at the receiver node which detect offset frequency and compensate it. Ppm value is sent to three-layer machine learning technique for device identification.

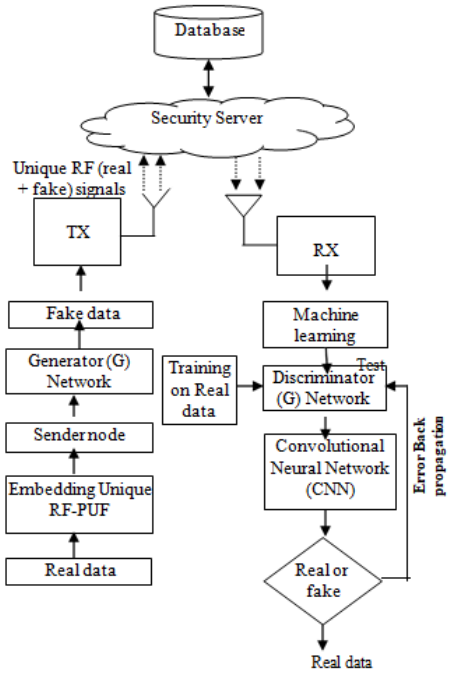

Fig 1. Machine Learning Based WSN Node Authentication and Data Security Framework

- **RUF-PUF Properties :** The efficient properties of PUF are very essential enhancing security and authentication application of proposed system.
- **Constructability:** The creation procedure P is invoked for creation of random PUF intense (P_r €P) where PUF class P is constructible. Create: $P_r \leftarrow$ P. The technical limitations can be exploited by creation of aims in RF-PU for fabrication of physical process in RF transmitters. Creation procedure P itself acts as manufacturing process. P is created for each instance of PUF in RF transmitter.
- **Evaluation:** A random PUF instance (P_r €P) is evaluated for a constructible PUF class P for a random challenge (x). A response y: y ← p can also be evaluated. Eval[$_{pr}$(x)]. The challenge input x is used for bit stream of transmitter in RF- PUF and for each PUF instance y is the unique analog response. Multiple features are attributed by the uniqueness in response.
- **Reproducibility:** A PUF class P can be reproduced if it can be evaluated when the intra-PUF variation probability is less than a system defined number. For RF-PUF, the reproducibility measurement is calculated by the difference among two evaluations ((x), y^1(x)). The difference (D_{intra}) of particular PUF is calculated on a challenge X.

D_i (x) ~ dist [y_1 (x) , y^l(x)]

D_{intra} is the intra chip distance which acts as a parameter for calculation of the resilience of RF-PUF due to changes in environmental condition. D_{intra} =0% is an ideal scenario for reproducibility.

- **Uniqueness:** the uniqueness of PUF class P is evaluated for the inter PUF variation probability is greater that the system defined number. For RF-PUF, the variation of response among two PUF instances derives the uniqueness of PUF instances (Y_1(X), Y_2(X)) which challenge X are evaluated.

D_i (x) ~ dist [y_1 (x) , y_2(x)]

- **Identification:** A PUF class P is simply identified when it is unique and reproducible. The probability of inter-PUF variation is greater than that of intra PUF variation.

($D_{intra} < D_{intra}$) ~ 1

2.2 Data security framework

The Generator network (G) is used to generate false data which is identical with real data samples. Such fake data is passed on to discriminator network (D) from the real distributive data inputs. The distribution of data training is learnt by designing G network whereas probability calculation of original data is designed by D network.

A pair of networks within competitive process results in derivation of back propagation from the network. It can be defined with the following equation

$$min\ G\ max\ D\ =\ x\ \varepsilon\ D\ \log\ D(x)\ +\ x\ \varepsilon\ D\ g\ \log\ (1-D(G(z)) \tag{1}$$

The GANs formal equation is represented with Equation (1).

The generator G passes fake data and real data (x) to D is presented as G(z). The probability of real data p(x) is considered as output. Here the network D is having ability reduce the probability of fake data and improve likeliness for identification of real data. The vector random number (z) is accepted as input by G network. The main intention of suggested system is to baffle the intruder to form identical fake data and real data produced by datasets and sensors. The probability of fake data is minimized to 0 and probability of real data is increased to 1 that helps D recognize real data.

- **Generator Network:** The Generator network (G) can use one sample to create different fake datasets. More specifically, generator does not have access to real datasets. G generates fake data by interacting with D. discriminator can access both fake data from datasets and the real data. Through back propagation error, the generator G obtains capacity to generate better quality fake data. The latent space is mapped to space of data by generator network. The equation that represents the mapping general formula is

g: g(z) $\rightarrow R^x$ where $z \in R^{|z|}$ is the latent space sample where $x \in R^{|x|}$ is data turns into multi layered neural network having θ_g weight. The G network uses Equation (2) to calculate it. G={} is generator output. Instantly generated fake data is represented using M_f by G by using random data samples as input $z = \{z\}_{=1}^{MF}$. The following equation presents G fake data generation.

$$G\ = \sum_{o=1}^{h} \sum_{i=1}^{N}\ ((w_i) + v_0) \tag{2}$$

The hidden neural nodes are represented with *h*, whereas input and output are represented using i and o of the hidden layers. The neural network function activation is represented by f. The input weight of i^{th} hidden node is represented by ω_i. The output weights are presented by β_0, and the threshold value is represented with V_0. Number of neurons of network range (0, 1) is taken as output. Sigmoid is applied on the last layer of activation function. The noise input is of first layer in G is fully connected with (8×5) size is inserted in convolutional layers. Fully connected layers are present in G's architecture.

- **Discriminator Network:** Both real and fake data is collected by the discriminator D which can differentiate between two data types. Both the G and D networks are designed to be compatible which each other. From error back propagation result passed to D network about 150 iterations to retain and update the real and fake data.

The discriminator inputs are defined as

$$D\ =\ \{x_i\}_{i=1}^{N} \tag{3}$$

Where sample datasets are represented by *N*. The following equation defines the discriminator Keras initiation as

$$D = \sum_{o=1}^{h} \sum_{i=1}^{N}\ \beta_0 f(w_i^t\ x_i + v_0) \tag{4}$$

The hidden neural nodes are represented with h, whereas input and output are represented using iand o of the hidden layers. The neural network function activation is represented by f. The input weight of i^{th} hidden node is represented by ω_i. The output weights are presented by β_o, and the threshold value is represented with V_o. The discriminator accepts input datasets as g =

$\{x\}_{i=1}^{MF}$ and D = $\{x\}_{i=1}^{N}$. The real data is taken as 1and fake data is taken as 0 respectively. The probability of newly generated fake data is determined by discriminator in particular intervals of time. D accepts input as real data and G network performs efficiently.

The new generated fake data g and real D datasets are integrated to pass entire data to base station which is the actual destination. The combined data is passed to the base station is defined as

$D = \{\}_{=1}^{+MF}$

Later, it is inserted into other discriminator to identify variation among real and fake data as they are filtered before data transmission. The multiple layers are present in D with weight θd of feed forward in neural network.

3 Results and discussion

In this section, Wireless Sensor Node Authentication Framework Using Machine Learning is implemented. The result analysis of presented approach is evaluated in terms of Probability of False Detection, Reliability and Uniqueness, Delay and throughput.

3.1 Analysis of RF-PUF Based Sensor Node Authentication

By making changes to RF impairments, the MATLAB Neural Network toolbox is used in simulation of RF-PUF and QAM simulation toolbox for the End-to-End mechanism. Variabilities in for manufacture of statistical model and process foundry information of a standard 65 nm technology is included in the simulations. Varying channel conditions required 10,000 PUF instances are used.

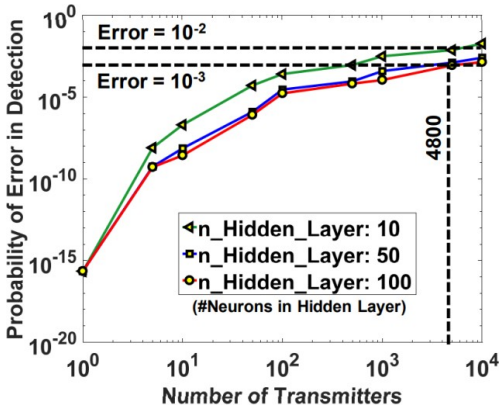

Fig 2. Probability of False Detection Accuracy Vs. Number o f Tx

- **Probability of False Detection:** the accuracy obtained in false detection of Tx device is represented in Figure 2 as a transmitter function in the network. It has error indication in $<10^{-3}$ for 4800 transmitters, and $<10^{-2}$ for 10,000 transmitters. Number of neurons present in hidden layer is increased to 50 from 10. Therefore, accuracy is also enhanced.
- **Reliability and Uniqueness:** Figure 3 presents the Reliability and Uniqueness of RF-PUF w.r.t. the input features provided to the ANN. Unlike a traditional digital PUF with multi-bit output, RF-PUF inherently embeds the unique signature of the Tx in the analog properties of the transmitted message, and hence the Intra-PUF and Inter-PUF distances can be plotted using the normalized parts-per-million (ppm) variation of the input features.

The total number of possible unique PUF samples has to be represented as $\prod_{i=1}^{n} 2^{16}$ (n = number of feature, 2^{16} =possible values for feature i when represented with 16 bits and hence we can intuitively utilize the geometric mean of the ppm values of all the features for a PUF instance. Figure 3 depicts the geometric mean of ppm values of parameters on X-axis for 1000 transmitters in the hardware devices.

The worst case inter-PUF variation for 1000 transmitters is found to be 3.9 ppm, while the corresponding intra-PUF variation is 2.9 ppm. Hence, it is possible to uniquely identify the 1000 transmitters, but the probability of false detection keeps on increasing as the number of transmitters reaches a few thousands, as the difference between inter-PUF distance and intra-PUF distance reduces.

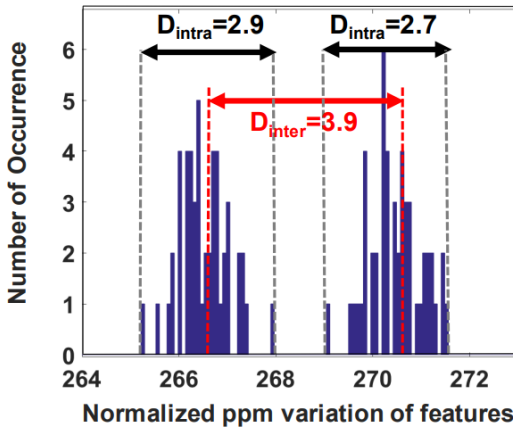

Fig 3. PUF Reliability and Uniqueness Analysis

3.2 Analysis of GAN-based wireless sensor security framework

This section evaluates the performance of our proposed GAN-based wireless sensor security framework and compare is with the present approaches on different scenarios such as throughput and end-to-end delay. The NS2 simulator is used with similar parameters for both approaches. The size of the network is $1500 \times 1500 m^2$ network topology. This network consists of hundred sensor nodes with 40 meters sensor range for 45 minutes of resolution time. 90 static nodes and 10 mobile nodes are present in the network. Malicious nodes passing are dropped at the time of transformation. When dropped packets indication is received, a malicious flag is assigned to the respective nodes by an algorithm. The location of malicious nodes is traced, and they are replaced with static nodes within the network.

- **Throughput:** The data transferred from source node to destination node is called Throughput.

$$Throughout = \frac{Number\ of\ bytes\ received\ at\ RX}{Total\ bytes\ transmitted\ at\ source\ nodes} \tag{5}$$

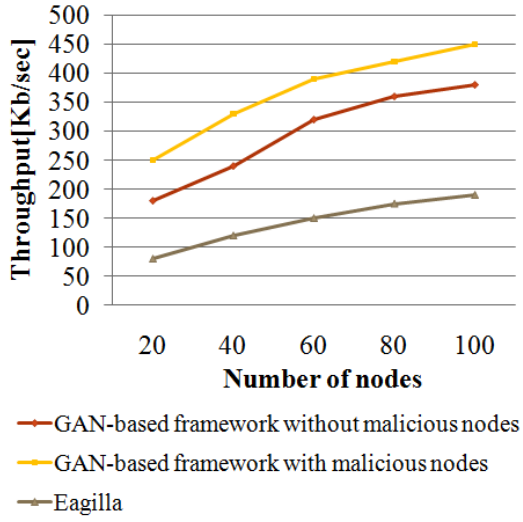

Fig 4. Comparative Analysis of Throughput

Figure 4 shows a comparison of network throughput for each of the three cases. As seen from Figure 4, it is clear that, compared to Eagilla approach, presented approach has high throughput. In Figure 4, the throughput of the network without

malicious nodes is significantly higher than the network with malicious nodes.

- **Delay:** the performance of framework is evaluated by end-to- end delay which is an important parameter for calculation of efficiency. In equation 6, it is noteworthy that the End-to-end delay is obtained by summing the delays of all the nodes and average is calculated for overall nodes. Equation 7 is used for calculating delay of each node and normalized by the total number of packets. The delay is calculated for node j.

$$End\ to\ end\ delay \sum n = \frac{D_{j=1}^{j}}{n} \tag{6}$$

$$D_j = \frac{\sum_{p=1}^{Prt} D_{rec}^{P} - D_{snd}^{P}}{Number\ of\ packets\ by\ node_j} \tag{7}$$

D^{P}_{rec} is transmission time at the source node. The arrival time is represented with D^{i} for destination packet P,

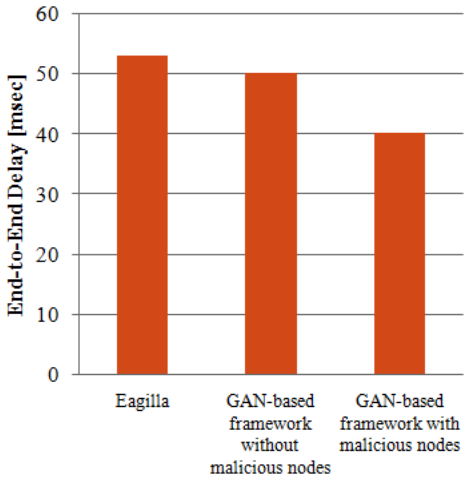

Fig 5. Comparative Analysis of Delay

Figure 5 shows that our GAN-based security framework without malicious nodes has less delay from end-to-end when compared with conventional practice of malicious nodes (SWSNM w/10 MN). The suggested framework is compared with Eagilla approach in respect to end-to-end delay. Compared to Eagilla approach, presented approach has less delay. The novelty of this work is using GAN's for providing security and authentication to wireless sensor nodes. Using GAN, presented approach works efficiently than other earlier approaches. The performance of presented approach is evaluated with and without attacks. Compared to previous works, this approach has achieved better results in terms of delay, throughput, probability false detection and uniqueness and reliability. This approach has achieved very less error indication in $<10^{-3}$ for 4800 transmitters, and $<10^{-2}$ for 10,000 transmitters which is significantly less compared to previous works. In addition, this approach has achieved higher throughout without malicious attacks and it has achieved better throughput with malicious attacks which is better than previous Eagilla approach. Therefore, this approach has obtained better results than earlier approaches.

4 Conclusion

A wireless sensor node authentication and data security framework was presented in this paper using machine learning techniques. A concept called RF-PUF is developed and presented with unsupervised learning for developing a security framework on wireless sensor networks WSN which offers end to end security encryption mechanism. This work explained that RF features of inherent properties are generated through manufacture phase of wireless node can make use of device authenticated strong PUF in IoT network with no requirement of transmitters. Then GAN-based unsupervised machine

learning algorithm is used which has a generator that creates false data in order to mislead the attacker by resolution of imbalanced data for proportion balancing system of data classes. D network is a strongest and clever network that has capability to identify the variation among fake and real data even when they are identical with each other. Simulation results produced by NS2 represents that the efficient security mechanism is generated by this algorithm. From the results it is clear that this mechanism is an efficient technique in reduction of end to end delay and promotes high throughput rate. An authentication method is developed having intrinsic properties with low cost consumption are embedded in RF signal without transmitter expenses in addition. Hence, this framework is proved as efficient and less expensive when compared with conventional practices. This approach overcomes the limitations of earlier Eagilla approach in terms of delay and throughput. In addition, this approach showed significant results without malicious attacks. However, this approach is effective only without malicious attacks. So, in the future, we will implement an approach using deep learning in order to provide better results during malicious attacks.

References

1) Hemanand D, Reddy GV, Babu SS, Balmuri KR, Chitra T, Gopalakrishnan S. An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). *International Journal of Intelligent Systems and Applications in Engineering*. 2022;10(3):285–293. Available from: https://ijisae.org/index.php/IJISAE/article/view/2167.
2) Kumar A, Dhabliya D, Agarwal P, Aneja N, Dadheech P, Jamal SS, et al. Cyber-Internet Security Framework to Conquer Energy-Related Attacks on the Internet of Things with Machine Learning Techniques. *Computational Intelligence and Neuroscience*. 2022;2022:1–13. Available from: https://doi.org/10.1155/2022/8803586.
3) Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan V. Quality of Service aware secure data transmission model for Internet of Things assisted wireless sensor networks. *Transactions on Emerging Telecommunications Technologies*. 2023;34(1). Available from: https://doi.org/10.1002/ett.4664.
4) Xu G, Delima AJP, Machica IKD, Arroyo JCT, He Z, Su W. Improvement of Wireless Sensor Networks Against Service Attacks Based on Machine Learning. *International Journal of Engineering Trends and Technology*. 2022;70(5):74–79. Available from: https://doi.org/10.14445/22315381/IJETT-V70I5P209.
5) Ifzarne S, Tabbaa H, Hafidi I, Lamghari N. Anomaly Detection using Machine Learning Techniques in Wireless Sensor Networks. In: The International Conference on Mathematics & Data Science (ICMDS) 2020 , 29-30 June 2020, Khouribga, Morocco;vol. Volume 1743 of Journal of Physics: Conference Series. ;p. 1–13. Available from: https://doi.org/10.1088/1742-6596/1743/1/012021.
6) Ataelmanan SKM, Ali MAH. Developing a Framework for Data Communication in a Wireless Network using Machine Learning Technique. *International Journal of Advanced Computer Science and Applications (IJACSA)*. 2021;12(3):333–342. Available from: https://doi.org/10.14569/IJACSA.2021.0120341.
7) Devi GSKG, Veni SK, Vidyavathi T, Ahmad SJ. Design of a Compact ISM-band Microstrip Slot Antenna for Wireless Sensor Nodes. *Indian Journal Of Science And Technology*. 2022;15(38):1958–1964. Available from: https://doi.org/10.17485/IJST/v15i38.1678.
8) Chinnaswamy S, Annapurani K. Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks. *Computers & Electrical Engineering*. 2021;91. Available from: https://doi.org/10.1016/j.compeleceng.2021.107130.
9) Prasad R, Das A, Laha R, Mohita, Arijoy. DC-DC Step-Down Converter with Wide Switching Range and Low Ripple Voltage for Wireless Sensor Node Applications. *Indian Journal of Science and Technology*. 2018;11(20):1–5. Available from: https://doi.org/10.17485/ijst/2018/v11i20/109855.
10) Maashri AA, Pathuri L, Awadalla M, Ahmad A, Ould-Khaoua M. Optimized Hardware Crypto Engines for XTEA and SHA-512 for Wireless Sensor Nodes. *Indian Journal of Science and Technology*. 2016;9(29):1–7. Available from: https://doi.org/10.17485/ijst/2016/v9i29/90026.
11) Marathe DS, and UPK. An Optimized Successive Approximation Register used in ADC for Wireless Sensor Nodes. *Indian Journal of Science and Technology*. 2016;9(44):1–6. Available from: https://doi.org/10.17485/ijst/2016/v9i44/102877.
12) Ashok J, Thirumoorthy P. Design Considerations for Implementing an Optimal Battery Management System of a Wireless Sensor Node. *Indian Journal of Science and Technology*. 2014;7(9):1255–1259. Available from: https://doi.org/10.17485/ijst/2014/v7i9.7.
13) Yu D, Kang J, Dong J. Service Attack Improvement in Wireless Sensor Network Based on Machine Learning. *Microprocessors and Microsystems*. 2021;80:103637–103637. Available from: https://doi.org/10.1016/j.micpro.2020.103637.
14) Miranda C, Kaddoum G, Bou-Harb E, Garg S, Kaur K. A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*. 2020;15:2602–2615. Available from: https://doi.org/10.1109/TIFS.2020.2973875.
15) Pandey A, Tiwari LK. Novel Security Framework for Wireless Sensor Networks. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019;8(4):8666–8672. Available from: https://www.ijrte.org/wp-content/uploads/papers/v8i4/D8733118419.pdf.
16) Ramesh S, Yaashuwanth C, Muthukrishnan BA. Machine learning approach for secure communication in wireless video sensor networks against denial-of-service attacks. *International Journal of Communication Systems*. 2020;33(12):e4073–e4073. Available from: https://doi.org/10.1002/dac.4073.
17) Shruthi N, Kousar S, Anitha K. Authentication of node in Wireless Integrated Sensor Networks using Certificate Authority. *International Journal of Engineering Research & Technology (IJERT)*. 2015;3(27):1–4. Available from: https://www.ijert.org/research/authentication-of-node-in-wireless-integrated-sensor-networks-using-certificate-authority-IJERTCONV3IS27141.pdf.