Analysis of Payload Confidentiality for the IoT/ LPWAN Technology 'Lora'

Bernard McWeeney, Ilya Mudritskiy and Renaat Verbruggen
School of Computing, Dublin City University, Dublin, Ireland

Keywords: LPWAN, IoT, LoRa, SCADA, P2P Communication, Payload Confidentiality, SDR, AES, Cryptography.

Abstract: Climate change necessitates a transition towards renewable energy sources like solar panels and wind turbines. The integration of the Internet of Things (IoT) has been pivotal in achieving these advances, offering the potential to optimise renewable energy system performance and efficiency through real-time data collection and predictive maintenance. Prominently, Low Power Wide Area Network (LPWAN) technologies like LoRa are aiding this transition, providing IoT with extended coverage, reduced infrastructure complexity, and ensuring low power consumption. With IoT playing a central role in critical infrastructure, secure communication is crucial to protect against potential cyber threats. Maintaining the integrity of sensitive data relayed through IoT devices is paramount. We provide an in-depth analysis of payload confidentiality in LoRa point-to-point (P2P) communication within remote smart grids. We explore the integration of IoT hardware encryption features and the implementation of user-controlled Advanced Encryption Standard (AES) algorithms on ESP32. We propose a robust solution for secure P2P communication using AES cryptography on ESP32 with LoRa. It is feasible to integrate end-to-end payload confidentiality in LoRa P2P communication. This study offers secure communication in remote smart grids, valuable insights into trade-offs and potential security risks in implementing LoRa P2P in IoT applications.

1 INTRODUCTION

Climate change, one of the most critical issues facing our world today, necessitates urgent action to protect global environmental sustainability and human livelihoods. Central to this challenge are the United Nations' Sustainable Development Goals (SDGs), particularly Goals 7, 11, and 13, which advocate for affordable and reliable energy, sustainable cities and communities, and prompt action to combat climate change (United Nations, 2023).

Addressing these pressing concerns requires a global transition towards renewable energy sources, fostering the advent of distributed energy generation and remote grids. This revolution in energy generation and distribution democratises access to resources, significantly reducing fossil fuel dependence (GIoTitsas, 2015). Here, the Internet of Things (IoT) plays a pivotal role, enabling the development of smart grids for real- time monitoring and control of energy production, distribution, and consumption (Khan, 2020). Thus, IoT-powered smart grids enhance renewable energy systems' efficiency and cost-effectiveness, balancing the intermittent nature of solar and wind power.

However, the integration of IoT into energy infrastructures presents its challenges. Data security becomes a paramount issue, particularly within the energy sector. A breach could result in grid instability or widespread blackouts, making the scrutiny of IoT device security vulnerabilities in this context critical.

A crucial component of these micro-grid networks is the SCADA system, ensuring power quality control. Historically, the lack of low-cost, secure, and authentic communication systems with minimal power consumption posed significant hurdles for SCADA systems within Smart Grids (Rizzetti et al., 2015), (Tawde, 2015). The Russian army's exploitation of the Georgian electric grid's SCADA system in 2008 (Fillatre, 2017) and the disruption of the U.S electrical grid control system in 2009 underline the importance of grid communication security. A secure communication system, therefore, necessitates message authentication, integrity, availability, and confidentiality.

McWeeney, B., Mudritskiy, I. and Verbruggen, R.
Analysis of Payload Confidentiality for the IoT/ LPWAN Technology 'Lora'.
DOI: 10.5220/0012271400003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 90-102
ISBN: 978-989-758-683-5; ISSN: 2184-4356

The advent of long-range wireless technologies and LPWANs provides solutions to these challenges, enabling long-range communications at a low bit rate among interconnected devices like battery-operated sensors (Petajajarvi, 2015). LPWAN technologies streamline the deployment process and offer extensive coverage areas, spanning several kilometres (Mekki, 2019). Prominent LPWAN technologies such as LoRa and SigFox have found applications in fields like smart grids and factory monitoring (Patil, 2022), where robust device security against potential threats is of utmost importance. These technologies allow individual devices to cover large distances, thus significantly reducing costs by eliminating the need for intermediate routing nodes.

LoRa (Long Range), a patented digital wireless data communication IoT technology developed by Cycleo (later acquired by Semtech), has positioned itself as a leading IoT service provider worldwide (Ahmadi, 2018). LoRa operates in the unlicensed sub-GHz ISM radio band, depending on the deployed regions (e.g., 863–870MHz in Europe, 902– 928MHz in the USA), but also obliges to the duty cycle regulations (e.g., 1% in Europe) (LoRa, 2023). Compared with short- range wireless standards and cellular technologies, LoRa shows remarkable results in long-range transmission and ultra-low power consumption. Specifically, its coverage range is up to 15 km (rural areas) and 5 km (urban areas) (Magrin, 2017), its device battery life is up to 10 years (Ferreira, 2020), and its data rate ranges from 0.3 to 37.5Kbps (Rawat, 2020). LoRa is rooted in spread spectrum modulation techniques derived from chirp spread spectrum (CSS) technology (Poursafar, 2017).

A typical LoRa network comprises end devices, gateways, and a network server implementing the long-range wide-area network (LoRaWAN) protocol. LoRaWAN, a cloud-based medium access control, primarily acts as the network layer protocol, managing communication between LPWAN gateways and end-node devices as a routing protocol (Devalal, 2018). Here, end devices handle the physical layer process, while gateways function as repeaters, collecting data from different end devices (Almuhaya, 2022).

Despite extensive deployment, IoT nodes, often located in remote areas, continue to face limited coverage. Additionally, the high subscription cost per node and the unnecessary infrastructure investment for applications not requiring extensive antenna and gateway setups led to the development of LoRa point-to-point (P2P) systems (Sinha, 2017). These systems allow for simple deployment and have demonstrated their utility in sectors such as agriculture, renewable energy monitoring, and logistics and transportation (Iqbal A. and Iqbal T., 2018; Chen et al., 2019; Setiabudi et al., 2022).

While numerous research papers have investigated the performance of P2P LoRa End Device Communication and analysed propagation measurements for LoRa networks in urban environments (Callebaut, 2019), (Iqbal, 2018), (Chen, 2019) , the security implications of employing a P2P LoRa communication link are often overlooked.

With these considerations, this paper offers a thorough end-to-end analysis of payload confidentiality in LoRa P2P communication within remote smart grids. We propose the deployment of algorithms to augment payload security in a P2P network. We explore the integration of IoT hardware encryption features and the implementation of user-controlled Advanced Encryption Standard (AES) algorithms on ESP32 using different modes. In addressing security concerns in SCADA systems, we propose a robust solution for secure P2P communication using AES-128 using CMAC CBC mode on ESP32 with two low cost LoRa devices.

The paper is structured as follows: Section two offers a review of relevant literature in LoRa and IoT security; section three outlines the research focus; section four details the methodology; section five identifies key components central to the research, including the experimental environments; section six presents the results; section seven compares the coverage and security standards of LoRa with other LPWAN providers; and the final section offers a conclusion, summarising the work and providing closing observations.

2 LITERATURE REVIEW

We Secure transmission of data is critical for the development and usability of IoT services in the smart grid. Within the context of the IoT domain, the research concentrates on LoRa and IoT communications security.

Focusing on IoT SCADA systems, the real-world application of LoRa P2P, the vulnerabilities of LoRa physical as well as the studies done on LoRa P2P encryption. A comprehensive review of current research in the area was conducted and some of the key papers and findings from this review are discussed in this section. In this 2022 study, Setiabudi et al (Setiabudi, 2022) develop a system which monitors and controls the speed and vibration of a wind turbine using an Arduino Uno microcontroller

and Bolt IoT WI-FI Module. The paper demonstrates that it can effectively control and monitor Wind Turbines from remote locations utilising the Bolt cloud server which processes the data. Similarly in this 2019 paper, Chen et al (Chen, 2019, develop an open-source SCADA system for solar photovoltaic monitoring and remote control. Again, it demonstrates that IoT SCADA systems can be used to replace traditional SCADA systems found in solar or wind energy generation systems. However, the use of short-range communication links such as Wi-Fi limits the flexibility of these approaches for off-grid or remote location.

The study Setiabudi et al (Setiabudi, 2022)], develop an alternative approach to a Wi-Fi communication for Solar Panel monitoring. They designed a wireless sensor network using P2P LoRa nodes and developed a waiting protocol to help improve packet reception. They integrate thinger.io website as a real-time monitoring medium. They were able to transmit packets over a distance of 3km. However, they neglect to assess any security implications of using LoRa communication which is an important aspect of energy infrastructure. Likewise in the recent 2023 study, Pradeep (Pradap et. al, 2022), presents an approach for detecting forest fires by using a ESP32 microcontrollers, fire detector sensors and LoRa P2P communication between the two ESP32 nodes.
While the results clearly illustrate the real-life application of LoRa P2P communication, the study does not provide any analysis on the need for encryption or applies encryption to the communication link.

LoRa P2P utilises the LoRa physical layer for communication, however serval studies have highlighted vulnerabilities in the layer. Focusing on the confidentiality aspects of the CIA triad, a common confidentiality vulnerability is the challenge of Chirp Spread Spectrum modulation where confidentiality cannot be guaranteed (Paredes, 2019). In the study they were able to record raw transmission of LoRa physical layer using an inexpensive software defined radio (SDR). Using the experimental gr- LoRa out-of-tree module from Bastille Research, they were able to demodulate and decode the LoRa transmission using a GNU radio. They stress the need for securing the LoRa physical layer. They also discuss several common LoRa radio vulnerabilities such as the “Packet in Packet” attack and Jamming attacks. The authors conclude by outlining future work on “further improving the physical layer”. The paper does not provide any means of encryption of the LoRa physical layer but stresses its importance for future work.

The study Pradap et al (Pradap, 2022) , proposes a secure long-range communication model using LoRa (Long Range) technology and ESP32 microcontrollers The study concludes that LoRa communication is possible over distances of 10-15km with minimal to no data loss, making it suitable for peer-to-peer communication style. The results clearly illustrate LoRa P2P encrypted transmission, but the study does not define the power consumption of the additional edge technology required for implementing this encryption, an important consideration of LPWAN and only shows AES basic encryption modes and a weak Caesar cipher methods implementation.

The paper of Ali et al. (Ali, 2022) explores a secure, low-cost communication system for remote micro-grids, implemented with AES cryptography on ESP32, utilising a LoRa module several cryptographic techniques are explored and compared, with the authors concluding that AES provides the most robust security for SCADA systems. The paper highlights the implementation of AES on the ESP32 with LoRa, explaining the steps and security of the algorithm. Test results affirm the system's security and cost- effectiveness, providing a compelling solution to communication challenges in remote micro-grids. However, the authors did not implement or provide a comparison of other AES encryption modes using only the basic AES encryption.

3 RESEARCH QUESTIONS

T The purpose of this paper was to present security issues of LoRa P2P regarding the payload confidentiality of the transmission, more specifically related to smart grids. The research questions to be answered were:

How does the physical layer (PHY) of LoRa implement device and network security for data transmission, and what are its strengths and weaknesses?

What capacities exist to enhance the security of P2P nodes in a LoRa network, and what would be the potential barriers and facilitators to such enhancements?

What potential encryption algorithms could be developed and tested for the integration of end-to-end payload confidentiality in LoRa P2P communication within remote smart grids?

What are the potential performance trade-offs when integrating end-to-end payload confidentiality in LoRa P2P communication within remote smart grids?

How does the integration of IoT hardware encryption features impact the security of LoRa P2P communication in remote smart grids?

4 METHODOLOGY

The procedure for this research unfolded systematically across several defined phases, each with a specific focus and purpose. Here, we elucidate each of these stages.

A. Research Topic Identification
The study is centred on building secure low-cost point to point data networks and examining the associated security challenges.

B. IoT Research and Selection
After outlining the scope, the next step was selecting an apt IoT device and communication network that would satisfy the intricate demands of SCADA communication. A thorough investigation was conducted to ensure an appropriate selection.

C. Literature Review
The comprehensive literature review revealed the enormity of IoT security issues. The review scrutinised numerous journals on various themes such as IoT SCADA systems, IoT communication, security of P2P nodes, software- defined radio, and data capture and demodulation. This helped refine the scope of the research, and specifically addressed research questions around security and encryption.

D. Environment configuration and IoT setup
To yield accurate results, it was necessary to ensure that quality experiments were defined and quality IoT devices and testing tools were used. IoT assembly; device integration; software functionality testing and upgrade; tool testing and selection; data capture and demodulation; C development were among the key challenges.

E. Configuration of Software Defined Radio (SDR)
Data capture and analysis necessitated extensive tool research and testing. The process involved identifying individual functionality requirements for SDR capture, signal playback, demodulation, and their integration and the technical challenges of integrating the software application with the devices.

F. Transmission Capture and Demodulation
Test messages of varying payload lengths were designed and generated for LoRa. The payloads were transmitted. The messages were captured during transmission in the .wav demodulation format. Demodulation of the dataset was performed, to assess potential message vulnerability and payload plaintext exposure.

G. Payload Analysis
Post-demodulation, the output was analysed with an emphasis on the payload. Recognisable patterns between known plaintext input and output were explored. Received messages on the LoRa node were included to provide a comprehensive end to end payload analysis. Visual identification of the captured transmission was reviewed to add to the insights.

H. Payload Encryption
Informed by the payload analysis, encryption mechanisms and algorithms were evaluated. We developed a mix of inherent services and user-level encryption solutions using the AES-128 algorithms to ensure data confidentiality on ESP32 LoRa devices. The test message data from Phase F was used as input data for each encryption algorithm, enabling a broad comparative analysis.

I. Results Evaluation
Data transmitted via ESP32 LoRa devices were captured, demodulated, and compiled for interpretation. The ciphertext data was cross-checked against the known plaintext input and the LoRa message structure. This was then analysed for patterns and vulnerabilities.

J. IoT LPWAN Benchmarking
Finally, a benchmarking analysis was conducted, comparing the LoRa IoT protocol against other similar LPWAN technologies. This step helped determine the standards and quality of security adopted by LoRa and its market competitors.

5 EXPERIMENTS

This section presents the development and implementation of the experiments. Two main experiments were conducted. Experiment one: LoRa transmission signal capture, demodulation, and analysis, involving 2 sub- experiments of pre and post encryption. Experiment two: Payload encryption and packet security, involving three sub-experiments using different AES encryption algorithms.

Each of the two main experiments required a different combination of software and hardware. The Heltec ESP32 V3 LoRa devices were common across all experiments.

Heltec ESP32 V3 LoRa devices were specifically chosen for the study based on them supporting the LoRa protocol and them being referenced in the

LoRaWAN official network operator “The Things Network” as a supported LoRaWAN Node (Triwidyastuti, 2019) . The Heltec ESP32 V3 LoRa devices also provide other network connectivity options of Wi-Fi and Bluetooth, but these were not utilised (Heltec, 2023).

Analysis conducted by Fatima, et al. 2019, pertaining to LoRa’s Chirp Spread Spectrum modulation, reveals LoRa signal transmission confidentiality cannot be guaranteed. In the study Hill et al 2019 (Hill, 2019), relating to LoRa’s application of integrity and authentication between P2P nodes, reveals LoRa is vulnerable to “Packet in Packet” attack and Jamming attacks and in the 2017 study of Aras et al revealed several vulnerabilities and stresses that LoRa “has serious security vulnerabilities that can be exploited by malicious third entities” (Taha, 2021). The LoRa P2P physical layer does not have any encryption, meaning the confidentiality of the payload is optional and up to developers and or manufacturers to implement security features of the LoRa physical layer (GK S., 2022).

Executing the experiments of the signal capture and demodulation and with the various encryption algorithms, required a constant test dataset predefined beforehand. The test dataset was constructed of plaintext payloads of various bytes. The different payload lengths were to test the boundaries of the payload and included special characters. The test dataset is presented in Table 1.

Table 1: Test dataset.

# of bytes	Plaintext payload	Plaintext in Hexadecimal
1	A	41
3	1A2	31 41 32
5	@1B2C	40 31 42 32 43
10	Ab12CD34@.	41 62 31 32 43 44 33 34 40 2E
15	mp047..!bd260h1	6D 70 30 34 37 2E 2E 21 62 64 32 36 30 68 31

5.1 Experiment 1

Experiment 1 performed a capture and evaluation of a LoRa transmission between two P2P nodes. The experiment setup apparatus seen in Figure 1, consisted of two Heltec ESP32 V3 LoRa devices (a sender and a receiver node), (Heltec, 2023) and a Digital RTL-SDR capable of capturing transmissions of DVB-T,FM,DAB,820T2 and LoRa. The software applications necessary to execute the experiments included custom Arduino C code with reference to Heltec manufacture documentation , for the sender and receiver nodes using the configuration settings outlined in Table 2. CubicSDR, an open-source software defined radio application was used for the transmission signal capture and audio file output, mainly used for visual analysis (CubicSDR, 2023). For demodulation of the LoRa signal capture, the open source Gqrx application (Gqrx, 2023) was used for capturing the transmission in .raw format. The open- source GNU Radio application (GNU Radio, 2023), the gr-sigmf out-of-tree (OOT) module for reading and writing SigMF datasets (SkySafe, 2023) and the gr-LoRa OOT module (RPP0, 2023) of GNU Radio blocks for the actual demodulation of the LoRa signal were utilised.

The Heltec ESP32 V3 LoRa devices was programmed, with one to transmit the test dataset and the other one to receive the payloads. The devices were programmed to transmit on the frequency channel of 867.9 MHz’s. CubicSDR was tuned to the LoRa frequency of 867.9 MHz and to recording mode for capturing .wav files. We utilised CubicSDR for its visual analysis of the transmission. However .wav file format is not great for demodulation of a LoRa signal. A better data format for radio frequencies (RF) is the sigmf data format (Hilburn, 2017) This required capturing the signal in a .raw file format. Gqrx application was used for capturing the signal and providing the data in Raw format.

The LoRa sender device transmitted the individual message and the LoRa transmission was picked up by Gqrx, where it was centring on each individual LoRa signal and recorded the transmission in Raw format. To convert the .raw file into the two sigmf data formats (.sigmf-data & .sigmf- meta) required the use of the GNU Radio application. GNU radio application provides signal processing blocks. We created a flow graph using a combination of blocks provided by gr-sigmf and GNU Radio to convert the Raw to .sigmf datasets.

Gr-LoRa, an open-source physical layer implementation of the LoRa protocol which supports demodulation of LoRa signals, was used to process the .sigmf datasets for demodulation and analysis.

Table 2: LoRa Configuration settings.

Configuration Type	Configuration Value
Radio Frequency	867.9 MHz
Output Power	10
Bandwidth	125
Spreading Factor (SF)	12
Preamble Length	8

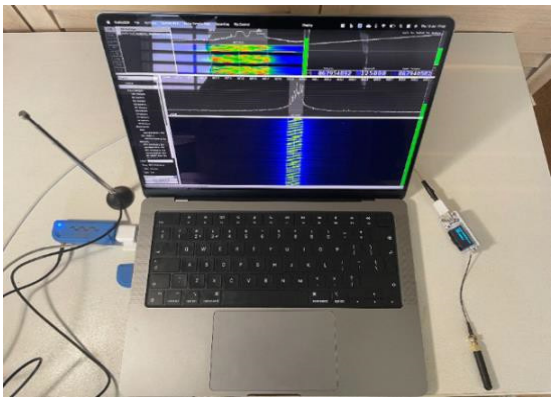

Figure 1: LoRa signal capture experiment apparatus.

5.2 Experiment 2

In Experiment 2, a sequence of tests was conducted to investigate the secure preparation, encryption, and transmission of messages within the ESP32-based LoRa communication system for a LoRa P2P network. For this purpose, we utilised AES encryption algorithms to protect the confidentiality of transmitted data.

The Advanced Encryption Standard (AES) is a globally accepted symmetric encryption algorithm (Rijmen, 2001). It can operate with a key length of 128, 192, or 256 bits, and a fixed block size of 16 bytes. It supports various modes of operation, including Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR), each with its own security characteristics and use cases. For our experiment, AES-128 was selected and a range of operation modes were experimented; ECB, CTR & CBC. Compared to AES-256 and RSA, AES-128 uses less resources and does not require high computational power for encryption and decryption, important for LPWAN devices . The libraries we used to implement AES-128 were verified against the data in the National Institute of Standards & Technology (NIST, 2001)

Using a minimal sized AES encryption library for embedded systems and low power chips was an important consideration for LPWANS. Using the tiny-AES-c library (KOKKE, 2023) the tiny-AES-CMAC-c library (Elektronika-ba,, 2023) and the Arduino c library (Arduino-libraraies, 2023). The tiny-AES-c library implemented all 3 modes of AES-128 encryption in a compact and small library useful for embedded systems. However, with this library there are no safety mechanisms for typical C and C++ issues such out of bounds memory access which required extra development work to implement in the embedded system.

1) AES – Electronic Code Book (ECB):
In ECB mode, each block of plaintext is encrypted independently using the same key. It's simple and fast but offers the least security among the modes. This is because identical plaintext blocks produce identical ciphertext blocks, making it susceptible to pattern attacks.

2) AES – Counter (CTR)
CTR mode effectively turns the block cipher into a stream cipher. It involves encrypting a sequence of incrementing counters (initially seeded with a nonce) with the cipher's key, and the resulting cipher stream is XORed with the plaintext to get the ciphertext. It's parallelisable and it supports input data of any length, and padding is not required (Conti, 2017). As padding is not required it saves on the size of the message, improving the transmission performance.

3) AES – Cipher Block Chaining (CBC)
CBC mode introduces dependency between blocks for increased security. Each plaintext block is XORed with the previous ciphertext block before being encrypted. An Initialisation Vector (IV) is needed for the first block. Due to chaining, it's not parallelisable and requires padding for non- multiple block size inputs. The specific key and IV values need to be managed and securely updated as part of our overall system design .

4) AES – CBC with Cipher-based message authentication code (CMAC)
In this setup, not only is the data encrypted using CBC mode, but an AES-CMAC is also computed for message authentication. CMAC is a type of Message Authentication Code (MAC) that provides assurance of data integrity and authenticity. The CMAC is computed over the data and appended to the end of the message, allowing the receiver to verify the integrity of the message upon decryption . The tiny-AES-CMAC-c library is flexible because it uses the original encryption functions as a call-back to calculate the digest of the original message.

Every subset of Experiment 2 was re-examined using the procedures from Experiment 1, which involved capturing the LoRa transmission signal, demodulating it, and analysing the executed code. Each subset experiment required the Heltec ESP32 V3 LoRa sender device to be flashed with the selected encryption algorithm.offers the least security among the modes. This is because identical plaintext blocks produce identical ciphertext blocks, making it susceptible to pattern attacks.

5) AES – Counter (CTR)

CTR mode effectively turns the block cipher into a stream cipher. It involves encrypting a sequence of incrementing counters (initially seeded with a nonce) with the cipher's key, and the resulting cipher stream is XORed with the plaintext to get the ciphertext. It's parallelisable and it supports input data of any length, and padding is not required (Lipmaa et al., 2020). As padding is not required it saves on the size of the message, improving the transmission performance.

6) AES – Cipher Block Chaining (CBC)

CBC mode introduces dependency between blocks for increased security. Each plaintext block is XORed with the previous ciphertext block before being encrypted. An Initialisation Vector (IV) is needed for the first block. Due to chaining, it's not parallelisable and requires padding for non- multiple block size inputs. The specific key and IV values need to be managed and securely updated as part of our overall system design (Almuhammadi and Al-Hejri, 2017).

7) AES – CBC with Cipher-based Message Authentication Code (CMAC)

In this setup, not only is the data encrypted using CBC mode, but an AES-CMAC is also computed for message authentication. CMAC is a type of Message Authentication Code (MAC) that provides assurance of data integrity and authenticity. The CMAC is computed over the data and appended to the end of the message, allowing the receiver to verify the integrity of the message upon decryption (Stanco, 2022)(The tiny-AES-CMAC-c library is flexible because it uses the original encryption functions as a call-back to calculate the digest of the original message.

Every subset of Experiment 2 was re-examined using the procedures from Experiment 1, which involved capturing the LoRa transmission signal, demodulating it, and analysing the executed code. Each subset experiment required the Heltec ESP32 V3 LoRa sender device to be flashed with the selected encryption algorithm.

6 RESULTS

6.1 Experiment One: LoRa Transmission Signal Capture, Demodulation and Analysis

The following section presents the outcomes from the LoRa data capture and analysis experiment. Output data are presented in the form of demodulated transmissions.

6.1.1 Visual Analysis

For each LoRa message transmitted, it can be observed in the Cubic SDR waterfall which visualises the frequency content of a signal over time, each individual chirp and the make-up of the transmission.

Chirp Spread Spectrum (CSS) modulation, as used in LoRa, is designed to enhance communication robustness, even in challenging conditions such as high noise environments, signal fading, or high network density. This is largely because CSS modulates the signal across a range of frequencies, which can make it more resistant to interference and noise that might be present at a single frequency.

The Heltec ESP32 V3 LoRa sender device transmission appears as a series of 'chirps'. These 'chirps' sweep across a range of frequencies. Depending on the spreading factor (SF) used, the chirp can be wider or narrower, slower, or faster. In our case we used a SF of 12 which is the highest spread factor so you can clearly see the thickness of the individual chirp across the frequency spectrum range.

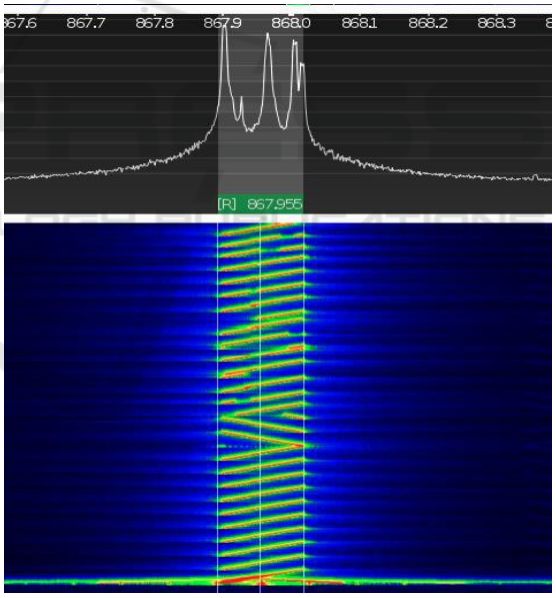

Figure 2: LoRa transmission waterfall captured by an SDR.

The Bandwidth of a LoRa signal is the range of frequencies over which a chirp sweeps. A higher bandwidth means that the chirp is longer in frequency, which shows up as a longer line in the waterfall display. These characteristics of the LoRa transmission help the signals get through high density spectrum.

The waterfall also visibly shows the preamble and Start of Frame. A continuous number of up-chirps is the preamble, and two down chirps is the start of

Table 3: LoRa Phy frame structure.

LoRa Phy Frame					
Phy Frame	***Preamble***	***PHDR (Physical Header)***	***PHDR_CRC (Header Cyclic Redundancy Check)***	***Phy Payload***	***CRC***
Size	Min 4.25 symbols	2 bytes	2 bytes	Max. 255 bytes	2 bytes
		Coding rate = 4/8		Coding rate = 4/(4 + CR), where CR = 0,1,2,3 or 4	

Table 4: LoRa p2p demodulation findings.

#[a] of bytes	Plaintext Payload	Captured Transmission Demodulated	Converted to Ascii
1	A	41	A
3	1A2	31 41 32	1A2
5	@1B2C	40 31 42 32 43	@1B2C
10	Ab12CD34@.	41 62 31 32 43 44 33 34 40 2E	Ab12CD34@.
15	mp047..!bd260h1	6D 70 30 34 37 2E 2E 21 62 64 32 36 30 68 31	mp047..!bd260h1

frame delimiter, and these indicate the start of the data frame.

Signal Capture and Demodulation

The Gqrx captured the Raw transmission. Using the GNU Radio to interface with the hardware SDR performed signal processing on the input transmission. The Gqrx Raw transmission was converted to the .sigmf format and then piped into the gr-LoRa application where demodulation of the LoRa transmission was performed as programmed.

Table 4 presents an analysis of findings from LoRa message transmission utilising the transmission configuration outlined in Table 2. The Gr-LoRa captured and demodulated payload content can be easily converted from its hexadecimal form to ASCII, revealing the original plaintext message.

6.2 Experiment Two: Payload Encryption

Having confirmed that LoRa P2P communication defaults to unencrypted payload transmission in Experiment 1, Experiment 2 consisted of multiple experiments integrating and testing the different AES algorithms in the Heltec ESP32 V3 LoRa devices. Performance cost and payload encryption quality were key considerations of the algorithm analysis.

1) AES – ECB Mode

In the first experiment, we implemented AES in ECB mode. ECB's simplicity became evident: each plaintext block is encrypted separately, making it a highly efficient mode. This independent block encryption allowed for a high-speed operation, with a processing time of just 49179 µs, a characteristic particularly beneficial for real-time systems. As ECB does not require Initialisation Vectors (IV), it reduces the overhead on resource limited IoT devices. However, the efficiency and simplicity of ECB mode comes with its own vulnerabilities. The deterministic nature of the encryption means the same plaintext block always yields the same ciphertext block when encrypted with the same key. This was empirically confirmed by our experiments, where identical plaintext messages consistently yielded identical ciphertext blocks, as seen in the ECB Mode of Table 6. This makes it susceptible to frequency analysis and pattern detection attacks.

2) AES – CTR Mode

The second experiment involved the implementation of AES in CTR mode. CTR, a type of stream cipher, encrypts a counter value initialised with a nonce rather than the plaintext itself. The resulting encrypted counter value is then XORed with the plaintext to produce the ciphertext. This approach breaks the deterministic relationship between the plaintext and the ciphertext, making it more challenging to detect patterns in the encrypted data. However, implementing CTR mode requires robust key and counter management solutions to maintain synchronisation. In our experiments, we encountered issues with key and counter synchronisation between the two devices, leading to failed transmissions or rejected messages, potentially due to system clock differences of the sender and receiver nodes or due to issues with the integration of the AES library with the Arduino library, we could not accurately narrow down the problem.

3) AES – CBC Mode

Our third experiment explored the AES in CBC mode. Unlike ECB and CTR, CBC introduces an inter-block dependency. Each plaintext block is XORed with the previous ciphertext block before being encrypted. This inter- block dependency effectively mitigates the issue of pattern detection present in ECB, yielding better data confidentiality. Our results, displayed in the CBC Mode of Table 7, demonstrate this benefit: identical plaintext blocks, when encrypted with the same key, produced different ciphertext blocks. However, CBC mode requires the use of an Initialisation Vector (IV) to enable this benefit, adding to the system complexity.

4) AES – CBC Mode with CMAC

In our final experiment, we appended an AES-CMAC (Cipher-based Message Authentication Code) to our CBC- encrypted messages. CMAC is a type of MAC that provides assurance of data integrity and authenticity. With CBC- CMAC, our LoRa P2P communication system offers both data confidentiality and integrity. This extra layer of security introduced additional computational overhead. As evidenced by the increase in processing time in our results to 65136 µs, it's clear that this mode, while secure, demands more processing resources although minimal. Comparing CBC and CBC-CMAC in the power consumption table, it is evident that the power consumption is slightly higher when CMAC is used, registering 0.06839 µW due to the additional computational steps involved in generating the MAC. The addition of the CMAC also appended more bytes to the message transmission. Our experiments revealed that the choice of encryption mode significantly impacts the confidentiality, data integrity, performance efficiency, and resource requirements of a LoRa P2P system. It highlighted the fact that there's no 'one-size-fits-all' solution and that a careful balance between these factors needs to be struck depending on the specific requirements of the system in question. In our case for P2P remote grid connections, CBC-CMAC offers the best security among the options tested.

Table 5: Encryption processing times and power consumption.

	Plaintext	**ECB**	**CBC**	**CBC-CMAC**
Processing Time	49179 µs [a]	50740 µs	54581 µs	65136 µs
Power Consumption	0.03408 µW [b]	0.068392 µW	0.05731 µW.	0.06839 µW

7 LPWAN IoT BENCHMARKING

LPWAN benchmarking was conducted to compare the main competing technologies in the LPWAN market: LoRa, NB-IoT, and SigFox. Benchmarking is key to evaluating competing providers, their key differentials, and their approach to security. The study conducted by (Pérez, 2022) performed a comparative study of LPWAN technologies LoRaWAN and SigFox . While the study conducted by (Stanco, 2022) on the performance of IoT LPWAN technologies for NB-IOT, SigFox and LoRaWAN. The results of the LPWAN benchmarking are presented in Table 8.

Table 6: Illustrating ECB encryption weakness.

ECB Mode – (LoRa-Is-a-LPWAN!)			
1	***2***	***3***	***4***
Transmission Number	***Plaintext Payload***	***Number Of Bytes***	***Ciphertext Payload***
1	A	16	9E72427DF27DD22A355C3FB13A3AB1A9
2	A	16	9E72427DF27DD22A355C3FB13A3AB1A9
3	mp047..!bd260h1	16	13B2805995F211854833169FD140361D
4	mp047..!bd260h1	16	13B2805995F211854833169FD140361D

Table 7: Illustrating CBC encryption strength.

CBC Mode – (LoRa-Is-a-LPWAN!)			
1	***2***	***3***	***4***
Transmission Number	***Plaintext Payload***	***Number of Bytes***	***Ciphertext Payload***
1	A	16	ceeec1b5d2ec3241f2d53fe07a759257
2	A	16	169e6d845226a055477d6c526ac722f5
3	mp047..!bd260h1	32	e6dac1f02e7df0457d4a245a3decac0a
4	mp047..!bd260h1	32	13dae2ac9c4653a3190de80a3d48ff00

Table 8: Illustrating CBC-CMAC encryption strength.

CBC-CMAC Mode – (LoRa-Is-a-LPWAN!)			
1	*2*	*3*	*4*
Transmission Number	*Plaintext Payload*	*Number of Bytes*	*Ciphertext Payload*
1	A	32	707154bb1243dce5dbc33a3eaa59fac8
2	A	32	4c8d0b498b4b4264dc8d1c9aa59abf3a
3	mp047..!bd260h1	32	de74920f3f4e1409fb9ba1b01fb6d454
4	mp047..!bd260h1	32	cc684825756423b8c56d3289f3928836

Starting with NB-IoT, it is built upon the Long-Term Evolution (LTE) wireless standard, which is a trusted and reliable standard for wireless communication of mobile devices and data terminals, hinging on GSM/EDGE technology. Mobile operators implement a layered model of security in NB-IoT, encompassing high encryption standards with AES 256 for communications and data storage. While its high infrastructure cost could be a barrier for some applications, its robust security measures and high payload capacity of 1600 bytes position it well for applications requiring secure and extensive data transmission.

SigFox offers an alternative approach with a unique ecosystem design where encryption is not implemented by default. This structure, along with its maximum payload limit of 12 bytes per message and 140 messages per day, may limit its applicability for high data transmission applications but proves cost-effective and efficient for use-cases accepting low data rates.

LoRa stands out with its proprietary standard operating primarily on the ISM band, offering deployment flexibility. A salient feature is its Chirp Spread Spectrum modulation that helps mitigate multipath propagation effects for more accurate transmission. While the LoRaWAN protocol ensures end-to-end AES 128 encryption, the LoRa physical layer (LoRa PHY) itself does not inherently include encryption. The lack of inherent encryption in LoRa PHY does raise security concerns as seen in this paper; however, it also lowers infrastructure costs due to its capacity for point- to-point communication, thereby eliminating the need for a gateway, unlike LoRaWAN. This trade-off is an important consideration for LoRa's adoption in IoT applications.

Each of the competing LPWAN technologies, LoRa, NB- IoT and SigFox present distinct strengths and potential limitations depending on the specific requirements of the use- case. For LoRa, it has a unique potential for low-cost, high- coverage range, and more accurate transmission owing to its modulation scheme.

Table 9: LPWAN Technologies Benchmarking.

	LoRa	**NB-IoT**	**SigFox**
Standard	Proprietary	Open	Proprietary
Spectrum	ISM	Licensed	ISM
Modulation	Chirp Spread Spectrum	Orthogonal Frequency-Division Multiplexing	D-BPSK [a]
Range	< 20km	< 10km	>40km
Payload	243 bytes	1600 bytes	12 bytes
Encryption	LoRa PHY: No inherent encryption, LoRaWAN: AES 128	end-to-end +AES 256	Transmission AES 128
Battery	+10 years	+10 years	+10 years
Cost	Low	High	Low

a. Differential Binary Phase Shift Keying

8 CONCLUSION

In our comprehensive study on LoRa P2P communication, particularly within the context of remote smart grids. We have focused on the critical aspect of payload confidentiality of a LoRa P2P network, exploring the potential of IoT hardware encryption features and the application of user-controlled AES algorithms on an ESP32 device. Our findings have culminated in a proposal for a robust solution that leverages AES cryptography in providing a more secure communication for LoRa P2P networks.

The experiments we conducted involved capturing and demodulating LoRa transmission signals, followed by a thorough analysis of the payload. We also assessed various encryption mechanisms and algorithms, leading us to develop encryption solutions at the user level using the AES algorithms. These solutions aim to ensure data confidentiality on ESP32 LoRa devices.

Our findings indicate that integrating end-to-end payload confidentiality in LoRa P2P communication is indeed feasible, although it may involve minor performance trade- offs. They reveal that the enhanced security considerably outweighs the minor performance degradation and a slight increase in battery usage. This research contributes significantly to the field of secure communication in remote smart grids, offering valuable insights into the potential security risks and trade-offs involved in implementing LoRa P2P in IoT applications such as remote smart grids.

In conclusion, our study has highlighted some key avenues for future investigations. Expanding the scope of encryption algorithms tested, specifically venturing into higher-strength solutions such as RSA and AES-256, focusing on finding the most effective and power-efficient algorithm offers promising new research. Furthermore, the investigation of secure LoRa P2P communication in challenging real-world scenarios, like in a P2P production environment, stands out as an important future endeavor, accentuating a long-term, empirical evaluation of remote grid performance. We also advocate for ongoing improvements in LoRa P2P system security, potentially presenting a cost- efficient alternative to LoRaWAN for point-to-point communication infrastructure needs.

Our research expansion has vital implications for secure IoT applications and aids in developing cyber-resilient energy infrastructures.

REFERENCES

Ahmadi, A., Moradi, M., Cherifi, C., Cheutet, V., & Ouzrout, Y. (2018, December). Wireless connectivity of CPS for smart manufacturing: A survey. In *2018 12th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)* (pp. 1- 8). IEEE.

Almuhaya, M. A., Jabbar, W. A., Sulaiman, N., & Abdulmalek, S. (2022). A survey on LoRa wan technology: Recent trends, opportunities,s imulation tools and future directions. *Electronics*, *11*(1), 164.

United Nations. "Sustainable Development Goals." [Online]. Available: https://sdgs.un.org/goals. [Accessed: June 20, 2023].

Devalal, S., & Karthikeyan, A. (2018, March). LoRa technology-an overview. In *2018 second international conference on electronics, communication and aerospace technology (ICECA)* (pp. 284-290). IEEE.

Ferreira, A. E., Ortiz, F. M., Costa, L. H. M., Foubert, B., Amadou, I., & Mitton, N. (2020). A study of the LoRa signal propagation in forest, urban, and suburban environments. *Annals of Telecommunications*, *75*, 333-351.

Fillatre, L., Nikiforov, I., & Willett, P. (2017). Security of SCADA systems against cyber–physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, *32*(5), 28-45.

GIoTitsas, C., Pazaitis, A., & Kostakis, V. (2015). "A peer-to-peer approach to energy production". *Technology in Society*, *42*, 28-38.

Khan, F., Siddiqui, M. A. B., Rehman, A. U., Khan, J., Asad, M. T. S. A., & Asad, A. (2020, February). IoT based power monitoring system for smart grid applications. In *2020 international conference on engineering and emerging technologies (ICEET)* (pp. 1-5). IEEE.

Rizzetti, T. A., Wessel, P., Rodrigues, A. S., Da Silva, B. M., Milbradt, R., & Canha, L. N. (2015, September). Cyber security and communications network on SCADA systems in the context of Smart Grids. In *2015 50th International Universities Power Engineering Conference (UPEC)* (pp. 1-6). IEEE.

Tawde, R., Nivangune, A., & Sankhe, M. (2015, March). Cyber security in smart grid SCADA automation systems. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-5). IEEE.

Petajajarvi, J., Mikhaylov, K., Roivainen, A., Hanninen, T., & Pettissalo, M. (2015, December). On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology. In *2015 14th international conference on its telecommunications (itst)* (pp. 55-59). IEEE.

Patil, V. H., Kadam, P., Bussa, S., Bohra, N. S., Rao, A., & Dharani,

(2022, December). Wireless Communication in Smart Grid using LoRa Technology. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 894-899). IEEE.

LoRa Alliance. [Online]. Available: https://LoRa-alliance.org/. [Accessed: June 21, 2023].

Magrin, D., Centenaro, M., & Vangelista, L. (2017, May). Performance evaluation of LoRa networks in a smart city scenario. In *2017 IEEE International Conference on communications (ICC)* (pp. 1-7).

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express*, *5*(1), 1-7.

Rawat, A. S., Rajendran, J., Ramiah, H., & Rana, A. (2020, August). LORA (Long Range) and LORAWAN technology for IoT applications in Covid-19 pandemic. In *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)* (pp. 419-422). IEEE.

Poursafar, N., Alahi, M. E. E., & Mukhopadhyay, S. (2017, December). Long-range wireless technologies for IoT applications: A review. In *2017 Eleventh International Conference on Sensing Technology (ICST)* (pp. 1-6). IEEE.

Sinha, R. S., Wei, Y., & Hwang, S. H. (2017). A survey on LPWA technology: LoRa and NB-IoT. *Ict Express*, *3*(1), 14-21.

Callebaut, G., & Van der Perre, L. (2019). Characterization of LoRa point-to-point path loss: Measurement campaigns and modeling considering censored data. *IEEE Internet of Things Journal*, *7*(3), 1910-1918.

Iqbal, A., & Iqbal, T. (2018, October). Low-cost and secure communication system for remote micro-grids using AES cryptography on ESP32 with LoRa module. In *2018 IEEE Electrical Power and Energy Conference (EPEC)* (pp. 1-5). IEEE.

Chen, T., Eager, D., & Makaroff, D. (2019, July). Efficient image transmission using LoRa technology in agricultural monitoring IoT systems. In *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 937-944). IEEE.

Setiabudi, D., Herdiyanto, D. W., Kurniawan, A., Muldayani, W., Chaidir, A. R., & Rahardi, G. A. (2022, November). Design Of Wireless Sensor Network (WSN) System Using Point to Point And Waiting Protocol Methods For Solar Panel Monitoring. In *2022 International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT)* (pp. 232-240). IEEE.

Paredes, M., Bertoldo, S., Carosso, L., Lucianaz, C., Marchetta, E., Allegretti, M., & Savi, P. (2019). Propagation measurements for a LoRa network in an urban environment. *Journal of Electromagnetic Waves and Applications*, *33*(15), 2022-2036.

Pradap, A., Latifov, A., Yodgorov, A., & Mahkamjonkhojizoda, N. (2023, March). Hazard Detection using custom ESP32 Microcontroller and LoRa. In *2023 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (pp. 36-40). IEEE.

Triwidyastuti, Y. (2019). Performance analysis of point-to-point LoRa end device communication. *Lontar Komputer: Jurnal Ilmiah Teknologi Informasi*, *10*(3), 140-149.

Ali, M. J., Mondal, A., & Dutta, P. (2022, June). Intelligent monitoring and control of wind turbine prototype using Internet of Things (IoT). In *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-6). IEEE.

Aghenta, L. O., & Iqbal, M. T. (2019, May). Development of an IoT based open source SCADA system for PV system monitoring. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* (pp. 1-4). IEEE.

Taha, F. A., & Althunibat, S. (2021, October). Improving data confidentiality in chirp spread spectrum modulation. In *2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1-6). IEEE.

Hill, K., Gagneja, K. K., & Singh, N. (2019, March). LoRa PHY range tests and software decoding-physical layer security. In *2019 6th international conference on Signal Processing and Integrated Networks (SPIN)* (pp. 805-810). IEEE.

GK, S. (2022). Encrypted P2P Communication using LoRa waves. Available: https://www.techrxiv.org/ndownloader/files/37603913/1 [Accessed: June 23, 2023].

"The Things Network," [Online]. Available: https://ttnet.org/device- repository. [Accessed: June 28, 2023].

"Heltec Automation" [Online]. Available: https://heltec.org/project/wifi-LoRa-32-v3/ [Accessed: June 28, 2023].

Aras, E., Ramachandran, G. S., Lawrence, P., & Hughes, D. (2017, June). Exploring the security vulnerabilities of LoRa. In *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)* (pp. 1-6). IEEE.

NooElec. "NESDR Mini 2: Tiny RTL-SDR & DVB-T USB Stick." [Online]. Available: https://www.nooelec.com/store/sdr/sdr-receivers/nesdr-mini-2.html. [Accessed: June 28, 2023]

Heltec Automation. "Quick Start Guide - ESP32 Series." [Online]. available: https://docs.heltec.org/en/node/esp32/quick_start.html. [Accessed: June 29, 2023]

CubicSDR. "CubicSDR Software." [Online]. Available: https://cubicsdr.com/. [Accessed: June 29, 2023]

GNU Radio. [Online]. Available: https://www.gnuradio.org/. [Accessed: June 30, 2023]

SkySafe. "gr-sigmf: GNU Radio blocks for reading and writing SigMF files." GitHub. [Online]. Available: https://github.com/skysafe/gr- sigmf. [Accessed: June 30, 2023]

RPP0. "gr-LoRa: A GNU Radio OOT module for LoRa transmission and reception." GitHub. [Online Available: https://github.com/rpp0/gr-LoRa. [Accessed: June 30, 2023]

"Gqrx Software Defined Radio Receiver." [Online]. Available: https://gqrx.dk/. [Accessed: June 30, 2023]

B. Hilburn, "SigMF: An Open Format for Capturing and Sharing Signal Metadata," presented at the GNU Radio Conference 2017, September 11-15,2017. [Online]. Available: https://www.gnuradio.org/grcon/grcon17/presentations/sigmf/Ben- Hilburn-SigMF.pdf. [Accessed: July 01, 2023]

Xu, Z., Tong, S., Xie, P., & Wang, J. (2023). From Demodulation to Decoding: Toward Complete LoRa PHY Understanding and Implementation. *ACM Transactions on Sensor Networks*, *18*(4), 1-27.

Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. *Proceedings of federal information processing standards publications, national institute of standards and technology*, *19*, 22.

Conti, F., Schilling, R., Schiavone, P. D., Pullini, A., Rossi, D., Gürkaynak, F. K., ... & Benini, L. (2017). An IoT endpoint system-on-chip for secure and energy-efficient near-sensor analytics. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *64*(9), 2481- 2494.

Lipmaa, H., Rogaway, P., & Wagner, D. (2000, October). CTR-mode encryption. In *First NIST Workshop on Modes of Operation* (Vol. 39).

Almuhammadi, S., & Al-Hejri, I. (2017, April). A comparative analysis of AES common modes of operation. In *2017 IEEE 30th (CCECE)* (pp. 1-4). IEEE.

Gladisch, A., Rietschel, S., Mundt, T., Bauer, J., Goltz, J., & Wiedenmann, S. (2018, October). Securely connecting IoT devices with LoRaWAN. In *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (pp. 220-229). IEEE.

Pérez, M., Sierra-Sánchez, F. E., Chaparro, F., Chaves, D. M., Paez- Rueda, C. I., Galindo, G. P., & Fajardo, A. (2022). Coverage and Energy-Efficiency Experimental Test Performance for a Comparative Evaluation of Unlicensed LPWAN: LoRaWAN and SigFox. *IEEE Access*, *10*, 97183-97196.

Stanco, G., Botta, A., Frattini, F., Giordano, U., & Ventre, G. (2022, May). On the performance of IoT LPWAN technologies: the case of SigFox, LoRaWAN and NB-IoT. In *ICC 2022-IEEE International Conference on Communications* (pp. 2096-2101). IEEE.

National Institute of Standards and Technology. (2001). Special Publication 800-38A, Appendix F: Example Vectors for Modes of Operation of the AES

KOKKE. "tiny-AES-c: A compact & portable AES implementation in C." [Online]. Available: https://github.com/kokke/tiny-AES-c. [Accessed: June 27, 2023]

Elektronika-ba. "tiny-AES-CMAC-c: Tiny AES CMAC implementation in C programming language." [Online]. Available: https://github.com/elektronika-ba/tiny-AES-CMAC-c. [Accessed: June 27, 2023].

Arduino-libraries. "Arduino Libraries." [Online]. Available: https://github.com/arduino-libraries. [Accessed: June 27, 2023]

Suárez-Albela, M., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (2018, June). A practical performance comparison of ECC and RSA for resource-constrained IoT devices. In *2018 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.