EVALUATION OF DIFFERENT ATTACKS TOWARD LORAWAN AND SECURITY SUGGESTIONS

[1]AHMED AL-HTHLOOL, [2]MOUNIR FRIKHA

[1]Department Of Computer Network, College Of Computer Science And Information Technology, King Faisal University, Al Hasa, Saudi Arabia

[2] Department Of Computer Network, College Of Computer Science And Information Technology, King Faisal University, Alhasa, Saudi Arabia

E-mail: 221445321@student.kfu.edu.sa

ABSTRACT

Nowadays, emerging trends in the field of technology related to big data, cognitive computing, and the Internet of Things (IoT) have become closely related to people's lives. The Internet of Things networks consist of a huge number of interconnected devices and sensors that process and transmit data. Such Activities require efficient energy to be performed at the highest quality and range, hence the concept of Long-Range Wide Area Network (LoRaWAN) introduced, which concerns about delivering lower energy consumption, supporting large networks and mobility. LoRaWAN is a protocol that is designed to connect to operated things to the internet in regional, global networks and target internet of things. LoRaWAN can help make the life of people easier, but it has problems regarding the security such as replay attack, bit-flipping, and others. In this article, the security mechanisms in LoRaWAN will be evaluated as well as simulating security attacks that aims to know how to improve security in LoRaWAN. We discuss security features, cryptographic, key management, message acknowledgement and activation methods of LoRaWAN. Simulation is done under virtual environment using many tools and most used is Mbed simulator. We did the simulation, and the result is the attacks breached to LoRaWAN and got to the network server. Finally, we highlight the mitigation of these attacks.

Keywords: *LoRaWAN, LoRa, cybersecurity, IoT*

1. INTRODUCTION

The technology industry is evolving every day and it's awesome and scary at the same time, internet applications, internet of things (IoT) and computers are examples of technology and many others. IoT is a major technology by which can produce various useful internet applications. IoT can be defined as a network in which all physical objects are connected to the internet through network devices or routers and exchange data. IoT deal with a lot of devices and domains, and this can produce security issues for users that uses this technology like privacy, availability, confidentiality, and integrity as known CIA model.

As technology changing fast, developers must ensure users security of their data, especially when it comes to privacy, it's what people's concern about nowadays [1]. Security and privacy are the most important things in internet of things. Incorrect device update, absence of efficient and strong security protocols, lack of knowledge, and well-known device tracking are within the challenges that IoT is facing [2]. To make the users feal safe of their devices, the IoT security must be powerful. And to keep the security powerful the article interduces the concept of LoRaWAN and it's one of IoT applications. LoRaWAN is low power wide area network protocol designed to connect to operated things to the internet in global, regional networks and targets internet of things. The distance required to receive and transmit data in LoRaWAN can be surrounded by 0.3 and 50 kbps [3]. The network architecture is deployed in as a star topology in which there are gateways and end devices, and they rely on each other and in between them central network server. The gateways are connected to network server via IP connections and act as a transparent bridge [3]. Example of LoRaWAN where it can be used in smart cities, homes, smart industry, and supply chain logistics. On the other hand, LoRaWAN suffers from some security problems like reply attack, bit flipping attack, eavesdropping and many others [4]. To keep security standers high is very difficult and challenging and it cannot be achieved straightforward. It is important to study and research many IoT and LoRaWAN security issues. Main objective of LoRaWAN security is to ensure confidentiality, provide privacy and grantee the availability of services by IoT ecosystem. The purpose of this article is to evaluate the security mechanism in the LoRaWAN, this includes a review and comparison of the current LoRaWAN protocol stacks, advantages and disadvantages of different security mechanisms applied in LoRaWAN. The security requirements introduced in LoRaWAN will be identified, and protocol stacks in LoRaWAN based on privacy, confidentiality, integrity, and availability will be compared. To evaluate the security problems, we used some tools that could help us do the work and one of them is ChirpStack network server. ChirpStack is an open-source network server that host LoRaWAN devices and simulate them whether it was real hardware or simulation. Other tool is Mbed simulator which is also open source IoT operating system with a well-defined API to develop your C++ application and simulate it. The approach is expected to follow is experimental research which can be manipulated by the researcher and changing hypothesis or parameters of the experiment. Using this method will be perfect for this article because it will see the causes and consequences for scenarios, and it will help analyzing them and for testing LoRaWAN vulnerabilities and burstiness. The article is organized this way, first part is discussing the related work which is some of the research within the same field. Second part is discussing the security features of LoRaWAN. Third part is discussing attacks happen to LoRaWAN. Finally, conclusion which where we conclude our results.

2. LITERATURE REVIEW

In this paper [5] the authors says that there are many challenges, such as spoofing and jamming attacks and accessing to file that is not authorized to access, which can compromise the integrity of the information. There are some possible solutions that can help any person to do many security precautions that will help to secure the IoT devices of the users. There are many privacy threats appeared in current days, and they can attack IoT devices and the network that is integrated with technology [6]. It is difficult handle the security of IoT devices in companies. The companies must monitor and have scanning tools for all the devices in IoT that might identify any threats associated with privacy and seek to reduce any risks are being violated.

In this paper [7] Miller gives a brief overview of LoRaWAN and how LoRa and transmit and receive low amounts of data over wide range without expensive cost. Miller explained how to configure security protocol in LoRaWAN. He also explained the important things for LoRaWAN setup, and how the flow of process could jeopardize backend. He also presented a survey on the issues of LoRaWAN and to avoid the attacks or issues is by application that has a good key management practice. One of weaknesses of key management is the uses of symmetric encryption, where there are two places for the key to be stored, the nods and network server. Miller indicated that great solutions need to be developed to prevent any attacks for end users. By knowing cyber security of evert stage for the company, you can develop a different way to give LoRa solutions that fits the company needs.

This paper [8] discuss about the burstiness of LoRaWAN network, and it has three classes A, B, C reflected to end user devices and to wide scope of users. This paper focuses of class A which is the default class for all end devices. End devices transmit data to gateways, and gateways delivers it to application server. Paper introduced a wildly protocol used called slotted ALOHA, which is a shared channel divided into discrete interval called time slot. The paper study's the impact of different burst length in the network performance, and the results shows when burst length increases the performance improves.

In this paper [9] Chiang Rai analyzes the LoRaWAN in terms of CIA modal and talk about the most important parameter that may harm this modal. Jhon McCumber invented a security cube that shows three aspects of security. First aspect is the CIA triad: confidentiality, integrity, and availability. The second aspect is data states, which is data operations, data at rest or in storage. And in last aspect is countermeasures, which is used to illustrate the disciplines, people, and skills to provide protection. The paper examined the vulnerability of the modal and shows the availability aspects of CIA modal is most affected, and the power of transmission increases the efficiency of contact.

In this paper [10] proposed a two-factor authentication based on blockchain for LoRaWAN. Blockchain is a system of recording information in a way that makes it difficult or impossible to change and it's a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. The author's objective is to propose two-factor of authentication primely based on blockchain for LoRaWAN to add extra layer of security in authentication system to construct trust with LoRaWAN end devices and servers. Authors simulated this framework using Ethereum blockchain and python client and the end devices for LoRa and network server. LoRaWAN network working in parallel with blockchain as an independent network and this framework has three stages. Setting up blockchain network is the first one which is deploying smart contract to network, which is a script that make blockchain more secure. After the reply from the address of smart contract, the device information is read from blockchain network and sends the transaction to gateway of smart contract. Initial authentication and registration are the second stage which validate the join request message by LoRaWAN network. Then the block id will be sent to network server, and it will be accepted it by LoRaWAN end devices. Two-factor authentication is the third stage which is checking the receiving of the message of join request from network server and give block id saved from blockchain network server. If they match the network server will give the join accept message and end devices will be connected. The result shows that the system provides great performance in condition of throughput and latency.

In this paper [11] authors are explaining how LoRaWAN enabling technologies under the area of smart cities and in order to gather data and process it, authors are evaluating and testing new methods and tools of different simulations to get the right or accurate results of LoRaWAN network. One of the examples of LoRa is non-culler merged with LoRaWAN medium access control (MAC) protocol used in LoRa system. It can be almost impossible to emulate a real-world scenario on a large network. In order to demonstrate the new contributions, they need to be evaluated. There are several network simulations and one of them is LoRaSim. The result shows that the authors analyze the nature of different LoRaSim implementations, and the different is having four groups of end devices and the parameters are payload, code rate, bandwidth and spreading factor. By applying a common propagation modal which is Okumura-Hata on the network that uses orthogonality between all devices, this diverseness increases its quality and efficiency.

In this paper [12] the authors propose a method to improve LoRa performance called sequencing transmission scheme. They used LoRaSim simulator to show the efficiency of the scheme. Authors said there will be an increasing number of sensors and IoT devices by 2030 and all transmission media will be crowed. LoRaWAN also no difference, the transmitted packet can be disrupted by collision or signal interference causing loss of packet and powdery of performance. So, to improve LoRaWAN performance authors propose sequencing transmission scheme which is non acknowledgement and non-repeating transmission. The result showed that the scheme ought to offer as much as 100% data extraction rate (DER) while the assigned time become enough for every node to transmit and give 5 – 10 % average increase in DER compared to the normal LoRaWAN scheme.

In this paper [13] authors are focusing on LoRaWAN technology specially in LoRaSim simulator to explain bidirectional communication using LoRaWAN MAC protocol. Also, offer some insight into LoRaWAN overall performance based on network via many simulations. Low power wide area (LPWA) technologies offer to connect enormous numbers of devices that are distributed at low cost. With a log battery life and rage and keeping the cost down, LPWA is the alternative future of large-scale deployments. LPWA having the ability to transmit downlink is really important due to the fact it's a required key for many applications of IoT, numerous network management function of LoRaWAN like network joining, handshaking etc. can't be executed without it, to get the best network performance employing communication requires feedback from gateways to end devices and to inform that end devices should adopt their radio parameters, the gateways keep an eye on the uplink signal quality. Results of this study shows LoRaWAN is affected negatively not only by the size of network, but also by attempts at retransmission and downlink traffic and it helps in reliability and throughput. Also, the paper emphasizes the careful selection of size of the network and parameter of LoRaWAN can give acceptable performance.

3. LORAWAN SECURITY FEATURES

This part of this article gives an overview of LoRaWAN security features. According to security classical definition, which it is caring about the availability, integrity, and confidentiality of the system. As IoT devices are composed and stocked and shipped to user who want to connect to their account, it becomes important to install application specific key for the unit. Next, will describe the method that LoRaWAN takes on each aspect.

3.1. Architecture of LoRaWAN

As shown in figure 1 the diagram for LoRaWAN network architecture follows a start topology. Through gateway the end-nodes can communicate data over LoRaWAN. When data are received, gateways communicate LoRa packets to network server (NS). At the end node NS provides network control and MAC commands. The application server (AS) is responsible for managing the end node key and payload received or sent by end node in the network.

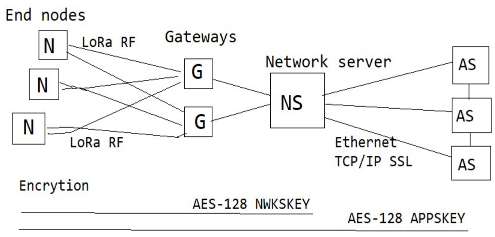


Figure 1. LoRaWAN diagram

There are three class in LoRaWAN that is classifies end node in three devices which are class A, B, C. class A lets bi-directional communication, each transmission for uplink comes after it two downlink receive windows. Class B lets bi-directional communication and in addition scheduling of receive slots, the network server uses synchronized beacons to synchronize end node listening time and schedule downlink transmissions. Class C end nodes have open receive windows almost continuously, except for uplink periods when they are sending data into the network [14].

3.2. LoRaWAN structure

When we talk about LoRa technology, we usually refer to the LoRaWAN open protocol and the LoRa modulation format. LoRa is a proprietary spread spectrum modulation scheme that is derived from Chirp Spread Spectrum modulation (CSS) [37], which can make data transfer with low energy and long distance. The architecture of LoRaWAN is usually structured in star of star topology without mash connections or repeaters. The end nodes which the gateways are acting as transparent bridge pass messages to the main NS. In this way, central server and gateways are assumed to be owned by network operator with end node owned by subscribers. Subscribers get an opportunity for transparency in bi-directional and secure data transfer to end nodes. LoRaWAN network consist of the subsequent elements: an application server, network server, gateway, end nodes [15] (fig. 2).

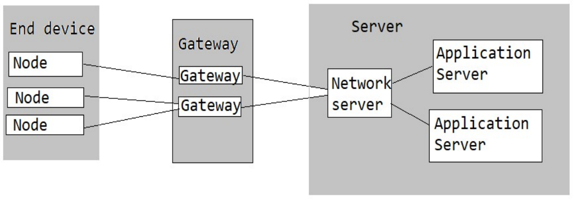


Figure 2. Structure of LoRaWAN network

Application server: collect data from end nodes and provide remote control over them.

Network server: manage the network, adapting data rate, setting up schedules, processing received data and store them.

Gateway: a receiving device for communication form end nodes and transferring them onto backhaul system.

End node: measuring functions and fulfills controlling. It contains a set of controlling elements and sensors.

3.3. Channel confidentiality

There are two pair of keys that LoRaWAN uses, the application key AppSKey and network key NwkSKey. LoRaWAN was developed with the business case of telecom or network in mind, which operate and implement LPWAN, while IoT service providers and device owners can use the infrastructure as black box to get connectivity between them. Since confidentiality and integrity check is needed with different amounts of data on the air interface between network infrastructure and IoT devices, and between third party application and IoT, AppSKey provide protected end to end connection while NwkSKey secure the former [4]. When a message is sent to application server, the payload of the frame is first encrypted using AppSKey. The confidentiality of the data is being protected by a block of cipher operating counter mode CTR. This construct, pseudo-random permutation can make a stream of random bytes using this method which is provided by block cipher. LoRaWAN follows CTR design down to last detail, takes AES block cipher as implementation and uses FCntDown or FCntUp as LoRa message counters which is incrementing repeatedly.

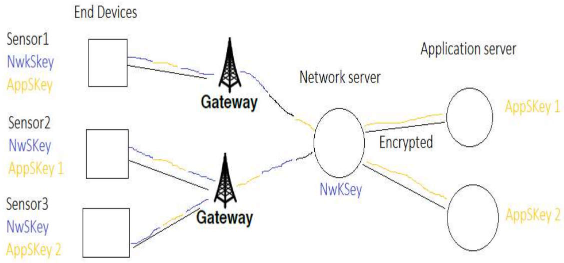


Figure 3. LoRaWAN key usage

3.4. Enrolment protocol

Since there are two keys needed to send out a frame to application and network server, the material of the keys must be downloaded to each IoT device. There are two mechanisms for LoRaWAN activation procedure, which are over the air activation (OTAA) and by personalization activation (ABP). Over the air activation works by sending a join request to end device containing 3 bytes of random number (DevNonce). When the join request is received by network server, it will check if the end device is accepted or not. If accepted, then it will send join accept message to end device. The accepting message has 3-byte of AppNonce made by network server. Else, any intruder could generate AppSKey and NwkSKey, OTAA draws the application and network keys by encrypting data with Appkey. ABP skips the exchange of join messages. Before activation, the end device is assigned to the unique parameters AppSKey, DevAddr, and NwkSKey and stored to the server. Once an end device is trying to communicate with the server, it sends messages directly. These messages are encrypted and signed so that only appropriate network server can read the messages [4].

3.5. Integrity and authenticity validation

LoRaWAN use cryptographic message integrity code (MIC) to provide an integrity check of the payload data and MAC header. We can calculate the data message for MIC using AESCMAC and NwKSKey method. The server first verifies the message integrity when uplink message arrives, and if it passes verification, transmit the whole message to the application server [4].

3.6. Replay protection

Counters are an essential component in reply protection, and how LoRaWAN uses the message counter to create key stream, they are important for the confidentiality of communication channel. Every end device has two frame counters which are FCntDown and FCntUP. FCntDown is counting downlink and FCntUP is counting uplink messages in network server. To keep them together in sync, there is a MAX FUNT GAP limit number [4], if this number is less than downlink and uplink messages then, subsequent frames will be discarded. After reseating, the counter value will be zero according to LoRaWAN specification.

4. LORAWAN ATTACKS

In this section, will present five vulnerabilities that could happen to LoRaWAN and explain them. To ensure these attacks can happen we have implemented two of them presented after this section. There are three main aspects of attacks of communication security: first, we establish that under certain circumstances it is possible to intercept and decrypt contents of a frame. Second, the content of a packet has been presented and showed that it can be changed outside of the integrity check provider by the protocol. Third, we highlighted that messages can replayed or tick a node into believing the gateway has received a message when in fact it hasn't, and we describe a battery drain attack that affect the availability of network. In following these are the attacks.

4.1. Replay attack

After the restarting of an ABP end device, the value of frame counter will reuse from 0 with the same key. An attacker can intercept the messages with large counter value in last session and reuse them in the current session. When the counter value gets to its highest, the counter is reset and restarted from zero. Using the last session's counter values and current session keys, an attacker can reply to previous messages to hack the communication between server and end device. Suppose that the malicious messages' uplink value is $FCnt_m$, and end device counter value is $FCnt_{curr}$, the accepted maximum counter gap is Gap. Third, any messages can be reply with $FCnt_m - FCnt_{curr} \leq Gap$ to confirm to LoRaWAN running widow algorithm and thus can be accepted by the network when they are replayed. This applies for both OTAA and ABP. An example of reply attack shown in figure 4, here will see the keys and large counter value, and the last message is the malicious message.

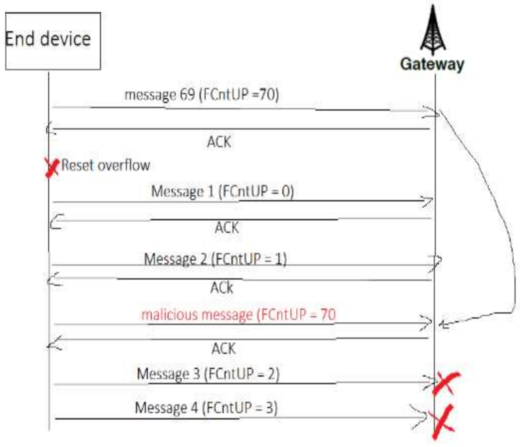


Figure 4. Replay attack for ABP

When the attacker sends this message to the network server in this session, and it is accepted, the message with smaller than 70 counter value from the victim will be ignored. If LoRaWAN structure it's a small and few end devices, the attacker must wait for a long time for counter overflow, the attack for ABP end device can be carried out in large deployments. Once the attacker obtains the highest possible count for an end device, they can continuously replay the message and permanently lock the end device. The attacker can implement a denial-of-service attack on LPWAN deployment.

4.2. Eavesdropping

As discussed above, channel confidentiality is implemented by LoRaWAN over AES counter mode. It takes the counter value as an input instead of setting it as nonce. Since a reset resets this counter value to specification while leaving the key in place, this means the block cipher recreates the exact key material. In a stream cipher, a plaintext P is combined through an exclusive OR with a key stream to obtain the ciphertext C. When given two messages P1 and P2 encrypted under the same keystream P_1 XOR K = C_1, P_2 XOR K = C_2, an adversary cloud eliminates the secret key as P_1 XOR P_2 [4]. This attack is considered it as a breach of confidentiality.

4.3. Bit-flipping attack

LoRaWAN messages are equipped and encrypted with integrity check, these two features are not applicable in the same scope. The protocol of cryptographic message integrity is checking the header information and payload data and transmitting them by infrastructure provider, while the application provider reverses the payload encryption that uses AppSKey. This means that the content cannot be verified for authenticity and integrity between IoT solution provider application and infrastructure provider servers. The connection between third party application and LPWAN operator would normally run over the internet so, it is a good practice placing the internal infrastructure into separate private network compartment. Unless other arrangements are made such as certificate pinning or tunning with validation, the content of messages between two parties could be redirected or changed. Block cipher is usually sensitive to bit-changes, avalanche effect principle that is normally render bit-flipping messages unreadable, since AES is only used as keystream generator and a stream cipher is easy to crack unless it is combined with encryption method.

Yet, LoRaWAN deviates from best practice of using authenticated encryption and stops integrity checking to early. It is possible for an attacker vector to insert themselves somewhere between IoT solutions and LPWAN operator as shown in figure 3. For this approach there are a variety of techniques, "ranging from routing-based approaches to physical and link-layer based attacks" [4]. As with stream cipher, the encrypted bit change in encrypted text is likely the same bit position in the plaintext, the attacker can change the content of the sensor readings.

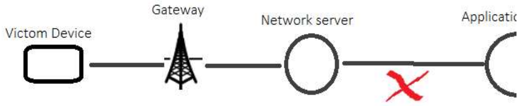


Figure 5. Bit-flipping attack module

4.4. ACK spoofing

To make the battery life extendable, the acknowledgment of the data in LoRaWAN is made optional to reduce the time it takes to be powered up. The acknowledgment message sent over air shown in figure 4. The ACK message does not specify which message it is acknowledging. There is a cryptographic integrity value in IoT device that allows it to confirm the authenticity of ACK, the ACK frame count is the sequence number of all messages. Therefore, the captured ACK could be delayed and used to selectively used to acknowledge receipt of another unrelated message event if it did not reach the backend provider. Since LoRaWAN depend on spread spectrum technique and with high spreading factor to establish fault tolerant link with minimal requirements, it takes relatively long time to transmit LoRaWAN packet. A skilled attacker without gain access to getaway could then prevent the IoT device form receiving acknowledgment via selective jamming and would then be able to drop all uplink messages when reading the previously cached ACK.

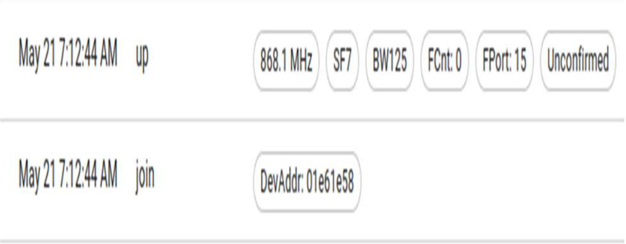
Table 1. ACK spoofing attack payload

MHDR	DevAddr	FCtrl	FCnt	MIC
60	88889999	20	0B00	BAE1557A

5. EXPERIMENTS

5.1. Bit-flipping

Our first experiment is bit flipping which as stated above it is an attack on a cryptographic cipher in which the attacker can change the ciphertext in such a way as to result in a predictable change of the plaintext. While LoRaWAN messages are both equipped with integrity check and encrypted, they are not applied in the same scope. Cryptographic message integrity code protocol is checking the header information and payload and it is terminated by the infrastructure provider, while the AppSKey is encrypting the payload is undone by application provider. This means that in between the IoT application server and the infrastructure network server, the content cannot be checked for authenticity and integrity. Block cipher is usually sensitive to bit changes, a principle known as the avalanche effect would normally render unreadable messages because of bit-flipping, since AES is used as key stream generator and this cipher is flexible if not an integrity check being performed combined with decryption [4]. However, LoRaWAN deviates from the best practices of using authenticated encryption and stops integrity check too early.

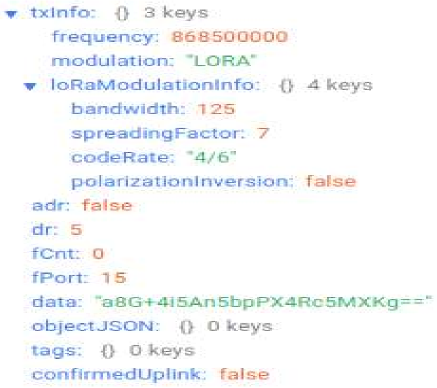


```
May 21 7:12:44 AM   up     868.1 MHz  SF7  BW125  FCnt: 0  FPort: 15  Unconfirmed

May 21 7:12:44 AM   join   DevAddr: 01e61e58
```

Figure 6. Message received from network server

As the network server search from IP address of the application server, there is a man in the middle (MITM) which is the packet goes through him to the application server. While network server sends the message, MITM takes that packet and change the message and send it to application server as it was coming from network server. The data sent is encrypted using AES algorithm by C++ programming language. As shown in figure 6 the data was received in application server.



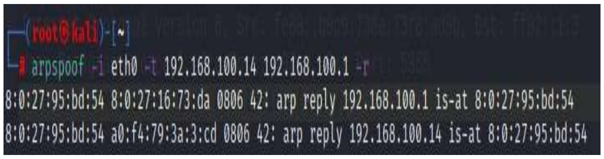
```
▾ txInfo:  {} 3 keys
    frequency: 868500000
    modulation: "LORA"
  ▾ loRaModulationInfo:  {} 4 keys
      bandwidth: 125
      spreadingFactor: 7
      codeRate: "4/6"
      polarizationInversion: false
  adr: false
  dr: 5
  fCnt: 0
  fPort: 15
  data: "a8G+4I5An5bpPX4Rc5MXKg=="
  objectJSON:  {} 0 keys
  tags:  {} 0 keys
  confirmedUplink: false
```

Figure 7. Message bit-flipped from network server

When we open the details in up message from the device as shown in figure 23, in field data the data in form of base64 have been altered from this original message (a8G+4i5An5bpPX4Rc6KeK==) which is the decrypted data from the device to what is showing in the figure which is wrong. The last 4 characters wore changed which verify that the bit has been flipped using AES algorithm and the experiment shows that the attack happens between network server and application server.

5.2. Address resolution protocol (ARP)

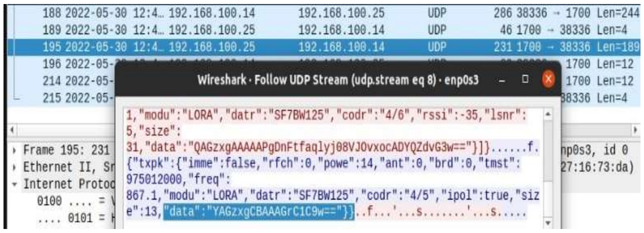
Our second experiment is address resolution protocol (ARP) spoofing, which is an attack happed to LoRaWAN by sending falsified ARP message over the network. It can be done by linking the attacker MAC and IP address with IP and MAC address of the victim device or a server on the network to make the packet sent from victim device goes through hacker device. Also linking IP address of the router or access point to hacker device to make the packet coming from router to victim device pass through hacker device. Since LoRaWAN relies on spread spectrum technique with high spreading factor to implement a fault-tolerant connection with minimal performance requirements, the transmission of LoRaWAN packet takes a relatively long time [4]. A skilled attacker could prevent receipt of acknowledgment by selectively jamming the IoT device without even accessing to a gateway, and then dropping all uplink messages while replaying to previously cached ACK.



```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 192.168.100.14 192.168.100.1 -r
8:0:27:95:bd:54 8:0:27:16:73:da 0806 42: arp reply 192.168.100.1 is-at 8:0:27:95:bd:54
8:0:27:95:bd:54 a0:f4:79:3a:3:cd 0806 42: arp reply 192.168.100.14 is-at 8:0:27:95:bd:54
```

Figure 8. connecting ARP spoofing

In this step we connected the victim and hacker devices to each other, once it is connected using the method shown in figure 8 which has name of the attack followed by -I which is the interface followed by -t which is setting the target IP address and the IP route followed by -r to make the IP route return the data to attacker device. Now the attacker is receiving any requested data coming or outgoing from this IP address which can be modified or intercepted or even stopped.



```
188 2022-05-30 12:4… 192.168.100.14   192.168.100.25   UDP   286 38336 → 1700 Len=244
189 2022-05-30 12:4… 192.168.100.25   192.168.100.14   UDP    46 1700 → 38336 Len=4
195 2022-05-30 12:4… 192.168.100.25   192.168.100.14   UDP   231 1700 → 38336 Len=189
196 2022-05-                                                       1700 Len=12
214 2022-05-                                                       1700 Len=12
215 2022-05-                                                      38336 Len=4

▸ Frame 195: 231                                                  np0s3, id 0
▸ Ethernet II, Sr                                                 27:16:73:da)
▾ Internet Protoc
    0100 .... = V
    .... 0101 = H
```

Wireshark · Follow UDP Stream (udp.stream eq 8) · enp0s3

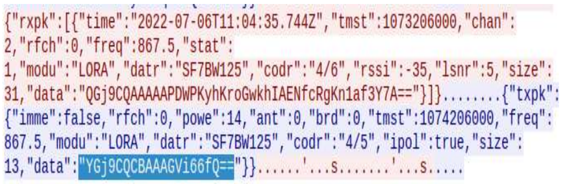
```
1,"modu":"LORA","datr":"SF7BW125","codr":"4/6","rssi":-35,"lsnr":
5,"size":
31,"data":"QAGzxgAAAAAPgDnFtfaqlyj08VJOvxocADYQZdvG3w=="}]}......f.
{"txpk":{"imme":false,"rfch":0,"powe":14,"ant":0,"brd":0,"tmst":
975012000,"freq":
867.1,"modu":"LORA","datr":"SF7BW125","codr":"4/5","ipol":true,"siz
e":13,"data":"YAGzxgCBAAAGrC1C9w=="}}..f...'...s.......'...s.....
```

Figure 9. WireShark for monitoring packets

We send a data from our simulator to the network server which is on this IP address 192.168.100.14. In the hacker device there is software called WireShark, which is to monitor the packet on the network, and we used it to see the packet sent from the simulator to network server device. Once we got the packet from the victim device, we filter it by the same IP address and pick the packet which is received to network server as shown in figure 9. In the same figure the data is shown to us highlighted the data transferred to network server device. Here the data transaction between the simulator and network server can be seen by the attacker before it been received.

5.3. Eavesdropping

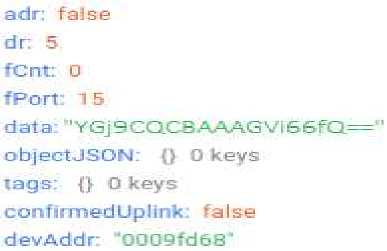
Eavesdropping is a major concern when it comes to cyber security, through this attack the sensitive information can be stolen such as passwords, card details while it is transferred from one device to the other. Since you do not raise any suspicions while the data is transmitted that's what makes this attack successful. Channel confidentiality being implements by LoRaWAN over AES in counter mode. The value of packet counter is used as an input instead of being set as nonce. According to the specifications this counter value is reset during a reset, while the key instead remains, which means that the block cipher recreates the same key material. After doing the experiment in virtual environment we picked up a stream of packets that is sent from one device to another. When we follow the stream of packets and open one of them in WireShark, we can see this information shown in figure 10. This is the data transferred to the other device which is in form of base64 encoded.



```
{"rxpk":[{"time":"2022-07-06T11:04:35.744Z","tmst":1073206000,"chan":
2,"rfch":0,"freq":867.5,"stat":
1,"modu":"LORA","datr":"SF7BW125","codr":"4/6","rssi":-35,"lsnr":5,"size":
31,"data":"QGj9CQAAAAAPDWPKyhKroGwkhIAENfcRgKn1af3Y7A=="}]}........{"txpk":
{"imme":false,"rfch":0,"powe":14,"ant":0,"brd":0,"tmst":1074206000,"freq":
867.5,"modu":"LORA","datr":"SF7BW125","codr":"4/5","ipol":true,"size":
13,"data":"YGj9CQCBAAAGVi66fQ=="}}......'...s.......'...s.....
```

Figure 10. WireShark data stream

And in figure 11 confirm the data was received from the client device as it is from figure 10.



```
adr: false
dr: 5
fCnt: 0
fPort: 15
data: "YGj9CQCBAAAGVi66fQ=="
objectJSON: {} 0 keys
tags: {} 0 keys
confirmedUplink: false
devAddr: "0009fd68"
```

Figure 11. Data received from server

In our experiment, a LoRa device was configured to send a message to network server. A malicious gateway keeps listen to the traffic and tracking the uplink message from LoRa device.

6. MITIGATION

In this section, we will consider possible counter measures and mitigations for the attacks discussed above.

6.1. Bit-flipping

Due to the early termination of the message integrity code, a bit flipping attack could happen in between the application provider and infrastructure in the system architecture. One solution can be provided is to prevent an attack with a malicious modification of payload is to not run integrity check value on network server but on the application server. Ideally, new design should apply authentication encryption rather than pure encryption, a lesson that affect repeatedly from log chain of attacks on protocol like TLS and Wi-Fi. This would disassemble some of the payload bytes in MAC to accommodate an application server verified MIC.

6.2. ARP spoofing

The essential problem is that ARP spoofing is enabled of previously stored ACK frames is the message does not know which message it confirms. The changes happen to MIC for both application server and network server, it is possible to add a cryptographic checksum to the confirmed return acknowledgement. And returned value must contain the hole packet sent by field device. With no additional byte cost, the IoT device can confirm that (a) the ACK belong to this message and (b) the value did not change during the transmission. Because ACK is tied to a specific message, it is not possible to store and forward ACK in different context.

6.3. Eavesdropping

Attack like eavesdropping can exploits the fact that block cipher in counter mode is not secure if the value of the counter is allowed to repeat itself. Monotonically case is the classic example of increasing counter value of how CTR is made can fill in practice with volatile memory. One solution here is proposed which is replacing the counter value into a nonce that is used only once driven from random number generator on the sensor platform. This solution could instantly reduce the probability of collision to the inevitable birthday paradox theory. Special care must be taken that the IoT device dose not start with the same initial value on all installation. It is challenging to collect unique entropy on embedded systems, but there are robust methods have been developed to achieve it.

6.4. Replay attack

Replay attack is based on two things, AppSKey and NwkSKey and they are used as a log term key and remains unchanged after counter reset. We could minimize this attack from happening by using activation through personalization and new keys should be changed regularly. However, device OTTA registration does not mean that end device is secure, as the counters can overflow. However, power on the renegotiation means that OTTA, an attack could wait a longer time to perform the attack. The end devices must be protected by any malicious parties from initiating system reset. It is difficult to achieve in a variety of IoT deployment context, non-volatile memory is an example of design changes that could preserve the counter value in between reset. The only way to perform this attack If the attacker can't reset counter is by waiting for it to overflow. These changes reduce vulnerability but need to change LoRaWAN specifications.

7. DISCUSSION

Our work is among the first to analyze security in LoRaWAN and exploit vulnerabilities through the simulation of different attacks. Based on numerous LoRaWAN vulnerabilities, we presented and analyzed different attacks. These attacks are simulated in the LoRaWAN environment and different suggestions, and security countermeasures are presented, which can be implemented with minimal changes in LoRaWAN Model. The simulations presented in this paper consider a simple traffic and mobility model, and in order to be able to present more realistic recommendations, it is necessary to extend these simulations for more complicated traffic and mobility models that are closer to reality. A physical implementation with all needed devices is also recommended in order to properly validate the results.

8. CONCLUSION

LoRaWAN is the key thing in IoT technology, it is simply to be able to support low power end device with two direction communication at wide rage. The protocol of network layer can offer efficient and scalable networks and allow adjustment and selection of key parameters to optimize the power utilization versus downlink/uplink latency trade off to meet the needs of different applications. This article presents an evaluation and a review and comparison of security in LoRaWAN protocol stacks and attacks of LoRaWAN and simulate them. Simulation of these attacks appear to be successful, and it breaches the LoRaWAN network server (ChirpStack) which something dangerous. These kinds of attacks must be prevented so that it could be safe to different individual to get them in their homes or workplaces. Some of the countermeasures for ARP spoofing is to use virtual private network (VPN), that way you can use encryption tunnel that largely blocks your activity from ARP spoofing hackers. Also, it helps if you use a detection tool that can help you determine whatever there is a spoofing in your network or not using a third-party tool such as XArp. One possible countermeasure for bit flipping is in the application server you should run integrity check value not in the network server [4]. The new protocol design should apply authentication encryption rather than pure encryption. In our feature work we will analyze the recent LoRaWAN specification and present how to include some changes which fix some of the discussed vulnerabilities, and we will validate the results through a real implementation.

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. 2751].

9. REFERENCE

[1] Georgios, M., 2017. *Security mechanisms for Internet of Things (IoT)*. London: University of East London.

[2] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IOT privacy and security: Challenges and solutions," Applied Sciences, vol. 10, no. 12, p. 4102, 2020.

[3] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "Lorawan security survey: Issues, threats and possible mitigation techniques," Internet of Things, vol. 12, p. 100303, 2020.

[4] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in Lorawan," 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), 2018.

[5] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer IOT in the Smart Home: Architecture, Challenges, and countermeasures," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 53–59, 2018.

[6] R. Chow, "Detecting Privacy Threats in IoT Neighborhoods," in *Proceedings of the 3rd ACM International Workshop on IOT privacy, trust, and security*, ACM, pp. 23–30.

[7]. *Miller R. MWR Labs Whitepaper,* **LoRa** *Security Building* **a** *Secure* **LoRa** *Solution.*

*Available at: <https://labs.f-secure.com/assets/BlogFiles/mwri-***LoRa***-security-guide-1.2-2016-03-22.pdf>[*Accessed: 12-Oct-2021.*]*

[8]. A. Tsakmakis, A. Valkanis, G. A. Beletsioti, P. Nicopolitidis, and G. Papadimitriou, "On the effect of traffic burstiness in Lorawan Networks' performance," *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, 2020.

[9]. C. Kamyod, "CIA analysis for Lorawan Communication Model," *2021 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunication Engineering*, 2021.

[10]. S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi and M. Rajarajan, "A Lightweight Blockchain Based Two Factor Authentication Mechanism for LoRaWAN Join Procedure," 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1-6, doi: 10.1109/ICCW.2019.8756673.

[11]. S. Francisco, P. Pinho and M. Luís, "Improving LoRa Network Simulator for a More Realistic Approach on LoRaWAN," 2021 Telecoms Conference (ConfTELE), 2021, pp. 1-6, doi: 10.1109/ConfTELE50222.2021.9435570.

[12]. K. Wongwatthanaroek and R. Silapunt, "Transmission Sequencing to Improve LoRaWAN Performance," 2021 18th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2021, pp. 1-5, doi: 10.1109/JCSSE53117.2021.9493820.

[13]. A. Pop, U. Raza, P. Kulkarni and M. Sooriyabandara, "Does Bidirectional Traffic Do More Harm Than Good in LoRaWAN Based LPWA Networks?," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8254509.

[14]. B. Oniga, V. Dadarlat, E. De Poorter and A. Munteanu, "Analysis, design and implementation of secure LoRaWAN sensor networks," 2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2017, pp. 421-428, doi: 10.1109/ICCP.2017.8117042.

[15]. Iskhakov, Sergey & Meshcheryakov, Roman & Iskhakova, Anastasia & Bondarchuk, Sergey. (2017). Analysis of vulnerabilities in low-power wide-area networks by example of the LoRaWAN. 10.2991/itsmssm-17.2017.69.