National College of Ireland

Enhancing LoRaWAN security: Authentication strategies to mitigate rogue device infiltration

Industrial Internship

MSc Cybersecurity

Adil Mustafa Khokhawala

Student ID: 22144188

School of Computing

National College of Ireland

Supervisor: Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Adil Mustafa Khokhawala
Student ID:	22144188
Programme:	Masters in Cybersecurity **Year:** 2023
Module:	Industrial Internship
Supervisor:	Jawad Salahuddin
Submission Due Date:	05-01-2024
Project Title:	Enhancing LoRaWAN security: Authentication strategies to mitigate rogue device infiltration
Word Count:	6369 **Page Count** 23

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Adil Mustafa Khokhawala

Date: 04-01-2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing LoRaWAN security: Authentication Strategies to mitigate rogue device infiltration

Adil Mustafa Khokhawala

22144188

Abstract

There is a rapid increase in the development of IOT applications which provides connectivity between devices but exposes them to security threats. LoRaWAN offers low power, cost-effective wireless communications across large networks. Robust authentication is essential for LoRaWAN networks as several vulnerabilities like device impersonation, replay attacks, MITM attacks can disrupt the entire system. This research develops an authentication strategy in which the data packet is appended with a time-synchronized random nonce generator, which is verified at the gateway to authenticate the devices. A proof-of-concept prototype solution was modelled in MATLAB to showcase this functionality. Upon security analysis and evaluation, factors like complexity and data processing time showed significant changes and the risk of spoofing, MITM attack, replay attack, bit-flipping attack have been reduced. The approach in this research does not tamper with the standard operating procedures of the LoRa protocol. Further potential exists to incorporate anomaly detection through machine learning models, and real-world deployments for immediate accuracy.

Keywords: *Authentication, LoRaWAN, Vulnerability, Encryption, Data Rate, MATLAB*

1 Introduction

Background

The Internet of Things (IoT) has brought about an exceptional level of connectivity and data interchange, opening a wide range of applications for smart devices, from industrial automation to smart cities. Within this vast IoT environment, the Long-Range Wide Area Network [LoRaWAN] protocol and Low Power Wide Area Network (LPWAN) technologies have become essential for effective, low-power, long-range communication for IoT devices with limited resources (Seller, 2021)**.** LoRaWAN is a preferred option for many applications, such as asset tracking, smart agriculture, and environmental monitoring, because of its adaptability. The previous decades used SCADA systems (Surveillance Control & Data Acquisition), which are wired systems that aid in data monitoring and infrastructure control. However, after IOT replaced these systems, long range communications, cost-effective solutions could be easily built-in for many organizations.

The Internet of Things (IoT) applications, sensor devices are often situated in uncontrolled environments, exposing them to numerous security threats that can lead to compromised

networks. Businesses frequently prioritize sensor functionality in their engineering efforts while ignoring cybersecurity assessments, risk analysis etc. As a result, there are still vulnerabilities in the IoT ecosystem that include physical tampering, denial-of-service attacks, replay assaults, man-in-the-middle attacks, signal jamming, and node impersonation through cloning etc. which can cause serious repercussions**.**

LoRa architecture

In the IOT ecosystem, the LoRaWAN technology comprises of gateways, central network server and couple of end devices which have sensor nodes that help in data transmission. In this star topology network, end-devices collect data that is transmitted to the gateway that relays the data packets to the application server (network server) for processing. The application server aids in integrity checks, duplicate packet removal, and other crucial procedures that produce the output of the incoming data. As the foundational modulation method for wireless communication between end devices and gateways, the LoRaWAN standard makes use of chirp spread spectrum. The spread factor that is set up determines how many encoded chirps are sent with each symbol in this technology. The channel bandwidth, coding rate, spreading factor, and output power are among the radio parameters that can be adjusted for a LoRaWAN transmitter. To successfully receive signals that are chirped by the sending end-device, the receiving LoRaWAN node at the gateway needs to be configured with the same radio parameters to correctly decode the symbols encoded in those signals. When the spreading factor and other important characteristics match, the receiving entity (which could be a gateway or another end-node) can appropriately decode and transfer the data payload. LoRaWAN networks generally belong to critical applications like temperature monitoring, industrial machinery, heart pacemakers, livestock monitoring, gas monitoring in factories etc. Although different security standards exist in these networks that are provided by the Lora Alliance, there is a need to enhance the authentication of the network, as threat actors can easily evade the current methods used by organizations.

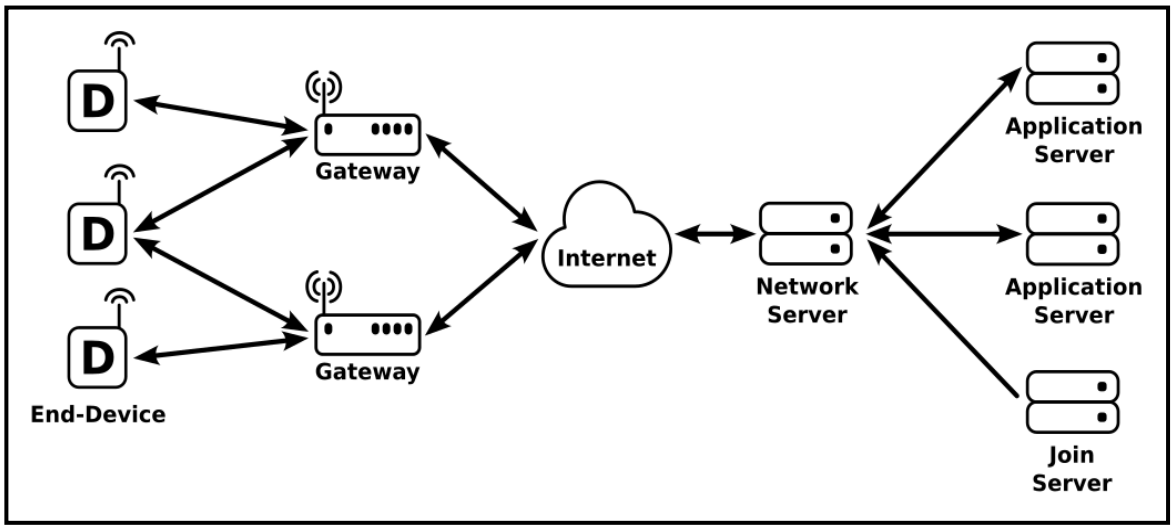


Figure 1: LoRaWAN architecture[1]

[1] https://prbs23.com/blog/posts/getting-started-with-a-private-lorawan-network/

Importance

To solve these issues various security protocols have been designed that provide encryption, authentication, confidentiality, and integrity of the data that is being transmitted around the network. The LoRaWAN protocol is one such media access protocol that is widely renowned for its long-range capabilities and low power usage. For example, in a heart pacemaker machine, the pulse readings need to be extremely accurate as it can determine whether the patient is alive or dead. Even a micro mistake in the readings can cause a serious repercussion to the patient. Similarly, if the data is not authenticated properly at the sensor node, it can be vulnerable to replay attacks, Man-in-the-middle attacks.

The objective of this research is to bridge the gap existing in the authentication schema for LoRaWAN based networks. The novelty of this research is a unique approach for verifying the authenticity of end-devices in the network, by using a time synchronized nonce checker which acts like a multi-factor authenticator present with the sensor node and network server, to prevent rogue device infiltration.

1.1 Research Question

Currently the LoRaWAN protocol authenticates end devices based on serial IDs that come from the manufacturer whilst building the network. This serial ID is verified at the end of the gateway to check whether it is a valid device or not. The major concern that could breach security in this case would be the infiltration of rogue devices that can clone the serial ID and pretend to be a malicious device transmitting and forwarding data in the network. The LoRa alliance, which is a technology alliance that promotes the use of LoRaWAN protocol according to proper standards states that the security mechanisms need enhancement to mitigate such impersonation attacks (LoRa Alliance 2022)[2]. The native device ID check provides insufficient authentication against modern adversaries equipped with software defined radios for launching spoofing attacks. Upon the recent findings, we can see the need to bridge the authentication gap in LoRaWAN based networks. This motivates us to answer the question :

How can LoRaWAN authentication be enhanced to mitigate rogue device entry and maintain network security?

1.2 Report Structure

The report is outlined in 7 sections elucidating the research conducted on authentication enhancement in LoRaWAN. Section 2 talks about the related work in LoRaWAN and the existing authentication schemes, vulnerabilities etc. Section 3 discusses the research methodology that was adopted for achieving the objectives of the research. Section 4 provides the design specifications; section 5 discusses the implementation of the prototype of the authentication mechanism to prevent rogue devices from entering the network. Section 6 talks about the evaluation, and finally section 7 talks about the conclusion and future work of the research.

[2] https://lora-alliance.org/lora-alliance-press-release/lora-alliances-2022-annual-report/

2 Related Work

In the field of security, there is considerable research being done on the LoRaWAN protocol. Several researchers have produced studies that highlight various aspects of security, end-to-end authentication, comparative examination of security protocols, etc. Nonetheless, security plays a crucial role in providing the three pillars of cybersecurity—confidentiality, integrity, and availability (CIA). The literature study delves into great detail about the LoRaWAN protocol, paying particular attention to the current authentication techniques in the market as well as any potential threats or vulnerabilities that might arise and interfere with network data transfer.

This section is structured into various subsections that talk about various existing research conducted prior to our proposed methodology. Subsection 2.1 talks about the comprehensive analysis of the LoRaWAN protocol, Subsection 2.2 discusses the Security vulnerabilities that exist in LoRaWAN, Subsection 2.3 discusses the existing authentication mechanisms in LoRaWAN, and lastly followed by Subsection 2.4 talks about analysis on the proposed solutions in authentication methodologies.

2.1 Comprehensive analysis of LoRaWAN protocol

In the IOT ecosystem, LoRaWAN has gained traction as it provides wide-range, low power wireless communication. LoRaWAN networks have a higher rate of scalability that ease the use of wireless communications over long range (20 km) and provide outputs that don't require high data rates or low latency. Notably, the research conducted by (Abeele, et al., 2017) and (Rahman, et al., 2020) states that the LoRaWAN protocol architecture enables bidirectional communication between endpoint devices and gateways that are connected in a star topology network which helps in optimizing energy efficiency across the network.

LoRaWAN has been popular in the IOT environment because it offers low-power, wide-range wireless communication. According to (Silva, et al., 2017) , offer outputs that don't require high data rates or low latency, and their faster rate of scalability makes it easier to deploy wireless communications across large distances (20 km). The study carried out by (Rahman, et al., 2020) highlights that the LoRaWAN protocol architecture facilitates bidirectional communication between gateways and endpoints connected in a star topology network, hence aiding in the optimization of energy efficiency throughout the network.

(Mehmet Ali Ertürk, et al., 2019), provides a comprehensive overview of the LoRaWAN protocol in which different literature review on LoRaWAN are discussed in detail. The report also talks about various factors in the lora networks which include the network architecture, security, energy efficiency, coverage tests, adaptive data rate etc. The author talks in detail about the security challenges faced by LoRaWAN networks which include vulnerabilities that could lead to attacks like replay attacks, Man-in-the-middle attack, bit flipping attack, jamming attack etc. The report emphasizes the need for implementing robust security measures.

2.2 Security Vulnerabilities in LoRaWAN

According to the research carried out by (Butun, et al., 2018) indicates that LoRaWAN contains several security flaws that an attacker may use to obtain unauthorized access to the network. Threat vectors that can destabilize and ruin a network include device impersonation

(rogue devices), packet manipulation, and information disclosure. Notably, the research conducted by (Naidu & Niranjan K, 2019) discusses the necessity of device authentication in LoRaWAN to safeguard against cyberattacks and add an extra degree of security to individual devices in IOT networks. The authentication methods currently available in the market offer a certain amount of protection, but they are not resilient to rogue devices breaking into the network and delivering fraudulent data to the gateway. It can be extremely challenging for a controller to identify which device in a widespread network is transmitting bogus data that is relayed from node to the central gateway if appropriate authentication mechanisms are not in place.

Research carried out by (Seller, 2021) and (Moraes & A. F. Conceição, 2021) shows that the various security vulnerabilities in Lora networks can corrupt the data passing to the gateway which can cause damaging consequences to the entire network. Device activation methods like OTTA (Over-the-air activation) and ABP (Activation by personalization) provide a secure linking procedure for a LoRa sensor to join a LoRaWAN network. Although this is secure, it is vulnerable to cybersecurity threats like replay attacks, jamming attacks during the activation phase, and threat actors can easily intercept the communication and manipulate the data according to their gain.

There are various issues with the existing authentication methodologies in LoRaWAN networks. The report by (Yang, et al., 2018) and (Elderfrawy, et al., 2019), talks about the drawbacks in the device ID based authentication, that can be easily replicated by a threat actor to replay packet data. This causes an attacker to modify the data packet and send false data to the gateway. Additionally, (Loukil, et al., n.d.) and (Emekcan, et al., 2017) talk about how use of static keys for encryption and authentication cannot evade Bit-flipping attacks and replay attacks. Another research carried out by (Naidu & Niranjan K, 2019) states that replicating sniffed unique identifiers and replaying past packets allows an attacker to impersonate legitimate sensor nodes.

2.3 Current Authentication methods in LoRaWAN networks

Currently, the LoRaWAN standard defines an authentication mechanism for end-device activation by using shared-keys/ derived keys to maintain the secrecy of the data that is being sent to the gateway for processing. The major issue in this type of authentication is that static keys cannot prevent replay attacks, or Bit-flipping attacks. Additionally, anomaly detection methods are also implemented on network level, to prevent misbehaving nodes that send data in varying patterns, which can be assumed as an anomaly. Although this method can prevent such nodes, but it would have lot of false positive cases. (Marin, et al., 2018) discusses about Bluetooth based proximity for confirming the identity of the sensor nodes in the network. External authenticator provides credentials which can be used to authenticate the node in the LoRaWAN network.

According to (Rademachar, et al., 2022) various LoRaWAN networks utilize application layer security controls like TLS certificates, VPN tunnels that connect the gateways to the central infrastructure. This prevents attackers that try to sniff the data during transmission between the gateway and application server. Whereas VPN create an encrypted tunnel in which the data is sent from point A to B, making sure that no attacker can intercept the data packet and modify it. Authentication in many IOT organizations is done on the device ID/serial ID that comes from the manufacturers. This way, the controller can verify the ID of the node and allow the

data to be transmitted till the application server. Although, this method has a major drawback, in which attackers can clone the device ID and replay the packet to send false data.

2.4 Analysis of alternate proposed authentication solutions to enhance LoRaWAN security

(Sanchez-Iborra, et al., 2018) proposed a lightweight symmetric key based mechanism that facilitates authentication by using device-based ID for verification of end-devices without using PKI (Public Key Infrastructure). Symmetric encryption enables faster data transmission compared to that of asymmetric, but it would still be vulnerable to impersonation attacks if the symmetric keys get compromised. The research carried out by (Song & Kim, 2017), designed an architecture for a dual-key schema that separates the network level and application layer authentication. This method creates authentication lists which are cached at gateway for processing data faster compared to the standard lora procedure. It verifies the authenticity of the data at every level; but if there is a breach in the gateway the entire authentication credentials would be exposed leading to exploitable vulnerabilities.

Notably, blockchain has been explore by (Danish, et al., 2019) in which each device contains a proof-of-work token via the immutable ledger for authentication purpose. This enables a clarity in the network, and the controller can easily verify every device through the ledger entries. Although the transparency in the network is increased, but the computational power can increase which can be a major problem for the IOT devices.

The article by (Jabbari & Mohasefi, 2022) proposes a novel protocol for authenticating end-devices and users by using mutual authentication. Although the paper addresses various security issues but provides only a ROR model (Real-or-random) which is yet to be tested for critical IOT applications. The protocol cannot address various security requirements for various applications. The research conducted by (Xing, et al., 2019) introduces a key management strategy which is able to achieve the trade-off between the computational cost, overhead, and security.

Although the existing proposed solutions have various advantages to mitigate vulnerabilities, they lack the authentication measures required to prevent rogue devices from penetrating the network and replaying spoofed data packets to the gateway server. The solutions above majorly rely on cryptographic techniques, where factors like complexity, timestamp, randomness are neglected. It would be easy for an attacker to penetrate a network that does not have a complexity barrier.

3 Research Methodology

This study offers a critical overview of the LoRaWAN protocol and shows how enhancing the authentication process can stop rogue devices from entering the network and sending fraudulent data. Based on the literature analysis, it is evident that there are several vulnerabilities in the LoRaWAN authentication schema that enables attackers to use a non-compliant or rogue device to penetrate through the network and cause havoc. Low computation power, less time for data transmission were given a greater weight in the overall Lorawan architecture than focusing on advanced security features. According to (Heeger & Plusquellic,

2020), cost-effective authentication solutions are required to effectively increase the Lorawan security and create complexity for attackers trying to replay false data in the system.

Specific set of steps were taken in consideration while approaching the novel authentication methodology that could prevent non-compliant/rogue device from entering the Lorawan network, which include:

3.1 Data Gathering

Data was gathered from various research articles, journals that gave insights on the working of the LoRaWAN protocol, parameter required for transmission of data, authentication, encryption, CRC, and other requirements in the protocol. There are several simulators available on the market that can be used to replicate the LoRaWAN protocol, including NS3, MATLAB, and Cooja etc. are present in the market. We chose to use MATLAB because of its well-known simulation setup, which offers signals, drag-and-drop blocks, function blocks, and other features.

3.2 Development of proposed solution

The proposed solution for this research provides an enhanced authentication approach by leveraging various factors to validate the integrity of the packet in the LoRaWAN network and overcome cybersecurity threats. To achieve the solution, we did not make a new authentication protocol, rather we introduced a time-synchronized nonce generator that would generate random bits and append it to the authentication packet. In our methodology, a time-synchronized random seed generator is created, and the produced seed is appended to the authentication packet before transmission to the gateway. This is verified along with the acknowledgement request and the gateway server. The gateway can then verify the authenticity of packet by checking the timestamp of the received packet along with the random nonce that was generated while transmitting the packet. If the sensor node and the gateway have the same timestamp and seed value in the packet, the gateway allows the packet to pass through and go to the application server for processing, otherwise the gateway drops that packet and assumes that the data is being sent from a rogue/malicious device. This helps in maintaining integrity of the packet, and prevents attacks like replay attacks, MITM (Man-in-the-middle) attacks etc.

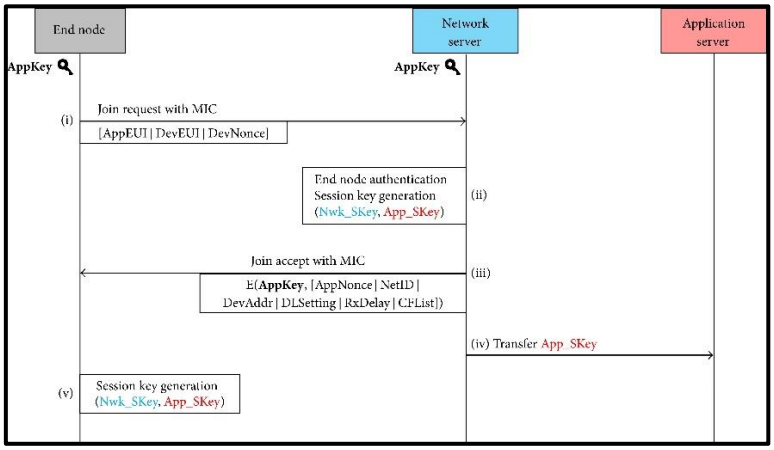


Figure 1: Over the Air Authentication Process

Figure 1 shows the OTA authentication process in LoRa protocol. According to (Song & Kim, 2017) vulnerabilities exist in the join procedures of the LoRaWAN network. This occurs because they use OTAA, as the join request are sent as a non-encrypted message which exposes the device nonce, APPEUI, DevEUI. Notably, this research proposes the authentication of the data packet once the join request has been created, i.e. after the ***AppSecKey, NwsKey*** sends the acknowledgment request, the random seed is appended to that authentication packet. By appending the random seed onto the ESP32 Chip after the acknowledgement request , no rules of the LoRa protocol are altered, which makes our solution effective in case any attacker tries to clone the Device nonce and joins the network.

In section 2.4, the proposed solutions given by researchers do not provide sufficient authentication on the sensor node end for verifying if the data is from an actual node in the network. This is where our novel solution can increase the complexity of the network and add an extra layer of security for the entire data packet before it reaches the network server.

The solutions were discussed with the research team in the Tynatech Ingeneous Ltd. And clearly the company was not interested in making any kind of change in the LoRa chip, i.e. **Prasgate** LoRa Node. The random nonce generator which verifies the authenticity can be added on an external chip which is present between the sensor node and the Prasgate LoRa Node. This will prevent the increase in data rate, computational power and reduce the range to control the Bit Error Rate(BER).

3.3 Simulation Environment Setup

In the next step, we setup a simulation testbed to simulate LoRaWAN protocol for a small network, containing 6-10 nodes. For implementing some MATLAB functions, a licensed version of the software and a hardware operating system with a least 6GB graphics were required. The simulation was carried out using a variety of factors, which include Simulink libraries, MATLAB function blocks, radio signal, and other MATLAB channel blocks.

3.4 Setup for LoRaWAN protocol

The LoRaWAN protocol was implemented to a certain extent in MATLAB using various end-devices (nodes), gateway, channel models, encryption blocks etc. The entire setup had to be configured manually, as MATLAB does not provide libraries for simulating LoRaWAN protocol as a drag-and-drop block in Simulink. We configured the lora transmitter and receiver to make it a functional node. The same was replicated to create multiple nodes that were connected to the central gateway.

A network was created where the nodes are connected in a star topology i.e., all connected to the gateway for data transmission. The nodes present in the network were configured manually, i.e., the transmitter, receiver, and transmission parameters like sampling frequency of 868 MHz, bandwidth of 125kHz, spreading factor that ranged from 7-9, transmission power of 14 dBm etc. were also taken into account. The LoRaWAN network showed a bidirectional communication between the end device nodes and the gateway, and the application server. A network visualization scope was embedded to monitor live traffic and waveform outputs from the node transceivers, providing time domain plots of transmitted and received signals at each device and the gateway. This allowed real-time signal analysis to ensure appropriate modeling of effects like interference and noise within the simulated propagation channel. The output was

in the ***Rx_Signals*** (Received signal) form which showed the communication between the nodes and the gateway.

Below attached is how the transmitter and receiver were connected to a MAC layer to form a complete sensor node.

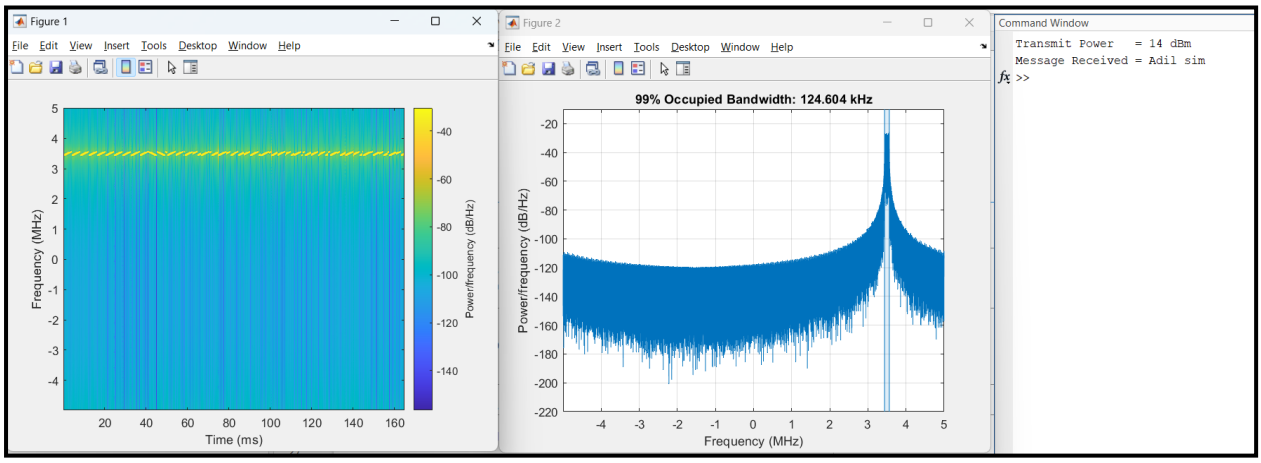


Figure 2: Lora Beacon Simulation

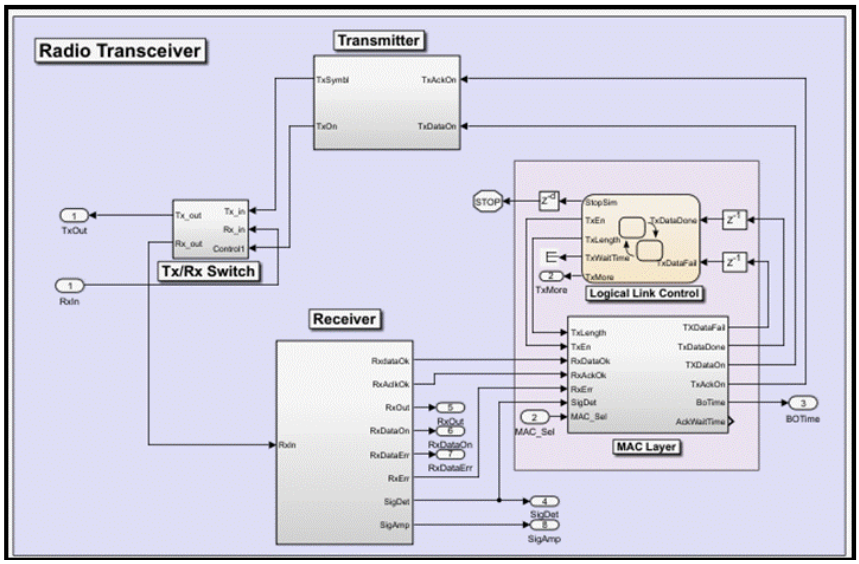


Figure 3: Transmitter and Receiver (Transceiver)

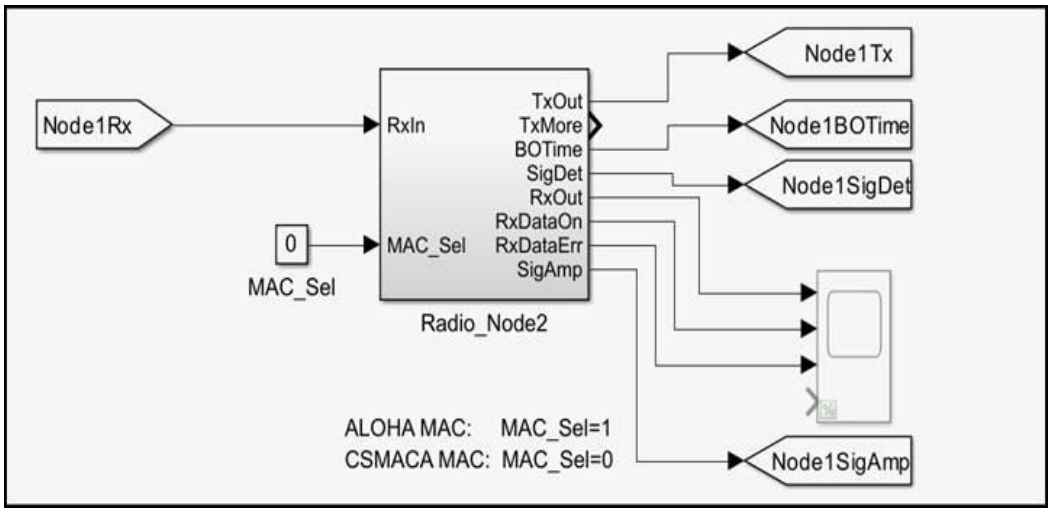


Figure 4: Complete Sensor Node

The nodes present in the system could be easily replicated to form a larger and complex network which could include more end-devices, gateways. This made the simulation-prototype more flexible for enhancing security features on a larger scale.

3.5 Encryption and Chip selection

Encryption is a crucial step in the LoRaWAN protocol, where the data transmitted from nodes undergoes AES encryption in CTR mode in the LoRa Chip. Due to the absence of built-in libraries for AES encryption module in MATLAB, a custom encryption module block was developed for simulation purposes. The code was embedded in the custom block to encrypt the data passing from the sensor node to the gateway. The company burnt the code onto the general purpose ESP32 Chip for implementation purposes.
The ESP32 Chip was selected due to the following features:

- Designed for IOT applications, mobile, hand gear electronics
- Low power [2.2V – 3.6V]
- Adjustable power modes, to prevent increase in computational power
- AES encryption and random nonce generation is supported
- Flash encryption is supported, can incorporate external codes onto the chip

4 Design Specification

This section of the report provides an overview of the design specification for achieving the objective of the research. The proposed solution ***does not change any rule/standard in the LoRa protocol***; but simply provides an additional security complexity layer before the data reaches the gateway for further processing. The architecture diagram below explains the flow of data from the sensor node till the gateway and shows how our proposed solution helps in enhancing the security and complexity of the authentication schema for the LoRaWAN network. The proposed authentication mechanism flow :

- The sensor nodes (End-devices) generate a random seed value using the random seed generator, which is appended to the authentication packet after the acknowledgment request.

- This entire process is flashed on the ESP32 Chip, which takes the authentication packet and passes it on for the LoRa AES encryption.

- Once the data is encrypted and sent to the gateway, the gateway verifies the data packet, and checks the frame for the random seed value sent initially.

- If both the values match and the timestamp is below 5 minutes, it allows the packet to pass through and reach the application server for processing. (NOTE: the random seed value should be valid within the timestamp generated)

- If the values don’t match , or the timestamp is exceeded, the gateway will discard the packet and display ‘Invalid Packet’.

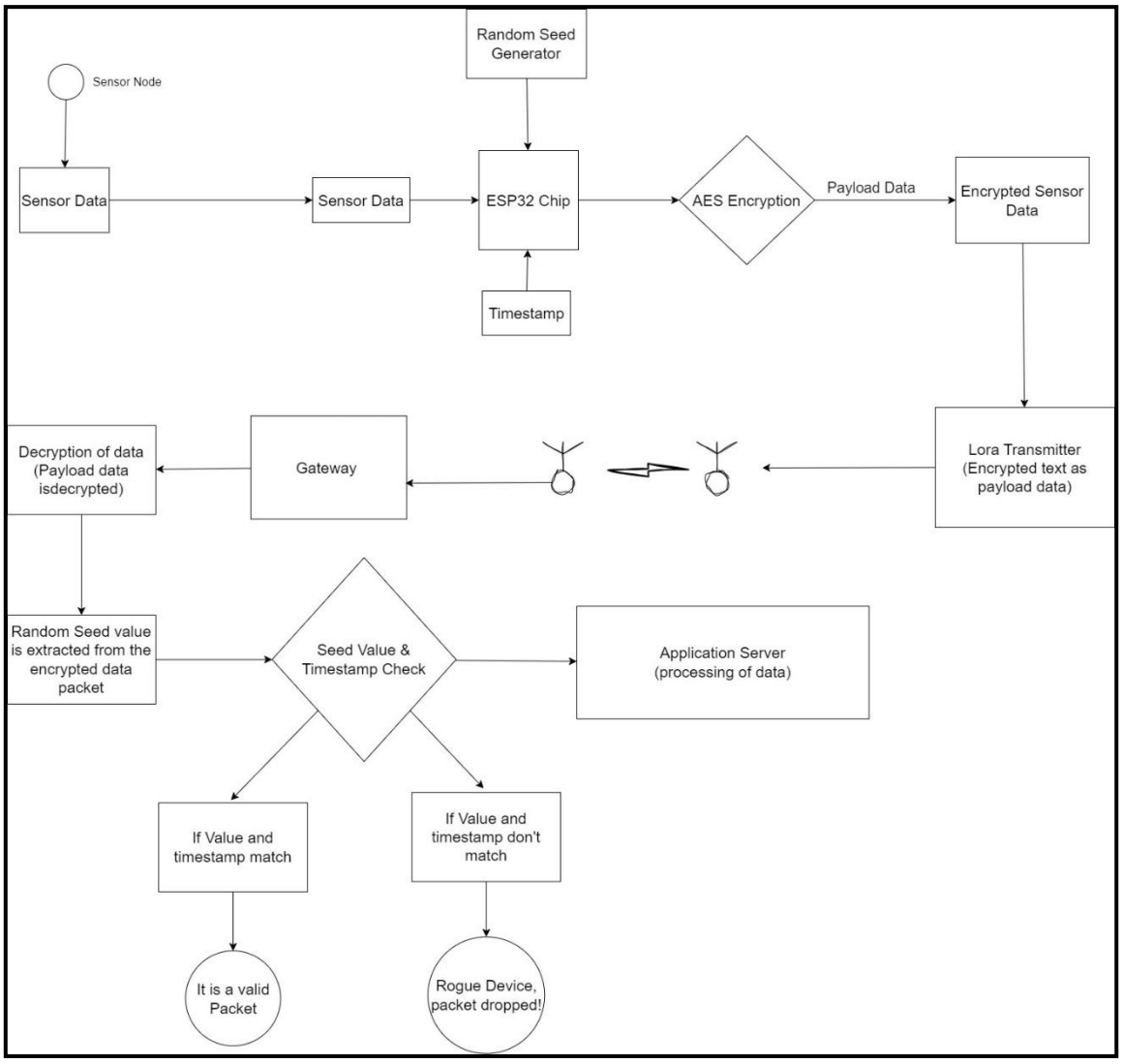


Figure 5: Architectural Design

5 Implementation

The section contains the discussion on how the proposed solution was implemented to enhance LoRaWAN Security.

5.1 Tools Used:

This section talks about the list of tools used to achieve the objectives of this research.

5.1.1 Hardware Specifications:

To conduct the simulation for the research the minimum requirement would be an Intel Core i5 processor Computer system, 8 GB RAM, 6 GB graphic card and a storage space of at least 10 GB.

5.1.2 Software Tools:

In this research, ***MATLAB version R2023a*** is the primary software used for simulating the entire LoRaWAN network. Additionally, C programming language was used to develop the AES encryption module for the Lora Chip encryption. The code is burnt on a general purpose ESP32 chip, which was tested by Tynatech Ingeneous.

5.2 Poc Implementation

To achieve the objective of the POC of the proposed solution for our research problem, we create an authentication schema that helps in verifying the authenticity of the end-devices during transmission in the network. A bidirectional communication takes place between the sensor nodes and the gateway, in which the data packet undergoes AES encryption according to the LoRa standards. **Figure 6** below shows how the data is passed on from the transmitter of every node in the network to the gateway, and similarly on the other end the gateway can send data to the receivers of the sensor nodes. Every node in the network contains a sensor data that passes through various channels like Rayleigh SISO, AWGN and reach the gateway.
Notably, refinements of the authentication mechanism for real-world deployment would require a physical hardware-based implementation in accordance with the LoRa alliance protocol.

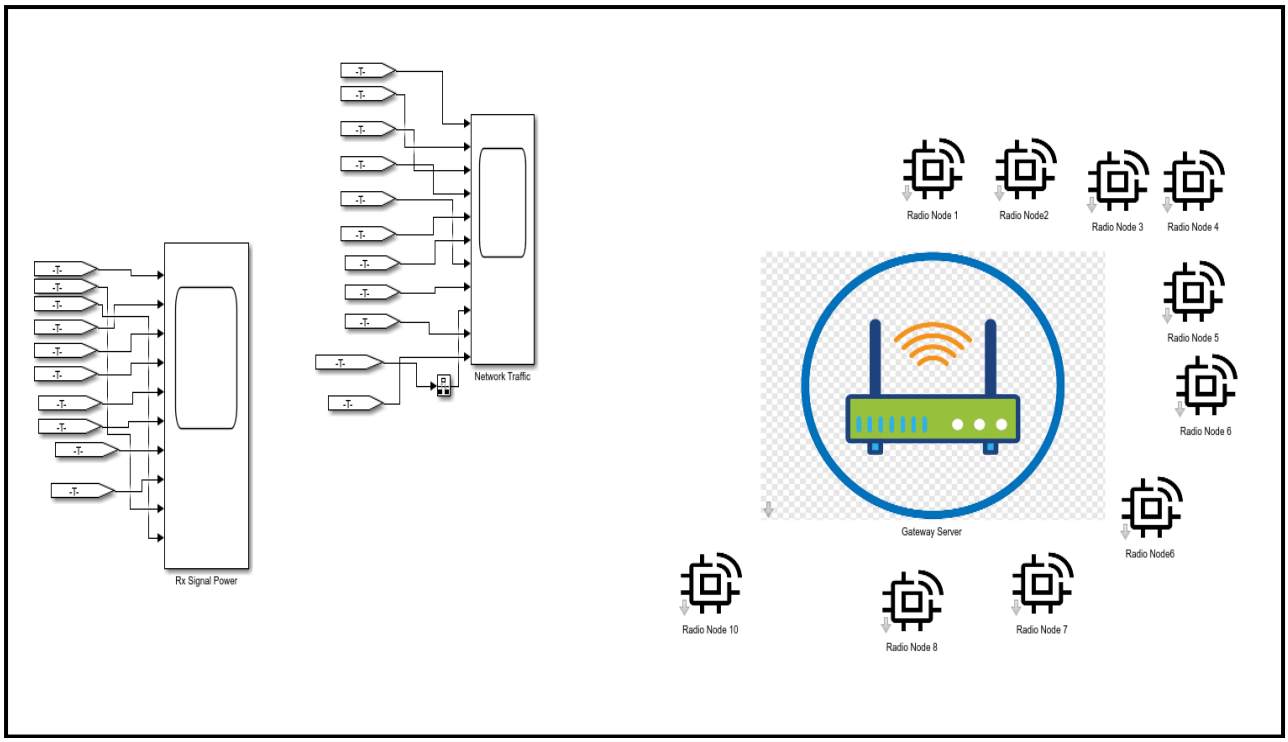


Figure 6: LoRa Network with 10 nodes

Our proposed solution generates a random seed value which takes place before the encryption of the packet reaching the gateway. The random nonce generates a random bit value which is appended to the authentication packet and sent forward for transmission. The random nonce acts like an authenticator which verifies if the packet is coming from a genuine device or a rogue/non-compliant device.

<nonce value>	b'53027dz12c5oJzqRLMrRU0mRz3128930dd3f52e3ea'

Figure 7 : Authentication packet

91b'53027dz12c5oJzqRLMrRU0mRz3128930dd3f52e3ea'

Figure 8: Appended packet sent for further transmission.

Figure 8 shows the authentication packet, in which an *8-bit nonce* is sent along with the packet to the gateway. The purpose for using a time-synchronized random seed generator is to add a layer of complexity in the packet which makes it difficult for an attacker to intercept the data in the network, and perform attacks like replay attack, bit-flipping attack, Man-in-the-middle attack etc. In these attacks the prime goal of the attacker is to manipulate the data that is being sent to the gateway and send false data, which makes the controller on the gateway end think that the data is received from a genuine sensor node in the network. For our research purposes, we have demonstrated the proposed solution occurring on a single node packet.

Ideally, the random number generator is time-synchronised which verifies the identity of the device/packet based on two factors : timestamp, value of the nonce appended. Both, the sensor node, and gateway have this generator to verify the values sent and received on the gateway end. The demonstrated results show no sign of time generation, as MATLAB does not support time generation and parallel processing. Therefore, we have shown a prototype of how the proposed solution would work in the real-world scenario.

Figure 9 below is a snapshot which shows the output of the scope in the LoRa network. In the 10 Node network, every node transmits data and sends it to the server in time domain. The signals show the nodes sending data to the server, and the gateway block plots the received network traffic from all the nodes (Node1- Node10).

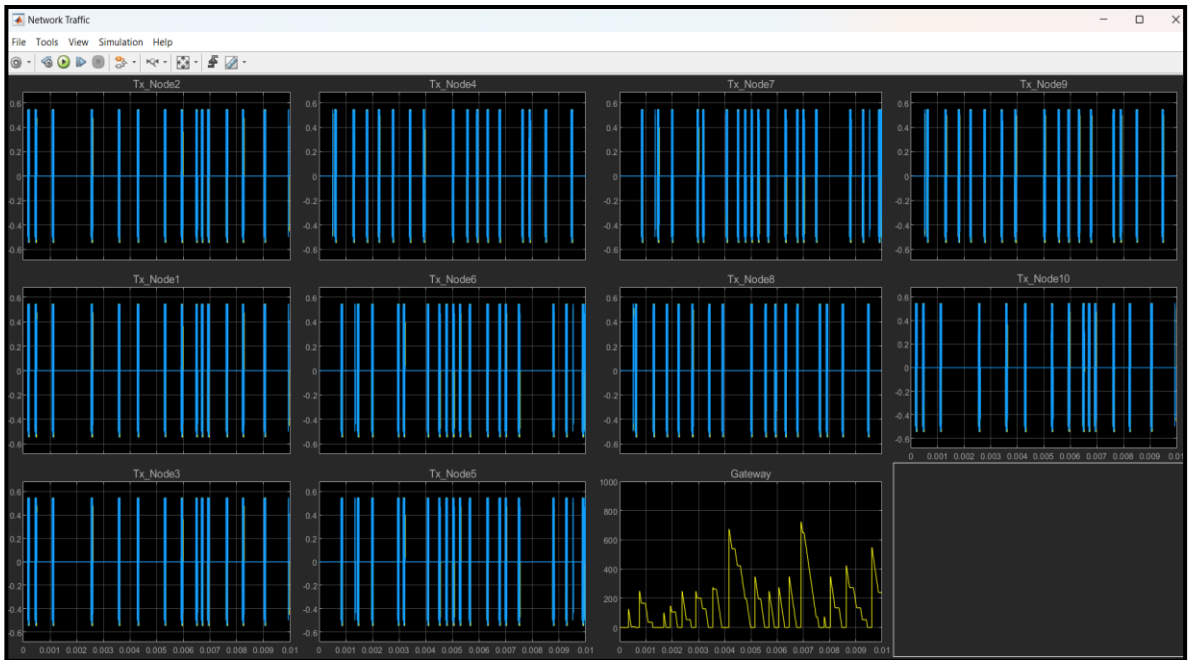


Figure 9: Transmitted Signals

Figure 10 shows the output in the form of plotted signals of received power at the nodes for the acknowledgement frame in the time domain.

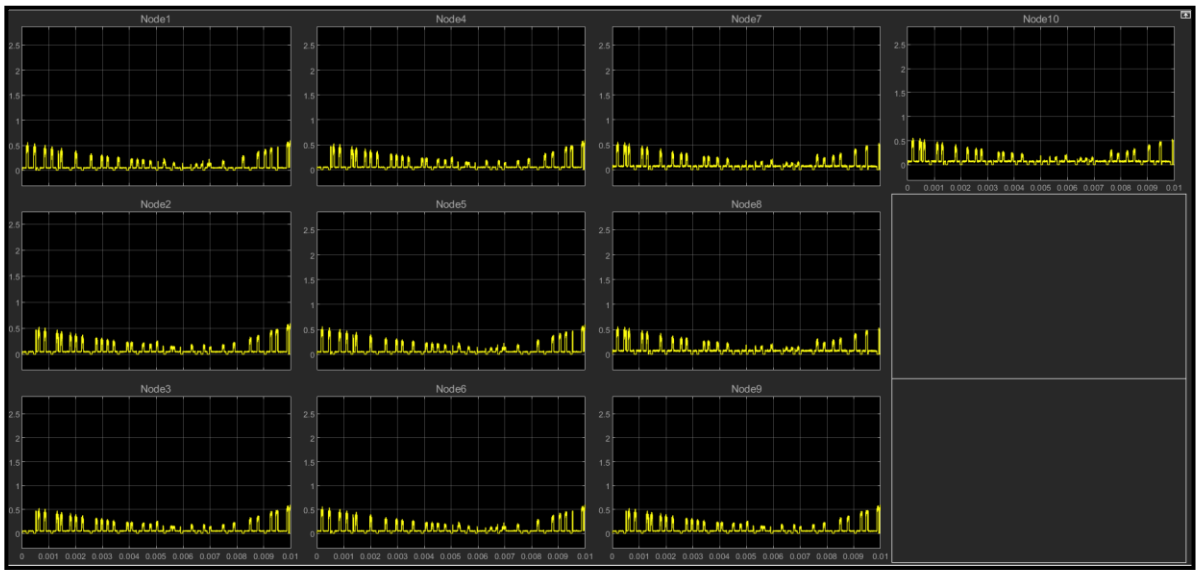


Figure 10: Received Power

5.3 Physical Implementation

The Physical implementation of the proposed solution was carried out by the company. The random nonce generator along with the authentication packet was integrated with the ESP32 Chip on the end-device end (sensor node). Additionally, the random seed is appended to the data packet along with a timestamp and random feed is passed on to the LoRa Node for encryption (AES encryption).

Similarly, the gateway server also has the time-synchronized random nonce generator. When the data reaches the gateway, a ***'CHECK'*** occurs, i.e. the seed value is checked after extraction of the random seed along with the timestamp. If the value match, the packet is allowed to pass through to the application server, else it discards the packet ad displays "Rogue Device, Packet Invalid". To implement the entire process in a real-world deployment, the standard operating procedure needs to be in accordance with the LoRa Alliance.

6 Evaluation

6.1 Aim & Methodology

The goal of this research was to create an authentication strategy that enhances the LoRaWAN security and prevents cyber-attacks like Man-in-the-middle attack, Bit Flipping attack, Replay attack. To achieve this a prototype simulation has been carried out on MATLAB to check the feasibility of the solution. Additionally, physical implementation trials have been performed by embedding the time-synchronized random nonce generator code into the ESP32 chip and Prasgate LoRa Node. The real-working implementation of the Poc of the proposed solution was evaluated by the company Tynatech Ingeneous. The main factors for evaluation were Latency, time penalty, data rate, range of transmission etc.

6.1.1 Evaluation Results

After conducting the Poc of the proposed authentication mechanism, we ended up with results showing some changes in the field of latency, data processing time, range, complexity, time penalty. Below is the list of critical observations after conducting the implementation :

- Latency : There was no significant change in the latency of the data.
- Data Processing Time : There was significant increase in the data processing time, as the data packet was appended with the random seed value before reaching the gateway server, and then it was verified by the gateway to prevent rogue device from entering the network.
- Range : No significant changes in the range.
- Complexity: The complexity of the network increased, as our proposed solution adds an extra layer of security, which makes it difficult for an attacker to intercept the packet and replay bogus data to the gateway.
- Time penalty: There was an increase in the time penalty of the data packet as it would undergo verification at the gateway end. The time penalty applies to the threat actor as well, i.e. they would not get enough time to manipulate the data packet and forward it in the network, as the random nonce generate is time synchronized.

The physical implementation trial results are evaluated by the company, below are the results:

TYNATECH

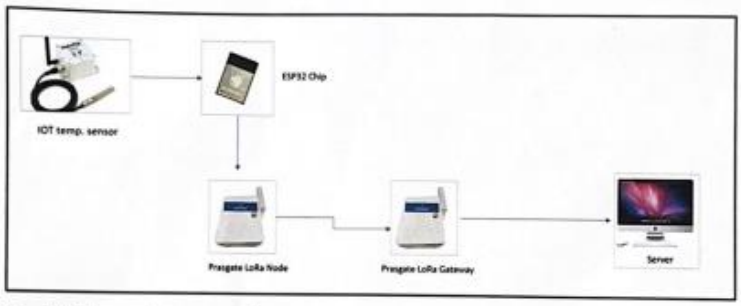
EVALUATION REPORT

Aim: The aim of the physical trials is to evaluate the time-synchronous authentication scheme for the LoRaWAN protocol.

Objectives: The objectives of the trials were as under: -

(a) Time-synchronized random nonce generator for improvising authentication at sensor end.
(b) Calculate time required for processing of the frame at the esp32 chip.
(c) Calculate time required for processing of the frame at the server end.
(d) Calculate battery drain after 1 hr of continued operation at the sensor end.
(e) Check the complexity of the network after the implementation of the authentication scheme.

Setup: The setup of the trial was as under: -

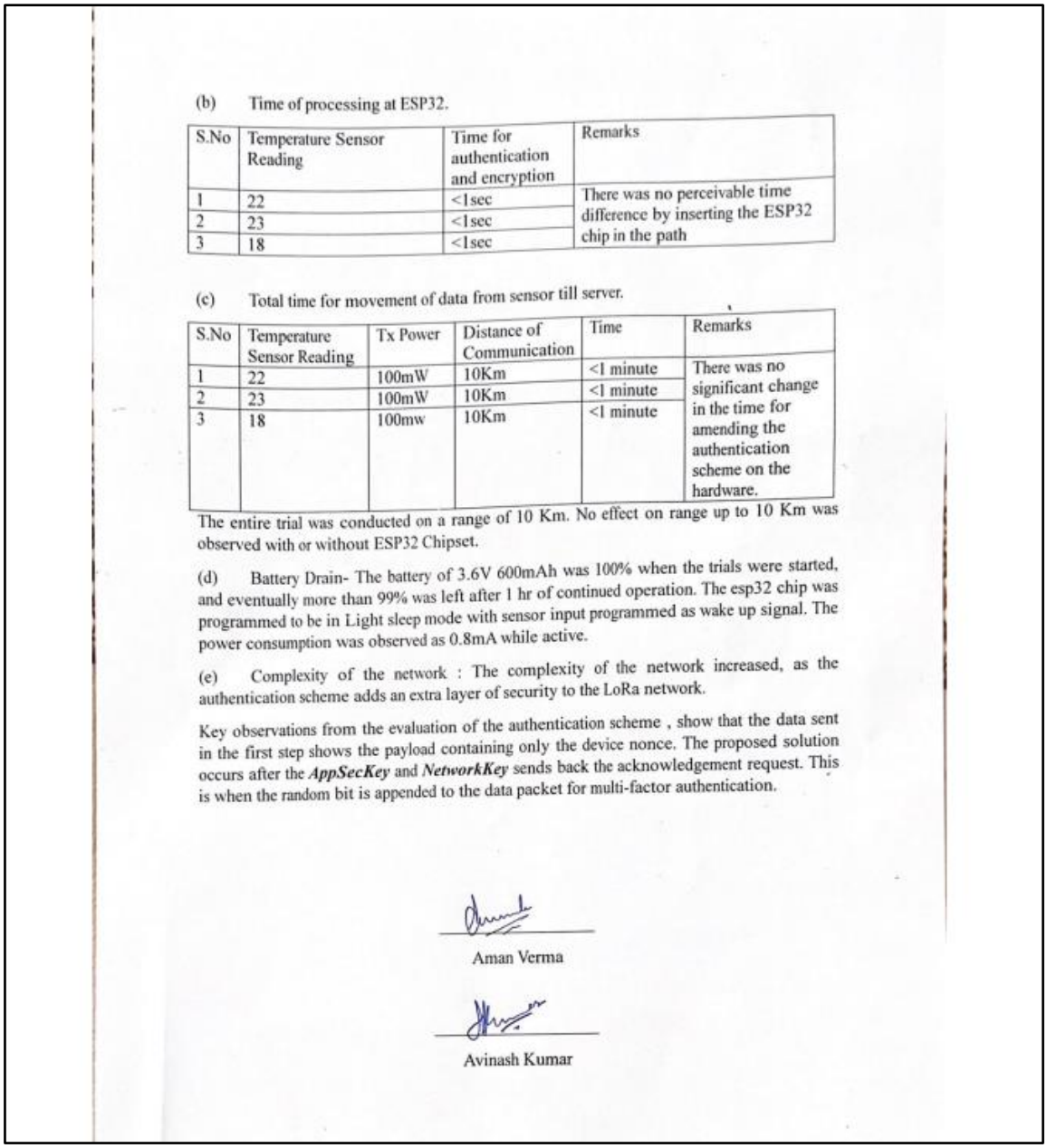


Results: The results are as under: -

(a) Time-Synchronous Random Seed Generator

S.No	Temperature Sensor Reading	Authentication after ESP 32	Verification of authentication at the server	Remarks
1	22	Yes	No	Changes were made at the gateway end to extract the random number from the original message.
2	23	Yes	Yes	
3	18	Yes	yes	

The random nonce generation code worked as expected. The random bits were successfully appended to the packet and sent to the gateway; verification at gateway end also was processed.



(b) Time of processing at ESP32.

S.No	Temperature Sensor Reading	Time for authentication and encryption	Remarks
1	22	<1sec	There was no perceivable time difference by inserting the ESP32 chip in the path
2	23	<1sec	
3	18	<1sec	

(c) Total time for movement of data from sensor till server.

S.No	Temperature Sensor Reading	Tx Power	Distance of Communication	Time	Remarks
1	22	100mW	10Km	<1 minute	There was no significant change in the time for amending the authentication scheme on the hardware.
2	23	100mW	10Km	<1 minute	
3	18	100mw	10Km	<1 minute	

The entire trial was conducted on a range of 10 Km. No effect on range up to 10 Km was observed with or without ESP32 Chipset.

(d) Battery Drain- The battery of 3.6V 600mAh was 100% when the trials were started, and eventually more than 99% was left after 1 hr of continued operation. The esp32 chip was programmed to be in Light sleep mode with sensor input programmed as wake up signal. The power consumption was observed as 0.8mA while active.

(e) Complexity of the network : The complexity of the network increased, as the authentication scheme adds an extra layer of security to the LoRa network.

Key observations from the evaluation of the authentication scheme , show that the data sent in the first step shows the payload containing only the device nonce. The proposed solution occurs after the ***AppSecKey*** and ***NetworkKey*** sends back the acknowledgement request. This is when the random bit is appended to the data packet for multi-factor authentication.

Aman Verma

Avinash Kumar

Figure 11: Tynatech Evaluation Report

6.2 Application

- Practical Application : From a practical view, the proposed solution provides an additional security layer for the sensor node data and provides authentication in the network. Our solution does not alter any rule of the Lora protocol. Notably, the solution can be incorporated on small to medium sized networks for achieving accurate results.

- Academic Application: This research contributes the research area of Authentication in LoRaWAN networks, and actively talks about the existing research that have been conducted, and how our solution is feasible for authenticating the data to prevent rogue device infiltration in the network.

7 Conclusion and Future Work

The research presented an authentication method for hardening the security against the intrusion of rogue devices in LoRaWAN networks. A prototype solution was implemented which increases the security complexity of the network by adding a random seed value to the authentication packet transmitted between the end-devices and the gateway. With the help of this approach, a gateway controller would have no trouble determining if data flowing from end devices is from rogue or verified devices. Before sending the incoming data packet to the application server, the gateway can authenticate it by validating the nonce using its own time-synchronized random nonce generator. Our solution provides an additional degree of security beyond the existing device ID based authentication in LoRa networks.

Some of the key challenges faced in this research was the time constraint to implement the entire LoRaWAN protocol-based network. Additionally, MATLAB stopped supporting the Lora blocks in Simulink. Also, MATLAB does not support parallel processing due to which the time-synchronized generation of the nonce could not be demonstrated in the prototype created in the research. However, the entire model was created by using alternate channels, radio signals which helped gain the visualization of how a LoRa network would work.

In conclusion, the proposed solution answers the research question and leverages factors like *timestamp, complexity barrier* to prohibit rogue devices from penetrating the network to replay false data to the gateway.

There are still more enhancements that might be added to this study, such simulating a genuine LoRaWAN network with endpoints and gateways to confirm the experiment's assessment in the real world. Furthermore, training models on typical end-device traffic patterns can be created to monitor potential network anomalies, and machine learning can be incorporated to dynamically modify threshold values in an effort to increase the localization accuracy. Notably, the random seed generator can be modified to store at least 200 seed values, so that there is no repetition of the seeds. This will prevent threat actors from sniffing the pattern of the generated nonce with the authentication packet.

The proposed solution has been appreciated by the company, the appreciation letter by the company is enclosed below :

TYNATECH

Tynatech Ingenious Private Ltd. LOGIX TECHNOVA, B606 Block B, Sector 132, Noida, Uttar Pradesh 201301

Dear Adil Mustafa Khokhawala,

I wanted to send my sincere appreciation for all your hard work during your internship with our company Tynatech Ingenious Private Ltd. . In these past few months, you contributed excellent efforts that demonstrated strong potential to thrive in wireless connectivity roles long-term. The solution proposed by you for securing it has a strong potential to be used in the interim till a comprehensive solution is approved by the LoRa alliance.

During your internship, I was thoroughly impressed with your high uptake level and eye for details in LoRaWAN protocol architecture, security standards, and hands-on development experience with LoRa transceivers. Your support ensured smooth upgrades for several gateways, solving repetitive issue arising in tickets, and client handling skills were excellent.

As you wrap up at Tynatech Ingenious Private Ltd. to head back for your final semester, I wish you the very best in your studies and future aspirations in IoT. Please do stay in touch, and don't hesitate to reach out if you ever need a professional reference or want to discuss potential return opportunities post-graduation. You've demonstrated the capabilities and motivation to accomplish great things, and I'm sure you would be a great asset to any organization.

Sincerely,

Ravikant Rai

CTO

Tynatech Ingenious Private Ltd.

Figure 12: Appreciation Letter

8 References

Abeele, F. V. d., Haxhibeqiri, J., Moerman, I. & Jeroen Hoebeke, 2017. Scalability Analysis of Large-Scale LoRaWAN Networks in ns-3. *IEEE Internet of Things Journal,* 4(6), pp. 2186-2198.

Butun, I., Pereira, N. & Gidlund, M., 2018. *Security Risk Analysis of LoRaWAN and Future Directions,* s.l.: Future Internet .

Danish, S., M, R., M, L. & Qureshi, H. K., 2019. A Lightweight Blockchain Based Two Factor Authentication Mechanism for LoRaWAN Join. *Journal of Network and Computer Applications,* Volume 2.

Elderfrawy, Butun, M., Periera & N.&, G., 2019. Formal Security Analysis of LoRaWAN. *Computer Networks,* Volume ELSEVIER, p. 148.

Emekcan, A., Ramchandran, G., Hughes, D. & Lawrence, P., 2017. *Exploring The Security Vulnerabilities of LoRa.,* s.l.: IEEE.

Heeger, D. & Plusquellie, J., 2020. *Analysis of IOT Authentication Over LoRa,* Alberqueue: IEEE.

Jabbari, A. & Mohasefi, J. B., 2022. A Secure and LoRaWAN Compatible User Authentication Protocol for Critical Application in IOT environment. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS,* 18(1).

Loukil, S., Fourati, L. & Nayyar, A., n.d. Investigation on Security analysis of LoRaWAN networks: COmpatibility scenarios. *IEEE Express,* Volume 10, pp. 101825-101843.

Marin, E., Singelee, D., Ackermann, L. & Preneel, B., 2018. On the Feasibility of Cryptography for a Multi-Vendor LoRaWAN Network. *Mobile and Ubiquitous Systems: Computing, Networking and Services,* Issue 10.4108, pp. 289-298.

Mehmet Ali Ertürk, Muhammed , A. A. & Muhammet , T. B., 2019. A Survey on LoRaWAN Architecture, Protocol and Technologies. *Future Internet,* Volume 11, p. 216.

Moraes, P. d. & A. F. Conceição, 2021. *A Systematic Review of Security in the LoRaWAN Network Protocol,* s.l.: arXiv.org.

Naidu, D. & Niranjan K, R., 2019. *Review on Authentication Schemes for Device Security in LoRaWAN,* s.l.: IEEE.

Rademachar, M., Linka, H., Jonas, K. & Hosrtmann, T., 2022. *Bounds for Scalability of TLS over LoRaWAN,* s.l.: Research Gate.

Rahman, H. U., Mudassar Ahmad, Haseeb Ahmad & Muhammad , A. H., 2020. *LoRaWAN: State of Art, Challenges, Protocols, Research Issues ,* s.l.: IEEE.

Sanchez-Iborra, R. et al., 2018. Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach. *Sensors,* 18(6).

Seller, O., 2020. *LoRaWAN security* , s.l.: IEEE.

Silva, J. d. C., Antonio M. Alberti, Petar Solic & Andre L. L. Aquino, 2017. *LoRaWAN — A low power WAN protocol for Internet of Things: A review and opportunities,* s.l.: IEEE.

Silva, J. d. C. & Joel J. P. C. Rodrigues, 2017. *LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities,* s.l.: Research gate.

Song, J. & Kim, J., 2017. A Dual Key-Based Activation Scheme for Secure LoRaWAN. *Advanced Wireless Communications and Mobile Computing Technologies for the Internet of Things,* Volume 2017.

Xing, J., Zhang, K. & Zheng, K., 2019. *An Improved Secure Key Management Scheme for LoRa System,* s.l.: IEEE.

Yang, X., Karampatzakis, E., Doerr, C. & Kuipers, F., 2018. *Security Vulnerabilities in LoRaWAN,* Netherlands: Cyber Threat Intelligence.