The University of Sydney

SCHOOL OF ELECTRICAL AND INFORMATION ENGINEERING

PROJECT CLEARANCE FORM

Unit of Study Code and Name **ELEC5021 Capstone Project B**

This is to certify that my student

Student Name Kunhong Edward Chen

SID 440302274

Has:

- **Returned all books and reference material;**
- **Returned all equipment and keys; and**
- **Tidied their work place.**

SUEIE Academic supervisor:

Signature: Phee Lep Yeoh Digitally signed by Phee Lep Yeoh
Date: 2020.11.20 14:59:07 +11'00' **Date: 20/11/2020**

Name: Dr. Phee Lep Yeoh

External supervisor (if applicable):

Signature: **Date:**

Name:

Physical layer security: Jamming attack in LoRaWAN network

ELEC5020 Capstone Project part B

THE UNIVERSITY OF SYDNEY

November 20th, 2020
Supervisor: Dr Phee Lep Yeoh
Student: Kunhong Edward Chen

Abstract

To resolve the issue of growing mobile network demands, the development of new wireless technologies has seen extensive success in the forthcoming prototyping of 5G and IoT. However, the increase in efficiency and capacity brought by new network architecture comes with unknown risks of malicious attacks. As a currently adopted IoT network system and as a simpler version of wireless communication protocol compared to 4G/LTE and 5G, LoRaWAN serves as a model to study wireless attacks against future wireless technology is of great research interest. In this paper we firstly discuss the existing attacks exploiting wireless networks' weaknesses on multiple network layer as background information, followed by delving deep into the physical layer, specifically on the most common attack types such as jamming and eavesdropping. Main experimental endeavor revolves around simulation of LoRaWAN network model and jammer device model in NS-3 (Network Simulator -3), demonstrating the vulnerability of physical layer against jamming attacks in LoRaWAN network, and to demonstrate the network behaviour against jamming attacks under retransmission scheme.

Table of Contents

[Glossary]

AKA ----- Authentication and Key Agreement
ARPF -----Authentication Credential Repository and Processing Function
AS---------Access Stratum
ASME --- Access Security Management Entity
AUSF ----Authentication Server Function
AUTN --- Authentication Token
C-RS -----Cell-specific Reference Signal
DC ------- Duty cycle
DSSS-----Direct Sequence Spread Spectrum
EAP ------Extensible Authentical Protocol
ECC-------Elliptical Curve Cryptography
ECDH-----Elliptical Curve- Diffie –Hellman
ED --------End devices
EPS -------Evolved Packet System
EMM -----EPS Mobility Management
eNodeB---Evolved Node B
E-UTRAN-Evolved Universal Terrestrial Access Network
FDD-------Frequency Division Duplex
FHSS------Frequency Hopping Spread Spectrum
HARQ ----Hybrid Automatic Repeat Request
HHS ------Home Subscriber Server
ICMP------Internet Control Message Protocol
JSR--------Jammer to Signal Ratio
MIB-------Master Information Block
MME --- -Mobility Management Entity
NAS-------Non-Access Stratum
OFDM----Orthogonal Frequency Division Multiplexing
PHICH ---Physical channel Hybrid ARQ Indicator Channel
PSS--------Primary Synchronization Signal
RRC ------Radio Resource Control
RAND --- Random number
SEAF -----Security Anchor Function
SIB---------System Information Block
SIDF ------Subscription Identifier De-concealing Function
SSS--------Secondary Synchronization Signal
TAU ------Tracking Area Update
TDD ------Time Division Duplex
TLS -------Transport Layer Security
UDM -----Unified Data Management
UE --------User Equipment
XRES --- Expected Response

Chapter 1. Introduction

In this introductory chapter we will look at network architecture of some of the most advanced and widely used wireless communication system, namely in 4G/LTE and in internet of things (IoT). With the development of telecommunication and internet technology, internet of things (IoT), has become a new trend of research due to its wide applications. Utilising a large number of end nodes with sensors, IoT is able to measure, record and manage a large variety of biological and environmental parameters. This detection and analysis of data in real time greatly reduces human intervention and increases the potential for economic growth in various industries. However, the implementation of IoT is limited and constrained by the transmission range and battery life of end devices. Traditional end devices such as WiFi and ZigBee have high data rage, but short range; on the other hand, cellular devices such as 4G/LTE devices have high data rage, long range, but high power consumption. In practice, a lot of application scenarios for IoT do not require high data rate, these include water level monitoring, target location tracking, and smart city, etc. Hence in response to providing viable internet protocols for IoT applications, many low power wide area network (LPWAN) protocols have emerged. This include NB-IoT, LoRaWAN, Sig-Fox, etc. These protocols have low power consumption and cover a long transmission range. The model for LPWAN to study in this paper focuses on LoRaWAN due to its wide acceptance in applications and simplicity in design. In the following subsections, we are going to compare the network architecture of 4G, 5G and LoRaWAN.

1.1 LTE network architecture

Featuring high data rate and low latency, LTE network usually consists of a E-UTRAN and an EPC. E-UTRAN contains e-Node B and several UEs. EPC comprises of MME, a serving gateway, an HSS, and a packet data network gateway (Fig 1).

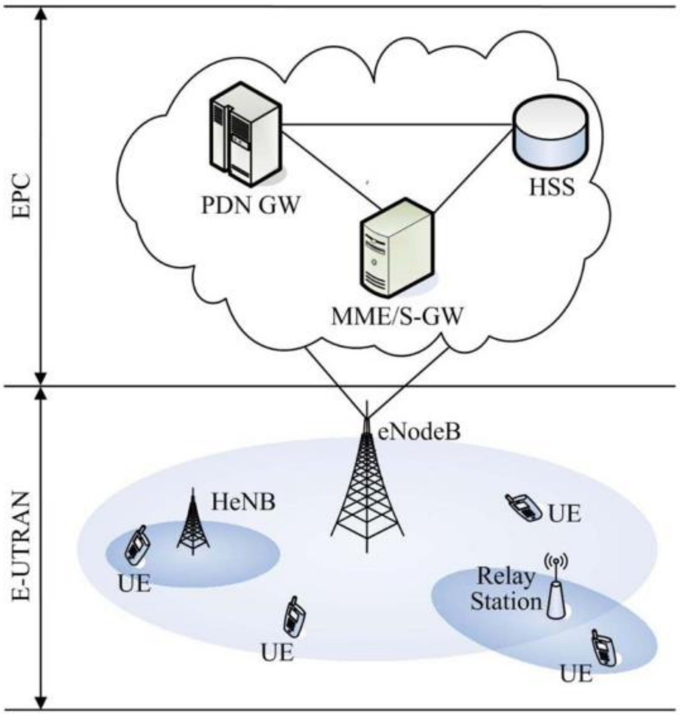


Figure 1. LTE architecture [1].

Data communication between UEs and EPC is protected by EPS-AKA procedure, which is a 2-way authentication process shown in Fig2. This mutual authentication is required, because only the UE with a legitimate subscription is allowed to camp on the network, while UEs need to ensure it is the correct network to attach to.

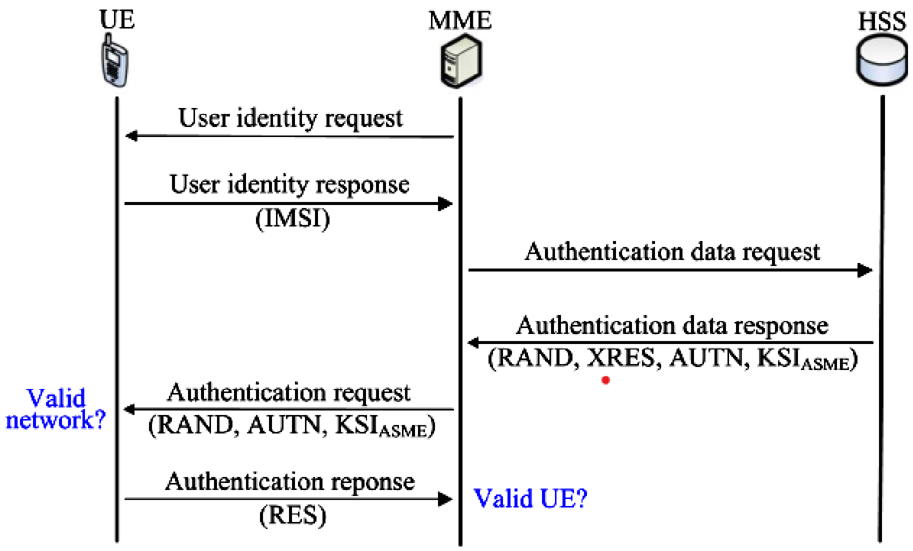


Figure 2. EPS-AKA authentication [4]. Description followed below.

Upon receiving Attach request from UE, MME needs to confirm IMSI of UE, followed by requesting authentication vectors generated by HHS. Authentication vectors contain: {RAND, $AUTN_{HSS}$, XRES, K_{ASME}}. MME selects one of the AVs and send part of it {RAND, $AUTN_{HSS}$} to UE, which is then able to compute $AUTN_{UE}$, XRES, and K_{ASME} based on EPS-AKA algorithm [1]. The authentication on UE's part is done by UE comparing its $AUTN_{UE}$ and $AUTN_{HSS}$ received from MME. If authenticated, UE forwards its XRES generated to MME. The authentication on MME's side is done by MME comparing XRES received from UE to that from HSS [1]. It is noteworthy that UE and MME share the same K_{ASME}, although it is not sent from MME to UE.

The attach request brings UE from EMM-deregistered state to registered state (Fig3). Only registered UEs have access to MME, SW-gateway and IP address. EPS bearer provide connection to the default data network.

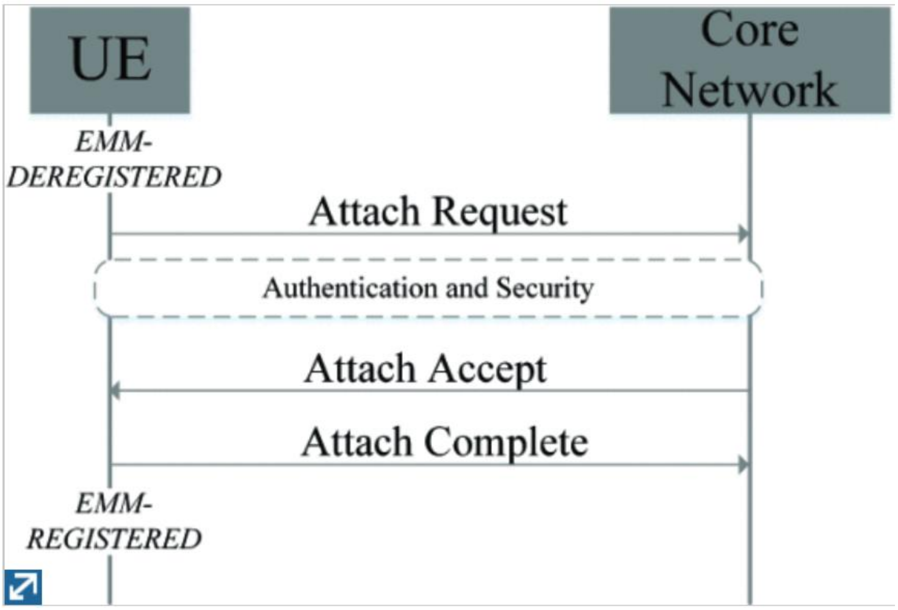


Figure 3. UE attachment process. Following UE's attach request, core network responds with attach accept, then UE sends attach complete to finish the process [1].

1.2 5G architecture

Based on service-based architecture, 5G introduces new entities, including SEAF (Security Anchor Function) as serving network, and AUSF (Authentication Server Function), together with UDM (Unified Data Management) /ARPF (Authentication Credential Repository and Processing Function) /SIDF (Subscription Identifier De-concealing Function) as the home network, shown in Figure 4.

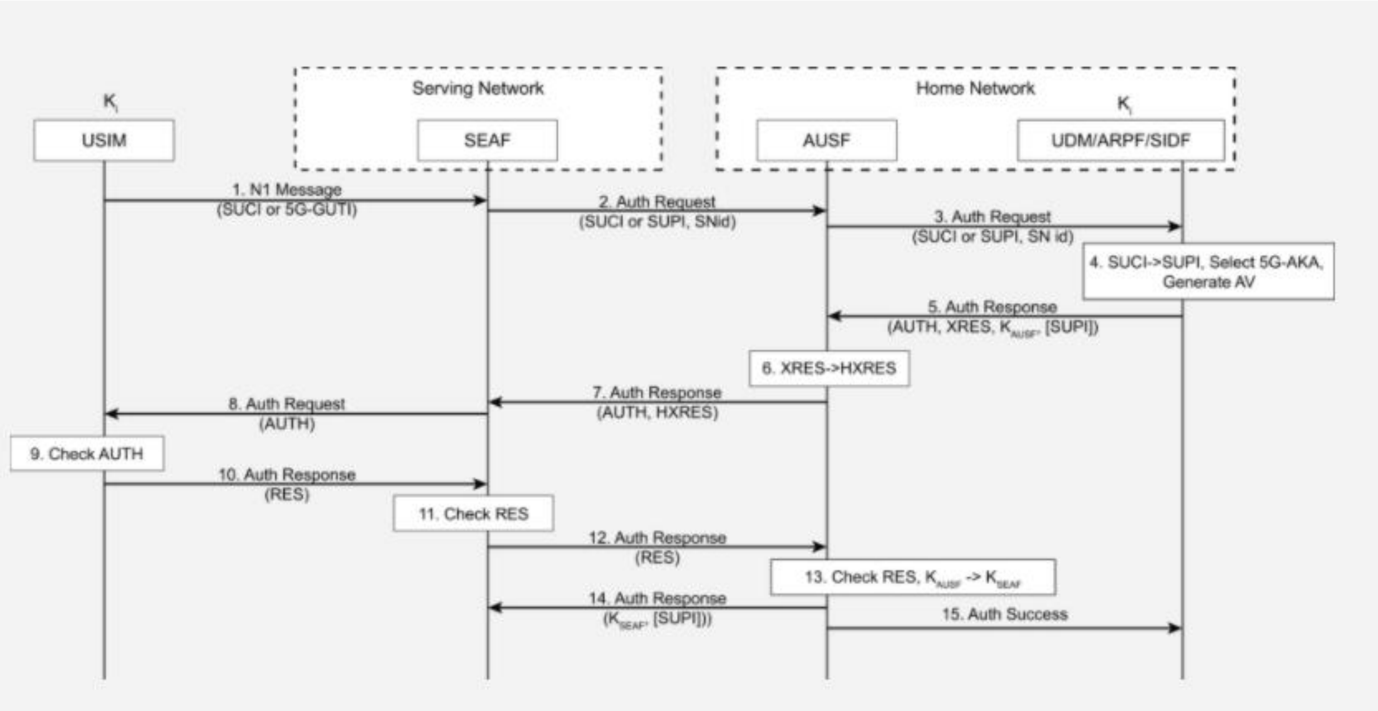


Figure 4. 5G network architecture [2].

Furthermore, the advantage of 5G network structure in terms of security include:

1) Higher security for UE permanent identifier. In 4G, UE sends its permanent identifier to radio network, whilst in 5G UE uses home network public key to encrypt its identity [2].
2) In 5G, final decision on UE authentication is made by home network (AUSF) instead of serving network [2].
3) Longer key hierarchy due to introduction of two immediate keys (K_{AUSF} and K_{AMF} (Access and Mobility Management Function)) instead of only one in 4G (K_{ASME}) [2].

1.3 LoRaWAN architecture

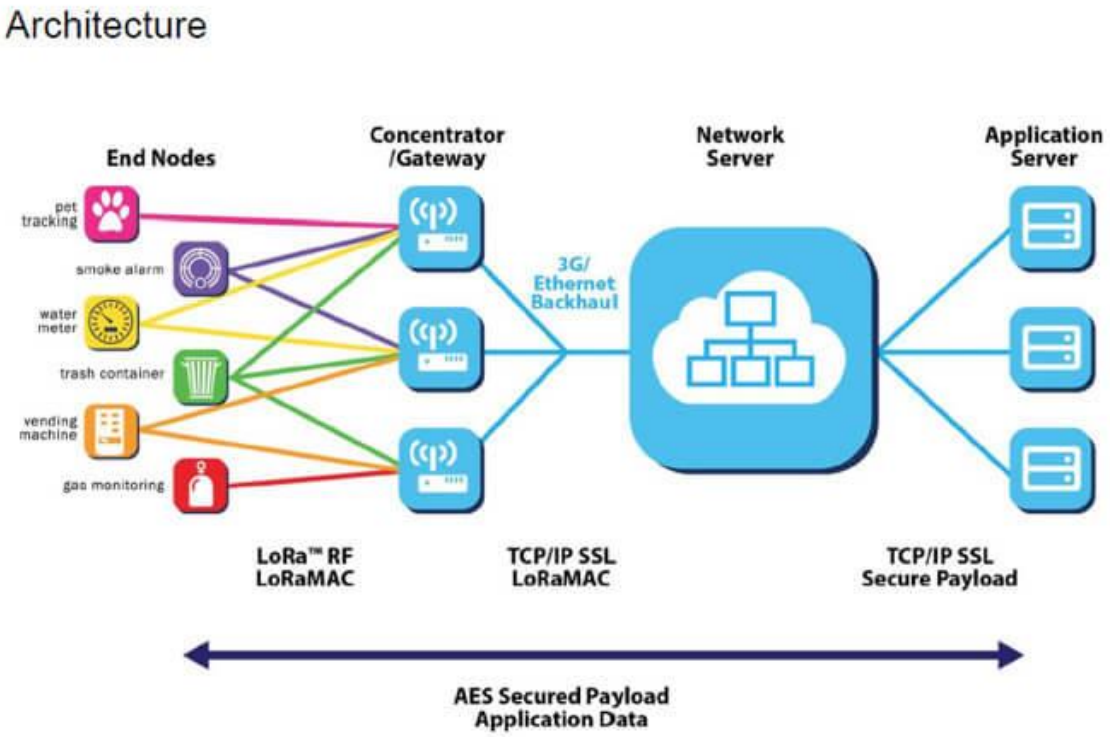


Figure 5. LoRaWAN network architecture.

In comparison to LTE and 5G, LoRaWAN as a wireless network has simpler design, and it also has base stations which share similarity with 5G and LTE. End devices send packets to the gateway, and the gateway act as small base stations that connect to network server via 3G or ethernet backhaul, which is then connected to application server. LoRaWAN upper layers has AES secured payload encryption, but its physical layer share basic principle with 4G and 5G therefore LoRaWAN can server as a model to study wireless network physical security issues.

Chapter 2 Wireless security

2.1 Issues in wireless security overview

Wireless communication is vulnerable to attacks from illegitimate users due to its broadcasting of radio wave propagation. The wireless network, similar to wired network, is also consistent to OSI model, comprising of physical layer, MAC layer, network layer, transmission layer, and application layer. Each layer has is unique susceptibility and challenges for protection against attacks, usually implemented by transmission protocols specific to each layer. In general, security requirements of wireless communication include authenticity, confidentiality, integrity and availability.

To protect the aforementioned four aspects of data transmission, cryptography solutions are widely used, despite the requirement for additional computational power and the resultant latency. Cryptography authentications at multiple layers combine to form the defence against security attacks, at the expense of high computation cost and latency [3]. However, due to the broadcast nature of wireless medium, wireless networks are still susceptible to attacks such as eavesdropping attack, DoS attack, MITM attack, and jamming attack, etc. The key to address each attack is to identify which layer is being exploited by the hacker and proposal of solutions can be generated based on a deeper understanding of wireless network characteristics, infrastructure components, and main protocols and specifications being used in each layer.

2.2OSI layers and types of attacks

According to OSI model, wireless communication systems in general can be divided into multiple layers, including PHY layer, MAC layer, network layer, transport layer and application layer. A generic OSI layered protocol architecture is represented in Fig6. The definition of multiple layers specifies the disciplinary scope professional engineers dedicate to. Malicious attacks above network layers, such as malware attacks are in general taken care of by software engineers, whereas network engineers are responsible for preventing and protection against lower level attacks.

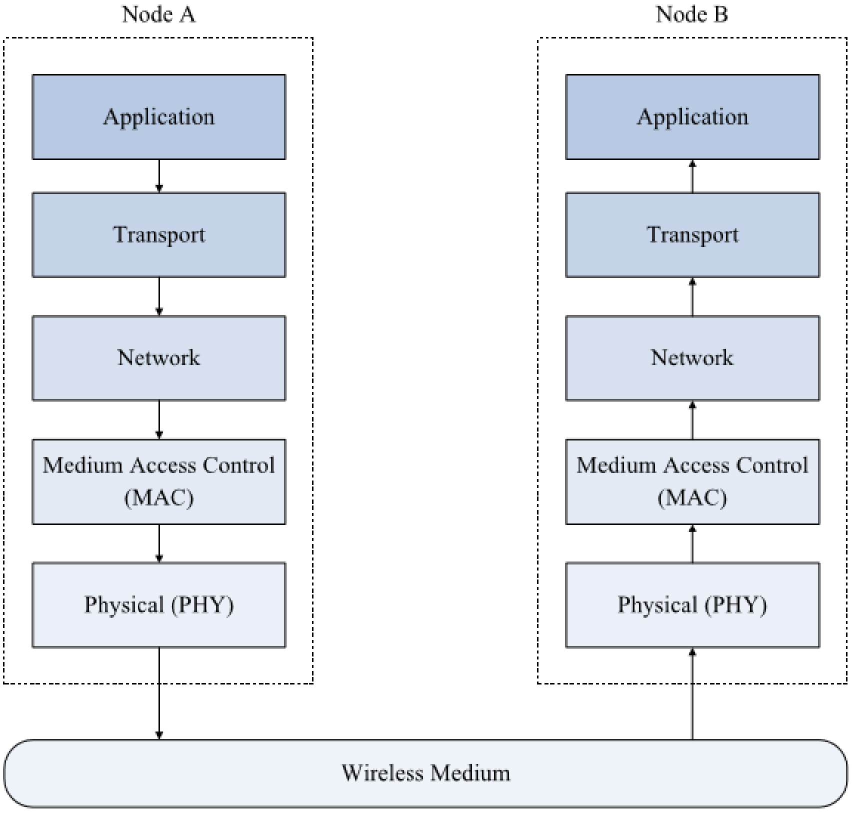


Figure 6. Generic OSI layers of wireless system [3].

For our research interest, a closer look is taken on 4G LTE structure specifically, called E-UTRAN (Evolved Universal Terrestrial Access Network) Protocol Stack, as shown in Fig7. This is followed by a brief description of each layer of interest, and a discussion showcasing their vulnerability against various types of attacks.

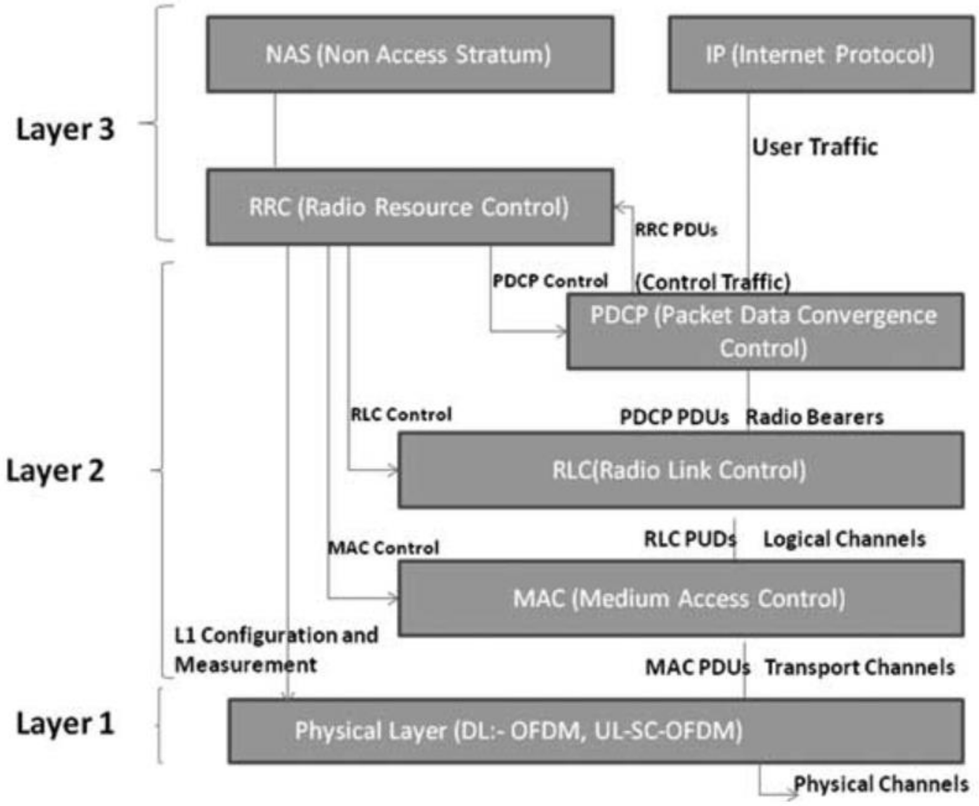


Figure 7. LTE lower level network architecture [4].

2.2.1 Physical layer:

Physical layer is responsible for transmission of information passed down from MAC transport channels over the air-interface. Its main function is to establish UE (User Equipment) cell search in terms of initial synchronization and handover, as well as measurements for RRC (Radio Resource Control) player. PHY is susceptible to following groups of attacks described below.

1) Eavesdropping attack: interception of confidential information. When the eavesdropper lies within the coverage area of the source node, it overhears the data of UE. The difficulty of performing eavesdropping attack will be massively increased with the implementation of cryptographic encryption at the physical layer, with the source node and destination node sharing a secret key, therefore the cipher text will remain difficult to translate. This can occur if the encryption is not completed at the air-interface. The attacker can use equipment to capture and store the data communication between UE and NW (Network), and after identifying the specific LTE frequency and timeslots, the captured traffic can be demodulated into IP packets [4].

2) Jamming: interruption of legitimate transmission. This happens when a malicious node intentionally interferes and disrupts data communication between UEs. Counter measures: spread spectrum techniques, DSSS (Direct Sequence Spread Spectrum)/FHSS (Frequency Hopping Spread Spectrum) techniques. Jamming attack disrupts data communication between UE and NW, as it exploits the radio frequency channel used to receive and transmit information. This is done by decreasing signal to noise ratio across at given frequency band [5]. Jamming between UE and NW or jamming between e-Node B (Evolved Node B) has been shown possible.

2.2.2 MAC layer:

MAC layer links and maps between logical channels and transport channels. It is also responsible for error detection through HARQ (Hybrid Automatic Repeat Request), UE priority handling through dynamic scheduling [6].

1) MAC spoofing: falsification of MAC address
2) Identify theft: stealing of a legitimate user's MAC identity
3) MITM attack: impersonate 2 parties through falsification of MAC address acquired via identify theft. Sometimes breaking the endpoint authentication is required.
4) Network injection: injection of false network commands

2.2.3 Network layer:

NAS and RRC are the main components of network layer. NAS (Non-Access Stratum) is the highest level of control plane between UE and MME (Mobility Management Entity), whilst RRC is responsible for paging and establishing connection between UE and E-UTRAN, broadcasting System Information from AS (Access Stratum), and establishing as well as managing keys for authentication. It is the layer where various attacks are targeted towards, and especially rogue base station attacks can occur in this layer, resulting in DoS, identity spoofing, and other disruption or revelation of UE service functions. Examples include:

1) IP spoofing: falsification of IP address
2) Smurf attack: to paralyze a network by overflooding of ICMP (International Message Control Protocol) requests

In relation to intrinsic vulnerability of network layer, mechanism of rouge base station attacks is described in the following steps involved:

1) Connecting UE to rouge BS，by sniffing SIB5 (System Information Block) and adjusting high priority, then rouge BS can broadcast same MNC (Mobile Network Code) and MCC (Mobile Country Code).
2) One of the EMM (EPS Mobility Management) procedure, called TAU (tracking area update) is exploited. TAU (Tracking Area Update) procedure updates the location of UE with MME, the outcome of which will decide the mode of network (i.e. 2G, 3G, LTE).
3) The rouge BS sends a fake TAU reject message to UE, hence disrupting UE's LTE service by preventing the UE from attaching to the rogue BS.

Rogue base station attacks can reveal user device identity (IMSI) and geographical tracking. It can also prevent emergency calls, or downgrade 4G LTE service to 2G. Hence it is very important to secure UE's authentication process with the core network, the mechanism and challenges of which will be described in the following section.

2.3 PHY-layer security in wireless networks

2.3.1 LTE PHY security

LTE air-interface serves as the layer1 and layer2 part of the network, it utilizes OFDM (Orthogonal Frequency Division Multiplexing) to reduce signal interference and ensure the orthogonality of signals. OFDM in LTE is well integrated with MIMO, making LTE significantly faster and bandwidth efficient. LTE supports both TDD (Time Division Multiplexing) and FDD (Frequency Division Multiplexing) transmission modes. Signals released from LTE transmitter can be seen as multitudes of frames, with each fame taking 10ms. Frames of physical channel transmission can be further divided into 10 subframes, while each 1ms subframes consists of two slots, each taking 0.5ms. Each slot consists of 6-7 OFDM symbols, depending on the cyclic prefix encoded.

On time-frequency resource block representation of LTE signals, signals in each slot are represented by 1 resource block. Since there are 12 subcarriers in 180kHz bandwidth, and for OFDM symbols of 7, in one RB we have 12 * 7 = 84 resource element. For example, a 5 MHz downlink signal could be described as 25 resource blocks wide or 301 subcarriers wide.

An OFDM symbol contains a complex value representing data from a physical channel signal. For channel estimation, receiver recognizes CSR in the Resource Block, and then it estimates other (signal) channels in the Resource Block. Then it can proceed to do symbol equalization [7]. Following this the UE can perform channel equalization, and they can remove the cyclic prefix of OFDM symbols thus decoding the symbols [7].

Physical channels are the lower layer implementation of transport channels. For user attachment process, UE has to recognize a series of physical channel signals, such as C-RS (Cell-specific Reference Signal) and SSS (Secondary Synchronization Signal). Firstly, during cell acquisition, UE search for and recognizes PSS and SSS to identify cell-ID. Afterwards, the UE gain information of signal transmission, such as duplex mode, cyclic prefix and frame timing. Once this is completed, UE can decode PBCH (Physical Broadcasting Channel) for gaining MIB (Master Information Block) information [8]. User has to look for C-RS which contains channel estimation matrix and number of antennas BS is using. MIB carries operating bandwidth, frame number and PHICH (Physical channel Hybrid ARQ Indicator Channel) configuration [8].

2.3.3 Existing research on PHY SEC

Physical layer security is different compared to other upper layer security, as it utilizes random nature of physical layer transmission media to achieve security goals. Traditionally PHY SEC does not need to consider which security protocols to use, and does not require cryptographic configurations, and it has the benefit of authenticating legitimate nodes quickly before demodulating the signals [8].

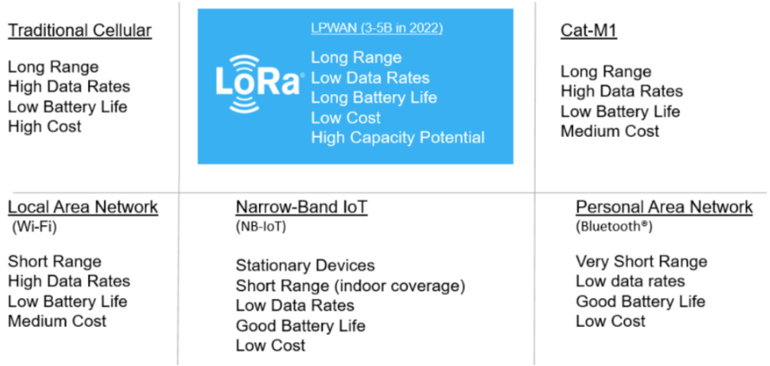
Shannon's information theoretic analysis shows that secrecy is achieved when the transmission rate is higher than the eavesdropping wiretap channel, thus the eavesdropper has to guess the bits of signal information [9]. Therefore, introducing high entropy and concept of equivocation are important aspects. This method of using signal processing technology to create a line of defense is about design secure code of random or structured nature, to maximize secrecy capacity. However, when the SNR of messenger is greater than SNR of wiretap, the capacity is too low to be useful in practice, and this wiretap coding scheme will be rendered ineffective [9]. Hence, PHY-Key generation methods have been the focus of researches.

A general way of generating PHY key is to utilize channel randomness, by measuring CSIs, RSS, and phase information. Alice and Bob use pilot signals to obtain their connection channel's CSI h_{ab}. By using a source coding scheme, A and B can derive and share a private key. While Alice and Bob share the same characteristics of channels, the eavesdropping located more than 1 have wavelength away cannot get the channel characteristics profile [9]. Due to some unique environmental impacts such as multipath delay, scattering the channel profile will be unique between Alice and Bob, and Bob can hence differentiate the attackers channel profile [9].

Challenges in PHY-Key generating using CSI profile have been studied. One challenge is the reconciliation process between A and B to agree on the secret key, if bit mismatch occurs, error control coding will consume time and space overhead [10]. Secondly, insufficient secrecy capacity and extra error bits render the key generation rates very slow. Thirdly, this security can be sensitive to impersonation attacks, as the attacker can maximize the likelihood of guessing Alice and Bob CSI profile based on observation of other channel CSI profile [10]. This way the attacker can pre-modify the transmission signal profile, and perform impersonation attack on receiver. Lastly, at low SNR Bob's judgment may not be robust, because there might be more overlapping part due to noises, channel variation, and path delay.

Chapter 3 LoRaWAN network

LoRaWAN is one of the most highly developed and recognised LPWAN in the current industry and market, due to its ultra long battery life and long transmission range that come with a low cost. A LoRaWAN end device has low power requirement in milliwatts (mW) and can have battery life lasting up to 10 year, and the transmission range in rural area can be as far as 15 kilometres. Even in urban area with dense data traffic the supported range is estimated to be around 5 kilometres. The factor that contribute to the low cost of LoRaWAN is that, unlike NB-IoT, LoRa operates in unlicensed spectrum, which means the users only need to purchase Gateway (GW) as small base station, and one gateway can support a large multitude of end devices. This makes LoRa an ideal candidate for applications that only utilizes modest data rates, such as agriculture monitoring, pasture animals tracking, and smart city applications such as water level.



Traditional Cellular

Long Range
High Data Rates
Low Battery Life
High Cost

LPWAN (3-5B in 2022)

LoRa

Long Range
Low Data Rates
Long Battery Life
Low Cost
High Capacity Potential

Cat-M1

Long Range
High Data Rates
Low Battery Life
Medium Cost

Local Area Network
(Wi-Fi)

Short Range
High Data Rates
Low Battery Life
Medium Cost

Narrow-Band IoT
(NB-IoT)

Stationary Devices
Short Range (indoor coverage)
Low Data Rates
Good Battery Life
Low Cost

Personal Area Network
(Bluetooth®)

Very Short Range
Low data rates
Good Battery Life
Low Cost

Figure 8. Comparison of different internet protocols.

LoRa uses Chirp Spread Spectrum (CSS) modulation scheme, where the original data signal is modulated onto a Chirp signal that continuously varies in frequency. CSS scheme share the same principle with FSK (frequency shift keying) and DSSS (direct sequence spread spectrum) scheme. FSK uses 2 frequencies to represent digital values, whereas in DSSS the original data signal is multiplied onto the carrier phase signal which has much higher frequency and hence the data is spread across a wider bandwidth. CSS scheme is more complex than FSK and DSSS, and is more resilient to noise, as unlike FSK it uses Chirp, which is the sweep up or down signal to encode digital values, and unlike DSSS it does not require a reference clock. For the Chirp signal, the frequency bandwidth is equivalent to its spectral bandwidth, which means it sweeps up or down between the highest frequency (f-high) and lowest frequency (f-low).

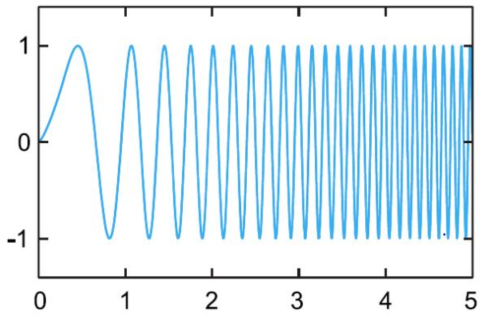


Figure 5: LoRa Chirp Spread Spectrum illustration

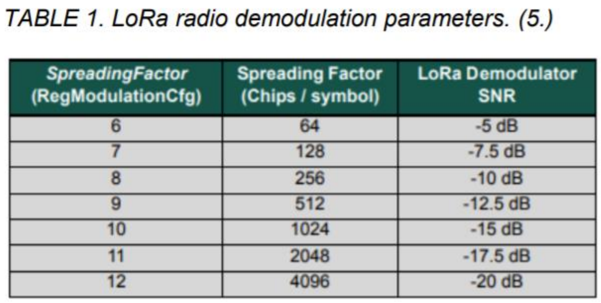


TABLE 1. LoRa radio demodulation parameters. (5.)

SpreadingFactor (RegModulationCfg)	Spreading Factor (Chips / symbol)	LoRa Demodulator SNR
6	64	-5 dB
7	128	-7.5 dB
8	256	-10 dB
9	512	-12.5 dB
10	1024	-15 dB
11	2048	-17.5 dB
12	4096	-20 dB

Figure 9 & Table 1. An illustration of LoRa CSS and a table for lora SF demodulator SNR.

There are two important parameters that are associated with the LoRa chirp signal, namely bandwidth and spreading factor (SF). Bandwidth is under international standard regulation, and it is 125k Hz for uplink and 250 kHz for downlink. Spreading factor determines how wide the code sequence signal encoding data is spread over time spectrum. SF represents how many raw bits of information one symbol can encode, and one symbol can hold 2^{SF} chips. There are 6 spreading factors for use in LoRa, ranging from 7, 8, 9, 10, 11 to 12. Higher value of SF has longer transmission range due to higher reception sensitivity, but this is compromised by lower data rate. Usually the end devices that are close to the gateway will take lower values of SF for transmission, such as 7 or 8, while end devices that are far away from gateway will take higher values of SF for transmission.

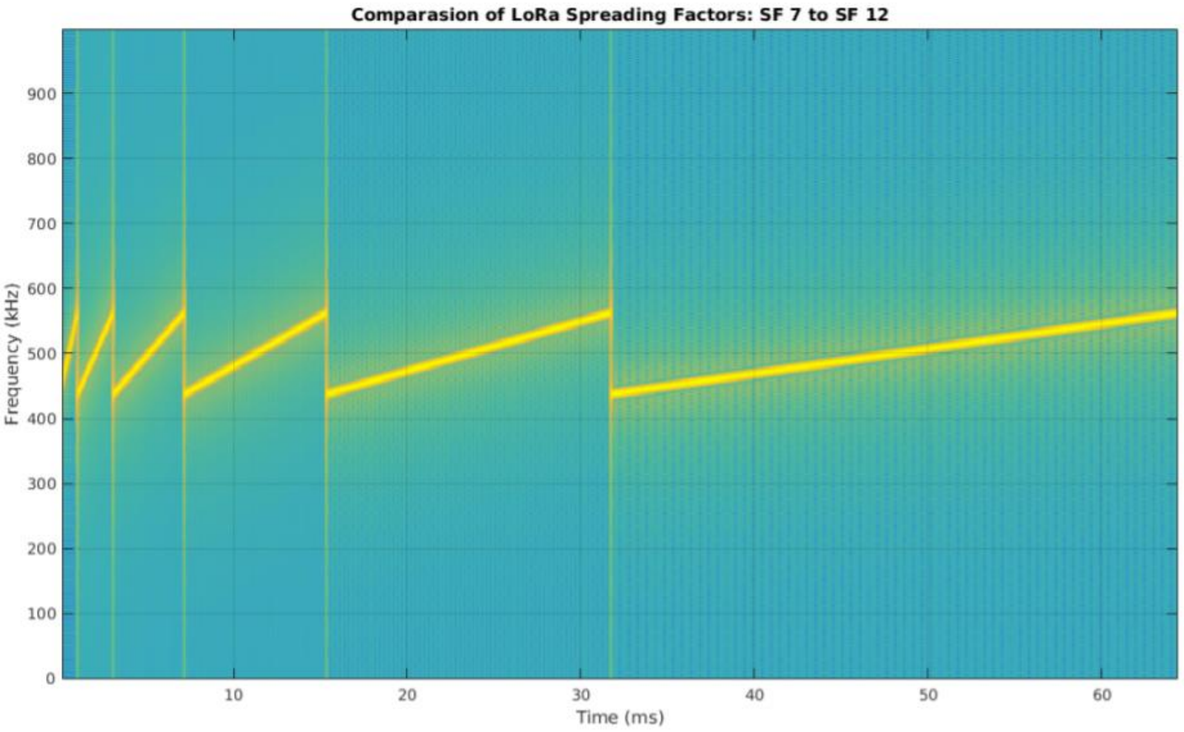
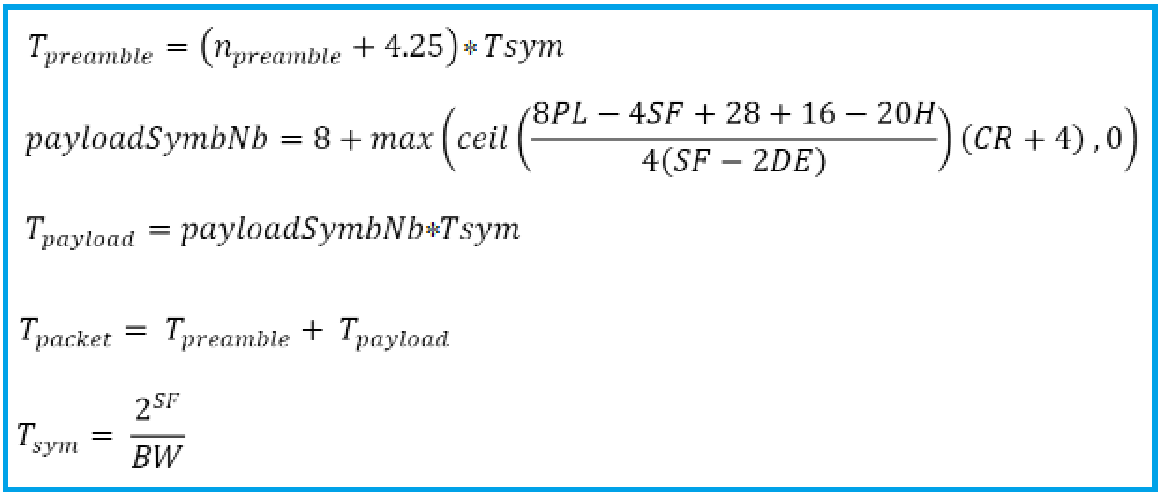


Figure 10. Spectrogram of different LoRa spreading factors.

A compromise to ultra-low power consumption in LoRa is that the end devices need to be designed with high constrain. This poses a security challenge as IoT network are susceptible to a range of malicious attacks. Currently, LPWANs such as LoRa utilizes 128-bit AES (Advanced Encryption Scheme) for upper layers, making the MAC layer and above reasonably secure against attacks at upper layers such as replay attack. However, LoRa is still vulnerable to jamming-type attack at the physical layer, where malicious nodes send out signals to interfere and disrupt communication between end devices and gateway by decreasing the Signal to Interference Noise Ratio (SINR).

As LoRa operates in the unlicensed band, it is important to constrain how much resources each device can occupy the channel. Therefore, it is under international regulation that the duty cycle for LoRa devices is 0.01, meaning the maximum percentage of the time during which an end device can occupy a channel is 1%. The transmission time for each spreading factor is different, this definition is time on air, which is calculated by adding up the transmission time for preamble and the payload, which is shown below.



$$T_{preamble} = \left(n_{preamble} + 4.25\right) * Tsym$$

$$payloadSymbNb = 8 + max\left(ceil\left(\frac{8PL - 4SF + 28 + 16 - 20H}{4(SF - 2DE)}\right)(CR + 4)\,,0\right)$$

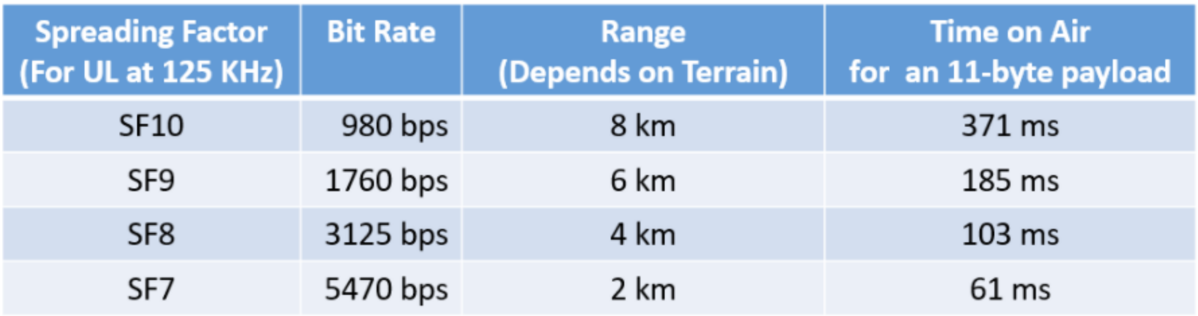
$$T_{payload} = payloadSymbNb * Tsym$$

$$T_{packet} = T_{preamble} + T_{payload}$$

$$T_{sym} = \frac{2^{SF}}{BW}$$

(DE=1 when the header is enabled, and CR is the coding rate, PL is payload bytes).

Greater SF has lower bit rate, longer time on air, and better receptor sensitivity.



Spreading Factor (For UL at 125 KHz)	Bit Rate	Range (Depends on Terrain)	Time on Air for an 11-byte payload
SF10	980 bps	8 km	371 ms
SF9	1760 bps	6 km	185 ms
SF8	3125 bps	4 km	103 ms
SF7	5470 bps	2 km	61 ms

Table 2. Summary of SF and corresponding bit rate and time on air.

As the transmitter sends signals encoded with different spreading factors, LoRa receivers are able to lock on the frequency received, providing sensitivity on the order of -130 dBm. The formula for LoRa receiver sensitivity is: $S = -174 + 10 \log_{10} BW + SNR$. This is why higher spreading factor result in higher sensitivity.

Previous works on LoRaWAN modelling have been focusing on delay, throughput, energy consumption etc. Simulation of LoRaWAN jamming attack received limited attention. The first complete NS-3 module for LoRaWAN was presented to test the scalability of LoRa in urban scenario setting [13], and it showed promising success rate for end devices in the range of 5 to 7 kilometres. Gateway is modelled to have 8 reception paths, end devices payload length (including preambles) to be 50 bytes, and receptor sensitivity following the Semtech SX1272 [14] data sheet. In a more recent research, the jamming module extension is added to enhance the functionality of LoRaWAN module [15]. Here we aim to utilize this module to explore the impact and extent of jamming attack on LoRaWAN network, and perform qualitative analysis on the results obtained.

Chapter 4 Simulation of LoRaWAN in NS-3

In this section we outline the major steps involved in simulating LoRaWAN network using NS-3 (Network Simulator -3) with Linux system. This is followed by brief introduction of C++ files which make up the LoRaWAN architecture, and a introduction of experimental parameters that we need to control/measure.

4.1 Virtual Machine:

As Windows system does not directly support NS3, first step is to download the linux system. The virtual machine serves as a platform that runs a virtual environment system in between the user and original system. With virtual machine as an interface, the user is then able to run software for the designated system. The virtual machine runs independently and takes up allocated virtual hard drive space.

For our project we used Oracle VM VirtualBox, which is an open-source virtual machine that can create environment of Linux system running on windows. The download link is from official Oracle website, and it will be provided in Appendix. In this project, Oracle VirtualBox version 6.1.16 is used.

4.2 Installation of NS3:

After downloading virtual box, we need to download the Linux system. With user friendly design and high operating stability, Ubuntu is a widely recognised free and open source Linux system. Ubuntu version 20.04 is selected as the operating system for this project. The iso file could be downloaded from the official website of Ubuntu, links provided in Appendix.

With the iso file of ubuntu downloaded, we need to set it up in the virtual machine. Select add virtual machine in the user interface, setting 64bit as the operating system with 4GB memory and 20Gb hard drive storage. Afterwards, select Ubuntu as the target of installation, this way the virtual machine will be set up.

Then, the terminal line commands for installation of Linux packages necessary for NS-3 are outlined below:

There are mainly 4 components of packages that support NS-3, firstly is the python 3 setup tools and secondly the modules that support NS-3 visualizer such as pygocanvas and qt-5. Then it is the grammar analyser and debugging tools such as uncrusify and doxygen. Finally support for open flow module and packet flow traces are installed.

1. Get the C++ packages required to run ns-3 from released tarball.

```
apt-get install gcc g++ python python3
```

2. Get Python set up tools

```
apt-get install python3-setuptools git mercurial
```

3. Install qt5 which is required for Net-anim

```
apt-get install qt5-default mercurial
```

4. Install girl-pygoocanvas for NS3-pyviz visualizer for Ubuntu

```
apt-get install gir1.2-goocanvas-2.0 python-gi python-gi-cairo python-pygraphviz
python3-gi python3-gi-cairo python3-pygraphviz gir1.2-gtk-3.0 ipython ipython3
```

5. Support for bake build tools

```
sudo apt-get install autoconf cvs bzr unrar
```

6. Download debugging tools

```
sudo apt-get install gdb valgrind
```

7. Support MPI-based distributed simulation

```
apt-get install openmpi-bin openmpi-common openmpi-doc libopenmpi-dev
```

8. Support for grammar analysis

```
sudo apt-get install flex bison libfl-dev
```

9. Checking Programme

```
apt-get install uncrustify
```

10. Doxygen and inline documentation

```
sudo apt-get install doxygen graphviz imagemagick
```

11. Supporting for Openflow module

```
sudo apt-get install libboost-signals-dev libboost-filesystem-dev
```

12. To read pcap packet traces

```
sudo apt-get install tcpdump
```

13. Database support for statistics framework

```
sudo apt-get install sqlite3 libsqlite3-dev
```

14. Generate modified python bindings

```
sudo apt-get install cmake libc6-dev libc6-dev-i386 ibclang-6.0-dev llvm-6.0-dev automake pip
```

4.3 LoRaWan module architecture:

The main components for simulation include the end devices, gateway, and the network server. They are constructed using NS-3 files individually, and the files generating each components are outlined below.

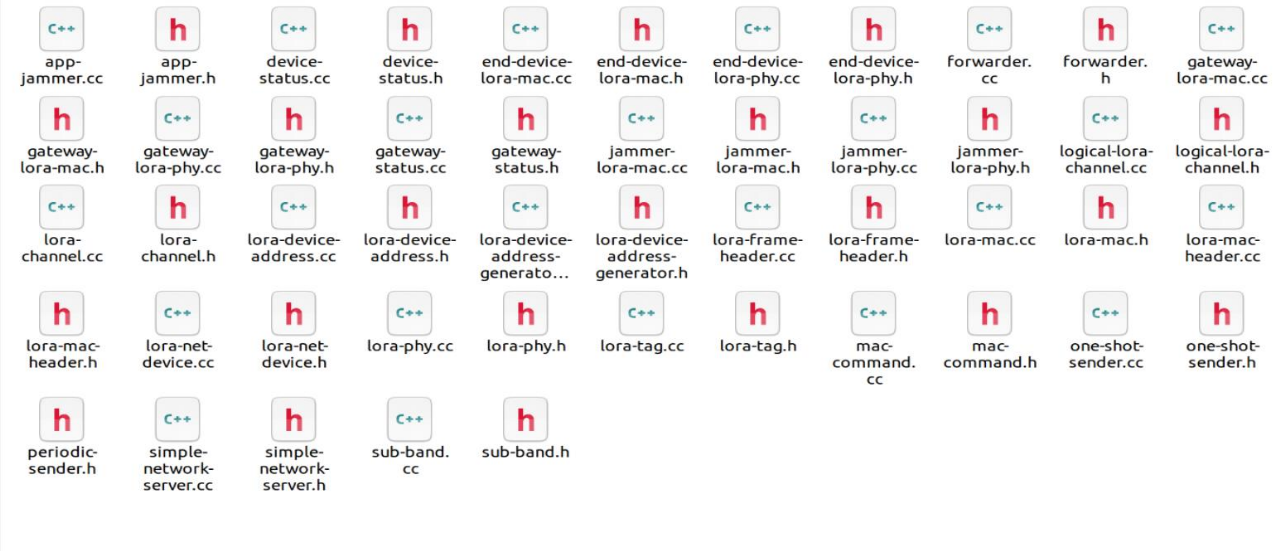


Figure 11. A screenshot of the .cc files and .h header files for component construction.

LoRaWAN files include gateway-lora-phy, gateway-lora-mac, gateway-status, end-device-phy, end-device-mac, lora-phy, lora-net-devices, mac-command, lora-frame-header, lora-device-address-generator, jammer-lora-phy, jammer-lora-mac.

All these files are written in C++, and they are complemented with corresponding header files for compilation purposes.

4.4 Experimental parameters:

- Number of End Devices in the network: 50

- Bandwidth information: 125 KHz bandwidth, on 868.1 KHz band

- Number of Gateway: 1

-Simulation time: 1 hour (3600s)

-Simulation period: 5 mins (300s), meaning packet are sent out every 5 mins on each ED

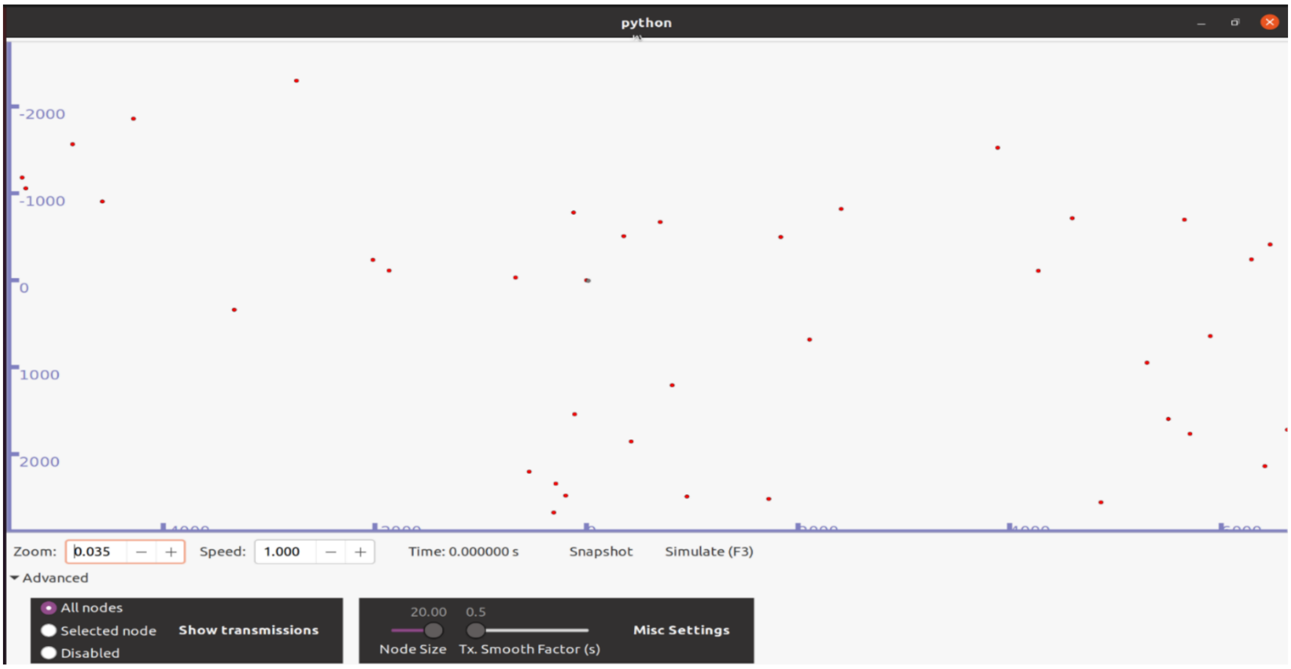
-Payload size: 50 bytes

-Range/distance to gateway: 2-7 km

-Duty cycle: End devices all have 0.01 as DC under regulation, jammers do not follow regulation can therefore take from 0 to 1 for DC value.

-Transmission power: EDs take 14 dB, jammers 20 dB.

4.4.1 End devices location model and spreading factor allocation:



Zoom: 0.035

Speed: 1.000

Time: 0.000000 s

Figure 12. Screenshot of Pyvis visualizer for ED mobility model. (50 end devices over 5km x 5km, with the point of centre being the gateway, indicated by the blue dot at x=0 y=0 location)

The end devices' locations are randomly generated using the mobility model provided in NS-3 module. The above screen shot is a picture taken using the NS-3 pyvis visualizer to illustrate the location setting of 50 end devices spread across an area of 5000 m x 5000 m dimension. They are assembled around the gateway with a star topology, and MAC layer communication protocol follows ALOHA scheme.

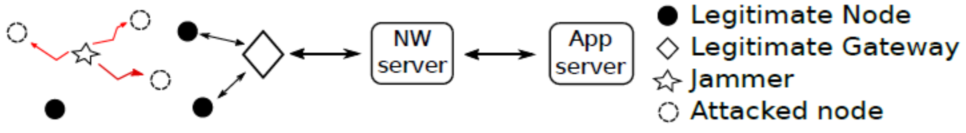


Figure 13. A threat illustration of end devices and jammers in the network.

Then each end devices are allocated the most suitable spreading factor (from 7 to 12) based on Adaptive Spreading Factor Selection Scheme provided by LoRa Semtech. This function calculates the effective transmission power that could be received by the gateway for the target end node, and compare it with the receptor sensitivity for different spreading factor, thus allocating the most suitable one. In our experiment, out of 50 end devices, around 70% took up spreading factor 7, and around 20% took up spreading factor 8, and spreading factor 9, 10, and 11 combined took up the remaining 10% of end devices.

Spreading factor	Number of end devices allocated	Percentage out of all end devices
7	34	68%
8	11	22%

9	2	4%
10	2	4%
11	1	2%

Table 3. Spreading factor allocation for End devices based on Adaptive SF Allocation scheme.

For jammers, their location mobility model used is the same mechanism as the end devices, and their spreading factor allocation scheme is treated as the same. Therefore, the majority of jammers take up spreading factor 7 whilst some take up 8.

Chapter 5 Analysis of LoRaWAN and jamming attacks

In this chapter we will explore a few key parameters in LoRa network, namely spreading factor, duty cycle, and how they can impact the packet success rate of the network.

In the first experiment, we tested the maximum transmission distance for different spreading factors under simulation scenario of 50 end devices with simulation application period of 5 mins per packet. The packet success rate for SF7 maintain around 90% for distance up to 4 kilometres, and it started dropping after the distance gets above 5 kilometres, indicating the signal attenuation has started to affect the transmission quality, and the RF receiver side sensitivity is starting to drop below the detection thresthold. This experiment is consistent with our knowledge that higher spreading factor are more suitable for long range transmission, with spreading factor 10 demonstrating good reception quality at up to 7 km distance range.

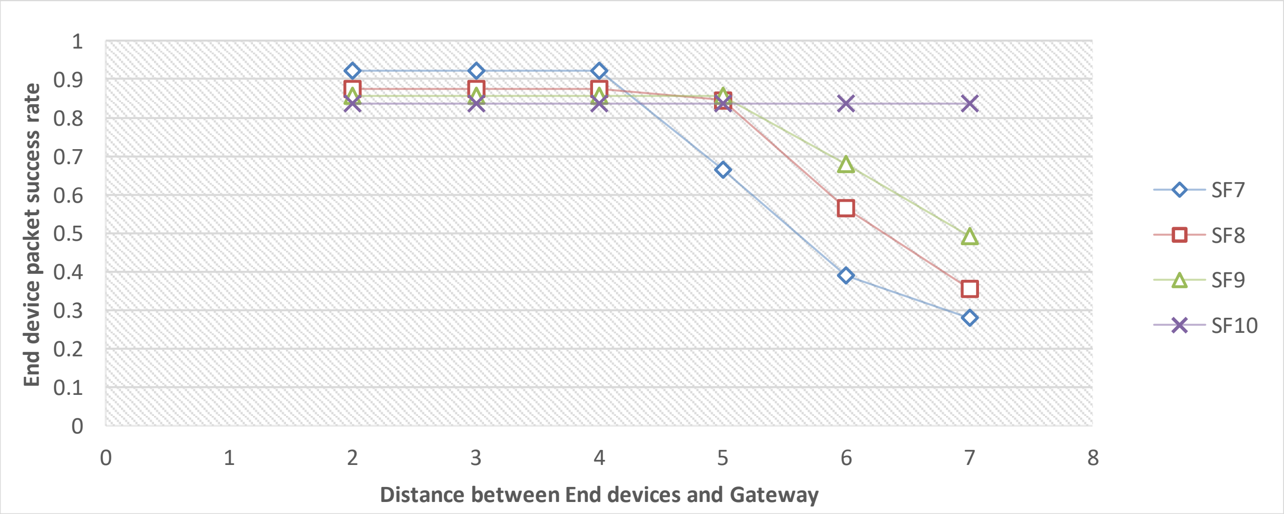


Figure 14. An illustration of transmission range of different spreading factors, shown by plotting end device packet success rate against end devices distance to gateway.

In the following experiment, we will introduce jammers into the normal network, and the main parameters to investigate are jammer duty cycle and jammer numbers. We are particularly interested in above which jammer duty cycle range jammers can cause significant damage to the network, and the jammer number required to cause significant disruption to the network. The results are recorded in Figure 15 and Figure 16.

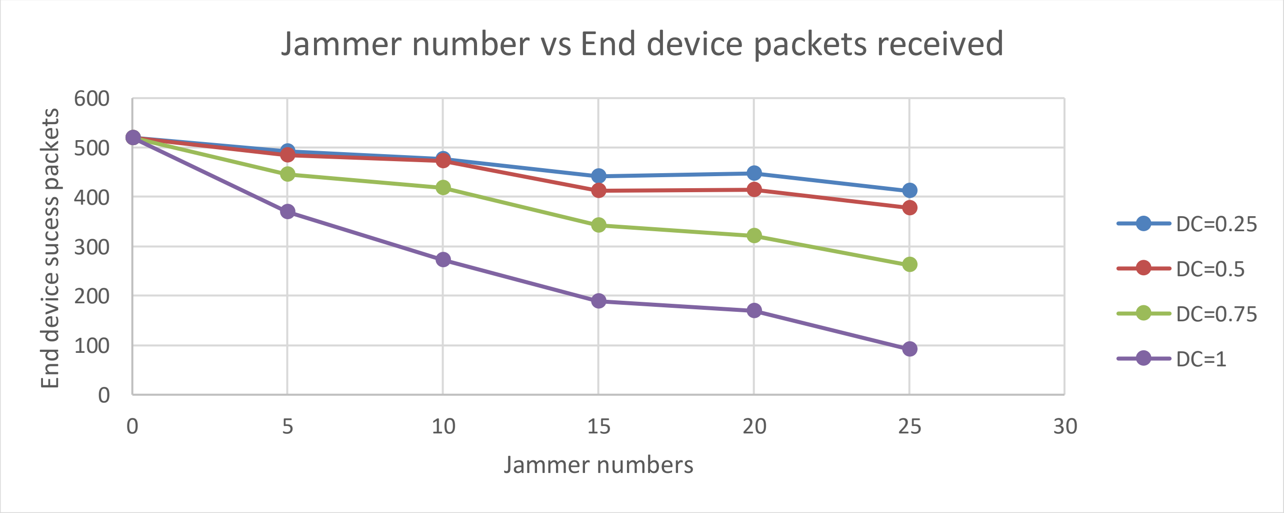


Figure 15. An illustration of jammers impact on LoRa network with 50 ED and 3600 s simulation time with an application period of 5 mins. Jammer's duty cycle is tested, varying from 0.25 to 1, indicated by different colours. It is noteworthy that for DC =1 and jammer number =25, the packet success rate is greatly reduced, to around 20% of its baseline performance level.

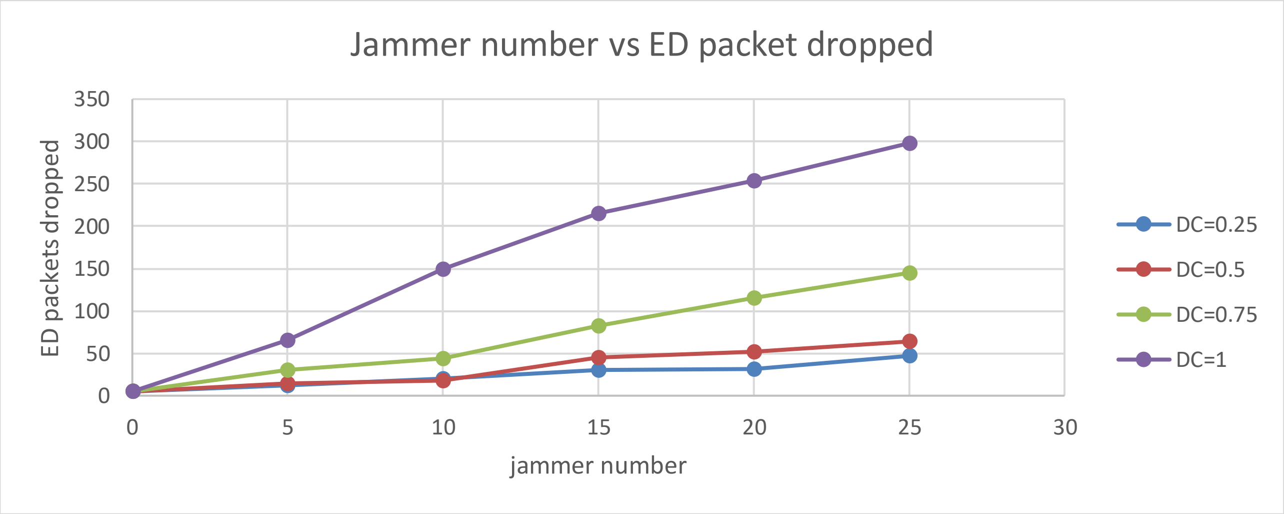


Figure 16. ED packets dropped plotted against jammer number, and jammer DC are indicated in different colours ranging from 0.25 to 1. The packet dropped are due to jammer interference since the gateway has only 8 paths for reception.

For a total simulation time of 1 hour (3600 s) and application period (defined as the period which packet is sent from end devices to gateway) of 5 minutes, each end devices are expected to send 11 times, therefore 50 end devices will yield a total of 550 packets. We can see from the results that when there's no jammer in the network, packets successfully delivered is equal to the ideal number of 550. But as the jammer's duty cycle and jammer's number increase, the collision between jammer signal and end devices packets increases and packet delivery success rate decreases.

For the next experiment, we will explore how to improve the total transmission success under jamming. We investigate the retransmission mechanism, and the parameter of interest is the maximum retransmission number, which is the number of times end devices can re-send an unsuccessful packet if the end device itself does not hear back the ACK message from the gateway. If this ACK is timed out, end devices will be programmed to retransmit the packet.

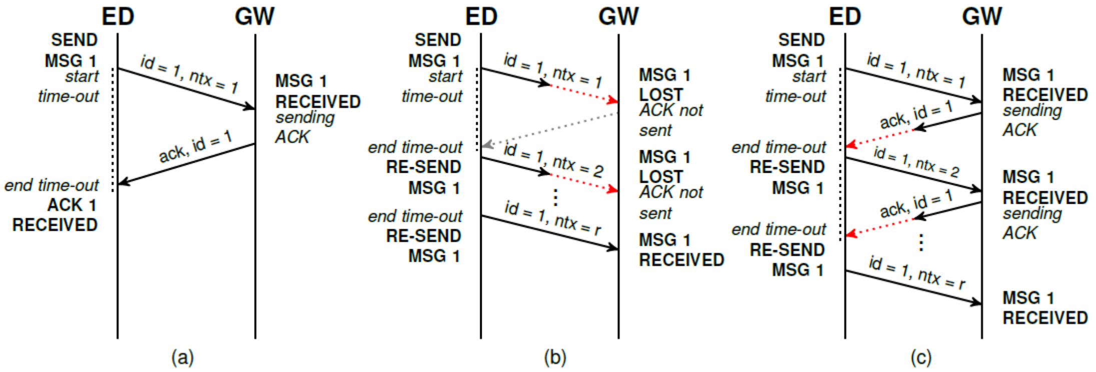


Figure 17. Retransmission scheme for end devices. In response of end devices message, gateway sends back acknowledge (ACK) message to end devices.

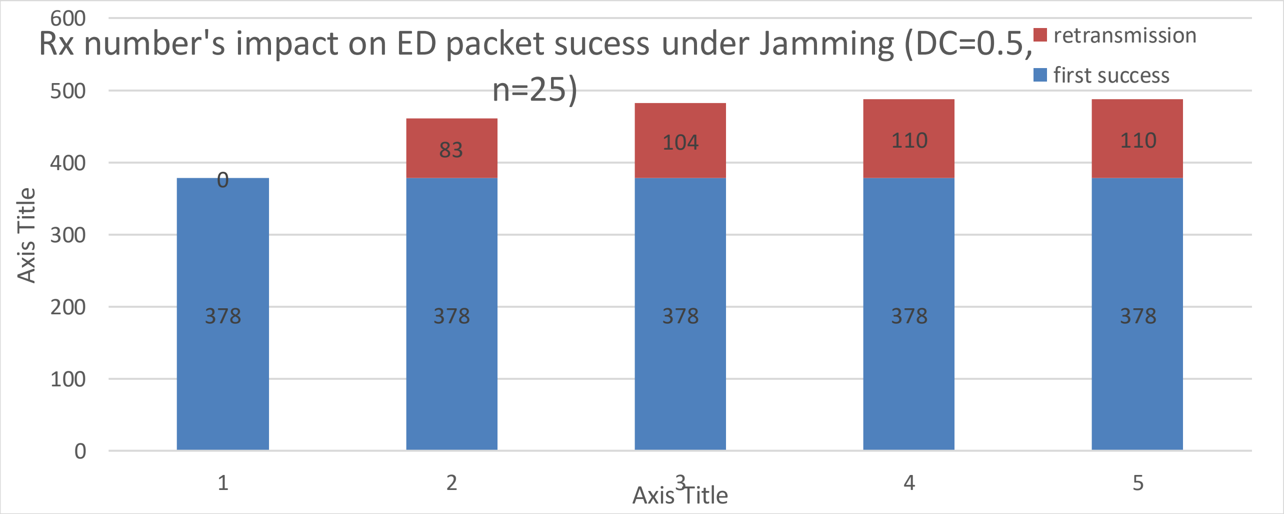


Figure 18. This is a bar graph showing the degree of retransmission success under 25 jammer scenario with DC = 0.5. The blue part represent the number of packets successfully delivered to

GW in ED's first attempt. The red part indicates the number of packets undergoing successful retransmission, thus increasing the overall packet delivery success.

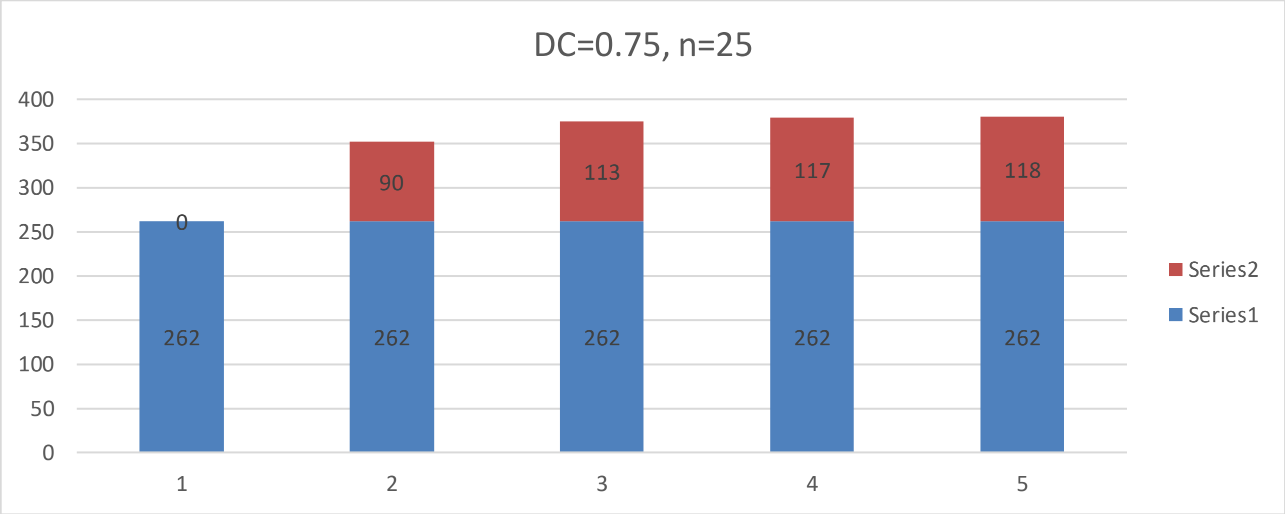


Figure 19. Similar to above, this is a bar graph showing the degree of retransmission success under 25 jammer scenario with DC = 0.75.

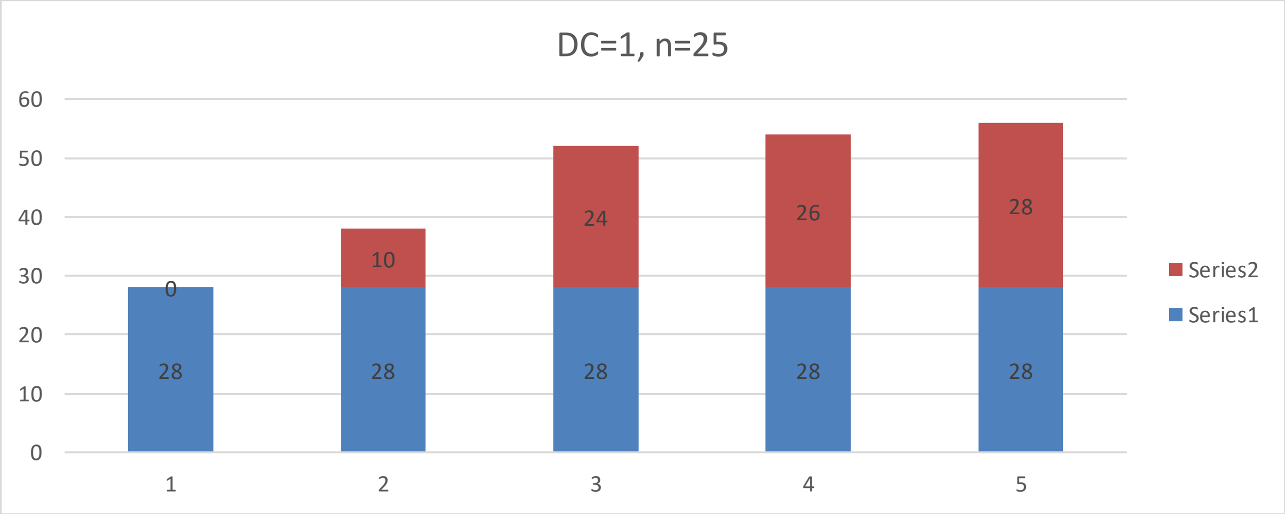


Figure 20. Similar to above, this is a bar graph showing the degree of retransmission success under 25 jammer scenario with DC = 1.

From the above 3 sets of experiments, we have proofed the following conclusions:

1. Higher spreading factor yields high sensitivity, and can be transmitted for longer distance, which is consistent with the LoRa existing knowledge and consolidate the correctness of our model.

2. When jammer duty cycle is below 0.5, the increase in jammer number does not have significant impact on end devices packet delivery success rate, which means under normal interference conditions, LoRa has high anti-interference resistance, and it is a good communication protocol/technology for IoT communication. Only when jammer duty cycle above 0.75 the increase in jammer number could result in significant drop in packet delivery success rate, and this is more likely due to the scenario of malicious jamming attacks.

3. For the improvement of total success rate, performance under retransmission scheme has been simulated. It is discovered that, the first retransmission can significantly increase the reception success rate, whilst the subsequent retransmissions are not as effective in enhancing overall performance. The maximum total packet success is achieved when maximum retransmission number equals to 4.

Chapter 6 Conclusion

In recent years, with the rapid development of IOT technology, the Internet has entered the era of industrial interconnection and interconnection of all things. Trillions of information nodes' data can be connected to the network, which brings the challenge of how to effectively collect and transmit node information. The traditional sensor consumes a lot of power and the transmission distance is the biggest problem. Therefore, a wide area network with ultra-long distance and low power consumption is the key to IoT, and LoRa is a new key technology developed in response to this.

Thanks to the chirp spreading spectrum technology, LoRa expands the node signal according to different spreading factors which are orthogonal to each other, which greatly improves the transmission distance and anti-interference ability. This paper verifies the long-distance transmission capability of LoRa under different SF parameters by using NS-3 simulation. Due to the large geographical and time span of the LoRa application, jammer interference may be another challenge. This article simulates the influence of jammers of different DCs on the LoRa network interference through NS3-, and analyzes the data of different numbers of jammers on the LoRa terminal under different DCs. The influence of the transmission success rate proves that LoRa has a strong anti-interference ability against jammers with lower DC. For super-strong jammer interference, we can resist by increasing the transmission power of terminal nodes and increasing the number of gateways. In addition, this article also investigates the effect of retransmission against jammer interference was simulated, and it was found that the first retransmission can effectively improve the data acceptance rate, but the effect of multiple transmissions above 4 times is not great.

This article simulates the impact of the jamming attack in the case of a single gateway. It is difficult for a single gateway to resist the rigid jamming attack. The combination of multiple gateways on the physical layer and the increase of the output power of the receiver to improve the anti-interference ability will be a method worth studying.

In short, LoRa technology provides IoT users with an efficient, independent, and cheap networking method, with strong anti-interference ability. Through the design optimization of the physical layer, MAC layer and application layer, the resistance to strong attacks by jammers will be further improved in the future.

Appendix

1. Oracle virtual box:
   https://www.virtualbox.org/wiki/Downloads

2. Ubuntu 20.04:
   https://releases.ubuntu.com/20.04/

3. NS-3 tutorial:
   https://www.nsnam.org/wiki/Installation

Bibliography

[1] W. Cao, N. Ma and P. Zhang, "Security analysis of DoS attack against the LTE-A system," *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, 2017, pp. 1287-1292, doi: 10.1109/CompComm.2017.8322750.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[3] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, Sept. 2016, doi: 10.1109/JPROC.2016.2558521.

[4] J. Henrydoss and T. Boult, "Critical security review and study of DDoS attacks on LTE mobile network," *2014 IEEE Asia Pacific Conference on Wireless and Mobile*, Bali, 2014, pp. 194-200, doi: 10.1109/APWiMob.2014.6920286.

[5] R. Ghannam, F. Sharevski and A. Chung, "User-targeted Denial-of-Service Attacks in LTE Mobile Networks," *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Limassol, 2018, pp. 1-8, doi: 10.1109/WiMOB.2018.8589140.

[6] D. Rupprecht, K. Kohls, T. Holz and C. Pöpper, "Breaking LTE on Layer Two," *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2019, pp. 1121-1136, doi: 10.1109/SP.2019.00006.

[7] T. Pushpalata and S. Y. Chaudhari, "Need of physical layer security in LTE: Analysis of vulnerabilities in LTE physical layer," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017.

[8] R. M. Rao, S. Ha, V. Marojevic, and J. H. Reed, "LTE PHY layer vulnerability analysis and testing using open-source SDR tools," *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, 2017.

[9] Liu, Y., Chen, H. and Wang, L., 2017. Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. *IEEE Communications Surveys & Tutorials*, 19(1), pp.347-376.

[10] C. Lipps, L. Strufe, S.M. Mallikarju, and H.D. Schotten, "Physical Layer Security for IIoT and CPPS: A Cellular-Network Security Approach," *German Research Center for Artificial Intelligence, Institute for Wireless Communication and Navigation, University of Kaiserslautern*, 2018.

[11] P. K. Panda, and S. Chattopadhyay, "An improved authentication and security scheme for LTE/LTE-A networks," *Journal of Ambient Intelligence and Humanized Computing*, 2019.

[12] A. Mukherjee, “Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints,” *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[13] D. Magrin, M. Centenaro, and L. Vangelista, “Performance evaluation of LoRa networks in a smart city scenario,” in 2017 IEEE International Conference on Communications (ICC). IEEE, may 2017.

[14] SEMTECH, “SX1272 LoRa Designer’s Guide,” Tech. Rep., 2013.

[15] I.Martinez, P.Tanguy and F.Nouvel, “On the performance evaluation of LoRaWAN under jamming”, 12th IFIP Wireless and Mobile Network Conference (WMNC), 2019