Technical Guidelines and Standards for IoT Network Deployment

(Phase 1: Preliminary Study)

Electrical and Mechanical Services Department

&

City University of Hong Kong

(August 2021)

Table of Contents

I. Purpose of the Project and Target Deliverables

This project is intended to provide technical guidelines to government departments, enterprises and contractors in deployment and utilization of LoRaWAN-based Government-Wide Internet of Things Network (GWIN) based on the illustration of case studies, evaluation of trial results and implementation of pilot testbeds.

The IEEE P2668 (IDex) is an international Internet-of-things (IoT) standard to evaluate the performance of IoT objects and deliver guidelines and regulations for IoT solutions. The compliance of the IEEE P2668 standard will proliferate the efficiency of deploying IoT objects and the future integration of various IoT objects. IEEE P2668 can be conveniently utilized to evaluate key services, to name a few, security ($IDex_{security}$), privacy ($IDex_{privacy}$), resiliency ($IDex_{resiliency}$), reliability ($IDex_{reliability}$), service ($IDex_{service}$),….etc. Based on IEEE P2668 standard, this document highlights GWIN infrastructure design, GWIN system deployment guidance, GWIN standardization design and industry best practices in implementation of smart applications.

To facilitate the blueprint of Hong Kong smart city, an optimal GWIN infrastructure with a redundancy design is suggested to deploy. As each application has its own characteristics and needs, companies are suggested to follow guidelines to implement smart applications on GWIN effectively and reliably.

To be specific, the technical guidelines involve:

a) Guideline on the selection of suitable IoT network technologies for specific sensor application;

b) Guideline on IoT network signal coverage planning, evaluation, simulation and optimization and evaluation criteria based the ATDI simulation tool;

c) International and industrial design standards related to IoT network and sensor deployment;

d) Network capacity planning and evaluation criteria;

e) Guideline on site survey methodology for gateway and sensor deployment;

f) Gateway and antenna deployment guidelines for different venues;

g) Sensor standardization, deployment strategy and evaluation criteria;

h) Guidelines for Acceptance Test Plan and Test Report for the end-to-end LPWAN infrastructure including network server, gateway, sensor deployment;

i) End-to-end Security measures and assessment criteria; and

j) Guideline on the workflow for IoT application deployment.

II. Project Descriptions

With the development of Internet of Things (IoT) technologies, it is projected that around 75.4 billion IoT devices will be in use all over the world by 2025 [1]. The massive network of billions of smart devices provides great convenience for our automated production and life. It has been applied in a variety of fields, including smart building, smart transportation, smart energy management, etc., which facilitates the construction of smart city.

Nowadays, Hong Kong government has launched smart city blueprint 2.0, which aims to build Hong Kong into a world-class smart city. To achieve this goal, HK Electrical and Mechanical Services Department (EMSD), as a pioneer, dedicates to establishing LoRaWAN-based GWIN to support various smart applications for the improvement of public service quality. To achieve the grant plan of GWIN, it is necessary to perform technical research, professional evaluation and pilot tests in advance to ensure the feasibility and reliability of entire network.

In this project, a series of technical guidelines for LoRaWAN-based GWIN based on illustration of case studies, evaluation of trial results and implementation of pilot testbeds are developed.

The technical guidelines are divided into three parts: network deployment, system standardization, and application implementation.

1) For the network deployment, guidelines of network planning, sensor deployment, gateway deployment, network server deployment, and interface coordination between GWIN and applications are provided. Based on above requirements, an optimal GWIN infrastructure with redundancy design is proposed. The system consists of five parties, IoT devices, gateway infrastructure, network server, Message Queuing Telemetry Transport (MQTT) broker and clients. The Things Network (TTN) enterprise LoRa Network Server (LNS) is selected for LoRa data processing. In particular, multiple LNS clusters with load balancer are suggested to improve the system security and reliability. To enable effective data exchange between clients' applications and LPWAN (i.e., LoRa, Sigfox, and NB-IoT), EMQ Enterprise MQTT broker is selected in GWIN. In the meanwhile, MQTT broker cluster is suggested to provide redundancy and effective management performance. Based on this infrastructure, smart applications could be implemented easily, effectively and reliably.

2) For the system standardization, general GWIN requirements and IEEE P2668 standards are defined. General GWIN requirements define compliances of GWIN utilization. IEEE P2668 standards define a performance evaluation methodology of three LPWAN technologies to facilitate the best practice of IoT applications. Besides, common security concerns in three-layer IoT framework (i.e., sensor layer, network layer, and application layer) are proposed in IEEE P2668 standard. To address these concerns, potential measurements to standardize the security in IoT system needs to be explored further. (which is out of this project's scope)

3) For application implementation, multiple pilot tests, including testbed of LoRWAN data logger for Water Supplies Department, Testbed of evaluation of personnel

tracking, testbed of multi-network harmonization, and testbed of LoRaWAN IoT message display system at China Ferry Terminal are implemented for reference.

The technical guidelines for LoRaWAN-based GWIN provide professional suggestions for government departments to deploy optimal network infrastructure, and technical assistance for enterprises to implement smart applications on GWIN effectively and reliably.

The organization of this report is as follows. The GWIN and LPWAN are introduced in Section III. The LoRaWAN-based GWIN infrastructure is proposed in Section IV. The GWIN system deployment guidelines, standardization guidelines are provided in Section V and Section VI respectively. The pilot tests implementation is elaborated in Section VII. Finally, the conclusion and way forward are given in Section VIII.

III. GWIN and LPWAN Introduction

Government-Wide IoT Network (GWIN) is a government network of wireless sensors installed throughout Hong Kong to support various smart applications to assist digitalization of Electrical and Mechanical (E&M) equipment and improve the public service quality. Through GWIN, it is possible for users to remote monitor asset efficiently, analyze operational data intelligently, and perform predictive maintenance and optimization.

In GWIN, sensors are connected through Low Power Wide Area Network (LPWAN). LPWAN is a type of wireless telecommunication wide area network designed to allow long-range communications at a low bit rate among connected devices [2]. There are three most popular LPWAN technologies: Long Range (LoRa), Sigfox, and Narrowband IoT (NB-IoT). LoRa is an open wireless standard that operates in below 1 GHz unlicensed band (920-925MHz in HK). LoRa technology utilizes chirp spread spectrum (CSS) modulation which expands the communication range. LoRaWAN is developed on LoRa modulation technique enabling long-distance communication link. In LoRaWAN, configuration flexibility of radio parameters (e.g., transmission power, bandwidth, data rate, etc.) is provided for developers to meet their own design requirements. Sigfox developed by a French enterprise also works on the unlicensed band (862-928 MHz in HK). Sigfox utilizes Ultra Narrow Band (UNB) modulation with 100Hz bandwidth enabling ultra-low noise level. In addition, lightweight protocol is adopted in Sigfox, which provides a cost-effective solution for short-message transmission in long distances. NB-IoT is a wireless technology based on cellular network proposed by 3GPP. NB-IoT utilizes single carrier-frequency division multiple access (SC- FDMA) modulation and orthogonal frequency-division multiplexing (OFDM) modulation for uplink and downlink transmission respectively. This enables large connectivity and reliable two-way communication. Compared with traditional wireless technologies (e.g., Wi-Fi, Bluetooth, ZigBee, etc.), LPWAN has advantages of 1) Low power consumption: several years' battery life; 2) Long range: a few kilometers in urban areas and over 7km in rural areas; 3) Low cost: communication modules for 50 HKD and even lesser.

Based on these LPWAN characteristics, GWIN is established as an efficient and private government IoT network. It provides a large-scale LoRaWAN architecture for users to deploy sensors with less complexity. In addition, it provides common data sharing platform for departments to supervise information together effectively. Furthermore, private network enabled in GWIN improves the security of the system and data without the need of using a third-party network.

The functionalities of GWIN are summarized as follows:

1) Support connections for LoRa devices

2) Provide connections of low powered IoT sensors (battery-powered)

3) Enable long range wireless transmission between sensors and gateways (~7km)

4) Suitable for lower data rate & less frequent data transmission application

5) Provide reliable and user-friendly IoT virtualization and management platform

6) Enable rapid and cost-effective implementation of applications

A variety of applications have been implemented in GWIN, including environmental monitoring, activity detection, E&M monitoring, smart metering, etc. For instance, smart sensors including temperature, humidity, and vibration sensors are deployed in EMSD Headquarters to provide operational data for lifts, escalators, photovaltic panels and chillers. Remote monitoring the status of these equipment, including fault alarm, remote diagnostics, and predictive maintenance are achieved in application server based on GWIN. Smart energy monitoring applications, including flood monitoring, smart flow metering, was implemented at underground environment. Sensors including ultrasonic water level, flow sensor could be swiftly and easily deployed. Flood monitoring and pipe leakage analysis are enabled in GWIN application server platform. At present, multiple participants including Drainage Services Department, Water Supplies Department, etc. have developed smart applications based on GWIN to improve management efficiency. To further facilitate the development of smart city, GWIN is seeking collaboration with more departments and enterprises.

IV. LoRaWAN-based GWIN Infrastructure

GWIN connects the IoT sensors cost effectively and facilitates the implementation of smart applications. Looking towards the working principle of GWIN, this section will introduce the core infrastructure of GWIN in detail.

GWIN is established on LoRaWAN structure, where applications using LoRaWAN protocol could be implemented. The common LoRaWAN structure (star topology) is shown as Fig. 1. In general, the basic LoRaWAN artichetecture consists of three parts, end devices, LoRaWAN gateways and network server [2]. Each end device communicates with multiple gateways within the coverage area through LoRaWAN. Messages from the end device are transmitted to gateways through single-hop link. Gateways aggregate and forward the messages to the network server via internet network. Smart applications could be implemented based on these data through Application Programming Interfaces (APIs) of network server. In particular, LoRaWAN architecture can be deployed both in public and private ways, which enables individuals and public organizations to offer service for their own purposes.

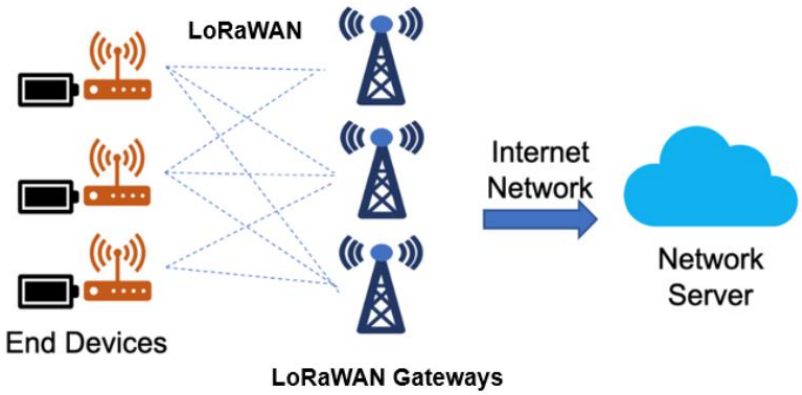


Fig. 1. LoRaWAN structure

The common LoRaWAN structure provides scheme about how to implement applications using LoRa protocol. However, it also poses some challenges. Multiple sensors using LoRa protocol may potentially not interoperate in some applications. In this case, the establishment of LoRa network and LoRa databases are needed, which leads to high complexity and huge cost of implementation. In addition, the deployment of a private LoRa network includes sensor deployment, LoRa gateway deployment and network server installation. The huge cost and great difficulty of LoRa gateway deployment and network server installation hinder the implementation of small LoRa applications.

To address these challenges, a cost-effective GWIN infrastructure based on LoRaWAN is proposed in this project. This infrastructure supports various applications using LoRaWAN protocol. Fig. 2 shows the proposed LoRaWAN-based GWIN infrastructure. The proposed system consists of five parties, IoT devices, gateway infrastructure, network server, Message Queuing Telemetry Transport (MQTT) broker and clients. In this system, large-scale gateways, network server and MQTT broker are included in

GWIN. In the gateway layer, LoRa private gateways are deployed by EMSD. In the network server layer, The Things Network (TTN) enterprise LoRa Network Server (LNS) and Chirpstack are suggested to be deployed in EMSD physical servers for data processing. In particular, multiple LNS clusters with load balancer are developed to improve the system security and reliability. (Note: The evaluation of different LNSs are given in Section V. C). To enable effective data exchange between clients' applications and LoRa network, EMQ Enterprise MQTT broker is suggested to be developed in GWIN. (Note: The evaluation of different MQTT brokers are given in Section V.E). In the meanwhile, MQTT broker cluster is designed to provide redundancy and effective management performance. Smart applications, including mobile app, application server, web app, etc. could be implemented as MQTT clients.

To be specific, the optimal deployment guidelines of the private LoRaWAN in GWIN are elaborated in the next section.

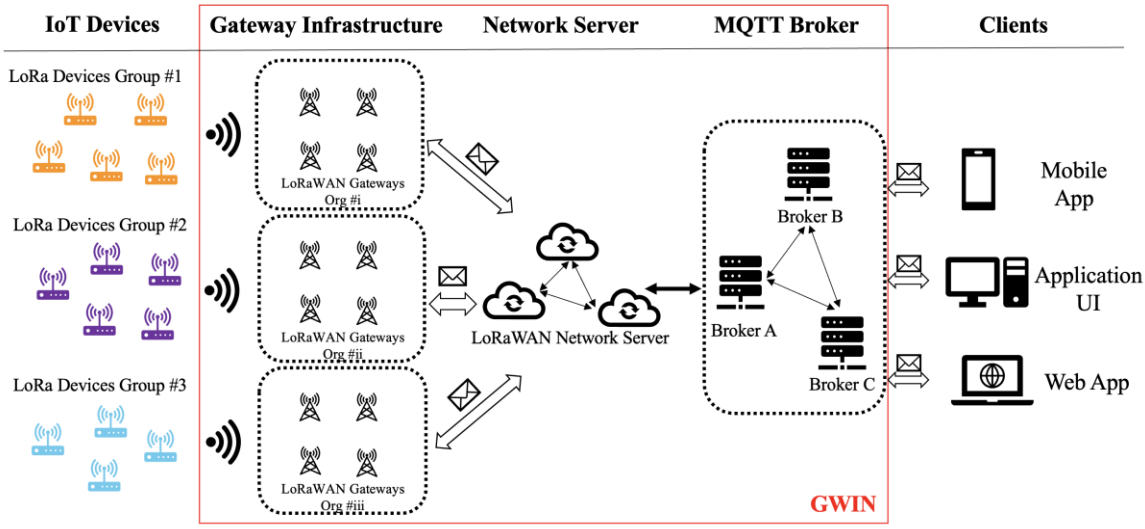


Fig. 2. The proposed LoRaWAN-based GWIN infrastructure

V. GWIN Deployment Guidelines

To facilitate the optimal GWIN infrastructure for private LoRaWAN, technical guidelines of network planning, sensor deployment, gateway deployment, network server deployment, and interface coordination between GWIN and applications are provided in this section.

A. LoRaWAN Network Planning Guidelines

LoRaWAN network planning is the most significant step before the practical GWIN deployment, which aims to obtain optimal network coverage in advance. Based on the simulation tool, ICS telecom from ATDI, the realistic radio environment could be simulated and the optimal network planning including the number of gateways, the gateway location, gateway radio configuration, could be developed. In this part, the guidelines of network planning based on ICS telecom tool are provided, and some case studies are given for references.

a. Simulation Tool Instructions

ICS telecom from ATDI is thought to be the most comprehensive radio planning solution [3]. It could be utilized in various methods, at all stages of a network's lifecycle. It could be used for network coverage planning before practical deployment of the network.

b. Coverage Simulation Instructions

(1) Project Configure

The first step is to configure the necessary files for the project when using ICS telecom. These configure files constitute a simulation project as a combination of multiple layers. The names and the file formats of these layers include (1) Vectors (.VEC), (2) Network element (.EWF), (3) Coverage (.FLD), (4) Map image (IMG + .PAL), (5) Clutter (SOL), (6) Buildings (.BLG), (7) Digital Elevation Model (.GEO). The basic function for each layer is described as follows [4].

i. Vector file (1) stores vector objects created by the user on a map.

ii. Network file (2) contains network elements, i.e. station type with associated coverage (if calculated and saved), path, and links.

iii. Coverage file (3) contains a coverage calculated.

iv. Map file (4) ensures proper display of the map for the area of interest.

v. Clutter file (5) contains Land Use / Land Cover definitions. It can be modified by the user as the clutter code of pixels can be changed.

vi. Building file (6) contains building footprints and height.

vii. Digital Elevation Model (7) contains the altitude model of the ground surface.

In general, layers (1), (4), (5), (6), (7) are settled default using files provided by ADTI official. Layer (2) is designed by the developer, and layer (3) is generated by the simulation tool based on settings.

(2) Signal coverage planning

(i) Selection of gateway location

The signal coverage planning mainly indicates the selection of proper gateway deployment sites. A coverage simulation before practical implementation could save the extra installation cost.

The choice of candidate gateway installation sites mainly depends on the availability in practice. On the one hand, these sites should be authorized for gateway installation. On the other hand, the gateways could be effectively monitored and protected (i.e., they will not suffer from external damage). Hence, it is better to explore the situation of the candidate installation sites firstly before simulation.

However, sometimes the simulation is done only to explore the possibility of coverage planning in the areas of interest. In this condition, there will be no previous practical exploration in advance. Hence, the developer could only select the candidate deployment sites based on other searching criteria. Firstly, it is still recommended to search the sites with authority and effective monitoring. In this view, public facilities administrated by the government could be preferential candidates. Except for that, the radiation performance of the gateway should be considered. For instance, the higher sites with an open view (e.g. building roof, etc.) could be preferred options because gateways could provide better signal coverage.

(ii) Configure the gateway parameters

After the determination of the installation sites, the other gateway parameters should also be decided. The key parameters of a gateway include the communication protocol (which type of network is being deployed), altitude, antenna height, Tx Gain, Rx Gain, Tx frequency, Rx frequency, Tx bandwidth, Rx bandwidth, nominal power, etc. In general, these parameters are decided based on the installation plan. Moreover, multiple values could be set for a specific parameter to compare the performance. For example, Tx/Rx gain could be allocated with different values to explore the coverage difference.

(3) Signal coverage simulation and optimization

After the signal coverage planning, the signal coverage simulation and optimization could be implemented. To obtain the signal coverage of all deployed gateways, the next step is to select the propagation model properly. ICS telecom has set a series of propagation models within the software. Based on the network type and other parameters settled previously, a proper propagation model could be decided. The detailed instructions could refer to the training document [5]. Except for the theoretical knowledge, the practical testing results could be an important reference.

The optimization can only be executed after complete the coverage simulation. It gives revision advice based on the current signal coverage and the desired objectives. If there has been an adequate or a redundant number of gateways on the map, the optimization will suggest closing some of them and propose the nominated sites for

gateway locations among the deployed ones. The detailed instructions could refer to the training document [6]. On the opposite, if the gateways are not enough to cover the whole area, the software may suggest keeping all gateways open. To further know how much blank is left, the coverage evaluation is needed, which will be introduced in the next section. Except for the gateway location, more optimizations could be done for antenna gain, antenna height, etc of a base station. The simulation tool will present configuration recommendations (i.e., antenna gain, etc.) among the candidate ones. The detailed instructions could refer to the training document [7].

(4) Signal coverage evaluation

The signal coverage evaluation indicates the coverage performance evaluation in the area of interest. In common, the performance is denoted by an indicator, namely coverage percentage (i.e., b%, b is the evaluated value between 0 and 100). This indicator realizes the percentage of the area covered by signals exceeds the threshold by one or multiple gateways simultaneously. The threshold could be determined based on the application requirement. To complete the evaluation, serval steps are required as follows.

(i) Bound the area of interest

Firstly, the developer should confirm the area of interest by clarifying the boundary. A common method is to refer to administrative areas proposed by the local government (e.g., 18 administrative areas in Hong Kong). Another solution is to manually design the boundary of the area of interest if there are other requirements. After that, the decided boundary should be drawn on the map of the simulation tool using polygon lines [8].

(ii) Implement the coverage simulation

The coverage simulation (and optimization if needed) is implemented following the designed networking deployment plan in this step. After that, the area of interest will be covered by various colors. The different colors represent the different coverage performances, which will be introduced as follows.

(iii) Execute the evaluation

As discussed, the evaluated coverage performance is denoted by the indicator, namely coverage percentage. Furthermore, indicators for 1-gateway-cover and N-gateways-cover are needed. In other words, the former is the coverage percentage by one gateway, while the latter is the overlap coverage percentage by multiple gateways (two in general). The end devices could normally operate when they are covered by one gateway. However, in practice, it is better to make the area covered by at least two gateways. This is to ensure signal stability. If one of the gateways breaks down, the end device could still work with the service from other gateways

(5) Signal coverage evaluation criteria

The signal coverage evaluation criteria mainly refer to the following aspects, i.e., implementation availability, cost optimization, network quality of service (QoS), coverage accuracy, etc.

The implementation availability indicates the possibility to implement network planning in practice as discussed in previous sections. The key point is to ensure the right for installation. Moreover, effective monitoring or protection should be available for installed gateways to prevent possible damage. Besides, the difficulty of installation

should be taken into consideration. For example, assuming that the gateway is installed on the rooftop of the building in simulation. However, in practice, it is found that the place is too narrow to install the gateway, or there is no power supply for the gateway. In this condition, the installation place should be adjusted accordingly and implement the simulation again.

The network QoS represents the network performance of the area of interest. The general objective of the network planning is to make most parts of important areas, particularly the region with a huge population such as urban, covered by the network generated by at least two gateways. Moreover, to ensure the QoS, the signal strength should be larger than the settled threshold (i.e., -110 dBm in general). This indicator could be checked by the mentioned signal coverage evaluation.

The cost optimization denotes the proper selection of gateway installation sites and optimization of station parameters. the number of deployed gateways could be minimized by selecting appropriate sites. Hence, the cost of gateway purchase and installation could be saved. Meanwhile, the network coverage performance is guaranteed. Besides, the most suitable values could be determined. This could be achieved by executing the optimization within the simulation tool.

The coverage accuracy could be further improved by revising the propagation model with test data if needed. The practically installed gateway should be configured with the same parameters as the simulated one (i.e., location, height, gain, etc.). Then, the signal strength measured in reality could be compared with that of the simulation. The difference between them could be decreased by adjusting the propagation model and parameter values [5].

c. Case Studies

(1) Overview

Multiple simulations have been done by the CityU team for EMSD in various regions of Hong Kong using ADTI ICS telecom. The names and abbreviations of simulation projects are as follows, namely Kowloon East (KLE), Shatin District (STD), Tai Po Pumping Station (TPP), Water Sports Center (WSC), City University of Hong Kong (CityU), Lantau Trail (LT), Water Supplies Department (WSD), Hiker Safety Project (HSP), Civil Engineering and Development Building (CEDD), Drainage Services Department (DSD), etc. Limited to the content, the case study in KLE will be described in detail while other ones will be briefly mentioned.

(2) Simulation for KLE

The objectives for this simulation are as follows.

a. Find the network coverage produced by deployed LoRaWAN gateways in the KLE area

b. Evaluate the network coverage to check if it meets the requirement of EMSD GWIN planning

Before the start of the simulation, the necessary configure files are given, as shown in Fig. 3

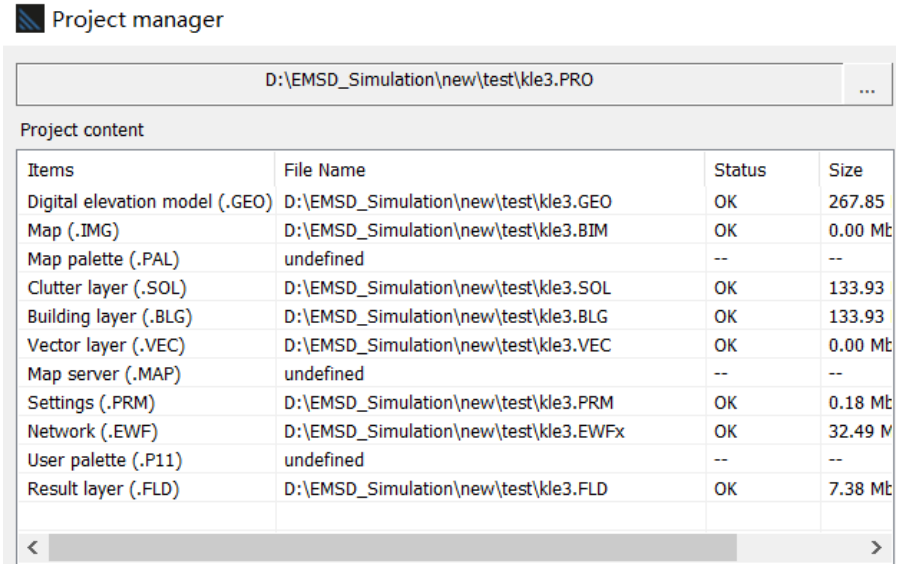


Fig. 3. The configure files for KLE simulation

Then, basic simulation parameters for LoRaWAN gateways are set as follows

Table 1. Basic simulation parameters (provided by EMSD)

Parameter	Altitude (m)	Antenna (m)	Tx Gain (dB)	Rx Gain (dB)	Tx Frequency (MHz)	Rx Frequency (MHz)	Tx BW (kHz)	Rx BW (kHz)	Nominal Power (W)
Value	2	2	3/6/9/10	3/6/9/10	923.2	923.2	125	125	1

Note: Other parameters setting (provided by EMSD)

a. 8 channels of LoRaWAN are allocated.

Tx: 923.2MHz, 923.4MHz, 923.6MHz, 923.8MHz, 924.0MHz, 924.2MHz, 924.4MHz, 924.6MHz.

Rx:923.2 MHz

b. Sensor receiving threshold is set as -110 dBm

c. The gateways are thought to be set on the top roof of buildings.

d. The overlapped order is set as 2 (for optimization use, it means that the objective is to make the area covered by two gateways simultaneously)

e. The Rx is thought to be deployed on the ground with a height of 2 meters.

f. The thresholds represented by different colors are shown in each figure and Table 2 as follows.

Table 2. The relationship between the color and the RSS threshold

Color	Deep blue	Mid blue	Shallow blue	Shallow green	Mid green	Deep green	Yellow	Blond	Red
Threshold (dBm)	-110	-100	-90	-80	-70	-60	-50	-40	-30

The following Table 3 illustrates the latest LoRaWAN gateway deployment sites with corresponding antenna gain.

Table 3. Full names, abbreviations, and LoRaWAN antenna gains of gateway deployment sites

Site No.	Full Name	Short Form	Antenna deployed
1	Zero Carbon Building	ZCB	6dBi
2	EKEO Office	EKEO	9dBi
3	Jordan Valley Park	JVP	6dBi
4	KAI TAK FIRE STATION	KTFS	9dBi
5	KLN BAY HEALTH CENTRE	KBHC	6dBi
6	KWUN TONG FIRE STATION	KWTFS	9dBi
7	KWUN TONG GOVT. PRIMARY SCHOOL (SAU MING RD.)	KTGPS	9dBi
8	KWUN TONG GOVT. SECONDARY SCHOOL	KTGSS	3dBi
9	LAM TIN AMBULANCE DEPOT	LTAD	9dBi
10	LAM TIN COMPLEX	LTC	9dBi
11	LAM TIN FIRE STATION	LTFS	9dBi
12	LAM TIN POLYCLINIC	LTP	9dBi
13	Morse Park No. 4	MPNo.4	3dBi
14	NGAU CHI WAN FIRE STATION	NCWFS	9dBi
15	NGAU TAU KOK JOCKEY CLUB CLINIC	NTKJCC	9dBi
16	Pong Kong Village Road Park	PKVRP	9dBi
17	PUBLIC WORKS CENTRAL LAB BLDG	PWCLB	9dBi
18	SHUN LEE FIRE STATION	SLFS	9dBi
19	TETRA BASE STATION (TBS) AT LOK SHUN HOUSE (TSZ WAN SHAN)	TBS	3dBi
20	Wong Tai Sin DSQ	WTSDSQ	9dBi
21	Wong Tai Sin Fire Station	WTSFS	9dBi
22	YUNG FUNG SHEE MEMORIAL CENTRE	YFSMC	9dBi
23	Lam Tin PTI	LTPTI	6dBi
24	Diamond Hill PTI	DHPTI	6dBi
25	KLE GOVERNMENT OFFICE	KLEGO	6dBi
26	EMSD HQs	EMSDHQS	9dBi
27	Kowloon Bay Sports Ground	KBSG	6dBi

The results are as follows.

The coverage percentage and coverage map are shown in Table 4 and Fig. 4.

Table 4. Coverage percentage in KLE (covered by one gateway only)

RSSI larger than…	-110 dBm	-100 dBm	-80 dBm	-60 dBm	-40 dBm
Coverage percentage (%)	99.96729	92.18138	39.62604	13.91097	0.91132

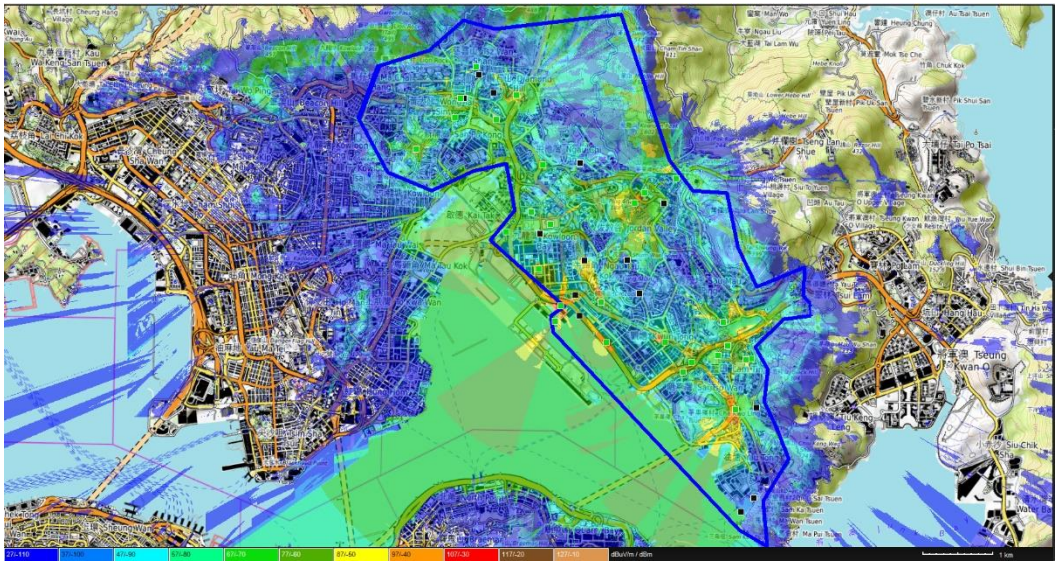


Fig. 4. Coverage map (baseline -110 dBm)

The various colors in Fig. 4 indicate various coverage threshold as mentioned in Table 4.

The overlap percentage (covered by two gateways concurrently) for covering areas is 97.43% and is shown in Fig. 5.

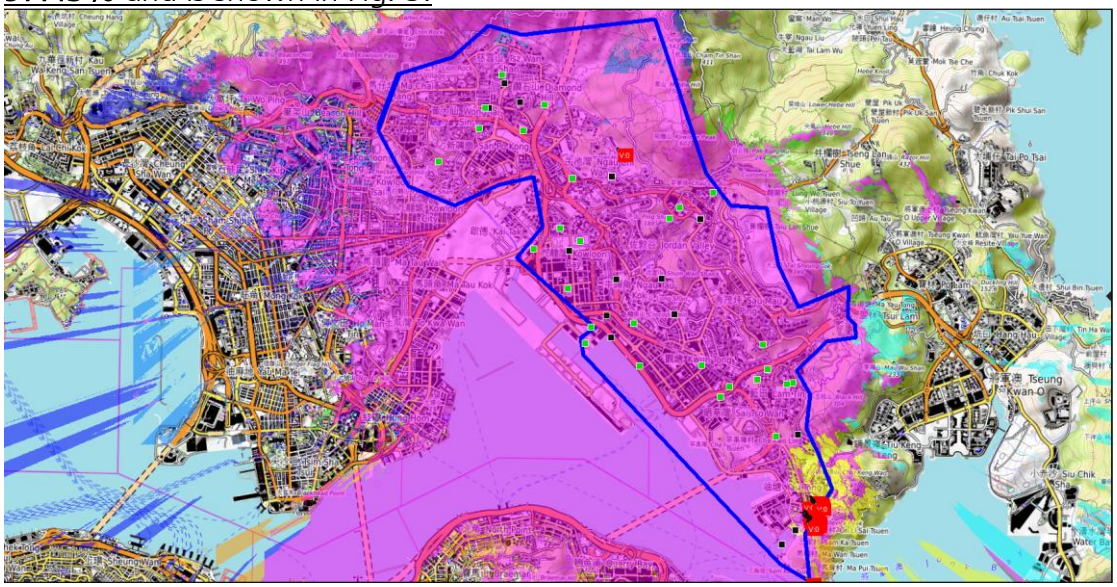
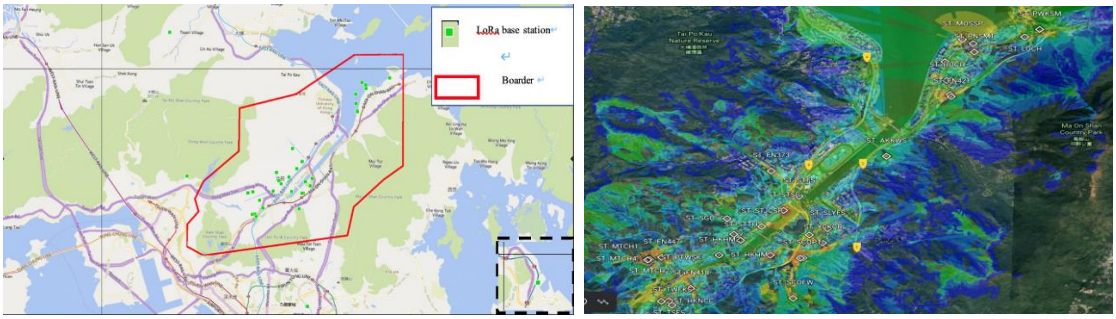


Fig. 5. Overlapped coverage map (baseline -110 dBm, represented by pink color), and uncovered area (represented by red and black color.)

(3) Other simulation cases

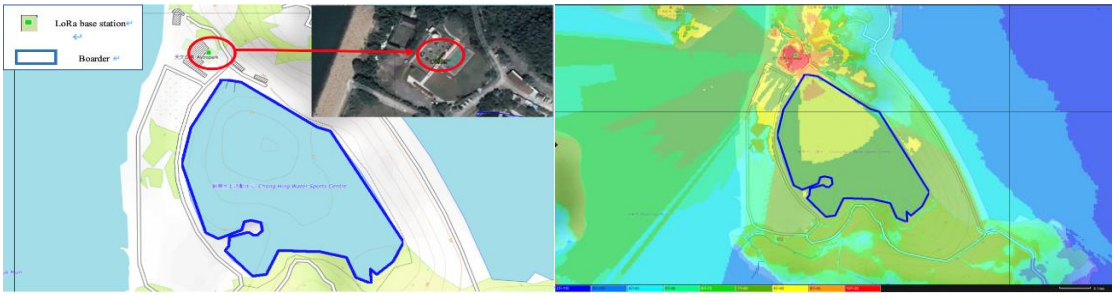
Other simulation cases are briefly introduced as follows.
In the following figures, the area surrounded by the blue borders is the desired one that needs IoT network coverage (which is drawn by the CityU team and decided by EMSD). The green points denote the place where LoRaWAN gateways plan to be deployed (basically provided by EMSD).
(1) Simulation in Shatin



(a) (b)

Fig. 6. (a) Simulation settings and (b) results in ST (marked by red bounder)

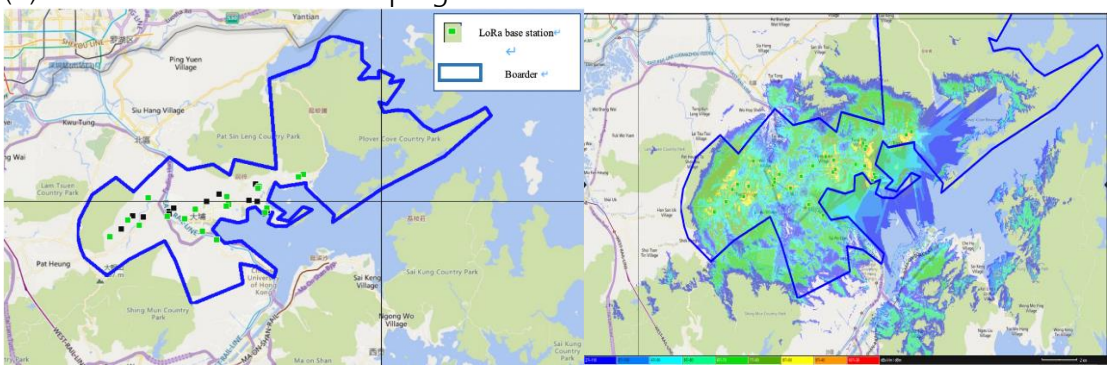
(2) Simulation in Water sports center



(a) (b)

Fig. 7. (a) Simulation settings and (b) results in WSC (Chong Hing Water Sports Centre for example) (marked by blue bounder)

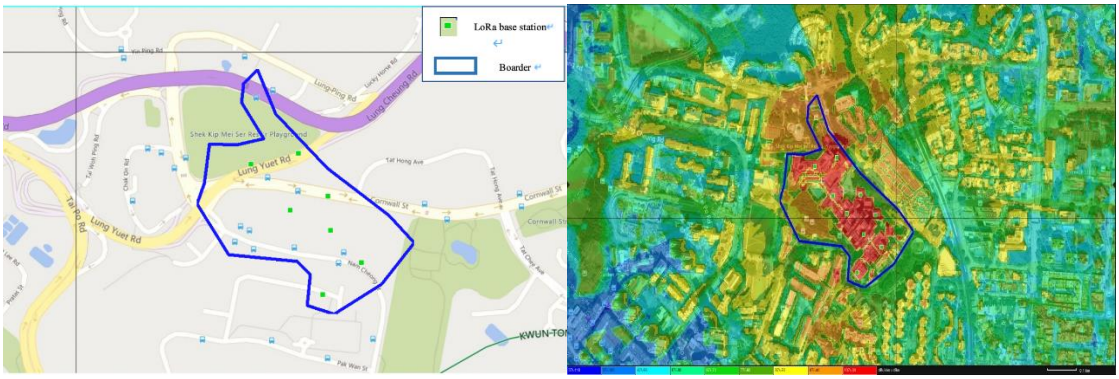
(3) Simulation in Tai Po Pumping Stations



(a) (b)

Fig. 8. (a) Simulation settings and (b) results in TPP (marked by blue bounder)

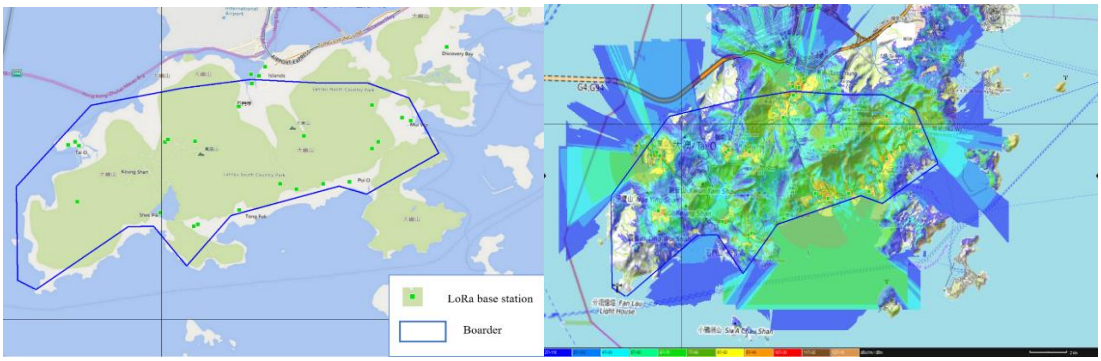
(4) Simulation in CityU



(a) (b)

Fig. 9. (a) Simulation settings and (b) results in CityU (marked by blue bounder)

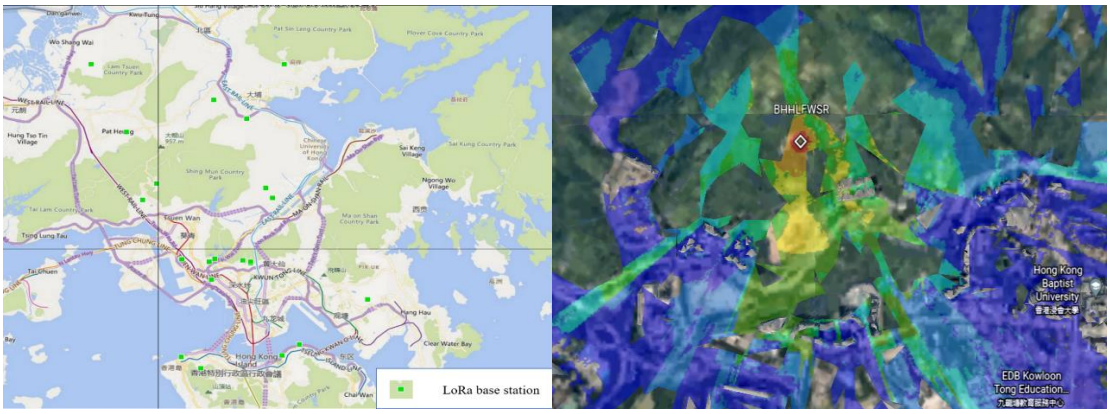
(5) Simulation in Lantau Trail



(a) (b)

Fig. 10. (a) Simulation settings and (b) results in LT (marked by blue bounder)

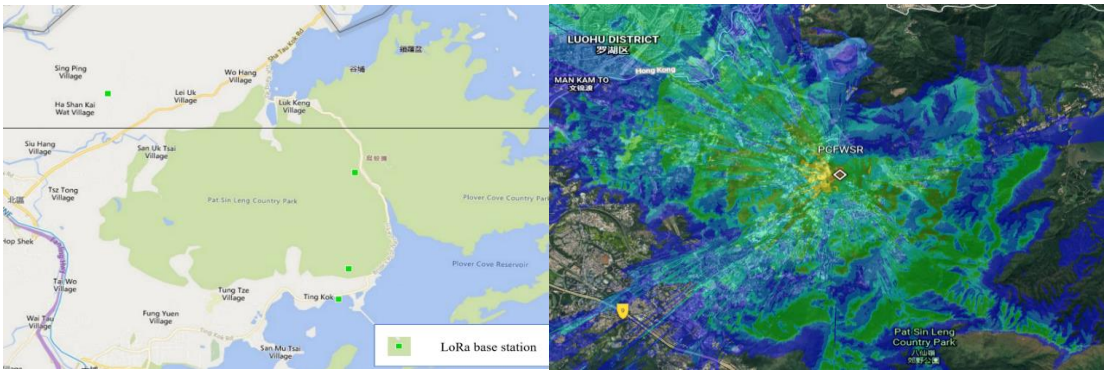
(6) Simulation in Water Supplies Department



(a) (b)

Fig. 11. (a) Simulation settings and (b) results in WSD

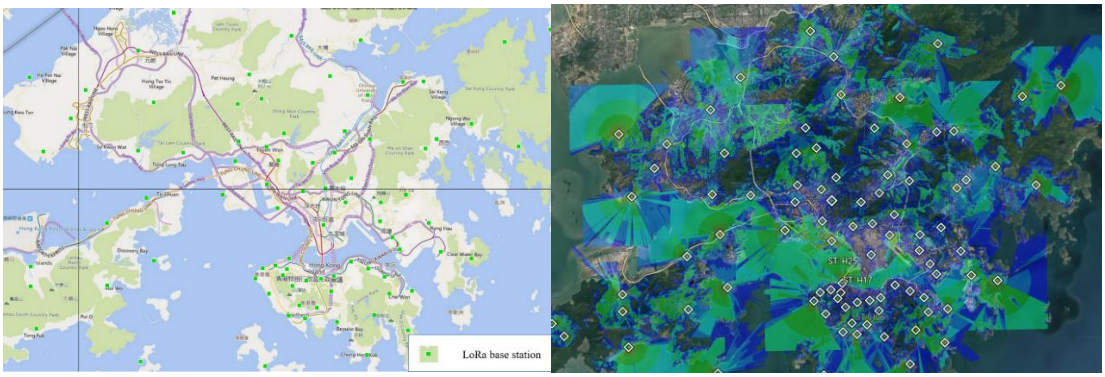
(7) Simulation in Hiker Safety Project



(a) (b)

Fig. 12. (a) Simulation settings and (b) results in HSP (some of the gateways for example)

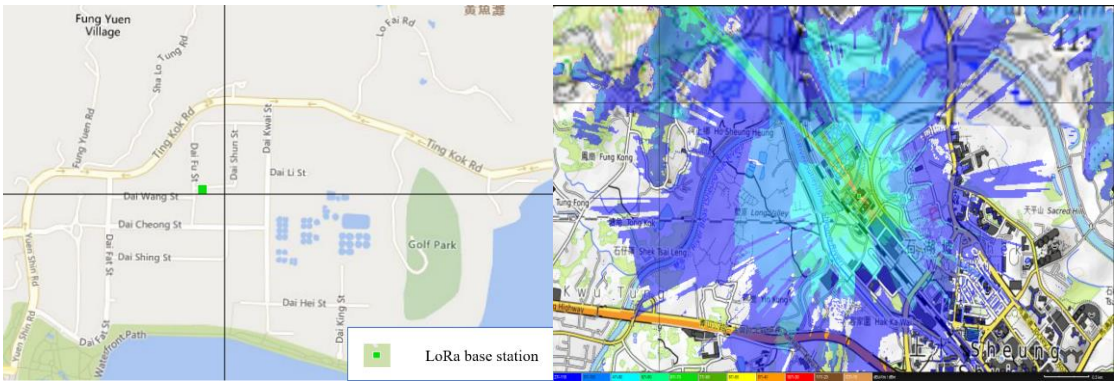
(8) Simulation in Civil Engineering and Development Building



(a) (b)

Fig. 13. (a) Simulation settings and (b) results in CEDD (some of the gateways for example)

(9) Simulation in Drainage Services Department



(a) (b)

Fig. 14. (a) Simulation settings and (b) results in DSD (one of the gateways for example)

B. LoRaWAN Gateway Deployment Guidelines

LoRa gateway is the core infrastructure in GWIN which serves to provide wireless signal coverage for the sensor devices installed on site. In general, applications have different signal coverage requirements and limitations of actual field deployment. Hence, after the simulation of network planning, site surveys are required to adjust gateway deployment plan and further determine the installation location of indoor and outdoor gateways. In this part, guidelines on site survey methodology for gateway deployment are provided, and the templates of site survey test plan and site acceptance test plan are given for reference.

a. Gateway Installation Methodology

1. General requirements for gateway installation

1.1 13A power socket/switched fused spur unit and power cables shall be ensured in correct position and in secure operating condition.

1.2 A waterproof cabinet (at IP66 better rating) shall be installed for each gateway with a mechanical lock and proper labeling.

1.3 Gateways shall comply with HKCA 1078 issue 1 dated December 2017.

1.3.1. Operating frequency should be in the frequency band 920-925 MHz;

1.3.2. The maximum allowed 20dB bandwidth of the hopping channel is 500 kHz;

1.3.3. The peak transmitter power shall not exceed 1W and the equivalent isotropically radiated power (EIRP) from the gateway shall not exceed 4W;

1.3.4. The spurious emission level shall not exceed 10μW (-20dBm) outside the

frequency band in which the fundamental frequencies are located.

1.4 4G LTE connectivity with public fixed IP address shall be enabled for each gateway, and the data rate shall not be less than 1 Mbps.

1.5 The LoRa signal strength of the gateway shall be measured both in the situations of Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS). The average measured LoRa signal strength shall meet the requirements of corresponding applications. The parameters for reference are: 1) Downlink RSSI $\geq$ -110dBm ($\pm$10dBm); 2) Downlink SNR $>$ -20dB; 3) Uplink RSSI $\geq$ -110dBm ($\pm$10dBm); 4) Uplink SNR $>$ -10dB; 4) DR is between DR0 to DR5.

1.6 Gateway shall enable Secure Shell (SSH) tunnel for firmware configuration and remote monitoring.

2. Extra requirements for outdoor gateways

2.1 For better outdoor coverage, the location of outdoor gateway is preferred to be at high location. (i.e. building rooftop). There are two typical installation locations for outdoor gateways.

2.1.1. Metal enclosure housing gateway and associated accessories (approximate 400mm W x 500mm L x 200mm D) being wall-mounted inside plant room area while the outdoor antenna (approximately 1000mm L) to be extended for mounting at outdoor locations using coaxial cables with cable distance not exceeding 10m.

2.1.2. Metal enclosure and outdoor antenna being wall-mounted at building rooftop.

2.2 The metal enclosure shall be located to accessible location for maintenance. The mounting details of the equipment for each mounting scenarios shall be certified by the Registered Structural Engineer (RSE). A protective conductor shall be provided for the metal enclosure.

2.3 220V 13A single phase fuse spur unit shall be provided by the project main contractor for each outdoor gateway locations

2.4 Lightning protection shall be provided by the project main contractor for the outdoor gateway and antenna.

2.5 Landline shall be provided by the project main contractor for each gateway location if a mobile network by local telecommunication company is not available.

3. Extra requirements for indoor gateways

3.1 For better indoor coverage, the location of indoor gateway is preferred to be at open area with less obstacles.

b. Gateway Site Survey Test Plan

In general, site survey would be required to determine the optimized locations of indoor

and outdoor gateways to serve the target sensor applications. The site test procedure is shown in Fig. 15.

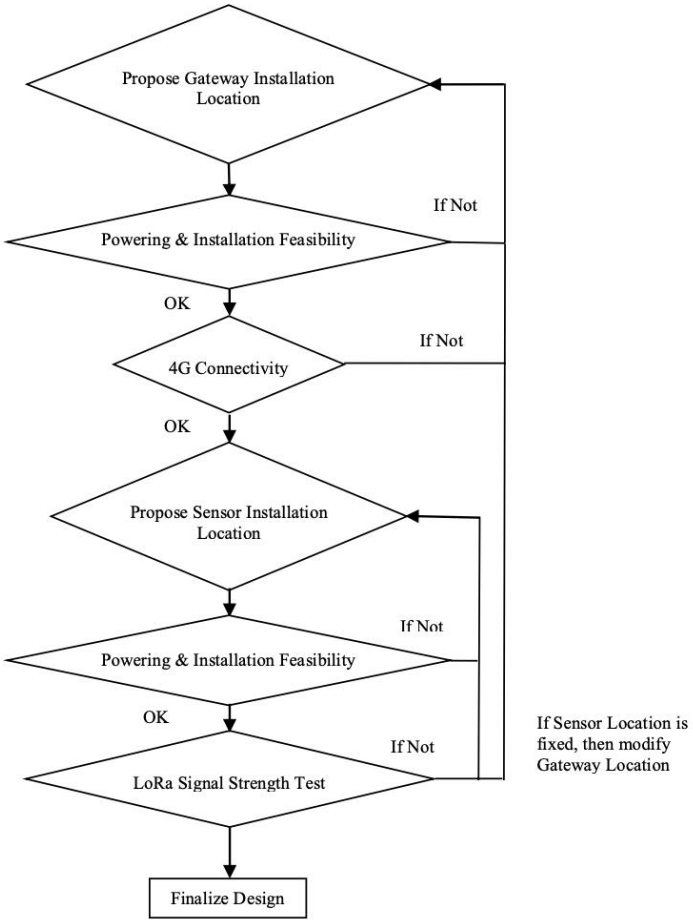


Fig. 15. Site survey test procedure

A sample of Site Survey Test Plan of Gateway is shown in Appendix 1.

c. Gateway Acceptance Plan

The gateway acceptance plan shall include the following contents:

1. Introduction
2. Cable Test & Commissioning
   - 2.1 Cable Testing: Power Cable
3. Field Equipment Test & Commissioning
   - 3.1 Visual Inspection
   - 3.2 Gateway Test & Commissioning
     - 3.2.1 Test Purpose

3.2.2 Tester

3.2.3 Test Procedure

3.2.3.1 Isolate the gateway and field tester in separate LNS during SAT

3.2.3.2 Check the health status of the gateway on indicator light

3.2.3.3 Check and Record the 4G connectivity

3.2.3.4 Check the configuration of gateway and gateway firmware by using putty

3.2.3.5 Verify and Record the performance of gateway complied with HKCA 1078 issue 1 dated December 2017 by using spectrum analyzer (Frequency band, Transmission power, EIRP, spurious emission level)

3.2.3.6 Check Antenna parameters (Type, Length, Gain, Return loss, VWSR, Connector)

3.2.3.7 Check the RF cable parameters (Length, Impedance, Cable Loss)

3.2.3.8 Field Test

3.2.3.8.1 Record the Tx power, SF, SNR, RSSI, Data rate, PLR both in Uplink and Downlink from field tester and LNS

3.2.3.8.2 Test with different antenna heights and directions (1 test point: below the antenna, at least 5 test point: 10m away from the antenna)

3.2.3.8.3 Test with fixed antenna

3.2.3.8.3.1 For outdoor gateway: LOS (16 test points: 1m, 10m, 100m, 200m, 500m, 1000m); NLOS (16 test points: one wall, a curve as references)

3.2.3.8.3.2 For indoor gateway: (20 test points: below the antenna, same floor of gateway location, adjacent floors of gateway location)

3.2.4 Expected Results

3.2.5 Test Record

The sample of Site Acceptance Test Plan of Gateway is shown in Appendix 2.

C. LoRaWAN Network Server Deployment Guidelines

LoRaWAN Network Server (LNS) is the critical part of GWIN which enables connectivity, management, and monitoring of devices, gateways and applications. LNS consists of

several functional components, gateway server, network server, application server, join server, and identity server, which aims to provide LoRa data routing and processing with high security, scalability, and reliability. At present, a variety of enterprises develop different LNS solutions. To select the most appropriate LNS for GWIN, it is necessary to evaluate the performances of these LNSs.

a. LNS Evaluation Methodology and Criteria

In this part, the most common LNSs are evaluated, including TTN Enterprise LNS, Orbiwise LNS, LORIOT, Actility, Tektelic LNS, and Trackcentral. To provide the most appropriate LNS for GWIN, the evaluation is performed from following aspects:

- LNS Technical Features
- Packet Forwarder Supporting
- Redundancy Design
- Management Supporting Services

1. LNS Technical Features:

(1) Basic Information of LNS: LNS Platform Name, Country of Origin, Type of Platform Delivery, Location of Hosting Server, Extra Function Server Platform and On-Premise Option, Service Logistics

(2) LoRaWAN and Internet Protocol Compliance: LoRaWAN Protocol Version, LoRaWAN Regional Parameters Version, Security Version and Internet Transmission Protocol

(3) Main Technical Features: Network Management Services, Channels Management, Gateway Management, Extra Gateway Scripts/Software, Device/End Node Management, User Application Interface Management, Access Control, VPN Feature

2. Packet Forwarder (PF) Supporting: Packet forwarder in LoRa gateways is applied to create connection(s) between LNS and LoRa gateway. LNS platforms may support three kinds of PF protocols, which are Semtech Pure UDP PF [9], Semtech LoRa Basics Station PF [10] and Platform-Defined PF.

(1) Semtech Pure UDP PF: This kind of PF is the most common used and embedded PF in different LoRa gateway models. Based on UDP connection, users could configure LoRa gateway to LNS for serving LoRa end devices. However, UDP based transmission protocol is mainly designed for video/big package-based services, which is unreliable services. This means that connections between LoRa gateway and LNS using UDP PF may lose packets from gateway-keepalive message or end device message. For IoT network service provider, this is a crucial problem that network users may be challenged by the low Quality of Services (QoS).

(2) Semtech LoRa Basics Station PF: Basics Station PF is a new generation PF published by Semtech, which is based on Websocket and HTTP with TLS. Compared to UDP

PF, the Basics Station PF occupy addressed advatages [10]:

- TLS and Token-based Authentication: Improve security level of connections between LoRa gateway and LNS
- Centralized Channel-Plan Management: Gateway deployment is no need to consider channel configuration in LoRa gateway but the specific channel plan is centralized managed by LNS.
- Easily Portable to Linux-based Gateways and Embedded Systems: Because Basics Station PF is developed by Semtech, most of the LoRa gateways could be embedded with this new PF quickly.
- Other advantages could be reference from [10].

(3) Platform-Defined PF: Some LNS platforms provide their own-designed PF on specific gateway models using extra installation scripts or software. The security level and deployment cost are acceptable. However, when new type of LoRa gateway is going to be deployed in the future, it will be a challenging work for both gateway provider and LNS platform provider because of extra development work.

As above, Semtech LoRa Basics Station PF should be considered as the highest priority because of its homogeneous, secure and easy-portable properties. Then, Platform-Defined PF is considered as the second Priority, but this kind of PF may limit the scalability of GWIN network. Semtech Pure PF should not be considered in such network considering on the security and reliability issues.

3. Redundancy Design: Redundancy design for LNS improves the single point of failure issue and provides load balancer to LNSs network.

(1) Single Point of Failure: It is assumed that there is only one LNS in LoRa network. When this server encounters running error/attack/other system errors, all of the gateways and end devices in the system could not receive services from server. In other words, single point of failure will cause damage to the LoRa network. Deploying multiple LNS clusters could efficiently improve this problem.

(2) Load Balancer: This technology aims to balance the input data flow to LNS clusters.

4. Management Supporting Services:

(1) Management Log Files:

- LNS Runtime Log: This kind of log file is applied to record packet flow and running flow of LNS, which is necessary services for management, maintenance and development.
- Log-in Events Log: This kind of log file is applied to record log-in/operation events of user/manager/administrator.

(2) LNS Maintenance

(3) Offline Resources/Online Resources/Debugging and Trouble Shooting/Service Level/Development and Future Expansion/System Support Services

b. The performance evaluation of different LNSs

Based on the above evaluation criteria, the evaluation was performed based on LoRaWAN function trails and LNS operational trails. The features of different LNSs are presented as follows:

1. TTN

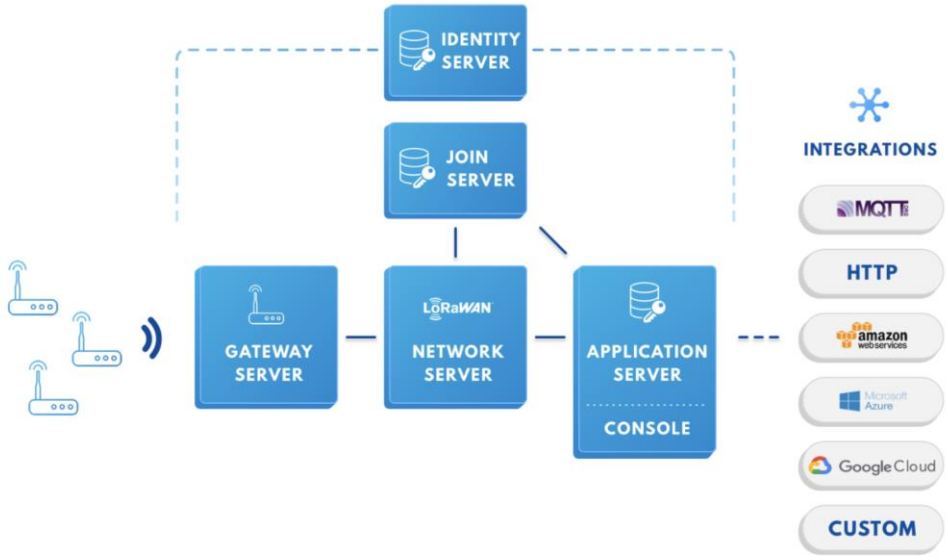


Fig. 16. TTN Network Structure

Table 5. Basic Information of TTN Platform

Server Information	Records
LNS Platform Name	The Things Network LoRaWAN Network Server (TTN)
Country of Origin	Denmark
Type of Platform Delivery	SaaS, Cloud-based
Location of Hosting Server	Hong Kong
Extra Function Server Platform	No Need (System has already embedded all the platform)
On-Premise Option	Support

Table 6. LoRaWAN and Internet Protocol Compliance of TTN Platform

LoRaWAN Protocol Version	LoRaWAN Protocol V1.0.x, V1.1 LoRaWAN Regional Parameters V1.0.x, V1.1
Security Policy	HTTPS, TLS1.2, HSM, AES, SSH
Internet Transmission Protocol	HTTP, HTTPS, MQTT, Websocket, Webhook

Table 7. Detailed Features of TTN Platform

Services	Negative/Positive	Remarks
LoRaWAN Network Management	TTN provides web services to manage networks (end devices, gateways, applications, etc.)	1. Clear UI Design 2. TTN directly apply gateway configuration in LNS to represent network, which is easy-to be understood.
Channels Management	TTN provides all the channels plan according to the LoRaWAN standard.	AS923.2-924.6 for Hong Kong
Gateway Management	Web services for managing gateways	Gateway Supported List: **Most of the LoRaWAN Gateway Models** 1. In Gateways Tab, it is efficient to register a LoRaWAN gateway with **Semtech Packet Forwarder**. This means TTN platform could support most of gateway types in the market with standardized LoRaWAN protocol. In addition, TTN server support **LoRa Basics Station PF** well. 2. The gateway management UI is simple to be understood for users. 3. Gateway Positioning Map 4. Support most of the channel plans and users could easily revise the channel plan of specific

		LoRa gateway.
Extra Gateway Scripts/Software	Standalone without requiring extra gateway scripts/software	1. Standard Semtech Pure UDP Packet Forwarder 2. Standard Semtech LoRa Basics Station PF 3. TTN PF (Not Recommended by TTI official) 4. No need other scripts
Device/End Node Management	Web services for managing devices or end nodes.	1. OTAA/ABP 2. Support Bulk Import 3. Class A, B and C 4. Device Positioning Map 5. TTN combines the device management functions and services into applications. (Need to define applications first) 6. No Statistic Records 7. TTN platform could define uplink and downlink payload formatters for better development of users' application
Users Application Interface Management	Web services for managing devices or end nodes.	Web UI Data Push Account Management Restful API, Websocket & MQTT
Access Control	Managed by web services (Administrator of TTN can manage the permissions of different customers or users.)	Method: 1. According to the account level to authorize different management access to different users 2. TTN should provide more resources on how to manage the permission of different customers or users.
VPN	Installed in the carrier operating system of TTN	OPENVPN (IPSec)

Table 8. Management Services of TTN Platform

Services	Negative/Positive	Remarks
LNS Runtime Log	Real-time monitoring by web services (gateway	1. TTN platform applies events concept to monitor the gateway

	logs, application logs, end device logs)	logs and users could easily find the all activities of each LoRaWAN gateway. 2. End devices activity monitoring is similar to gateway logs record. 3. History log of radio tracing is lack.
Log-in Events Log	Monitoring by backup services	Functions Provided in Join and Identity Server. In addition, this kind of log could be collected from server backup running logs.
Development Programming Language	Decided by the developers	Javascript, etc. (Decided by developers)
LNS Maintenance: Depend on contract between TTI and EMSD		
Offline Resources: 1. TTN platform mainly provides user manuals and system structure files to introduce their platform. 2. The offline and online resources are enough.		
Online Resources: 1. Manuals: Very good organization on online document from TTN official website. TTN not only introduce the methods to use their platform but also provide enough knowledge about LoRaWAN technology and network resources (Google, Baidu and etc.) to help users to solve the development problem. 2. Papers: From TTN LoRaWAN Official Website: https://www.thethingsnetwork.org/docs/ Source codes/configuration templates: For TTN Official Website (It is better for EMSD and TTN to arrange a training course for TTN platform.)		
Debugging and Trouble Shooting: 1. Contact TTN by Email or On-Site Discussion at Hong Kong 2. Log files feature could be added before deploying the TTN server.		
Service Level: Guarantee on Uptime, Downtime (LNS Reliability, N-Nine Level): 2 or 3 Nine availability (Suggest 99.9% Uptime)		
Development and Future Expansion: Depend on TTI (This should be considered in future contract.) 1. History log monitoring 2. Data exchanging with other network server platform		
Man-Power Arrangement: Depend on TTN and EMSD		
System Support Services: 1. Team Support: Yes 2. Location of Support Team: Hong Kong 3. Remote Support or On-site Support: Both 4. Development Support: Yes 5. Charging Model: 20000 HKd (To be confirmed by TTN and EMSD)		

Table 9. Mandatory and Other Features of TTN Platform

Mandatory Features: Migration of Gateways and Sensors: Good (TTN can transfer gateways into other platforms. If the destination platform could support standard LoRaWAN packet forwarder and basics station PF, the migration process could be finished efficiently.) Failover Configuration: To be confirmed by TTN Support Team Gateway Position on Map: Yes Provision of Infrastructure Summary in One Click: The platform logistics is clear and concise. With one click, users could find their desired information efficiently. Dashboard Generation: Yes (1. Gateways Dashboard and Applications Dashboard 2. Management Dashboard could be found under applications management dashboard)	Other Features: 1. Redundancy Design: According to TTI resources, TTN LNS could form clustering network to deal with single point of failure issue and embed with load balancer to balance traffic to different TTN LNS clustering. The cluster deployment is based on docker property, which is a lightweight and efficient technology. 2. Support true carrier-grade multi-tenancy with centralized gateway management. 3. Support a massive, open, vendor-maintained device repository/database with each of the device profiles 4. Support fast-track device provisioning, skipping manual handover of keys, and enable automatic skip-steps in the provisioning process 5. Support Sustainable innovation 6. Support peering exchange to enable 3rd party Lora networks to exchange traffics among them 7. Support FUOTA (Firmware Update Over The Air) for device updates to improve the device performance, fix device bugs, increase device product life cycle and security continuously (Need to deploy specific End device to support

	this function) 8. LoRa device geolocation (Need gateway support stable GPS signal)

- Application management and Device Management in TTN: Users could create their own applications in Application tab. For each application, the end LoRa devices could be added into. From the end device management Web UI, users could design their own payload format to parse the uplink and downlink message, which is a flexible way to monitor data flow with Javascript, GPRC service and etc. In order to build connection with users' application server, the integrations in application management tab could provide MQTT and HTTP methods to do it. In addition, the TTN server could be regarded as a MQTT broker to exchange messages for different applications. There is a scenario that multiple users may share the data from common application and the Collaborators management for each application could provide an efficient method.

- Gateway Management: There is no network concept in TTN platform. Users need to configure the gateways to TTN platform through general UDP PF or basics station protocol. If the basics station protocol is applied, the TTN platform could automatically distribute the frequency channel plan to the gateway. In other words, TTN platform is flexible on changing the frequency plan for users' gateways.

- Client Management: TTN platform provide the function for different users to create their own accounts. The administration account could manage these registered accounts too. Under the private account, users could configure their own gateway and create the applications to form private LoRa network. Hence, the client accounts in TTN is isolated to each other. For the administrator, it can absolutely manage these client accounts on gateway management, application management, access control, client collaboration and etc.

- Trouble shoot: Because TTN service is provided in Hong Kong vendor, the trouble shoot services could be provided on-site. In addition, TTN official website has already published much resource on TTN platform. Considering on the privacy issue, EMSD needs to deploy the LNS platforms in its own data center and the management is inefficient if there is only online support and trouble shoot service.

- Log Support: The instant log is shown in the applications and gateway management UI.

- MQTT Connection: It is not recommended to configure the TTN platform as MQTT broker, since the single point of failure problem may cause to damage on both

MQTT broker and LNS. Hence, in this part, it mainly discusses the MQTT client/publisher of TTN platform. The MQTT integration is embedded in the Application/Integration shown in the UI. It supports MQTT with TLS. However, the MQTT publisher in TTN platform only supports single application data stream publishing. In other words, it is difficult to integrate all the data stream from different applications into single publishing topic.

- Security Level: The security mechanism or standardization should be provided by the platform providers. On-site server deployment of different platform should be recommended by the platform provider too. (Why can the security of the platform be ensured? Any methodologies, standardization or common method?)

2. Orbiwise

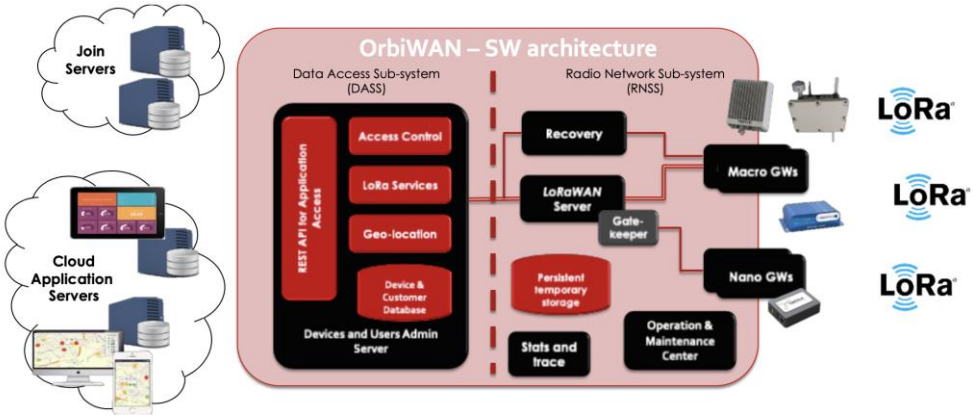


Fig. 17. Orbiwise Network Structure

Table 10. Basic Information of Orbiwise

Server Information	Records
LNS Platform Name	ORBIWAN (Orbiwise)
Country of Origin	Switzerland
Type of Platform Delivery	SaaS, Cloud-based
Location of Hosting Server	Hong Kong
Extra Function Server Platform	None
On-Premise Option	Support

Table 11. LoRaWAN and Internet Protocol Compliance of Orbiwise Platform

LoRaWAN Protocol Version	LoRaWAN Protocol V1.0.x LoRaWAN Regional Parameters V1.0.x (Optional: v1.1)
Security Policy	HTTPS, TLS1.2, HSM, AES, SSH
Internet Transmission Protocol	HTTP, HTTPS, Websocket, MQTT

Table 12. Detailed Features of Orbiwise Platform

Services	Negative/Positive	Remarks
LoRaWAN Network Management	Orbiwise provide two isolated webs to manage the networks.	Network Concept is not very clear in this platform. This LNS service logistics are constructed by Device Management, Gateway Management and Application Management.
Channels Management	The channels management is decided and designed by the customer in the web services.	AS923.2-924.6 for Hong Kong
Gateway Management	Web services for managing gateways	Gateway Supported List: Kerlink (OK) MultiTech (OK) Tektelic (OK) The registration of gateway includes unblocking gateways and configure gateways RF parameters. The registration procedures are disorder. Users need to finish the registration with switching between NST and DASS. But these steps could be accepted if the resources are enough. However, these steps could improve the security level of LNS.
Extra Gateway Scripts/Software	Extra gateway scripts/software is needed to be installed. (Provided by Orbiwise)	1. Support Standard Semtech Pure UDP Packet Forwarder 2. The firmware installation guide does not describe need to fallow gateway's vendor setup

		guide to config network 3. Basics Station protocol supporting is not clear. 4. Firmware installer does not provide auto-config mobile network 5. The extra installation image on gateway may cause extra security issues. Need Orbiwise provide more information on the installation.
Device/End Node Management	Web services for managing devices or end nodes.	1. OTAA/ABP 2. Batch Registration 3. Class A, B and C 4. Device Positioning Map 5. Device registration UI is informative.
Users Application Interface Management	Web services for managing devices or end nodes.	Web UI Data Push Account Management Restful API, Websocket & MQTT
Access Control	Managed by web services (Administrator of Orbiwise can manage the permissions of different customers or users.)	Method: 1. Multiple Level user access control 2. Switches on functions for multiple level user
VPN	Installed in the carrier operating system of Orbiwise	Support OpenVPN

Table 13. Management Services of Orbiwise Platform

Services	Negative/Positive	Remarks
LNS Runtime Log	Detailed runtime and history log records in the web.	1. Gateway Alarm 2. Data Traces (Detailed message classification) 3. Log File Export and download to local
Log-in Events Log	Monitoring by backup services	Didn't find any records or logging logs for multiple level user.
Development	Decided by the	Javascript, node.js, etc. (Decided by developers)

Programming Language	developers	
LNS Maintenance: Depend on contract between Orbiwise and EMSD		
Offline Resources: 1. Orbiwises have provided enough user manuals, papers and feature or technical details on configuring, using and practicing. 2. For the MQTT interface, Orbiwise should provide more documents on it. 3. Gateway extra installation software should be introduced with technical details (Service port, service framework, etc.)		
Online Resources: 1. Orbiwise provides detailed training course on how to use the LNS. 2. Manuals: Didn't find any manuals from LNS and official website. 3. Papers: A brief introduction on features in the official website (No detailed introduction) Source codes/configuration templates: Didn't find any resources about this but only introduced in online training course.		
Debugging and Trouble Shooting: 1. Contact Orbiwise by Email and Online Meeting		
Service Level: Guarantee on Uptime, Downtime (LNS Reliability, N-Nine Level): 2 or 3 Nine availability (To be confirmed by EMSD and Orbiwise Contract)		
Development and Future Expansion: Suggest to improve the logistic and gateway installation complexity to support more gateway models		
Man-Power Arrangement: Depend on Orbiwise and EMSD		
System Support Services: 6. Team Support: Yes 7. Location of Support Team: Non-Local 8. Remote Support or On-site Support: Remote Support 9. Development Support: Yes 10. Charging Model: 48000 HKd		

Table 14. Mandatory and Other Features of Orbiwise Platform

Mandatory Features: Migration of Gateways and Sensors: Not Absolutely (1. Revise Gateway Tags to migrate gateways 2.Revise Device group to migrate end devices But their extra scripts/software installation in gateway may finally influence the migration.) Failover Configuration: To be confirmed Orbiwise Team Gateway Position on Map: Yes	Other Features: 1. Redundancy Design: Full Horizontal scaling of solution by live addition of extra server hardware, Scalable Cassandra Database for state and data storage 2. LoRa Geo-Localization with LoRa Localization Capable Gateways (V2 Gateways) 3. Management of device QoS

Provision of Infrastructure Summary in One Click: No Dashboard Generation: Yes (1. Gateway Management Dashboard 2. Channels Management Dashboard)	based on QoS class or QoS profiles for balanced radio resource and billing purposes 4. Improved multicast downlink scheduling, optimizing gateway usage and minimizing usage of downlink capacity 5. Network security between gateway and network server is based on Orbiwise own packet forwarder.

- Application management and Device Management in Orbiwise: The devices management and applications management are isolated in Orbiwise DASS. The devices management function aims to import and register devices into the constructed network. The main function of the applications management is defining the data flow from different end devices to different application server. As tested, the Orbiwise platform could also support MQTT connection. Because there are too many sub-window UI design, users need to cost much time on finding out the desired configurations in Orbiwsie platform.

- Gateway Management: The main gateway management services are distributed in DASS and NST. In order to configure the gateway into Orbiwise platform, it is necessary to install the Orbiwise-Developed firmware into the gateway which is much different from TTN or Chirpstack. Then, the firmware-installed gateway should be configured as passed in NST. This process improves the security level of the network but also limits the supported kinds of gateway models. In addition, the main function of Gateways management TAB in DASS is not clear in managing the network.

- Client Management: In Orbiwise DASS, the administration accounts could add new user account. However, the more detail account rights management service is provided in NST platform.

- Trouble shoot: The main trouble shoot services of Orbiwise are through online contact. There is insufficient online resource to help on trouble shooting provided at Orbiwsie official website. Considering on the privacy issue, EMSD needs to deploy the LNS platforms in its own data center and the management is inefficient if there is only online support and trouble shoot service.

- Log Support: Orbiwise platform has good arrangement on logs and history record. The Analytics tab in NST provide two kinds of logs, which are Reports and Traces. The Reports function records the alarms statistics of gateways deployed in the network and Traces function records the data flow of devices, including uplink and downlink messages. Users can access the history efficiently.

- MQTT Connection: Orbiwise platform mainly provides MQTT publisher for transmitting the messages to application server. In the Applications tab of DASS, the MQTT publisher configuration is embedded in adding new application. Additionally, it is emphasized that the "Start Push" button of each application should be activated, otherwise, the application server could not receive any messages from Orbiwise platform.

- Security Level: The Orbiwise mainly applies the security mechanism that the gateway is installed with an extra firmware to ensure the connection between gateways and Orbiwise platform. The main connection between gateway and LNS is through TLS. In addition, the Orbiwise platform could block/unblock the gateway to avoid some attacks from other networks.

3. LORIOT

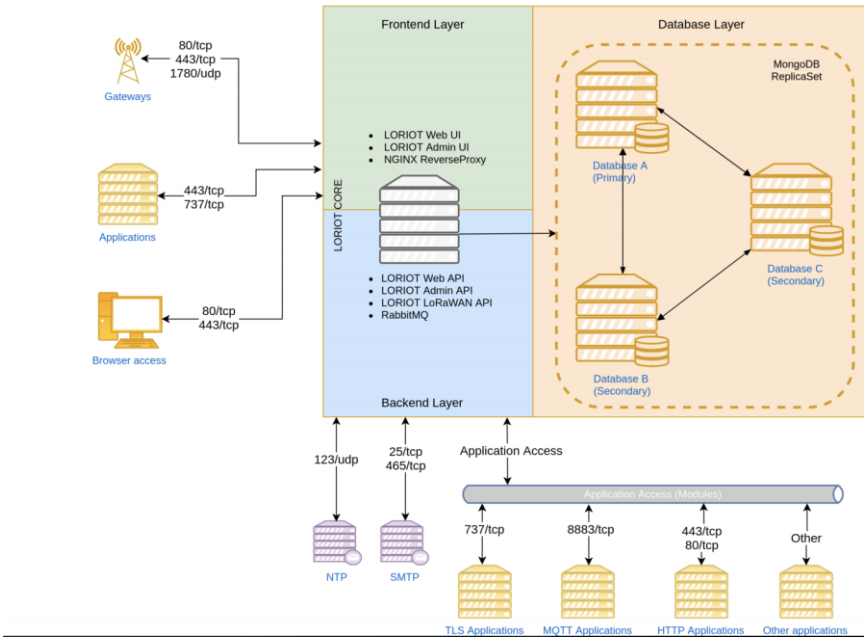


Fig. 18. LORIOT Network Structure

Table 15. Basic Information of LORIOT

Server Information	Records
LNS Platform Name	LORIOT LoRaWAN Network Server (LORIOT)
Country of Origin	Switzerland
Type of Platform Delivery	SaaS, Cloud-based
Location of Hosting Server	Hong Kong (Azure)
Extra Function Server	None

Platform	
On-Premise Option	Support

Table 16. LoRaWAN and Internet Protocol Compliance of LORIOT Platform

LoRaWAN Protocol Version	LoRaWAN Protocol V1.0.x, V1.1 LoRaWAN Regional Parameters V1.0.x, V1.1
Security Policy	HTTPS, TLS1.2, HSM, AES, SSH
Internet Transmission Protocol	HTTP, HTTPS, MQTT, Websocket

Table 17. Detailed Features of LORIOT Platform

Services	Negative/Positive	Remarks
LoRaWAN Network Management	LORIOT provide web services to manage the networks.	1. Clear Network management platform 2. Users could define various network for different applications. 3. Easy to build different networks.
Channels Management	The channels management varies with different gateway model and decided by users.	AS923 (But 924.6 frequency point is not supported)
Gateway Management	Web services for managing gateways	1. Gateway Supported List: 2. Kerlink (OK) 3. MultiTech (OK) 4. Tektelic (ok, but works on lower band AS923) 5. Clear gateway status monitoring UI 6. The registration steps are clearly introduced in the platform. 7. For the reference on RF parameters configuration, LORIOT should be improved. 8. Don't find manual channel plan configuration functions.

		9. Gateway management information are clear to be shown.
Extra Gateway Scripts/Software	Extra gateway scripts/software is needed to be installed. (Provided by LORIOT web services)	1. Support Standard Semtech Pure UDP Packet Forwarder 2. This platform has supported tens of gateways with different design using LORIOT-Defined PF. 3. Don't support Basics Station protocol. 4. The extra scripts or software installations of this platform vary from different gateway models. But it could be accepted because of the easy installation method. 5. For other gateways not listed in the LNS, LORIOT may need to provide support for them.
Device/End Node Management	Web services for managing devices or end nodes.	1. OTAA/ABP 2. Bulk Import 3. Class A, B and C 4. Device Positioning Map 5. LORIOT combines the device management functions and services into applications. (Need to define applications first) 6. LORTIOT LNS main logistics include applications (Devices and applications APIs for development) and networks (Gateways). Users should occupy some knowledge for LoRaWAN technology. 7. Statistics are good for management.
Users Application Interface Management	Web services for managing devices or end nodes.	Web UI Data Push Account Management Restful API, Websocket & MQTT
Access Control	Managed by web services (The permission of different service level is controlled by the	Method: 1. Different users create different log-in account. 2. Multitenancy management

	backup system.)	
VPN	Installed in the carrier operating system of LORIOT	OPENVPN

Table 18. Management Services of LORIOT Platform

Services	Negative/Positive	Remarks
LNS Runtime Log	Detailed runtime and history log records in the web.	1. Gateway Alert UI is great 2. Data Traces (Detailed message classification) 3. Log File Export and download to local
Log-in Events Log	Monitoring by backup services	Didn't find any records or logging logs for multiple level user.
Development Programming Language	Decided by the developers	Javascript, etc. (Decided by developers)
LNS Maintenance: Depend on contract between LORIOT and EMSD		
Offline Resources: 1. LORIOT mainly provides user manuals and system structure files to introduce their platform. 2. The offline and online resources are enough.		
Online Resources: 1. LORIOT provides detailed training course on how to use the LNS. 2. Manuals: Very good organization on online document 3. Papers: A brief introduction on features in the official website Source codes/configuration templates: LORIOT has already embedded the instructions into online platform. But for data output, the resources or manuals should be improved. E. g. MQTT configuration.		
Debugging and Trouble Shooting: 1. Contact LORIOT by Email 2. There is no log file to record data push tracings.		
Service Level: Guarantee on Uptime, Downtime (LNS Reliability, N-Nine Level): 2 or 3 Nine availability (To be confirmed by EMSD and LORIOT contract)		
Development and Future Expansion: 1. The support on gateway firmware could be improved. 2. The channel plan could be standardized for users and customers.		
Man-Power Arrangement: Depend on LORIOT and EMSD		
System Support Services: 1. Team Support: Yes 2. Location of Support Team: Korea		

3. Remote Support or On-site Support: Remote Support Only 4. Development Support: Yes 5. Charging Model: 48000 HKd

Table 19. Additional Features of LORIOT

Mandatory Features: Migration of Gateways and Sensors: Not Absolutely (LORIOT can transfer gateways into other networks. But their extra scripts/software installation in gateway may finally influence the migration.) Failover Configuration: To be confirmed by LORIOT Team Gateway Position on Map: Yes Provision of Infrastructure Summary in One Click: Relative Clear Dashboard Generation: Yes (1. Network configuration and management 2. Application configuration and management)	Other Features: 1. Redundancy Design: Support Database replications 2. Support LoRa device geolocation 3. Efficient Log Analyser for managing gateway data flow, device data flow, etc. 4. Network security between gateway and network server is based on LORIOT own packet forwarder.

- Application management and Device Management in LORIOT: Similar to TTN platform, LORIOT integrate the device management in application management. In Applications Tab, users could access into each application and enroll or delete end devices in the platform. LORIOT supports many kinds of connection methods to application server, which are integrated in applications management. The enrollment of end devices is also user friendly.

- Gateway Management: LORIOT platform applies network concept to manage gateways. This platform also supports pure UDP PF and LORIOT-Developed scripts installed to gateways. If the registered gateway installed with LORIOT scripts, the platform can provide more features to manage the gateway, such as remote access, channel plans and etc. However, the frequency band support of LORIOT is not good. For instance, the Tektelic gateway with LORIOT scripts cannot be configured to AS923.2 to 924.6 MHz band but RAK gateway can do it. Hence, there is a necessary to improve the frequency management consistence among different model of LoRa gateway.

- Client Management: If the user access into LORIOT platform as normal status, the basic functions are discussed in the above. Because CityU doesn't occupy the administration status, the access control or management is not clear in the evaluation.

- Trouble shoot: The main trouble shoot services of LORIOT are through online contact. LORIOT official website has already provided enough resources on right configuring the networks, applications and gateways. Considering on the privacy issue, EMSD needs to deploy the LNS platforms in its own data center and the management is inefficient if there is only online support and trouble shoot service.

- Log Support: The traffic flow of gateway is recorded in the registered gateway page. For the log of different applications, LORIOT platform provides two kinds of logs, which are Statistics and Log. Statistics clearly inform the traffic history in amount of the messages for last 24 hours. The Log function records all the history traffics and shows them with detailed UI.

- MQTT Connection: MQTT is one of the integration methods of LORIOT to communicate with application server. In the applications management tab, the MQTT connection could be found at "Output" tab. The basic configuration of MQTT in LORIOT is similar to TTN and Orbiwise.

- Security Level: The security mechanism or standardization should be provided by the platform providers. On-site server deployment of different platform should be recommended by the platform provider too. (Why can the security of the platform be ensured? Any methodologies, standardization or common method?)

4. Actility

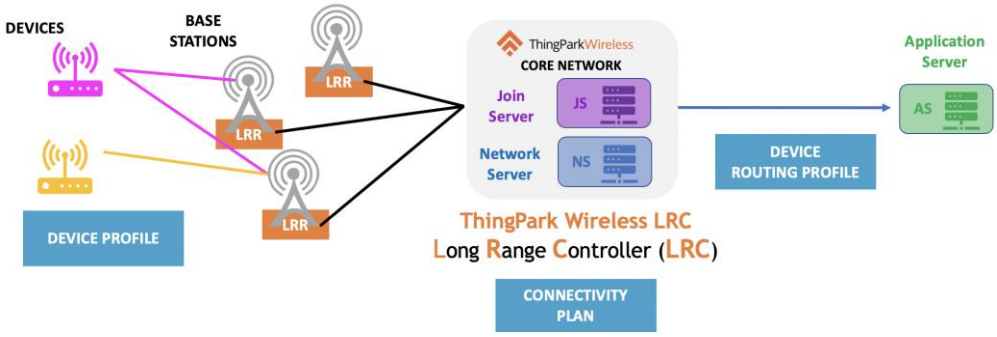


Fig. 19. Actility-Thingpark Network Structure

Table 20. Basic Information of ThingPark

Server Information	Records
LNS Platform Name	ThingPark Platform
Country of Origin	France
Type of Platform Delivery	SaaS, Cloud-based
Location of Hosting Server	Hong Kong (Azure)

Extra Function Server Platform	None
On-Premise Option	To be confirmed

Table 21. LoRaWAN and Internet Protocol Compliance of ThingPark Platform

LoRaWAN Protocol Version	LoRaWAN Protocol V1.0.x, V1.1 LoRaWAN Regional Parameters V1.0.x, V1.1
Security Policy	HTTPS, TLS1.2, HSM, AES, SSH
Internet Transmission Protocol	HTTP, HTTPS, MQTT (Manually)

Table 22. Detailed Features of ThingPark Platform

Services	Negative/Positive	Remarks
LoRaWAN Network Management	Actility provides web services to manage the networks.)	Provided by Network Supplier: ➢ Base Station Long Range Relay (LRR): A ThingPark defined packet forwarder for building communication between base stations and ThingPark platform. ➢ Base Station Profile: Record the basic information of supported LoRa gateways ➢ The role of Network Supplier should be created by Operator of ThingPark Platform.
Channels Management	The channels management is defined in the network management and developers could revise the channel management plan.	AS923 (The channels plan should be revised and provided in the LRR firmware developed by ThingPark team.)

Gateway Management	Web services for managing gateways	ThingPark provides a detail gateway management platform. Function Tab Position: Suppliers -> Search -> EMSD Network Provider -> Impersonate -> Network Manager 1. The LRR firmware must be installed to base stations first. 2. To create the new base station in the network, LRR ID and gateway manufacturers must be defined. 3. Go into the impersonate of each base station, the detailed information are shown: ➢ Base station basic information ➢ Installation: Power source of base station, GPS receiver, antenna, WAN backhaul, software, VPN and authentication ➢ System Indicators: Hardware utilization rate ➢ RF cell indicators: LoRa modem performance ➢ Backhaul indicators: The information of connections between base station and ThingPark Platform. ➢ Uplink/Downlink Packets Statistics These gateway management services are powered by LRR firmware. If the gateway applies the pure UDP PF, then it cannot work on ThingPark Platform.
Extra Gateway Scripts/Software	Extra gateway scripts/software is needed to be installed. (Provided by Actility support)	Long Range Relay (LRR) is necessary for each gateway. 1. pubkey file 2. cpkg file ThingPark Platform supports several base stations: 1. Kerlink 2. Multitech 3. Tektelic 4. Cisco

		5. Unispace
Device/End Node Management	Web services for managing devices or end nodes.	ThingPark provides a detail end device management platform. Function Tab Position: Subscribers -> Search -> EMSD Team 1 or 2 -> Impersonate -> Device Manager (Wireless Logger) 1. ThingPark Platform supports standardized LoRaWAN end devices. 2. To create the end device, connectivity plan and application server routing profile should be defined. Connectivity Plan: Created by Connectivity Supplier (Operators create connectivity suppliers) Function Tab Position: Suppliers -> Search -> EMSD Connectivity Supplier -> Impersonate -> Connectivity Manager ➢ End device quantity limitation ➢ Define uplink/downlink traffics (uplink/downlink rate, buffersize, etc.) ➢ Adaptive data rate configurations ➢ Device status: battery level, signal margin, etc. ➢ Roaming: OTAA, handover ➢ Payload Routing Options: Third party application servers routing: HTTP (MQTT should be further informed by Actility) ➢ Geolocation: TDOA, RSSI, BOTH (Gateway installation must be with GPS signal) Application Servers: HTTP, Kafka
Users Application Interface Management	Web services for managing devices or end nodes (Wireless Logger)	HTTP (Webhook) MQTT (Informed by Actility, the MQTT feature must be enabled manually and there is no enough guidance on this problem.)

Access Control	Managed by web services (Framework of access control is shown in Fig. 5)	Detail and Professional Access Control
VPN	Installed in the carrier operating system of Actility	Openvpn (IPSec)

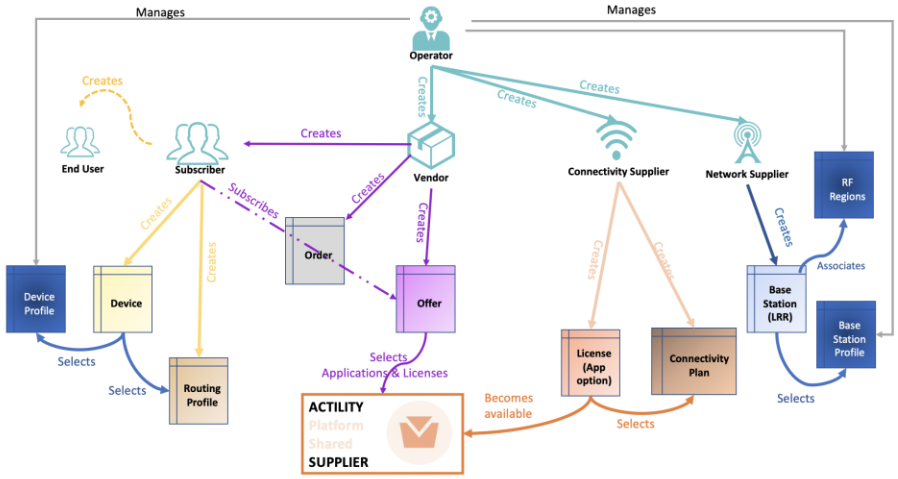


Fig. 20. Access control of ThingPark Platform

Table 23. Management Services of ThingPark Platform

Services	Negative/Positive	Remarks
LNS Runtime Log	Detailed runtime and history log records in the web.	1. Gateway traffic log: ➢ No packet traffic log shown in the UI (To be confirmed by Actility) ➢ Active alarms of base stations: GPS failure, LRR software restarted, etc. ➢ Packet Statistics 2. Wireless Logger (Detail End device traffics log records): ➢ Timestamp of each packet and directions ➢ DevEUI records ➢ RSSI, SNR, ESP ➢ Decoder: ThingPark platform support different kinds of decoder to parse the received LoRa packets

		The wireless logger provides a good data flow management feature.
Log-in Events Log	Monitoring by backup services	Should be informed by Actility (Backup control can get the log) The actility platform could inform the main operations of operators, suppliers, vendors and subscribers.
Development Programming Language	Decided by the developers	Javascript (ThingPark X API)
LNS Maintenance: Depend on contract between Actility and EMSD		
Offline Resources: 1. The offline resources mainly introduce the network framework of ThingPark Network. 2. The offline resources are enough to manage the platform 3. LRR firmware of base station should be improved to support more models.		
Online Resources: 1. Training courses 2. Email Contact 3. There is insufficient online resources to help the users to manage the platform, base stations and end devices. (This feature should be improved by Actility.)		
Debugging and Trouble Shooting: 1. Contact Actility by Email 2. No on-site support		
Service Level: Guarantee on Uptime, Downtime (LNS Reliability, N-Nine Level): 2 or 3 Nine availability (To be confirmed by EMSD and Actility contract)		
Development and Future Expansion: 1. More gateway models could be supported. 2. Extra web services on managing connection between LNS and user's applications are needed. (MQTT, HTTP, etc.)		
Man-Power Arrangement: Depend on Actility and EMSD		
System Support Services: 1. Team Support: Yes 2. Location of Support Team: France 3. Remote Support or On-site Support: Remote Support Only 4. Development Support: Yes 5. Charging Model: The price is provided by Actility.		

Table 24. Additional Features of ThingPark Platform

Mandatory Features: Migration of Gateways and Sensors: Not Absolutely (The gateway in Actility platform is transferred to other platform based on removing the LRR firmware.) Failover Configuration: To be confirmed by Actility Team Gateway Position on Map: Yes Provision of Infrastructure Summary in One Click: Clear and Detail Dashboard Generation: Yes (1. Network Manager and Device Manager function manage the network configuration and end device configuration (2. Wireless Logger manages the data traffic from end devices.	Other Features: 1. Redundancy Design: Support (To be confirmed by Actility) 2. Support LoRa device geolocation (RSSI and TDOA) 3. Efficient Log Analyser for managing gateway data flow, device data flow, etc. 4. Network security between gateway and network server is based on Actility own PF firmware.

- Application management and Device Management in Actility: Actility provides professional management on applications and devices. In this platform, users could clearly define the configuration on applications or devices through the end device management web services.

- Gateway Management: The gateway management of Actility is introduced in Table 18. The main problem is that Actility LNS only supports several models of LoRa gateway and the extra software/scripts must be provided by Actility in advance. There is also lack of a common place to store these extra scripts/software in the LNS.

- Client Management: Actility provides a professional management on access control. As shown in Fig. 5, LNS manager could create different role for users and distribute different service level for them. This kind of management is appropriate for market network. But Actility should provide more support on how to manage the roles/permissions of different customer. Hence, more man-power should be grouped.

- Trouble shoot: The main trouble shoot services of Actility are through online contact. The online resources of Actility should be improved given the lack of trouble-shooting resources from internet. Considering on the privacy issue, EMSD needs to deploy the LNS platforms in its own data center and the management is inefficient if there is only online support and trouble shoot service.

- Log Support: The Wireless logger function in Actility is a high-efficiency tools. This tool provides a detailed tracing logs to store the radio traces of end devices, applications. But the user's log-in record is lacked and Actility could provide a

scheme to support it (By backup or web services).

- MQTT Connection: Actility platform should improve the support on this integration because only manual configuration on MQTT is supported in this LNS version. It is better to support web service similar to TTN, LORIOT and Orbiwise.

- Security Level: The security mechanism of Actility applies the common methods as TTN, LORIOT and Orbiwsie. The professional access control of users could improve the security of the system. Hence, actility platform could be regarded as the most secure platform than others.

5. Tektelic and Trackcentral LNS(s)

There are no supporting services provided by Tektelic and Trackcentral platform, hence these two kinds of LNS(s) cannot be deployed for enterprise-level service. The main features of the two LNS(s) is addressed as following:

Tektelic:

- Mainly designed for Tektelic LoRa gateway (The main features such as firmware update cannot support other types of LoRa gateway produced by other companies.)

- Online and Offline Resources is not enough for users/managers.

- Pure Semtech UDP PF

Trackcentral:

- LNS service logistics is not clear. LoRa gateway is named as "Router" in the system.

- Data pushing development should be based on programming, which is not efficient for users' define applications.

c. Evaluation result

1. All the six enterprise LNSs could perform normal LoRaWAN services. But most of them could not meet the enterprise network-requirements.

2. The evaluation is based on four properties, which are LNS Technical Features, Packet Forwarder Supporting, Redundancy Design and Management Supporting Services. Each property occupies 25% marks.

3. For each evaluation property: Perfect (5) Good (4) Fair (3) Average (2) Not Provide (1)

Table 25. LNS Evaluation Marks

Items / LNS	LNS Technical Features	Packet Forwarder Supporting	Redundancy Design	Management Supporting Services	Overall Grades

TTN	5	5	4	4	4.5
Orbiwise	5	3	4	4	4
LORIOT	5	4	3	4	4
Acitility	4	3	4	5	4
Tektelic	3	2	1	1	1.75
Trackcentral	3	2	1	1	1.75

From the overall marking, TTN Server could be one of the LNS recommendations for enterprise GWIN LoRa network.

D. LoRaWAN Sensor Deployment Guidelines

LoRaWAN sensor plays a significant role in data collection and transmission of applications. To ensure the effectiveness and reliability of application, each sensor is covered by multiple gateways depending on the quality of service (QoS) required for the applications. As mentioned in last section, sensor site survey is carried out together with the gateway site survey to coordinate and achieve acceptable signal coverage plan for applications. Based on the preliminary results of site survey, site acceptance test plan of sensors is required to determine the final deployment plan.

a. Sensor Installation Methodology

1. General requirements for sensor installation

1.1 A waterproof case (at IP66 better rating) shall be installed for each LoRaWAN sensor with proper labeling.

1.2 LoRaWAN sensors shall comply with the LoRaWAN v1.0.2 or the lastest version issued by LoRa Alliance™.

1.3 LoRaWAN sensors shall meet the requirements as follows:

1.3.1. Support uplink random LoRaWAN channel selection from 920-925MHz;

1.3.2. Supports Adaptive Date Rate (ADR);

1.3.3. Support Over-the Air Activation (OTAA) activation mode;

1.3.4. Support the characteristics of LoRaWAN class A or B or C;

1.3.5. Support heartbeat message at least once a day;

1.3.6. Support automatic and/or scheduled and/or manual re-join mechanism

1.3.7. Support configurable DEV_EUI, APP_EUI, APP_KEY (and NWK_KEY for

LoRaWAN v1.1)

1.3.8. The maximum transmission duty cycle shall be 1%, and the maximum dwell time per frequency channel shall be 400 millisecond. (Note: Special cases need to be approved by EMSD)

1.3.9. The maximum application payload size shall be 242 bytes [11]

1.4 The average measured LoRa signal strength of each location shall meet the requirements of corresponding applications. In general, for the sensor covered by multiple gateways, the LoRa signal strength from the best gateway is considered as the signal strength of this location. The parameters for reference are: 1) Downlink RSSI $\geq$ -110dBm ($\pm$10dBm); 2) Downlink SNR $>$ -20dB; 3) Uplink RSSI $\geq$ -10dBm ($\pm$10dBm); 4) Uplink SNR $>$ -10dB; 4) DR is between DR0 to DR5. Besides, the PLR needs to meet the requirements of applications to ensure the reliability of transmission.

b. Sensor Acceptance Plan

The sensor acceptance plan shall include the following contents:

1. Test Purpose

2. Test Equipment

3. Test Procedure

3.1 Inventory Check (For LoRa: Device ID, Device EUI, Detailed location, Activation mode, Transmission interval, Transmission Power)

3.2 Health Check

3.3 Sensor Configuration (For LoRa: Device EUI, Application EUI, and Application Key (and Network Key for LoRaWAN v.1.1 devices))

3.4 Record the SNR, RSSI both in Uplink and Downlink from LNS

3.5 Check Data Accuracy (According to specific sensor type)

3.6 Check PLR

The sample of Site Acceptance Test Plan of Sensor is shown in Appendix III

E. Interface Coordination between GWIN and Applications Guidelines

To enables effective data exchange between clients' applications and LPWAN (LoRaWAN, Sigfox, NB-IoT), Message Queuing Telemetry Transport (MQTT) broker is adopted in GWIN. Compared with other common network protocols (e.g., HTTP, AMQP, XMPP, etc.), MQTT is an open, lightweight, publish-subscribe network protocol, which is more adaptable to resource-constrained applications based on GWIN. In this part, to achieve the best practice, multiple MQTT broker solutions are evaluated and an overall solution recommendation is provided.

a. MQTT introduction

MQTT (Message Queuing Telemetry Transport) is an open, lightweight, publish-subscribe network protocol (over TCP/IP) that transports messages between devices [12]. It can be supported by any network protocol that runs over TCP/IP and enables bi-directional and async communication between devices.

In Internet of Things (IoT), devices need to be connected to Internet to enable data communication. Apart from MQTT, there are also multiple network protocols choices, such as HTTP, Advanced Message Queuing Protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP), etc. These protocols are popular in some high-performance communication scenarios, but they show limitations for IoT applications.

HTTP is a synchronized network protocol based on request-respond mode [13]. Based on HTTP protocol, clients need to wait for the response of the server, which sacrifices the scalability. In the IoT field, a large number of devices and possibly unreliable or high-latency networks make this synchronous communication become a problem. In addition, HTTP only supports one-way communication, and the connection must be initiated by the client. In IoT applications, devices or sensors are usually clients, which means that they cannot passively receive commands from the server. Hence, it is not suitable for bi-directional IoT applications. Besides, it is difficult and expensive to deliver messages to all devices on the network through HTTP protocol, but this is a common use case in IoT area.

AMQP is the most popular network protocol in enterprise systems [13]. It dedicates to achieving reliability and interoperability in enterprise applications. However, AMQP requires high-performance environments with enough computing power and low network latency, which is not suitable for resource-constrained IoT applications.

XMPP is an Instant Messaging (IM) protocol which carefully defines all the message formats and requires that all messages be in XML [13]. The IM features requires relatively high overhead of XMPP protocol and large power consumption, which is contrary to the original intention of most IoT applications.

Compared with above network protocols, MQTT is much more appropriate for IoT applications with following characteristics:

1) MQTT is an open and lightweight network protocol, which enables developers to implement on resource-constrained devices.

2) MQTT has minimized data packets (up to 256MB) [13], which mitigates the overhead of protocol exchanges and requires low network usages.

3) MQTT adopts the publish-subscribe mode, which supports one-to-many message transmission to provide a high network scalability.

4) MQTT is implemented over TCP/IP protocol, which provides bi-directional and effective data transmission.

With above advantages, MQTT is greatly adaptable to resource-constrained IoT devices and bandwidth-limited IoT network. Besides, the high feasibility of MQTT makes it

possible to provide supports for diverse application scenarios of IoT devices and services.

In MQTT architecture, there are two major parties: a MQTT broker and MQTT clients. A MQTT broker, acting as a server, receives all messages from the clients and then routes the messages to the destination clients. A MQTT client can be any device that communicates with the MQTT broker, such as IoT sensors, user applications, etc. This MQTT architecture separates the message sender from the receiver in space and time, so it can be extended when a large number of devices are added. In GWIN system, LPWAN devices or LPWAN network servers send messages within a certain topic to MQTT broker. MQTT broker routes these messages to all user applications that subscribe to the topic. In turn, the messages from user applications can be transmitted to LPWAN devices under the same topic through MQTT broker. The MQTT architecture in GWIN system is shown in Fig. 1.

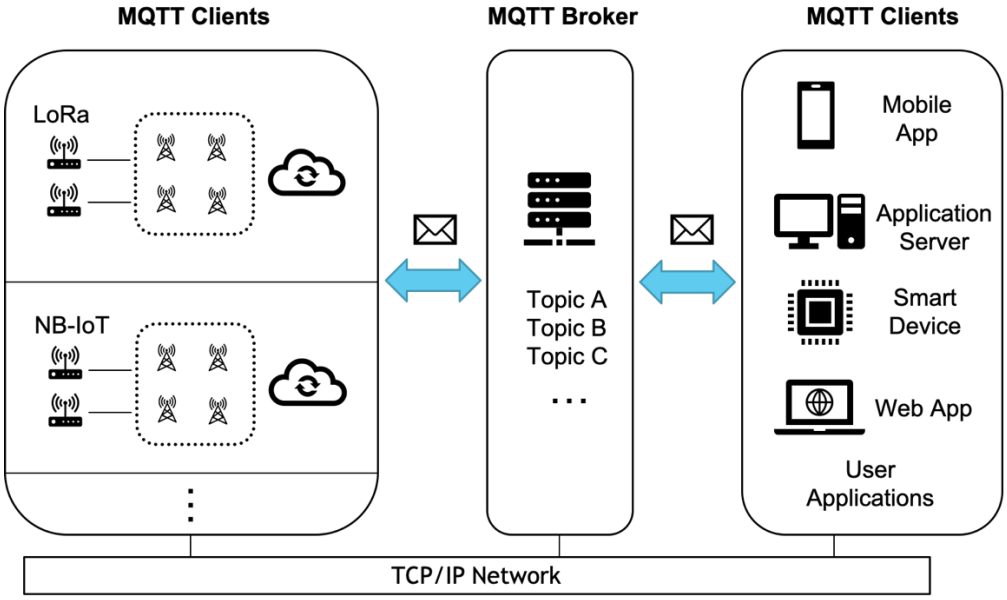


Fig. 21. MQTT architecture in GWIN system

b. MQTT Evaluation Methodology and Criteria

In this section, the most common MQTT brokers are evaluated, including Mosquitto, VerneMQ, EMQ, and HiveMQ. To provide the most appropriate MQTT broker for GWIN, the evaluation is performed from following aspects:

- MQTT Broker Basic Features
- Functionality Supports
- Redundancy Design
- Management & Maintenance

1. MQTT Broker Basic Features:

(1) Basic Information of MQTT Broker: MQTT Broker Name, Country of Origin, Software

License, Type of Broker Delivery, Development Language, Platform Support, On-Premise Option, and Partners.

(2) Protocol Compliance: MQTT Protocol Version, Security Policy, and Connection Methods.

2. Functionality Supports: MQTT broker provides message communication channels between IoT devices and destination user application based on MQTT protocol. To ensure the efficient and effective transmission, it is necessary to evaluate the performance of MQTT brokers based on different functionalities.

(1) Core Functionalities: IoT Protocol Support, QoS Support, Retained Message, Persistence, Last Will and Testament. These functionalities are the core of MQTT protocol, which ensures the effectiveness of MQTT data transmission.

(2) Advanced Functionalities: Shared Subscription, Database Extension, Bridge. These advanced functionalities support the extension of MQTT messages to other data processing softwares, which improves the scalability of MQTT broker and management flexibility.

3. Redundancy Design: MQTT broker is a critical part of messaging infrastructure and is the key part of the GWIN system backbone that must not fail. The communication between a large number of clients depends on the MQTT broker as central message distributor. It is assumed that there is only one MQTT broker in network. When this server encounters running error/attack/other system errors, all of the clients in the system could not receive services from MQTT broker. In other words, single point of failure will cause damage to the entire network. In order to avoid the single point of failure in messaging systems, a MQTT broker cluster is needed. Redundancy design provides clustering support and load balancing management among MQTT broker nodes.

(1) Clustering: A cluster forms an internal connection between multiple MQTT broker node that deployed in distributed servers. When the single MQTT broker node of the MQTT broker cluster fails, other nodes could take over its work to keep the normal messaging service. Hence, it is necessary to implement MQTT broker cluster to guarantee the availability, reliability and resilience of GWIN messaging infrastructure.

(2) Load Balancer: This technology aims to balance the input data flow to MQTT broker nodes, which provides the overload protection for each node in the cluster.

4. Management & Maintenance.

(1) Management: Authentication, Access Control, Dashboard, Message Processing Management, Backup & Restore, Tracing Recordings, Overload Protection, MQTT Broker Runtime Logs. These are necessary services for management, maintenance and development.

(2) Maintenance: Offline Resources and Online Resources, Debugging and Trouble Shooting, Development and Future Expansion, System Support Services, Pricing

Model

c. The performance evaluation of different MQTT brokers

Based on the above evaluation criteria, the evaluation was performed based on MQTT broker function trails and MQTT broker operational trails. The features of different MQTT brokers are presented as follows:

1. EMQ

Table 26. Basic Information of EMQ X Enterprise

MQTT Broker Information	Records
MQTT Broker Name	EMQ
Software License	EMQ X Enterprise: Enterprise-ready MQTT broker
Country of Origin	China
Development Language	Erlang
Platform Support	Linux, MacOS, Windows, FreeBSD, Docker/K8S, Public Cloud, Private Cloud, Physical Server
Latest Release	V4.1
On-Premise Option	Yes
Partners	The EMQ has served 50+ counties and nations. There are 6000+ enterprises cooperating with EMQ worldwide, including 50+ Fortune Global 500, such as Huawei, Cisco, Intel, China Mobile, etc.

Table 27. Protocol Compliance of EMQ X Enterprise

Compliance	Records
MQTT Protocol Version	MQTT Protocol V3.1.1, V5.0 (V5.0 is the latest version)
Security Policy	TLS/SSL one-way/two-ways authentication, the X.509 certificate, load

	balance SSL, etc. SSL/TLS supports for all protocols supported by EMQ X
Connection Methods	TCP, Websocket, TCP/SSL, Websocket/SSL

Table 28. Functionality of EMQ X Enterprise

Functionality	Yes/No	Remarks
IoT Protocol Support	YES	Supported IoT protocols: LoRaWAN, NB-IoT, WiFi, 2G/3G/4G, 5G, etc.
QoS Support	YES	QoS Levels: QoS0, QoS1, QoS2
Retained Message	YES	5. Multiple options of storage location, including RAM, Disk, and external databases. It is efficient to store remained message into external database, which expands the capacity of retained messages and saves the limited resources of nodes. 6. Configurable maximum number of retained message, configurable maximum payload size, configurable expiration time.
Persistence	YES	5. Support data persistence in Redis or various databases (i.e. MySQL, PostgreSQL, MongoDB, Cassandra, DynamoDB, InfluxDB, OpenTSDB, Timescale). Data persistence to external Redis or databases saves hardware resources of nodes. 6. Support two ways of persistence: one-to-one, one-to many. It is efficient for subscribers to receive messages.

Last Will and Testament	YES	Will Messages include will topics, will payload.
*Shared Subscription	YES	Support shared subscription with/without group
*Database Extension	YES	Support various databases, including MySQL, PostgreSQL, MongoDB, Cassandra, DynamoDB, InfluxDB, OpenTSDB, Timescale.
*Bridge	YES	Support various bridges, including Kafka, RabbitMQ, Pulsar, other EMQ X nodes, and other MQTT brokers (i.e. Mosquitto, HiveMQ, RabbitMQ, VerneMQ)
*Additional Functionalities 1. Apart from MQTT, EMQ X also supports MQTT-SN, CoAP, Websocket, HTTP, Stomp/SockJS, LWM2M, etc. protocols. 2. Support delayed publish, topic rewrite to ensure effective transmission 3. Support HTTP APIs for integration EMQ X with external systems, which provides users with a more flexible management approach. 4. Support blacklist function through HTTP API or direct ban of usernames and IP addresses, which is an efficient way to prevent malicious clients. 5. Support rule engine to configure the processing and response rules of EMQ X message flows and device events, which improves the flexibility, usability, and efficiency of system. 6. Supprot Schema Registry, provide data encoding and decoding capabilities for EMQ X events and messages		

*(*denotes advanced functionalities)*

Table 29. Redundancy Design of EMQ X Enterprise

Services	Yes/No	Remarks
Clustering	YES	1. Support both manual and auto clustering approaches, including static, mcast, dns, etcd, k8s. 2. Support scalability. It is easy to add or remove nodes in a cluster without stopping the service. 3. Support infrastructure outage scheme. Even if parts of the cluster fail, the cluster system as a

		whole could be available to avoid service interruptions. 4. Network Outage Scheme: Auto-heal from Network partition. Network outage can lead to partition, EMQ X supports automatic recovery from a network partition. 5. Support Zero Downtime Upgrades. With proper deployment strategies, such as blue/green deployment, downtime of upgrading EMQ X can be greatly reduced, zero downtime is possible
Load Belancer	YES	1. Support various choices of load balancers, such as HAProxy, NGINX, AWS ELB. 2. Enable TLS/SSL offload on EMQ X nodes. 3. Suggestions when the load balancer is interrupted: As a nature of a service component behind the LB, the EMQ X doesn't have the ability of sensing the interruption of LB. But as an application level solution, the client device can have a backup address pointing to EQM X directly and bypass the LB when necessary.
Performance Evaluation and Deployment Suggestions: 1. Single EMQ X node can handle up to 1 million connections. An EMQ X cluster can handle 10 million concurrent connections. 2. Deployment Suggestions for around 10,000 concurrent connections: EMQ Suggestions: If there isn't any special requirement (very high message rate, very large		

message size, etc), very common server hardware available in the market should be enough to sustain 10,000 concurrent connections. 4 CPU cores + 4GB RAM shall be sufficient for 10K connections under normal load. But still, EMQ X suggest enough capacity for a future-proof deployment. EMQ X support multiple ways of auto clustering, but there is no good approach or bad approach. The clustering approach is subject to the nature of over-all deployment strategy. For HA, it is suggested to deploy at least 2 nodes in cluster. It is suggested that to enable TLS/SSL on load balancer, so that 1) the Certificate ban be unified managed; 2) the special/optimized software/hardware on load balancer is fully used.

Table 30. Management & Maintenance of EMQ X Enterprise

Services	Yes/No	Remarks
Authentication	YES	EMQ X Enterprise supports various types of authentications, including basic built-in MQTT-based authentication (username/Client ID/Mnesia), authentication of external common databases (i.e. LDAP, MySQL, PosgreSQL, Rdis, MongoDB), HTTP authentication, and JWT authentication, which ensures the security from multi-level authentications.
Access Control	YES	1. Support ACL through ACL plugins. 2. Support built-in Publish/Subscribe ACL. The ACL rules are based on a simple logic, which is easy to set. The ACL rules could define global rules for all clients and specific rules for each client through username or IP address, which is efficient for managers to perform global or individual control. 3. ACL cache is provided to enable clients to cache ACL rules into memory, which improves connection efficiency. 4. Support various external

		database ACLs, such as MySQL ACL, PostgreSQL ACL, Redis ACL, MongoDB ACL. These database ACLs follow similar logic, which is easy to define. 5. Support HTTP ACL.
Dashboard	YES	1. Clear Web UI. 2. The statuses of all nodes in the cluster could be monitored through the dashboard of each node. 3. Support real-time clients and topics monitoring. 4. Support plugins management. 5. Support multi-level users (administrator/viewer). 6. Support rule engine management.
Message Processing Management	YES	Support highly efficient message processing scheme through Inflight and Message Queue
Backup & Restore	YES	User data, including the rule engine rules and resources, can be exported and imported as Json file on dashboard.
Trace Recordings	YES	1. Support filtering logs for ClientID or Topic. 2. Support 8 levels of log tracing.
Overload Protection	YES	1. Support rate limit on connection, publishing, which avoids system overload from the entrance and guarantees system stability and predictable throughput. 2. Support load balancing of nodes in a cluster.
MQTT Broker Runtime Logs	YES	1. Support 8 levels of logs. Different levels of logs can be stored separately, which is efficient to manage. 2. Support 2 output formats: console and file. 3. Default max log storage size is 50MB. When the latest log excesses the

<table>
<tr><td></td><td></td><td>max size, it will be overwritten from the oldest log.
4. Clear log format.
5. Efficient hierarchical log system based on log level and log handlers.
6. Support modifying log levels at runtime.</td></tr>
<tr><td>Debugging and Trouble Shooting</td><td>YES</td><td>1. 24/7 Support or 8/5 Support (To be confirmed by EMSD)
2. Support updating, upgrading, correcting bug fixes for the software.</td></tr>
<tr><td colspan="3">Development and Future Expansion: To be confirmed by EMQ and EMSD (This should be considered in future contract)</td></tr>
<tr><td colspan="3">Supporting Resources:
1. Online Manuals: Very good organization on online documents from EMQ official website in both Chinese and English.
2. Offline Resources: EMQ mainly provides user manual, benchmark report to introduce EMQ X. EMQ not only introduces the methods to use their broker but also provides knowledge about MQTT protocol.
3. Sources Codes: In Github
4. Tutorials: Clear configuration templates in EMQ official website
5. Training courses: It is better for EMSD and EMQ to arrange a training course for EMQ X Enterprise broker.</td></tr>
<tr><td colspan="3">System Support Services:
1. Team Support: Yes
2. Location of Support Team: Hangzhou and Shenzhen
3. Remote Support or On-site Support: Both. On-site support is arranged on requirement.
4. Customized Functionality Support: Yes
5. Delivery Method: If there is no customization, the EMQ X soft is downloadable on its website. The license key is delivered by a way agreed by both parties. If there is customization in deliverable, it is delivered by a way agreed by both parties.
6. Development and Deployment Support: Yes
7. Debugging and Trouble Shooting Method: Email, IM chat, telephone call, remote access/assistance.</td></tr>
<tr><td colspan="3">Pricing Model:
<table>
<tr><th>Max Concurrent Connections</th><th>Subscription Price (USD/YEAR) 8/5 helpdesk</th><th>Subscription Price (USD/YEAR) 24/7 helpdesk</th></tr>
<tr><td>1,000</td><td>3500.00</td><td>13500.00</td></tr>
<tr><td>5,000</td><td>5000.00</td><td>15000.00</td></tr>
<tr><td>10,000</td><td>6500.00</td><td>26500.00</td></tr>
<tr><td>50,000</td><td>15000.00</td><td>35000.00</td></tr>
<tr><td>100,000</td><td>20000.00</td><td>40000.00</td></tr>
<tr><td>200,000</td><td>30000.00</td><td>50000.00</td></tr>
<tr><td>500,000</td><td>50000.00</td><td>70000.00</td></tr>
</table></td></tr>
</table>

EMQ X Enterprise Features Summary (Including advantages and disadvantages):

1) EMQ X Enterprise is based on Erlang which is a great technology currently available to build highly scalable messaging systems.

2) EMQ X Enterprise supports good redundancy design with various fault solutions.

3) EMQ X Enterprise dashboard integrates fully functionalities and enables multi-level user access, which is very convenient for EMSD management.

4) Apart from MQTT, EMQ X Enterprise supports other network protocols, which could be scaled for other services in the future.

5) EMQ X Enterprise supports various databases extensions, which provides high flexibility for database integration.

6) EMQ X Enterprise has simple ACL logic and is convenient for managers to perform individual or global control.

7) Sufficient Online and Offline resources are provided by EMQ. And the configuration process is relatively simple and convenient.

2. HiveMQ

Table 31. Basic Information of HiveMQ Enterprise

MQTT Broker Information	Records
MQTT Broker Name	HiveMQ
Software License	HiveMQ Enterprise: Enterprise-ready MQTT broker
Country of Origin	Germany
Development Language	Java
Platform Support	Linux, MacOS, Windows, FreeBSD, Docker/K8S, Public Cloud, Private Cloud, Physical Server
Latest Release	V4.4
On-Premise Option	Yes
Partners	The HiveMQ has served over 100 international enterprises. The application fields involve automotive, logistic, manufacturing, electronics, etc. Some of partners include, such as Audi, BMW,

	MATTERNET, Daimler, etc.

Table 32. Protocol Compliance of HiveMQ Enterprise

Compliance	Records
MQTT Protocol Version	MQTT Protocol V3.1.1, V5.0 (V5.0 is the latest version)
Security Policy	TLS/SSL one-way/two-ways authentication, the X.509 certificate, load balance SSL, etc.
Connection Methods	TCP, Websocket, TCP/SSL, Websocket/SSL

Table 33. Functionality of HiveMQ Enterprise

Functionality	Yes/No	Remarks
IoT Protocol Support	YES	Supported IoT protocols: LoRaWAN, NB-IoT, WiFi, 2G/3G/4G, 5G, etc.
QoS Support	YES	QoS Levels: QoS0, QoS1, QoS2
Retained Message	YES	1. It is convenient to check retained messages in dashboard, through snapshot. 2. Data are usually stored in local storage. The max number of messages that could be stored depends on the RAM size. 3. Only InfluxDB database extension is supported to connect HiveMQ by now. MongoDB extension is under preparation. 4. Whether the common rules, like the maximum number of retained message, maximum payload size, etc. could be configured in HiveMQ (To be confirmed by HiveMQ).

Persistence	YES	Support data persistence in local storage, Kafka extension, and InfluxDB.
Last Will and Testament	YES	Will Messages include will topics, will QoS, will retained.
*Shared Subscription	YES	Support shared subscription with QoS 0 and QoS 1. It should be noted that shared subscriptions with QoS 2 are automatically downgraded to QoS 1.
*Database Extension	YES	Only support InfluxDB by now.
*Bridge	YES	Support bridges to Kafka, and other MQTT-5 compliant brokers (i.e. Mosquitto, HiveMQ, RabbitMQ, VerneMQ)
*Additional Functionalities 1. Support Rest API to provide an interface for applications to interact programmatically with HiveMQ Enterprise MQTT broker. 2. Support blacklist and whitelist permission through HiveMQ extension. 3. Support Interceptors extension, which provides a convenient way for extensions to intercept and modify MQTT messages.		

*(*denotes advanced functionalities)*

Table 34. Redundancy Design of HiveMQ Enterprise

Services	Yes/No	Remarks
Clustering	YES	1. Support both manual and auto clustering approaches, including static, multicast, broadcast, extension. 2. Support scalability. It is easy to add or remove nodes in a cluster without stopping the service. 3. Support infrastructure outage scheme. Even if parts of the cluster fail, the cluster system as a whole could be available to avoid service interruptions. 4. Network Outage Scheme (To be confirmed by HiveMQ).

		5. Support Zero Downtime Upgrades.
Load Belancer	YES	1. Support various TCP load balancers, such as HAProxy, NGINX, AWS ELB. 2. Enable TLS/SSL offload on EMQ X nodes. 3. When the load balancer is interrupted, it is suggested to implement a local queueing mechanism on clients.
Performance Evaluation and Deployment Suggestions: 1. An HiveMQ cluster can handle 10 million concurrent connections. 2. Deployment Suggestions for around 10,000 concurrent connections: HiveMQ Suggestions: 3 nodes with 4 CPU cores + 4GB RAM/node		

Table 35. Management & Maintenance of HiveMQ Enterprise

Services	Yes/No	Remarks
Authentication	YES	The supported authentications include username/Client ID authentication, and databases authentication. HiveMQ Enterprise handles these authentications via security extensions.
Access Control	YES	1. Support ACL through extension system. 2. Support fine grained Publish/Subscribe ACL. However, the ACL rules are set through XML format, which is complex and not convenient for managers to configure. 3. Support blacklist and whitelist permission.
Dashboard	YES	1. Clear Web UI. 2. The statuses of all nodes in the cluster could be monitored through the dashboard of each node.

		3. Support real-time clients and topics monitoring. 4. Support viewing trace recordings and retained messages.
Message Processing Management	YES	Support intercepting and modifying MQTT messages through Interceptors.
Backup & Restore	YES	Support backup & restore in HiveMQ control center.
Trace Recordings	YES	1. Support filtering logs for ClientID or Topic. 2. Support various types of MQTT message log tracing.
Overload Protection	YES	1. Support rate limit on connection, publishing. 2. Support different overload protect levels for each node. 3. Support load balancing of nodes in a cluster.
MQTT Broker Runtime Logs	YES	1. Support 5 levels of logs. Different levels of logs can be stored separately, which is efficient to manage. 2. Support 2 output formats: console and file. 3. Default longest storage time is 30 days. 4. Clear log format. 5. Efficient hierarchical log system based on log level and log handlers. 6. Support modifying log levels at runtime. 7. Support log management through external extension.
Debugging and Trouble Shooting	YES	24/7 Support
Development and Future Expansion: To be confirmed by HiveMQ and EMSD (This should be considered in future contract)		
Supporting Resources: 1. Online Manuals: Sufficient online documents from HiveMQ official website in English. 2. Offline Resources: E HiveMQ mainly provides user manual, benchmark report to introduce HiveMQ. HiveMQ also provides related knowledge about MQTT protocol. 3. Sources Codes: In Github (community edition) 4. Tutorials: A large number of configuration templates in google, etc.		

5. Training courses: It is better for EMSD and HiveMQ to arrange a training course for HiveMQ Enterprise broker.
System Support Services: (To be confirmed by HiveMQ) 1. Team Support: Yes/No 2. Location of Support Team: 3. Remote Support or On-site Support: 4. Customized Functionality Support: Yes/No 5. Delivery Method: 6. Development and Deployment Support: Yes 7. Debugging and Trouble Shooting Method:
Pricing Model: (From HiveMQ) List price for 3 nodes at 4 CPUs would be117.600 EUR, but for a government organization and if this really for purchase in Sept, I have approval to offer this for 88.200 EUR per annum in case of a commitment for a longer term, e.g. 3 years there is some more flexibility that we can discuss.

HiveMQ Enterprise Features Summary (Including advantages and disadvantages):

1) HiveMQ Enterprise is based on Java which is a mature development language and there is large number of Java engineers in market.

2) HiveMQ Enterprise supports good redundancy design with various fault solutions.

3) HiveMQ Enterprise dashboard integrates most major functionalities of MQTT broker, which is very convenient for EMSD management.

4) HiveMQ Enterprise Kafka Extension is the only pre-built solution ready to use from HiveMQ.

5) HiveMQ Enterprise supports fine-grained ACLs, but the ACL rules are set through XML format, which is complex and not convenient for managers to configure.

6) Sufficient Online and Offline resources are provided by HiveMQ.

3. VerneMQ

Table 36. Basic Information of VerneMQ

MQTT Broker Information	Records
MQTT Broker Name	VerneMQ
Software License	Open Source Software (Enable enterprise support contracts)
Country of Origin	Switzerland

Development Language	Erlang
Platform Support	Linux, MacOS, Docker, Public Cloud, Private Cloud, Physical Server (does not support Windows)
Latest Release	V1.10.3
On-Premise Option	Yes
Partners	The VerneMQ has used by multiple enterprises, such as Microsoft, Volkswagen, Arduino, etc.

Table 37. Protocol Compliance of VerneMQ

Compliance	Records
MQTT Protocol Version	MQTT Protocol V3.1.1, V5.0 (V5.0 is the latest version)
Security Policy	TLS/SSL one-way/two-ways authentication. SSL/TLS supports for all protocols supported by VerneMQ
Connection Methods	TCP, Websocket, TCP/SSL, Websocket/SSL

Table 38. Functionality of VerneMQ

Functionality	Yes/No	Remarks
IoT Protocol Support	YES	Supported IoT protocols: LoRaWAN, NB-IoT, WiFi, 2G/3G/4G, 5G, etc.
QoS Support	YES	QoS Levels: QoS0, QoS1, QoS2
Retained Message	YES	1. The retained messages could be stored in RAM, and could be viewed in terminal. 2. Configurable maximum number of retained message, configurable

		maximum payload size, configurable expiration time.
Persistence	YES	Support data persistence in Redis and databases (i.e. MySQL, PostgreSQL, MongoDB, CockroachDB).
Last Will and Testament	YES	Will Messages include will topics, will payload.
*Shared Subscription	YES	Support shared subscription with three message distribution policies (prefer_local, random, and local_only)
*Database Extension	YES	Support various databases, including MySQL, PostgreSQL, MongoDB, CockroachDB.
*Bridge	YES	Support bridges, including other VerneMQ nodes, and other MQTT brokers (e.g. Mosquitto, EMQ X, etc.)
*Additional Functionalities Support HTTP API and Webhooks for integration VerneMQ with external system.		

*(*denotes advanced functionalities)*

Table 39. Redundancy Design of VerneMQ

Services	Yes/No	Remarks
Clustering	YES	1. Support manual and k8s clustering. 2. Support scalability. It is easy to add or remove nodes in a cluster without stopping the service. 3. Support infrastructure outage scheme. Even if parts of the cluster fail, the cluster system as a whole could be available to avoid service interruptions. 4. Network outage can lead to partition, VerneMQ supports recovery from a Netsplit.
Load Balancer	YES	Support external load balancers that provided by the cloud provider

Performance Evaluation and Deployment Suggestions: 1. Single VerneMQ node can handle 1 million connections. (To be confirmed by VerneMQ).

Table 40. Management & Maintenance of VerneMQ

Services	Yes/No	Remarks
Authentication	YES	VerneMQ supports various types of authentications, including basic built-in MQTT-based authentication (username/Client ID), authentication of external common databases (i.e. MySQL, PostgreSQL, MongoDB, CockroachDB), and HTTP authentication, which ensures the security from multi-level authentications.
Access Control	YES	1. Support ACL through ACL plugins. 2. Support built-in Publish/Subscribe ACL. The ACL rules are based on a simple logic, which is easy to set. The ACL rules could define global rules for all clients and specific rules for each client through username or client ID. Note that the ACL rule is just based on ALLOW rule (DENY is not included). 3. Support various external database ACLs, such as MySQL ACL, PostgreSQL ACL, Redis ACL, MongoDB ACL, CockroachDB ACL. These database ACLs follow similar logic, which is easy to define. 4. Support HTTP ACL.
Dashboard	NO	Need to integrate Netdata Agent for data visualization
Message Processing Management	YES	Support efficient message processing scheme through Message Queue.

Backup & Restore	YES	Support backup data in local storage.
Trace Recordings	YES	Support filtering logs for ClientID
Overload Protection	YES	1. Support rate limit on connection, publishing, which avoids system overload from the entrance and guarantees system stability and predictable throughput. 2. Support load balancing of nodes in a cluster.
MQTT Broker Runtime Logs	YES	1. Support 4 levels of logs. 2. Support 2 output formats: console and file. 3. Clear log format. 4. Efficient hierarchical log system based on log level.
Debugging and Trouble Shooting		To be confirmed by VerneMQ
Development and Future Expansion: To be confirmed by VerneMQ and EMSD (This should be considered in future contract)		
Supporting Resources: 1. Online Manuals: Online documents are available in VerneMQ official website in English. 2. Offline Resources: To be confirmed by VerneMQ. 3. Sources Codes: Open-source code in Github 4. Tutorials: There are less VerneMQ configuration templates in google 5. Training courses: It is better for EMSD and VerneMQ to arrange a training course.		
System Support Services: (To be confirmed by VerneMQ) 1. Team Support: Yes/No 2. Location of Support Team: 3. Remote Support or On-site Support: 4. Customized Functionality Support: 5. Delivery Method: An pre-configure, optimised package with added functionality (like a realtime observer plugin), but it uses the same open-source license. 6. Development and Deployment Support: Yes/No 7. Debugging and Trouble Shooting Method:		
Pricing Model: The subscription to the pre-compiled installer packages with added functionality is 1500 CHF (swiss francs) per server per year. (This comes without support, but support can be added to package subscriptions.)		

VerneMQ Features Summary (Including advantages and disadvantages):

1) VerneMQ is based on Erlang which is a great technology currently available to build highly scalable messaging systems.

2) VerneMQ supports good redundancy design with various fault solutions.

3) VerneMQ does not have pre-built dashboard. Need to integrate Netdata Agent for data visualization.

4) VerneMQ supports various databases extensions, which provides high flexibility for database integration.

5) VerneMQ has simple ACL logic and is convenient for managers to perform individual or global control.

6) There are less VerneMQ configuration templates and tutorials online.

4. Mosquitto

There are no management services provided by Mosquitto, hence it is not suggested to be deployed for enterprise-level service. The main features of Mosquitto is addressed as following:

1) Mosquitto is the most common open-source MQTT broker. There are a variety of tutorials and blogs for users.

2) Mosquitto does not support clustering and load balancing, which is likely to have single point of failure.

3) Mosuqitto does not have management services and there is no dashboard support, which is unfriendly for user management.

4) Mosquitto needs external bridges to support databases extensions, which is not convenient to configure.

5) Mosquitto has simple ACL logic and is convenient for managers to perform individual or global control.

d. Evaluation result

1. All the four MQTT Brokers could perform normal MQTT services. But some of them could not meet the enterprise-level requirements.

2. The evaluation is based on four properties, which are MQTT Broker Basic Features, Functionality Supports, Redundancy Design, and Management & Maintenance. Each property occupies 25% marks.

3. For each evaluation property: Perfect (5) Good (4) Fair (3) Average (2) Not Provide (1)

Table 41. MQTT Broker Evaluation Marks

Items / LNS	MQTT Broker Basic Features	Functionality Supports	Redundancy Design	Management & Maintenance	Overall Grades
EMQ X Enterprise	**5**	**4**	**5**	**5**	**4.75**
HiveMQ Enterprise	5	4	5	3	4.25
VerneMQ	5	4	5	2	3.75
Mosquitto	5	2	1	1	2.25

From the overall marking, **EMQ X Enterprise** could be the MQTT Broker recommendation for enterprise GWIN architecture.

VI. GWIN System Standardization Guidelines

GWIN provides complete system infrastructure for LPWAN applications. Standard compliance will facilitate the growth of GWIN infrastructure and its peripherals that the future GWIN applications and/or IoT objects can be integrated with the GWIN efficiently. To maximize the utilization of GWIN and ensure the effectiveness of GWIN applications, a series of GWIN standards are defined, including IEEE P2668 standards and GWIN general requirements. The IEEE P2668 standard, as the global IoT evaluation standard, provides a unified quantitative method to evaluate LPWAN technologies and select the most suitable LPWA candidate for a specific application. GWIN general requirements provide fair and secure guarantees for each GWIN user.

A. IEEE P2668 Standard on LPWAN Technologies Evaluation

IEEE P2668 standard is the first global standard to evaluate, grade, and rank the performance of IoT objects by using quantitative indicator values, namely IoT Index (IDex) [14]. IDex shall classify the objects into five levels (from lowest level 1 to the highest level 5) of performance. For GWIN system, the idea of IDex is utilized to provide a numerical comparison among LPWAN technologies (i.e., LoRa, NB-IoT, Sigfox) from the perspective of application requirements. With the IDex, a comprehensively quantified evaluation of the various applied LPWAN technologies regarding the application can be obtained. In this part, key performance metrics for LPWAN technology evaluation are summarized, unified evaluation methodology is proposed, and a case study for intelligent parking system is implemented.

a. LPWAN Technologies Evaluation Criteria

Internet of Things (IoT) based applications, has become one of the most essential parts in building smart city worldwide. In smart city, as the number of IoT users increases, Large coverage is required to achieve the best performance. Low Power Wide Area Network (LPWAN), as a branch of Internet of Things (IoT) technology, is an alternative to fulfill this requirement. Since 2013, several organizations and industrial consortia have created more than 10 LPWAN technologies in both licensed and unlicensed frequency bandwidth. These technologies are competitive in the market and generate selection problems for developers. Heterogeneous LPWAN technologies share similar key superiorities such as long-range, low-power operation, low hardware cost, and massive device capacity. However, their differences in protocol design have resulted in different technical specifications.

Thus, in IEEE P2668 standard, a LPWAN Index, namely LPWAN-I is proposed to quantitatively evaluate the applicability of LPWANs and select the most suitable LPWAN candidate for a specific application.

The LPWAN-I provides two-fold guidance to developers who consider adopting LPWANs. First, it can estimate the applicability of LPWANs for a specific application based on three applicable factors. Second, it can select the most suitable candidate for the application based on another four IoT success factors, as LPWAN Performance Index.

The applicable factors are designed to identify the key features that may not be provided by LPWANs. Generally, LPWANs have obtained advanced properties at the

expense of data rate, latency, and reliability. Therefore, they are defined as the applicable factors.

Latency is defined as the time interval between the data collection at the end device and the data aggregation at the server.

Reliability is defined as the likelihood that a packet transmitted in the network layer is lost from either unacceptable delay or noise. Thus, reliability is identified by the packet loss rate (PLR), which is impacted by the interference, channel occupancy conflicts, and environmen- tal dynamics.

Data capacity refers to the maximum amount of data that can be transmitted by each end device each day.

Developers will index the requirements of the target application pertaining to the three factors. **Once there is a factor with index 3 or higher, LPWANs may not be applicable in this application.** It is thus seen that, by using the applicability index, developers can easily determine whether to adopt LPWANs based on the application's demands.

Table 42. List of applicability index [47]

Index	Latency (l)	PLR (p)	Data capacity (C)	LPWAN
1	More than 10 s	More than 10^{-1}	Less than 1680 B	Yes
2	Less than 10 s	Less than 10^{-1}	Less than 13.18 Mb	Yes
3	Less than 1 s	Less than 10^{-2}	Less than 100 Mb	No
4	Less than 100 ms	Less than 10^{-5}	Less than 1 GB	No
5	Less than 10 ms	Less than 10^{-7}	More than 1 GB	No

The LPWAN Performance Index is defined to quantitatively rank the performance of different LPWANs on each factor. The metrics of the LPWAN performance index are shown in the table as below.

Table 43. List of LPWAN performance index [47]

Index	Network practical simplicity		Long-term cost efficiency		Feasibility			Information security		
	Self-simplicity	Application scale (per BS)	Service fee	Updated on air	End device feasibility	Environmental feasibility	Interoperability	C.	I.	A.
1	Low	Floor-wide or smaller	Yes	No	No	No	No	No	No	No
2	Low	Building-wide	No	No	No	Yes	No	No	Yes	No
3	Middle	Building-wide	Yes	Yes	Yes	No	No	Yes	No	No
4	Middle	City-wide	No	Yes	Yes	Yes	No	Yes	Yes	No
5	High	City-wide	No	Yes (automatic)	Yes	Yes	Yes	Yes	Yes	Yes

Network practical simplicity illustrates the amount of effort (mainly manpower)

demanded by the developer to construct the network. The ranking of this factor falls into two aspects, namely self-simplicity and application scale. Self-simplicity reflects the effort that will be devoted to the network infrastructure. The higher the self-simplicty, the less effort will be required.

Application scale refers to the target area of the common applications which can be classified as floor-wide, building-wide, and city-wide.

Long-term cost efficiency describes the amount of long-term cost after a network has been deployed. This factor consists of two terms, namely the service fees and the allowance of the update on air. Generally, if a network is a public network (provided by a service provider), the adopter may need to pay the operator service fee according to the amount of data transmission. On the con- trary, if a network is an adopter's private network (self-build), no service fee will be charged.

Feasibility is an assessment of the practicality of LPWANs in an application. It is divided into end device feasibility, environmental feasibility, and interoperability. Various scenarios in the application may demand different specifications. Thus, device feasibility refers to the working mode of end devices that is adjustable and based on the application's demands. Environmental feasibility refers to the adaptability of LPWANs in various complex environments, such as the outdoor and deep indoor environments. Interoperability identifies the ability for systems or components of systems to communicate with each other, regardless of their manufacturer or technical specifications.

Information security identifies the strength of the data protection in LPWANs. It should be noted that, given the low-power-consumption and low-storage design, the strength of the security protection in LPWANs is nowhere near the strength of the protection on the Internet. Therefore, this estimation is focused on whether the LPWAN has protection on information security rather than the strengths of different protections. Information security falls into three categories: confidentiality, integrity, and availability.

Based on these criteria, the LPWAN-I value for common LPWANs can be derived as follows.

Table 44. The ranking results of various LPWANs [47]

Success factors	NB-IoT	Sigfox	Weightless-P	Dash7	LoRa
Network practical simplicity	4	4	3 (public) 2 (private)	1	4
Long-term cost efficiency	3	1	3 (public) 4 (private)	3	3
Feasibility	3	1	1 (public) 2 (private)	4	3
Information security	4	3	4	4	4

For different applications, the consideration priority of each factor varies accordingly.

Therefore, the weighting of each factor should be estimated by considering the condition of the target application. In LPWAN-I, weightings of success factors are estimated with the ana- lytic hierarchy process (AHP), which derives weighting through pairwise comparisons between every criterion pair. The developer needs to consider the target application and quantize the importance level of every pair of factors with discrete 9-point AHP scales. These estimated importance levels will form a criteria comparison matrix.

After checking the consistency of the matrix, the normalized eigenvector corresponding to the largest eigenvalue of the matrix is the estimated weighting vector. This weighting vector reflects the factors' priorities of the target application.

Based on this general evaluation method for LPWAN technologies, a case study of intelligent parking system is provided for illustration.

b. Case Study of Intelligent Parking System

Parking sensors play an essential role in the smart parking system, which has been proposed as an effective solution to achieve intelligent management of the parking lots. The parking sensor could achieve continuous and automatic monitoring of the occupied/free status of the parking space spots. The sensors will collect the detection signals and transmit the message to the server through wireless communication techniques (in this case, they are LPWAN technologies). Then, the parking lot manager is able to understand the usage situation of parking lots expediently by checking the received information on the server. To achieve this object, the LPWAN technology that brings better performance in this application should be determined.

In terms of the intelligent parking system, the evaluation mainly consists of four main steps, i.e., the survey of candidate LPWAN technologies, the identification of key indicators of LPWAN comparison, the weighting allocation of identified indicators, and the final determination of the most suitable LPWAN technology.

1. Survey of candidate LPWAN technologies

Nowadays, various kinds of LPWAN technologies have been developed. Among them, the most popular ones which account for most of the market are LoRa, Sigfox, and NB-IoT. Evaluation on each indicator for each candidate should be made and a grade is given for each aspect. In practice, the candidates depend on the determination of users.

2. Identification of key indicators of LPWAN comparison

In this implementation, combining comments from CityU and EMSD, six key indicators are identified for intelligent parking system, i.e., (a) Network Coverage and Capacity, (b) Data transmission and data accuracyNetwork performance, (c) Sensor performance, (d) Power consumption, (e) Security, (f) Cost. Proper adjustments could be adopted in the practical application if needed.

3. Weighting allocation of identified indicators

According to the application requirement, various weightings are allocated for these six indicators. Prior indicators that users focus on should own a higher weighting

4. Final determination of the most suitable LPWAN technology

The final score for each candidate LPWAN technology is calculated by the addition of the product of the grade of each aspect and the weighting, i.e.,

$$\text{Final score} = S_{1,a} * W_{1,a} + S_{2,a} * W_{2,a} + \ldots + S_{i,a} * W_{i,a} \quad (1)$$

where $S_{i,a}$ denotes the Score for the indicator i for technology a and $W_{i,a}$ denotes the weighting for the aspect i.

The candidate with the highest final score will be decided as the most suitable one.

The evaluation details of intelligent parking system is decribed as follows:

1. Survey of candidate LPWAN technologies

The candidate LPWAN technologies in this application are LoRaWAN, Sigfox, and NB-IoT.

1.1 LoRaWAN

LoRa is an open wireless standard that works on the unlicensed frequency band. Different frequency plans are defined for different countries and regions. Hong Kong utilizes AS923-1 frequency plan with 920-925MHz frequency band [11]. The detailed network stack protocol is presented as LoRaWAN proposed by LoRa Alliance. LoRaWAN is developed based on LoRa physical layer and modulation technique which creates a long-range communication link. LoRa utilizes chirp spread spectrum (CSS) modulation which maintains the same low power characteristics as FSK modulation but significantly increases the communication range. The average communication range is commonly agreed on as 5km in urban areas and 20km in rural environments [15]. According to the requirements of specific IoT applications, the practical range can be adjusted through configuring LoRa modulation parameters. These parameters are spreading factor (SF), data rate, and bandwidth. In Hong Kong, 125kHz and 250kHz bandwidths are used in practice [16]. SF determines the number of chirps that are transmitted per second. The SF value can be selected from SF7 to SF12. Lower SF implies more chirps can be transmitted per second. Hence, the effective data rate will be higher and airtime will be shortened. Conversely, higher SF indicates that fewer chirps can be sent per second, hence, the effective data rate will be lower and airtime will be extended, but the communication range will be longer. The choice of SF value is a trade-off between communication range and data rate. All these settings increase the capacity and scalability of LoRaWAN network

- Flexible network establishment

The LoRaWAN could be established privately without Internet Service Providers (ISP). It saves a cost on subscription and management fees although there will be an extra cost on gateway purchase. As a whole, the cost of LoRaWAN network establishment decreases. The details could refer to the introduction on cost. Besides, since the LoRaWAN gateways are deployed by users themselves, it is more flexible to use LoRaWAN network comparing to other networks that need service from ISP. The users could deploy the gateway at the most suitable sites, which makes most devices available

to transmit and receive high-quality signals. The ability of flexible network establishment is a unique advantage of LoRaWAN.

- Adaptive data rate

The adaptive data rate (ADR) is a unique function of LoRaWAN which makes the communication achieve optimal performance. It is dependent on SF. The SF value can be selected from SF7 to SF12. Lower SF implies more chirps can be transmitted per second, thus, the effective data rate will be higher and airtime will be shortened opening up more potential space for other nodes to transmit. The ADR also optimizes the battery lifetime of a node. All these settings increase the capacity and scalability of LoRaWAN network. The function of ADR is also available to choose the maximum data rate automatically under an acceptable signal-to-noise ratio (SNR). ADR is another unique advantage for LoRaWAN network. The theoretical bit rate Rb of LoRaWAN is shown in equation (2) [17]:

$$R_b = sf * \frac{bw}{2^{sf}} * cr \tag{2}$$

where bw represents the bandwidth and sf indicates the spreading factor. There are 2^{sf} chirps in a LoRa symbol in which the chirp rate equals bandwidth. cr indicates the forward error correction code rates that LoRa supports.

- Three Device Classes

In LoRaWAN specification, end devices are divided into three classes A, B, C. In class A, each uplink message is followed by two short downlink slots., In class B, devices open an extra downlink slot compared with class A. In Class C, devices are operated in constant receiving mode. The benefit of class C is continuous downlink communication. As a cost, the power consumption is high. For most IoT applications, class A is the optimal choice considering the low power consumption.

Bi-directional end-devices (Class A): Class A devices allow bi-directional communication. Each device has two short downlink reception windows following an uplink transmission. The planned transmission slot is designed based on the communication requirements and random time with a small change (Aloha type protocol). Class A provides the lowest power consumption for these applications that only perform downlink communication from the server shortly after the terminal device sends an uplink transmission. Downlink communications from the server will have to wait for the next scheduled uplink. Class A defines the default function mode of the LoRaWAN network and must be supported by all LoRaWAN devices.

Bi-directional end-devices with scheduled receive slots (Class B): Class B devices allow an additional receiving window. For the devices which open their receiving window at a predetermined time, they receive a time synchronization beacon from the gateway. Class B is utilized to decouple upstream and downstream transmissions.

Bi-directional end-devices with maximal receive slots (Class C): The receiving window of the Class C device is opened almost continuously, and only closed when making a transmission. Class C devices need more power to operate compared to Class A or Class B. As a reward, they own the lowest latency for server-to-terminal communication.

- LoRaWAN security [18]

Table 45. Summary of LoRaWAN V1.1 parameters and keys

Name	Type	Description
DevAddr	Address	Device Network Address. Involves a prefix from NS identifier
AppKey	Root Key	Specific device root key; In OTAA, used to derive Application Session Key
NwkKey	Root Key	Specific device root key (updated in LoRaWAN V1.1); In OTAA, used to derive Network Section Keys
AppSKey	Session Key	Used to encrypt or decrypt application payloads
NwkSEncKey	Session Key	Network Session Encryption Key. Used to encrypt or decrypt MAC payloads.
FNwkSIntKey	Session Key	Forwarding Network Session Integrity Key. Used for message integrity code of uplink messages
SNwkSIntKey	Session Key	Severing Network Session Integrity Key. Used for message integrity code of downlink messages

In LoRaWAN, the security of data transmission is ensured by the Advanced Encryption Standard (AES) using 128-bit encryption keys and algorithms. One point to note about security in LoRaWAN V 1.1 is that by using two separate keys, network trust and application trust are completely separated. The parameters are summarized in Table 1. Each LoRaWAN device is personalized with a unique 128 bit AES key (called AppKey) and a globally unique identifier (EUI-64-based DevEUI), both of which are used during the device authentication process. Moreover, the keys are specific to each device, and disclosure of these keys should only affect terminal devices. A message integrity code (MID) is generated and verified using the network session key. The MID could guarantee the integrity of the message by creating a unique signature for each device.

In terms of Activation by Personalization (ABP) and Over-the-Air-Activation (OTAA) end

devices, LoRaWAN provides different authentication keys. Device root keys (AppKey & NwkKey) are AES-128-bit keys in IEEE 802.15.4. Devices that only support ABP mode do not need NwkKey and Appkey, but they are needed in OTAA mode. In OTAA mode, NwkKey is used to generate FNwkSIntKey, SNwkSIntKey, and NwkSEncKey, and AppKey is used to generate AppSKey. After activation, the terminal can get information: DevAddr NwkSEncKey SNwkSIntKey FNwkSIntKey and AppSKey.

1) ABP. There are two key distribution methods in ABP. The first is that the manufacturer puts the session key from a predefined pool key to the terminal device (determined by a unique serial number (such as DevEUI)). The second is that the application manager manually distributes them to terminal devices and servers. The security of ABP deployment is reduced because ABP devices often use the same session key during their life cycle (the device can be manually reconfigured). In ABP, the terminal device only needs to configure the required network (NwkSEncKey, SNwkSIntKey, FNwkSIntKey) and application (AppSKey) session key

2) OTAA. OTAA is the recommended one of the two activation methods. It provides a flexible and secure method to establish a session key with the server. The terminal device transmits the join_request message to be processed by the Network Server (NS), which verifies it with the help of Join Server (JS) and responds with the join_accept message. Using two device-specific root keys (NwkKey and AppKey and the information in the join_accept message, terminal devices derive their session keys. Note that now the network session key comes from the root key of NwkKey, and the application session key comes from the root key of AppKey.

1.2 Sigfox

Sigfox is another well-known LPWAN technology developed by a French company. So far, Sigfox network has been deployed in about 70 countries, covering an area of 5 million square kilometers [19]. Sigfox also works in this unauthorized band. Sigfox's frequency band ranges from 862 to 928 MHz. Sigfox divides the global region into 7 regions, RC1 to RC7 [20]. Each area specifies different operating rules for Sigfox devices, including frequency range, data rate, multiple access mechanisms, and hardware specifications. In Hong Kong, Sigfox devices operate on RC4 with 920.8MHz uplink frequency and 922.3 MHz downlink frequency. The data rate of RC4 upstream and downstream transmission is 600 bps. Sigfox uses a lightweight protocol to implement short message transmission to ensure low power consumption. This lightweight protocol usually limits up to 140 upstream transmissions per day with a maximum of 12 bytes of payload and a maximum of 28 bytes of downstream transmissions for upstream recognition only [21]. The users could request the downlink through the server. But only 4 downlinks could be done each day. The frequency hopping used in RC4 allows each message frame to be broadcast three times on different frequencies. Besides, the second transmission can be performed after 20 seconds. Therefore, the delivery of the package can be ensured. Sigfox utilizes Ultra Narrow Band (UNB)

modulation with 100Hz bandwidth, which leads to ultra-low noise levels. Hence, long-distance transmission against noise at the transmitter end and high sensitivity at the receiver end can be achieved.

- Sigfox security:

A conflict exists between the literature studies and Sigfox official website regarding the Sigfox security mechanism [22][23]. Some researches indicate that Sigfox has no encryption mechanism [15] while the official website declares that optional AES-128 encryption is supportive based on device key [23]. Users could determine whether to enable this function themselves. A security risk will emerge if they choose to disable it. In Sigfox security mechanism, the main components involve over-the-air uplink security, over-the-air downlink security, and payload encryption [23]. The air security of the uplink implements several mechanisms: a message counter for replay attack protection, AES128 in CBC mode for authentication and integrity checking, and CRC-16 for error detection. The air security of the downlink implements the following mechanisms: AES128 is used for identity verification and integrity checking, BCH is used for error correction, and CRC-8 is used for error detection. Payload encryption is a process of encrypting the payload of application information over the air in uplink and downlink communications. It uses the CTR encryption key in AES128 algorithm mode, which is unique for each device.

1.3 NB-IoT

NB-IoT is a wireless technology based on a cellular network proposed by 3GPP to meet requirements of large coverage and low power consumption [25]. At present, NB-IoT has achieved billions of device connectivity supported by more than 30 ISP worldwide [22]. These ISPs can simply deploy the NB-IoT network on the existing network architecture with slight firmware modification, which facilitates the NB-IoT developing process. In Hong Kong, China Mobile has achieved NB-IoT network deployment in licensed band B3 (1800MHz) and B8 (900MHz). There are 12 subcarriers inside the channel and each subcarrier is separated by 15 kHz. NB-IoT uses single carrier frequency division multiple access (SC-FDMA) modulation and orthogonal frequency division multiple access (OFDM) modulation for uplink and downlink transmissions. This makes large connections and reliable two-way communication possible. Since it is deployed in the licensed band, NB-IoT has a relatively large throughput, which enables device firmware to be updated over the air. The NB-IoT uplink effective data rate is 0.5-140kbps, and the downlink effective data rate is 0.3- 125kbps. Besides, NB-IoT benefits from a licensed band with no duty cycle restrictions. But the disadvantage is the high deployment cost of narrowband IoT. The 128-256 bit encryption defined by 3GPP ensures the security of the Internet of Things [24]. To reduce power consumption, NB-IoT uses Power Saving Mode (PSM) and Extended Discontinuous Reception (eDRX) [26]. A device using PSM gets into a deep sleep and cannot be reached. A re-connection is unnecessary for PSM mode because devices are still registered with the network, which

not only saves energy but also avoids traffic congestion. The periodicity of receiving mode of eDRX is reduced for an NB-IoT device. Meanwhile, the sleep cycle is further extended in idle mode than in connected mode. According to the developing guideline of NB-IoT, a re-connection of the device to the network should not be designed in a robust way to prevent looping [27]. Otherwise, a constant re-connection by huge numbers of devices may lead to a signal storm. Besides, the Handover mechanism has been removed from NB-IoT for saving energy [24].

- Three deployment modes

NB-IoT has three network deployment methods: in-band, guard-band, and stand-alone [24]. For the in-band method, NB-IoT spectrum is deployed inside the LTE spectrum band with 180kHz bandwidth which is one resource block of an LTE channel. For guard-band deployment, the 180kHz NB-IoT spectrum is placed by ISPs in the existing LTE signal's guard bands. It is proved that better downlink performance could be achieved by adopting a guard-band mode [25]. NB-IoT spectrum can also be entirely separated from the existing LTE spectrum in a stand-alone solution. These deployment methods achieve great spectral efficiency for licensed bands.

- NB-IoT security:

Since NB-IoT is a technology that uses the LTE spectrum for data transmission, it inherits the security mechanisms for confidentiality and authentication from LTE networks. The perception layer (i.e, one of the layers of IoT architecture, involving a series of sensors that identify things and collect information) could be vulnerable to various kinds of attacks on data confidentiality, integrity, and authenticity. LTE provides symmetric encryption and signature mechanisms to prevent data leakage and uses SIM cards to authenticate and identify devices in the network [28].

These three LPWAN technologies all utilize similar network topology (star topology) to deploy network architecture. The network architecture is composed of end nodes, base station/gateway, network server, and application server. In an LPWAN network, each end node does not connect to a specific gateway. Instead, sensor data collected by a node are transmitted to multiple base stations/gateways through radio links. These base stations/gateways forward the received sensor data to the network server. The communication link between the base station/gateway and network server can be backhaul, cellular, Ethernet, satellite, or Wi-Fi. The network server is responsible for packet management, security check, and acknowledgment. The application server is responsible for data accessing from a network server and implementing specific functions. Compared with NB-IoT and Sigfox deployed in a public platform, LoRaWAN network architecture can be deployed both in public and private ways, which enables individuals and public organizations to offer service for their purposes.

2. Identification of key indicators of LPWAN comparison

In this case study, six key indicators are evaluated: (a) Network Coverage and Capacity, (b) Network performance, (c) Sensor performance, (d) Power consumption, (e) Security, (f) Cost.

2.1 Network Coverage and Capacity

Network Coverage and Capacity is a significant factor to deploy an optimal network. The coverage could be indicated by the link budget, transmission power, etc. A larger link budget makes the signal own a larger transmission distance. A link budget considering all the gains and losses between the transmitter to the receiver. It includes free space, cable, waveguide, fiber, etc. It could be represented by an equation (3) below [29]

$$\mathrm{P}_{RX} = \mathrm{P}_{TX} + G_{TX} - L_{TX} - L_{FS} - L_{M} + G_{RX} - L_{RX} \quad (3)$$

P_{RX} = received power (dBm)

P_{TX} = transmitter output power (dBm)

G_{TX} = transmitter antenna gain (dBi)

L_{TX} = transmitter losses (coax, connectors...) (dB)

L_{FS} = path loss, usually free space loss (dB)

L_{M} = miscellaneous losses (fading margin, body loss, polarization mismatch, other losses...) (dB)

G_{RX} = receiver antenna gain (dBi)

L_{RX} = receiver losses (connectors...) (dB)

Besides, the coverage is related to the modulation scheme. As is discussed previously, technology using a lower data rate could distribute more energy on power transmission, which enables a larger range. Thus, the coverage is a comprehensive study on transmission power, link budget, receive sensitivity, etc. Considering this, practical coverage results could provide more convincing results. In this case, previous studies on coverage of three LPWAN could provide a significant reference.

The network capacity reflects the amount of traffic that a network could handle during a given period [30]. It could be quantified as the maximum number of supported end devices for each base station [31].

2.2 Network Performance

Network performance could be indicated by two main features, i.e., data transmission and data accuracy. The data rate, payload length, and latency are involved as the main indicators in reflecting the performance of data transmission. The higher data rate enables more devices to transmit more information, which improves the data transmission ability. A larger payload size makes more information transmitted in one turn. Latency is the basic parameter for LPWAN design and is significant for critical applications. The value of latency has a great influence on the efficiency of LPWAN applications.

The data accuracy represents the success rate of the data to be transmitted from the sensor to the server, which could be indicated by packet loss rate, and packet error rate. The former represents the ratio of the number of lost packets to the total transmitted number. The latter denotes the ratio of the number of inaccurate received data to that of the total received data. In this report, the data accuracy is discussed along with the sensor performance. The evaluation results of data accuracy and sensor performance are represented by the indicator, detection accuracy (i.e., the ratio of the number of accurate detection results to the total detection results).

2.3 Sensor Performance

Sensor performance is the most intuitive manifestation of LPWAN application performance. In current EMSD applications, sensor performance is compared using parking sensors with three LPWAN techniques. As is discussed in previous sections, the best candidate should be selected based on the requirement of users of the applications. For parking sensors, the most important indicators are set as Accuracy Rate (AR), and Response Time (RT). The AR decides the basic performance of parking sensors. After all, the main function of parking sensors is to detect the status of parking lots correctly. Then, RT indicates the time interval between the time slot when the vehicles park in the parking space and the time slot when the server receives the message. RT is also an essential indicator of testing. If the RT is too long, the server may provide error information for users particularly when it is crowded in parking lots. For example, a parking lot is occupied by vehicle A. But before the server receives this message, the parking lot keeps showing free. A new coming driver may consider the parking lot is still empty based on information from the server. The time waste and matter is made when it is finally found that the parking lot has been occupied. A total of three parking sensors is included.

The normal operation workflow of the parking sensor is as follows. Firstly, vehicles or other magnetic subjects move into the parking lots. The occupied status could be detected by the parking sensors. The sensor then sends a message to the server through the applied wireless network (LoRaWAN/NB-IoT/Sigfox in this testing)

The testing parking sensors are listed in Table 463.

Table 46. Parking sensors evaluated in this testing [32]

Sensor name	NHR	CMHK	IoTPark
Applied technology	LoRaWAN	NB-IoT	Sigfox

Accuracy Rate (AR) is defined as the correct rate for the parking sensor to detect the occupied or free status of parking lots. It could be calculated by equations (4) and (5).

$$R_{in} = C_{in} / C_{tol} \times 100\% \quad (4)$$

$$R_{out} = C_{out} / C_{tol} \times 100\% \quad (5)$$

In the equations, Rin and Rout represent the AR for parking sensors to detect whether it is occupied or free respectively. Cin and Cout indicate the counts parking sensor detects the occupied and free status of the parking lot respectively.

Response Time (RT) is defined as The time interval between the time slot that the car is stopped stably and the time slot that the occupied state is shown on the parking state board (which acquires data from the server). It could be calculated by equations (6) and (7).

$$t_{in} = T_{in} - T_{show} \quad (6)$$

$$t_{out} = T_{out} - T_{show} \quad (7)$$

In the equations, tin and tout indicate RT when vehicles are occupying or leaving the parking lots. T_{in} and T_{out} indicate the time slot when vehicles are occupying or leaving the parking lots. As a more clear description, T_{in} is recorded when the parking sensor is blocked in the top view. T_{out} is recorded when the sensor is unblocked. T_{show} is the time slot of vehicle detection recorded by the server.

2.4 Power Consumption

The performance of power consumption is critical to battery-powered IoT terminal devices since unrealistic expenses will be spent on replacing batteries for large networks frequently. Many LPWAN applications, such as temperature & humidity sensors, are dedicated to maintaining the lowest power consumption to prolong the battery life of sensor devices. Since different operation statuses have different power consumption, the power value of main modes (peak, and sleep) should be considered. Besides, the working period for different modes, which decides the duty circle of each technology. For example, a longer sleep mode results in lower power consumption.

2.5 Security

Security of smart applications should be guaranteed to prevent data breaches and hacking because the transmitted data may link to personal information and privacy [33]. The details of security for each LPWAN technology have been depicted in the previous part. It is hard to compare the three security techniques directly. Based on the application requirement (for smart parking), three key security parameters, namely authentication, encryption, and network access are proposed. The authentication ensures that the data would not be changed when they are from the device to the cloud. Likewise, the cloud could also be guaranteed to the device that it is the true one. With encryption, the information can only be accessed by the cloud with decryption keys. The private network ensures information security. For specific, the company or organization that uses a private network could establish and ask members to connect to its internal network instead of the Internet.

2.6 Cost

Cost is one of the most essential factors that deserves deep consideration when making the selection. On the one hand, the budget for implementing a smart application

cannot be unlimited. Thus, the developer should make the plan with a cost lower than the budget cap. On the other hand, some products with better performance and higher prices may own a lower cost performance. For instance, a type of product has superior performance in some aspects which are not adequately important in the application. However, it costs a lot additionally. In this condition, the developer should seriously consider whether superior performance is necessary.

The cost is considered from the following aspects: sensor cost, gateway cost, installation cost, subscription cost, management cost, and sensor recurring cost. A total cost is calculated for each of the products for comparison.

3. Comparison of the six key indicators

The comparison is implemented based on theoretical analysis and experimental analysis, i.e., through a comprehensive analysis of the reliable information from the published references and the practical tests. The combination of theory and practice renders the persuasion of the comparison consequence.

In previous sections, the basic knowledge of the three LPWAN technologies has been described. To better distinguish the difference between the three technologies, a comparison table for theoretical analysis is listed as follows in Table 44. The comparison table depicts the three LPWAN technologies in terms of the basic information and the mentioned key indicators.

Table 47. Comparison of three LPWAN technologies [2] [15] [22] [24] [34] [35] [36] [37] [38]

Specification	LoRaWAN	Sigfox	NB-IoT
Technology	LoRa-Alliance	Proprietary	Open LTE
Standardization	LoRa-Alliance [2]	Sigfox company is collaborating with ETSI on the standardization of Sigfox-based network [2]	3 GPP [2]
Frequency bands	Unlicensed bands (920-925 MHz in HK)	Unlicensed band [920.8 MHz (UL) 922.3 MHz (DL) in HK]	Licensed band [900 MHz(B8) 1800 MHz(B3)] (for China Mobile HK)

Bandwidth	125, 250 kHz in practical [15]	100 Hz [15]	180 kHz [15]
Uplink Modulation	LoRa CSS [24]	DBPSK [24]	QPSK , BPSK [24]
Downlink Modulation	LoRa CSS [24]	GFSK [24]	QPSK [24]
Connectivity per cell	over 1,000,000 [24]	over 1,000,000[24]	52,547[24]
Maximum Payload Size	243 bytes [15]	12 bytes (UL), 8 bytes (DL) [15]	1600 bytes [15]
Maximum Date Rate	50 kbps [2]	100 bps [2]	200 kbps [2]
Pricing Model	Unlimited [15]	140 (UL), 4 (DL) [15]	Unlimited [15]
Transmission Power	14 (UL/DL)(Europe); 20-30 dBm (UL), 27 dBm(DL)(USA) [24]	14 dBm (UL) / 27 dBm(DL)(100bps); 22 dBm (UL), 30 dBm (DL) (600 bps) [24]	14 / 20-23 dBm [24]
Link Budget	154 dB [34]	163.3 dB [24]	155 dB (14 dBm), 164 dB (20 or 23 dBm) [24]
Uplink Sensitivity	-137 dBm [24]	-142 dBm (100bps) -134 dBm (600bps) [24]	LTE Tower Sensitivity [24]
Downlink Sensitivity	-137 dBm [24]	-130 dBm (100bps) -129 dBm (600bps) [24]	-141 dBm [24]

Number of channels*	10 (Hong Kong, Europe) 64+8+8 (USA) [35] [36]	400 (Europe) [22]	Depends on band used [37]
Encryption	AES-128 [24]	Light weight security (optional AES-128)[24]	3GPP 128-256 bit [24]
Network type	Public and private [2]	Public [2]	Public [2]
Range	5km (urban), 20km (rural) [15]	10km (urban), 40km (rural) [15]	1km (urban), 10km (rural) [15]
Peak current	32 mA [34]	30 mA [38]	120/130 mA [34]
Sleep current	1 μA [34]	6 nA [38]	5 μA [34]

Note: UL refers to uplink link, DL refers to downlink, HARQ refers to Hybrid automatic repeat request; UE refers to user equipment

**Typical values for "Number of channels" as reference*

Then it comes to the experimental analysis for the comparison

The LPWAN technologies are compared according to the mentioned six aspects, Network Coverage and Capacity, network performance, sensor performance, power consumption, security, and cost. It should be mentioned that the comparison is based on the experimental results and theory. Thus, in this part, the results of testing are given first. Then the comprehensive analysis between the three LPWAN technologies is given.

The results for coverage and capacity (connectivity per cell), network performance, power consumption can be found in Table 44.

For coverage, the typical coverage in the urban area for LoRaWAN, Sigfox, and NB-IoT are 5km, 10km, and 1km respectively according to the previous study. It could be concluded that Sigfox owns the best performance among the three technologies according to the range in previous studies. For capacity, it is indicated that Sigfox and

LoRaWAN are the potential to support one million devices while NB-IoT is available for about fifty thousand ones [24].

For data transmission, from Table 44 it could be seen that NB-IoT dominates in data rate and payload length. Besides, Sigfox has maximum data transmission limitation per day, which lowers its rating in this aspect. As for latency, NB-IoT offers the advantage of the low latency among the three technologies [15]. For LoRaWAN, Class C could also process low-bidirectional latency but the expense is the increased energy consumption.

The testing results of parking sensors are shown in Table 45. It could be seen that sensors from NHR reach the best performance on accuracy rate while sensors from CMHK own the shortest response time.

Table 48. The comparison of LPWAN sensor performance

Type	Accuracy rate	Response time/s (occupy)	Response time /s (leave)
NHR (LoRaWAN)	98%	30.00	21.00
CMHK (NB-IoT)	95%	15.22	12.89
Honoh (Sigfox)	90%	19.28	18.91

The peak power and sleep power for each technology are given in Table 44 separately. Besides, it should be mentioned that, since there is regular synchronization for NB-IoT, it consumes additional battery energy. OFDM or FDMA for NB-IoT also requires more peak current for transmitters [15]. Thus, it could be concluded that NB-IoT consumes the most energy among the three technologies. The power consumption of LoRaWAN and Sigfox is similar.

From Table 44, it could be reported that all of them support authentication, and encryption in reliable ways. LoRaWAN supports private networks so that it could block Internet attacks by using the private network. This feature enables LoRaWAN another available way to ensure security. However, from the whole perspective, it is hard to say which technology owns the best security mechanism.

An illustration of the cost for three LPWAN technologies is shown in Table 46. It could be checked that, among the three LPWAN technologies, the sensor cost of LoRaWAN is the lowest. But it is necessary to deploy gateways by users themselves when using LoRaWAN. For NB-IoT and Sigfox, since the service is provided by ISP, there is no need to purchase gateways. However, it is needed to submit a subscription fee for them each year. Besides, the deployment fee using LoRaWAN is much lower than using Sigfox and NB-IoT. Recurring cost for Sigfox and NB-IoT is also needed. As a result, LoRaWAN,

Sigfox, and NB-IoT based sensors will consume $639,200, $899,750, $1,095,000 in five years.

Table 49. The comparison among LPWAN technologies about cost [32]

Cost	LoRaWAN	Sigfox	NB-IoT
Sensor Cost	$2,200 per sensor	$2,199 per sensor	$2,880 per sensor
Gateway Cost	$22,300 per gateway	N/A	N/A
Sensor Network Subscription	No subscription fee	$120 / sensor /year	$100 / sensor / year
Data Management Platform	Included	$200,000	$250,000
Number of sensors for HQs	250	250	250
Number of gateways installed	4	N/A	N/A
Initial deployment cost (CAPEX) for 1st year	$446,700	$779,750	$995,000
Annual network subscription cost for 2nd to 5th year	No recurring cost	$30,000 / year	$25,000 / year
Total Cost for 5 years	**$639,200**	**$899,750**	**$1,095,000**

Remark: Sensors maintenance cost is excluded in the cost comparison

4. Weighting allocation of identified indicators.

A comprehensive analysis is done in terms of the mentioned six aspects: A1. Network Coverage and Capacity, A2. Network performance, A3. Sensor performance, A4. Power consumption, A5. Security, and A6. Cost. At first, a weighting allocation strategy based on the application requirement is given. It is a qualified method to illustrate the performance of LPWAN at each aspect. The analytic hierarchy process (AHP), a popular, effective, and practical tool dealing with complex decision issues, is employed to complete the weighting allocation process [39]. The developer needs to take into account the application requirements and to decide the importance of each factor, represented by a 9-point AHP scale. The 9-point AHP scale denotes the 9 relative importance levels between two factors. The relative importance level enhances as the

number gets larger. For specific, the relationship is as: 1 - indifference, 3 - moderate preference, 5 – strong preference, 7 – very strong or demonstrated preference, 9 – extreme preference. 2, 4, 6, 8, indicates the middle degree between the mentioned description [39].

In this case, a criteria comparison matrix is formed as follows.

$$A=\begin{bmatrix} 1 & 1 & \frac{1}{5} & \frac{1}{4} & \frac{1}{2} & \frac{1}{3} \\ 1 & 1 & \frac{1}{5} & \frac{1}{4} & \frac{1}{2} & \frac{1}{3} \\ 5 & 5 & 1 & 2 & 3 & 2 \\ 4 & 4 & \frac{1}{2} & 1 & 3 & 2 \\ 2 & 2 & \frac{1}{3} & \frac{1}{3} & 1 & \frac{1}{2} \\ 3 & 2 & \frac{1}{2} & \frac{1}{2} & 2 & 1 \end{bmatrix} \tag{8}$$

Or formulated as:

	A1	A2	A3	A4	A5	A6
A1	1	1	1/5	1/4	1/2	1/3
A2	1	1	1/5	1/4	1/2	1/3
A3	5	5	1	2	3	2
A4	4	4	1/2	1	3	2
A5	2	2	1/3	1/3	1	1/2
A6	3	2	1/2	1/2	2	1

The matrix list all relative importance levels between any two indicators. For example, A_{31} (Row 3 Column 1 in the matrix) = 5 means that the sensor performance is strongly important than network performance and capacity in this application. The justification is as follows.

If the consistency of the matrix is available, i.e., the importance level for each factor is not conflicted, the weighting strategy could be obtained by calculating the normalized eigenvector of the criteria matrix. Then, the weighting allocation strategy could be calculated. The weighting vector is as

$$W = [0.0603 \quad 0.0603 \quad 0.3518 \quad 0.2594 \quad 10.51 \quad 16.31] \tag{9}$$

The reasons for such a strategy are as follows. Firstly, the main function of the parking sensor is to detect the availability of parking lots. Thus, the most significant performance factor is the detection accuracy, i.e. sensor performance. Besides, if the application scale is large, the total cost to implement will be another important point. In this case, the cost for each parking sensor counts. Moreover, due to installation difficulty, it is not easy to change the parking sensors once installed. Hence, a longer usage period with no need for change will be profitable. Thus, the candidate with lower power consumption which results in a longer usage period will be more valuable. As for the difference in signal coverage and capacity, network performance, and security among the candidates are not identically important by comparison. Thus, they are not taken into consideration as the main concerns. It needs to point out that, the weighting allocation strategy is not unique. If there are other requirements, a more reasonable strategy should be designed. For example, assumes that the number of base stations/gateways is limited by local policy in the area of interest. To cover a large area by the network, the coverage and capacity of a gateway should be excellent. Then, the weighting of Network Coverage and Capacity turns higher in this allocation strategy.

5. Final determination of the most suitable LPWAN technology

The final comprehensive analysis of the three LPWAN technologies is given in Table 6. Besides, the performance for each technology is represented by numbers 1-3 (i.e., 1 indicates the poorer performance while 3 represents the better one). (In general, IDex set a 5-level matric for evaluation. Here a 3-level metric is customized to illustrate the difference between each LPWAN). The numbers are given based on theoretical analysis and experimental results mentioned in previous sections.

Table 50. The comprehensive analysis on LoRaWAN, Sigfox, NB-IoT based on theoretical and experimental results

	LoRaWAN	Sigfox	NB-IoT	Weight
Network Coverage and Capacity	2	3	1	6.03%
Network performance	2	1	3	6.03%
Sensor Performance	3	1	2	35.18%
Power consumption	3	3	1	25.94%

Security	3	2	3	10.51%
Cost	3	1	2	16.31%
Total	2.8794	1.6826	1.9076	100%

According to the comprehensive analysis, it is found that LoRaWAN achieves the best selection in parking sensor-based LPWAN comparison.

B. IEEE P2668 Standard on IoT Security

In this part, IEEE P2668 standard defines IDex-security that evaluates IoT security level and further provides a series of common security solutions in IoT framework systematically. The common IoT security concerns based on IEEE P2668 are summarized and the directions for further enhancing GWIN security are proposed as below.

a. Common IoT Security Concerns

In general, an IoT framework consists of sensor layer, network layer and application layer. The end devices in sensor layer mainly perform the sensing data collection and transmission to IoT network layer for processing. The network layer provides the wireless coverage or connection for end devices in sensor layer, including networking components, internet core network provided by internet service provider, cloud. In application layer, users could apply their apps or client device to transmit or collect data from the network. The overview of IoT framework is shown in Fig. 22. However, in both research and industrial area, the lack of standards to protect the security of IoT systems may render serious damages (e.g., Data leakage, Out of Services, etc.). Based on the proposed IoT framework in Fig. 22, a series of common security concerns in standardization framework is summarized.

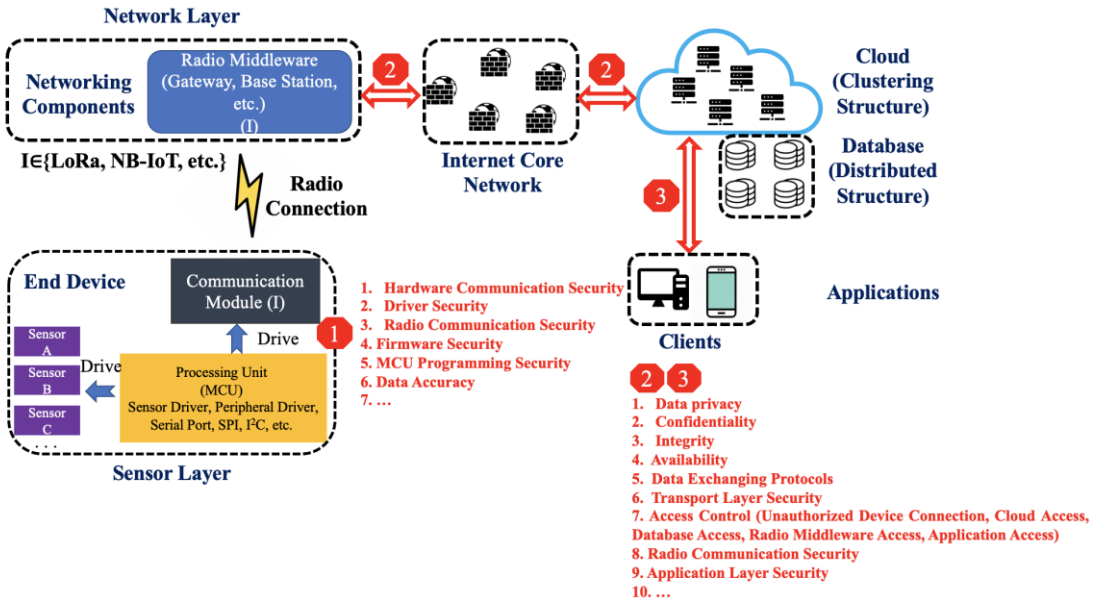


Fig. 22. Overview of IoT system and common security concerns

1. Sensor Layer Security

As shown in Fig. 22, the sensor layer are constructed with three major parts including Microcontroller unit (MCU), sensors (e.g., temperature, humidity, etc.) and communication module (e.g., LoRa, NB-IoT, etc.). The common concerns on sensor layer security include Hardware Communication Security, Driver Security, Radio Communication Security, Firmware Security, MCU Programming Security, and Data Accuracy. All of these security challenges shall be considered and protected for developing the end device in IoT system.

1) Hardware Communication Security: The communications between hardware components in end device through the commonly applied hardware interfaces and managed by the drivers. Insecure design (e.g., Unreliable driver resources, incompatible hardware specification, etc.) on the hardware communication may lead to damage to end device even to the network.

2) Driver Security: The end devices may integrate series of drivers to manage different hardware component. All of these drivers must be maintained by trusted organization to avoid unreliable design on end devices. In addition, the update on end device's drivers must be managed by authorized people and avoid casual installation of new drivers (i.e., end device software/firmware access control).

3) Radio Communication Security: The radio signal transmitted by end devices is actually received by the devices with the same receiving frequency. To avoid the information leakage and attacks, the information transmitted by the end devices shall be protected by the crypto methods (e.g., AES128 with Session Key mechanism in LoRa, etc.). The encryption is secured by the keys. To avoid the attacks on the key, it is necessary to generate the key with complex algorithm (e.g., Elliptic Curve Diffie, X509, etc.).

4) Firmware Security: In addition to drivers, the end devices may run other services (e.g., watch dog, timer, RTC, etc.). All of software with hardware drivers construct the firmware of the end devices. Many manufacturers may provide the firmware through internet services and the reliability of the firmware shall be ensured to avoid damage to the end devices and network.

5) MCU Programming Security: The firmware and drivers are developed by different integrated development environments (IDEs, e.g., Keil, IAR, etc.). The developers must ensure the IDEs are provided by reliable given that some malicious attacks may be hidden in the development tools or software to attack the end device or developer's computer. These attacks may leak the important information of network and lead to damage to the network.

6) Data Accuracy: Inaccurate sensor data transmitted to applications may cause damage to the system. Thus, the sensors or other hardware must be provided by reliable manufacturers or resources. In addition, the hardware configuration should not be revised by unauthorized operations.

2. Network Layer Security

The networking components in network layer provide the coverage, data exchanging, device connection functions to build communication between end devices and cloud. the common concerns in this layer include Data Privacy, Confidentiality, Integrity, Availability, Data Exchanging Protocol, Transport Layer Security, Access Control, Radio Communication Security and Application Layer Security. All of these security challenges shall be considered and protected for deploying the network and application in IoT system.

1) Data Privacy (Networking Components to Internet Core Network, Internet Core Network to Cloud): All the users with authorization from ISPs can share data in ICN. Thus, it is a high risk for leaking the exchanging data between radio middleware, ICN and cloud, rendering the privacy leakage. To overcome this issue, the exchanging data among components in network layer shall be confidential and limit the access authorization.

2) Confidentiality: The exchanging data in network layer shall be encrypted to avoid data leakage (e.g., AES, Authentication, etc.).

3) Integrity: The exchanging data may be revised or transmitted with mistake in network layer, rendering the error data exchanging and damage to the network. To ensure the integrity, the technologies such as hash, blockchain, and etc. can be applied.

4) Availability: This item refers that the end devices/users could receive the services when they ask for serving. Generally, the most serious attack to cause out of service is the massive attacks (e.g., Distributed Denial of Services (DDoS)). To avoid this kind of attacks, the distributed server structure is recommended to provide much higher computation power.

5) Data Exchanging Protocols (e.g., MQTT, HTTP, CoAP, XMPP, TCP, UDP, etc.): Unlike the conventional Web services, there are multiple data exchanging protocols in IoT system. For example, the MQTT protocol provide an efficient transmission between radio middleware and cloud, while the reliability is also ensured. All the application layer protocols (e.g., MQTT, HTTP, CoAP, XMPP, etc.) are designed based on the transport layer protocols (TCP and UDP). Thus, the security of these application layer protocols is based on transport layer security.

6) Transport Layer Security (TLS): To avoid the message leakage and insecure communication between radio middleware and cloud, the transport layer security shall be considered.

7) Access Control:

   - Avoid Unauthorized Device Connection: In the network, some attackers may deploy the abnormal device to try to access into the network to send or attack network layer. To avoid the attacks, the abnormal data or operations by the unauthorized device shall be monitored.

- Cloud Access: The cloud may be maintained by different people who cooperate to develop the network. Thus, to limit the unauthorized operations on the cloud, there is an access-control distribution for different people or different role. In addition, to avoid data abuse, the end devices belong to different applications shall be also managed.

- Database Access: The database is mainly applied for storing the exchanging data in the network. The access control of database provides cross-level access on the database. Additionally, the management operations of database shall be also protected.

- Radio Middleware Access: The radio middleware is sometimes deployed remotely and maintained by the Secure Shell (SSH). The attacks may happen when the password key of SSH is lightweight to be forced out. Thus, the management of radio middleware shall be deployed based on private communication tunnel and the access resource is required to be limited. Additionally, there are some hardware ports in radio middleware remained to manage them. The attackers may access into the radio middleware through these hardware port. Hence, it is necessary to limit the management right to access into the radio middleware.

- Application Access: Different applications may be deployed in the same network. To avoid the data leakage and attacks, different applications shall be distributed with different permissions to access their storage data in the cloud.

8) Radio Communication Security: Similar to the communication security in sensor layer

9) Application Layer Security: The clients in Fig. 1 ask for service from cloud through ICN. Thus, the security issues of network layer can be also applied to application clients.

b. The Way to Enhancing GWIN Security

Based on the common concerns introduced above, the security of GWIN infrastructure could be improved in following aspects:

1. Sensor Layer Security:

1) There is lack of a global sensor development standard to anti-security challenges.

2) Only Over-The-Air-Activation (OTAA) and AES 128 security measurements are included in current GWIN sensor layer, which are basically applied LoRaWAN security methods.

3) The Hardware Communication Security, Driver Security, Radio Communication Security, Firmware Security, MCU Programming Security and Data Accuracy is not included.

2. Network Layer Security:

1) There is lack of radio communication among sensor layer and network layer in GWIN structure.

2) There is lack of reliable data storage structure in the GWIN network (e.g., Blockchain structure).

3) The access control shall be improved.

4) Lack of efficient security evaluation standard for current GWIN network structure

In the future, potential approaches will be developed to deal with these security challenges of GWIN infrastructure.

C. GWIN General Requirements

In this part, technical requirements, contractor's responsibilities, testing and commissioning requirements, and application interfacing requirements with GWIN LoRaWAN are defined to ensure fair and secure GWIN utilization.

c. Technical Requirements

1. The LoRaWAN equipment shall comply with the following requirements, as a minimum:-

(a) Radio Equipment Specifications (HKCA 1078) - Performance Specification for Radio Equipment Operating in the 920 – 925 MHz Band for the Provision of Public Telecommunications Services issued by Office of the Communications Authority, HKSARG; and

(b) LoRaWAN specification v1.0.2 or latest version issued by LoRa AllianceTM.

2. This supply and installation of low power wireless network system shall base on LoRaWAN specification v1.0.2 or latest version issued by LoRa Alliance™ for the Government in Hong Kong Special Administrative Region (HKSAR).

3. The LoRaWAN sensor devices shall be manufactured and configured to support and capable of communicating with the existing LoRaWAN compatible equipment in LoRaWAN specification v1.0.2 or latest.

4. All equipment that emits radiowaves shall have been type-approved by the Office of the Communications Authority (OFCA) or shall fall within the licensing exemption(s) provided for by legislation, including (but not be limited to) the Telecommunications (Telecommunications Apparatus) (Exemption from Licensing) Order (Cap 106Z).

5. The LoRaWAN equipment shall comply with LoRaWAN specification v1.0.2 or latest standard, Chapter 106 of the Telecommunications Ordinance, HKCA 1078, and other subsidiary legislations of Hong Kong. If applicable, the Contractor shall liaise with the Office of the Communications Authority (OFCA) for the approval of frequency band

for the completion of Works. All provided radio equipment shall be complied with OFCA standards and Type Approval Certificate (issued from OFCA or authorized organizations) shall be provided.

6. All LoRaWAN equipment shall operate with the parameters as specified below:

(a) Frequency range: 920MHz – 925MHz

(b) Regulation: Radio Equipment Specifications (HKCA 1078) issued by OFCA

(c) Standard: Compliant with LoRaWAN specification v1.0.2 or latest version issued by LoRa Alliance™

7. All LoRaWAN sensor devices shall comply with the requirements below as a minimum:

(a) Over-the-Air Activation (OTAA) activation mode

(b) Support Adaptive Data Rate (ADR)

(c) Support random LoRaWAN channel selection

(d) With battery level in payload, if applicable

(e) Support heartbeat message at least once a day

8. The use of frequency bands and transmission powers shall comply with the requirements set by OFCA and LoRa Alliance on LoRaWAN equipment and applications.

9. The LoRaWAN equipment shall be capable of operating in the full band of the frequency range (920MHz – 925MHz). Exact operating frequencies in the aforementioned frequency band may be altered and finalized after the contract award.

10. The LoRaWAN equipment shall be interoperable with major LoRaWAN network servers in the market such as The Things Network, etc.

d. Contractor's Responsibilities

1. The Contractor shall be responsible for the registration, decoding and configuration for sensor devices supplied under this Contract to EMSD's LoRa network servers.

2. The Contractor shall be responsible to register and configure the sensor devices supplied under this Contract to EMSD's LoRa network. The Contractor shall liaise with the Engineer's Representative(s) to obtain the user manual, login ID and password for the use of EMSD's LoRa network server web-based platform after the contract award.

3. The Contractor shall follow the instructions for sensor device registration (i.e. join request & accept using OTAA) and decoding standard, if applicable which will be provided by the Engineer's Representative(s) after the contract award.

4. The Contractor shall, at his own cost, to perform necessary on-site troubleshooting and configuration services, including but not limited to, re-joining of sensors, sensor parameters updates, sensor parts replacement and firmware updates, to ensure the connectivity to EMSD's LoRa network and proper configuration of deployed sensors so that the equipment can function normally under the requested scope of works.

5. The Contractor shall ensure the firmware of the LoRaWAN equipment to be the latest version available in the market. The Contractor shall be responsible to update and provide patches to all software and / or firmware so that the equipment can function normally under the requested scope of works.

6. The Contractor shall submit the material submission for approval by the Engineer's Representative(s). In case the proposed LoRaWAN equipment is not compatible with EMSD's LoRa network, the Contractor must provide alternative proposals or substitutions on the material submission at his own cost and obtain in writing an explicit approval from the Engineer's Representative(s).

7. The Contractor shall provide all technical documents including the payload format and configuration specification for LoRaWAN equipment supplied under this Contract.

8. The Contractor may be required to arrange samples of equipment and conduct connectivity test with EMSD's LoRa network before the approval of material submission. The Contractor shall, at his own cost, arrange the required samples and necessary accessories and complete the test within 1 week at the request of the Engineer's Representative(s).

9. The Contractor may be required to submit samples of equipment for the Engineer's Representative's evaluation during the course of the Contract if they elect to offer equipment which has not been approved by the Engineer's Representative(s) due to equipment offered becoming obsolete or due to other causes. The Contractor shall, at his own cost, submit the required samples for evaluation within 1 week at the request of the Engineer's Representative(s).

10. During the Nursing Period and Defect Liability Period, the Contractor is responsible for remote monitoring the health status of the sensors deployed under this contract through system provided as stipulated in b.2. The Contractor may be required to submit regular health reports or on-demand of the sensors to keep-track of the wellbeing and rectification progress of the end-devices.

e. Testing and Commissioning Requirements

1. The Contractor shall submit the Site Acceptance Test (SAT) plan, schedule, procedures, forms and testing methodology to the Engineer's Representative(s) for prior approval before the tests.

2. Unless otherwise specified, any test instrument or field tester for the tests should be provided by the Contractor. Should any transportation of these equipment to test site be required, the Contractor is also responsible for the delivery.

3. The Contractor shall ensure the sensor device installation and documentation to meet the following minimum pre-requisite before the commencement of SAT.

(a) Sensor's baseline information should be recorded in the test form, i.e. brand, model, serial number, device ID, device name, device EUI, installed location with geospatial data;

(b) Sensor's baseline configuration should be recorded in the test form, i.e., heartbeat, frequency, reporting interval, triggering event;

(c) The parameters for test environment should be recorded including but not limited to the RSSI, package loss rate taken on site with field tester as the reference value for the sensor under test;

(d) The latest activity for the sensor from the LNS should be recorded i.e. the sensor activity for last 7 days before the SAT; and

(e) The sensor device should be alive for at least 7 days before the SAT.

4. The Contractor shall perform signal test for the sensor devices under this Contract during the SAT recording the parameters including, but limited to uplink Received Signal Strength Indicator (RSSI), uplink Signal to Noise Ratio (SNR), Spreading Factor (SF), Data Rate (DR) of acceptable level as stipulated in the approved test plan.

5. Upon the completion of SAT, the Contractor shall submit the sensor device inventory list recording the information including, but not limited to brand, model, serial number, device ID, device name, device EUI, installed location with geospatial data based on the template as required by the Engineer's Representative(s).

f. Application Interfacing Requirements with EMSD's LoRa network

1. The Contractor shall develop interfaces on the system applications or data platform for data exchange with API (i.e. via MQTT and/or HTTP call-back with SSL) with the EMSD's LoRa network in accordance to the associated EMSD standards which will be provided by the Engineer's Representative(s) after the contract award.

2. The Contractor shall, at his own cost, retain data collected by sensor devices deployed under this Contract to meet the system functional requirements under the requested scope of works. Data exchange methods stipulated in d.1 shall be means of data transfer between EMSD's LoRa network and the systems and/or applications deployed by the Contractor under this Contract. EMSD's LoRa network is not obligated to retain any data collected by the sensors and/or applications deployed under this Contract.

3. The Contractor shall liaise with the Engineer's Representative(s) to obtain the user manual, login ID and password for the use of EMSD's LoRa network server web-based platform after the contract award.

4. The Contractor shall be responsible for the provision, upkeep and troubleshoot of servers, applications and/or connectivity that integrate with the data exchange methods as stipulated in d.1.

The entire GWIN system hierarchy is shown in Fig. 23.

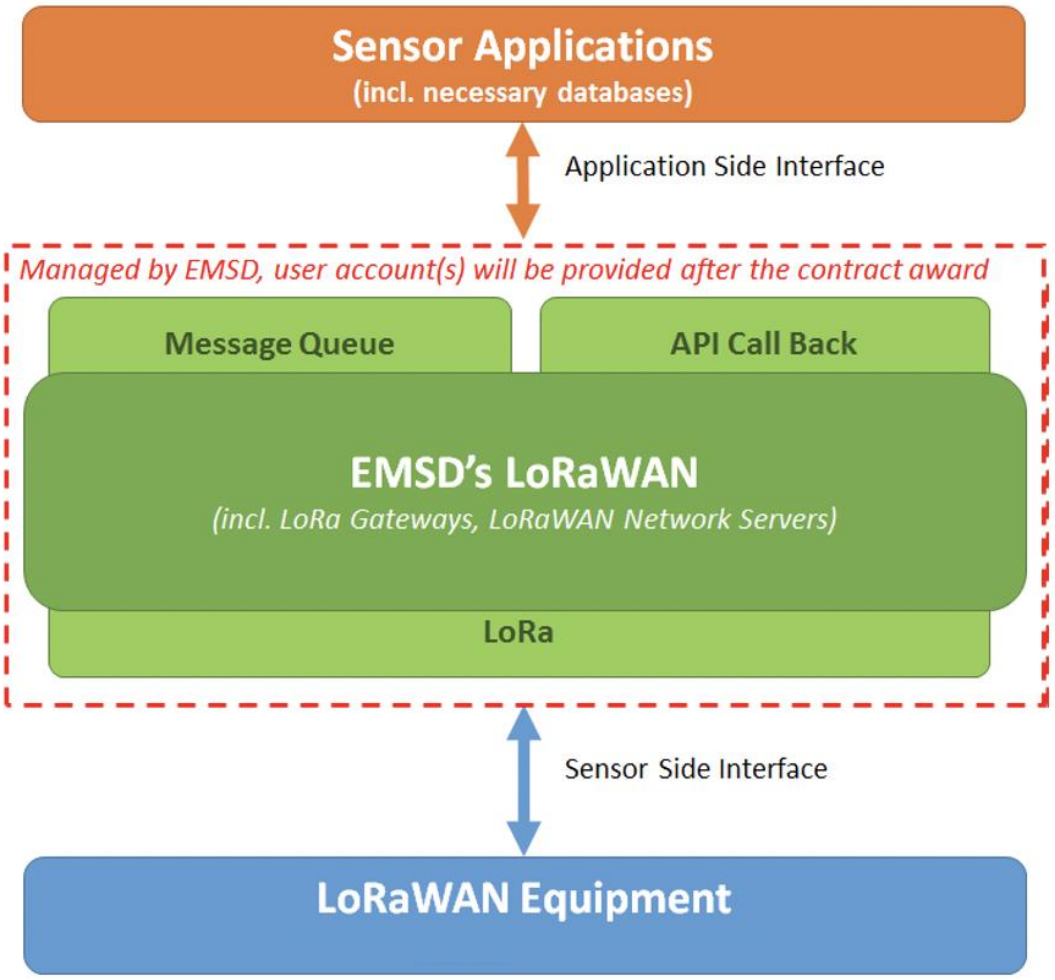


Fig. 23. GWIN System Hierarchy

VII. Pilot Tests Implementations

So far, GWIN has covered Kowloon East, Kowloon West, New Territories East, New Territories West, HK, Islands, etc. districts. GWIN provides connection tunnel for IoT sensors and data acquisition APIs for clients. Through GWIN, users only need to concern about IoT sensor deployment and the realization of specific functions. In the section, three pilot tests, including testbed of LoRaWAN data logger for Water Supplies Department, testbed of evaluation of personnel tracking, and testbed of LoRaWAN IoT Message Display System at China Ferry Terminal were implemented.

A. Testbed of LoRaWAN Data Logger for Water Supplies Department

a. Project Statement

The WSD pilot test aims to develop a LoRa-based data logger to retrofit existing flowmeter for flow data transmission at manhole (underground) environment

b. Expected Outcomes

- LoRa-based data loggers can remotely transmit captured water flow signals from WSD flowmeter
- Water flow rate data can be collected at LoRa network server via LoRaWAN

c. Equipment List

- ABB EM Flowmeter (1 No.)
- Flowmeter Transmitter AquaMaster 3 (1 No.)
- Flowmeter Transmitter AquaMaster 4 (1 No.)
- Cello Data Logger (1 No.)
- Battery set (1 No.)
- Cable WABC 2010/10 (1 No.)
- Earth rings (2 No.)
- Manual (2 No.)
- LoRa transmitter with power saving mode (1 No.)
- 3.6V Li batteries
- LoRa gateway (1 No.)
- Digital oscilloscope (1 No.)
- Programmable DC power supply (1 No.)

- Android Phone with NFC (1 No.)
- LoRaWAN network server platform
- ELSYS ELT-2 module (1 No.)

d. Methodology

1. The design of LoRa-based data logger

In this pilot test, a LoRa-based flowmeter system structure is developed, as shown in Fig. 24. This proposed system consists of three main parts: LoRa-based flowmeter nodes, LoRa gateway and network server. The system records flow information of water distribution network for smart monitoring and remote management.

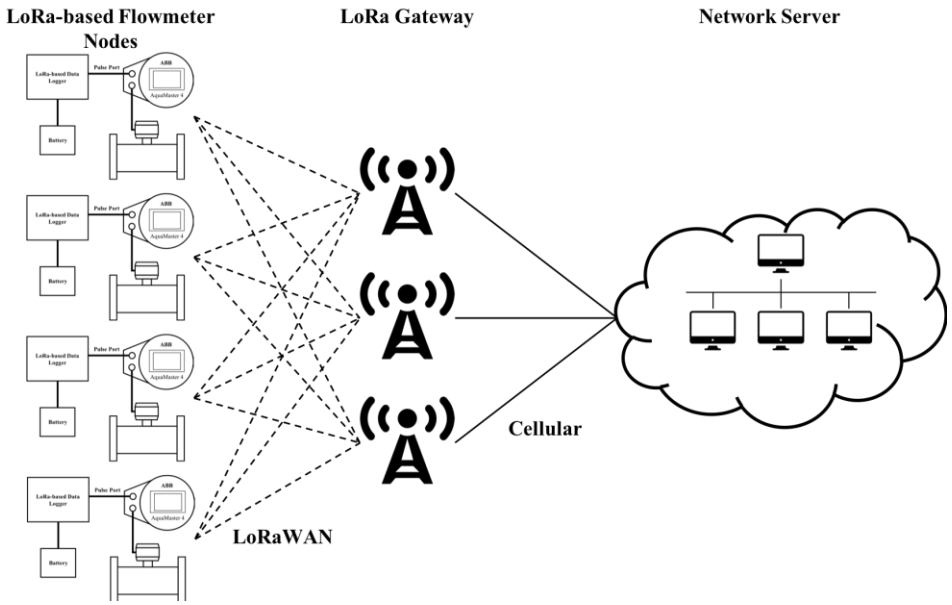


Fig. 24. LoRa-based flowmeter system structure

To achieve flow data collection and transmission function successfully, the design of LoRa-based flowmeter node is focused on. The core of LoRa-based flowmeter node is LoRa-based data logger which is composed of Microcontroller Unit (MCU), LoRa communication module, embedded Real-time clock (RTC) and battery (as shown in Fig. 25). MCU collects pulse information and sends them out at a fixed transmission frequency through LoRa communication module. RTC is a computer clock that can be integrated with MCU to keep track the current time. In addition, RTC is able to maintain accurate time with low power consumption. The entire data logger module is powered by a 3.6V battery.

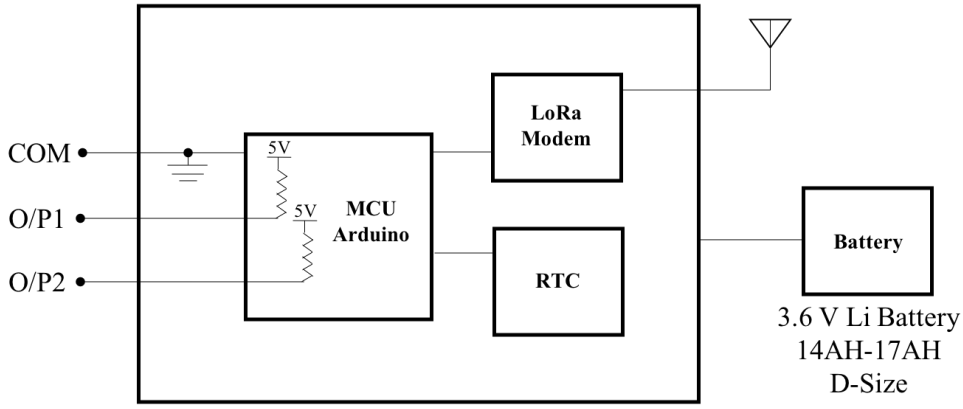


Fig. 25. LoRa-based data logger

2. System setup

In this pilot test, MCU, RTC and LoRa modem are integrated into one developing board, which is based on LoRaWAN standard and compatible with Arduino development environment.

LoRa module configuration is the first step to develop the LoRa-based data logger. MCU connects LoRa communication module through UART. LoRa module is in compliance with LoRaWAN protocol and is set at AS923 frequency band. There are two common modes for LoRa communication module to join the LoRa network: Over-the-Air Activation (OTAA) and Activation by Personalization (ABP). In this system, OTAA mode, the more secure method, is configured for connection between LoRa communication module and LoRa network. To guarantee the longest battery lifetime, ClassA is configured in this LoRa-based data logger. LoRa end devices are identified with unique DecEui, AppEui and AppKey. After these three values are set in both LoRa end device and network server, the end device will enter the network successfully with its identity.

Given the limitations of experimental environment, ABB flowmeter is set on simulation mode to generate pulses automatically. The pulse output is ON/OFF pulse with a maximum 50Hz frequency and 50% nominal duty cycle. "O/P1" (Orange Line) records forward only or forward plus reverse pulses. "O/P2" (Red Line) records reverse pulses or direction indicator. In this stage, "O/P1" is selected as the main output port. The port assignments are shown in Fig. 26. For the simulation configuration, the flow rate simulation value is set at 50 mm/s. The pulse output is simulated with 2Hz frequency and 10ms pulse width. Fig. 26 shows the system setup.

Fig. 26. LoRaWAN Data Logger System setup

3. Data transmission

As shown in Fig. 26, the voltage of pulse port stays high level when there are no pulse signals. The voltage is triggered to a low level when pulse signal is generated. In MCU, there is a loop function to keep counting the number of pulses. The pulse information in a time duration will be sent out through LoRa radio by using interrupt function. The flow information is usually described as flow rate. The conversion from pulse counts to flow rate is developed. To meet the requirement of different meter sizes, an adaptive conversion formulation is also designed, as shown in following equation:

$$Flow\ rate = N_{pulse} * U/1000 * 1/T \quad (10)$$

where N_{pulse} is the number of pulses in the time period. U is the volume of each pulse. For meter size <= 100mm, U = 10 litre/pulse. For meter size >= 150mm, U = 100 litre/pulse. T is the duration in hour. (Note: this equation is from the email of ABB company)

To keep accurate transmission duration, an RTC module is used to synchronize the time of end device to LoRa network server through downlink transmission. Compared with synchronization by GPS, this method has lower latency (~50ms) and lower cost.

To save power, the transmission duty cycle will be set as 15min or 1h. Here, to check the transmission accuracy easily, in this simulation, the developed LoRa-based data logger transmits pulse information flow rate every 1 min. When the meter size is 80mm, the flow rate is 72 m^3/h.

4. Alternative Solution

Based on the above LoRa-based data logger design, a market-ready product ELT-2 was explored to be an alternative solution in this pilot test, which is better for mass production.

ELT-2 is a LoRa-based pulse counter, as shown in Fig. 27 [40]. It has an internal antenna, which makes the device easier to install and mount at manhole environment. In addition, it is even more waterproof and very difficult to break. Hence, ELT-2 is a potential solution for large-scale deployment.

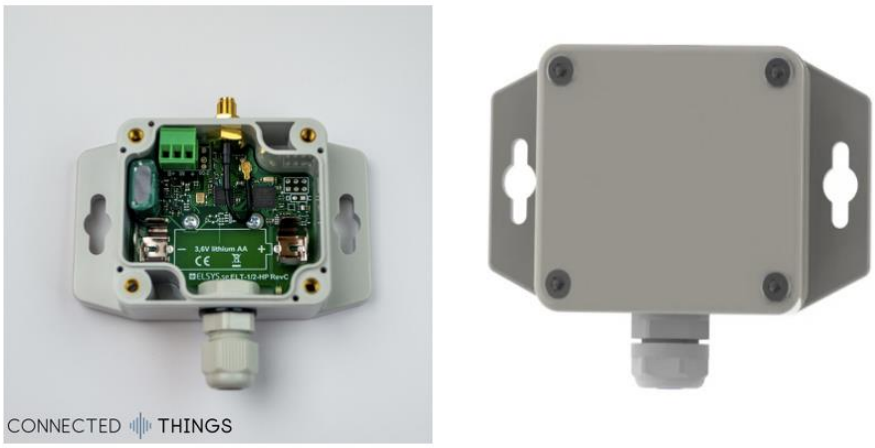


Fig. 27. ELT-2 LoRa-based pulse counter

5. Implementation and performance evaluation

The complete experimental testbed was shown in Fig. 28. In the experiment, the 80mm flowmeter was used for testing. The pulse frequency was simulated as 2Hz, and the period of pulse generation was 10ms. The designed LoRa data logger collected pulse information and transmitted out every 1 min. The final flow rate result (72 m^3/h) is displayed in each uplink message. The data record and the testing websocket client were shown in Fig. 29.

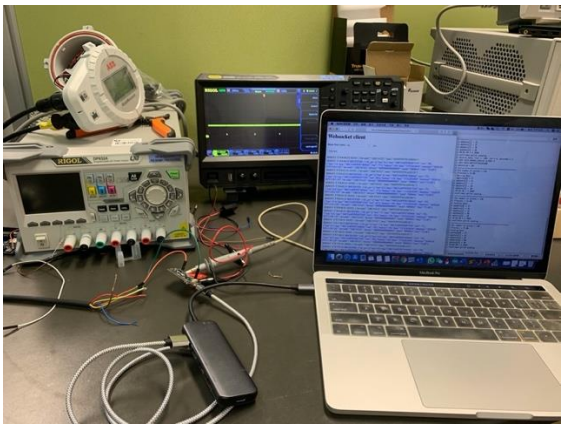


Fig. 28. Experimental testbed

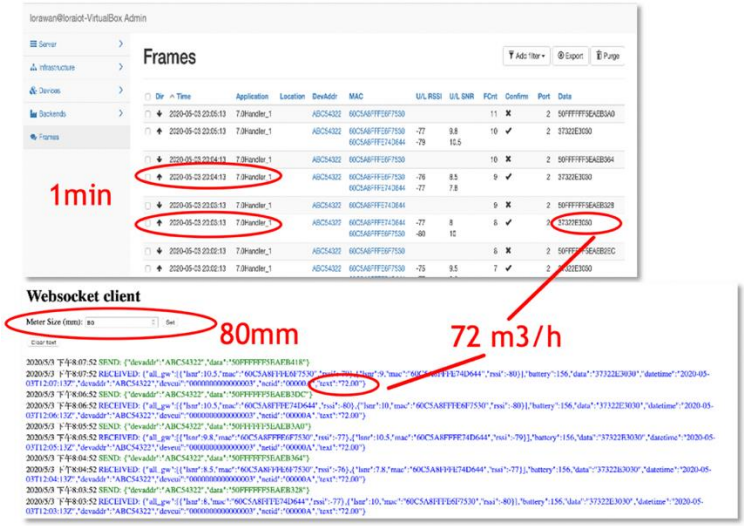


Fig. 29. Data record in network server and websocket client

According to the data record for several months, the results demonstrated that the designed LoRa-based data logger can accomplish >95% data accuracy and about 3s transmission time. The measured value of sleep current is about 0.01mA. According to the LoRa Energy Calculator, when the transmission cycle of flowmeter is about 15min = 900s, the 14Ah battery can support the logger about 50%*6.7 = 3 years. [41] (Note: It is just the theoretical value, the lifetime may also be affected by other factors, such as environment temperature, etc.)

6. Conclusion

In conclusion, LoRa-based data loggers using pulse counting to retrofit existing flowmeter for flow data transmission was developed. The designed logger achieved the collection, transmission and conversion of water flow signals successfully. The experimental results showed that this design has high transmission accuracy, low transmission latency while maintaining low power consumption.

B. Testbed of Evaluation of Personnel Tracking

a. Project Statement

This project aims to evaluate LPWA-based GPS tracking solutions, including Sigfox-based Xsense Tracker, Sigfox-based SimplePack 3.0 Plus Full Tracker, and NB-IoT-based CSL G20 Pro Tracker. Contributed by the GWIN, these GPS trackers could present the positioning functions in both indoor and outdoor environment. Considering different application deployment, the appropriate scenario for each tracker is suggested based on the evaluation of its wireless technology and functionality.

b. Expected Outcomes

- Evaluate the basic functions or features of tracking solutions (System structure, system working flow or logistics and etc.);

- Evaluate the performance of tracking solutions in terms of indoor & outdoor positioning accuracy;
- Evaluate the power consumption of the trackers; and
- Evaluate the appropriate scenario for each tracker based on the wireless technology and functionality.

c. Equipment List

- Sigfox-based Xsense Tracker
- Sigfox-based SimplePack 3.0 Plus Full Tracker
- NB-IoT-based CSL G20 Pro Tracker

The following figure shows the above tested three trackers. The detailed specifications of three trackers are shown in Appendix 4.

Fig. 30. Three Trackers (Xsense Tracker, SimplePack 3.0 Plus Full Tracker, CSL G20 Pro Tracker from left to right)

d. Methodology

1. Indoor Positioning Accuracy Testing: The indoor positioning accuracy testing should be implemented based on the "MAC-address to Coordinates" algorithm or methodology.

2. Outdoor Positioning Accuracy Testing: Not Applicable

3. Transition of Indoor & Outdoor Positioning: This test aims to find out the transition mechanism from indoor to outdoor or outdoor from indoor.

4. Battery Life Testing: As discussed with EMSD, this test is based on 14 days testing. In other words, if the trackers could perform positioning function more than 14 days, the testing outcome could be regarded as "Pass". The theoretical transmission performance could be referenced from LPWAN Comparison and Evaluation Project.

5. Geo-fencing Function: This function is to stipulate the inbound area for each tracker. If the tracker is outbounded, then alarm will be sent to managers for monitoring.

e. Implementation and performance evaluation

Based on the proposed criteria, the tests of three trackers were implemented in both CityU and EMSD buildings. The data records of three trackers was collected and evaluated at the same time to ensure the effectiveness of the results. The detailed test procedure and test outcomes are shown in Appendix 5. The evaluation results of three trackers are illustrated as follows.

1. Xsense performance evaluation

(1) The Sigfox signal of Xsense is much better than SimplePack Plus 3.0 who won't receive any Sigfox signal in the testing at EMSD HQs.

(2) The triggering methods of Xsense is not same to the working diagram of Xsense in Fig. 5 which is provided by EBSL. (Need EBSL to double check the triggering mechanism of Xsense)

(3) Indoor localization accuracy: Based on Wifi, indoor localization accuracy of Xsense is decided by the Wi-Fi Aps locations. Outcome shows that the indoor localization accuracy varies from 18 meters to 50 meters at different testing points.

(4) Outdoor Localization: Based on GPS technology, the outdoor localization accuracy is less than 100 meters which is the typical value of GPS technology.

(5) Transition of Indoor & Outdoor Positioning: Because the triggering method cannot works with Fig. 5. Hence, most of the testing data are collected from static testing at each testing points.

(6) Battery life is enough for 14 days.

(7) Geofencing function cannot work in Zenzi platform by now.

(8) Preliminary Outcome: As above, Xsense is better to be applied in the assest tracking without many mobility. For quarantine cases, considering on the indoor localization accuracy, most 3 Wi-Fi MAC addresses may not be enough to give a less than 10 meters localization.

2. SimplePack performance evaluation

(1) Cannot receive any Sigfox Signal in the testing.

(2) The triggering methods of SimplePack is not clear in the testing.

(3) Indoor Localization Accuracy: N.A

(4) Outdoor Localization Accuracy: Not support

(5) Transition of Indoor & Outdoor Positioning: Not Support

(6) Battery Life is enough for 14 days.

(7) Geofencing function cannot work in Zenzi platform by now.

(8) Preliminary Outcome: SimplePack is not recommended to be applied in tracking project since its unstable signal quality.

3. G20 Pro performance evaluation

(1) Signal Strength: G20 Pro is based on CSL NB-IoT network. In the testing, the NB-IoT signal is stable t EMSD HQ.

(2) Triggering Method: Confidential design of CSL

(3) Indoor localization accuracy: Based on Wi-Fi MAC addresses, NB-IoT is the carrier to send to Petbiz for tracking. The estimation on the indoor accuracy varies from 70 meters to 85 meters because the Petbiz App cannot support show out the current positions coordinates directly.

(4) Outdoor localization accuracy: Based on GPS technology, the outdoor accuracy is less than 100 meters which is the typical localization accuracy of GPS technology.

(5) Battery life is enough for 14 days.

(6) Transition of Indoor & Outdoor Positioning: The triggering method

(7) E-fance: The E-fance UI cannot be found at Petbiz APP. This function needs to be further tested.

(8) Preliminary test outcome: If the functions of Petbiz app could be customized, G20 Pro is a potential tracker to be applied in quarantine project considering on its licensed NB-IoT network coverage. In addition, in order to apply trackers in quarantine, the working diagram must be clear in order to design the rational quarantine policy in Hong Kong. G20 Pro trackers also support asset tracking project.

g. Conclusion

In conclusion, the performance of three GPS tracking solutions, XSense, SimplePack, and G20 Pro Tracker were evaluated in terms of basic functions evaluation, positioning accuracy, power consumptions and management platform.

The experimental results showed that 1) Xsense is better to be applied in the assest tracking without many mobility; 2) SimplePack is not recommended to be applied in tracking project since its unstable signal quality. 3) G20 Pro tracker is suggested to be applied in asset tracking and quarantine project.

C. Testbed of LoRaWAN IoT Message Display System at China Ferry Terminal

a. Project Statement

This project aims to provide technical guidance for downlink-based LoRaWAN IoT message display system at China Ferry Terminal (CFT).

b. Expected Outcomes

- Evaluate the downlink performance of LoRaWAN Class C deivces.
- Provide technical guidance for downlink-based LoRaWAN IoT message display system in terms of payload size and transmission cycle.

c. Equipment List

- CubeCell HTCC-AB01 module
- Libelium gases pro module
- LoRaWAN IoT message display system via GWIN network in CFT
  - 2 sets 43" display system for Local and Destination graphical weather update in 1/F; 2 sets 65" display kiosk for Sailing Information Display Systems (SIDS) in 1/F;
  - 2 sets 43" display system for SIDS in G/F;
  - 2 sets 65" display system for SIDS in G/F;
  - 1 set transmitter for Gas Master alert in G/F;
  - 1 set transmitter for UPS alert in 8/F;
  - 3 sets portable sensor for temperature, humidity and air quality monitoring in 2/F; 1 set server computer;
  - 1 set 4G router;
  - 1 set control station for message update and admin. control in 2/F;


IoT-TV01 (43" TV)


IoT-TV02 (43" TV)


IoT-TV03 (65" kiosk TV)


IoT-TV04 (65" kiosk TV)


IoT-TV05 (43" TV)


IoT-TV06 (43" TV)


IoT-TV07 (65" kiosk TV)


IoT-TV08 (65" kiosk TV)

Fig. 31. IoT display system in CFT

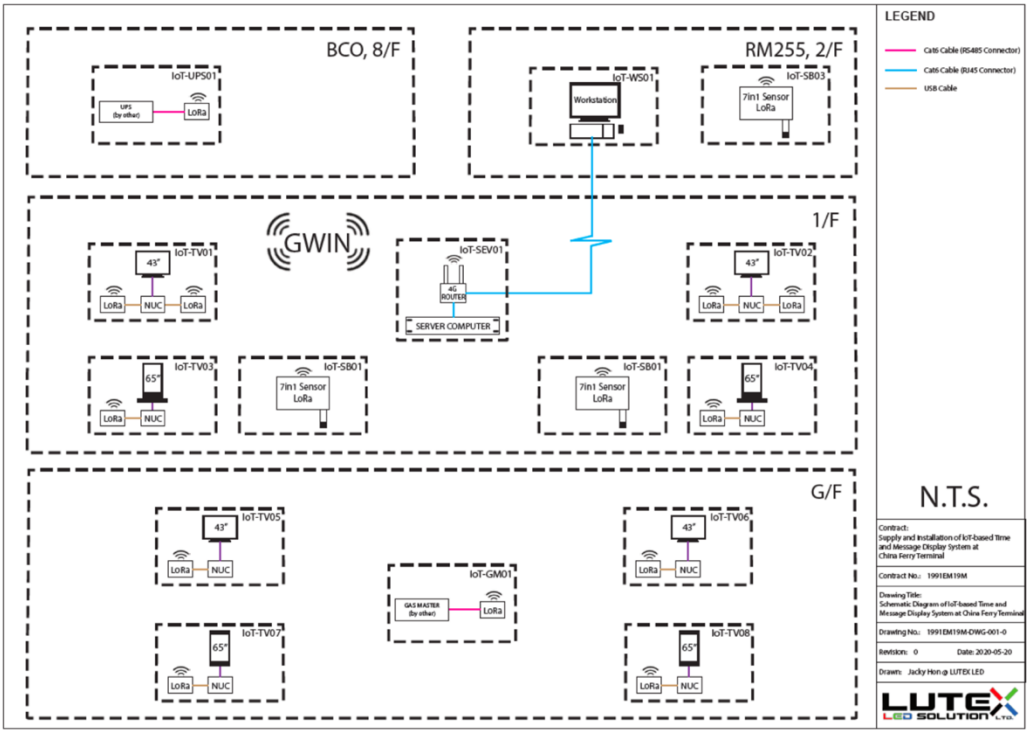


Fig. 32. The network architecture of LoRaWAN IoT message display system

d. Methodology

The LoRaWAN IoT message display system via GWIN in CFT is based on the LoRaWAN downlinks of class C devices. In this system, LoRa end device connected to each IoT display TV works in Class C mode. The workstation IoT-WS01, as the application server, transmits downlink messages (i.e., SIDS signal, temperature, humidity, etc.) to each LoRa end device via GWIN. Once these messages are received by LoRa end devices, the SIDS information is updated and displayed in the IoT-TVs. The network architecture is shown in Fig. 32.

In this system, LoRa downlink message generally carries a lot of information including berth No. boarding line, timetable, temperature, humidity, etc., which means a large packet size. In addition, SIDS information is required to be updated frequently in a short time while maintaining reliable transmission. To address these challenges, two main parameters to implement LoRaWAN IoT message display system are evaluated: 1) the payload length 2) transmission cycle.

1) Payload Length (PL): Payload length is determined by the length information that needs to be transmitted in the specific application. The larger the data packets, the longer the transmission airtime. In LoRaWAN protocol, different maximum MAC payload lengths are given to each SF respectively. The maximum effective application payload length in the absence of protocol overhead is eight bytes lower than the MAC payload value [4]. The maximum payload length, data rate, and SNR limit in different SFs are shown in Table 51.

Table 51. Parameters of LoRaWAN in different SFs in AS923 [11]

	Data Rate(bit/s)	**Max Mac Payload Length(bytes)**		**Max Application Payload Length(bytes)**		**SNR LIMIT (dB)**
		DwellTime = 0	DwellTime = 1	DwellTime = 0	DwellTime = 1	
SF = 7	5470 (DR5)	250	250	242	242	-7.5
SF = 8	3125 (DR4)	250	133	242	125	-10
SF = 9	1760 (DR3)	123	61	115	53	-12.5
SF = 10	980 (DR2)	59	19	51	11	-15
SF = 11	440 (DR1)	59	N/A	51	N/A	-17.5
SF = 12	250 (DR0)	59	N/A	51	N/A	-20

(Note: DwellTime = 0 means no transmission time limit, DwellTime = 1 means maxTOA = 400ms)

From the above table, the effective application payload length can reach up to 242 bytes. The information longer than 242 bytes should be divided into multiple packets for transmission.

2) Transmission Cycle (T_{cycle}): Transmission cycle refers to the average time duration between two continuous data packets per device. This parameter is usually determined according to the specific application requirements and it also is limited by duty cycle defined in LoRaWAN specification [11]. According to the LoRaWAN v1.0.2 standard specification, the duty cycle should be less than 1% in AS923 band. Duty cycle is the fraction of one period (usually one day) in which a signal or system is active. The relationship between transmission cycle and duty cycle can be expressed as

$$duty\ cycle = \frac{ToA}{T_{cycle}} = (n * ToA)/86400 \tag{11}$$

$$T_{cycle} = T_{interval} + ToA \tag{12}$$

where T_{cycle} denotes transmission cycle with unit of second; ToA denotes the average time on air of each packet with unit of second; $T_{interval}$ denotes waiting time between the end of previous packet and the beginning of next packet with unit of second; n is the number of transmitted packets within a day.

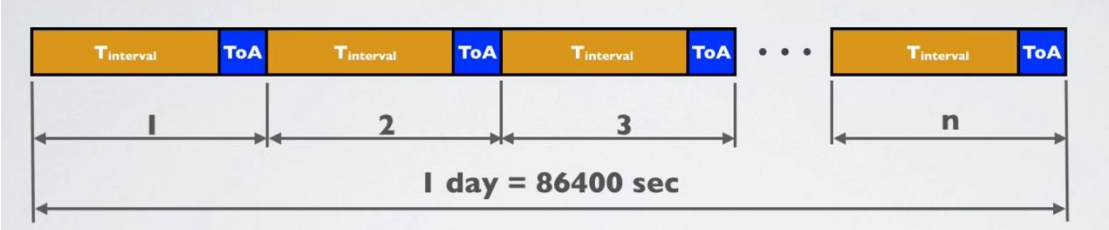


Fig. 33. The relationship between duty cycle and transmission cycle.

It is clearly that when the duty cycle is fixed, the transmission cycle is related to ToA. The value of ToA depends on LoRa configuration parameters, such as payload length, Spreading Factor (SF), etc., which could be estimated through LoRa calculator [42].

For this application, there are two main signals, SIDS signal and common signals (like temperature, humidity, etc.). As we all known, other signals, like temperature, usually changed gradually rather than extreme increase or decrease in very short time, thus these signals (e.g. temperature) could be transmitted in a longer interval, like 5min. SIDS signal has higher priority than other signals (e.g. temperature, humidity), which requires faster updating frequency. In terms of this situation, the temperature/humidity signals and SIDS signals are suggested to transmit separately. Through reduce the payload length of the packet, SIDS signals could be transmitted with shorter interval to meet requirements.

e. Implementation and performance evaluation

The feasibility test of LoRaWAN IoT message display system via GWIN were performed at CFT. The testbed is shown in following figure.

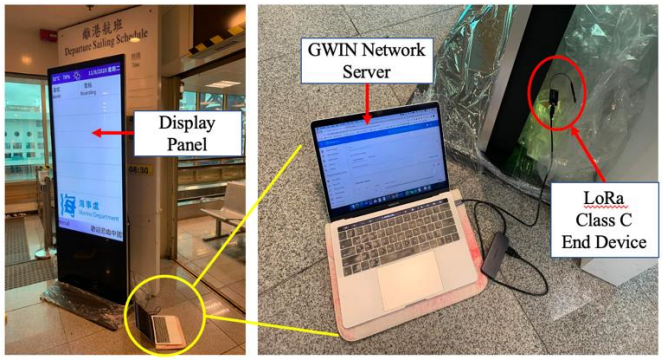


Fig. 34. Testbed of LoRaWAN IoT message display system via GWIN

The LoRa end device is placed behind the display panel and it was under the coverage of two GWIN gateways on 1st Floor and ground Floor in CFT building. In order to ensure that data packets can be transmitted regardless of SF values, payload length of 50 bytes was set in this test. As the transmission cycle increases from 3 seconds to 12 seconds, the packet loss rate reduces gradually from about 50% to 0%. Fig. 35 shows the successful downlink transmission from GWIN network server to LoRa end device.

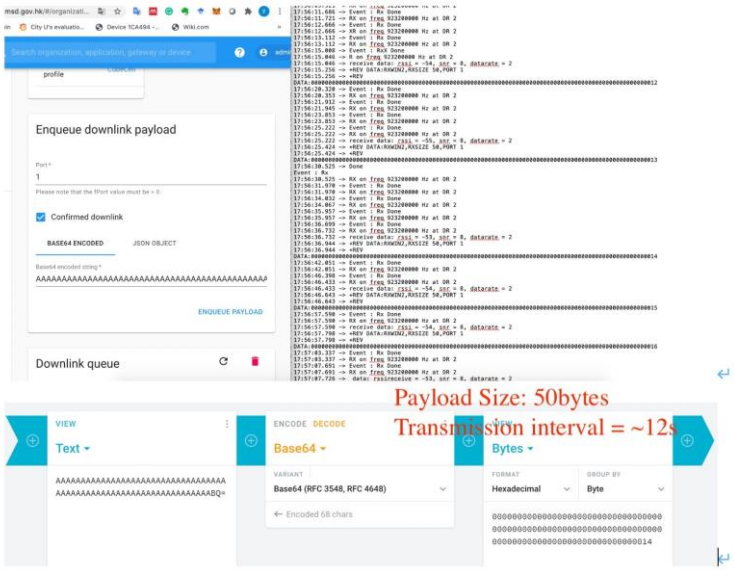


Fig. 35. Downlink transmission from GWIN network server to LoRa end device

To ensure both high reliability and short transmission cycle, each information of system is suggested to be divided into multiple small packets to transmit separately. In the meantime, the transmission cycle needs to comply with the limitation of 1% duty cycle.

h. Conclusion

GWIN supports downlink transmission of LoRaWAN Class C devices. The maximum application payload length defined in the LoRaWAN specification is 242 bytes. Through downlink transmission based on GWIN, it is feasible to implement the LoRaWAN IoT message display system at CFT, while the transmission cycle needs to comply with the 1% duty cycle rule.

D. Testbed of IoT Harmonization for GWIN

a. Project Statement

Nowadays, numerous Internet of Things (IoT) solutions and applications have been developed and applied based on various emerging wireless protocols, namely LoRa, Sigfox, NB-IoT, 5G, etc. Among these IoT protocols, those based on unlicensed frequency bands have gained more favor in most low-cost smart applications. However, the potential rise of unlicensed-band protocols may increase the overhead of the shared spectrum. As such, the massive IoT connectivity potentially incurs interference, thus more harmonization effort will be desperately demanded.

In view of this situation, this project aims to evaluate the impact of closely located IoT networks, and focus on the unlicensed band in Hong Kong (i.e. 920 – 925MHz). Investigation will explore potential interference, coexistence, network traffics and security when there is a mix of numerous IoT networks in the same general area, and formulate a guideline to optimize the co-existence of multiple networks.

b. Expected Outcomes

- Performance evaluation on single LoRa network in terms of duty cycle, payload length, Spreading Factor (SF) value, module density, operating channel, etc.
- Performance evaluation on multiple LoRa networks in terms of network density, module density, etc.
- Guidelines on harmonization of IoT networks operating in 920 – 925MHz, and
- Guidelines on harmonization of Government-Wide Internet of Things Networks (GWIN).

c. Significance of Harmonization Test

In the GWIN network, smart sensors or things are connected to gateways via the low power and private LoRa network. Various smart applications are able to be implemented based on the GWIN. However, there is no unified standard or guideline to allocate the GWIN resources to multiple users effectively. As a result, each application would try to occupy redundant network resources to achieve its best performance. Obviously, it is not efficient and feasible for GWIN with limited resources. Unreasonable resource allocation greatly reduces the efficiency of spectrum usage, and as the number of IoT devices and applications continues to increase, there would be serious collisions and interferences, resulting in a decline in the QoS of the entire network. The three major reasons for LoRa network performance degradation are described as follows.

Packet collision due to the pure ALOHA scheme used by LoRaWAN. Pure ALOHA is a medium access control (MAC) protocol for transmission of data via a shared network channel [43]. In pure ALOHA, it allows the end devices to transmit data at any time whenever they want, rather than waiting for the channel to be free. This scheme provides the advantages of low power consumption, but it also increases the packet collision probability. In one LoRa network, one LoRa gateway supports multiple end devices. Once more than one packet tries to occupy the channel (same channel and same SF) at the same time, packet collision would happen. With the increasing number of connected end devices, packet collision would be more serious. Fig. 36 shows the typical collision due to pure ALOHA scheme in LoRa network.

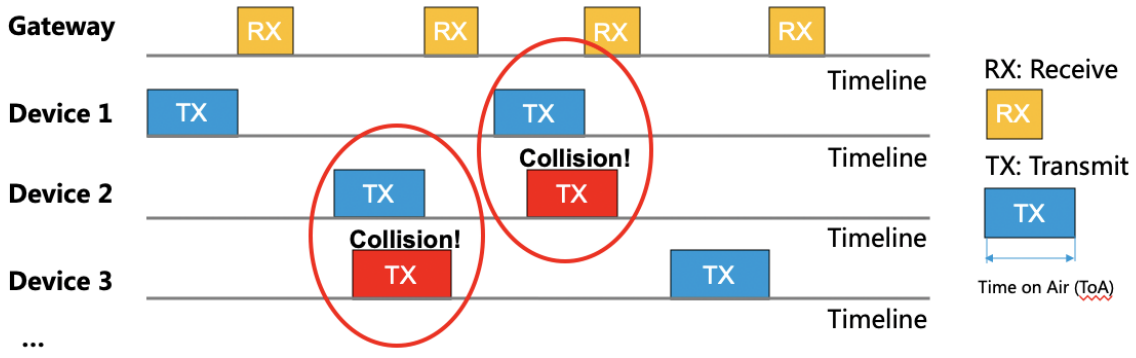


Fig. 36. Packet collision due to pure ALOHA scheme in LoRa network (End devices use same channel and same SF for transmission)

Packet collision due to unreasonable resource allocation. At present, there is no unified standard to allocate the resources of unlicensed band fairly. As a result, some applications would try to occupy redundant network resources with a very large duty cycle to achieve their best performance. However, when these devices transmit packets with large duty cycle, the whole channel resources are nearly fully occupied, so that other devices cannot join the network anymore and loss almost all data packets. This situation is illustrated in Fig. 37.

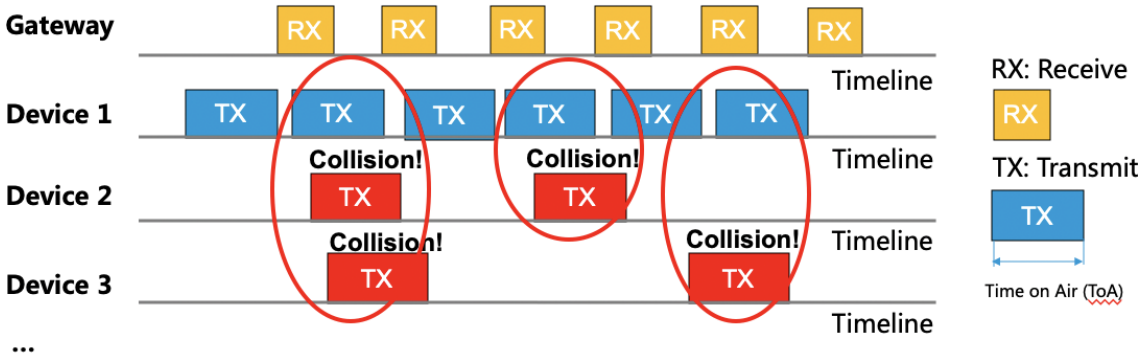


Fig. 37. Packet collision due to unreasonable resource allocation in LoRa network (End devices use same channel and same SF for transmission)

Interference due to overlapping of LoRa networks. In general, LoRa gateways could receive data packets of all devices within its coverage, even though the devices do not belong to its network. Take three overlapping LoRa networks, A, B and C, (as shown in Fig. 38) as an example, each LoRa network has its own registered end devices. Some devices are deployed in the intersection area of three LoRa networks. For the LoRa gateway of network A, apart from data packets of its own devices, it could also receive the data packets of the devices from network A and B in the intersection area. However, these unwanted signals for the LoRa network A would be considered as noises, thus leading to interferences. As the GWIN is growing, network overlap is inevitable so that the interference would become more serious.

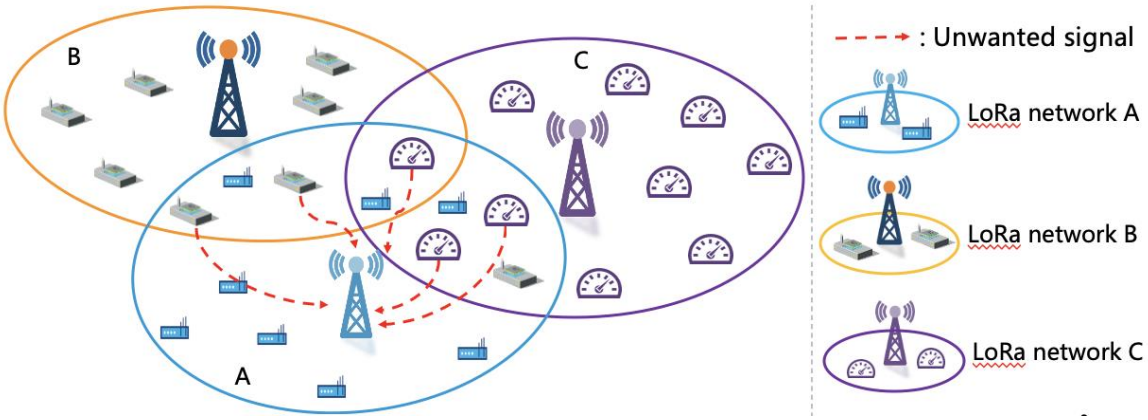


Fig. 38. Interference due to overlapping of LoRa networks

As discussed above, with the expansion of GWIN, packet collision and interference would be more serious in the uncoordinated networks, further leading to low QoS of smart applications. Even worse, without effective coordinated measures, all connections would be jammed and emergency services would be unreliable. Therefore, to address these challenges, the harmonization test will be performed to evaluate the effect of signal coexistence/interference and provide harmonization guidelines, thus facilitating the optimization of network planning and increasing service reliability.

d. Network Construction and Configuration

1. Network Construction

In the testing building, a CLP mesh network is deployed for smart metering, which is constructed with 2 gateways and 25 smart meters. Two gateways are deployed in meter rooms on G/F and 5/F respectively. Smart meters are deployed in G/F x 1, 1/F x 7, 2/F x 3, 5/F x 7, 6/F x 1, 7/F x 6. Four concurrent LoRa networks are established with typical star topology to coexist with CLP mesh network. Four LoRa gateways are deployed in I.T room on 1/F. Within the coverage of LoRa gateway, LoRa devices are deployed in 10 selected points with the total number of 100 devices. Table 1 shows the deployment scheme of IoT networks. The LoRa network construction is shown in Fig. 5.

Table 52. The deployment scheme of IoT networks in Science Park 2W Building

Floor No.	CLP Mesh Network		EMSD GWIN Network	
	The Number of Gateways	The Number of Devices	The Number of Gateways	The Number of Devices
7/F		6		
6/F		1		
5/F	1	7		
3/F				
2/F		3		
1/F		7	4	100
G/F	1	1		
Total	2	25	4	100

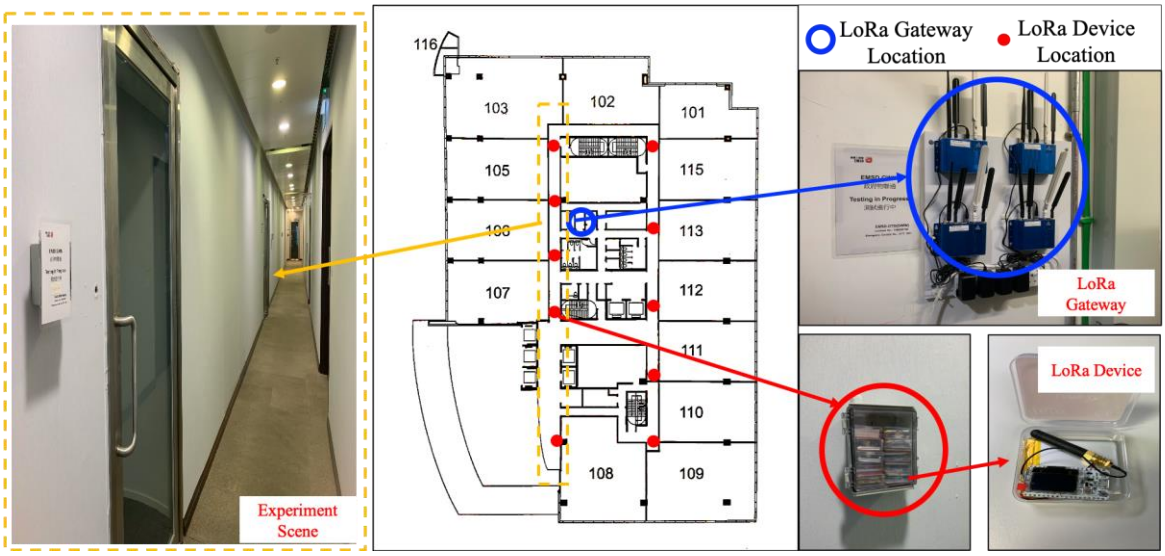


Fig. 39. LoRa network construction

2. Network Configuration

In this project, the four concurrent LoRa networks are considered as four different applications to better match the real situations. Each application or each LoRa network is constructed by one network server one LoRa gateway and corresponding connected LoRa devices. The Fig. 6. shows the structure of the four LoRa networks. To eliminate the influence of different brands of product on signal performance, the same type of LoRa device (i.e. Heltec LoRa 32 v2), the same type of gateway (i.e. Multitech) and the same type of LoRa network server (i.e. Chirpstack) are selected. In each LoRa network, data packets are transmitted from the LoRa device to its own gateway via LoRa radio. Then, the gateway forwards these data packets to the corresponding LoRa Network Server (LNS) through LTE network (i.e. Smartone). After that, these data could be fetched in Grafana database for performance analysis.

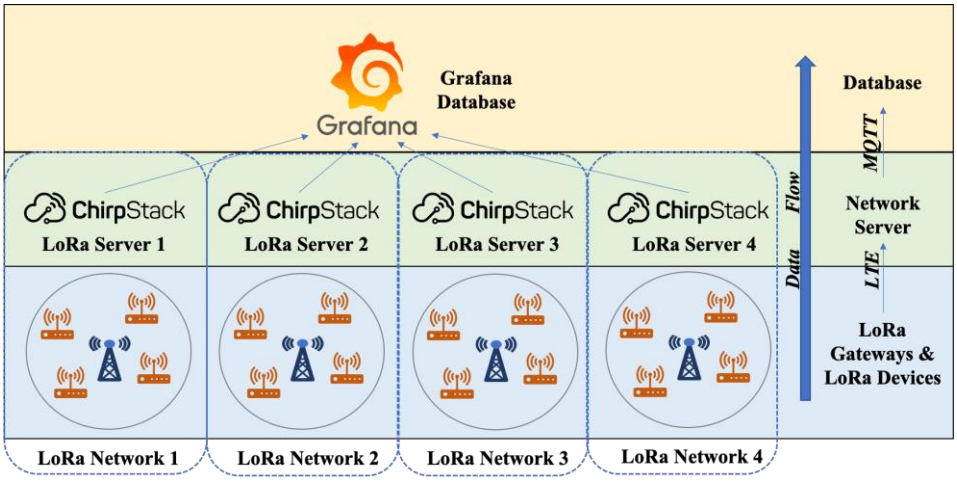


Fig. 40. The structure of four LoRa networks

For the configuration of LoRa gateways, all gateways are deployed on AS923 frequency band according to the LoRaWAN v1.0.2 standard [11]. This frequency band defines 8 channels

with 125kHz bandwidth. All these 8 channels are enabled by LoRa gateways for testing. And all LoRa gateways utilize the same LTE network (i.e. Smartone) to avoid the impact caused by different networks.

Similarly, the LoRa devices should be also deployed on AS923 frequency band. Over-The-Air Activation (OTAA) is selected as the activation method of LoRa modules with the advantage of the high-level security. To maximize the reliability of network, testing is based on the performance of unconfirmed messages. Besides, we mainly focus on Class A modules which is the optimal choice for most practical applications to save energy.

In general, configuration parameters such as channel, Spreading Factor (SF), transmission interval, etc. are set by users. When numerous LoRa networks coexist, different configurations would have different influences on signal performances. To explore the influence of different configurations on signal performance, parameters including payload length, SF, transmission cycle, duty cycle, the number of devices were studied. Consistent with LoRa gateway, 8 frequency channels from 923.2 to 924.6 MHz could be configured. The SF parameter could be configured from SF7 to SF12. The transmission cycle of LoRa devices is considered ranging from seconds to minutes. The packet size varies from 1bytes to 242 bytes.

To ensure the effectiveness of harmonization tests, we made the assumptions as follows:

1) CLP network and LoRa networks operate on the unlicensed frequency band at 920-925MHz;

2) One LoRa gateway deployed on its own LoRaWAN Network Server (LNS) forms an individual LoRa network;

3) Only stationary LoRa applications are considered in this test.

4) In this test, OTAA is selected as the activation method of LoRa modules to ensure the higher level of security;

5) Half duplex LoRa gateways are used in this test [44] and the same type of LoRa gateways have similar signal performances, including link budget, signal coverage, etc.;

6) The performance of uplink transmissions of Class A modules is mainly considered in this test to meet the requirements of energy saving in most practical applications.

e. Methodology

Harmonization test consists of two parts, feature test of single network, harmonization test of multiple networks. The Part 1- feature test of single network was simulated at first by

taking into consideration distinct configuration parameters, including payload length, Spreading Factor (SF), transmission interval, duty cycle, the number of devices, etc. Part 2 - harmonization test of multiple networks was conducted to study the coexistence performance. Part 2 was performed in Science Park 2W Building.

To study the performance of large-scale indoor LoRa networks, we design the harmonization test using following assumptions. In a smart building, about ten LoRa-enabled IoT applications are deployed in each room and each room is about 20 m^2. Hence, the device density is about 0.5 device/m^2. In our test building, the total testing area is about 2000 m^2. To achieve the scenario with the device density of 0.5 devices/m^2, 100 LoRa devices were used at a significantly accelerated transmission cycle to mimic the traffic that would be generated by 1000 devices. For example, the traffic of 1000 devices sending packets with 0.1% duty cycle can be roughly equivalent to the traffic of 100 devices sending packets with 1% duty cycle.

To evaluate the coexistence/interference performance, the Packet Loss Rate (PLR) parameter is analyzed to quantify the performance level. The degradation of LoRa network performance caused by the above three reasons in the second session can all be reflected in this parameter. This parameter PLR is defined as the ratio of the number of received packets to the total number of transmitted packets, which is formulated as following equation:

$$PLR_i = \frac{NR_i}{NT_i},\ i \in [1, num] \tag{13}$$

where PLR_i denotes the packet loss rate of ith device; NR_i is the number of received packets of ith device during the testing period; NT_i is the total number of transmitted packets of ith device during the testing period, and num is the number of devices of the experiment.

1. Feature Test of Single Network

To better understanding the performance of single LoRa network, feature test was performed using simulation to evaluate the ideal performance in interference-free environment. As we all known, LoRa network is usually configured by users with different parameters. Different configuration parameters would have different influences on signal performance. The four main parameters are evaluated, namely Spreading Factor (SF), Payload length (PL), Transmission Cycle (T_{cycle}), and duty cycle.

Spreading Factor (SF): Spreading factor determines the number of chirps that are transmitted per second. Six SF values (SF7 to SF12) are defined by LoRa, which are orthogonalized with each other to enable high interference resilience. Lower SF implies more chirps can be transmitted per second, thus, effective data rate will be higher and

airtime will be shorten. Conversely, higher SF indicates less chirps can be sent per second, hence, effective data rate will be lower and airtime will be extended, but the tolerant SNR limit will be lower and the communication range will be longer. The choice of SF value is a trade-off between communication range and data rate.

Payload Length (PL): Payload length is determined by the length information that needs to be transmitted in the specific application. The larger the data packets, the longer the transmission airtime. In LoRaWAN protocol, different maximum MAC payload lengths are given to each SF respectively. The maximum effective application payload length in the absence of protocol overhead is eight bytes lower than the MAC payload value [11]. The maximum payload length, data rate, and SNR limit in different SFs are shown in Table 48.

Transmission Cycle (T_{cycle}): Transmission cycle refers to the average time duration of between two continuous data packets per device. This parameter is usually determined according to the specific application requirements, ranging from seconds to hours. For instance, smart metering usually requires reporting data every 15minutes, while time-critical applications have small transmission cycle around several seconds.

Duty Cycle: Duty cycle is the fraction of one period (usually one day) in which a signal or system is active. This parameter is used to define the channel utilization rate of each device. The duty cycle can be expressed as a ratio or as a percentage. According to the LoRaWAN v1.0.2 standard specification [11], the duty cycle should be less than 1% in AS923 band.

To evaluate the impact of each parameter on PLR performance, four modeled scenarios are set in single LoRa network with only one channel and one SF. For each scenario, only the parameter being studied and the number of devices vary, while other parameters keep constant. The parameter options of single LoRa network test are given in the following Table. After analysis, the single network capacity was estimated.

Table 53. Parameter options of single LoRa network test

Parameter	Options
SF	7,8,9,10,11,12
PL	1 byte, 50 bytes, 100bytes, 150bytes, 200bytes, 242bytes
T_{cycle}	3s, 5s, 10s, 20s, 30s, 1min, 2min, 3min, 4min, 5min, 10min, 15min
Duty cycle	1%, 0.1%, 0.05%

2. Harmonization Test of Multiple Networks

Harmonization test of multiple networks was performed on the 1st floor in Science Park 2W Building. In this stage, four concurrent LoRa networks coexist with CLP mesh network.

In the environment with interference, the performance of LoRa networks was studied in

following three scenarios: 1000 LoRa end devices transmit packets with 1% duty cycle, 0.1% duty cycle and 0.05% duty cycle. All LoRa end devices transmit packets with 10-byte application payload which is a typical size that applies to all SF values. Table 4 shows the three scenarios in terms of duty cycle, average transmission cycle and daily traffic volume.

Table 54. The target traffic of three testing scenarios

	Duty Cycle	Average Transmission Cycle (s)	Total Daily Traffic Volume (packets)
Scenario 1	1%	37	2335,100
Scenario 2	0.1%	371	233,500
Scenario 3	0.05%	741	116,800

Scenario 1 was conducted at the most stressful traffic conditions at 1% duty cycle that is allowed by LoRaWAN v1.0.2 specification [11]. Each LoRa end device transmits packets on average 37 seconds. The total traffic volume would be reached at 2335,100 packets per day. While the Scenario 1 is the densest network environment with a significantly high probability of packet collision, Scenario 2 and 3 created more practical traffic conditions to alleviate the entire channel load.

f. Performance evaluation

1. Performance Evaluation of Single Network

The PLR performance of single LoRa network with different configuration parameters (SF, payload length, transmission cycle and duty cycle) are analyzed.

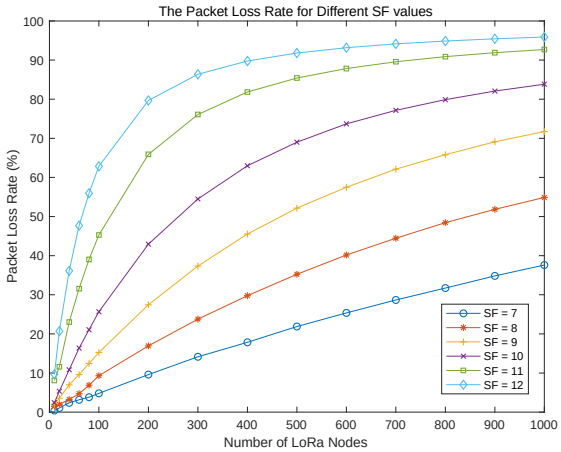


Fig. 41. The packet loss rate for different SF values (i.e. SF = 7,8,9,10,11,12)

Fig. 41 shows the influence of different SF values on the PLR performance (The results are similar with [43]). In this case, LoRa packets with 10-byte length are transmitted every 1min. As the number of LoRa nodes increases, the PLR increases accordingly in all SF values. When the same data packet is transmitted with a higher SF, the packet transmission time increases, the collision probability of the data packets increases, and the packet loss rate becomes higher.

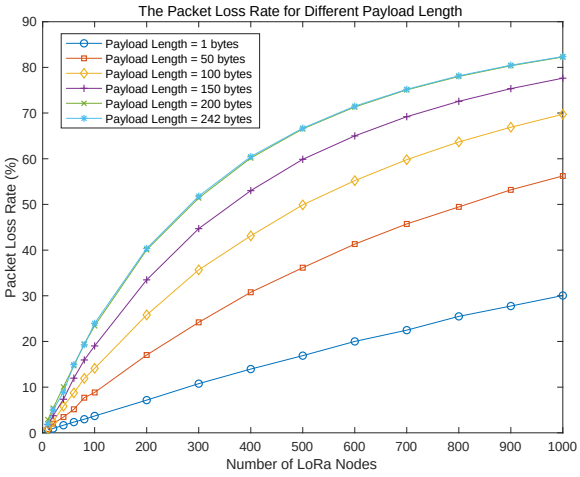


Fig. 42. The packet loss rate for different effective payload length (i.e. 1, 30, 50, 100, 150, 200, 242 bytes)

Fig.42 illustrates the effect of varying effective payload length on the PLR performance. (The results are similar with [45]). According to LoRaWAN v1.0.2 region specification, the allowed effective payload length reaches the maximum value as 242 bytes when SF is equal to 7 (as shown in Table 48). To study the whole payload length range, SF7 is selected and the effective payload length varies from 1 byte to 50 bytes, 100 bytes, 150 bytes, 200 bytes and 242 bytes. It is obvious that the larger the data packet sent, the higher the PLR. Besides, as the number of nodes increases, this impact would be more significant. It is because that when the data packet is larger, the transmission time is longer, and the possibility of collision would increase.

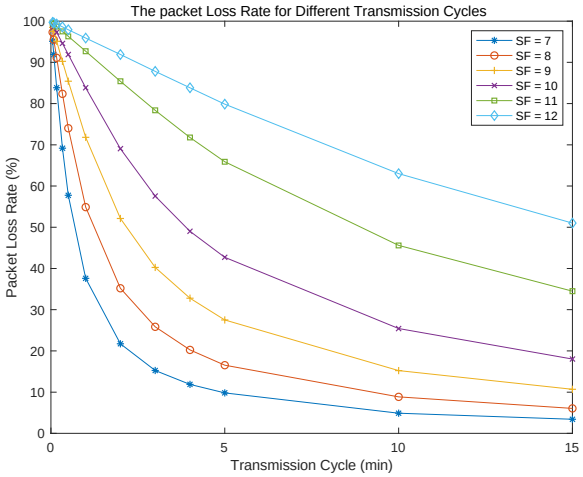


Fig. 43. The packet loss rate for different transmission cycles (i.e. from 3s to 15min)

The PLR performance when 1000 LoRa nodes transmit packets with different transmission cycles is shown in Fig. 43. (The results are similar with [45]). The experimental results show that data packets collision is extremely serious when the transmission interval is less than 1min. Increasing the transmission interval is a very effective approach to alleviate the packet collisions. It can be noticed that the packet loss rate could be maintained below 10% when 1000 LoRa nodes transmit 10-byte packets using lower SFs every 15min in one channel.

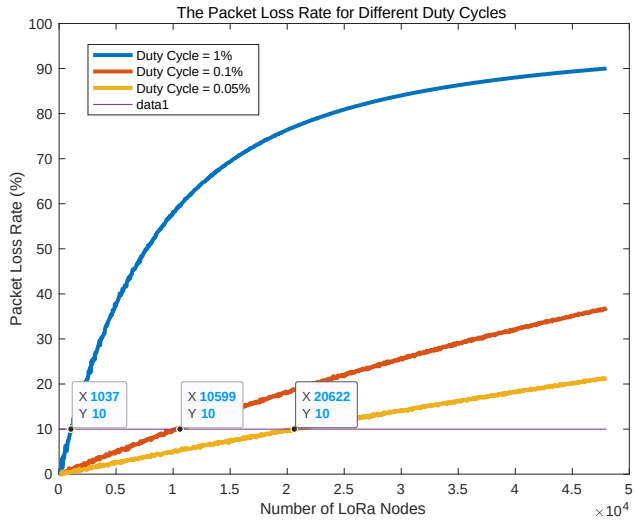


Fig. 44. The packet loss rate for different duty cycles (i.e. duty cycle = 1%, 0.1%, 0.05%)

Fig. 44 illustrates the impact of different duty cycles on the packet transmission performance. (The results are consistent with [46]). In this case, payload length is 10 bytes and all 8 channels and 6 SFs are fully utilized ideally to simulate the ideal capacity of one gateway. As expected in this scenario where the duty cycle is decreased, the packet transmission rate is decreased, and the channel occupancy is also decreased; this reduces the chances of packet

collisions. From the experimental results, when duty cycle is matched with the rule of LoRaWAN standard at 1%, one gateway is able to support about 1000 LoRa nodes (Payload length = 10 bytes) with PLR is less than 10%. As the duty cycle decreases, the number of LoRa nodes that can be supported increases gradually.

2. Performance Evaluation of Multiple Networks

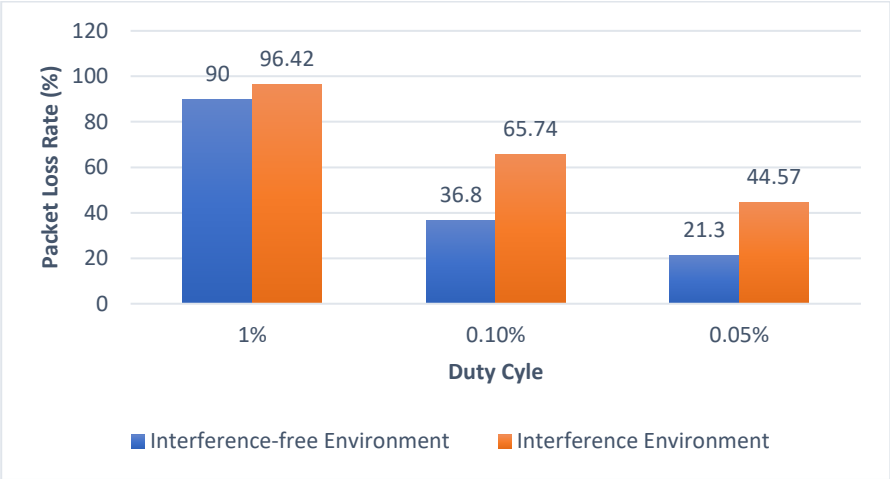


Fig. 45. The comparison of packet loss rate for different interference environment

Under the interference of CLP mesh networks, the PLR performance of one LoRa network was analyzed. To compared with the result of Fig. 44, the configurations (channel = 924.0MHz, SF = 10, Payload Length = 10 bytes, the number of nodes = 1000) were same as before. The comparison of packet loss rate for interference-free and interference environment is shown in Fig. 45. It can be seen that interfered by CLP mesh network, almost all LoRa packets are lost when duty cycle is 1%. The PLR of LoRa network is still larger than 40% even if the duty cycle is decreased to 0.05%. The serious interference nearly doubled the PLR of LoRa network. It is mainly because of the extremely dense signal transmission of CLP mesh network with the transmission cycle of ranging from several milliseconds to minutes. Besides, the signal transmission power of CLP signals is as high as 27dBm, which leads to serious interference on LoRa signals. Hence, to harmonize networks on 920MHz-925MHz, the limitation of duty cycle should be applied to all networks not just LoRa networks.

In summary, there are some harmonization suggestions for 920-925MHz IoT networks:

- To harmonize networks on 920MHz-925MHz, the limitation of duty cycle (< 1%) should be applied to all networks not just LoRa networks.
- To ensure the QoS of data transmission, lower SF values are supposed to be used within the signal coverage.

- The data package structure is as concise as possible to avoid the increased PLR due to redundant data length.
- The average PLP performance is related to the number of nodes of networks.
- When duty cycle < 1%, one gateway theoretically is able to support about 1000 LoRa nodes (Payload length = 10 bytes) with PLR is less than 10%.

g. Conclusion

In conclusion, with the GWIN expansion, three main reasons for LoRa network performance degradation were analyzed. In this situation, harmonization test were performed to alleviate this problem. This test consists of three phases, harmonization test of single LoRa network, harmonization test of multiple networks, and harmonization test of multiple applications. Based on the experiment results of the first two phases, technical guidelines for 920-925MHz IoT networks were provided. In the future, IoT harmonization phase 2 will be conducted to further investigate the best practice of the harmonization of IoT networks.

VIII. Conclusion and Way Forward

This report provided technical guidelines to government departments, enterprises and contractors in deployment and utilization of LoRaWAN-based GWIN through evaluation of trial results and implementation of pilot testbeds. An optimal GWIN infrastructure with redundancy design was proposed through comprehensive evaluations. IDex level based on IEEE P2668 standard was provided to facilitate the management in the decision on the network performance, aid participants to understand their IoT products, and provide guidance on blending of IoT products to evolve into better performance. Multiple pilot tests including LoRaWAN data logger for WSD, personnel tracking evaluation, and IoT message display system at CFT were implemented to provide guidance for future applications.

In the future, the IEEE P2668 standard and a series of solutions will be developed to enhance the GWIN performance and accelerate the industrialization process of GWIN.

- END OF REPORT -

City University of Hong Kong

Electrical and Mechanical Services Department

20-August-2021

Reference

[1] Alam, Shadab, et al. "Internet of Things (IoT) enabling technologies, requirements, and security challenges." Advances in data and information sciences. Springer, Singapore, 2020. 119-126.

[2] Mekki, Kais, et al. "A comparative study of LPWAN technologies for large-scale IoT deployment." ICT express 5.1 (2019): 1-7.

[3] "ICS telecom the ultimate radio network planning tool" [Online]. Available: http://www.iritel.com/images/pdf/ics_telecom_brochure_web.pdf

[4] ADTI support. "Getting Start ICS telecom.pdf", available in ATDI library

[5] ADTI support. "Radio propagation in atdi tools.pdf", available in ATDI library

[6] ADTI support. "Select stations according to surface covered (by station).pdf", available in ATDI library

[7] ADTI support. "Station parameter optimizing.pdf", available in ATDI library

[8] ADTI support. "Vector polygon coverage analysis.pdf", available in ATDI library

[9] TTN Forum: https://www.thethingsnetwork.org/docs/gateways/packet-forwarder/semtech-udp.html

[10] Semtech LoRa Basics Station Protocol: https://doc.sm.tc/station/index.html

[11] LoRa Alliance, "LoRaWANTM 1.0.2 Regional Parameters". [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_regional_parameters_v1.0.2_final_1944_1.pdf

[12] MQTT, "MQTT". [Online]. Available: https://mqtt.org/

[13] Naik, Nitin. "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP." 2017 IEEE international systems engineering symposium (ISSE). IEEE, 2017.

[14] IEEE SA, "P2668 - Standard for Maturity Index of Internet-of-things: Evaluation, Grading and Ranking". [Online]. Available: https://standards.ieee.org/project/2668.html

[15] Mekki, Kais, et al. "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT." 2018 ieee international conference on pervasive computing and communications workshops (percom workshops). IEEE, 2018.

[16] S. Corporation, "An1200.22, lora modulation basics," semtech.com/images/datasheet/an1200.22.pdf, 2015, online; accessed 10-December-2017.

[17] Butun, Ismail, Nuno Pereira, and Mikael Gidlund. "Analysis of LoRaWAN v1. 1 security." Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects. 2018.

[18] LoRa Alliance, "LoRaWANTM 1.1 Specification". [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm_specification_-v1.1.pdf

[19] Sigfox, "Sigfox". [Online]. Available: https://www.sigfox.com/en

[20] Sigfox, "Sigfox connected objects: Radio specifications", [Online]. Available: https://storage.sbg.cloud.ovh.net/v1/AUTH_669d7dfced0b44518cb186841d7cbd75/prod_medias/b2be6c79-4841-4811-b9ee-61060512ecf8.pdf

[21] Lavric, Alexandru, Adrian I. Petrariu, and Valentin Popa. "Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions." IEEE Access 7 (2019): 35816-35825.

[22] U. Raza, P. Kulkarni, and M. Sooriyabandara, ''Low power wide area networks: An overview,'' IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[23] Sigfox, "Sigfox Device Radio Specifications." [Online]. Available: https://build.sigfox.com/sigfox-device-radio-specifications

[24] Buurman, Ben, et al. "Low-Power Wide-Area Networks: Design Goals, Architecture, Suitability to Use Cases and Research Challenges." IEEE Access 8 (2020): 17179-17220.

[25] R. Ratasuk, J. Tan, N. Mangalvedhe, M. H. Ng and A. Ghosh, "Analysis of NB-IoT deployment in LTE guard-band", Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring), pp. 1-5, Jun. 2017.

[26] Popli, Sakshi, Rakesh Kumar Jha, and Sanjeev Jain. "A survey on energy efficient narrowband internet of things (NBIoT): Architecture, application and challenges." IEEE Access 7 (2018): 16739-16776.

[27] GSMA, "Development guide for industrial using nb-iot". [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2019/08/201902_GSMA_IoT-Development_Guide_NB-IoT_for_Industrial.pdf

[28] GSMA. Security Features of LTE-M and NB-IoT Networks. [Online]. Available: https://www.gsma.com/ iot/resources/security-features-of-ltem-nbiot.

[29] "Link Budget". [Online]. Available: https://en.wikipedia.org/wiki/Link_budget

[30] Gambiroža, Jelena Čulić, et al. "Capacity in LoRaWAN Networks: Challenges and Opportunities." 2019 4th International Conference on Smart and Sustainable Technologies (SpliTech). IEEE, 2019.

[31] Lauridsen, Mads, et al. "Coverage and capacity analysis of LTE-M and NB-IoT in a rural area." 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall). IEEE, 2016.

[32] EMSD provided file, " EMSD Sharing on Smart Carpark Trial Presentation for TD.pdf"

[33] Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of security of internet-of-things." IEEE Transactions on Emerging Topics in Computing 5.4 (2016): 586-602.

[34] Sinha, Rashmi Sharan, Yiqiao Wei, and Seung-Hoon Hwang. "A survey on LPWA technology: LoRa and NB-IoT." Ict Express 3.1 (2017): 14-21.

[35] LoRa Alliance, LoRaWANTM What is it?. [Online]. Available: https://lora-alliance.org/about-lorawan/

[36] THE THINGS NETWORK. Frequency Plans. [Online]. Available: https://www.thethingsnetwork.org/docs/lorawan/frequency-plans.html

[37] ROHDE, J. Schwarz D., and J. Schwarz. "Narrowband Internet of Things Whitepaper." (2016). [Online]. Available: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma266/1MA266_0e_NB_IoT.pdf

[38] Sigfox, "Sigfox Technical Overview" [Online]. Available: https://www.avnet.com/wps/wcm/connect/onesite/03aebfe2-98f7-4c28-be5f-90638c898009/sigfox-technical-overview.pdf?MOD=AJPERES&CVID=magVa.N&CVID=magVa.N&CVID=magVa.N

[39] Saaty, Thomas L. "Decision making with the analytic hierarchy process." International journal of services sciences 1.1 (2008): 83-98.

[40] Elsys.se, "ELT-2 Internal antenna". [Online]. Available: https://www.elsys.se/shop/product/elt-2-i/?v=f003c44deab6

[41] SecureThings.UK, "LoRaWAN Energy Calculator released". [Online]. Avaliable: https://securethings.uk/

[42] LoRaTools, "Calculate the air time of your LoRa frame". [Online]. Available: https://www.loratools.nl/#/airtime

[43] Wikipedia, "ALOHAnet". [Online]. Available: https://en.wikipedia.org/wiki/ALOHAnet

[44] The Things Network, "Limitations of LoRaWAN". [Online]. Available: https://www.thethingsnetwork.org/docs/lorawan/limitations.html

[45] Haxhibeqiri, Jetmir, et al. "LoRa scalability: A simulation model based on interference measurements." Sensors 17.6 (2017): 1193.

[46] Semtech, "Understanding the LoRaWAN Capacity White Paper". [Online]. Avaliable: https://blog.semtech.com/understanding-the-lorawan-capacity-whitepaper

[47] Zhu, Hongxu, et al. "Index of Low-Power Wide Area Networks: A Ranking Solution toward Best Practice." IEEE Communications Magazine 59.4 (2021): 139-144.

Appendices

Appendix 1: Site Survey Test Plan of Gateway

Table of Contents

1 INTRODUCTION

This document describes the test specification for site survey for gateway and sensors, which shall be installed for Supply and Installation of Low Power Network System Based on LoRa Standard at Various Locations in Kowloon East for the Government of HKSAR under Contract 1075EM19M.

2 FIELD TEST METHODOLOGY

This section defines the field test methodology and specific test procedures for gateway and sensors for the Supply and Installation of Low Power Network System Based on LoRa Standard at Various Locations in Kowloon East for the Government of HKSAR under Contract 1075EM19M. Test results should be recorded down in the test result sheets.

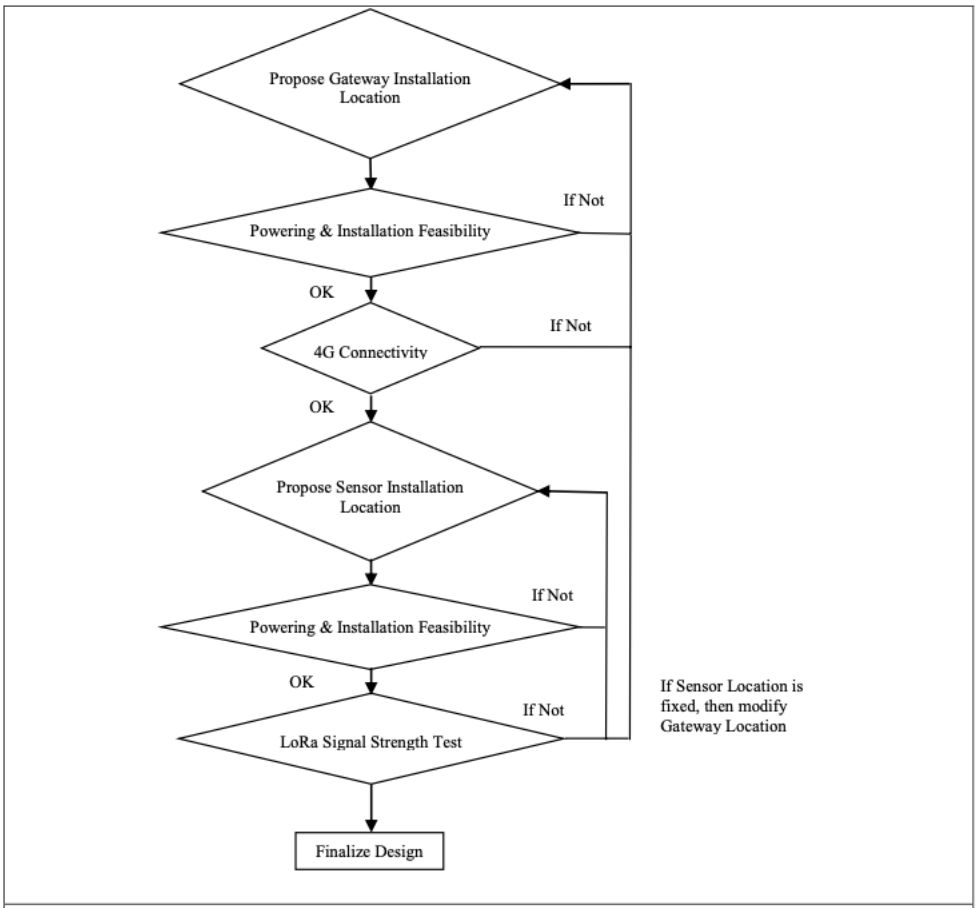


Figure 1 – Site Survey Methodology

2.1 GATEWAY TEST

Test purpose

To confirm the Powering & Installation Feasibility and 4G connectivity at proposed installation location.

Tester

a) Smartphone – OFCA Broadband Performance Test App

Testing procedures

a) Powering & Installation Feasibility Test
   i.) Check if there exists suitable spare MCB or RCBO or spare space in the MCB Board.
   ii.) Check the existing spare MCB or RCBO rating if it is suitable for the proposed gateway; Check the existing spare space if it is suitable for new MCB or RCBO installation for proposed gateway.
   iii.) Assessment of the site condition for the proposed routing and installation method for proposed gateway.
b) 4G Connectivity Test
   i.) Use the OFCA Broadband Performance Test App on Smartphone to simulate the 4G backhaul of the gateway, testing the connectivity at proposed installation location. Test all Network Service Provider's connection under the Contract 1075EM19M (i.e. SmarTone, CSL, etc).
   ii.) Upload and Download data rate: >1Mbps at least; >3Mbps preferable. Record the results. Take the average out of 3 samples.

Possible Action

a) Powering & Installation Feasibility Test
   i.) Existing MCB Board has spare MCB or RCBO and suitable:
      ➔ Use existing spare MCB or RCBO.
   ii.) Existing MCB Board has no spare MCB or RCBO and has spare space:
      ➔ Install new MCB or RCBO.
   iii.) Existing MCB Board has spare MCB or RCBO but is not suitable, and has no spare space:
      ➔ Replace existing spare MCB or RCBO.
   iv.) No available MCB board at site:
      ➔ Evaluate the possibility of installing new MCB board.
   v.) Otherwise:
      ➔ Consult with venue owner for further action.
b) 4G Connectivity Test
   i.) More than one Network Service Provider has reception:
      ➔ Pick the Network Service Provider that has better connection.
   ii.) Only one Network Service Provider has reception:
      ➔ Pick the only choice.
   iii.) No reception:
      ➔ Pick another location.

Test Record

Test form refers to Appendix 1 – Site Survey Record for Gateway and Sensor.

2.2 SENSOR (TYPICAL) TEST

Test Purpose

To measure the LoRa signal strength at proposed installation location.

Tester

a. LoRaWAN Field Tester – Rising HF, RHF4T003

Figure 2: User Interface

The LoRa Field tester will be used for the field test. This unit is to simulate the actual sensor for the measurement of the LoRa parameters. The relevant data will be obtained from the tester and LNS accordingly: Field Tester: Downlink Received Signal Strength Intensity (RSSI), Signal to Noise Ratio (SNR) and Data Rate (DR); LNS: Uplink RSSI and SNR.
In which, the downlink parameters are determining factors while uplink parameters are for reference. The tx power for the tester is set at 14dBm.

Test Procedure

a) Powering & Installation Feasibility Test (Powering test for sensors requiring grid power only)
   i.) Check if there exists suitable spare MCB or RCBO or spare space in the MCB Board.
   ii.) Check the existing spare MCB or RCBO rating if it is suitable for the proposed sensor; Check the existing spare space if it is suitable for new MCB or RCBO installation for proposed sensor.
   iii.) Assessment of the site condition for the proposed routing and installation method for proposed sensor.
b) LoRa Signal Strength Test
   i.) Use the field tester's evaluation mode to evaluate LoRa signal strength at proposed location. Setup a dummy gateway at the proposed installation location. Establish LoRaWAN connection to the LNS.
   ii.) Check Downlink parameters according to field tester, Uplink parameters according to LNS. For each measurement, take the average out of 5 samples. Record the results.
   iii.) LoRa Signal Strength
      1. Downlink RSSI: >= -110dBm (±10dBm)
      2. Downlink SNR: > -20dB
      3. DR: 7 – 12
      4. Uplink RSSI: > -100dBm (±10dBm), for reference only
      5. Uplink SNR: > -10dB, for reference only

iv.) LoRa Signal Strength Reference (Indoor gateway)

Distance from gateway (Line of Sight)	RSSI (dBm)	SNR (dB)
<= 0.1 m	-31	5
<= 1 m	-50	5
<= 3 m	-64	4
<= 10 m	-80	3
100 m ~ 1 km	-90 ~ -110	2 ~ 0

Possible Action

a) Powering & Installation Feasibility Test
   i.) Existing MCB Board has spare MCB or RCBO and suitable:
      ➔ Use existing spare MCB or RCBO.
   ii.) Existing MCB Board has no spare MCB or RCBO and has spare space:
      ➔ Install new MCB or RCBO.
   iii.) Existing MCB Board has spare MCB or RCBO but is not suitable, and has no spare space:
      ➔ Replace existing spare MCB or RCBO.
   iv.) No available MCB board at site:
      ➔ Evaluate the possibility of installing new MCB board.
   v.) Otherwise:
      ➔ Consult with venue owner for further action.
b) LoRa Signal Strength Test
   i.) Acceptable signal reception:
      ➔ Install the sensor as proposed.
   ii.) Poor signal reception:
      ➔ Pick another location for installation.
c) Additional interface provision is required for connection from the existing equipment to the proposed sensor, for potential sensor application (such as: marshalling box with interface terminals, Modbus RS485 interface provision, etc):
      ➔ Associated interface requirements shall be clearly stated and coordinated with the representative of relevant service division or venue owner.

Test Record

Test form refers to Appendix 1 – Site Survey Record for Gateway and Sensor.

Site Survey Record for Gateway and Sensors

Proposed Gateway Location: _____ Date: _____
Dummy Gateway Equipment ID: _____ Site Visited: _____

LoRa Signal Strength Test

	Proposed Sensor Location	Non-Essential (for reference only)		Uplink		Downlink			Selected ? (Please tick)	Proposed Sensor Model	Additional Interface Provision for the Proposed Sensor Required ? (Please tick)
		Latitude (N)	Longitude (E)	RSSI (-dBm)	SNR (dB)	RSSI (-dBm)	SNR (dB)	DR			
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

4G Connectivity Test

Network Service Provider		
Upload Datarate (Mbps)		
Download Datarate (Mbps)		
Selected ? (Please Tick)		

* i.e. CSL, SmarTone, etc
** 4G Data rate measurement should be taken as average out of 3 samples

Reference Table

LoRa Parameters	Passing Criteria
Downlink RSSI	>= -110 dBm (±10dBm)
Downlink SNR	>= -20 dBm
Uplink RSSI	>= -100 dBm (±10dBm)
Uplink SNR	>= -10dB
DR	Between 7 - 12

* LoRa measurement should be taken as average out of 5 samples

Remark:

Tested by SHSI: Witnessed by EMSD:

Name: _____ Name: _____
Signature: _____ Signature: _____
Date: _____ Date: _____

Appendix 2: Site Acceptance Test Plan of Gateway

Table of Contents

1 INTRODUCTION

This document describes the test specification for site acceptance for gateway and cables, which shall be installed for Supply and Installation of Low Power Network System Based on LoRa Standard at Various Locations in New Territories East for the Government of HKSAR under Contract 1050EM19M.

2 CABLE TEST & COMMISSIONING

This section defines the testing and commissioning (T&C) specification of cables required for the Supply and Installation of Low Power Network System Based on LoRa Standard at Various Locations in New Territories East for the Government of HKSAR. This T&C document includes acceptance standard and test procedures, there the test result should be recorded down in the test result sheets

2.1 CABLE TESTING: POWER CABLE

Test purpose
To confirm the 13A power socket / switched fused spur unit and power cables are in correct position and in good operating condition.

Tester
a) Digital Multimeter
b) Insulation Tester

Test Configuration
a) Insulation Resistance Test

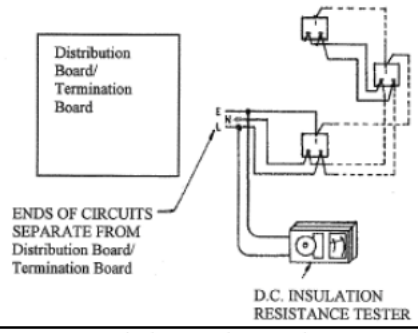


Figure 1 - Insulation Resistance between to Earth Test (L and E)

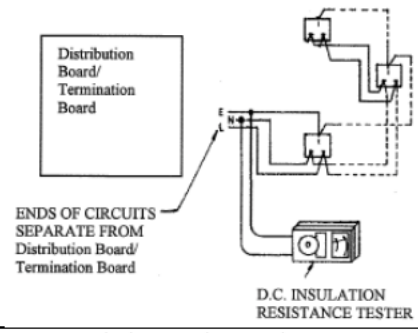


Figure 2 - Insulation Resistance between to Earth Test (N and E)

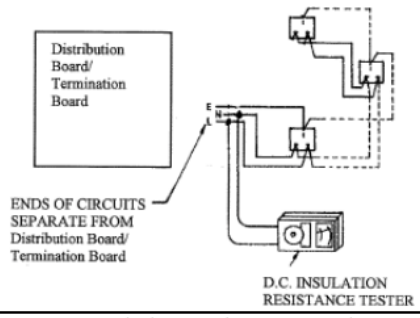


Figure 3 - Insulation Resistance Test between Phases (L and N)

b) Continuity Test

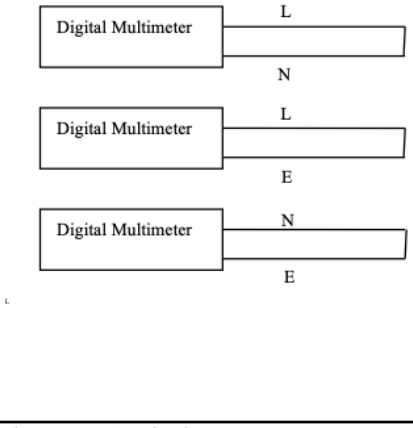


Figure 4 - Continuity Test

Testing procedures with inputs and expected output

a) Visual Inspection
- i.) Visual inspection by checking against drawings.
- ii.) Check the Cables, glands, bushes and sockets are securely fixed.
- iii.) Visual check of the electricity supply to 13A power socket / switched fused spur unit

b) Insulation Resistance Test
- i.) Use the Insulation tester and set up as figure 1-3, using 500VDC for testing.

c) Continuity Test
- i.) Use the digital multimeter and set up as figure 4.

d) Issue of WR1
- i.) SHSI will provide EMSD with WR1 form to cover fixed electrical installation completed by SHSI.

Expected Test Result

a) Insulation Resistance Test
Using 500VDC in tester, cable insulation resistance is at least 500M ohms.

b) Continuity Test
Use the digital multimeter, the cable resistance is less than or equal to 0.99 ohms.

Test Record

Test form refers to Appendix 1 – Test Record for power cable.

3 FIELD EQUIPMENT TEST & COMMISSIONING

3.1 VISUAL INSPECTION

Before the functional test, check the following task:

Item	Description	Expected Result
1	Gateway Cabinet is installed with right location. Installation is of acceptable workmanship.	Equipment is located as Drawing.
2	Gateway Cabinet is properly installed with proper labeling which includes contract number and inquiry contact point. Installation is of acceptable workmanship.	Equipment is installed with proper labeling as Drawing.
3	Gateway Cabinet is properly secured with lock.	The lock of Gateway Cabinet is in good condition.
4	Visual check all cables are properly wired and terminated with labelling. Installation is of acceptable workmanship.	Cables are wired and terminated as Drawing.

3.2 GATEWAY TESTING & COMMISSIONING

Test Purpose

a. To measure the LoRa signal strength and coverage
b. To check 4G connectivity
c. To check health status of the gateway
d. To check the configuration of gateway and gateway firmware
e. To verify the performance of gateway complied with HKCA 1078 issue 1 dated December 2017

Tester

a. LoRaWAN Field Tester – Rising HF, RHF4T003

Figure 5: User Interface

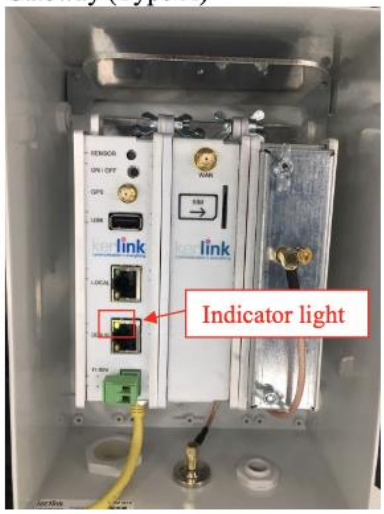
The LoRa Field tester will be used for the field test. The relevant data will be obtained from the tester and LNS, for example, Downlink, Uplink, Spreading factor (SF) and signal-to-noise ratio (SNR).

b. Spectrum Analyzer – Rohde & Schwarz FSH4

The Spectrum Analyzer will be used for verify the performance of gateway complied with HKCA 1078 issue 1 dated December 2017.

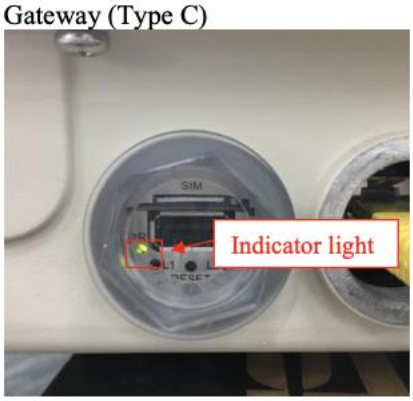
Test Procedure

1. Isolate the gateway and field tester in separate LNS during SAT
2. Check the health status of the gateway on indicator light
   i) Gateway (Type A)



ii) Gateway (Type B)

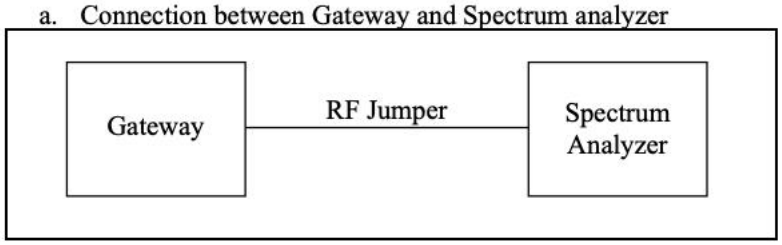
iii) Gateway (Type C)



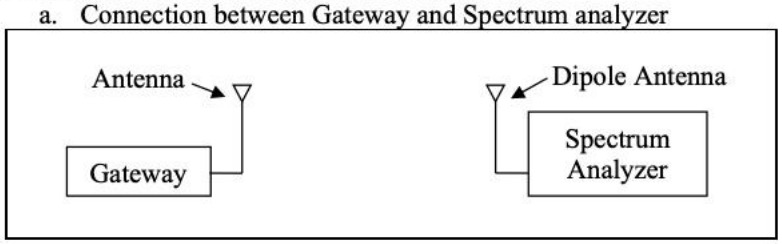
iv) Gateway (Type D)

v) Gateway (Type E)

3. Check and Record the 4G connectivity
4. Check the configuration of gateway and gateway firmware by using putty
   i) Login gateway
   ii) Record gateway system information (firmware version)
   iii) Ping LNS gateway address
5. Verify and Record the performance of gateway complied with HKCA 1078 issue 1 dated December 2017 by using spectrum analyzer (Make sure the spectrum analyzer is under the calibration period)
   i) Measure and Record the operating frequency, and Check the operating frequency is in the frequency band 920 – 925 MHz
   ii) Measure and Record the bandwidth of hopping channel is 500kHz, and Check the bandwidth < 20dB
   iii) Measure and Record the peak transmitter power, and Check the peak transmitter shall not exceed 1W
      a. Connection between Gateway and Spectrum analyzer



   iv) Measure and Record the equivalent isotropically radiated power (EIRP) from the gateway, and Check the EIRP shall not exceed 4W
      a. Connection between Gateway and Spectrum analyzer



   v) Measure and Record the spurious emission level of the gateway, and Check the

spurious emission level shall not exceed 10μW (-20dBm) outside the frequency band in which the fundamental frequencies are located.

6. Field Test
   i) Record the Downlink, Uplink, SF and SNR (Uplink and Downlink) from field tester and LNS
   ii) Test point selection
      a) For outdoor gateway
         16 test points in total (LOS and NLOS)
         - 1 test point below the antenna
         - at least 6 test points: within 100m
         - at least 6 test points: between 100m to 1km
      b) For indoor gateway
         20 test points in total
         - 1 test point: below the antenna
         - at least 4 test points: same floor of gateway location
         - at least 10 test points: adjacent floors of gateway location

Expected Results

1. Isolated the gateway and field tester in separate LNS
2. Indicator light is ON
3. Data Rate >1Mbps
4. The configuration of gateway and gateway firmware is shown in putty
5. Verified the performance of gateway complied with HKCA 1078 issue 1 dated December 2017
   i) The operating frequency is in the frequency band 920 – 925 MHz
   ii) The bandwidth < 20dB
   iii) The peak transmitter shall not exceed 1W
   iv) The EIRP shall not exceed 4W
   v) The spurious emission level shall not exceed 10μW (-20dBm) outside the frequency band in which the fundamental frequencies are located
6. Downlink, Uplink, SF and SNR (Uplink and Downlink)
   i) Downlink (general test point) > -110dBi (±10dBi)
   ii) Downlink (test point below the antenna) > -60dBi
   iii) SF between 7 – 12
   iv) SNR (Uplink) within -10dB
   v) SNR (Downlink) within -20dB

Test Record

Test form refers to Appendix 2 – Test Record for Gateway
Test form refers to Appendix 3 – Test Record for LoRa signal Coverage Field Test

APPENDIX 1 - TEST RECORD FOR POWER CABLES

Date: _____

Location: _____

1. Tester

Tester	Description	Serial Number	Calibration Cert. No.	Calibration Due Date
1	Digital Multimeter			
2	Insultation Tester			

2. Visual Inspection

Cable Laid and Tied Properly	Cable Marking (Both End)	Cable Terminated Properly
Yes / No	Yes / No	Yes / No

Remark:

_____

_____

Test by SHSI:

Name: _____

Signature: _____

Date: _____

Witnessed by EMSD:

Name: _____

Signature: _____

Date: _____

APPENDIX 2 - TEST RECORD FOR GATEWAY

Date: _____
Location: _____
Latitude (N) _____
Longitude (E) _____
Gateway Equipment ID: _____
Structure Calculation (if necessary) _____

1. Tester

Tester	Description	Model
1	Field Tester	Rising HF, RHF4T003
2	Spectrum Analyzer	Rohde & Schwarz, FSH4 Calibration Certificate no.:_____ Calibration Due Date: _____

2. Specification

Item	Description	
1	Gateway altitude (m)	
2	Antenna type (e.g. omnidirectional/directional)	
3	Antenna connector (e.g. Type-N, UHF, standard TNC)	
4	Antenna length (m)	
5	Antenna gain (dBi)	
6	RF cable length (m)	
7	RF cable impedance (ohm) (e.g. 50ohm/75ohm)	

(Please check the product specification)

3. Test Result Record

Item	Description	Result	Pass / Fail
1	Gateway indicator light Pass if ON	ON / OFF	Pass / Fail
2	Data Rate of 4G connectivity (Mbps) Pass if Data Rate>1Mbps		Pass / Fail
3	Gateway firmware version		

4	Ping LNS gateway address Pass if Success	Success / Failure	Pass / Fail
5	Antenna VWSR		Pass / Fail
6	RF cable loss (dB)		

4. The design and performance of gateway complied to HKCA 1078 issue 1 dated December 2017

Item	Description	Result	Pass / Fail
4.1	Gateway Operating frequency (MHz) Pass if Operating frequency is in frequency band 920 – 925MHz		Pass / Fail
4.2	Bandwidth of the hopping channel (500kHz) Pass if Bandwidth < 20dB		Pass / Fail
4.3	Peak transmitter power (W) Pass if peak transmitter power ≤1W		Pass / Fail
4.4	Equivalent Isotropically Radiated Power, EIRP (W) Pass if EIRP from the gateway ≤ 4W		Pass / Fail
4.5	The spurious emission level of the gateway Pass if the spurious emission level ≤ 10μW (-20dBm) outside the frequency band in which the fundamental frequencies are located		Pass / Fail

Remark:

Test by SHSI:

Name: _____

Signature: _____

Date: _____

Witnessed by EMSD:

Name: _____

Signature: _____

Date: _____

APPENDIX 3 - TEST RECORD FOR LORA SIGNAL COVERAGE FIELD TEST

	Test Point Location	Antenna Height(m)	Distance away from gateway (m)	Latitude(N)	Longitude(E)	Channel	SF	Tester Tx Power(dBm)	Tx Interval(s)	Retry times	Uplink(-dBm)	Downlink(-dBm)	SNR(Uplink)	SNR(Downlink)	PLR(%)	Floor No. (Just for indoor)	Signal Strength according to Downlink (Excellent/ Good/ Fair/ Poor/ No Signal)
1	Below the Antenna																(Excellent/ Good/ Fair/ Poor/ No Signal)
2	LOS																(Excellent/ Good/ Fair/ Poor/ No Signal)
3																	(Excellent/ Good/ Fair/ Poor/ No Signal)
4																	(Excellent/ Good/ Fair/ Poor/ No Signal)
5																	(Excellent/ Good/ Fair/ Poor/ No Signal)
6																	(Excellent/ Good/ Fair/ Poor/ No Signal)
7																	(Excellent/ Good/ Fair/ Poor/ No Signal)
8																	(Excellent/ Good/ Fair/ Poor/ No Signal)
9																	(Excellent/ Good/ Fair/ Poor/ No Signal)
10																	(Excellent/ Good/ Fair/ Poor/ No Signal)
11																	(Excellent/ Good/ Fair/ Poor/ No Signal)
12																	(Excellent/ Good/ Fair/ Poor/ No Signal)
13																	(Excellent/ Good/ Fair/ Poor/ No Signal)
14																	(Excellent/ Good/ Fair/ Poor/ No Signal)
15																	(Excellent/ Good/ Fair/ Poor/ No Signal)
16																	(Excellent/ Good/ Fair/ Poor/ No Signal)
17																	(Excellent/ Good/ Fair/ Poor/ No Signal)
18																	(Excellent/ Good/ Fair/ Poor/ No Signal)
19	NLOS																(Excellent/ Good/ Fair/ Poor/ No Signal)
20																	(Excellent/ Good/ Fair/ Poor/ No Signal)
21																	(Excellent/ Good/ Fair/ Poor/ No Signal)
22																	(Excellent/ Good/ Fair/ Poor/ No Signal)
23																	(Excellent/ Good/ Fair/ Poor/ No Signal)
24																	(Excellent/ Good/ Fair/ Poor/ No Signal)
25																	(Excellent/ Good/ Fair/ Poor/ No Signal)
26																	(Excellent/ Good/ Fair/ Poor/ No Signal)
27																	(Excellent/ Good/ Fair/ Poor/ No Signal)
28																	(Excellent/ Good/ Fair/ Poor/ No Signal)
29																	(Excellent/ Good/ Fair/ Poor/ No Signal)
30																	(Excellent/ Good/ Fair/ Poor/ No Signal)
31																	(Excellent/ Good/ Fair/ Poor/ No Signal)
32																	(Excellent/ Good/ Fair/ Poor/ No Signal)
33																	(Excellent/ Good/ Fair/ Poor/ No Signal)
34																	(Excellent/ Good/ Fair/ Poor/ No Signal)
35																	(Excellent/ Good/ Fair/ Poor/ No Signal)

APPENDIX 4 – EQUIPMENT SCHEDULE

Date: _____

Location: _____

1. Gateway information

Product brand: _____

Model: _____

Serial number: _____

Equipment ID: _____

SIM card no.: _____

SIM card start date: _____

2. Equipment Schedule

Item	Description	Quantity	Remark
A1.1	Supply and installation of Gateway (Type A) and necessary accessories		
A1.2	Supply and installation of Gateway (Type B) and necessary accessories		
A1.3	Supply and installation of Gateway (Type C) and necessary accessories		
A1.4	Supply and installation of Gateway (Type D) and necessary accessories		
A1.5	Supply and installation of Gateway (Type E) and necessary accessories		
A1.7	Supply and installation of PoE+ injector and necessary accessories		
A1.8	Supply and installation of gateway (provided by EMSD) and necessary accessories		
A1.9	Relocation of gateway and accessories		
A1.10	Supply and installation of cabinet for gateway		
A1.11	Supply and installation of additional 6dBi antenna (omni-directional) for gateway with accessories		
A1.12	Supply and installation of additional 6dBi antenna (directional) for gateway with accessories		
A1.13	Supply and installation of additional 9dBi or higher gain antenna (omni-directional) for gateway with accessories		
A1.14	Supply and installation of additional 9dBi or higher gain antenna (directional) for gateway with accessories		
A1.15	Supply and installation of CAT6 STP Cable with GI conduit, adaptable box and accessories, per meter		
A1.16	Supply and installation of Power Supply Cable with GI conduit, adaptable box and accessories, per meter		
A1.17	Engineering service for venues (footbridge)		

A1.18	Engineering service for venues (PTI)		
A1.19	Engineering service for venues (subway)		
A1.20	Engineering service for venues (building)		
A1.21	Engineering service for venues (lamppost)		
A1.22	Engineering service for venues (traffic light pole)		
A1.23	Engineering service for venues (other venues)		
A1.24	4G mobile service subscription (each for 24 months)		
A1.40	Erection and subsequent dismantle of working platform at a height between 2 meter to 5 meter from finished floor		
A1.41	Erection and subsequent dismantle of working platform at a height above 5 meter but not exceed 8 meter from finished floor		
A1.42	Erection and subsequent dismantle of working platform at a height above 8 meter but not exceed 15 meter from finished floor		
A1.43	Normal working hour, per hour		
A1.44	Outside normal working hour, per hour		
A1.45	Others		

Test by SHSI:

Name: _____

Signature: _____

Date: _____

Witnessed by EMSD:

Name: _____

Signature: _____

Date: _____

Appendix 3: Site Acceptance Test Plan of Sensor

Table of Contents

1 INTRODUCTION

This document describes the test specifications for Site Acceptance Test Plan for Current / Power Meter Sensor as listed in 1050EM19M-MAT-007, which shall be installed for Supply and Installation of Low Power Network System Based on LoRa Standard at Various Locations in New Territories East for the Government of HKSAR under Contract 1050EM19M. This document is applicable to the following sensor models:

Model No.	Description
Netvox R718N1	Single phase, Solid core, 30A CT, 100mA to 30A(± 1%)
Netvox R718N13	Single phase, Split core, 30A CT, 100mA to 30A(± 1%)
Netvox R718N17	Single phase, Split core, 75A CT, 100mA to 75A(± 1%)
Netvox R718N115	Single phase, Split core, 150A CT, 1A to 150A(± 1%)
Netvox R718N125	Single phase, Split core, 250A CT, 1A to 250A(± 1%)
Netvox R718N163	Single phase, Split core, 630A CT, 1A to 630A(± 1%)
Netvox R718N3	Three phase, Solid core, 3 x 60A CT, 1A to 50A(± 1%)
Netvox R718N37	Three phase, Split core, 3 x 75A CT, 1A to 75A(± 1%)
Netvox R718N315	Three phase, Split core, 3 x 150A CT, 1A to 150A(± 1%)
Netvox R718N325	Three phase, Split core, 3 x 250A CT, 1A to 250A(± 1%)
Netvox R718N363	Three phase, Split core, 3 x 630A CT, 1A to 630A(± 1%)

* The testing procedures for CT devices requiring temporarily power off should be stated separately also indicating the duration required for the testing and safety measures required.

2 SENSOR SAT METHODOLOGY

This section defines the Site Acceptance Test methodology and specific test procedures for Current / Power Meter Sensor as listed in 1050EM19M-MAT-007, for the Supply and Installation of Low Power Network System Based on LoRa Standard at Various Locations in New Territories East for the Government of HKSAR under Contract 1050EM19M. Test results should be recorded down in the test result sheets.

2.1 PRE-REQUISITES FOR TEST

a) *Inventory Check*

Maintain an inventory record for installed sensors at test location before commencing SAT..

i) **Baseline information**

Sensor's baseline information should be recorded in the test form, i.e. brand, model, S/N, Device ID, Device EUI, installed location. This can be copied from the inventory record.

ii) **Baseline Configuration**

Sensor's baseline configuration should be recorded in the test form, i.e. heartbeat frequency, reporting interval, triggering event. This can be copied from the inventory record.

iii) **Sensor Specification**

Sensor's specification should be recorded in the test form, i.e. sensor technology, hardware specification. This can be fulfilled by including factory datasheet in the sensor SAT report as an attachment.

b) *Test environment check*

The parameters for test environment should be recorded.

i) Distance or relative position between test points and gateways(within 1km)

ii) Gateway(within 1km) information: Brand, model, antenna gain, LNS

iii) Packet loss: A sample packet loss rate is taken on site with the field tester. This would be the reference value for the sensor under test.

c) *Health Check*

The Sensor is properly installed and operating at the designated location. Health status should be checked before commencing SAT.

i) **Parameters**

Check the latest activity for the sensor from the Grafana dashboard, i.e. the sensor activity for last 7 days before the SAT.

ii) **Acceptance criteria**

The sensor should be alive for at least 24 hrs before the SAT.

d) *Test Equipment*

Item	Model	Purposes	Remarks
A	Dell Latitude 5491 or equivalent devices with internet capability	Access the LNS for checking the health status, uplink message; send downlink command	

B	Huawei P20 Lite or equivalent smartphone with internet capability, camera, video recorder	Take photos or video recordings for reference (Primary) Access the LNS for checking the health status, uplink message; send downlink command (Secondary, can replace Item A)	
C	Fluke 355 Clamp Multimeter	Third party equipment, for reference	
D	RisingHF RHF4T003 FieldTester	Field Testing tool for simulation of sensor packet loss	

2.2 WORKMANSHIP AND VISUAL INSPECTION

Test purpose

To confirm the installation work was in accordance with the approved site preparation plan.
To ensure the installed sensor was not damaged before commencing the SAT.

Item	Description	Expected Result
Equipment Labeling	Sensor is properly installed with proper labeling, including contract number and inquiry contact point.	Equipment is installed with proper labeling as stated in the site preparation plan.
Secured Installation	Sensor is installed in the correct location with acceptable workmanship and comply with manufacturer's recommendation.	Equipment is installed as stated in the site preparation plan and comply with manufacturer's recommendation.
Tidiness & Cleanness	All cables and magnets are properly wired and terminated with labeling. Installation is of acceptable workmanship.	Cables and magnet are wired and terminated as stated in the site preparation plan.

*Magnet termination as shown below:

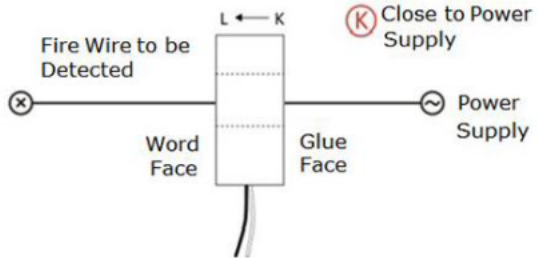


Figure 1 CT sensor magnet direction

Test Record

Test form refers to Appendix 1 – Site Acceptance Test Record Form for Current / Power Meter Sensor.

2.3 FUNCTIONALITY AND SIGNAL TEST

Test Purpose

To ensure the Current / Power Meter Sensor can properly report data to LNS.
To ensure the Current / Power Meter Sensor can report data with acceptable accuracy.

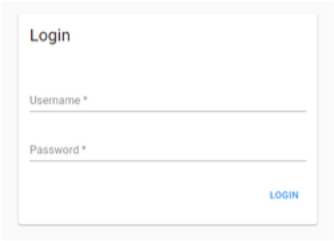
Test Procedure

a) Measure the current of the E&M equipment power supply cables / MCB board final circuit wirings where the current / power meter sensor is installed with the multimeter. This is the reference value to be recorded in the test form.
b) Take three or more samples of the sensor uplink. Record the uplink type, RSSI, SNR, SF/DR, uplink sequence no. and Battery as shown in the uplink payload on the test record form. Pass if the sensor can properly report data to the LNS and with acceptable LoRa parameter.
c) Mark the reported value from the sensor and compare to that of the multimeter. Calculate the % difference, compare with the reference value from factory datasheet. Pass if the sensor readings are within the accuracy range as stated in the factory datasheet.
d) Use the field tester to run a simulation for 10 mins at site. Select a few sample locations, i.e. clean(RSSI<90dBm), noisy(90dBm<RSSI<110dBm), very noisy(RSSI>110dBm). Run a simulation at each of the above environment. Use this packet loss % as a reference. Then compare the last day sensor activity for its packet loss %. Pass if there is no significant packet loss.

e) Detailed Steps

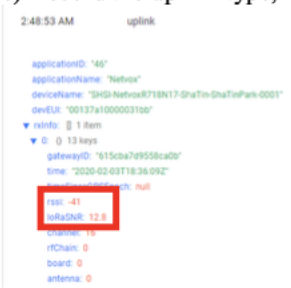
1) Measure the current with multimeter. Record the value on the test form.
Expected Results: The recorded value is reasonable
Remarks: Wait until the reading is steady before recording the value.

2) Record the sensor reported data from LNS.
a) Login to LNS
url: https://loraserver.gwin.emsd.gov.hk/#/login
Username: shsi
Password: sHsi123456!



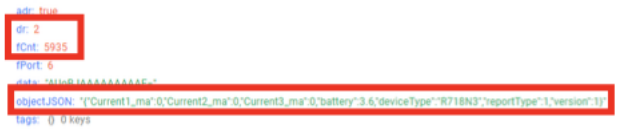
b) Find the sensor page
Path: Applications/Netvox/Device/Sensor_ID/Device Data
Or directly search the Sensor_ID / Device EUI

c) Record the uplink type, RSSI, SNR, SF, uplink sequence no. and Battery



For single phase:

For three phase:



Expected Results: Reasonable reading within the rating of the CT magnet (see part 1). Report reading close to the reference reading.

Uplink type: button-trigger, heartbeat, join, error, start-up:
RSSI: uplink RSSI should not exceed 110dBm:
SNR: uplink SNR should not exceed -10dB;
SF/DR: for this deployment, SF should be SF7-SF12, DR2-DR5, record either SF/DR as shown on the LNS;
Uplink sequence no.: Record the fcnt value, this is the seq. no. for this sensor uplink message, mark this down for each sample to show consistence and insignificant packet loss;
Battery: fresh battery ~3.6V, still functional ~2.7V

d) Mark the reported value from the sensor. Calculate the % difference.
1-phase: 1 current reading is reported, unit in mA
3-phase: 3 current readings are reported, unit in mA
Expected Results: Reported data is of reasonable accuracy according to factory datasheet

e) Repeat the process until 3 valid samples are collected.
Uplink message can be manually triggered by button press, this can speed up the process.

3) Use the field tester to run a simulation for 10 mins at site. Select a few sample locations, i.e. clean(RSSI<90dBm), noisy(90dBm<RSSI<110dBm), very noisy(RSSI>110dBm). Run a simulation at each of the above environment. Use this packet loss % as a reference. Then compare the last day sensor activity for its packet loss %. Pass if there is no significant packet loss.
Expected Results: The sensors should have packet loss % similar to the reference value.
Remarks: One reference value for each type of environment, i.e. clean(RSSI<90dBm), noisy(90dBm<RSSI<110dBm), very noisy(RSSI>110dBm).

Test Record
Test form refers to Appendix 1 – Site Acceptance Test Record Form for Current / Power Meter Sensor.

APPENDIX 1 – SITE ACCEPTANCE TEST RECORD FORM FOR CURRENT / POWERMETER SENSOR

Site Acceptacne Test Record Form for Current/Power Meter Sensor (Per sensor)

Date: ____________________ Venue: ____________________

Sensor baseline information

Brand: ____________________
Model: ____________________
S/N (if any): ____________________
Device ID: ____________________
Device EUI: ____________________
Installed location: ____________________

Sensor baseline configuration:

Heartbeat frequency: ____________________
Reporting Interval: ____________________
Triggering Event: ____________________

Sensor Specification: See datasheet

Workmanship and Visual Inspection

MCB Board Name (if available):	
MCB Way (if available):	
Cable ID (L/N/E):	
Equipment Labels (DevEUI, Contact):	Pass / Fail
Secured Installation*:	Pass / Fail
Tidiness & Cleaness*:	Pass / Fail

*Take photos for the installed sensor for record

Health Check

	Alive?
Last 24 hrs	
Last 7 days	

Test Equipment

Digital Multimeter Model	Serial No.	Cert No./ Cal. Due Date
Fluke 355 Clamp Multimeter		

Actual Readings

Current 1 (mA)	
Current 2 (mA)	
Current 3 (mA)	

Functional and Signal Test

Uplink Seq. # (✓ if Pass)	Uplink Type	Uplink RSSI (dBm)	Uplink SNR (dB)	SF / DR	Battery (V)	Current 1 (mA)	% Diff.	Current 2 (mA)	% Diff.	Current 3 (mA)	% Diff.
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							
☐		☐	☐	☐							

Reference Table

LoRa Parameters	Passing Criteria
Uplink RSSI	>= -110 dBm (±10dBm)
Uplink SNR	>= -10dB
SF / DR	Between 7 – 12
% Difference	±1%

Packet Loss Test

	# Tx packet	# Rx packet	% packet loss
Last day activity(check from Grafana)			

Tested by SHSI:
Name: ____________________
Signature: ____________________
Date: ____________________

Witnessed by EMSD:
Name: ____________________
Signature: ____________________
Date: ____________________

Remarks:

Test Environment check (Per site)

Date: _____ Venue: _____

Nearby gateways(within 1km)

Gateway ID	Brand	Model	Antenna gain (dBi)	LNS	Distance from site

Packet Loss Test

Tester Model: RHF4T003
Tx power: 16dBm
SF/DR: DR5
Interval: 10s

Tester Device ID: _____
Tester Device EUI: _____

Reference	# Tx packet	# Rx packet	% packet loss
Clean (RSSI<90dBm)			
Noisy (90dBm<RSSI<110dBm)			
Very Noisy (RSSI>110dBm)			

Remarks: _____

Tested by SHSI:
Name: _____
Signature: _____
Date: _____

Witnessed by EMSD:
Name: _____
Signature: _____
Date: _____

Appendix 4: The Specifications of Three GPS Trackers

1. Xsense Tracker with Sigfox network subscription

Fig. 1. Xsense Tracker

Xsense Tracker is an IP68 certified mutli-sensor device that embeds sensors including button, temperature, accelerometer, magnetometer, ambient light, reed switch and Wi-Fi sniffer. The specification of the tracker is as follows:

Table 1 – Specification of Xsense Tracker

Item No.	Indicator name	Index parameter
1	Dimension	Device: L100*W45*H16 mm Box: L120*W80*H40 mm
2	Weight	82g
3	Supporting agreement	Sigfox RC4, Wi-Fi 2.4GHz GPS (-165 dBm)
4	Sigfox radio frequency	920-923 MHz (RC4)
5	Sigfox Maximum transmission speed	100 or 600 bit/s (Different Operation Regional)
6	Sigfox Transmission distance	Kilometer level (Urban City)
7	Support terminal type	Browser (Zenzi Platform)
8	Output power	22.5dBm
9	Transmission interval	Action Triggered
11	Power Source	Custom Rechargeable Li Ion Pokymer 530 mAh
12	Battery life	Up to 2.4 months once daily GPS location, up to 1.7 months 9 daily GPS locations per each full charge

13	Operating Temperature	-20°C ~60°C
14	Minimum number of messages	30000
15	Other features	- Accelerometer, Humidity, Temperature, Pressure, reed switch Clicking button with haptic feedback

Xsense Tracker utilizes web-based management platform – Zenzi with the following features:

(a) Main dashboard showing locations of all trackers;

(b) Detailed dashboard showing location history of individual trackers;

(c) Alarm panel for managing geo-fencing alerts; and

(d) Device status display table for the last seen timestamp and battery level.

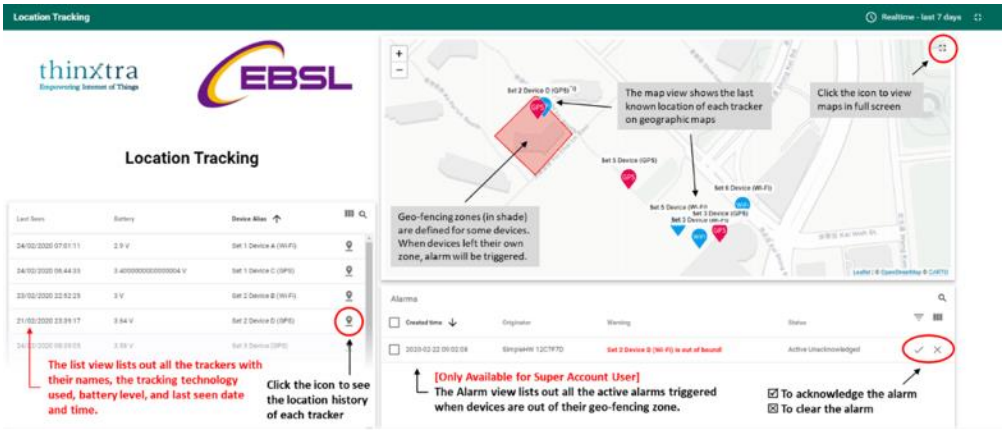


Fig. 2. Main dashboard of Zenzi platform

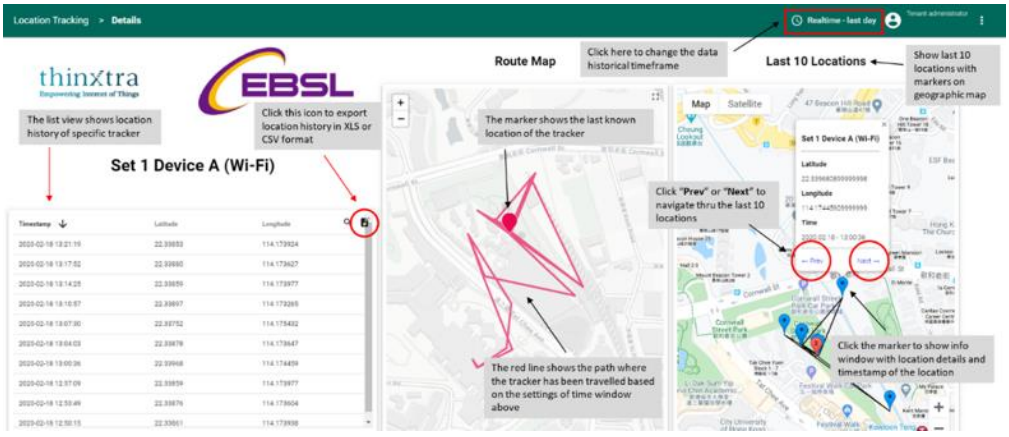


Fig. 3. Detailed dashboard of Zenzi platform

Refer to Fig. 2, the Sigfox tracker performs the positioning functions and make use of

the Sigfox network offered by the service provider for data transmission. It should be noted that the Sigfox network coverage depends on the service provider and thus is not under the scope of evaluation in this report. In this system architecture, the web-based management platform (Zenzi) is a cloud-platform as the user interface offering the positioning services for users.

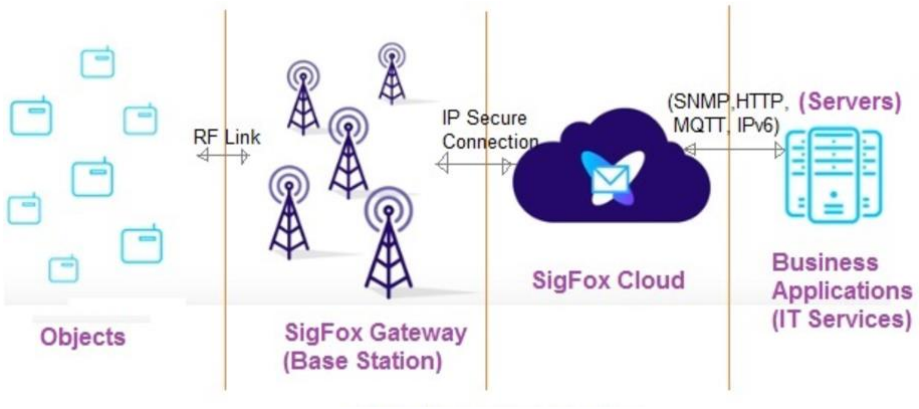


Fig. 2. General Sigfox System Architecture

2. SimplePack 3.0 Plus Full Tracker with Sigfox network subscription

Fig. 5. - SimplePack 3.0 Plus Full Tracker

SimplePack 3.0 Plus Full is an IP68 certified mutli-sensor device that embeds sensors including button, temperature, accelerometer, magnetometer, ambient light, reed switch and Wi-Fi sniffer. The specification of the tracker is as follows:

Table 2 – Specification of SimplePack 3.0 Plus Full Tracker

Item No.	Indicator name	Index parameter
1	Dimension	81 x 29.5 x 12 mm
2	Weight	30g
3	Supporting agreement	Sigfox RC4, Wi-Fi 2.4GHz
4	Sigfox radio frequency	920-923 MHz (RC4)
5	Sigfox Maximum transmission speed	100 or 600 bit/s (Different Operation Regional)

6	Sigfox Transmission distance	Kilometer level (Urban City)
7	Support terminal type	Browser (Zenzi Platform)
8	Output power	22.5dBm
9	Transmission interval	Three mins under continuous motivation (No motivation no transmission)
11	Power Source	Primary LiMnO2 1500 mAh (non-rechargeable & non-replaceable)
12	Battery life	10 years
13	Operating Temperature	-20°C ~60°C
14	Minimum number of messages	30000
15	Other features	- Accelerometer, magnetometer, ambient light, reed switch - Clicking button with haptic feedback Vibration sensitivity threshold setting

The SimplePack3.0 Plus Full Track utilizes the same web-based management platform – Zenzi with Xsense.

3. CSL G20 Pro Tracker with NB-IoT network subscription

Fig. 6. CSL G20 Pro Tracker

The specification of the tracker is as follows:

Table 3 - Specification of CSL G20

Item No.	Indicator name	Index parameter
1	Dimension	54 x 33 x 18 mm
2	Weight	26.6g

3	Supporting agreement	CSL NB-IoT, GPS, Wi-Fi 2.4GHz
4	NB-IoT radio frequency	900MHz
5	NB-IoT Maximum transmission speed	250 kb/s (180kHz bandwidth)
6	NB-IoT Transmission distance	Kilometer level (Urban City)
7	Support terminal type	Petbiz APP (IOS & Android)
8	Output power	23 dBm
9	Transmission interval	Activation Triggered
11	Power Source	Rechargeable Battery
12	Battery life	30 days
13	Operating Temperature	N.A (Compliance with HK Environment)
14	Water Resistant	IPX7
15	SIM Card	Embedded Sim Card

CSL G20 Pro Tracker utilizes the mobile application – Petbiz (IOS & Android) with the following features:

(f) Device location history;

(g) Geo-fencing configuration and alerts;

(h) Device status display;

(i) Low battery alert; and

(j) e-leash alert (Bluetooth close range).

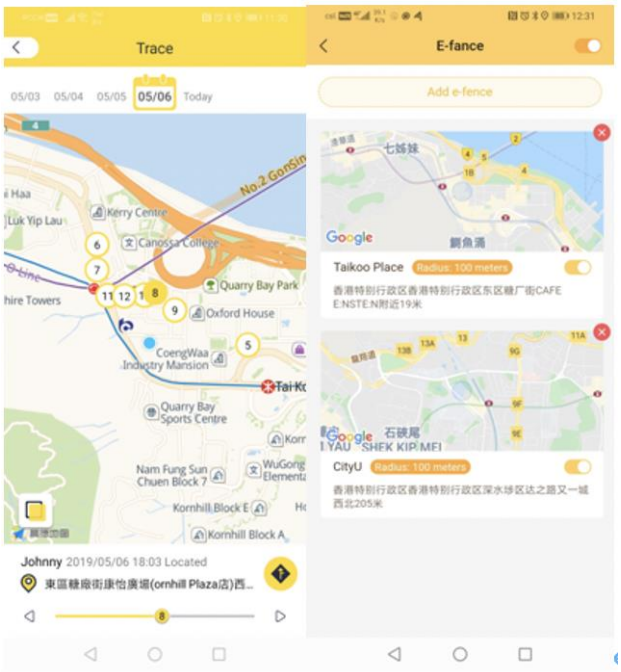


Fig. 7. Mobile Application

Refer to Fig, the NB-IoT tracker performs the positioning functions and make use of the NB-IoT network with gateway/base stations deployed by Internet Service Provider for data transmission. It should be noted that the NB-IoT network coverage depends on the service provider and thus is not under the scope of evaluation in this report. In this system architecture, the application server transmits positioning messages generated by G20 Pro trackers to the mobile application Petbiz APP, which is the user interface offering the positioning services for users.

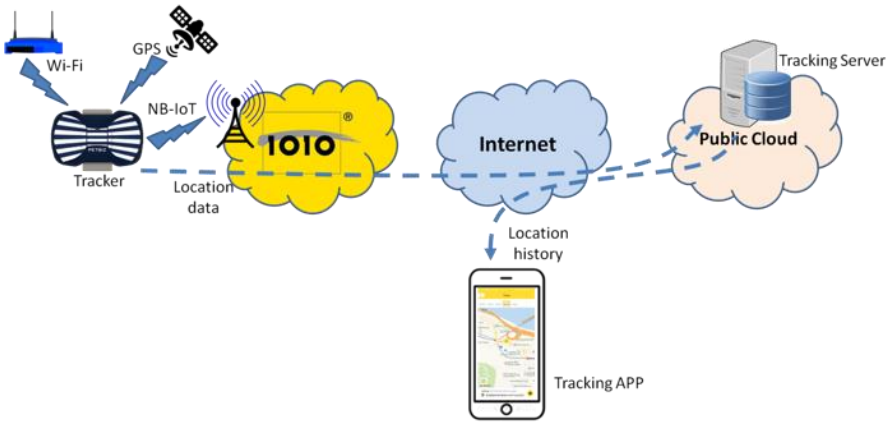
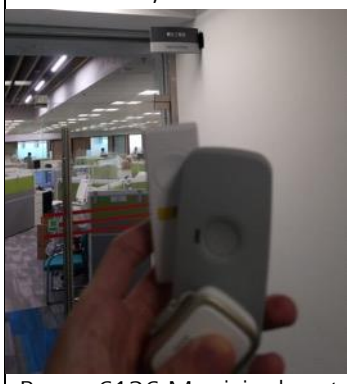


Fig. 8. GPS Tracker System Architecture

Appendix 5: The Test Outcomes of Three GPS Trackers

1. Xsense test outcome

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
1	Signal broadcasting interval	Measuring the broadcasting interval of the sampled Xsense Tracker	The shortest interval found in the test is about 2mins.
2	Outdoor Positioning Accuracy (Comparing to the phone map location at each testing point which is applying for outdoor positioning testing)	Take the Xsense Tracker to 3 designated outdoor locations, and then check the position displayed on the platform. The 3 designated outdoor locations include:	EMSD to KITAC bridge middle 22.32469, 114.203531 (~52.7m) 22.32467,114.203474 (~54.32m) Phone: 22.325158,114.203450 22.325251,114.203415 22.325239,114.203463 KITAC tesla 22.32469, 114.203531 (~18.4m) Phone 22.324531,114.203508 22.324550,114.203386 22.324556,114.203425 (Description: The coordinates of Phone refer that these coordinates are collected from phone map for accuracy evaluation reference in each testing location. Other collected coordinates are the practical testing outcome of each testing trackers. Below is the same.)
		EMSD HQ Piazza	EMSD Cafe G/F 22.32557, 114.203843 (~18.02m) Phone: 22.325636,114.203683
		Richland garden Point 1	N/A
		Richland garden Point 2	N/A

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
	City University of Hong Kong Outdoor Area	CityU Port A	 22.33640, 114.174006 (~20m) 22.33640 114.174012 (~19m) 22.33640, 114.174025 (~18m) Phone Location: 22.33656, 114.174172
3	Indoor Positioning Accuracy (Comparing to the current phone map location at each testing point which is applying for indoor positioning testing)	Place the Xsense Tracker at different places in 4/F and 6/F. Check if the tracker could communicate with Zenzi Platform through Sigfox radio. Take the tracker to the designated indoor position of 4/F and 6/F, and then check the position shown on the platform. The designated Location are:	衛生工程部 6/F 22.32546, 114.203626(73.5m) Phone 22.325568,114.202921 22.325578,114.202929 22.325570,114.202909  Room 6136 Municipal sactor 22.32586, 114.203743(61.8m) Phone 22.325800,114.203145 22.325796,114.203120 22.325798,114.203122

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
			22.32532, 114.203552 
		4/F GWIN Booth	22.32532, 114.203552 (~39.46m) Phone 22.325553,114.203237 22.325529,114.203242 22.325564,114.203245 
		4/F Male Toilet in E&M Innozone	22.32501, 114.203607 (~68.41m) Phone  22.325463,114.203157 22.325449,114.203138 22.325437,114.203141
		4/F No. 19 booth in E&M Innozone	Booth 19 Not Found

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
		6/F SE's Room in DTD Office	Phone 22.326761,114.203983 22.326740,114.203957 22.326757,114.203958 No signal 
		6/F BIM-AM Centre Room A	22.32645, 114.204644 (~75.8m) phone: 22.326778,114.203998 22.326775,114.203982 22.326783,114.203983 
	City University of Hong Kong Indoor Test	1 FungYungWah building FYW 1372	 No Signal Received

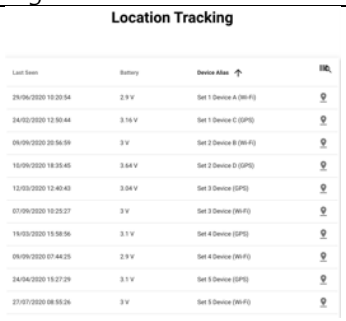
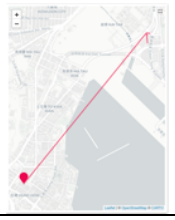
Item No.	Description	Testing Procedure	Remark/Comments/Outcome
		2 CityU Innovation Center (Indoor Area)	 No Signal Received
5	Transition of Indoor & Outdoor Positioning	Install the XSense Tracker at the ground floor in EMSD HQ. Test the positioning radio carrier usage.	About 15 minutes to change the localization method
6	Battery Life	Check whether the XSense Tracker can continuously work more than 14 days.	Yes

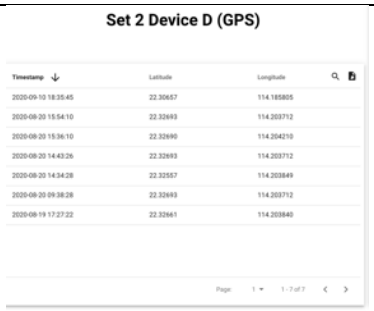
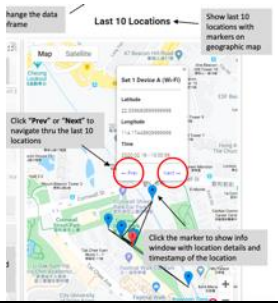
2. SimplePack test outcome

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
1	Signal broadcasting interval	Measuring the broadcasting interval of the sampled SimplePack Tracker	No Sigfox signal (The practical triggering interval cannot be measured.)
2	Indoor Positioning Accuracy (Comparing to the current phone map location at each testing point which is applying for indoor positioning testing)	Place the SimplePack Tracker at different places in 4/F and 6/F. Check if the tracker could communicate with Zenzi Platform through Sigfox radio. Take the tracker to the designated indoor position of 4/F and 6/F, and then check the position shown on the platform. The designated Location are:	No Sigfox Signal Received in EMSD HQ. The triggering method of Simplepack is different to the resources provided by EBSL.
		4/F GWIN Booth	
		4/F Male Toilet in E&M Innozone	
		4/F No. 19 booth in E&M Innozone	
		6/F SE's Room in DTD Office	
		6/F BIM-AM Centre Room A	
		6/F Working spaces	
	City University of Hong Kong Indoor Test	1 FungYungWah building FYW 1372	
		2 CityU Innovation Center	
		3 CityU Exit Port A Lift (Indoor Area)	
3	Battery Life	Check whether the SimplePack Tracker can continuously work more than 14 days.	

Zenzi Platform Tests:

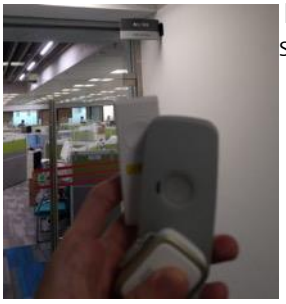
Item No.	Description	Testing Procedure	Pass Criteria
1	Login page		 Redirect to Home Page of the platform in 10 seconds

		Open Login Page, enter 'Username', 'Password' and login	
2	Devices management	 The registered trackers information is shown in the webpage of Zenzi Platform. (Last seen, Battery Voltage, Device Alias and Finding)	List shown the trackers.
3	Tracker Distribution Map	After logged-in, the tracker distribution map is shown in the main page.	Display the outdoor location of all devices.   Click the track label to view the detailed information included: Latest Latitude, Latest Longitude and Show Details.
4	Tracker Alarm	Displayed in the main page of Zenzi platform (Mainly for Geo-fencing function)	
5	Route Map	Click one of the listed tracker in 4.3 and display the "Route Map"	Display the "Route Map" of the selected trakcer. 

6	Tracker History Data	Click one of the listed tracker in 4.3 and display the "Tracker Name + (Positioning Carrier)" with tracker position records	 Display the detail information of selected tracker.
7	Last Ten Locations	Click one of the listed tracker in 4.3 and display the "Last Ten Locations"	Display the last ten locations of selected tracker. 

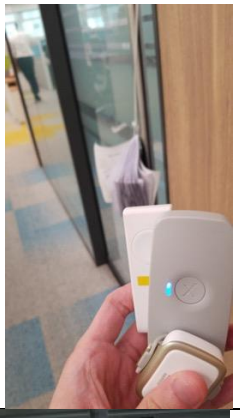
3. G20 Pro test outcome

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
1	Input to the platform.	Check if the G20 Pro Tracker has been launched on the Perbiz App.	
		Check the tracker position whether match with that of the App.	
2	Signal broadcasting interval	Measuring the broadcasting interval of the sampled G20 Pro Tracker	
3	Outdoor Positioning Accuracy (Comparing to the phone map location at each testing point which is applying for outdoor positioning testing) Petbiz App cannot support show out the positions coordinates directly.	Take the G20 Pro tracker to 3 designated outdoor locations, and then check the position displayed on the platform. The 3 designated outdoor locations include:	
		EMSD HQ Piazza	Outdoor 22.326056,114.203923 (52.82m) Phone: 22.325636,114.203683 (Description: The coordinates of Phone refer that these coordinates are collected from phone map for accuracy evaluation reference in each testing location. Other collected coordinates are the practical testing outcome of each testing trackers. Below is the same.)
		Richland garden Point 1	N/A
		Richland garden Point 2	N/A

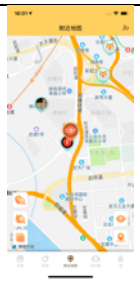
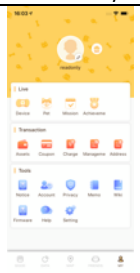
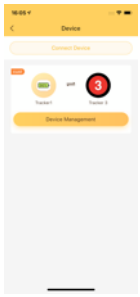
Item No.	Description	Testing Procedure	Remark/Comments/Outcome
	City University of Hong Kong Outdoor Area	CityU Port A	 22.33640, 114.174035 (~ 17m) 22.33640, 114.174020 (~ 18m) 22.33640, 114.174024 (~ 18m) Phone Location: 22.33656, 114.174172
4	Indoor Positioning Accuracy (Comparing to the current phone map location at each testing point which is applying for indoor positioning testing) Petbiz App cannot support show out the positions coordinates directly.	Place the G20 Pro Tracker at different places in 4/F and 6/F. Check if the tracker could communicate with Petbiz App through NB-IoT radio. Take the tracker to the designated indoor position of 4/F and 6/F, and then check the position shown on the platform. The designated Location are:	Health sactor 6/F 22.325323,114.203528 (~68.12m) 22.325290,114.203524 (~69.30m) 22.325285,114.203518 (~69.00m) Phone 22.325568,114.202921 22.325578,114.202929 22.325570,114.202909  Municipal sactor 22.326260,114.203787 (~83.5m) 22.326259,114.203788 (~83.54m) Phone 22.325800,114.203145 22.325796,114.203120 22.325798,114.203122

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
			
		4/F GWIN Booth	22.325486,114.203556 (33.65m) 22.325494,114.203557 (33.56m) 22.325501,114.203562 (33.93m) Phone 22.325553,114.203237 22.325529,114.203242 22.325564,114.203245 
		4/F Male Toilet in E&M Innozone	22.325491,114.203553 (40.85m) 22.325488,114.203558 (41.34m) 22.325498,114.203565 (41.34m) Phone 22.325463,114.203157 22.325449,114.203138

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
			22.325437,114.203141 
		4/F No. 19 booth in E&M Innozone	No. 19 booth not found
		6/F SE's Room in DTD Office	22.326256,114.203783 (60m) 22.326256,114.203784 Phone (60m) 22.326761,114.203983 22.326740,114.203957 22.326757,114.203958 
		6/F BIM-AM Centre Room A	22.326711,114.203963 (82.74m) Phone 22.326778,114.203998 22.326775,114.203982

Item No.	Description	Testing Procedure	Remark/Comments/Outcome
			22.326783,114.203983 
	City University of Hong Kong Indoor Test	1 FungYungWah building FYW 1372	 No Signal Received
		2 CityU Innovation Center	
5	Transition of Indoor & Outdoor Positioning	Install the G20 Pro Tracker at the ground floor in EMSD HQ. Test the positioning radio carrier usage.	About 15 minutes to change the localization method
6	Battery Life	Check whether the G20 Pro Tracker can continuously work more than 14 days.	Yes

Petbiz APP Test

Item No.	Description	Testing Procedure	Test Outcome
1	App Login page	 Open Login Page, enter 'Phone Number', 'Password' and login	 Redirect to Home Page of the platform in 10 seconds
2	Devices management	 Choose "MY" button in the below docker and find the "Device" and access into	List shown the trackers.  To connect new trackers, push the "Connect Device" button and input the necessary information (Device Name, Device ID) Pass if this step could be completed.
3	Tracker Distribution Map	After logged-in, the tracker distribution map is shown in the main page.	Display the outdoor location of all devices.  Click one tracker in the map, there would be a contact window 

4	Trace Map	Click the "Trace" button in the Map and it will show the history traces in the map	Display the "Trace" of the selected trakcer. 
5	E-fance		Display the "E-fance" task of the selected trakcer.