ATLANTIS PRESS

Advances in Computer Science Research (ACSR), volume 72

IV International Research Conference "Information Technologies in Science, Management, Social Sphere and Medicine" (ITSMSSM 2017)

Analysis of vulnerabilities in low-power wide-area networks by example of the LoRaWAN*

Sergey Iskhakov
Faculty of Security
Tomsk State University of Control Systems and Radioelectronics
Tomsk, Russia
iskhakov.sy@gmail.com

Roman Meshcheryakov
Faculty of Security
Tomsk State University of Control Systems and Radioelectronics
Tomsk, Russia
mrv@security.tomsk.ru

Anastasia Iskhakova
Faculty of Security
Tomsk State University of Control Systems and Radioelectronics
Tomsk, Russia
shumskaya.ao@gmail.com

Sergey Bondarchuk
Faculty of Biology and Chemistry
Tomsk State Pedagogical University
Tomsk, Russia
isbi@mail.ru

***Abstract*— The increasing number of automated systems using the global network for management has led to the need to search for new technologies for transmitting data from various sensors over long distances with minimal energy consumption. Today, there are several similar technologies on the market that claim to be the world standard in the concept of the Internet of things, but none of them has yet been studied in detail from the point of view of security. This article is devoted to the analysis of one of the most common protocols in order to identify potential vulnerabilities.**

Keywords*— *Internet of Things; modulation; network; vulnerability; replay attack; spoofing.

I. INTRODUCTION

In recent years, a concept of Internet of Things (IoT) [1,2] has gained widespread acceptance, it can be defined as a global dynamic network infrastructure, where physical and virtual "things" have identifies and physical attributes, and are integrated into the information network, using different interfaces. The logical IoT structure can be represented as a set of interacting smart devices. From a technical point of view, any interaction technologies, as well as data processing and transmission methods can be used in IoT, regarding to their intended functions. The concept includes many different technologies and standards and is taken as one of the most important trajectories of the information technology market development. The IoT concept is based on a pervasive presence in the environment of different technological objects ("things") that are able to interact with people whenever and wherever they are using different communication networks. The global integration of IoT determined the predominant role of wireless communication technologies over low-power wired networks, not least because of reductions in system installation costs, allowing for in-service modifiability and scalability. Attention is being increasingly focused on wireless communications, allowing the creation of Low-Power Wide-area Network, LPWAN [3]. The examples are intelligent public lighting networks, environment and transport monitoring systems etc. In spite of high level of wireless technology development and the availability of high-speed mobile internet, most of them (e.g. Wi-Fi [4] or LTE [4]) are not suited for LPWAN solutions, because they involve technologies allowing interaction with low-power, long-range and at the same time low-cost IoT devices.

Imagine there is an apartment building, where water- and power-supply systems are connected to IoT and transmit data automatically to a monitoring station. Firstly, while it's easy to provide a regular supply for electricity meter, while cable connecting to water meters negates the advantages of the concept of wireless technologies application. In view of this, radio module for a meter should be operated from a local energy source (battery). The power consumption of today's Wi-Fi and LTE modules results in the reduction of battery life to several days; it can lead to inexpediency of their using in the presence of large amount of sensors. Secondly, there will be hundreds of sensors in terms of the apartment building. Notwithstanding low traffic volumes they produce, almost all resources of the nearest mobile network transmission stations will be employed for establishing communication with such a number of "subscribers". An additional point is that LPWAN solutions are focused on other priorities. There is no need to use fast-acting communication channels for meter data transmission. Nevertheless, it is essential that the communication channel with a minimum speed and a minimum power level will cover a required distance, even if there is a signal with very low noise level.

Today, IoT solutions have a very significant influence on the everyday life of people, and therefore, in order to achieve recognition, it is essential to provide not only equipment protection, but protection of personal information that machines are accessing (e.g. consumer habits data). Trust is one of the main challenges too as IoT framework is

The work was funded by the Russian Federation Ministry of Education and Science (grant 2.3583.2017/4.6).

characterized by different types of devices processing data according to user needs and privileges. The issue of data security protection became important as the first computer-to-computer link was established. The number of issues has increased in this area, gradually with the commercialization of the Internet covering confidentiality of personal data, financial transactions safety and cyber security. In the case of IoT security is inseparable from safety. For example, accidental or malicious insider threat of manipulating a pacemaker device as well as a car or nuclear-power reactor is dangerous to human life and health.

Accordingly, one of the most important aspects is providing security of devices that generate and process the information. Besides, one more significant aspect is providing security of IoT devices against DDoS attacks [5-7] and botnets [7,8]. The most probable cause of such a high degree of vulnerability is the fact that many things in the IoT arena are delivered with insecure default settings or generated with unsafe code. To lower system vulnerability many challenges need to be addressed, such as the problems with lack of specific IoT standards and cooperation of different architectural solutions for device creation. The other problem is related to the lack of security planning in development methodologies, IoT deployment process in insecure frameworks and resource limitation for security tools release.

Solution to these problems is contingent upon combination of many technologies and protocols and upon collaboration between vendors, but it requires the common problems and vulnerabilities to be identified in different technologies. In this article was made an attempt to generalize methodologic experience in the area of LPWAN solutions security protection.

II. LPWAN STANDARTS

Currently, there are two main development trends of wireless technologies concerning the LPWAN area: licensed band technologies and, in contrast, technologies without the need for license. LoRaWAN [9,10] and NB-IoT [9,11] standards are the most common networks.

NB-IoT is a digital cellular standard for digital telemetry units with low-volume data communications. It is developed by 3GPP Consortium based on current cellular standards and published in 2016 [9]. So that the NB-IoT network is relating to mobile communications, the devices working in it must "wake up" and be synchronized with network. Otherwise, you cannot receive and send a massage. On grounds that NB-IoT works in the licensed band, the devices must be synchronized with network frequently enough. It expends battery resources.

LoRaWAN is a datalink protocol based on patented technology, the LoRa modulation [11], announced by the companies Semtech and IBM Research in 2015. LoRa is not the cellular standard. License for LoRaWAN connection is not required. The asynchronous data transmission of LoRaWAN means the transmission of data only once they exist. If the device has nothing to transmit, it "sleeps' saving battery life. Personnel can transmit the data according to the schedule set or at any time. Herewith, synchronization with the network is not required. Only application kind in the band of asynchronous types determines how long the device can "sleep". Therefore, this helps to save the battery.

NB-IoT gives maximum working capacity in complex built-up areas. Suburban areas and countryside will create surplus network capacity. The LoRaWAN protocol is not reliant on the mobile data, and its coverage remains resilient regardless of the location. LoRaWAN is considered ideal for applications and devices that require modest data rate and the amount of transmitted data; however, the devices must provide long-life battery at minimum maintenance costs.

Both of the above-mentioned standards are currently dominant at the LPWAN solutions market. They have their benefits and drawbacks and serve different segments of the IoT market. Nevertheless, in most aspects, such as ease of deployment, ecosystem, deployment capacity, battery life and operation in private networks LoRaWAN cost ratio surpasses that of NB-IoT. As such, in this article much attention will be given to providing security of the solutions using LoRa technology.

Despite the fact that LoRaWAN networks are still at the early stage of their development, they have already started to spread in many countries. For example, in the Netherlands KPN LoRa network deployment has been given start throughout the country. LoRaWAN standard is to be used in railway control systems, security alarms systems and monitoring stations of Industrial Control Systems (ICS). In Russia, deployment of a full-fledged LoRaWAN network throughout the whole territory of the Republic of Tatarstan is planned to start in 2018. Thus, the market potential of these systems is immense. In light of this, this article, being a part of research on IoT infrastructure security, considers LoRaWAN protocol.

III. LORAWAN STRUCTURE

When speaking of LoRa technology, LoRa modulation format and LoRaWAN open protocol are normally referred to. LoRa is a proprietary spread spectrum modulation scheme that is derivative of Chirp Spread Spectrum modulation (CSS), which allows for data transfer over long distances and low energy consumption. LoRaWAN, in its turn, is a low-power wide-area datalink protocol for multi-node networks. LoRaWAN network architecture is typically laid out in a star-of-stars topology with no repeaters and mesh connections. It has end nodes through which gateways acting as transparent bridges relay messages to the central network server. In this approach the gateways and the central sever are assumed to belong to network operators with end nodes belonging to subscribers. Subscribers are provided with an opportunity of transparent bidirectional and secured data transfer to end nodes. The typical LoRaWAN network consists of the following elements: end nodes, gateways, a network server and an application server (Fig.1) [10,11].

- **End Node** fulfills controlling and measuring functions. It contains a set of necessary sensors and controlling elements.

- **LoRa Gateway** is a device receiving the communications from the end nodes and then transferring them onto the backhaul system. This network can be Ethernet, cellular or any

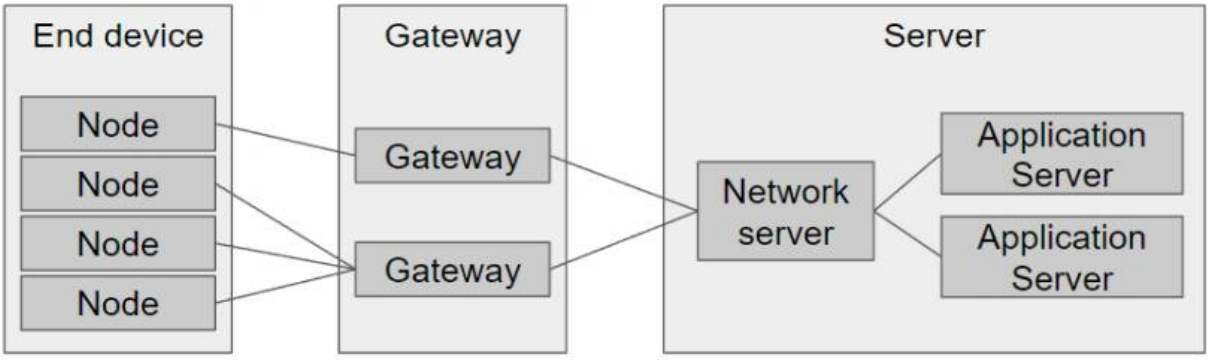

Fig. 1. The structure of typical LoRaWAN network

other telecommunications channels. Gateways and end devices build up a star network topology. Normally, this device contains multi-channel transmitters for processing signals simultaneously or even several signals through one channel. Consequently, several devices of this kind provide for network coverage and transparent bi-directional data transfer between end nodes and the server.

• **Network Server** manages the network: setting up schedules, adapting data rates, storing and processing received data.

• **Application Server** provides remote control over end nodes and collects data from them.

There are three types of end devices for solving various problems and serving different purposes in the LoRaWAN network:

1. Bi-directional end-devices, Class A [12]. Devices of this class are implemented when the lowest power consumption in transferring data to the server is required. The trigger for the communication session is the end node sending data packages, which is followed by two receive windows during which it waits for downlink communications from the server. Thus, data transfer from the server is only possible with the end device is connected.

2. Bi-directional end-devices, Class B [12]. The main difference from Class A devices is that Class B devices open an extra receive window at scheduled times. In order for the end device to open its receive window at the scheduled time it receives a time synchronized signal from the gateway. This extra receive window allows the server to start data transfer at a predetermined time.

3. Bi-directional end-devices, Class C [12]. Devices of this type have nearly continuously open receive windows, only closed when transmitting. This makes Class C devices suitable for completing tasks which require receiving a large amount of data.

As LoRaWAN is designed for building up a global network, developers have given heed to security and confidentiality of transmitted data at several levels. The following keys are used [11,13]: Unique Network key (EUI64), Unique Application key (EUI64) and Device specific key (EUI128).

Owing to the fact that LoRaWan is a rather new protocol, its security level is underdeveloped and requires analysis and revision. So far, there's been no systematic research on the protocol vulnerabilities in the literature. Although LoRa technology does provide for some security mechanisms, such as encryption and digital signature, its security level is still in need for elaboration. Possible attacks on LoRaWAN protocol will be considered further on.

IV. Analysis Of Vulnerabilities

Adding new devices to the network is one of the most vulnerable stages in the work of IoT infrastructure. To ensure the security of whole network it is necessary to implement the «activation stage»: before the end devices can interact with the network server, they must be activated through the connection procedure. This mechanism is designed to control the access of unidentified devices to the network and prevent their interaction with other objects on the network. In the case of the LoRaWAN protocol, there are two possible activation methods: Activation by Personalization (ABP) [9] and Over-The-Air Activation (OTAA) [9].

Over-The-Air Activation consists of two stages between end device and a server, which are called "Join request" and "Join accept". OTAA method provides several security mechanisms. First, it uses identifiers that must be unique among terminal devices. In this case, compromising one terminal device does not mean compromising the entire network. Secondly, there is a DevNonce [9,14] buffer to prevent a replay attack. Each time the server requests a connection, the server checks the buffer for the presence of such a number among the previously used ones. In this case, it is impossible to copy a connection request and reuse it.

In comparison with OTAA method, Activation by Personalization skips connection and confirmation requests. In this case, before activation the device are assigned unique parameters [13] (DevAddr, NwkSkey and AppSkey), which are stored on the server. When activated, the end device sends these values to the server directly. At the same time, messages are encrypted and signed with a digital signature. It is assumed

that only a network server with the appropriate parameters can process this data as text.

Replay attack during activation

Obviously, the ABP activation method has certain vulnerabilities. For end devices activated in this way, static keys are used, which in turn means that after the restart these keys will not be changed and will remain the same. In addition, unlike OTAA, there is no connection procedure. Therefore, a malicious message can be received by the network server if it meets the following requirements:

- the session keys matches one of the activated devices;
- DevAddr parameter coincides with one of the activated devices;
- the value of the device counter is acceptable. In this scenario, the attacker can select and resend the messages before the restart, and the server can not determine whether these messages are from this session or from the session before the reset.

It is worth noting that the approach to using counters is also unsafe, because the protocol specification says that after the "Join request"-"Join accept" message exchange or reboot the end device that already activated the counters on it and the counters on the network server are reset to 0.

Thus, the end device activated by the ABP method will reuse the counter value from 0 with the same keys after reboot. In this case, an attacker can intercept messages in the last session with large counter values and use it in the current session. So, the replay attack is possible regardless of how the device was activated, by ABP or OTAA method. Alos it is possible to reset the counter by overflow: the counter will be reset and restart from 0 after it reaches the maximum value.

If an attacker knows the counter values of the previous session and the keys of the current session, he can replay previous messages to disrupt the communication between the end device and the server. The main purpose of the replay attack is to achieve a repetition of the counter value. Therefore, in networks with OTAA activation, an attacker must wait until the value of the counter of the end device reaches the maximum and is reset to achieve the goal. For devices activated by the ABP method, an attacker can also wait for the counter overflow or reboot of the end device, because in this case the counter value will reset to 0. As for ABP activation method, such an attack will take much less time than using OTAA activation, if the attacker has the ability to restart the end device.

This kind of attack designed for spoofing in LoRaWAN networks and denial of service (DoS). In the case of a server, the main purpose is spoofing, because if attack is implemented, the server will accept a malicious message from the attacker's device, meaning that it is an activated verified device. If the victim of attack is the end device, the main purpose is DoS, because if it is implemented the message from the activated device will not be accepted by the server. The DoS period depends on the type of message for replay.

Thus, to implement a replay attack during activation in LoRaWAN networks, an attacker must have:

- knowledge of the format of physical representation of data in LoRaWAN messages;
- knowledge of the wireless frequency band of the terminal equipment - the victim;
- the presence of a device for capturing wireless messages LoRaWAN;
- the presence of a device sending messages LoRaWAN with a certain frequency;
- the ability to save and read plain text in LoRaWAN messages.

If an intruder does not select a specific before an attack, he does not need a lot of time in the large LoRaWAN network to wait for the counter to overflow. However, if an attacker makes an attack on a small network, it is more advantageous for him to identify a specific end device and try to reboot it in order to shorten the waiting time.

To implement this attack, an attacker can use a sniffer to intercept traffic, and a LORA transmitter to replay messages. Such an attack can be extremely dangerous for end devices activated by the ABP method in a large LoRaWAN network. In the case of a small network, an attacker may need a considerable amount of time to overflow the counter. However, on a large network with many endpoints, the wait time for any of the rebooted endpoints is greatly reduced. As soon as the attacker receives the maximum counter value for end device, he can periodically repeat this message to permanently reboot the attacked device. If the session keys for the target device are changed, it will not be able to function after the reboot. In addition, if an attacker finds a way to reboot the device (for example, turning off the power), then he will not have to wait for the counter to overflow. If the device is rebooted and the message with the maximum counter value is repeated, messages from the victim device will be rejected by the server.

ACK Spoofing

In LoRaWAN networks, the gateway is connected to the Internet by one of the interfaces usually. It causes an increase in the number of potential vulnerabilities. For example, it is possible to create a malicious gateway that can be added to the network through attacks such as UDP spoofing [7]. The potential vulnerability of the protocol lies in the fact that the ACK message does not contain information about the message that it actually confirms, it only confirms the last message received. So, it is possible that a compromised malicious gateway can retain confirmation and support it for future messages from end devices.

The purpose of the ACK spoofing attack is to allow an attacker to intercept and re-send the same ACK message to confirm various messages from the end device. To implement such an attack attacker must have:

- the ability to gain control over the gateway;
- the ability to recognize ACK messages and embed them into the process of transferring them between the gateway and the destination device;
- the ability to read and select the required ACK messages;
- the ability to send selected ACK messages from the gateway to the end device.

The possibility of this attack is based on the assumption that the gateway is already infected and is malicious, or the attacker has conducted an attack on the gateway's spoofing (he completely monitors the gateway and can enable spoofing of ACK messages). Theoretically, in the LoRaWAN network, the gateway is used to send messages. So, if an attacker controls a gateway, he can only harm at the physical level. However, in view of the above drawback in the ACK design, gateways become a serious point of failure in the LoRaWAN network.

V. CONCLUSION

The rapid development of the IoT market entailed the need to develop new standards and technologies for data transmission, since the use of existing infrastructure, such as cellular networks or Wi-Fi, does not allow achieving the goals and objectives of the Internet of things. One of the examples is the wide distribution of solutions based on the LoRaWAN protocol, which has all chances to become the world standard in IoT. However, the fact that human life and health can often depend on the IoT of operation of devices, consumers of this market dictate the requirements for security guarantees and confidentiality of data processed by such devices.

In this article, the authors present the results of analyzing the specifications for this protocol in order to identify potential vulnerabilities. The received results show that, despite the serious approach of developers to ensure the protection of devices in the network, the level of security of the LoRaWAN protocol is not sufficiently developed and requires analysis and improvements.

The review of publications and technical documentation demonstrates how many problems remain unsolved problems, sheds light on the research directions in the field of security LoRaWAN and IoT in general. Identified vulnerabilities can be used for further research, as well as to reduce the risk of compromising end devices.

REFERENCES

[1] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, “Security, Privacy & Trust in Internet of Things: the road ahead,” Computer Networks (Elsevier), 2015, vol. 76, pp. 146–164.

[2] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, “Standardized protocol stack for the internet of (important) things,” IEEE Commun. Surv. Tutorials, 2013, vol. 15, № 3, pp. 1389–1406.

[3] George Margelis, Robert Piechocki, Dritan Kaleshi, and Paul Thomas. Low throughput networks for the iot: Lessons learned from industrial implementations. In Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, 2015, pp. 181–186.

[4] G. Altangerel, E. Tsogbaatar and D. Yamkhin, “Performance analysis on IPv6 transition technologies and transition method,” 11th Int. Forum on Strategic Tech. (IFOST), Novosibirsk, 2016, pp. 465-469.

[5] G. Howser and B. McMillin, “A Modal Model of Stuxnet Attacks on Cyber-physical Systems: A Matter of Trust,” Eighth Int. Conf. on Soft. Sec.and Reliability (SERE), San Francisco, CA, 2014, pp. 225-234.

[6] O. Evsutin, A. Kokurina, R. Meshcheryakov, O. Shumskaya, “An adaptive algorithm for the steganographic embedding information into the discrete fourier transform phase spectrum”, Advances in Intelligent Systems and Computing, 2016.

[7] S. Iskhakov, A. Shelupanov, R. Meshcheryakov, “Simulation modelling as a tool to diagnose the complex networks of security systems” J. of Phys.: Conf. Series, 2017, vol. 803. 012057.

[8] J. Jerkins, “Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code,” *IEEE 7th Ann. Comp. and Comm. Workshop and Conf. (CCWC)*, Las Vegas, NV, 2017, pp. 1-5.

[9] Andrew J Wixted, Peter Kinnaird, Hadi Larijani, Alan Tait, Ali Ahmadinia, and Niall Strachan. Evaluation of lora and lorawan for wireless sensor networks. In SENSORS, 2016 IEEE, pp. 1–3. IEEE, 2016

[10] LoRa Alliance. Online available :https://www.lora-alliance.org/. In Civilian Conservation Corps (CCC) (2016), 2016.

[11] Semtech Corporation. Lora modulation basics. In AN1200.22, May 2015

[12] Sarra Naoui, Mohamed Elhoucine Elhdhili, and Leila Azouz Saidane. Enhancing the security of the iot lorawan architecture. In Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), International Conference on, pages 1–7. IEEE, 2016.

[13] Y. Zhao, “Research on data security technology in internet of things,” 2nd Int. Conf. on Mechatronics and Control Engineering (ICMCE), Dalian, China, 2013, pp. 1752–1755.

[14] Mohamed Abomhara and GM Kien. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4:65–88, 2015.