4ZA-06

Study on ZigBee Security: Physical and Replay Attacks

XIE WEN, Alaa Allakany, Koji OKAMURA

* Department of Information Science, Kyushu University, Japan

** Cybersecurity Center, Kyushu University

*** Research Institute for Information Technology Kyushu University, Japan.

Abstract— *With the rapid development of the Internet of Things these years, ZigBee, as a low-speed short-distance transmission of wireless network protocols, has been widely used in IOT devices. It has the advantages of low power consumption, low cost, supporting for a large number of network nodes, fast and reliable, thus improving the performance of IOT devices. However, for various reasons, many cyber-attacks pose a threat to the security of ZigBee and further cause huge losses to users. The objective of this research is analyzing the principles and characteristics of two attacks against ZigBee network (physical and replay attacks), addressing ZigBee vulnerabilities related to these attack, simulating these attacks, and then providing security measures to avoid such attacks against ZigBee network. We built a Lab. ZigBee Network used for simulating these attacks.*

Keywords— *Internet-of-Thing (IoT), ZigBee, Reply attack.*

I. INTRODUCTION

ZigBee is an open source wireless technology for low-power embedded devices which facilitates efficient communication between machines and machines while maintaining a low cost. It is built on the IEEE 802.15.4 standard and is supported by the ZigBee Alliance [1]. The protocol stack of ZigBee is mainly consisted of the following two parts: 1- The Network and Application security layer implemented by the IEEE 802.15.4 standard. And 2- The MAC layer and physical layer implemented by ZigBee Alliance itself as shown in Figure 1.

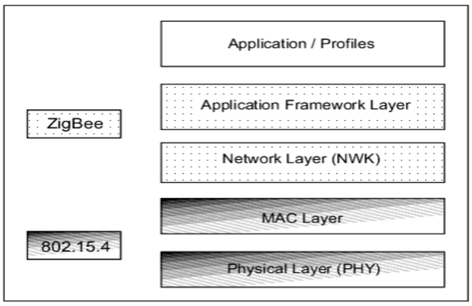
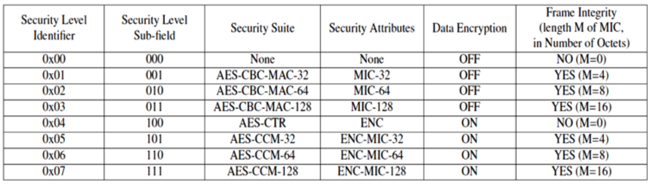


Figure 1: Example of educational material

Recently, ZigBee protocol has been more popular, many companies started to use ZigBee on its products. ZigBee protocol defines three types of logical devices: Coordinators, Routers, and End devices. All these devices are communicated based on different security levels defined by ZigBee. Table 1 shows the different security levels on ZigBee. Security attacks on ZigBee devices are increasing, almost due to failing on implementation of ZigBee security, especially in personal home, medical equipment and automation, etc., the securely application of ZigBee devices should be guaranteed to avoid such attacks. For more understanding to ZigBee security the following subsections will introduce security on ZigBee and the security configuration.



Security Level Identifier	Security Level Sub-field	Security Suite	Security Attributes	Data Encryption	Frame Integrity (length M of MIC, in Number of Octets)
0x00	000	None	None	OFF	NO (M=0)
0x01	001	AES-CBC-MAC-32	MIC-32	OFF	YES (M=4)
0x02	010	AES-CBC-MAC-64	MIC-64	OFF	YES (M=8)
0x03	011	AES-CBC-MAC-128	MIC-128	OFF	YES (M=16)
0x04	100	AES-CTR	ENC	ON	NO (M=0)
0x05	101	AES-CCM-32	ENC-MIC-32	ON	YES (M=4)
0x06	110	AES-CCM-64	ENC-MIC-64	ON	YES (M=8)
0x07	111	AES-CCM-128	ENC-MIC-128	ON	YES (M=16)

Table 1: Different security levels on ZigBee

ZigBee Security configuration: ZigBee protocol supports two types of security model: Centralized security network and distributed security model. IEEE 802.15.4 provides robustness against interference from other networks and uses AES with a 128-bit key length to ensure data security and integrity. Security is primarily guaranteed by encrypting the data payload and execution, and integrity is achieved by using message integrity code (MIC) or message authentication code (MAC).

IEEE 802.15.4, does not specify how to manage the key or the type of authentication policy applied. These issues are managed by ZigBee. The ZigBee standard supports the following optional security services: encryption/decryption, replay attack protection, device authentication, and more. Table 1 shows more details about security measures. However, the IoT devices developer and users can apply or not the high security level, thus many vulnerabilities can be detected and exploited with low security levels.

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.

The objective of this paper: 1- Studying the ZigBee security and different vulnerabilities resulting from applying or not applying high security level based on ZigBee specification, 2- Analyzing the principles and characteristics of the two basic attacks against ZigBee (physical and reply attack), 3- Setting up a ZigBee network communication and then simulating these attacks in our Test Lab., and 4- Suggesting security measures which could be added to secure ZigBee communication and mitigating these attacks. Next section will introduce related works and implementation of this research.

II. Physical and replay attacks in ZigBee.

The target of physical attacks against any ZigBee device is to obtain sensitive information of this device for applying more attacks against ZigBee network. For instance, ZigBee network key or link key can be obtained by a physical attack. The keys can be extracted from ZigBee devices' flash memory once a physical access is achieved [2].

In replay attack, the attacker can sniff a packet or record packets traffic in a network and send it back at a later time so that will result in a malicious attack. ZigBee implements a mechanism to avoid replay attacks by using a frame counter. Each node in the ZigBee network contains a 32-bit frame counter that is incremented each time a packet is transmitted. The only time the frame counter be reset to 0 is to update the network key.

Olawumi et al. proposed a timestamp integrated with the encryption mechanism. If an attacker obtains and replays a packet, the packet will be rejected by the receiver due to the time difference. However, in order to save the last timestamp, the coordinator needs to call more storage space [3]. Cache et al. proposed that the ZigBee stack should be configured to ensure that the sequence number of the received frame is greater than the previous received packet. Unfortunately, the ZigBee protocol is currently not satisfactory, and due to the limited entropy, ZigBee's NWK sequence number field must not exceed 8 bits [3].

III. design

As we mentioned before that the objective of this research is analyzing the principles and characteristics of the two basic attacks against ZigBee (physical and reply attack) by analyzing the vulnerability and then simulating these attacks in our Test Lab. In this section, we will explain some existing vulnerabilities that will exploit to apply these attacks and the environment setup for simulating these attacks.

A. *Environment setup*

We will use the same hardware and software to setup the network in the two attacks simulation. The ZigBee network consists of 3 nodes, one as a coordinator and the other two as routers. A motion detector will be connected with sender device, a light will be connected with receiver device, and the last node will be used for physical attack. Figure 2 shows the ZigBee network used on our test.

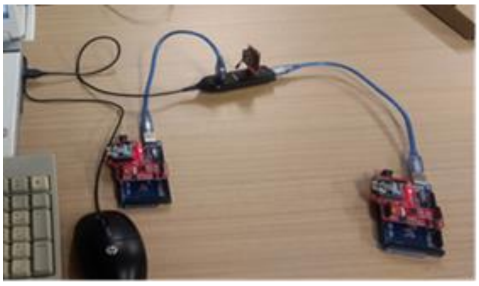


Figure 2: ZigBee Network Setup

B. *Physical Attack*

One of the main weakness of ZigBee is that once a device is removed from the network, ZigBee won't invalidate the keys and generate new ones, therefore, allow tempering the whole network [2]. We will apply physical attacks against the third node in this network and extract the required information for applying the reply attacks against this network.

C. *Reply Attack*

When the coordinator restarts due to some reasons such as power failure or when the attacker gets access to the power supply and turns off the power, the frame counter will be restored to zero, which will result in an attack. Now we focus on finding a way to force the coordinator to reset the frame counter to zero and applying the reply attack against the ZigBee network by using the data gotten form physical attack.

IV. CONCLUSION

This study focuses on studying the ZigBee security and analyzing the principles and characteristics of two of the basic attacks against ZigBee (physical and reply attack). We found that in order to effectively avoid replay attacks, it is required to automatically updating the NWK key each time the frame counter is reset. We build a ZigBee network for simulating these attacks. Our future work will focus on propose a more effective solution for NWK update to avoid replay attacks.

Acknowledgment

This research was supported by Strategic International Research Cooperative Program, Japan Science and Technology Agency (JST), SICORP and JSPS KAKENHI Grant Number JP16K00480.

References

[1] Digi International. (2015). XBee / Xbee-Pro ZigBee RF Modules. User's Guide. Retrieved October 12, 2015 from www.digi.com/resources/documentation/digidocs/pdfs/90000976.pdf.

[2] G. Dini and M. Tiloca. "Considerations on Security in ZigBee Networks", in IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (2010). pp. 58–65, 2010.

[3] F. Farha and H. Chen. "Mitigating replay attacks with ZigBee solutions", Network Security, Volume 2018, Issue 1, January 2018, Pages 13-19.

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.