Implementing cryptography in LoRa based communication devices for unmanned ground vehicle applications

Melvin P. Manuel¹ · Kevin Daimi¹

Received: 15 September 2020 / Accepted: 13 February 2021 / Published online: 1 March 2021
© The Author(s) 2021

Abstract

In this study, a Long Range (LoRa) based bidirectional secured communication link for controlling and monitoring the robots from a remote location is proposed. The security features and structure of the LoRa is build upon the standard protocol called LoRa wide area networks (LoRaWAN). To take advantage of these features, LoRa devices/end modules need to be connected to a network server through a LoRa gateway. However, for certain military scenarios like war zones, terrorist attack sites, disaster sites etc., the availability of standard network cannot be guaranteed, and therefore, the security features available with LoRaWAN protocol cannot be guaranteed. To overcome this critical limitation, a LoRa based secured device for establishing a bidirectional communication link between the base station and the robots without relying on any network is proposed. To secure the exchanged data, a cryptographic protocol is developed, and confidentiality, authenticity and integrity of the transmitted data between the base station and the robot are ensured. The protocol is then implemented with a pair of LoRa devices and its functionality is tested from a remote location by controlling and monitoring a Pioneer-P3Dx robot from a distance of 1.2 miles. The test shows that the proposed cryptographic protocol can securely control and track the robot from a remote location.

Keywords LoRa · Cryptography · Robotics · Pioneer-P3Dx · ROS Indigo · AES encryption · HMAC-SHA-256

1 Introduction

The challenges faced by various agencies involved in search and rescue operations are unpredictable and in many cases, diverse in nature. In case of a seriously affected disaster scenario, lack of a stable communication network, devastated pathways, power failure, unavailability of instruments and equipment, etc., are some of the challenges they might face. In case of rescue mission after a terrorist attack, the military troop can expect network threats, in addition to the above mentioned challenges. Advancement in robotics technologies results in the development of many intelligent, complex robots that finds very helpful for performing highly dangerous tasks in this kind of applications. Robots can operate in areas

where humans cannot survive, they can work continuously for hours without needing rest, and they can even exceed human performance in places which are dangerous, toxic and risky. Different countries are giving more importance on the development of various new robot technologies, that can be helpful for applications like military operations and in disaster management. There are many different types of military robots available nowadays. They are Intelligence, Surveillance and Reconnaissance (ISR) robots, Search And Rescue robots (SARs), combat support robots, mine clearance robots, Explosive Ordinance Disposal (EOD) robots and fire fighting robots [1]. This paper is empathized mainly on one of the main categories of military robots named Search and Rescue robots (SARs). Search and Rescue (SAR) robots plays an important role in

✉ Melvin P. Manuel, manuelmp@udmercy.edu | ¹Department of Electrical and Computer Engineering and Computer Science, University of Detroit Mercy, 4001 W. McNichols Road, Detroit, MI 48221, USA.

rescue operations as a part of disaster management, after any natural and man-made disasters. As opposed to natural disasters resulting from natural hazards, man-made disasters have an element of human intent, negligence, or mistake involving a failure of a man made systems. Crime, arson, civil disorder, terrorism, war, biological/chemical hazard, cyber-attacks, etc. are such man-made disasters [2, 3]. Most of the SARs are capable to operating from a remote base station and in many cases they can perform certain tasks autonomously without the intervention of a human operator. Considering a SAR based military rescue operation, like after a terrorist attack, the dangers and risks faced by the military are uncertain. The enemies usually are exceptionally organized, innovative and intelligent. Hence, the robots used for such operations also need to be more intelligent [4].

Another important constraint in operating military robots is the availability of reliable communication links between a base station and the robots involved in the mission. In most cases, it is extremely possible that communication systems in the disaster zone have been destroyed or are not functional. Common communication networks like 3G/4G or Wi-Fi networks will not be available or cannot be assured in the wide range of affected area that the robots to be covered. Also, a proper communication system is crucial for sharing real time information between the robots, for proper coordination of different rescue operations in a disaster site. Currently available communication techniques includes establishing a private wireless communication link or a wired private network. Wireless communication suffers from low communication range (200 to 1000 m) [5]. Many practical implementation of wireless communication between robots and rescue teams are documented. Freeman et al. [6] proposes a wireless communication system with SARs by using wireless sensor networks which consists of fixed nodes and moving nodes between the robots and rescue teams. Kuntze et al. [7] explained about , SENEKA—sensor network with mobile robots for disaster management project, which proposed a dynamic wireless networking of different heterogeneous robots (UGVs, UAVs), sensors and human rescue teams. For communication between robots and other systems, they used IEEE 802.11 (WiFi) components in a multi hop topology. In all these cases, if any of the robots acting as a router/relay became inoperative, then the whole network will be collapsed. On the other hand, if we consider wired network based communication systems, it has the limitation of the length of wire and also will adversely affect the free mobility of the robots [8]. In view of the above discussions, it requires a simple communication system, which is based on wireless technologies to overcome the problem faced by infrastructure damages and which should be capable to operate by using an independent power sources like small

batteries. Another important constraint that we need to consider is the security of messages/data that is communicated between the robots, base station and the victims. Also, the whole communication infrastructure needs to be completely controlled locally by an operator from a rescue team. The main reason behind this decision is the fact that any third party managed communication infrastructure may not be secure and dependable in a severely affected disaster environment. Considering the above requirements and disadvantages of current communication systems in disaster zones, a LoRa based secured control device for controlling and monitoring Unmanned Ground Vehicles UGVs from a remote location is proposed.

The paper is organized as follows: Sect. 2 describes the approach that we followed in the development of the cryptographic protocol, Sect. 3 discusses, the details of experiments performed and its results, Sect. 4 is a brief discussion of the results, and the paper is concluded in Sect. 5.

1.1 Background

In this section, we provide a brief description about LoRa technology and some basic idea about LoRaWAN communication system. LoRa, stands for long range . LoRa is a wireless communication technology that operates in the sub-gigahertz band of radio spectrum, which is owned by a company called Semtech [9]. LoRa employs a spread spectrum modulation technique derived from Chirp Spread Spectrum (CSS) technology [10, 11]. This modulation technique is resistant to multipath fading and is ideal for noisy environments like disaster sites, with the goal of providing low throughput communication links with ranges of more than 30 miles by consuming low power [12–14]. The CSS modulation technique was developed in 1940's for military radar applications. Chirp Spread Spectrum is also being used in space communication and military applications for decades due to its advantages like long communication distances and its robustness to interference with other frequencies. Based on CSS modulation technology, LoRa is the first of its kind developed for commercial low cost usages [15]. LoRaWAN MAC protocol is the general standard used with LoRa, which is promoted by the LoRa Alliance, [16] an agency which, states the regulations for LoRa based devices and also defines both the data link and physical layer standards for LoRa networking technology. The LoRaWAN protocol is developed for providing secure wireless bi-directional communication between the end nodes (IoT devices) and the application that processes the data. LoRaWAN specification also defines the allotted frequency bands for LoRa based communication systems [17]. In USA, LoRa operates in the 915MHz band, while in Europe, it operates in the 433MHz

and 868MHz ISM frequency bands [18, 19]. One of the main disadvantages of a LoRa based communication system is its lack of security of data communicating between devices. In a standard implementation, the safety features associated with LoRa are built on LoRaWAN, which are generally used in IoT based applications. The communication between the LoRa devices/nodes and the gateway are through the LoRa physical layer (Wireless) and the connection between the gateways and the central network servers are handled through an Internet Protocol(IP)-based network. All the security features provided by LoRaWAN protocol are highly dependent on the applications and way the LoRa based link implemented [20, 21].

For accessing the LoRaWAN security features the receiver/gateway needs to be connected to a standard network to access the central server. However, due to the damaged infrastructure, we cannot guarantee any network connectivity in case of military applications or search and rescue operations and so, the security features offered by the standard LoRaWAN protocol will not be accessible. Also, it is not necessary to use network-dependent LoRaWAN in the event of a local military operation or rescue mission, as the operations would usually be organized and coordinated within a particular affected region. A novel method of using LoRa module to create a safe communication link between the base station and the robots is proposed in this paper. Here, we are not utilizing the LoRaWAN standards for securing the data, instead, a novel secure Cryptographic protocol has been developed and has been implemented on individual LoRa modules. The proposed Cryptographic protocol ensures the confidentiality, integrity and authenticity of the data communicating between the base station and the robot. A Pioneer-3Dx robot is used for evaluating the performance of the control device and the developed Cryptographic protocol in a real time lab setup. The robot uses a predeveloped navigation algorithm named Fuzzy Inference System Vector Field Histogram (FISVFH) for navigating through a devastated environment [22]. The reason for choosing this algorithm is due to its capability to drive the robot to its assigned destination quickly and safely without depending on a pre-build map.

1.2 Related works

In the recent years, several research publications have analyzed different aspects and emerging applications of the LoRa technology. Some of the studies emphasizes on security threats on the LoRa, the LoRaWAN architecture and its various applications especially in the field of robotics. Published research articles based on security issues related to LoRa end to end devices and its proposed solutions are

discussed in this section. Some of the applications of LoRa devices in the field of robotics are also listed below.

Basu et al. [23] discusses about various security issues of Low Power Wide Area Networks in the context of LoRa networks in their survey paper. Another similar kind of survey on security of Low Power Wide Area Networks, its threats, challenges, and potential solutions are done by Adefemi Alimi et al. [24]. Iqbal et al. [25] addresses numerous security and authenticity problems involved with the SCADA system for LoRa-based wireless communication. As a solution, they developed an Advanced Encryption Standard (AES) based algorithm and tested it on an ESP32-based LoRa module to secure micro-grid communication links. A unique message authentication code (MAC) has been developed and used to achieve authenticity. Jebiril et al. [26] discuss about the development and implementation of a covert channel called CloakLoRa, which demonstrates the possibility of creating a covert channel over the physical layer of LoRa. With this study, they researched the risk of leaking sensitive information through LoRa by developing and integrating CloakLora with LoRa devices. Bhatnagar et al. [27] addresses the advantages of the LoRa protocol, in terms of power demand, communication range, communication rate, etc.. Here, a LoRa-based algorithm for manipulating a UGV to autonomously follow a target has been developed and tested. Maneekittichote et al. [28] discussed the use of a hybrid combination of long range and localization strategies to manage four mobile robots. The method used were based on RFID, different sensors and the long range network (LoRa) to communicate information between robots. The LoRa communication link has been used to send and receive information/command from and to the robots. Lestari et al. [29] presents the test results for the implementation of the LoRa communication system as a long-distance transmitting medium for the collection of river water quality data from multiple sensors from four river water quality monitoring robots. They have conducted a test about the communication range of LoRa with four nodes and one gateway with LoRa transceiver paired with Arduino boards. Kim and Song [30] proposes a stable link establishment mechanism to safeguard the connectivity of device to device (D2D) communication in LoRaWAN. Two new MAC commands named SecureD-2DReq and SecureD2DAns were introduced in this scheme. Both messages are shared between the D2D nodes and the network server, and the security parameters are transferred from the network server to the D2D node server. These two D2D nodes generates the cryptographic keys for protecting D2D communication by using the obtained security parameters. They indicated through the security analysis that their method ensures mutual authentication, confidentiality, and integrity.

From the above literature reviews, it is clear that many of the papers have done extensive analysis about security risks of LoRaWAN. However, they didn't address the security threats that are unique to LoRa devices for securing device to device communication. Many of the applications discussed above depends the LoRaWAN protocol for securing their data. We also did not see many papers focused on secure LoRa-based communication systems in the field of robotics after exhaustive searching.

1.3 Contributions

Provided the many benefits of LoRa technology and the high demand for a secure long-range, low-power communication system for military robotics applications, a secured control device has been proposed that can establish a long-range communication link between a base station and the robots. A new Cryptographic protocol was developed based on certain standard cryptographic techniques (AES-128 encryption and HMAC SHA-256) to secure data communication between the robot and the control device (base station), which ensures the Confidentiality, Integrity and Authenticity (CIA) of the data communicated through the LoRa physical layer. A pair of LoRa transceiver development board based on SX1276 LoRa chip and ESP32 microcontroller was used as the hardware for implementing and testing the protocol. One of the LoRa module will act as a single channel gateway at the remote base station and another LoRa module acts as a transceiver on the robot. The location information of the destination point to be driven by the robot was first encrypted and transmitted to the robot, through the LoRa module from the remote base station. The LoRa transceiver which is a part of the robot, receives this information and decrypts it. Once the robot receives the location information, the same will be given as input to the FISVFH navigation algorithm [22]. The FISVFH drives the robot to the required location by avoiding all the obstacles along its path. The robot's location information was sent back to the base station for continuous monitoring of the robot's current location remotely. An encryption method based on bit-wise rotation operations, perform complement, and XOR-ing was used to secure this information.

2 Methodology

There are mainly three properties that are necessary for securing data communication between the robot and the control device (base station). They are Confidentiality, Integrity and Authenticity (CIA) [31]. The Advanced Encryption Standard (AES) came out as the first candidate after analyzing the best encryption algorithm to use with

a security critical application and something related to the federal security system. According to National Institute of Standards and technology (NIST), AES algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century". From this statement itself, it is clear that AES is mainly meant for maintaining confidentiality. Also, AES is the method adopted by U.S. government for protecting classified information and is successfully implemented in both hardware and software levels to encrypt any sensitive data [32]. For achieving integrity and message authentication, the well-known and established method called HMAC was used. HMAC (hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. It can be used to simultaneously verify both the data integrity and the authentication of a message, as with any MAC. In this paper, cryptographic hash function, called SHA-256 has been used for calculation of HMAC. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size and quality of the key and the size of its hash output. Coming back to the discussion about data security, there are mainly three methods to secure any data. They are Encrypt-then-MAC, MAC-then-Encrypt and Encrypt-and-MAC. All of them has its own properties and advantages. After doing literature reviews, most researchers recommend Encrypt-then-MAC (EtM) [33]. EtM protects the data against Cipher-text attacks, because MAC can avoid the decryption of incorrect messages. In this project, for incorporating confidentiality, integrity and authenticity on the data (sending from the controller at the base station to the LoRa module on the robot), AES along with HMAC SHA-256 algorithm has been used and implemented. For monitoring the real-time location of the robot (location feedback from the robot), another simple encryption method based on bit-wise rotate, complement and XOR operation has been developed and implemented.

2.1 Implementation of cryptography in LoRa devices

The hardware that used to develop the prototype of the control device is developed based on TTGO T-Beam LoRa ESP32 development board. LoRa ESP32 is known for prototyping many LoRa based implementations, since they combine an ESP32 micro-controller, a LoRa transceiver SX127x, an OLED 128 × 64 display and LiPo/Li-Ion battery on a small PCB board. At the base station, one of the TTGO ESP32 modules was used and another one was mounted on the robot.

The different terminologies used in this paper are presented in Table 1. There will be more than one robot in the team that can split the duties among themselves, taking into account any military or rescue operation. In such situations, if the base station control device has to communicate with more than one robot simultaneously, each robot needs to have a pair of LoRa devices tuned to a particular bandwidth at different frequencies. Otherwise it may results in inter-channel interference. Please note that, in this analysis, we considered communication between the base station and a single robot (Pioneer-P3Dx) to demonstrate the efficiency of the cryptographic protocol we developed. The general parameters that are to be configured for LoRa devices are spreading factor (SF), coding rate (CR), and bandwidth (BW). Spreading factor denotes the number of chips per symbol and its values ranges between 7 and 12. Spreading factor determines the range and the data transfer rate. CR is the ratio of non-redundant data to all data within the transmit and receive frames, whose values varying between 4/5 and 4/8. One of three values that can be used for BW is 125, 250, or 500 kHz. Since LoRa packet modulation and demodulation are affected, these parameters must be accepted between the transmitter and the receiver for effective communication [34, 35]. The LoRa modules serving the base station and the robot were assigned a frequency of 915MHz. For both LoRa modules, the allocated bandwidth is 125 KHz. The Spreading Factor assigned was 10. The choice of these values was made on the basis of the study of time analysis, which will be discussed in Sect. 3.

There are mainly two modes of operation performed at the base station. The transmitter mode, named as Mode-1 (BTx), and the receiver mode, named as Mode-2 (BRx). The operator at the base station with the LoRa control device can send control commands directly to the robot during Mode-1 (BTx), which is the transmitter (Tx) mode of the LoRa secured control device. The block diagram of the overall process on the control device during Mode-1 (BTx) is shown in Fig. 1. The location information to which the robot needs to send is the sample control command that used here. For sending the control command, the operator needs to enter the command and then enable

the “Tx” switch on the LoRa control device. The module first encrypts the data and then frames the encrypted data into a LoRa data packet. Then the LoRa packet is sent to the receiver module attached to the remote robot. Various cryptographic operations performed on the control device which is at the base station are discussed below.

2.2 Operations at secured LoRa control device during Mode-1(BTx)

The operator would have the exact position information at the base station of the location where the robot needs to be sent. Once the operator enters the Location Information (LI) in the machine (PC connected to the LoRa module), as the first operation of the Cryptographic Protocol, the AES-128 encryption on the LI is carried out. The resulting Ciphertext after performing AES-128 encryption is represented as,

$$\text{Ciphertext} = E(K, LI) \quad (1)$$

After performing AES-128 encryption, the next step is to perform HMAC SHA-256 on the resulting Ciphertext. HMAC SHA-256 is a hash key algorithm developed from SHA-256 the hash function. This algorithm is generally used as hash-based message authentication code (HMAC). The HMAC process mixes the Ciphertext with a secret key, hashes the result with the hash function, mixes the hash value with the secret key again and then applies the hash function again. For convenience of explanation, the resulting MAC of the Ciphertext is named as HMAC_Result and is represented as,

$$\text{HMAC_Result} = \text{HMAC} [K_{mac}, E(K, LI)] \quad (2)$$

For identifying the LoRa modules used in this study, the LoRa module fixed on the robot has been assigned with a three digit device ID and is represented as “DID”. When more robots are engaged in a given mission, this DID would be useful in distinguishing LoRa modules mounted on each robot. This DID is dynamic in nature and is assigned by the operator who is at the base station.

Fig. 1 Operations performed at the base station LoRa module during Mode-1 (BTx)

Fig. 2 Secured message from LoRa Tx to LoRa Rx

Table 1 Terminologies used

1	Rx	Receiver
2	Tx	Transmitter
3	LI	location information
4	DID	Device ID
5	Kmac	MAC Key
6	E	Encryption
7	K	Encryption Key
8	D	Decryption
9	H	Hash
10	LIR	location information of robot
11	RID	Robot ID
12	R	Rotate operation
13	C	Complement operation
14	Kxor	XOR key

Once the robot receives the DID sent from base station, it uses it to encrypt its real-time position information. Section 2.3 describes the thorough explanation of this process. The Ciphertext, the HMAC_Result and the DID is then concatenated and transmitted from the base station to the LoRa module fixed on the robot. All these steps involved are named as Mode-1 (BTx) mode of operations. The LoRa packet, which is the result of Cryptographic protocol at the

base station during Mode-1 (BTx) is named as “Tx-Packet” and is as follows.

$$\begin{aligned} &Tx - Packet \\ &= E(K, LI) || HMAC[K_{mac}, E(K, LI)] || DID \end{aligned} \quad (3)$$

Figure 2 shows the message being transmitted from the base station (LoRa transmitter) to the robot (LoRa receiver). The terminal response from the Arduino IDE at the sender side (base station) is shown in Fig. 3. For testing purpose, the plain text that used for testing the Cryptographic protocol is the GPS coordinates of University of Detroit Mercy. The AES encryption key used for testing purpose is “Uni-DetroitMercy”. The resulting Cipher text is shown in Fig. 3. HMAC-SHA-256 has been applied to the Ciphertext using the test key, “ECECS”. The HMAC SHA 256 output is also shown in Fig. 3. Figure 4 shows the LoRa device at the base station displaying the unencrypted location information for the operator at the base station.

Mode-2 (BRx) is the default control device mode which is used by the operator at the base station. In this mode, the system will operate as a receiver (Rx). The steps performed during Mode-2 (BRx) will be addressed in Sect. 2.4.

2.3 Securing the data communicated through LoRa device mounted on robot

As mentioned in Sect. 2.2, a 915 MHz tuned LoRa ESP32 module is fixed on the robot to receive secured messages from the base station. Here also, there are two operating modes for this LoRa module. Mode-1 (RRx), the default mode of the module that is the receiver mode and Mode-2 (RTx), which is the transmit mode.

Fig. 3 Arduino IDE Terminal response at the base station (LoRa sender Tx)

```

Encryption Key      : UniDetroitMercy
Plain text         : 42.414081, -83.138062
Cipher text        : 禱ŒS@#Œx;ŒLŒŒŒWŒoDŒlŒ=ŒŒ
Cipher text (Hex)  : 0e20e7a6b49353402381783bb2014ce2ef06e757e2999e6f44d9816ceb3dd4f4
HMAC Key           : ECECS
HMAC SHA256_Output : bb7f8c2b8987fbfb7414ff12e91c58aa8cba01042e46660a38703caf47a2a25e

```

Fig. 4 Un-encrypted location information displaying on the Tx device for the operator

2.3.1 Operations performed on LoRa device during Mode-1 (RRx)

During Mode-1 (RRx), the LoRa transceiver on the robot acts as a receiver unit. The received LoRa packet has three parts which were concatenated and sent from the base station control device. The received packet obtained from the LoRa module is named as “Rx-Packet” and is represented as,

$$\begin{aligned} \text{Rx - Packet} \\ = E(K, LI) \parallel \text{HMAC}[K_{\text{mac}}, E(K, LI)] \parallel \text{DID} \end{aligned} \quad (4)$$

The operations performed on the LoRa module mounted on the robot during Mode-1 (RRx) are shown in Fig. 5. The first step performed by the receiver is to parse the DID from the received packet (Rx-Packet). The extracted device ID is then used as the ID of the robot and is represented as “RID”. The next step is to parse the Ciphertext from the Rx-packet. The parsed Ciphertext is represented as,

$$\text{Ciphertext Rx} = E(K, LI) \quad (5)$$

The message, which is the location information LI, is then extracted from the Ciphertext Rx by AES decryption using

the AES key. The LI obtained after decryption is represented as,

$$LI = D(\text{Ciphertext Rx}) \quad (6)$$

The next step, according to the Cryptographic protocol, is to compare the HMAC sent from the base station with the HMAC created from the received Ciphertext Rx. The HMAC result sent from the base station is parsed out from the received LoRa packet (Rx-Packet) and is expressed as,

$$\text{HMAC_Result Tx} = \text{HMAC} [K_{\text{mac}}, E(K, LI)] \quad (7)$$

The suffix “Tx” is used here to distinguish the origin of the message. In this case, this HMAC_Result is originated from the transmitter, i.e. the base station. Next step is to perform HMAC SHA-256 on the received Ciphertext to generate the HMAC. The resulting HMAC, that is generated at the receiver after this operation is expressed as,

$$\text{HMAC_Result Rx} = \text{HMAC} [K_{\text{mac}}, \text{Ciphertext Rx}] \quad (8)$$

The next step of the Cryptographic protocol is to perform the comparison between HMAC_Result Tx and HMAC_Result Rx. If both messages matched, the authenticity of the received data is guaranteed. If the HMACs didn’t match, it is apparent that the information was hacked and the authenticity of the incoming data has been lost.

The Arduino IDE terminal response from the LoRa receiver module mounted on the robot is shown in Fig. 6. The received packet consists the Ciphertext, the Device ID and the HMAC_Result from the transmitter. The AES decryption key and HMAC SHA 256 key that used in the receiver module were the same that used in the transmitter side. The decrypted text will be displayed on the OLED display, which is a part of the LoRa module and is shown in Fig. 7. The sample LI shown in Fig. 7 is the GPS coordinate of our University (University of Detroit Mercy).

Fig. 5 Operations performed on LoRa device mounted on robot during Mode-1 (RRx)

Fig. 6 Terminal response at the LoRa receiver fixed on robot

```

/dev/ttyUSB3

ReceivedPacket : 禱ŦS@#Ŧx;Ŧ LŦŦ ŦWaoDŦŦŦŦŦŦ=ŦŦ:bb7f8c2b8987fbfb7414ff12e91c58aa8cba01042e46660a38703caf47a2a25e:DID 121
Ciphertext      : 禱ŦS@#Ŧx;Ŧ LŦŦ ŦWaoDŦŦŦŦŦŦ=ŦŦ
HMAC SHA256-Result_Tx: bb7f8c2b8987fbfb7414ff12e91c58aa8cba01042e46660a38703caf47a2a25e
Device ID       : DID 121
Decryption Key  : UniDetroitMercy
Ciphertext(Hex) : 0e20e7a6b49353402381783bb2014ce2ef06e757e2999e6f44d9816ceb3dd4f4
HMAC Key       : ECECS
HMAC SHA256-Result_Rx: bb7f8c2b8987fbfb7414ff12e91c58aa8cba01042e46660a38703caf47a2a25e
Decrypted Text  : 42.414081, -83.138062
Hacking status  : Not Hacked

```

Fig. 7 LoRa module displays the received information after decryption

Finally, the decrypted text, which is the LI where the robot needs to navigate is taken as input for the FISVFH navigation algorithm. As introduced in Sect. 1.1, FISVFH is a navigation algorithm suitable for search and rescue (SAR) robots to navigate to a desired location through the devastated environment without relying on a pre-built map [22]. Once the robot started navigating to its desired location, the LoRa module on the robot will change its mode from Mode-1 (RRx) to Mode-2 (RTx).

2.3.2 Operations performed on the robot's LoRa module during Mode-2 (RTx)

Once the robot starts navigating to the desired target position, the operator at the base station requires the robot's current location information to continuously track its route. The robot's current location is actually a sensitive piece of information with several possibilities for hacking. The hacker can gain control of the robot by hacking this data or, in worst situations, they can locate the robot and

can destroy it. In order to prevent this sort of scenarios, the location information sent back to the base station must be encrypted. A simple encryption scheme that consumes less computing power from the LoRa module's computer is proposed to protect data that are sent back to the base station/gateway. The proposed encryption system uses encryption techniques, such as bit-wise rotate operations, complement and then execute XOR on the data. The Robot ID and the current position details of the robot are the data considered for sending back to the base station. Please note that the device ID (DID) that sent from the base station will be used as the ID of the robot and the same is used as the Robot ID (RID). Each robot will have a unique ID, which is represented by a three digit number.

As a first step of the encryption process, the Robot ID will be translated into its corresponding binary equivalent. Suppose the DID assigned to a robot named "robot_01" from the base station was 121. The same ID has been used here as its Robot ID (RID). The RID is first converted to its binary equivalent. For robot_01 with RID 121, the binary

equivalent is "00000001 00000010 00000001". For ease of understanding, we named it as RID_01, which infers the binary equivalent of the robot_01's ID.

The next detail to be encrypted is the robot's position data. To obtain the robot's current position information, a GPS receiver has been interfaced with the LoRa module attached to the robot. To test the efficiency of the encryption protocol, the LoRa module is configured in such a way that the location information from the GPS module is updated every 5 s (which can be varied by program). The longitude and latitude part of the GPS data, obtaining from the GPS module is of 20 bytes size. For example, consider the sample data 42.406571, -83.128376 (GPS Coordinates of University of Detroit Mercy) obtaining from the GPS module. The binary equivalent of the above location information is, "00110100 00110010 00101110 00110100 00110000 00110110 00110101 00110111 00110001 00101100 00100000 00101101 00111000 00110011 00101110 00110001 00110010 00111000 00110011 00110111 00110110".

For instance, the binary equivalent of robot's location is represented as "LOC_xx". Therefore, considering robot_01, it will be interpreted as "LOC_01". The next step to be performed in the protocol is to concatenate the binary equivalent of the robot's position information and the RID and to be identified as,

$$LI_RID_Txx = LOC_xx || RID_xx \quad (9)$$

Please note that the LOC_xx is of 160 bits long and RID_xx is of 16 bits long. Together, LI_RID_Txx is 176 bits long. Please note that "xx" represents the robots number. For robot_01, "xx" will be 01. As part of the encryption process, the first operation to be performed is to perform the complement function on LI_RID_Txx. The resulting data after performing the complement is represented as,

$$LI_RID_Txx_C = \overline{LI_RID_Txx} \quad (10)$$

After performing the complement operation, the next process is to apply rotate operation on LI_RID_Txx_C. There are 23 bytes on LI_RID_Txx_C and each byte was performed rotate operation individually. All even numbered byte was performed with a 3 bit Rotate Right (ROTR) operation and all the odd numbered byte was performed with 3 bit Rotate Left (ROTL) operation. The resultant byte array after performing the rotate operations is represented as "LI_RID_Txx_C_R".

The next step in the proposed encryption method is to perform the XOR operation on the "LI_RID_Txx_C_R" byte array. A sample 8-bit key (10110101) is used here to perform the XOR operation. To avoid ambiguity, the same 8 bit (1 byte) key has been reused for the duration of the 23 byte data. The resulting binary data after XOR operation

is represented as "TRNS_xx" which is the encrypted data, ready to transmit to the base station. Please note that the 8 bit key is represented as " K_{xor} ".

$$TRNS_xx = LI_RID_Txx_C_R \oplus K_{xor,xx} \quad (11)$$

This encrypted information (TRNS_xx) will then be sent to the base station once every 5 s through the LoRa module.

2.4 Operations at the LoRa module at the base station during Mode-2 (BRx)

At the base station, the LoRa receiver module receives the encrypted data transmitted from the LoRa module fixed on the remote robot. To obtain the RID and the location information, various decryption steps must be performed at the base station and are as follows. The encrypted data packet received at the base station is represented as REC_xx.

$$REC_xx = LI_RID_Txx_C_R \oplus K_{xor,xx} \quad (12)$$

For performing the decryption operation, the XOR key for each robot (K_{xor}) is required. This key will be available at the base station as a database. The operator at the base station uses this keys for performing the XOR operation on the received data which is the "REC_xx". The resulting data after performing the XOR operation is represented as "LI_RID_Rxx_C_R".

$$LI_RID_Rxx_C_R = REC_xx \oplus K_{xor,xx} \quad (13)$$

After completing the XOR operation with the incoming packet, the next step is to perform the rotate operation on "LI_RID_Rxx_C_R". In this case, all the even numbered bytes was performed with a 3 bit Rotate Left (ROTL) operation and all the odd numbered bytes was performed with 3 bit Rotate Right (ROTR) operation. The resulting string after rotate operation is represented as "LI_RID_Rxx_C", which is the complement of location information and robot ID. Once the rotate operation is completed, the next move is to execute the complement operation on "LI_RID_Rxx_C". The resulting decrypted data after complementing "LI_RID_Rxx_C" is represented as,

$$LI_RID_Rxx = \overline{LI_RID_Rxx_C} \quad (14)$$

From the decrypted data "LI_RID_Rxx", the location information LOC_xx and RID_xx are separated. A binary to decimal conversion operation will then be performed on both data, resulting in robot's location information and Robot ID. These informations are then used for tracking the real-time location of the robot. By means of this encryption scheme, we can ensure that no one else can access the robot's current location information which ensures the secure and proper use of robots for a specified military task.

3 Experimentation and results

To imitate a war-zone/disaster site, and for testing the performance of the developed cryptography algorithm, an indoor environment has been set up within our laboratory. The testing environment where the robot was tested is shown in Fig. 8. The test site is approximately 70 m long and 30 m wide. For selecting the optimized values for Spreading Factor (SF), Coding Rate (CR) and Bandwidth, a time analysis study has been performed. The default SF values range from 7 to 12 and the higher the SF values, the larger the range and the lower the data rate. CR is the ratio of non-redundant data to all data within the transmit and receive frames, varying between 4/5 and 4/8. BW can be 125, 250, or 500 kHz. A time analysis has been conducted for the optimal selection of the above parameters which suits for implementing our protocol on the TTGO ESP32 development board. The analysis was carried out by keeping the LoRa transmitter module, 500 m away from the receiver.

For analysis, we considered 20 continues transmission and noted down the time delay between each reception and then calculated the average value. The test was conducted by keeping CR value a constant and by varying the SF values from 7 to 12. This has been done for all values of CR. Figure 9 shows the time analysis plot, which shows that a value of 4/5 for CR and 10 for SF takes only 1.62 s to complete the process of encryption and transmission of data from the LoRa transmitter to the receiver. Based on this analysis, we selected the values for CF, SF and BW as 5, 10 and 125 kHz respectively. In the usable

Fig. 9 Time analysis for selecting CR, SF and BW values

ISM frequency range, the selection of 125 KHz for BW is intended to fit more LoRa modules.

Due to the unavailability of GPS signals inside the laboratory, the local coordinate of the target location was sent to the robot to demonstrate the proof of concept. The target coordinates, which are the local X, Y coordinates of the robot, encompass the values $X = 30$, and $Y = 1$. Figure 10 reveals the location information displayed on the LoRa module held by the operator at the distant base station.

The LoRa module installed on the robot which was set to receiving mode, (RRx mode explained in Sect. 2.3.1) receives the encrypted data which contains the information about the coordinates of the destination point. After decrypting and confirming that the data is not compromised, the coordinates are displayed on the OLED, which is part of LoRa ESP32 module fixed on the robot. This is illustrated in Fig. 11. Details of the Unmanned Ground Vehicle that we used for testing are as follows. A Pioneer-3Dx robot has been used for testing the Cryptography protocol and also to demonstrate the performance of the

Fig. 8 Testing site with obstacles

Fig. 10 Location information sent from the base station to the robot

Fig. 11 Location information received at the robot

LoRa based secured control device. Pioneer-P3Dx is a small differential drive mobile robot designed for indoor applications. The Indigo version of Robot Operating System (ROS) [36] was used for programming the robot. As stated earlier, a fuzzy based navigation algorithm, FISVFH, has been used to navigate the robot to the desired location. The coordinates of the destination location received from the remote control device will be read by the FISVFH navigation algorithm. FISVFH algorithm was developed based on the data obtained from the odometer of the robot, and also the data acquired from a Hokuyo UST-10LX LIDAR. FISVFH then drives the robot to the destination by avoiding the obstacles in-front of it.

The robot will now start moving to the destination by avoiding obstacles on its way. Figure 12 shows different locations (A-F) of the robot from the starting location until it reaches its destination. The path followed by the robot on its way to the destination is shown in Fig. 13. When the robot starts to navigate to its assigned destination point, the LoRa module of the robot will switch to the transmitter

Fig. 12 Navigation of Pioneer-P3Dx robot from starting location (A) to the destination point (F)

Fig. 13 Path followed by the robot to the destination

Fig. 14 Location information showing on serial monitor at base station

(Tx) mode as explained in Sect. 2.3.2. At the same time, the LoRa module at the base station will switch back to the receiver mode (BRx) as explained in Sect. 2.4. The odometer data (which is encrypted) obtained from the robot are used as the current location information (LI). This is used at the base station for real-time monitoring of the position of the robot. We send the encrypted odometer data back to the base station every 5 s. Even-though we can send data in every 1.64 s (as per the timing analysis plot), the selection of 5 s is for saving the available LoRa bandwidth. Figure 14 shows the location information displayed on the serial monitor of the computer at the base station. Figure 15 shows the current location information displayed on the LoRa module at the base station. This display was updated once in every 5 s. For testing the security protocol, a wrong XOR key was provided at the base station to

Fig. 15 Location information displaying on LoRa module at base station

Fig. 16 Trial with wrong XOR key shows no location data

decrypt the location information coming from the robot. The result of this test is shown in Fig. 16. Once the robot reaches the destination, the LoRa module of the robot will then switch back to receiving mode and wait for the next command from the base station.

4 Discussions

The need for a long-range communication link which can be easily setup to suit for communicating with mobile robots during military operations and rescue missions are demanding nowadays. The various advantages of using LoRa based wireless communication system, makes it a suitable candidate for controlling military robots from a remote location. Up to our knowledge, no published work that uses LoRa

to control robots currently exists. The main constrain in using LoRa for military applications is the security of data communication through the LoRa link. As mentioned in Sect. 1.1, all the standard security features of LoRa are solely based on the LoRaWAN protocol. To utilize these features, the LoRa gateway needs to be connected to the LoRaWAN server through a network. In most military applications, the availability of standard communication network cannot be guaranteed. So dealing with these kind of situations, a secure communication link purely based on LoRa physical layer is proposed and developed. To invest the advantages of LoRa without sacrificing data security, a cryptographic protocol has been developed that secures the data transfer between two LoRa end devices. LoRa has been used with LoRaWAN in many IoT applications, where the end devices (sensor nodes) send data periodically to the gateway. Here, the communication is happening only in one direction, i.e., between LoRa end devices and the gateway. For controlling and monitoring a robot from a remote location, there is a need for a bidirectional communication system. In our work, two LoRa modules are used for establishing the bidirectional communication link. One of the LoRa module (which acts as the base station) sends some commands secured by the cryptography protocol discussed in Sect. 2. Another LoRa module on the robot receives it and decrypts it. Once the robot receives the control command, the LoRa module on the robot will switch to transmit mode and send secured data back to the base station for continuously monitoring the location of the robot. This bidirectional secured communication link, which can control a remotely located robot, is the highlight of this paper. The encryption scheme used in the protocol also ensures the current location information of the robot is not accessible to any other user/hacker except the authorized person who has the key database. The range achieved was purely based on the LoRa hardware used. This range is relatively less as compared to the ranges promised by LoRa technology. Nevertheless, there are enormous methods and advanced hardware for achieving long range. With the same ESP32 TTGO module that we used in this paper, Koyanagi [37] stressed that a long-range UHF 5/8 wave antenna was used that achieved a range of 6.5 kms. The functionality of the system has been tested with a pair of LoRa module which is similar to a single channel gateway. Eight or sixteen channel gateways can be used for incorporating many different channels to communicate with many robots if needed.

5 Conclusion

A LoRa-based bidirectional secured communication link for controlling and monitoring the robots from a remote location has been developed and tested. For ensuring

the security of the transmitted message, certain cryptographic operations have been applied to the data which are being transferred between a pair of LoRa transmitter and receiver. For testing the functionality of the device and the cryptographic protocol, location information is considered as the essential data to be sent to the robot. The location information was first encrypted and then authenticated to ensure security and integrity of the information exchanged between the LoRa modules. This project is the stepping stone for developing and applying security on individual LoRa module without depending on private networks for achieving data security. The performance of the system was tested on a Pioneer-3DX robot. Location information, transmitted from 1.2 miles away, was fed to the navigation algorithm, FISVFH. The robot was able to move to the desired location through a cluttered environment, and the base station successfully received the real time location information of the robot on a LoRa module.

As a future enhancement, the algorithm has to be tested in an outdoor environment with a gateway, which can handle many robots, to give better and more accurate insight on handling many nodes without losing the authenticity and integrity of the transmitting data.

Compliance with ethical standards

Conflict of interest The authors declare no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Kumari, AM, Simpy (2018) Military robots play a pivotal role as a tactical and operational tool for armed forces. <https://blog.marketresearch.com/military-robots-play-a-pivotal-role-as-a-tactical-and-operational-tool-for-armed-forces>. Accessed 20 Nov 2020
2. Man-Made Disaster | Monroe County, FL - Official Website. <http://www.monroecounty-fl.gov/>, <http://www.monroecounty-fl.gov/904/Man-Made-Disaster>. Accessed 20 Nov 2020
3. Manmade Disasters | Wichita Falls, TX - Official Website—. <http://www.Wichitafallstx.Gov>, <http://www.wichitafallstx.gov/1699/Man-Made-Disasters>. Accessed 24 Nov 2020

4. Murphy RR et al (2008) Search and rescue robotics. In: Siciliano B, Khatib O (eds) Springer handbook of robotics. Springer, Berlin. <https://doi.org/10.1007/978-3-540-30301-5-51>
5. DeLisle J-J (2015) What's the difference between IEEE 802.11af and 802.11ah. <http://www.Mwrf.com>, <http://www.mwrf.com/technologies/active-components/article/21846205/whats-the-difference-between-ieee-80211af-and-80211ah#:~:text=IEEE20802.11af20may20reach>. Accessed 24 Nov 2020
6. Freeman J, Omanan V, Ramesh VM (2011) Wireless integrated robots for effective search and guidance of rescue teams, pp 1–5. <https://doi.org/10.1109/WOCN.2011.5872919>
7. Kuntze H, et al (2012) SENEKA - sensor network with mobile robots for disaster management. In: 2012 IEEE conference on technologies for homeland security (HST), Waltham, MA, pp 406–410. <https://doi.org/10.1109/THS.2012.6459883>
8. Shin S, Yoon D, Song H, Kim B, Han J (2017) Communication system of a segmented rescue robot utilizing socket programming and ROS. In: 2017 14th international conference on ubiquitous robots and ambient intelligence (URAI), Jeju, pp 565–569. <https://doi.org/10.1109/URAI.2017.7992670>
9. Semtech LoRa Technology Overview | Semtech. <http://www.Semtech.com>. <http://www.semtech.com/lora>. Accessed 24 Nov 2020
10. Gambi E, Montanini L, Pignini D, Ciattaglia G, Spinsante S (2018) A home automation architecture based on LoRa technology and Message Queue Telemetry Transfer protocol. Int J Distrib Sens Netw. <https://doi.org/10.1177/1550147718806837>
11. "What is LoRaé ?," Semtech. <https://www.semtech.com/lora/what-is-lora>. Accessed 23 Sep 2019
12. Augustin A, Yi J, Clausen T, Townsley WM (2016) A study of LoRa: long range & low power networks for the internet of things. Sensors 16:1466. <https://doi.org/10.3390/s16091466>
13. Centelles RP, et al (2019) A LoRa-Based Communication System for Coordinated Response in an Earthquake Aftermath. In: Proceedings, vol 31, no 1, 21, p 73. <https://doi.org/10.3390/proceedings2019031073>. Accessed 24 Nov 2020
14. LoRa (LoRaWAN) Module | LPWA Products | Connectivity Modules | Murata Manufacturing Co., Ltd. <http://www.Murata.com>, <http://www.murata.com/en-us/products/connectivitymodule/lpwa/lora>. Accessed 24 Nov. 2020
15. Mekki K, Bajic E, Chaxel F, Meyer, A comparative study of LPWAN technologies for large-scale IoT deployment. <https://www.sciencedirect.com/science/article/pii/S2405959517302953>
16. LoRa Alliance Technical Committee. LoRaWAN 1.1 Specification; 2017. <http://lora-alliance.org/lorawan-for-developers>. Accessed 1 Nov 2019
17. Augustin A, Yi J, Clausen T, Townsley WM (2016) A study of LoRa: long range low power networks for the internet of things. Sensors 16(9):1466. <https://doi.org/10.3390/s16091466>
18. Ayele ED (2017) Performance analysis of LoRa radio for an indoor IoT applications. <https://doi.org/10.1109/IOTGC.2017.8008973>
19. Yang X, Karampatzakis E, Doerr C, Kuipers F (2018) Security Vulnerabilities in LoRaWAN. In: 2018 IEEE/ACM third international conference on internet-of-things design and implementation (IoTDI), Orlando, FL, pp 129–140. <https://doi.org/10.1109/IoTDI.2018.00022>
20. LoRaWANé Is Secure (but Implementation Matters) | LoRa Alliance. <http://lora-alliance.org/resource-hub/lorawan-secure-implementation-matters>. Accessed 24 Nov 2020
21. About LoRaWANTM | LoRa AllianceTM (2018) <https://lora-alliance.org/>. <http://lora-alliance.org/about-lorawan/>. Accessed 24 Nov 2020
22. Balan K, Manuel MP, Faied M, Krishnan M, Santora M (2019) A Fuzzy Based Accessibility Model for Disaster Environment. In: 2019 international conference on robotics and automation (icra), Montreal, QC, Canada, pp 2304–2310. <https://doi.org/10.1109/ICRA.2019.8793602>
23. Basu D, Gu T, Mohapatra P (2020) Security issues of low power wide area networks in the context of LoRa networks. [arXiv:2006.16554](https://arxiv.org/abs/2006.16554)
24. Adefemi Alimi, Kuburat Oyeranti et al (2020) A survey on the security of low power wide area networks: threats, challenges, and potential solutions. Sensors 20(20):5800. <https://doi.org/10.3390/s20205800>
25. Iqbal A, Iqbal T (2018) 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), Toronto, ON, pp 1–5. <https://doi.org/10.1109/EPEC.2018.8598380>
26. Akram Jebri et al (2018) Overcoming limitations of LoRa physical layer in image transmission. Sensors 18(10):3257. <https://doi.org/10.3390/s18103257>
27. Bhatnagar O, Surendran N, Alam MM (2020) Development of an algorithm for a target platform-following robot using LoRa signals. In: 2020 11th international conference on computing, communication and networking technologies (ICCCNT), Kharagpur, India, pp 1–5. <https://doi.org/10.1109/ICCCNT49239.2020.9225679>
28. Maneekittichote T, Chanthasopeephan T (2020) Mobile robot swarm navigation and communication using LoRaWAN. In: 2020 6th international conference on mechatronics and robotics engineering (ICMRE), Barcelona, Spain, pp 22–25. <https://doi.org/10.1109/ICMRE49073.2020.9064973>
29. Lestari RD, Rusdinar A, Murti MA, Tawaqal G, Lee D (2019) Design of IoT-based river water monitoring robot data transmission model using low power wide area network (LPWAN) communication technology. In: 2019 IEEE international conference on internet of things and intelligence system (IoTaIS), BALI, Indonesia, pp 201–205. <https://doi.org/10.1109/IoTaIS4734.7.2019.8980377>
30. Kim J, Song J (2018) A secure device-to-device link establishment scheme for LoRaWAN. IEEE Sens J 18(5):2153–2160. <https://doi.org/10.1109/JSEN.2017.2789121>
31. Confidentiality, Integrity, Availability: The three components of the CIA Triad. (n.d.). Retrieved from <http://www.Monroecounty-FL.Gov9>
32. What is Advanced Encryption Standard (AES)? - Definition from WhatIs.com, SearchSecurity. [Online]. Available: <http://www.monroecounty-fl.gov/904/Man-Made-Disaster0>. [Accessed: 23-Sep-2019]
33. Ramachandran GS, Yang F, Lawrence P, Michiels S, Joosen W, Hughes D (2017) Micropnp-wan: Experiences with LoRa and its deployment in dr congo. In: COMSNETS, 9 edn
34. Kim S, Lee H, Jeon S (2020) An adaptive spreading factor selection scheme for a single channel LoRa modem. Sensors (Basel, Switzerland) 20(4):1008. <https://doi.org/10.3390/s20041008>
35. LoRa (LoRaWAN) Module- LPWA Products -Connectivity Modules -Murata Manufacturing Co., Ltd. <http://www.Monroecounty-FL.Gov2>, <http://www.Monroecounty-FL.Gov3>. Accessed 24 Nov. 2020
36. Indigo - ROS Wiki (2018) <http://Wiki.Ros.org>, <http://wiki.ros.org/indigo>. Accessed 27 Nov 2020
37. Koyanagi, F (2018) ESP32 LoRa: you can reach up to 6.5 Km!. <http://www.instructables.com/ESP32-LoRa-You-Can-Reach-Up-to-65-Km/>. Accessed 27 Nov 2020

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.