Security mechanisms and Vulnerabilities in LPWAN

Smilty Chacko.

P.G Scholar , Department of Computer Science and Engineering,
St. Joseph's College of Engineering and Technology, Palai, Kerala.

Email: smiltychacko1993@gmail.com

Mr. Deepu Job.
Assistant Professor, Department of Computer Science and Engineering,
St. Joseph's College of Engineering and Technology, Palai, Kerala.

Email: deepu.job@sjcetpalai.ac.in

Abstract. The count of Internet of things (IoT) devices getting connected to internet are exponentially growing and is proposed to be 75 billion by 2025. IoT devices uses Low Power Wide Area Network (LPWAN) that are precisely build to operate at a lower cost with greater power efficiency and long range connectivity than traditional wireless networks. LPWAN are inherently prone to security threats since they are also wireless communication network. Secure communication is essential for LPWAN and most LPWAN technologies uses simple cryptography methods. Despite of this security mechanisms, LPWAN is vulnerable to wide range of attacks. In this paper Network architecture and Security mechanisms of LPWAN technologies (LoRa, Sigfox, NB-IoT and DASH7) are discussed and are compered in terms of IoT factors. As a case study, vulnerabilities of LoRa is also being analyzed.
Keywords: LPWAN, Wireless network, LoRa, IoT.

1. Introduction

Internet of things (IoT) is defined as a network of devices or physical objects with electronics, sensors, software and network connectivity that enables them to exchange information and communicate with each other. IoT applications can be used for smart homes, smart metering, factory monitoring, agriculture, smart buildings etc. In IoT wireless technologies such as Bluetooth, WiFi, ZigBee etc. are used to meet the communication requirements, but they can offer only a short range connectivity. In order to overcome the limitations of short range protocols Low Power Wide Area Networks (LPWAN) are introduced, which offer a long range connectivity in the order of kilometers. LPWAN [1] is getting wide acceptance in industrial and research communities due to its low power long range characteristics. LPWAN [2] can offer long range connectivity up to 2 to 50 km depending upon rural and urban areas. Long battery life is one of the key feature of LPWAN technologies. The data rate offered by LPWAN is from 100 bps to 250 kbps and data rate is selected based on range requirements. LPWAN is suitable for IoT applications since it need to send only small amount of data to a long range. There are many LPWAN technologies and among them LoRa, Sigfox, NB-IoT and DASH7 are getting wide acceptance now a day which have many technical differences.

The paper is organized as follows: the first section discusses various LPWAN network architecture. In second section, since security is an essential requirement of wireless communication technologies, how

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

security is assured by these technologies is discussed and a comparison is made based on the IoT factors such as Quality of Service, Battery life & latency, Network coverage & range, Deployment model, Cost etc. In the third section vulnerabilities in LoRa is discussed as a case study.

2. Technical differences: LORA, SIGFOX, NB-IOT and DASH7

IoT applications require long battery life in order to avoid costly replacements. Many IoT use cases are used within buildings and current technologies have limited coverage and are too costly too. In order to fill this gap LPWAN technologies are introduced. In this section we discuss about technical features of LPWAN technologies such as LORA, SIGFOX, NB-IOT and DASH7.

2.1. LoRa

LoRa is a radio modulation technology by Semtech Corporation. LoRa [3] provides connectivity about 15 to 20 km using chirp spread spectrum technique in which entire band width is used to transmit single signal. LoRa [8] uses 868 MHz to 900 MHz ISM bands for its operation and data rate is 0.3 kbps. Since LoRa have a long battery life, cost of replacement of devices can be reduced and its deployment is not so complex. LoRa use symmetric key cryptography to ensure security to its devices. Chirp spread spectrum used by LoRa can reduce the signal degradation, noise etc. while transmitting signal. LoRa devices support bidirectional communication and it communicates to LoRa gateways. This gateways are connected to the network server and it is connected to the applications. LoRa can use different topologies like star, mesh etc.

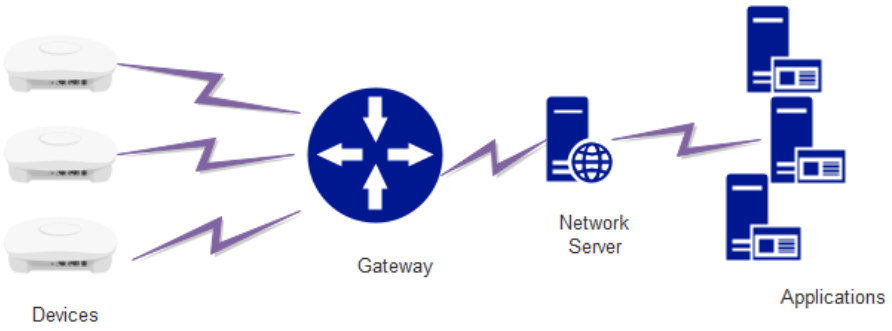

Figure 1. LoRa Network Architecture

2.2. Sigfox

Sigfox is a LPWAN technology which provides low power low data and low cost communication devices. It operates in global network and is used for IoT communications. Even though there ara plenty of wireless technologies Sigfox is widely accepted due its cheaper connection and an extended battery life. Sigfoix [2] enables new IoT applications and it can provide backup connectivity for higher bandwidth devices. Communication using Sigfox can be performed when it detect an event or measure something, it will power on the communication module and send the message. The message is then picked up by the network and the data is received on your server. Sigfox is designed to maximise the energy efficiency. Sigfox consumes very low power when it transmit a data and no maintenance is required. Depending on the topology and environment Sigfox can provide long range connectivity about a few kilometres to tens of kilometres. Sigfox uses unlicensed ISM bands and it uses frequencies, 868 MHz in Europe and 915 MHz in US. Sigfox payload size is 12 bytes anda data rate is 100 bps.

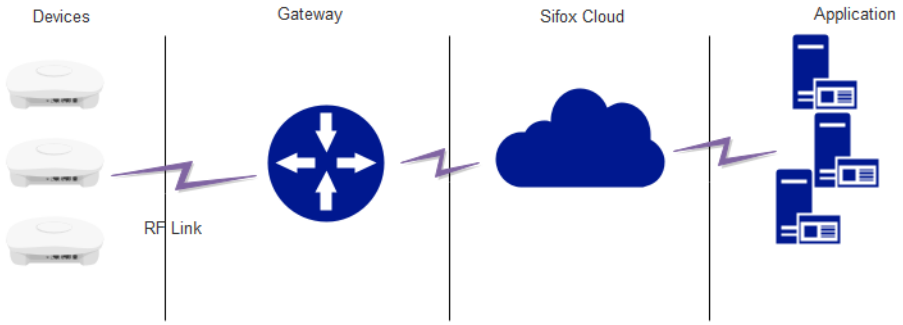

Figure 2. Sigfox Network Architecture

2.3. NB-IoT

Narrow band IoT (NB-IoT) [7] is a technology that offer long battery life and long range connectivity. NB-IoT use cellular telecommunication band to connect wide range of devices. NB-IoT [8] is standardised by third generation partnership project (3GPP). The frequency bandwidth of NB-IoT is 700 MHz, 800 MHz and 900 MHz and NB-IoT is based on LTE (long term evolution) protocol. The functionality of LTE is reduced by NB-IoT to its minimum and it enhances the functionalities as required by IoT applications. NB-IoT improves the power consumption rate of devices, spectrum efficiency and system capacity. NB-IoT can offer a very low power consumption and a battery life more than ten years. The capacity of NB-IoT is about 5000 connections per cell and it support 40 device per household. The data rate offered by NB-IoT is 200 kbps and the transmitting power is +23 dB. Device cost of NB-IoT is less than dollar 5 per module.

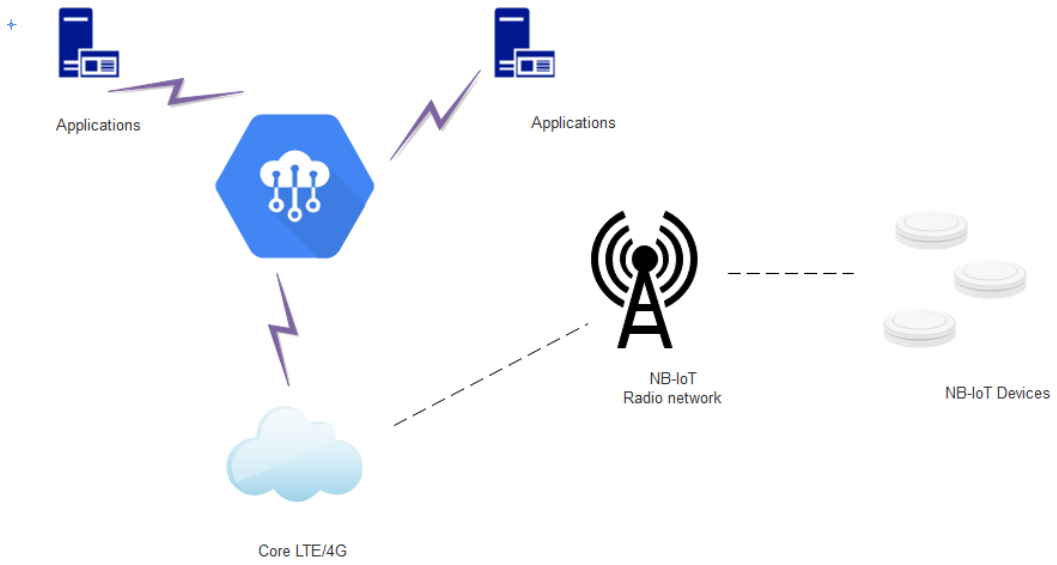

Figure 3. NB-IoT Network Architecture

NB-IoT supports three frequency spectrum that is standalone, In-Band and Guard Band. A new bandwidth is used by standalone deployment type and a bandwidth reserved in guard band deployment type. NB-IoT can be used for personal use, public use, IoT applications and industrial use and it is a secure and reliable technology.

2.4. DASH7

DASH7 Alliance protocol is an Actuator network protocol and it is an open source wireless sensor network. DASH7 operates in 433 MHz, 868 MHz and 915 MHz unlicensed ISM bands. DASH7 can provide a range up to 2km. For security AES 128 bit shared key encryption is used. Data rate offered by DASH7 is 28 kbps and it uses wakeup signal to achieve low power, low latency and elegant architecture. Wakeup mechanism needs a little overhead and latency of only 2.5 to 5 seconds. DASH7 can offer months or years of battery life and it can use calculator-style solar cell, energy harvesting and flat-flex batteries.

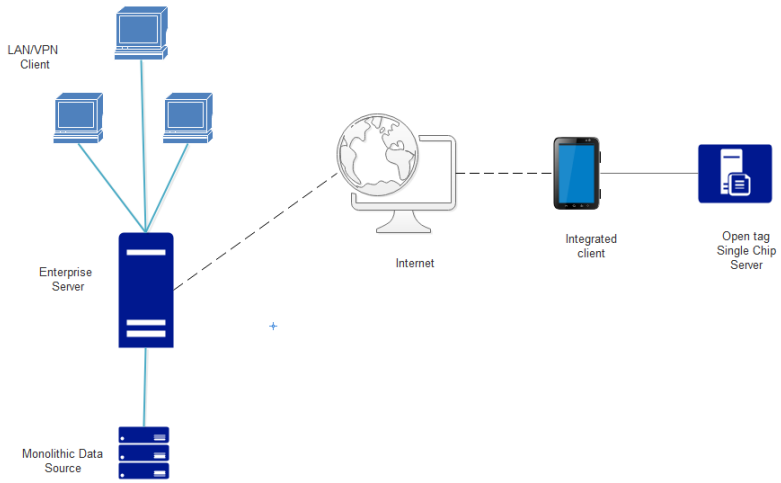

Figure 4. DASH7 Network Architecture

DASH7 [10] uses BLAST networking technology. BLAST means Bursty Light data Asynchronous and Transitive. In bursty, data transfer is abrupt and it does not contain contents like audio and video. In light, multiple consecutive packet transmission is generally avoided and the packet size is limited to 256 bytes. DASH7 communicates through command- response and therefore periodic hand shaking is not required. The whole network of devices is considered as transitional and there is no need routing information or management information. DASH7 use star or tree topology and there will be only one hop between the endpoint and gateway. The packets are acknowledged by at least one gateway and it provide sensor to cloud communication. All OSI layers are covered by DASH7. DASH7 [11] file system contains collection of structured data elements with their properties such as permission and storage class. DASH7 have wide range of applications such as bird tracking, green house monitoring applications etc.

3. Security in LPWAN

Security is a challenge for IoT communication. IoT broadens the platform of attack due to its long range connectivity and comparatively large transmission time. Every device in the network is a potential point of vulnerability and every technology have its own security mechanism to ensure secure communication. In the next section, the mechanism used by different LPWAN technologies to ensure security is discussed [12].

3.1. Security in LoRa

Security in LoRa [5] is handled using AES-128 encryption method. It provides multiple layer of encryption in LoRaWAN. In LoRa, network and application keys are used to ensure security to the packets in the network. Using 128 bit AES application key (Appkey) two session keys, Network session key and Application session key are generated. A message integrity code [6] is generated and verified using Network session key which is shared by end devices and network server. This message integrity code is used to assure integrity of the message. It can be used to create a unique signature for each device. Application session key is used for encryption and decryption of data. An XOR operation is used

to encrypt each message and it also uses a key stream generated by network session key, application session key and uplink and downlink message counter to generate encrypted payload. But the length of the message before and after encryption is same in LoRa and it provides an opportunity to the malicious entity to recreate the key stream from encrypted message. Despite of the security mechanism LoRa devices are susceptible to jamming attack, compromising device and network keys, replay attack and wormhole attack.

3.2. Security in Sigfox

In Sigfox security challenge is addressed through a systematic process. Sigfox is one of the most secure LPWAN technology and it is unique in design. Sigfox devices predominantly operate in offline with a built-in behaviour. When Sigfox needs to transmit or receive data from the internet, the Sigfox device will broadcast a radio message. This broadcasted message is received by base stations and the message is then transmitted to Sigfox core network, which is then delivered to corresponding IoT applications. This Sigfox network architecture provides an air gap and it is not possible to access an end point through internet maliciously.

In Sigfox, [9] each device is given by a unique symmetrical authentication key during the manufacturing time itself. If one of the device is compromised, it can only make a limited impact on the network. A cryptographic token is computed using this authentication key for each sending or receiving message. This token is used for authentication of sender and integrity of message. In order to detect the replay attempts sigfox core network uses a sequence counter contained in each Sigfox message. Since Sigfox deice are not IP addressable there is no over the air activation (OTA) mechanism and it reduces the possibility of attacks. In Sigfox a user can choose whether or not encrypt the message using the encryption solutions provided by Sigfox. The users are also allowed to use their own encryption methods if necessary.

3.3. Security in NB-IoT

NB-IoT inherits LTE's authentication and encryption. NB-IoT [8] consists of three layers, perceptron layer, transmission layer and application layer. Security requirement of NB-IoT aims this three layer architecture. The bottom layer is the perceptron layer and it is susceptible to both active and passive attacks. In passive attack the attacker will simply monitor the network traffic and active attack will affect the integrity of message, falsification of data enc. To prevent this cryptographic algorithms can be used to encrypt the data, integrity authentication and verification. In perceptron layer, each node can directly communicates with base station and this routing security problems during networking can be avoided.

In transmission layer NB-IoT change the network deployment which is complicated and the gateway collects information which is then feeds back to base station. By this, many problems like multi-network networking, high capacity battery, and high cost etc. despite of security threats are there such as access to high capacity NB-IoT terminals, open network environment etc. Application layer in NB-IoT store massive amount of data efficiently. Therefore the main security requirements are identification and processing of this massive heterogeneous data, integrity and authentication of data and access control of data.

3.4. Security in DASH7

To implement an open source code (OpTag) is used and it was released to debug the source code and performance test. To ensure confidentiality of data link layer OpTag beta two includes software based advanced encryption standard (AES) but network layer security is not implemented [11]. To ensure security of data link layer and network layer DASH7 [10] AES-counter with CBC-MAC is used. CCM can be operated by using AES 128 bit block cipher and the message is encrypted using the counter mode. CBC-MAC mode is used to compute the authentication field. In DASH& the sender will generate a packet and the packet is then encrypted using counter mode and it is then authenticated with CBC-MAC. After encryption and authentication, the packet is transmitted through air. The receiver receives the

packet and it will then decrypt the packet and verify it. If it is a legitimate packet the process will be continued.

Table 1. Comparison of LPWAN Technologies

	LoRa	NB-IoT	Sigfox	DASH7
Bandwidth	125 KHz	180 KHz	100 Hz	25 KHz/200KHz
Frequency	Below 1 GHz	Below or above 1GHz	Below 1 GHz	Below 1 GHz
Downlink peak data rate	50 Kbps	250 Kbps	600 bps	55.55 Kbps
Uplink peak data rate	50 Kbps	250 Kbps	100 bps	9.6 Kbps
Module cost	Low	Low	Very low	Low
Data confidentiality	Yes	Yes	No	Yes
Authentication and encryption	Yes(AES 128)	Yes (LTE Encryption)	No	Yes
Bidirectional	Yes/Half-duplex	Yes/Half-duplex	Limited/Half-duplex	Yes/Half-duplex
Standardization	LoRa Alliance	3GPP	Sigfox company	DASH7 Alliance
Range	15-20 km	22 km	30-50 km	2 km
Battery life	10 years	10 years	10 years	10 years

4. Security Vulnerabilities of LPWAN by example of LoRaWAN

LoRaWAN [3] provides end-to-end security using application and network keys. However, an attacker with physical access may compromise the LoRa end-devices. If an attacker gains physical access to a device, he/she may extract the keys. Usually, end-devices contain a LoRa radio module and a host microcontroller unit (MCU). The radio module communicates with the host microcontroller via UART or SPI interface. Commands and data exchanges between the host and the radio module can be intercepted using external hardware. For instance, if UART interface is used between two ICs, a basic FTDI interface can be used to extract all the key exchanges. Contemporary radio modules on the market does not provide built-in encryption support to secure the interactions between the host microcontroller and radio module. In such cases, there is no way to understand that the commands sent to the radio module were issued by the host MCU or a malicious entity. Also a malicious entity could intercept all the data exchanges between the host MCU and the radio module and use this intercepted information to create a mock device with the same credentials or manipulate the data payload. Therefore, application developers must not perform sensitive operations such as setting security keys for each data transmissions as it may expose critical information to malicious entities.

4.1 Compromising devices and Network keys

LoRa

To prove the feasibility of this attack, the Xignal mousetrap was used as a target device. The hardware unit was tampered to expose the UART serial lines between the MCU and the LoRa radio module. A regular FTDI chip was connected to the serial line to read intercept all the transactions between them. Whenever the mousetrap was reset, the host MCU issues commands to configure the network keys of the radio module. Using these keys and custom LoRa device, we impersonated a LoRa mouse trap and sent data as if it were coming from the mouse trap.

4.2 Jamming attack

Jamming attack [5] is one of the main problems for IoT. Malicious entities can transmit a powerful radio signal in the same strength of application devices and interrupt the radio transmissions. It is possible to jam LoRa devices using commercial-off-the-self LoRa hardware. Concurrent LoRa transmissions at same frequency and spreading factor can interfere with each other. This vulnerability in LoRa physical layer allows malicious entities to use commercial-off-the-shelf (COTS) LoRa devices to jam LoRa networks. It is hard to prevent jamming attack because there are workarounds to overcome this issue. Firstly, the jamming of the whole network or frequency can be easily detected since all the devices that communicate in that frequency would suddenly start to drop out from the network. By detecting such behaviour, network administrators can take appropriate action to prevent the impact of jamming.

4.3 Replay Attack

A replay attack [13] is an attack on security protocol, re-sending or repeating the valid data transmission by the malicious entity. The main purpose of this attack is fooling the device or module by using handshake messages or old data from the network. In order to perform the attack in wireless networks, the entity should know the communication frequencies and channels to sniff data from transmission between devices. In LoRaWAN, it is not possible to decrypt transmissions between end-devices and gateways without AppSKey, since the entire payload of the LoRaWAN message are encrypted by it. Additionally, since tampering with the data will make the MIC check fail, it is not possible to do it without NwkSKey. Although the malicious entity can resend the message consecutively, using frame counters which are defined in LoRaWAN specifications these messages or attacks can be detected and discarded. Once the end-device is activated, these counters are both set to 0 and each message coming from the gateway or the device increments counters. If a message is received with a lower frame counter than the last message, it is ignored. However, the LoRaWAN specification handling off frame counters is specifically left to the application and developer. Therefore, networks which do not track these frame counters could be vulnerable to replay attacks.

4.4 Wormhole Attacks

End-devices in LoRaWAN network can be jammed by using off-the-shelf hardware. Together with replay attack, a wormhole attack can be performed against LoRaWAN network. In this type of attack, one malicious device captures the packets from one device and transmits them to other distant located device to replay the captured packet. This can easily be launched by malicious entity without prior knowledge of the network or cryptographic mechanism.

In LoRaWAN network, a wormhole attack [14] could be performed by using two type of device that are sniffer and jammer. The sniffer captures packets and, signals to the jammer to notify that it captured the packet. The captured packet never reaches to the gateway and, validation of captured message stays valid. The captured message can be replayed any time. Gateway and Network server forwards to the packet to the application layer. Therefore, the important alarm messages can be jammed and regular messages which are captured before and never reached to the gateway, could be sent to the gateway as if there is no alarm. Since there is no time-related information in LoRaWAN messages, it is hard to detect this attack in LoRaWAN networks. A general mechanism, called *packet leashes* is used for detecting and thus defending against wormhole attacks.

5. Conclusion

This paper summarizes the network architecture, security mechanisms and vulnerabilities of LPWAN (LoRa, Sigfox, NB-IoT and DASH7). Each technology has its own advantages and limitations in term of IoT factors. NB-IoT and Sigfox offer long range connectivity and low cost devices. Most of the technologies offer long battery life, reliable communication. Among them NB-IoT will give high-value in IoT markets. NB-IoT offers low latency and high quality of services. NB-IoT use LTE encryption while other technologies use AES encryption methods. The actual battery life, security and performance of NB-IoT is currently an open question. From the case study of LoRa and its security vulnerabilities it

is clear that LoRa devices are prone to various security attacks despite of the security mechanism offered by it.

6. Research challenges and future scope

LPWAN still have problems that are to be resolved, such as secure key management and authentication. Most of the LPWAN technologies uses Advanced Encryption Standard for security which are not designed to run in low power devices. AES can be replaced by light weight block cyphers specially designed and build to run in low resource devices. Future research have to be made to make LPWAN a promising network for the 5th generation (5G) wireless mobile communication that would lead to a global LPWAN solution for IoT applications.

7. References

[1] Lukas Krupka; Lukas Vojtech; Marek Neruda *The issue of LPWAN technology coexistence in IoT environment*, 2016 17th International Conference on Mechatronics - Mechatronika (ME) on 2016.
[2] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara *Low Power Wide Area Networks: An Overview*, IEEE Communications Society on, 16 January 2017.
[3] Emekcan Aras, Gowri Sanker Ramachandran, Piers Lawrence, Danny Hunghes *Exploring the Security Vulnerabilities of LoRa*, 3rd IEEE International Conference on Cybernetics on 2017.
[4] Rashmi Sharan Sinha, Yiqiao Wei, Seung-Hoon Hwang *A survey on LPWA technology: LoRa and NB-IoT*, ICT Express, March 2017.
[5] Sigfox Technical Overview, available at https:// www.disk91.com/wpcontent/uploads/2017/05/4967675830228422064.pdf, May 2017
[6] Kais Mekkia, Eddy Bajica, Frederic Chaxela, Fernand Meyerb *A comparative study of LPWAN technologies for large-scale IoT deployment*, ICT Express, 4 January 2018.
[7] Hwajeong Seo and Howon Kim, Member, KIICE *Network and Data Link Layer Security for DASH7*, journal of information and communication convergence engineering, Sep. 2012.
[8] Glenn Ergeerts, Maciej Nikodem, Dragan Subotic, Tomasz Surmacz, Bartosz Wojciechowski, Paul De Meulenaere, Maarten Weyn *DASH7 Alliance Protocol in Monitoring Applications*,10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2015.
[9] *LPWA Technology Security Comparison*, A White Paper from Franklin Heath Ltd, 02 May 2017. Available: http://www.huawei.com/en/events/mwc/2016/summit/global-nb-iot/nb-iot-enabling-new-business-opportunities
[10] Sunakshi Jaitly; Harshit Malhotra; Bharat Bhushan *Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor N etworks: A survey*, International Conference on Computer, Communications and Electronics, 2017.
[11] J. P. Tomás, *Operators in Korea, Netherlands deploy LoRa networks for IoT* 2016, Available:http://www.rcrwireless.com/20160704/carriers/operatorskoreanetherlandsdeploy-lora networks-iot-tag23.
[12] Yonghua Song, Jin Lin, Ming Tang, Shufeng Dong *An Internet of Energy Things Based on Wireless LPWAN*, Engineering, August 2017.
[13] *Narrowband-IoT: pushing the boundaries of IoT*. Available: vodafone.com/iot/nb-iot.
[14] Alex Goldschmidt *Replay Attack Vulnerabilities and Mitigation Strategies*, www.cs.tufts.edu/comp/116/archive/fall2015/agoldschmidt.pdf on 2015.
[15] Y.-C. Hu, A. Perrig, and D. Johnson, *Packet leashes: a defense against wormhole attacks in wireless networks*, in 22nd Annual Joint Conference of the IEEE Computer and Communications on 2003.