A comprehensive security approach to mitigate Replay and MITM attacks in LoRaWAN protocol

Industrial Internship

MSc Cybersecurity

Roopesh Srivastava

Student ID: 22164162

School of Computing

National College of Ireland

Supervisor: Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Roopesh Srivastava		
Student ID:	22164162		
Programme:	Masters in Cybersecurity	**Year:**	2023-24
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:	6804	**Page Count**	25

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: Roopesh Srivastava

Date: 05/01/2024

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):	

A comprehensive security approach to mitigate Replay and MITM attacks in LoRaWAN protocol

Roopesh Srivastava

22164162

Abstract

The development of numerous new Internet of Things (IoT) applications have been made possible by low-power, long range wide-area technology (LoRaWAN), which provides energy and cost-efficient wireless connectivity for large deployments of autonomous sensors. The security of LoRaWAN operating in the license-free frequency band, has received somewhat limited attention and numerous investigations have identified security flaws that makes it susceptible to network attacks such as Replay, Man in the Middle (MiTM) and bit-flipping attack. Current research has identified that LoRaWAN in its present form lacks synchronization between communicating parties, has a vulnerable key management and encryption process. The research has proposed an improvement in the form of dual encryption and time stamp-based synchronization check, which tends to negate these network attacks. This approach neither tampers with the core of the LoRaWAN nor the recommendations of the LoRa Alliance. The approach will lead to enhanced attack detection and mitigation capability of the protocol and make it robust for critical nodes and applications.

Keywords: *LoRaWAN, MATLAB, MiTM, Replay attack, Bit flipping Attack, Vulnerability, Encryption***.**

1 Introduction

Wireless technologies have become a disruptive force in the constantly changing communication and networking landscape, changing how we engage with the digital world. Wireless technologies have overcome the limitations of wires, requirement of new infrastructure, which in the concrete urban world is difficult to achieve (Editor, 2021). Thus, providing seamless and untethered communication with flexibility, scalability, and mobility, in contrast to traditional wired systems that rely on physical connections. Data, voice, and video can be transmitted over airways using a wide range of protocols and standards, which have grown integral to our everyday lives. From the pervasive Wi-Fi networks that power our homes and offices to the complex cellular networks that enable worldwide mobile communication, Wireless technology is fundamentally about breaking down physical constraints to offer mobility, flexibility, and accessibility on a never-before-seen scale.

During the last two decades, industries have developed wired Supervisory Control and Data Acquisition (SCADA) Systems to monitor and control the infrastructure. These systems included a sensor (essentially a Transducer) connected to wired technology to remotely transmit environmental and operational data enabling the industries to centrally manage the infrastructure (Wangsness, 2023) . This, however, had limitations of distance and required huge Capex and Opex. Advancement in Wireless technology and the concepts of SCADA were eventually amalgamated, and the Internet of Things (IoT) was developed, which provided a suitable low-cost alternative.

The Internet of Things (IoT) 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. However, the reliability of IoT was still in doubt and thus the research endeavors over the years were aimed at increasing the reach, data rate, making the communication lightweight and finally ensuring the CIA (Confidentiality Integrity and Availability), while retaining the benefits of IoT. The Long-Range Wide Area Network [LoRaWAN] protocol and Low Power Wide Area Network (LPWAN) technologies emerged as frontrunners because of its long-range and energy-efficient characteristics and has become a key communication standard in this dynamic terrain (Aras, et al., 2017). Numerous Internet of Things applications, such as asset tracking, smart cities, and environmental monitoring, are made possible via LoRaWAN.

As proliferation of IoT devices increased and IoT networks started sending increasingly valuable data, the protocol garnered attention of nefarious actors and serious vulnerability also come to light. Further the very nature of its unmanned deployment, exposes them to numerous security threats that can lead to compromised networks. The balance between functionality and security is seldom achieved and thus often sensor functionality is prioritized in engineering efforts while ignoring comprehensive cybersecurity readiness. Consequently, the protocols continue to have vulnerabilities such as physical tampering, denial-of-service attacks, replay attacks, man-in-the-middle (MiTM) attacks, bit flipping attacks, signal jamming, and node impersonation through cloning etc. which can lead to serious repercussions in critical applications (Aras, et al., 2017) (Coman, et al., 2019). This research primarily focuses on devising solutions for mitigating MiTM and Replay attacks in LoRaWAN protocol.

1.1 LoRaWAN Architecture

The LoRaWAN network architecture comprises of central network servers, Gateways and multiple end devices which have sensors, organized in hierarchical star topology. The sensor measures the data and passes to the LoRa node which essentially creates a frame by adding the header required for the protocol to function and transmits it to the gateway through RF transmission. The data is encrypted using AES symmetric encryption and encapsulated in the payload field and a CRC check is appended at the end of the frame. Thus, protocol caters for confidentiality and integrity, though loosely. The node is authenticated via an offline activation or through an OTAA (Over the air authentication) process. The gateways act as intermediary nodes to relay data from multiple nodes to the central servers. The application servers perform integrity checks, duplicate packet removal, data decryption, node identification and other crucial procedures to extract the output from the incoming frame. The frames are transmitted in air using RF spectrum at 868 MHz with bandwidth of 125KHz. The modulation used between end devices and gateways is chirp spread spectrum. The spread factor that is set up determines how many encoded chirps are sent with each symbol. The channel bandwidth, coding rate, spreading factor, and output power are among the radio parameters that are adjusted for a LoRaWAN transmitter and receiver. When the spreading factor and other RF characteristics match, the receiving entity (which could be a gateway or central node) can appropriately decode the data payload.

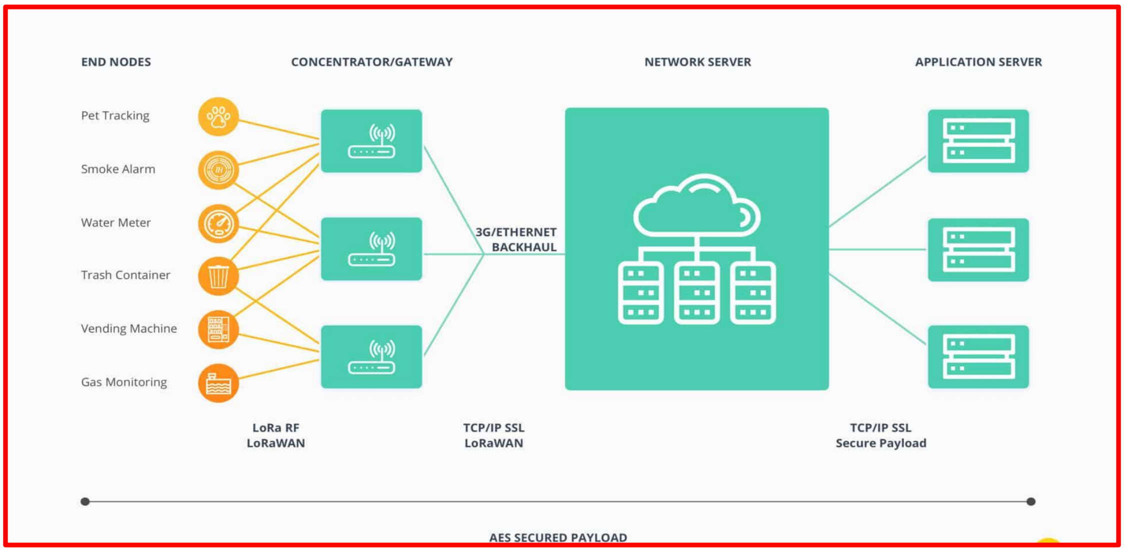


Figure 1: LoRaWAN Network Architecture (Wedd, 2020)

1.2 Importance of Research

Critical IoT applications such as temperature monitoring, industrial machinery, heart pacemakers, livestock monitoring, asset monitoring, power grid monitoring, water management etc are using LoRaWAN technology. The data transmitted is confidential, time sensitive and used for taking critical automated decisions, and thus ensuring CIA is essential. For example, in the case of cold storage for medicines, temperature monitoring is critical. As seen in the era of Covid 2019, one of the vaccines had to be stored in subzero temperature and any exposure for more than 10 minutes for temperature more than 1 degree could spoil the vaccine. Therefore, if any nefarious actor could carry out MiTM and change the value to normal, when actually the temperature was more than 1 degree, he could delay the corrective actions and all vaccines would be spoiled. On the other hand, even if the temperature is less than 1 degree, any nefarious actor can carry out MiTM,bit flipping attack to transmit a higher value and force an unnecessary response.

This research aims to bridge the gap existing in the encryption schema for LoRaWAN based networks with particular focus to mitigate Replay, MiTM and Bit flipping attacks. The novelty of this research is a unique approach for complicating and delaying the actions of a nefarious actor, trying to affect these attacks, so that they can be detected and negated by the Central servers.

1.3 Research Question

Currently the LoRaWAN protocol uses the AES symmetric encryption in CTR mode for encrypting the data. Two different keys are used, one for encrypting the network traffic and other for encrypting the sensor data. These keys are negotiated and calculated by the application server and end device during the authentication process. Two authentication mechanisms are used in LoRaWAN such as ABP (Activation By Personalization) and OTAA (Over the Air authentication). The major concerns that could breach security in this case stems out from the fact that initial traffic during authentication process is not encrypted and keys are stored in the end device in clear. Moreover, one single key is used for encrypting all

sensor data and thus an attacker can brute force the key in near real time by capturing multiple frames. 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 attacks (LoRa Alliance 2022). The native static encryption key use provides insufficient confidentiality against modern adversaries equipped with software defined radios for launching MiTM and Replay attacks. This premise motivated the research to find an appropriate answer to the following question:
How can LoRaWAN encryption be augmented to mitigate Replay and MiTM attcks to maintain confidentiality?

1.4 Report Structure

The report is organized in 7 sections elucidating the research conducted on augmentation on encryption in LoRaWAN. The section 2 introduces the vulnerabilities, related work and possible solutions proposed by other researchers in LoRaWAN for mitigating network attacks. Section 3 discusses the research methodology that was adopted for achieving the objectives of the research. Section 4 provides the design specifications and section 5 discusses the implementation of the prototype of the LoRaWAN simulation and proposed mechanism to mitigate MiTM and Replay attacks. Section 6 talks about the practical implementation and the evaluation, and lastly section 7 talks about the conclusion and future work of the research.

2 Related Work

The world off late has realised the importance of cybersecurity, and major research are being directed to ensure the three pillars of cybersecurity i.e. confidentiality, integrity, and availability (CIA) in true sense in every communication protocol, as the consequences of data tampering and loss are grave. LoRaWAN protocol is no exception and in last one decade much research has been carried out in the field of security. Initially we observed research were more focussed on unravelling the existing vulnerabilities, however recent ones have highlighted and evaluated the possible mitigation strategies. The literature review produced here in the report goes into detail about the LoRaWAN protocol, the existing vulnerabilities with particular attention to the encryption techniques and network attacks such as Reply and MiTM. Further it also highlights the solutions proposed by researchers for their possible mitigation.

This section has been divided into various subsections based on broad research areas. The report starts with analysis of the protocol and then existing vulnerabilities, Network attack methodologies and the alternative solutions proposed are stated and evaluated.

Subsection 2.1: Comprehensive analysis of the LoRaWAN protocol.
Subsection 2.2: Security vulnerabilities in LoRaWAN.
Subsection 2.3: Existing encryption mechanisms in LoRaWAN.
Subsection 2.4: Replay and MiTM attack in LoRaWAN.
Subsection 2.5: Analysis of proposed alternative solutions to mitigate Replay and MiTM attacks.

2.1 Comprehensive analysis of LoRaWAN protocol

In the field of IOT communication, LoRaWAN has become the preferred protocol as it provides long-range wireless communication, ease in installation & management even in greenfield isolated setup with continued operation for years on a small portable power source. LoRaWAN is immensely scalable, and thousands of end nodes can communicate wirelessly over long range (20 km). The protocol has been designed for low data rates or low latency according to (Silva & Joel J. P. C. Rodrigues, 2017). The study by (Rahman, et al., 2020) concludes that the bidirectional communication between endpoints and gateways connected in a star topology network is made possible by the LoRaWAN protocol design, which improves the network's overall energy efficiency.

A encompassing study on LoRaWAN has been carried out by (Mehmet Ali Ertürk, et al., 2019), with perspective and facts collected from large amount of literature available to clearly state the peculiarities in the protocol. The study discusses various aspects in the LoRa networks to include the network architecture, existing security schema, factors leading to increased energy efficiency, evaluation of range & coverage through tests, concept of adaptive data rate, Sequencing etc. The study also mentions in detail about the security challenges, vulnerabilities faced by LoRaWAN networks that could lead to network attacks such as replay attacks, Man-in-the-middle (MiTM) attack, bit flipping attack, jamming attack etc. The study aptly summarises and emphasizes the requirement for securing the protocol with more robust security measures. According to (Noura, et al., 2020) the tradeoff between security, performance, and power efficiency needs to be balanced for resource constrained IoT devices.

2.2 Security Vulnerabilities in LoRaWAN

A systematic security analysis of the LoRaWAN protocol carried out by (Yang, et al., 2018) provides review of the security features present in LoRaWAN such as activation methods, key management, cryptography, counter management, and message acknowledgement. The study then discovers and analyses several vulnerabilities through 5 proof-of-concept attacks as under.

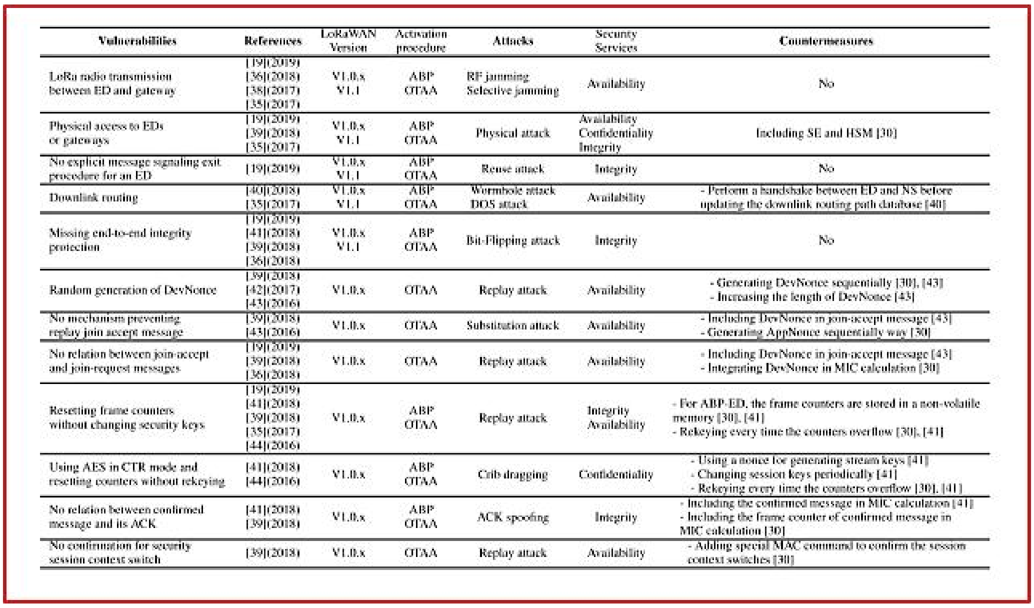
- A replay attack that leads to selective denial-of-service on individual IoT devices
- Plaintext recovery through decryption of messages when frame counters repeat due to overflows.
- Malicious message modification through bit-flipping attacks that exploit the lack of end-to-end encryption.
- Falsification of delivery reports by reusing cached ACKs from previously dropped packets.
- A battery exhaustion attack in class B networks by transmitting falsified gateway beacons to frequently wake up sensors.

The study discusses feasible mitigation strategies to address the vulnerabilities, including changes to handle key material and frame counters more securely, extending the integrity protection end-to-end, binding ACKs to specific messages, and cryptographically protecting network beacons. They note that LoRaWAN v1.1 incorporates some specification changes to improve security, but issues continue to remain duly highlighting areas needing improvement.

The study by (Yang, 2017) and (Coman, et al., 2019) provides a comprehensive analysis of the vulnerabilities associated with LoRaWAN technology and offers practical solutions to mitigate these risks. The author, identifies key security features of LoRaWAN and introduces a vulnerability analysis method outlining four possible attacks against LoRaWAN, including the use of a many-time pad attack and a brute-force attack. The study conducts PoC attacks that demonstrate the existence of vulnerabilities in both the standards and off-the-shelf hardware and services.

The research by (Ingham, et al., 2019) delves into the specific vulnerabilities of LoRaWAN-based IoT devices and presents a simulated predictive signal jamming attack designed to block the successful transmission of device data. The study contributes to the understanding of security weaknesses in LPWAN functionality. The literature review provides a comprehensive analysis of IoT security concerns, the operational steps of LoRaWAN, known attacks, and experimental frameworks for analysing security vulnerabilities. It also discusses the proposed prediction-based jamming model and its implications.

A study by (LOUKIL, et al., 2022) has investigated the security risks associated with LoRaWAN compatibility scenarios and provide an overview of the LoRaWAN communication protocol, its architecture, and the role of each component. They discuss the security challenges faced by the LoRaWAN standard and establish a catalogue of vulnerabilities in LoRaWAN v1.0.x and v1.1 which include data sniffing, Jamming between end device and the gateway, regeneration of same device nonce, no mechanism preventing replay join-accept message, no relation between join-request and join-accept messages, resetting of frame counters in AES CTR mode without changing security keys, no relation between confirmed message and its ack , no confirmation for security session context switch etc. The authors also assess the vulnerabilities in this catalogue on compatibility scenarios and provide future scope for research.



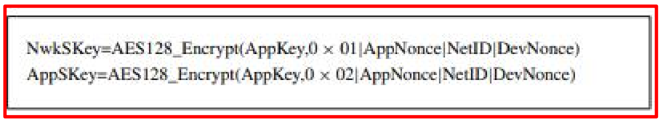
Vulnerabilities	References	LoRaWAN Version	Activation procedure	Attacks	Security Services	Countermeasures
LoRa radio transmission between ED and gateway	[19](2019) [36](2018) [38](2017) [35](2017)	V1.0.x V1.1	ABP OTAA	RF jamming Selective jamming	Availability	No
Physical access to EDs or gateways	[19](2019) [39](2018) [35](2017)	V1.0.x V1.1	ABP OTAA	Physical attack	Availability Confidentiality Integrity	Including SE and HSM [30]
No explicit message signaling exit procedure for an ED	[19](2019)	V1.0.x V1.1	ABP OTAA	Reuse attack	Integrity	No
Downlink routing	[40](2018) [35](2017)	V1.0.x V1.1	ABP OTAA	Wormhole attack DOS attack	Availability	- Perform a handshake between ED and NS before updating the downlink routing path database [40]
Missing end-to-end integrity protection	[19](2019) [41](2018) [39](2018) [36](2018)	V1.0.x V1.1	ABP OTAA	Bit-Flipping attack	Integrity	No
Random generation of DevNonce	[39](2018) [42](2017) [43](2016)	V1.0.x	OTAA	Replay attack	Availability	- Generating DevNonce sequentially [30], [43] - Increasing the length of DevNonce [43]
No mechanism preventing replay join accept message	[39](2018) [43](2016)	V1.0.x	OTAA	Substitution attack	Availability	- Including DevNonce in join-accept message [43] - Generating AppNonce sequentially way [30]
No relation between join-accept and join-request messages	[19](2019) [39](2018) [36](2018)	V1.0.x	OTAA	Replay attack	Availability	- Including DevNonce in join-accept message [43] - Integrating DevNonce in MIC calculation [30]
Resetting frame counters without changing security keys	[19](2019) [41](2018) [39](2018) [35](2017) [44](2016)	V1.0.x	ABP OTAA	Replay attack	Integrity Availability	- For ABP-ED, the frame counters are stored in a non-volatile memory [30], [41] - Rekeying every time the counters overflow [30], [41]
Using AES in CTR mode and resetting counters without rekeying	[41](2018) [44](2016)	V1.0.x	ABP OTAA	Crib dragging	Confidentiality	- Using a nonce for generating stream keys [41] - Changing session keys periodically [41] - Rekeying every time the counters overflow [30], [41]
No relation between confirmed message and its ACK	[41](2018) [39](2018)	V1.0.x	ABP OTAA	ACK spoofing	Integrity	- Including the confirmed message in MIC calculation [41] - Including the frame counter of confirmed message in MIC calculation [30]
No confirmation for security session context switch	[39](2018)	V1.0.x	OTAA	Replay attack	Availability	- Adding special MAC command to confirm the session context switches [30]

Figure 2: Vulnerabilities Observed (Coman, et al., 2019)

According to (Butun, et al., 2018) (Noura, et al., 2020) (Aras, et al., 2017) (Eldefrawy, et al., 2019) vulnerabilities exist with key storage, frame counters, and backwards compatibility. The keys are stored in an insecure manner in the end devices and thus physical access to it can jeopardise the security. Further frame counter can be reset, and the replay attacks can be executed. While some additional security has been built in Version 1.1 but when it is operated in the backward compatibility mode with Version 1, all new features are negated.

2.3 Existing encryption mechanisms in LoRaWAN

A study by (LOUKIL, et al., 2022) comprehensively describes the AES 128 in CTR mode used for encryption in the LoRaWAN protocol. It also describes generation of session context between the end device and the central servers, device authentication in OTAA and ABP mode, network and session keys generation based on Device nonce and application nonce and the encryption process.



NwkSKey=AES128_Encrypt(AppKey,0 × 01|AppNonce|NetID|DevNonce)
AppSKey=AES128_Encrypt(AppKey,0 × 02|AppNonce|NetID|DevNonce)

Figure 3: Network & Application Key Generation

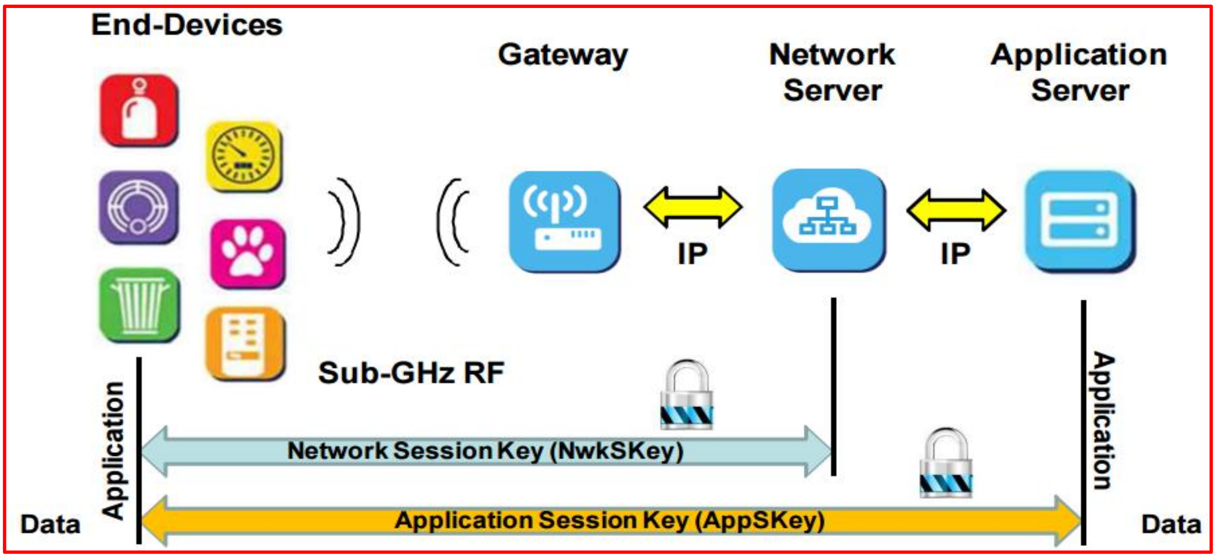


Figure 4: Encryption in LoRaWAN

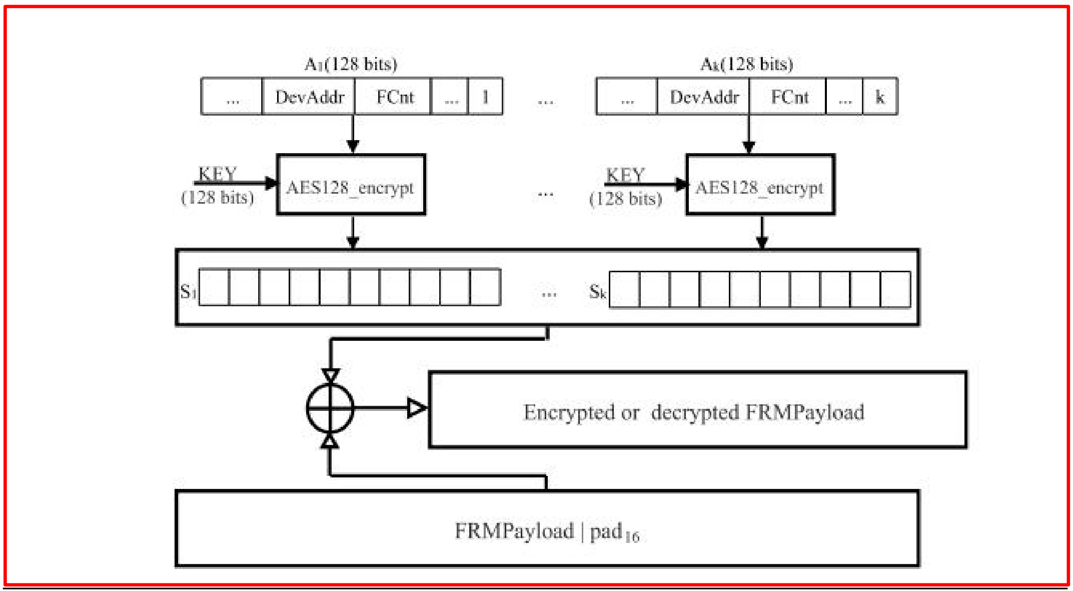


Figure 5: Encryption Process (LOUKIL, et al., 2022)

2.4 Replay and MiTM attacks in LoRaWAN

Replay attacks are the attacks that are performed by retransmission of the sniffed packet at a separate time without any changes. MiTM attacks are, however, executed by making changes in the sniffed packet. During execution the receiver is temporarily jammed and changed packet is subsequently transmitted to the receiver. MiTM essentially inserts the attacker in the path transparently.

According to (Na, et al., 2017) (Sung, et al., 2018) and (Eldefrawy, et al., 2019) a vulnerability exists in the LoRaWAN network join procedure, which uses Over-The-Air Activation (OTAA) as the Join requests are sent unencrypted, exposing device identifiers and nonces. The lack of synchronisation between the device and the server adds to this vulnerability. The authors perform an experiment showing join requests are easily sniffed and a replay attack can be executed by analysing request patterns to determine optimal attack timing and launching replay attack by sending captured join requests at scale, preventing target devices from connecting.

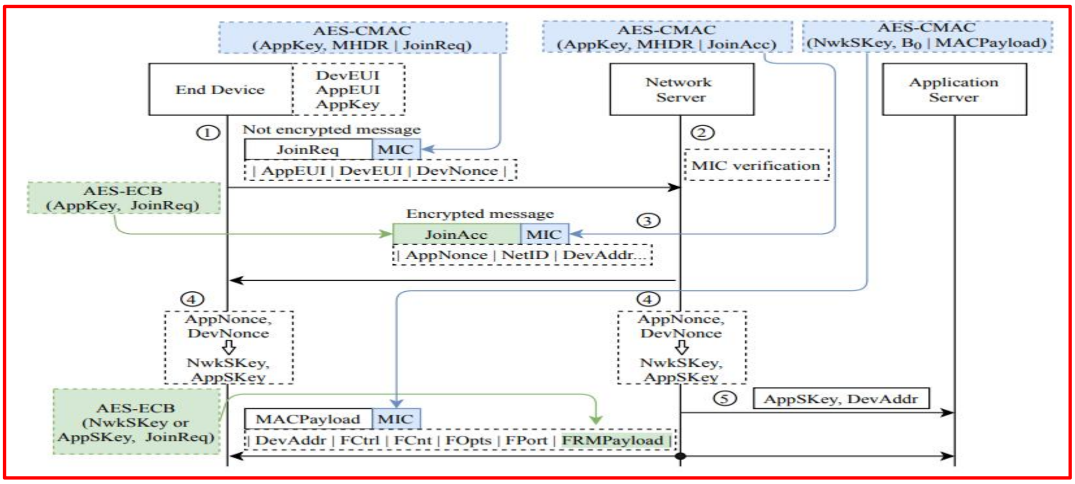
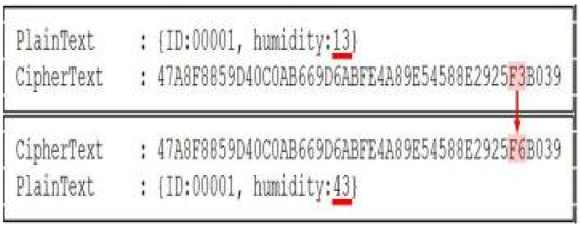


Figure 6: OTA Authentication Process (Pospisil, et al., 2021)

According to (Yang, 2017) (Coman, et al., 2019) and (Eldefrawy, et al., 2019) encryption used in LoRaWAN has vulnerability owing to use of preconfigured or the same keys again and again. Thus, using known cyphertext and brute force attacks the keys can be recovered and MiTM attacks can be executed. Therefore, a more robust key management is essential.

Another variant of the MiTM is Bit Flipping attack (Pospisil, et al., 2021) where a frame is not decrypted but the bits in the encrypted text are flipped to falsify the data. This attack, however, require precise knowledge of the place field of the data in the frame. According to (Lee, et al., 2017) such an attack is feasible in AES CTR mode.



```
PlainText    : {ID:00001, humidity:13}
CipherText   : 47A8F8859D40C0AB669D6ABFE4A89E54588E2925F3B039

CipherText   : 47A8F8859D40C0AB669D6ABFE4A89E54588E2925F6B039
PlainText    : {ID:00001, humidity:43}
```

Figure 7: Example -Bit Flipping Attack (Lee, et al., 2017)

2.5 Analysis of Proposed Alternative Solutions to mitigate Replay and MiTM Attacks.

2.5.1 Replay Attacks

A countermeasure is proposed by (Na, et al., 2017) using XOR masking of join requests with extracted session key bits to create uniqueness across messages. This prevents captured requests from being reusable without extra computation or new key generation. This increases the complexity.

Proposed methodology by (Sung, et al., 2018) includes a novel method utilizing Received Signal Strength Indicator (RSSI) and a new Proprietary Hand-Shaking technique to protect end-devices from such attacks. The solution aims to distinguish between legitimate users and attackers by leveraging the physical characteristics of RSSI measurements and introducing a secure hand-shaking process. The use of RSSI is highlighted as a reliable measure, difficult to forge arbitrarily. This however is subject to deployment area and the weather conditions. (Butun, et al., 2018) have proposed proper handling of frame counter as a countermeasure to mitigate Replay attacks, which is an effective countermeasure.

Improved key storage, join procedure and robust encryption remains a primary countermeasure to mitigate replay attacks according to (Aras, et al., 2017) (Eldefrawy, et al., 2019) and (15).

2.5.2 MiTM Attacks

According to (Huang, et al., 2017) a dual key-based activation scheme to address security loopholes in LoRaWAN's key update and session key generation is an effective countermeasure. This however increases a complexity, time of device activation and power performance.

According to (Thomas, et al., 2020) a technique involves implementing a Galois Counter Mode cryptographic algorithm to protect the encrypted communication between two peer modules over the wireless network. This algorithm requires creation of authentication tag and thus when MiTM gets executed, at the receiver end the value of tag changes and the packet can be discarded. This is an effective countermeasure, albeit with increased complexity and time penalty.

According to (MMind & Butun, 2020) implementation of Public Key cryptography is an effective countermeasure, however asymmetric cryptography is slow and requires a trusted third party for certificate management, which may not be feasible. The time penalty will tamper with the protocol niche.

According to (Raad, et al., 2019) use of adaptive elliptic curve cryptography can mitigate MiTM attacks. The technology is still asymmetric and will make implementation complex and will have effect on the time, cost, and power requirement.

2.5.3 Bit Flipping Attack

According to (Lee, et al., 2017) cyclic rotation of encrypted bits will make it difficult for an attacker to know the exact place value of the data bits and carryout bit flipping attacks. This is an effective countermeasure but with increased complexity.

3 Research Methodology

The literature review has clearly revealed that there are several vulnerabilities in the LoRaWAN protocol that enable attackers to execute the replay, MiTM and bit flipping attacks. The solutions proposed by recent recearches are effective but tamper with either the time, cost or power performance of the protocol. Moreover individual solutions tackle respective problem and not all attacks in entirity. LoRaWAN has three important niche parameters such as long range, low datarate and power efficiency. Therefore the security performance has to compliment time, power and range performance and a balance is required to be achieved. Further, the proposed solution should either be accepted by LoRa alliance or should confirm to the specifications of approved protocol stack.

The research followed a logical methodology starting from data gathering to solution development, PoC simulation, PoC testing, analysis of results, physical implementation and practical result analysis.

3.1 Data Gathering

Data was gathered from various research papers, technical articles, journals to gain an insight on the working of the LoRaWAN protocol, data transmission parameters, frame creation, authentication, encryption of payload, CRC, and data extraction process at central servers. It was well understood that the simulating the actual beacon parameters is essential for correct results and subsequent analysis. The open-source simulators available in the market to simulate the LoRaWAN protocol, such as NS3, MATLAB, and Cooja etc. were studied in detail, but unfortunately none of them provide ready solution for LoRa beacon simulation and provide results for understanding the effect of change in transmission parameters. MATLAB was eventually used to create a simulation for studying the effect of transmission parameters.

3.2 Simulation Environment Setup

To carryout PoC of the proposed solution, simulation of actual LoRaWAN protocol was essential. Therefore, a small network, containing 10 nodes was simulated on MATLAB. For implementing few MATLAB functions, a licensed version of the software and a latest operating system with a least 6GB RAM is required. The simulation used a variety of libraries which include Simulink, MATLAB function blocks, RF toolbox, SimEvents toolbox, and other MATLAB channel definition blocks.

3.3 LoRaWAN protocol Setup

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 gateway and central servers. The nodes were connected in the star topology and the environment parameters were calculated through a MATLAB function.

Once all parameters were obtained, a complete 10-node network was created. The modelled transmitter and receiver were created as basic building blocks and were eventually compacted to model a LoRa node. The transmission parameters were configured manually, i.e., the transmitter, receiver working frequency of 868 MHz, bandwidth of 125kHz, spreading factor that ranged from 7-9, transmission power levels etc. 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 Tx_signal (Transmitted signal) and Rx_Signals (Received signal) were plotted.

The building blocks of the transmitter, receiver, Media Access Control (MAC) layer and switching to form a transceiver sensor node is as below.

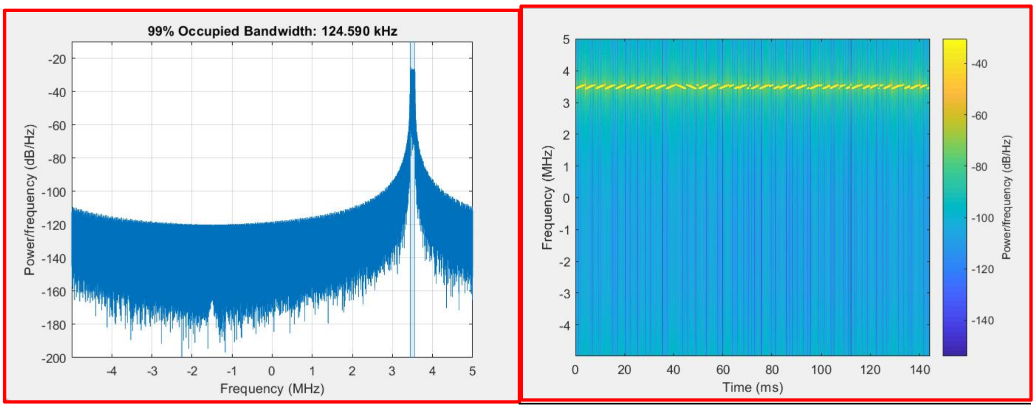


Figure 8: LoRa Beacon

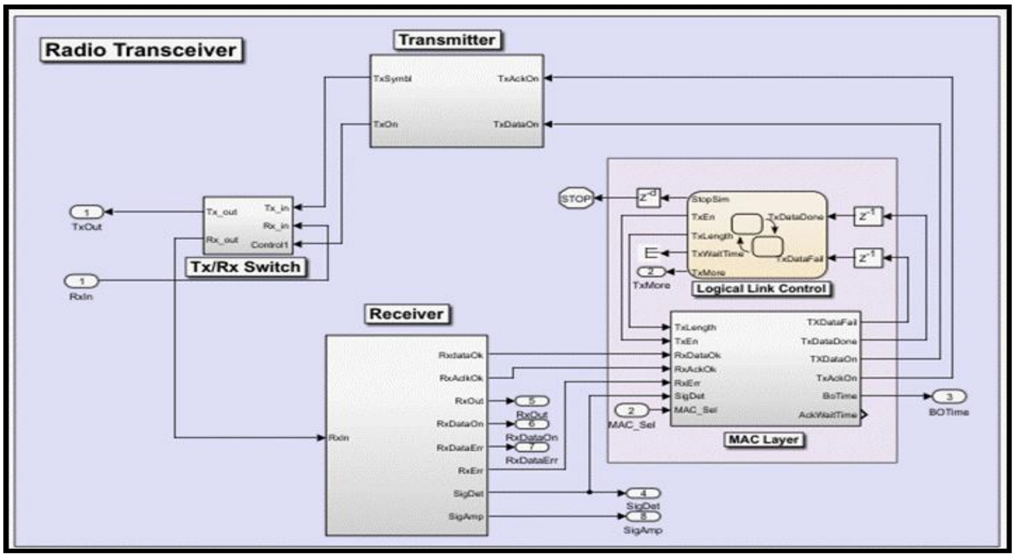


Figure 9: LoRa Transceiver

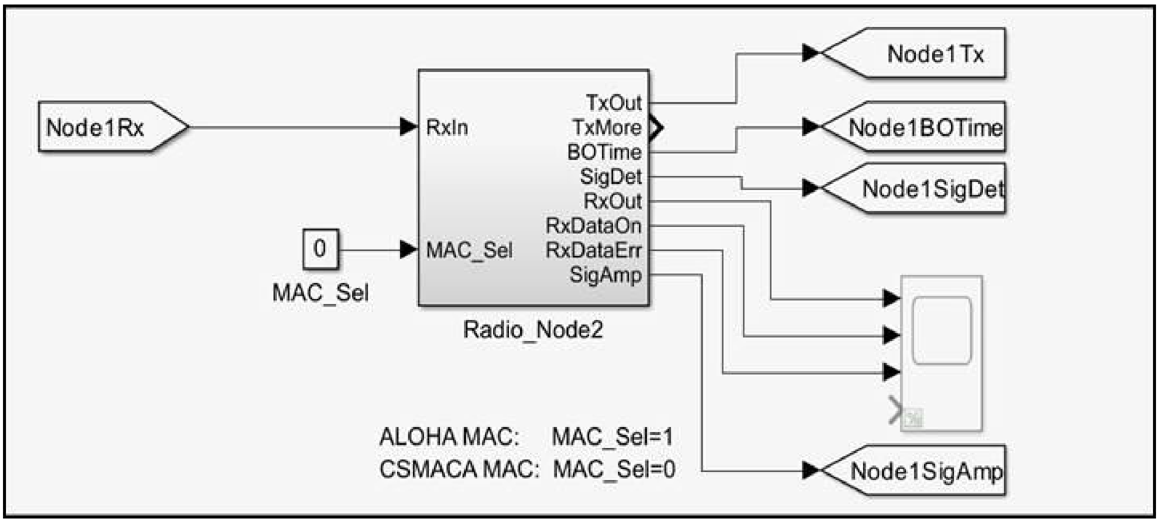


Figure 10: Complete LoRa Node

The nodes were then replicated to form a larger and complex network which could include more end-devices, gateways. This made the simulation-prototype on a larger scale.

3.4 Proposed Solution Development

Alternate solutions to mitigate the replay, MiTM and bit flipping attacks proposed by technical papers were evaluated but, none of them provide a comprehensive solution and tackle all three attacks simultaneously. Either they are increasing a substantial time penalty, or they are increasing the complexity. LoRaWAN is popular due to core functionalities i.e long range, low latency, low complexity, low data rate and minimal cost. Therefore, any increase in data rate would incur a time penalty (latency) and reduce the ranges to control the BER.

The solutions were discussed with the research team at Tynatech Ingeneous and it was understood that the company was not in favour of tampering with LoRa chip (Prasgate LoRa Node) with link budget of 168 dB, RF output 100mW and battery capacity of 4000mAh.On analysis, it was understood that if the management of cryptographic keys can be worked out, it would be very complex, and time consuming for an attacker to exploit and effect these attacks. Moreover, all three attacks can be mitigated simultaneously. After deliberation the following solution was developed

- An external low power chip to be inserted between the sensor and LoRa node.
- A double encryption scheme to be implemented for sensitive nodes.
- A bank of 10 cryptographic keys for AES encryption in ECB mode can be used in chip.
- A Random generator to be used for selection of key.
- Random feed and timestamp appended to the encrypted sensor data should be passed as payload to LoRa node.

3.5 Selection of Chip

The major considerations for the selection of chip were low power operation, compute to support AES and random generator, integration with sensor & LoRa node and could be powered by a small battery. After evaluating multiple options ESP 32 was selected due to the following features.

- ESP32 is designed for mobile, wearable electronics, and Internet of Things (IoT) applications.

- It is low power chip with adjustable power modes. ESP32 can be woken up periodically or only when a specified condition is detected to minimize the amount of energy that the chip expends.
- Support for AES encryption and random generator.
- Easy to flash and supports flash encryption.
- Power supply: 2.2 V to 3.6 V

3.6 PoC Simulation & Evaluation

A proof of concept was simulated in MATLAB to evaluate the feasibility of the solution. However, MATLAB has limited support to encryption and therefore the parameters were hardcoded and simulated as a lookup table rather than actual encryption process. The model for the same is as under.

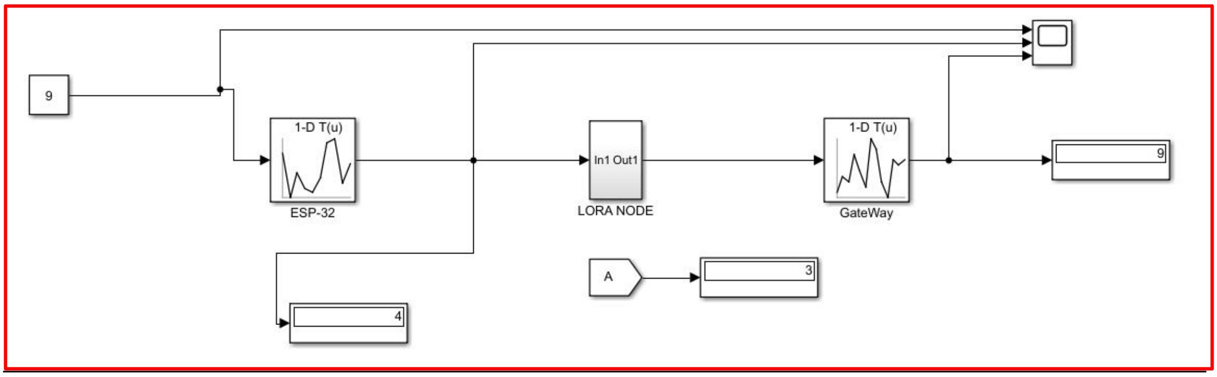


Figure 11: PoC Simulation

As seen from the model above an original message of “9” was encoded as “4” by the ESP 32 and passed as payload to LoRa node which again encrypted it as “3” and send it to the gateway. At the gateway end two decryption were done one after the other to finally decode the original message as “9”.

3.7 Research Timeplan

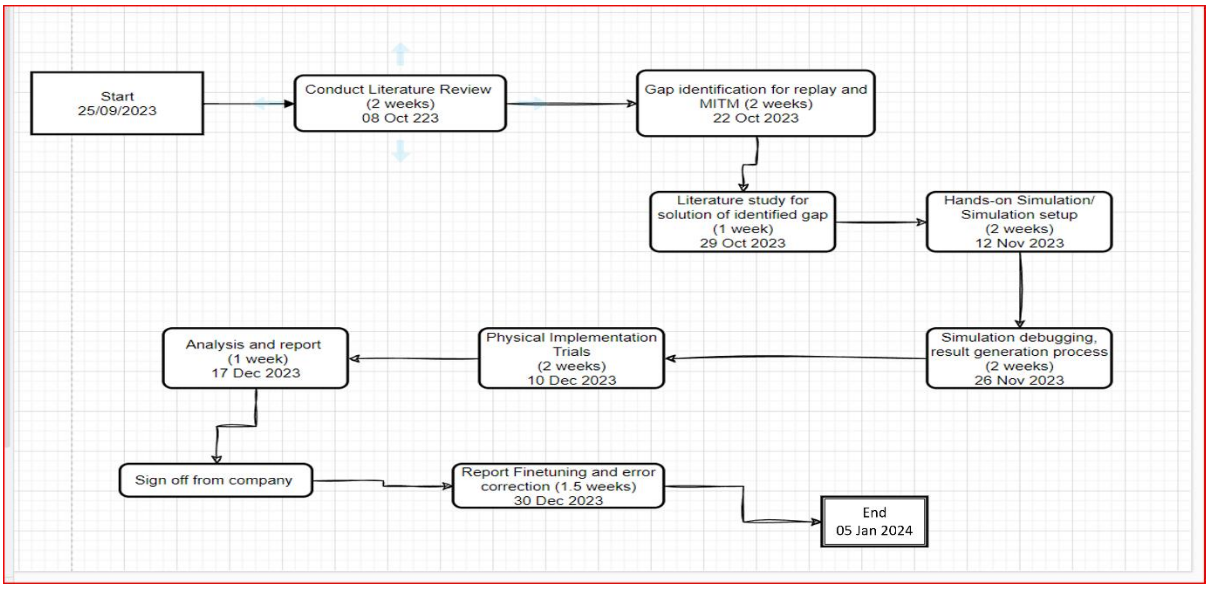


Figure 12: Timeplan

4 Design Specification

This section gives an overview of the design specification of the solution for achieving the objectives of the research. The proposed solution as described in the section 3 ***does not alter the standard LoRa protocol***; but introduces an external chip to implement a double encryption scheme for critical nodes. The solution is designed to increase encryption complexity so that the attacks suffer time penalty. This approach combined with rule to check legitimacy of data based on timestamp and the calculated standard time at the gateway can negate the efforts of an attacker to brute force the key for MiTM. Further an encrypted timestamp is passed in the payload field, which negates the replay attack. Also, the encrypted payload does not have a fixed place value for data and thus bit flipping attacks are not feasible. The architecture diagram below explains the flow of data from the sensor node till the gateway and shows how our proposed solution helps in improvising the encryption schema for the LoRaWAN network.

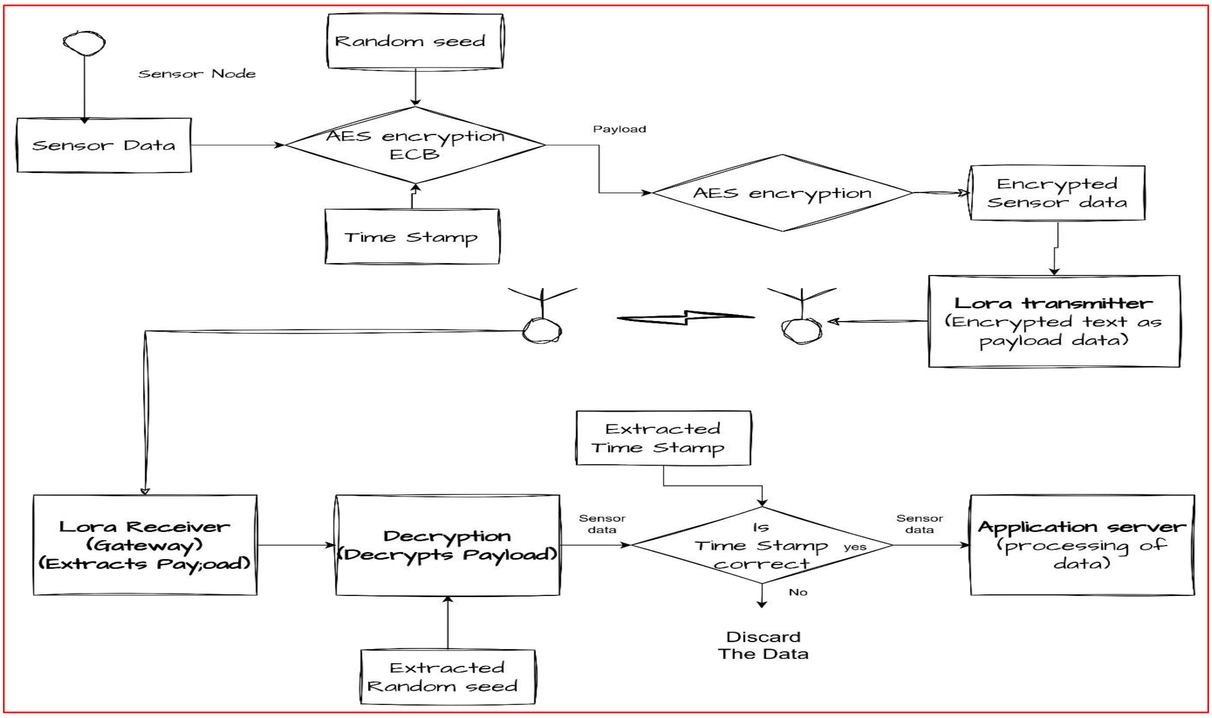


Figure 13: Solution Flow Chart

5 Implementation

Implementation was done in MATLAB simulation, SDR as well as practically on the ESP 32. The details are as follows.

5.1 Simulation

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.

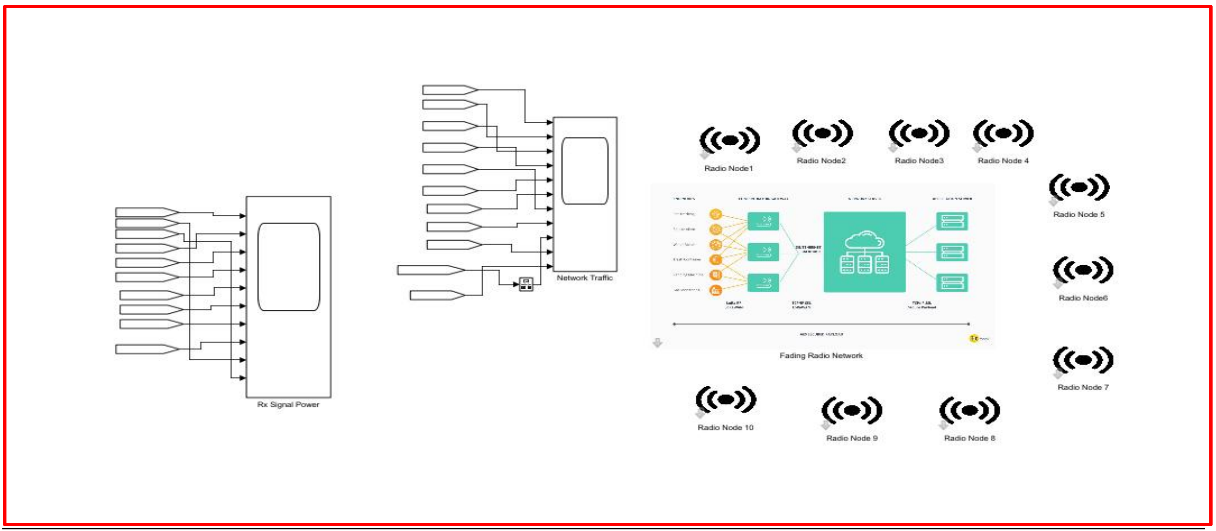


Figure 14: 10 nodes LoRa Network

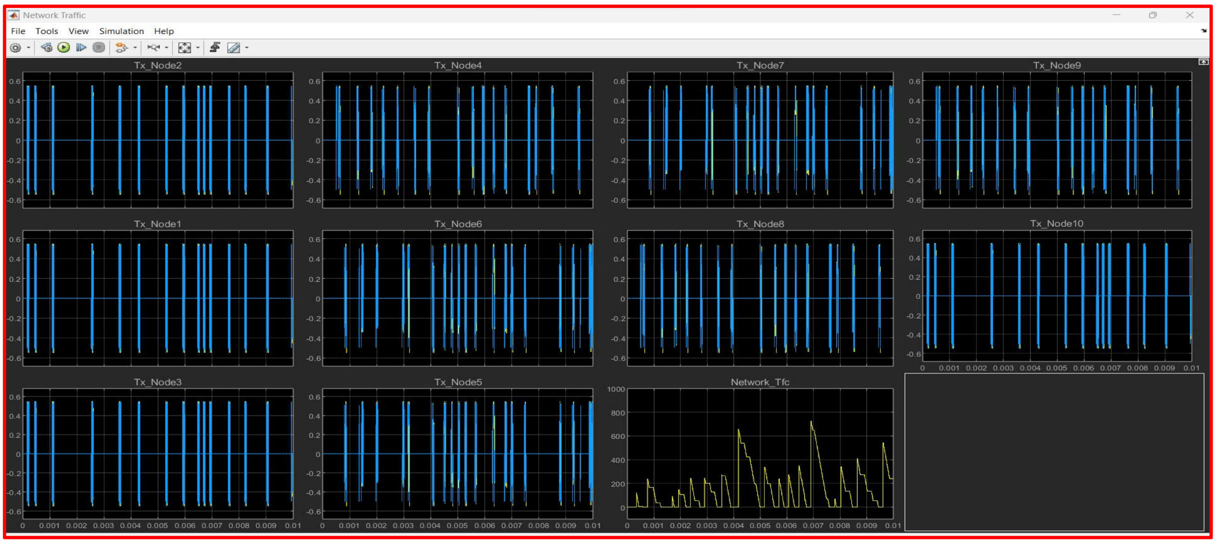


Figure 15 : Transmitted Signal

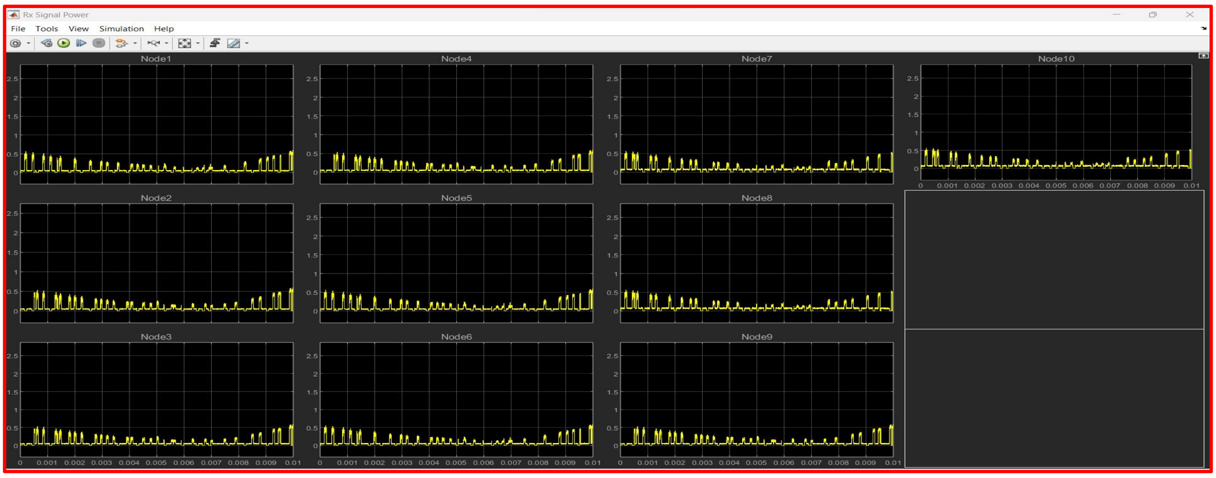
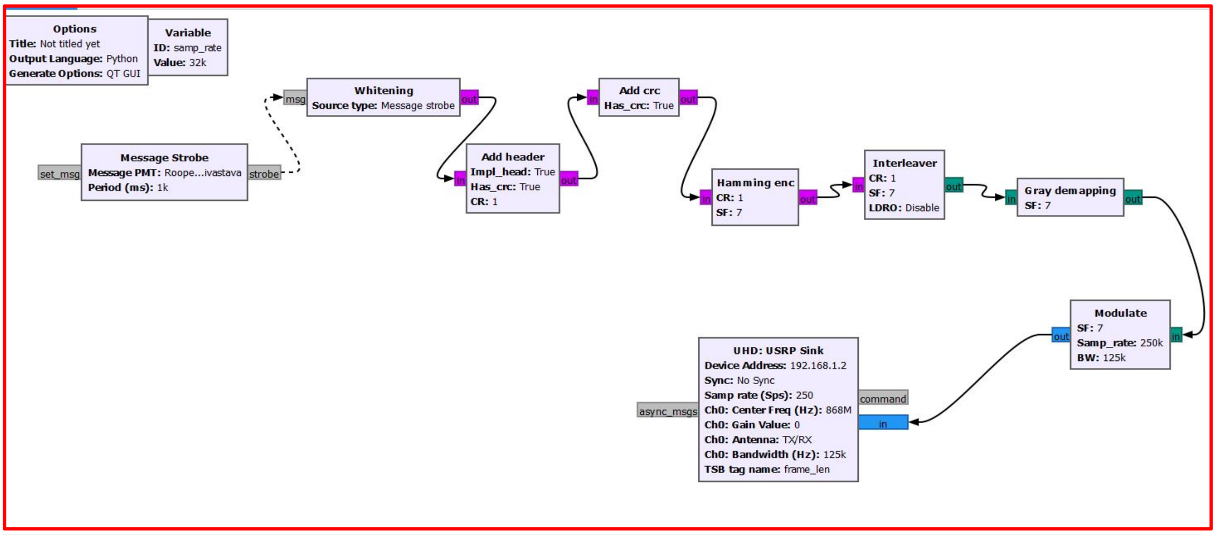


Figure 16: Received Power

5.2 SDR Based Implementation

An additional requirement was given by the company to create LoRa transmitter and Receiver using Software defined radio. We used GNU radio to generate the source file for the LoRa transmitter and the LoRa receiver. GNU Radio is a free & open-source software development toolkit that provides signal processing blocks to implement software radios. It can be used to create software-defined radios using easily accessible, reasonably priced external RF gear, or it can be utilized in a simulation-like environment without any hardware. It is widely used to assist real-world radio systems and wireless communications research in research, industry, university, government, and hobbyist domains.

The transmitter and the receiver flow graph were created, and the python file generated was provided to the company for flashing on Raspberry Pi circuit board. Blade RF SDR with bandwidth of 6GHz was used for radio. The flow graph is as under.



Options
Title: Not titled yet
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 32k

Message Strobe
Message PMT: Roope...ivastava
Period (ms): 1k

Whitening
Source type: Message strobe

Add header
Impl_head: True
Has_crc: True
CR: 1

Add crc
Has_crc: True

Hamming enc
CR: 1
SF: 7

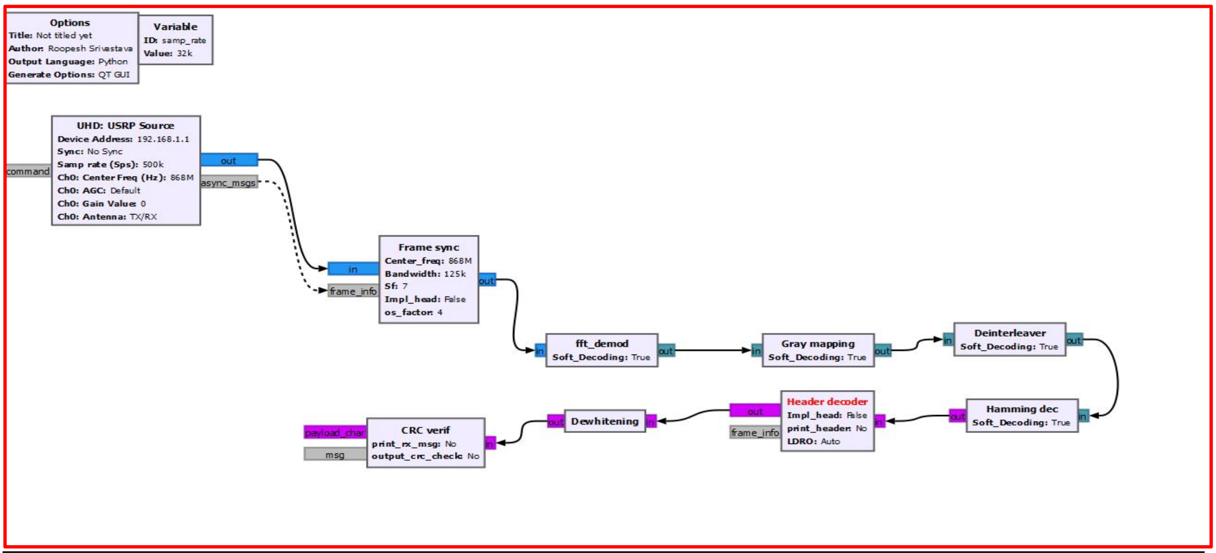
Interleaver
CR: 1
SF: 7
LDRO: Disable

Gray demapping
SF: 7

Modulate
SF: 7
Samp_rate: 250k
BW: 125k

UHD: USRP Sink
Device Address: 192.168.1.2
Sync: No Sync
Samp rate (Sps): 250
Ch0: Center Freq (Hz): 868M
Ch0: Gain Value: 0
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 125k
TSB tag name: frame_len

Figure 17: LoRa Transmitter Flow Graph



Options
Title: Not titled yet
Author: Roopesh Srivastava
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 32k

UHD: USRP Source
Device Address: 192.168.1.1
Sync: No Sync
Samp rate (Sps): 500k
Ch0: Center Freq (Hz): 868M
Ch0: AGC: Default
Ch0: Gain Value: 0
Ch0: Antenna: TX/RX

Frame sync
Center_freq: 868M
Bandwidth: 125k
Sf: 7
Impl_head: False
os_factor: 4

fft_demod
Soft_Decoding: True

Gray mapping
Soft_Decoding: True

Deinterleaver
Soft_Decoding: True

Hamming dec
Soft_Decoding: True

Header decoder
Impl_head: False
print_header: No
LDRO: Auto

Dewhitening

CRC verif
print_rx_msg: No
output_crc_check: No

Figure 18: LoRa Receiver Flow Graph

5.3 Physical Implementation

Physical implementation of the solution was carried on ESP 32 chip at sensor end and the network server at the centre. A C language program for AES encryption was written. The code selects one key out of the bank of 10 keys based on the random feed from a random generator. The encrypted text is then appended with a time stamp and the random feed passed as output to the LoRa node. The code flashed onto the chip and the dependencies were resolved with the help of research team of the company.

A decryption code was inserted to the output of LoRa decryption module at the server end to completer the process. The final output was decrypted sensor data. A check code was implemented to check elapsed time between the current time and the recovered timestamp from the payload and compared with standard anticipated time. If the variation was more than designed value, the data frame was discarded as "May have been tampered".

Notably, refinements of the authentication mechanism for real-world deployment would require a physical hardware-based implementation in accordance with the LoRa alliance protocol.

6 Evaluation

6.1 Objective and Methodology

The primary objective of this research was to develop a methodology to mitigate Replay, MiTM and Bit flipping attack in LoRaWAN. MATLAB simulation has been carried out to check the feasibility and there after physical implementation has been carried out using ESP 32 chip and Prasgate LoRa node and the gateway. The simulation model worked served as a PoC and the actual implementation was evaluated by the company focusing on latency, data rate and the range.

6.1.1 Findings

- **Range**: The results show no change in range upto 10 kms.

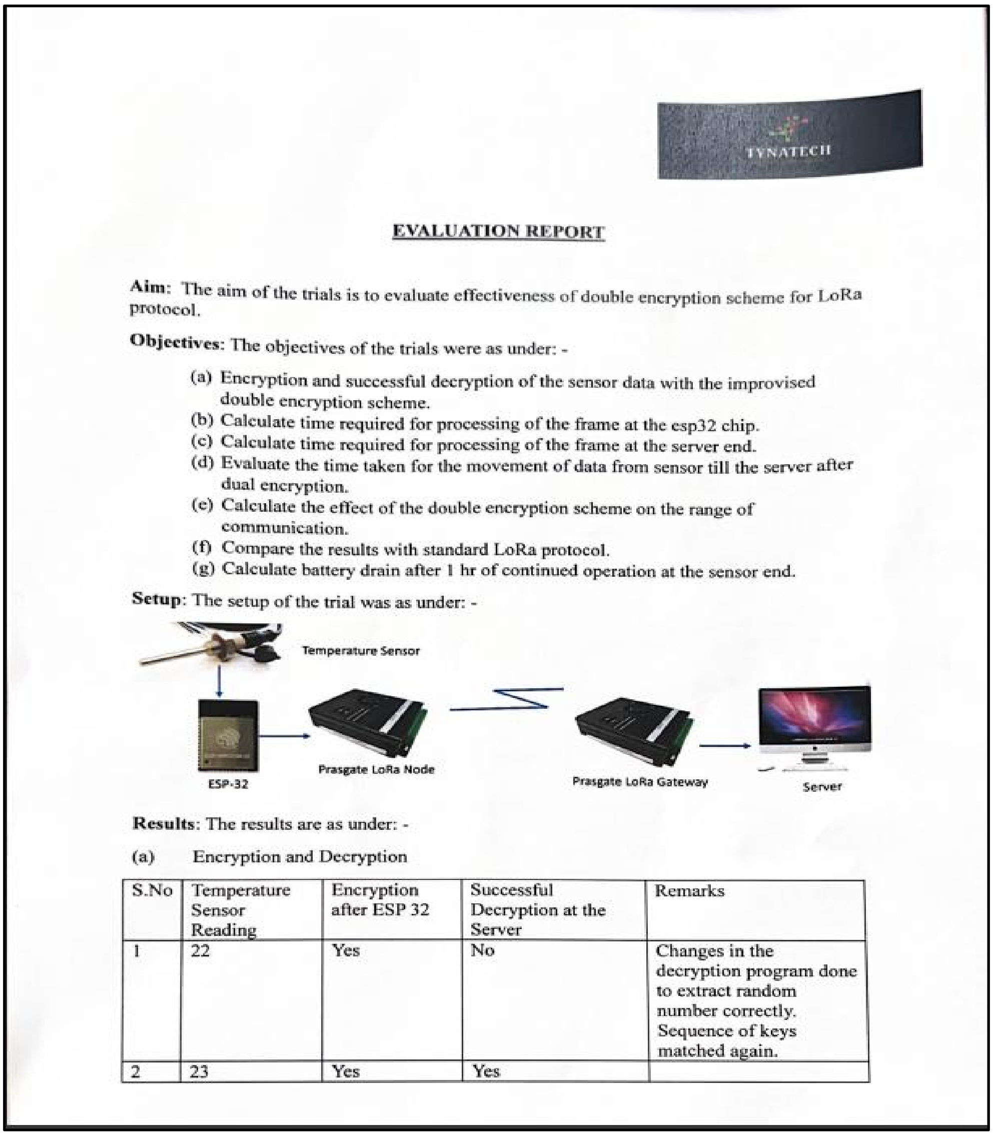
- **Latency**: The data rate remained same and so the latency. No perceivable difference was observed with introduction of double encryption.

- **Processing Time**: There was a marginal increase in the processing time as an additional decryption step has been added. However, it was very non perceivable during trials.

- **Decryption time for an Attacker**: With double encryption and multiple keys the decryption time is expected to increase substantially. This feature could not be evaluated during trials. Further with increase in processing resources, this time can be shortened. Thus, adding a time check wrt Timestamp of frame creation and frame received can be optimised and that would ensure detection a data is probably changed enroute through an attack, such a frame can be discarded easily.

- **Power Consumption**: Battery drain was optimised during trials using Light sleep mode. Power consumption of 0.8mA was observed when the esp32 was active. With 600mAh battery, it is expected to provide continued operation for more than six months.

- The results obtained by the company during evaluation trials are as under.



TYNATECH
Temperature Sensor
ESP-32
Prasgate LoRa Node
Prasgate LoRa Gateway
Server

EVALUATION REPORT

Aim: The aim of the trials is to evaluate effectiveness of double encryption scheme for LoRa protocol.

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

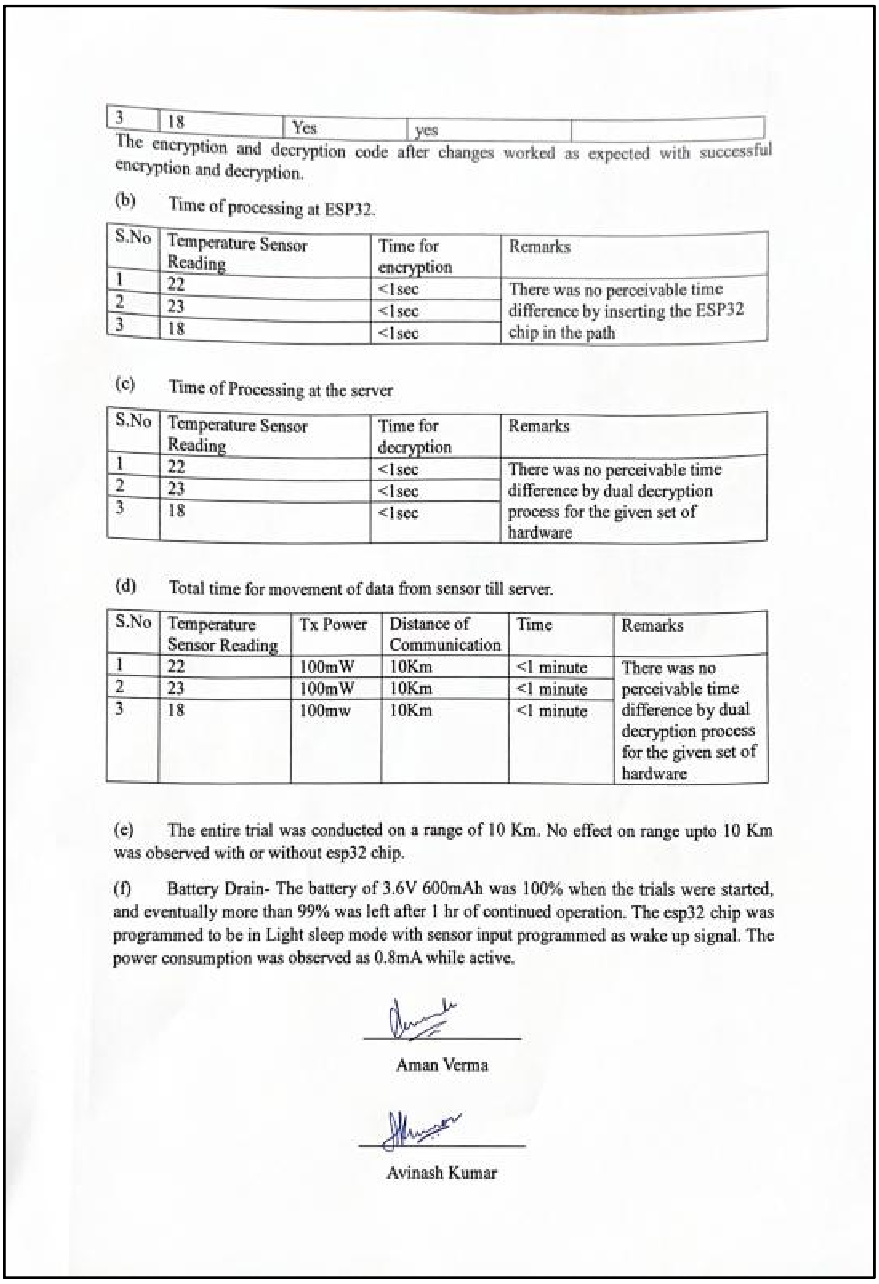
(a) Encryption and successful decryption of the sensor data with the improvised double encryption scheme.
(b) Calculate time required for processing of the frame at the esp32 chip.
(c) Calculate time required for processing of the frame at the server end.
(d) Evaluate the time taken for the movement of data from sensor till the server after dual encryption.
(e) Calculate the effect of the double encryption scheme on the range of communication.
(f) Compare the results with standard LoRa protocol.
(g) Calculate battery drain after 1 hr of continued operation at the sensor end.

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

Results: The results are as under: -

(a) Encryption and Decryption

S.No	Temperature Sensor Reading	Encryption after ESP 32	Successful Decryption at the Server	Remarks
1	22	Yes	No	Changes in the decryption program done to extract random number correctly. Sequence of keys matched again.
2	23	Yes	Yes	



3	18	Yes	yes	

The encryption and decryption code after changes worked as expected with successful encryption and decryption.

(b) Time of processing at ESP32.

S.No	Temperature Sensor Reading	Time for 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) Time of Processing at the server

S.No	Temperature Sensor Reading	Time for decryption	Remarks
1	22	<1sec	There was no perceivable time difference by dual decryption process for the given set of hardware
2	23	<1sec	
3	18	<1sec	

(d) 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 perceivable time difference by dual decryption process for the given set of hardware
2	23	100mW	10Km	<1 minute	
3	18	100mw	10Km	<1 minute	

(e) The entire trial was conducted on a range of 10 Km. No effect on range upto 10 Km was observed with or without esp32 chip.

(f) 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.

Aman Verma

Avinash Kumar

6.1.2 Implications

- **Academic**: The research contributes to the field of Encryption in LoRaWAN protocol, providing a feasible and effective solution to mitigate the network attacks on the protocol.

- **Practical**: From a practical standpoint, the solution is effective and can serve as an interim solution for critical nodes in a LoRaWAN network. This neither tampers with the essence of the protocol nor with the approved recommendations of the LoRa alliance

7 Conclusion and Future Work

LoRaWAN is becoming more and more popular as a deployment option for Internet of Things ecosystem because of its highly desirable properties, like cheap cost, low latency, ease of deployment and long-range communications. The research has explored the core traits, architecture, vulnerabilities, and salient features of LoRaWAN, revealing its potential to completely transform the way we connect and collect data. Because of its scalability, energy efficiency, and long-range capabilities, LoRaWAN is especially well-suited for applications like industrial monitoring, smart cities, and agricultural, among others. It differs from conventional wireless technologies in that it can cover wide geographic regions while consuming less power and can pass through obstacles, making it an affordable and environmentally friendly option for Internet of Things deployments. The broad acceptance of the technology is facilitated by standardised initiatives and the ecosystem, which also creates a cooperative atmosphere for research and development.

Various research have concluded that the protocol in its current version suffers from lack of synchronisation between parties and management of cryptographic keys that lends it susceptible for Replay, MiTM and bit flipping attacks. LoRa alliance has acknowledged that an improvement is warranted in the encryption schema. Therefore, there exists an apprehension while using it for critical sensor nodes as any tampering of data while in transit can be catastrophic.

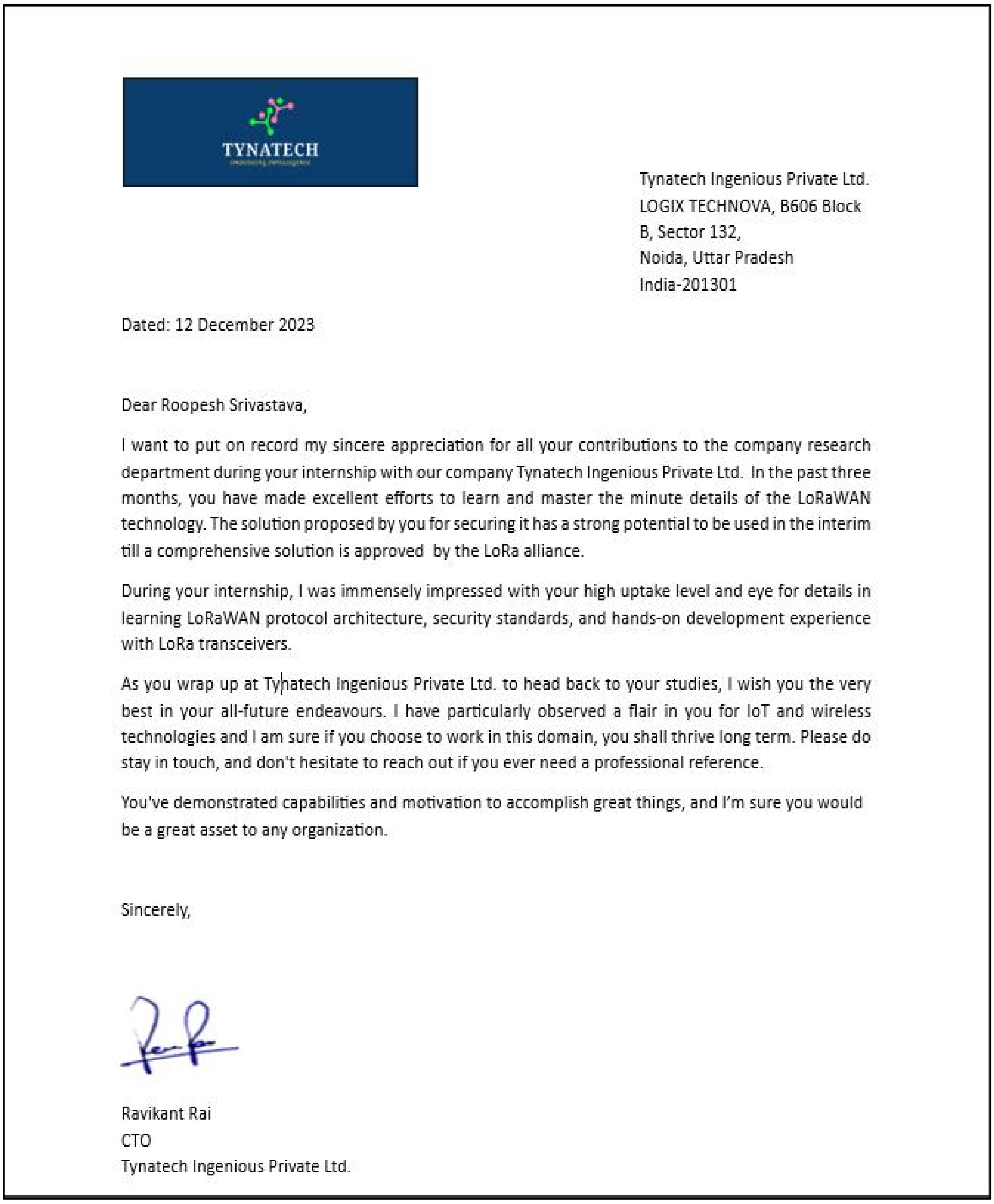
This research has proposed an improvement in the terms of dual encryption and the time-based check procedure, which has been found to be practical and can serve as an interim solution. The solutions target towards introducing a higher time penalty in the work function of an attacker, which improves the attack detection and mitigation capability of the protocol.

The proposed solution mitigates MiTM, Replay attack and Bit flipping attacks effectively. As regards bit flipping attack, the dual encryption scrambles the payload field and thus making it virtually impossible to change the sensor data while being encrypted. Further, the payload when finally decrypted can detect the attack and can discard the instant sensor data.

This research has been constrained due to paucity of time and resources, therefore, there are more enhancements feasible and can be taken as a future work.

- Simulating a genuine LoRaWAN network with endpoints and gateways on a paid simulator which can provide changes in the parameters to confirm the experiment's assessment in the real world.
- A synchronous nonce akin to two factor authentication can be used for key selection. This would negate the requirement of appending the random feed within the payload.
- Possibly a scheme for the network server to behave as a trusted party can be implemented to ensure timed rotation of key bank.
- New faster asymmetric encryption algorithm can be used to ensure CIA in better sense.
- An attacker can still attempt bit flipping attack without knowing the data place value. This, however, will not be effective as same can be detected and discarded but can lead to Denial-of-service scenario, if continuous attempts are made. Therefore, if some error correction capability can be added to the frame, even that scenario can be negated.

The solution was largely appreciated by the company and the appreciation letter issued at the end of internship is enclosed as under:



TYNATECH

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

Dated: 12 December 2023

Dear Roopesh Srivastava,

I want to put on record my sincere appreciation for all your contributions to the company research department during your internship with our company Tynatech Ingenious Private Ltd. In the past three months, you have made excellent efforts to learn and master the minute details of the LoRaWAN technology. 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 immensely impressed with your high uptake level and eye for details in learning LoRaWAN protocol architecture, security standards, and hands-on development experience with LoRa transceivers.

As you wrap up at Tynatech Ingenious Private Ltd. to head back to your studies, I wish you the very best in your all-future endeavours. I have particularly observed a flair in you for IoT and wireless technologies and I am sure if you choose to work in this domain, you shall thrive long term. Please do stay in touch, and don't hesitate to reach out if you ever need a professional reference.

You've demonstrated 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.

8 References

Aras, E., Ramachandran, G. S., Lawrence, P. & Hughes, . D., 2017. *Exploring The Security Vulnerabilities of LoRa.* s.l., IEEE.

Na, S., Hwang, D. Y., Shin, W. & Kim, K. H., 2017. Scenario and Countermeasure for Replay Attack Using Join Request Messages in LoRaWAN. *ICOIN 2017,* pp. 718-720.

Pospisil, O. et al., 2021. Testbed for LoRaWAN Security: Design and Validation through Man-in-the-Middle Attacks Study. *Applied Sciences,* 11(Aug 2021).

Thomas, J., Cherian, S. ,., Chandran, S. & Pavithran, V., 2020. *Man in the Middle Attack Mitigation in LoRaWAN.* Coimbatore, India, ICICT.

Butun, I., Pereira, N. & Gidlund, M., 2018. *Analysis of LoRaWAN v1.1 Security,* California: Future Internet.

Butun, I., Pereira, . N. & Gidlund, M., 2019. Security Risk Analysis of LoRaWAN and Future Directions. *Future Internet,* 11(3), p. 22.

Coman, F. L., Malarski, K. M., Petersen, M. N. & Ruepp, S., 2019. *Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT.* Aarhus, Denmark, IEEE.

Editor, R., 2021. *Advantages and disadvantages of wireless technologies.* [Online] Available at: https://roboticsbiz.com/advantages-and-disadvantages-of-wireless-technologies/ [Accessed 19 12 2023].

Eldefrawy, M., Butun, I., Pereira, N. & Gidlund, M., 2019. Formal security analysis of LoRaWAN. *Computer Networks,* 148(ELSEVIER).

Huang, H., Kim, J. & Song, J., 2017. A Dual Key-Based Activation Scheme for Secure LoRaWAN. *Wireless Communications and Mobile Computing,* Volume 2017, p. 6590713.

Ingham, M., Marchang, J. & Bhowmik, . D., 2019. IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. *IET,* 14(4), pp. 368-379.

Lee, J., Hwang, D., Park, J. & Kim, K.-H., 2017. *Risk Analysis and Countermeasure for Bit-Flipping Attack in LoRaWAN.* Da Nang, Vietnam, IEEE.

LOUKIL, S., FOURATI, L. C., NAYYAR, A. & SO-IN, C., 2022. Investigation on Security Risk of LoRaWAN: Compatibility Scenarios. *IEEE EXPRESS,* Volume 10, pp. 101825-101843.

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

MMind, F. & Butun, I., 2020. *Activation of LoRaWAN End Devices by Using Public Key Cryptography.* Lausanne, Switzerland, IEEE.

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

Noura, H. et al., 2020. LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet of Things,* Volume 12, pp. 1-37.

Raad, N., Hasan, T., Chalak, A. & Waleed, J., 2019. *Secure Data In LoRaWAN Network By Adaptive Method Of Elliptic-curve Cryptography.* Kirkuk, Iraq, IEEE.

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

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

Seller, O., 2021. *LoRaWAN security,* s.l.: s.n.

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

Sung, W.-J., Ahn, H.-G. & Kim, J.-B., 2018. *Protecting End-Device from Replay Attack on LoRaWAN.* Chuncheon, Korea (South), ICACT, pp. 167-171.

Wangsness, C., 2023. *What is a SCADA System and How Does It Work?.* [Online]
Available at: https://www.onlogic.com/company/io-hub/what-is-a-scada-system-and-how-does-it-work/
[Accessed 01 01 2024].

Wedd, M., 2020. *What is LPWAN and the LoRaWAN Open Standard?.* [Online]
Available at: https://www.iotforall.com/what-is-lpwan-lorawan
[Accessed 23 12 2023].

Yang, X., 2017. *LoRaWAN: Vulnerability Analysis and Practical Exploitation,* Delft, Netherlands: Delft University of Technology.

Yang, X., Karampatzakis, E., Doerr, C. & Kuipers, F., 2018. *Security Vulnerabilities in LoRaWAN.* Orlando, Florida, USA, IEEE.