Encrypted P2P Communication using LoRa waves

Sanjay G K, Sai Bharath R Rao, Amith G, *Students* of Electronics and Communication Engineering, R.N.S Institute of Technology, Bengaluru, Karnataka, 560098 INDIA e-mail: (see https://www.rnsit.ac.in/contact-us/).

***Abstract*—Secure communication over large distances is not possible with conventional Wifi or cellular networks. A long range secure communication model is required for such conditions. This paper puts forth a communication model suitable for information exchange over a such large distances.**

LoRa (Long Range) is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology. The typical range provided by LoRa can be up to three miles (5 km) in urban areas, and up to 10 miles (15 km) or more in rural areas of line of sight. LoRa's high range is characterized by high wireless link budgets of around 155 dB to 170 dB. ESP32 is a series of low-cost, low-power system on chip microcontrollers. The LoRa modem is available as the SX127X module which is connected to the ESP32 boards.

Data security is ensured by performing data encryption on the sender board and data decryption on the reciever board. The algorithms for encryption and decryption shown in this article is the AES method. This paper also explores the possibility of hijacking the data while transmitting and shows which algorithms are immune to attacks and which can be easily broken. The use cases for such a communication system could be for secure 2-way communication, communication in remote areas where cellular and Wifi are not available, effecient control of IOT devices over a much larger distance, control of unmanned ground and aerial vehicles, etc.

***Index Terms*—LoRa, ESP32, Lora module, Encryption, Cryptanalysis, Chirp Spread Spectrum, cryptographic hardware acceleration.**

I. Introduction

IN the age of WiFi 6 and superior cellular network, there is still need for a mode of communication that incorporates the features of WiFi and also the coverage distance similar to that of a cellular network. This study proposes one such method of communication using LoRa waves. LoRa stands for Long Range, these waves can travel upwards of 20km in the direction of line-of-sight and around 10-15km with obstructions or disturbances. As WiFi has a range of only a few 100 metres, and the infrastructure required to set up a cellular network being high, LoRa communication becomes a feasible option available for remote and inaccessible areas.

By using an ESP32 board to control the LoRa module, data security can also be ensured by performing encryption and decryption of data. ESP32 is a microcontroller which supports all kinds of encryption methods. Even though there might be other options which may be applicable in identical situations the reasons we chose the LoRa method are:

1) Low Power requirements: The Semtech SX127X LoRa radio transceivers are designed for battery-powered LoRa applications and complies with the LoRaWAN radio transmission standard. When transmitting or receiving data, it draws only 4.2 milliamperes(mA) with an RF output power of +22 dBm. A lower power version, the SX1261, has an RF output power of +15 dBm. Both are half-duplex transceivers that operate in the sub-GHz range and handle constant envelope modulation schemes such as LoRa, as well as frequency shift keying (FSK).

2) Lower Infrastructure Costs: There is no major infastructure required to setup this unit. Since these waves can travel through walls as well the unit is functional anywhere and everywhere.

3) Data transfer Rate: The LoRa model paired with an ESP32 can manage data transfer rates between 300 bps to 37.5 kbps. These speed are great for transferring control instructions or crucial information, for example, confidential warfare data to and from the battlefield., and other such information where high transfer rates are not important.

4) Range: The LoRa module has a line-of-sight range of around 15KM, which is way farther than what WiFi can manage.

5) Error Correction: This makes use of the Forward Error Correction coding which is used for controlling errors in data over unreliable or noisy communication channels. The central idea is the sender encodes the message with redundant information in the form of an ECC. The redundancy allows the receiver to detect a limited number of errors that may occur anywhere in the message, and often to correct these errors without re-transmission. The maximum fractions of errors or of missing bits that can be corrected is determined by the design of the ECC code, so different error correcting codes are suitable for different conditions. In general, a stronger code induces more redundancy that needs to be transmitted using the available bandwidth, which reduces the effective bit-rate while improving the received effective signal-to-noise ratio.

In summary the objectives of this paper are:

- Design two units containing LoRa module, ESP32 board and Antenna each to act as transmitter and reciever.
- Create a successful link between transmitter and reciever.
- Transfer encrypted data and show recieved data after decryption.
- Perform Cryptanalysis attacks on the data being transferred to ensure security during data transfer.

These objectives will enable us to portray a working communication channel using the LoRa waves.

II. Prerequisites

A. ESP32

ESP32 is a series of low-cost, low-power system on a chip microcontrollers with integrated Wi-Fi and dual-mode Bluetooth. The ESP32 series employs either a Tensilica Xtensa LX6 microprocessor in both dual-core and single-core variations, Xtensa LX7 dual-core microprocessor or a single-core RISC-V microprocessor and includes built-in antenna switches, RF balun, power amplifier, low-noise receive amplifier, filters, and power-management modules. ESP32 is created and developed by Espressif Systems,a Shanghai-based Chinese company, and is manufactured by TSMC using their 40 nm process. It is a successor to the ESP8266 microcontroller.

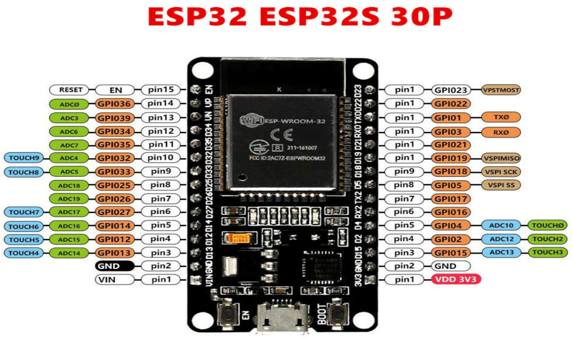


Fig. 1: Pin configuration of ESP32

B. SX127X LoRa module

The SX1276/77/78/79 transceivers feature the LoRa® long range modem that provides ultra-long range spread spectrum communication and high interference immunity whilst minimizing current consumption. Using Semtech's patented LoRa modulation technique SX1276/77/78/79 can achieve a sensitivity of over -148dBm using a low cost crystal and bill of materials. The high sensitivity combined with the integrated +20dBm power amplifier yields industry leading link budget making it optimal for any application requiring range or robustness. LoRa also provides significant advantages in both blocking and selectivity over conventional modulation techniques, solving the traditional design compromise between range, interference immunity and energy consumption.

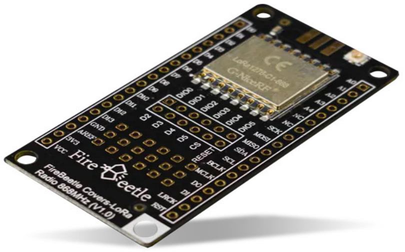


Fig. 2: LoRa module

C. LED display

Just a simple LED display mounted on top of the LoRa module to display the required parameters.

D. Antenna

This is required to aid the transmission and reception of data from the LoRa modules.

Fig. 3: LED Display and Antenna

E. Software

To interact with the ESP32 board we need an arduino environment and the encryption and decryption algorithms are coded using the C++ programming language.It is well known that this C++ is a general-purpose programming language created by Bjarne Stroustrup as an extension of the C programming language, or ”C with Classes”. The language has expanded significantly over time, and modern C++ now has object-oriented, generic, and functional features in addition to facilities for low-level memory manipulation. It is almost always implemented as a compiled language, and many vendors provide C++ compilers. Its main features of designed with an orientation toward systems programming and embedded, resource-constrained software and large systems, with performance, efficiency, and flexibility of use are the reasons why this was chosen as the language for the algorithms.

We also require the Mbed TLS library which is a C library that implements cryptographic primitives and certificate management among several other functions. Its small code footprint makes it suitable for embedded systems.

III. Design and Development

Initially, the LoRa modem has to be soldered onto the ESP32 board while carefully matching the their pins as any one wrong connection will cause damage to the entire board. A LED display should also be soldered in a similiar fashion. Here, we make use of a pre-built unit from Heltec and power it using a micro-USB cable. The pin Diagram is shown in Figure 4.

Figure 5 represents the entire working setup required, where the transmitter block is one ESP32 board and LoRa module unit and the receiver block is the other unit with same configuration. The medium or channel of propagation of signal is the air between the antennae. Exchange of data is done in a point to point communication model using the LoRa RF signals. The RF range that LoRa uses is the 865 MHz to 867 MHz frequency range as these are license free in India.

Encryption and Decryption are performed on a PC connected to the ESP32 board. The reason for using a PC is that the ESP32 board in itself is incapable of running the entire

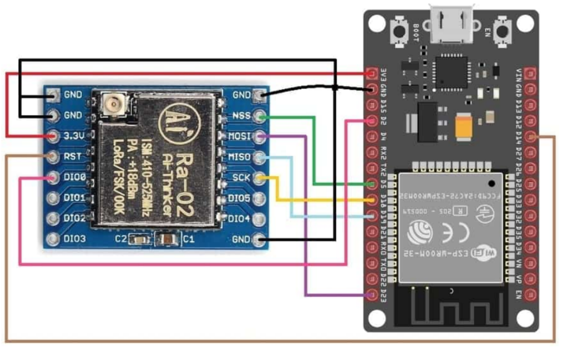
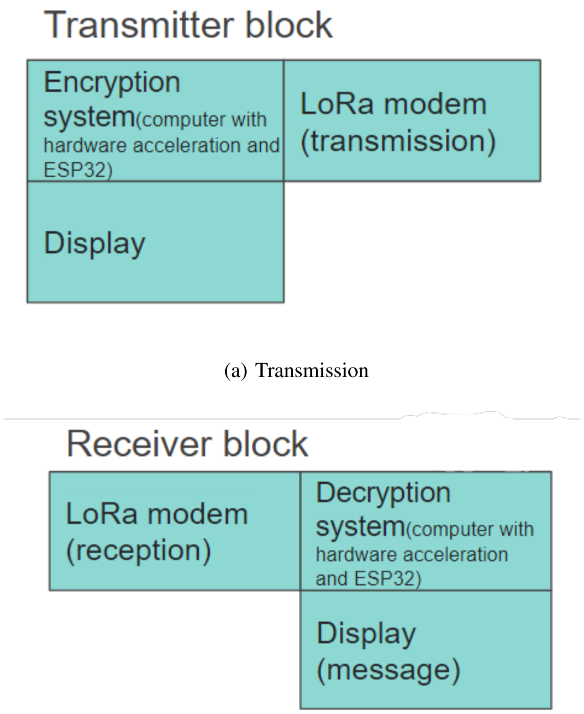


Fig. 4: Pin configuration

encryption algorithm on its CPU, this is because the AES is a fairly new encryption method compared to the ESP32 and as technology increases the amount of computing the processors that enable gadgets and technologies have to do rapidly increases as well and the ESP32 can not handle this computation requirement. So we make use of the on-board Cryptographic Hardware Accelerators, which assist the ESP32 in running the algorithm on another capable processor but integrate that process as though it was executed on the ESP32 board itself in realtime. The performance metrics of the system is analysed with varied key and message lengths by checking the range of the system, RSSI and packet loss.


Transmitter block
Encryption system(computer with hardware acceleration and ESP32)
LoRa modem (transmission)
Display
Receiver block
LoRa modem (reception)
Decryption system(computer with hardware acceleration and ESP32)
Display (message)

(a) Transmission

(b) Reception

Fig. 5: System Block Diagram

After each unit is setup for transmission and reception, encryption algorithms are ready then the ESP32 is powered up and the code is dumped onto it. The ESP32 is quick in transmitting data of small size. Here since we are using AES method the key for decryption has to be hardcoded into the source code and compiled along with the rest of the algorithm. Now various tests can be done to analyse the durability of this system. Cryptanalysis methods are done so as to ensure the safety of the AES encryption method. Attack methods applied on the AES were:

- Side-channel attack: Attempts to obtain the cryptographic key, partial state information, full or partial plaintexts and so forth by monitoring the AES T-table entry, CPU timing etc. i.e it utilizes the physical effects of the operation of the cryptography.
- Biclique attack: It utilizes a biclique structure to extend the number of possibly attacked rounds by the MITM (meet-in-the-middle)attack.
- Related-key attack: Creates a mathematical relationship connecting the keys.
- Brute-Force attack: Generates and tries all possible key combinations
- Frequency attack: It is based on the study of the frequency of letters or groups of letters in a ciphertext. In all languages, different letters are used with different frequencies.

Also to show that the cryptanalysis methods do work on other methods and prove that AES is an improvement to older encryption methods, Caesar Cipher encryption method was also included. Performing cryptanalysis on the Caesar cipher method shows that this encryption method is extremely weak and can be easily broken.

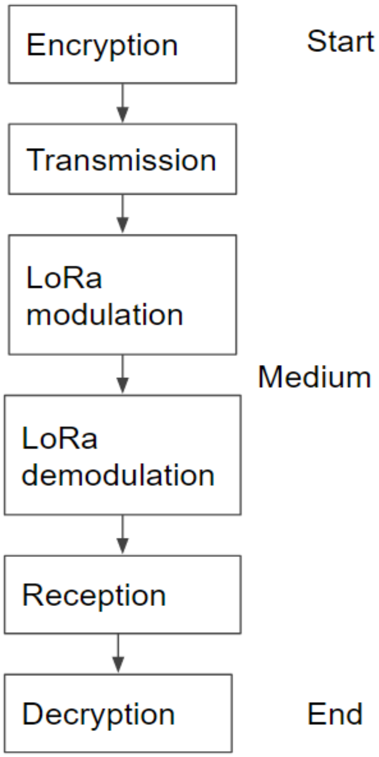


Fig. 6: Overview of communication process

IV. Testing and Analysis

The various tests performed for analysis were:

- Distance.
- Line-of-sight obstruction.
- Varied data sizes

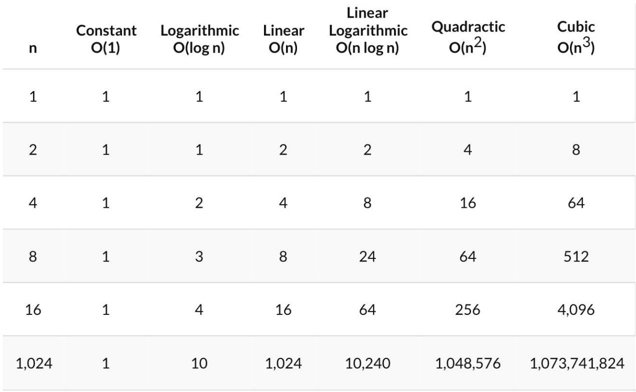
The analysis of the results obtained from the test mentioned earlier, provides us with a Distance vs RSSI(Received Signal Strength Indicator) plot which is shown in figure 7. This Graph shows us that the received signal starts fading as the distance between sender and receiver reaches the 15km mark. Realistically the optimum range was found to be 10-12km in the presence of noise and undetermined interference since the tests were performed in an urban city with various pre-existing wifi and other communication channels . It was also found that this system can be tuned based on suitable requirements with the help of the Data rate formula shown below:

$$R_b = SF * \frac{\frac{4}{4+CR}}{\frac{2^{SF}}{BW}} * 1000 \tag{1}$$

where,

- SF == Spreading Factor
- CR == Code Rate
- BW == Bandwidth in KHz
- $\mathrm{R_b}$ == Data Rate or Bit Rate in bps

We also took into consideration the speed at which the algorithm was executed considering the number of computations required to perform the AES encryption or decryption. To determine the computation complexity we make use of a concept called the Big-O notation. This is a mathematical notation that describes the limiting behavior of a function when the argument tends towards a particular value of infinity. It is also used to determine how an algorithm performs and scales. Most of these algorithms are normally only working on a fixed block size and take approximately the same time independently of input, thus they are said to be O(1). The different classifications of Big-O notations are :



n	Constant O(1)	Logarithmic O(log n)	Linear O(n)	Linear Logarithmic O(n log n)	Quadractic O(n^2)	Cubic O(n^3)
1	1	1	1	1	1	1
2	1	1	2	2	4	8
4	1	2	4	8	16	64
8	1	3	8	24	64	512
16	1	4	16	64	256	4,096
1,024	1	10	1,024	10,240	1,048,576	1,073,741,824

Based on these classifications each algorithms and the respective computation number is found. Comparing this with the time taken by the processor to complete running the algorithm we determine the how fast the ESP32 can handle complex algorithms.Data loss was also observed for, but it was found that there was no data loss of any kind when within the optimum range.

V. Conclusion and Future Scope

In summary, in this study we propose a novel ESP32 based LoRa communication applicable mainly in remote or secluded areas. We start by integrating the LoRa module with the ESP32 board and also install an antenna for the board. Once this integration is accurately done taking into consideration the pin configurations of the ESP32 board as well as the LoRa module, the software environment has to be set up for the ESP32 to execute the selected encryption and decryption algorithm. Both AES and RSA cryptographic methods can be performed but we have executed only the AES method.

For future improvements, key transfer in the case of AES method has to be improved since hardcoding the key into the software program each time is not very end-user friendly. Also since AES was not done directly on the ESP32 board itself, the project can be improved by introducing a microcontroller with higher computing capabilities so that the requirement of an external device for control of the board can be eliminated making the process of maintenance and extending software support much simpler. Although this method is incapable of transferring data at very high speeds like WiFi, the current rates are enough to transfer crucial data where other forms of communication are not applicable.

The testing of the end product was done under regular conditions, hence much more rigorous testing might reveal various other challenges that have to be overcome. But with current test results it can be concluded that the LoRa communication is possible over distances of 10-15km and there is minimal to no data loss encountered when transferring data over such large distances. This setup can handle Duplex communication, which makes it a peer-to-peer communication style, where data can be transferred from both ends of the communication channel.

Hence, this work represents a Peer-to-Peer communication method using LoRa waves achievable over large distances for transfer of data or control instructions. The results obtained revealed a definite path for solving real world problems using this technology, some of them being:

- Secure 2 way messaging. Messaging can be off the grid in remote areas where cellular and wifi may be unavailable
- More efficient for IOT devices due to very low power consumption.
- Unmanned vehicles (aerial and ground) as LoRa waves have a maximum range of 20 km.
- LoRa devices have geolocation capabilities which can be used for trilateration of positions of devices via timestamps from gateways.

Further fine-tuning of this system will lead to a stable and reliable communication method in places where WiFi and cellular networks are not possible.

Acknowledgment

The joy and satisfaction that accompany the successful completion of any task would be incomplete without thanking

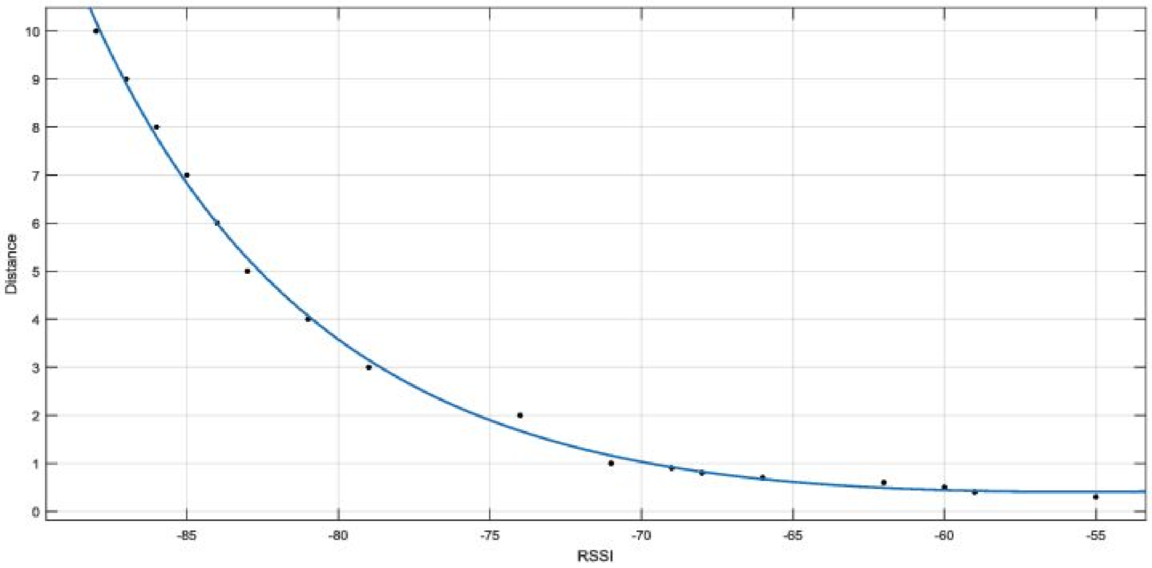


Fig. 7: Quality Metrics

those who made it possible. We consider ourselves proud to be a part of RNS Institute of Technology, the institution which moulded us in all our endeavors. We express our gratitude to our beloved Chairman **Dr. R N Shetty**, for providing state of art facilities. We would like to express our sincere thanks to **Dr. M K Venkatesha**, Principal and **Dr. Vipula Singh**, Professor and HOD, Department of ECE, for their valuable guidance and encouragement throughout our program.

We express our profound gratitude to the coordinators who have given valuable suggestions and guidance throughout the project. We would like to express our sincere gratitude to our Guide **Mrs. Smitha Gayatri D**, Assistant Professor and Reviewer **Mrs. Leena Chandrashekhar**, Assistant Professor for their guidance, continuous support and motivation in completing the project successfully.

Finally, we take this opportunity to extend our earnest gratitude and respect to our parents, teaching and non-teaching staff of the department, the library staff and all our friends who have directly or indirectly supported us.

References

[1] Tommaso Addabbo, Ada Fort, Alessandro Mecocci, Marco Mugnaini, Stefano Parrino, Alessandro Pozzebon, and Valerio Vignoli. *"A LoRa-based IoT Sensor Node for Waste Management Based on a Customized Ultrasonic Transceiver"*. July, 2019.

[2] Nur Aziemah Azmi Ali and Nurul Adilah Abdul Latiff. *"Environmental Monitoring System Based on LoRa Technology in Island"*. July, 2019.

[3] Tuncer Can Aysal and Kenneth E. Barner. *"Sensor Data Cryptography in Wireless Sensor Networks"*. June, 2008.

[4] Marek Babiuch, Petr Foltýnek, and Pavel Smutný. *"Using the ESP32 Microcontroller for Data Processing"*. July, 2019.

[5] Oleksii Barybin, Elina Zaitseva, and Volodymyr Brazhnyi. *"Testing the Security ESP32 Internet of Things Devices"*. April, 2020.

[6] Vageesh Anand Dambal, Sameer Mohadikar, Abhaykumar Kumbhar, and Ismail Guvenc. *"Improving LoRa Signal Coverage in Urban and Sub-Urban Environments with UAVs"*. June, 2019.

[7] Clément Demeslay, Philippe Rostaing, and Roland Gautier. *"Theoretical Performance of LoRa System in Multipath and Interference Channels"*. September, 2021.

[8] Phoebe Edward, Minar El-Aasser, Mohamed Ashour, and Tallal Elshabrawy. *"Interleaved Chirp Spreading LoRa as a Parallel Network to Enhance LoRa Capacity"*. September, 2020.

[9] Tallal Elshabrawy and Joerg Robert. *"Interleaved Chirp Spreading LoRa-Based Modulation"*. January, 2019.

[10] Lloyed Emmanuel, Dr. Wisam Farjow, and Dr. Xavier Fernando. *"LoRa Wireless Link Performance in Multipath Underground Mines"*. September, 2019.

[11] Abbas A. Fairouz, Monther Abusultan, Viacheslav V. Fedorov, and Sunil P. Khatri. *"Hardware Acceleration of Hash Operations in Modern Microprocessors"*. July, 2020.

[12] MD. Asif Iqbal. *"A Fully Automatic Transport System with LoRa and Renewable Energy Solution"*. June, 2020.

[13] Melvin Manuel and Kevin Daimi. *"Implementing cryptography in LoRa based communication devices for unmanned ground vehicle applications"*. April, 2021.

[14] Nur A Alam Munna, Mominul Ahsan, Md. Abdul Based, and Julfikar Haider. *"Smart Monitoring and Controlling of Appliances Using LoRa Based IoT System"*. March, 2021.

[15] George-Cristian Patru, Dumitru-Cristian Tranca, Ciprian-Marian Costea, Daniel Rosner, and Razvan-Victor Rughinis. *"LoRA based, low power remote monitoring and control solution for Industry 4.0 factories and facilities"*. October, 2019.

[16] Ondrej Perešíni and Tibor Krajčovič. *"More efficient IoT communication through LoRa network with LoRa@FIIT and STIOT protocols"*. April, 2019.

[17] A. Pohl, G. Ostermayer, R. Steindl, F. Seifert, and R. Weigel. *"Fine tuning of data rate enhances performance of a chirp spread spectrum system"*. September, 1998.

[18] Kun-Lin Tsai, Yi-Li Huang, Fang Yie Leu, Ilsun You, Yu-Ling Huang, and Cheng-Han Tsai. *"AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments"*. July, 2018.

[19] V. Li Vigni, A. Di Stefano, R. Candela, and E. Riva Sanseverino. *"A Two-end Traveling Wave Fault Location System for MV Cables Based on LoRa Technology"*. June, 2017.

[20] Alireza Zourmand, Andrew Lai Kun Hing, Chan Wai Hung, and Mohammad AbdulRehman. *"Internet of Things (IoT) using LoRa technology"*. September, 2019.