Journal of Engineering and Applied Sciences 13 (1): 254-258, 2018
ISSN: 1816-949X

A Study on Improvement of Device Removal Processes from ZigBee Network

Jae-young Lee
School of Information and Communication Systems, Semyung University 65,
Semyeong-ro, Jecheon-si, 27136 Chungcheongbuk-do, Republic of Korea

Abstract: Device removal from TC starts when TC transmits a remove-device command to ZA. ZA which received the remove-device command, transmit a remove-device command back to ZB. When commands are all transferred, TC deletes ZB from the device management list and all devices in the network delete their shared keys with ZB. At this time, the remove-device command from TC is encrypted by LKA, however, the leave command from ZA to ZB is not encrypted. The proposal from the thesis is as follows. First of all, make sure that devices which transmitted a command have the capability to be identified by including MIC, a shared key between two devices in the command that cannot ensure its integrity as it is not encrypted. Second, make counterfeit and falsification of a command by other devices impossible through encryption of the command for a removal process with a shared key between two devices. The result of the thesis as follows. First of all, upon possible counterfeit and falsification of a command originating from a leave command which has not been encrypted being transmitted from ZA to ZB, ensure the integrity of the command via encryption with LKAB and allow the sender of the remove-device command to be identified as TC by including MIC (LKB) in the leave command. Second by including MIC(LKB) value in the leave command, the sender of leave command can be identified as ZB, then through encryption with LKAB, other devices which do not know the code are made impossible to counterfeit or falsify the command. The improved proposal for device removal processes from ZigBee network assumes that there is a key safely shared between devices. Hence, when the shared key is exposed to other devices counterfeit and falsification becomes available with the key, further, other devices can disguise themselves as proper devices. Thus, additional research is necessary to securely store and manage the shared key.

Key words: ZigBee network, security, authentication, SKKE, wireless sensor network, protocol, MEA

INTRODUCTION

Component devices of ZigBee network is added to the device management list via. application and authentication procedures of the devices can utilize the network resources after being added to the list, then can transmit and receive data with other devices in the network after reception of NK to their TC.

Affiliated devices to ZigBee network are removed from the device management list of the network through a removal process and the process is divided into two types based on the proceeding direction of the removal. The removal process which starts from TC involves transmission of a remove-device command incorporating ZB data from TC to ZA, identification of the received remove-device command by ZA and transmission of a leave command from ZA to ZB. When ZB is removed from the network, ZA deletes its shared key with ZB. TC deletes ZB from the device management list and its shared key with ZB.

The removal process that starts from ZB, gets initiated as ZB transmits a leave command to ZA. ZA which received the leave command, identifies the command, then transmits an update-device command that announces the removal of ZB to TC. At this point, all devices delete their shared key with ZB.

During the device removal process starting from TC, the remove-device command being transmitted from TC to ZA is encrypted by LK_A, hence, cannot be counterfeited or be falsified. However, the leave command from ZA to ZB is not encrypted and it is impossible to prevent other devices from disguise themselves as ZA and sending a leave command to ZB. During the device removal process starting from ZB, the leave command sent from ZB to ZA is encrypted by NK that is shared by all devices in the network, it is impossible to prevent other malicious devices from disguising themselves as ZB and transmitting a leave command.

Accordingly, this thesis would like to propose a method to improve security issues that can occur during device removal processes from ZigBee network.

Literature review

ZigBee network: ZigBee network is a wireless sensor network based on 802.15.4, the communication standard set by IEEE (ZigBee Alliance, 2008; IEEECS., 2012). The

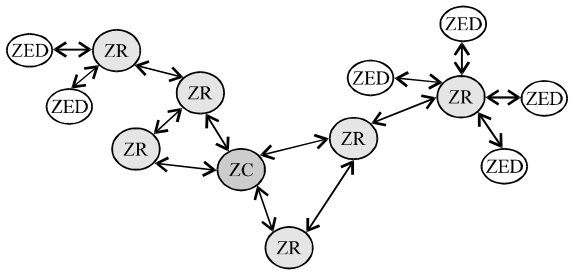

Fig. 1: ZigBee network

component device of ZigBee network requires low cost for the network establishment and low electricity consumption as advantages although its performance is low (Bonghwan, 2014).

Component devices of ZigBee network are differentiated based on their roles as ZC (ZigBee Coordinator), ZR (ZigBee Router) and ZED (ZigBee End Device) and based on their performances as Full Function Device (FFD) and Reduced Function Device (RFD).

In general, ZigBee network is comprised of one ZC and several subordinates linked to the ZC. ZC manages data of all devices in the ZigBee network and handles the communication with other ZigBee networks. ZR serves the role of data collection of ZED which involves small data transmission range within the ZigBee network. As ZR does not require as many functions as ZC, ZR uses relatively low amount of memory, hence, requires lower cost. ZED is the device at the lowest level in the ZigBee network and it measures data and transmits the data to ZR. ZED can communicate with other devices, however, still requires low terminal cost thanks to its simple functional use (Kim and Park, 2013; Back *et al*., 2014).

FFD is used as ZC and ZR in ZigBee network in general. FFD has all functions including data collection, management and network control in ZigBee network, hence can be used as any device in ZigBee network and can practice all types of topology configuration. RFD only possess an extremely simple function, thus cannot play the roles of coordinator and router but the role of ZED, a terminal device of ZigBee network, practicing Star topology configuration (Jihoon, 2010).

Composition of ZigBee network is shown in Fig. 1. Existing TC (Trust Center) in ZC takes in charge of all devices in the network. TC generates the encryption key that is required for data encryption in the network and practices a renewal of the existing encryption key that is proceeded regularly or by a request given by a device. Furthermore, TC intervenes processes of an access of a new device and a removal in the network (Oh *et al*., 2012; Jang and Kim, 2014).

Table 1: How to get the key type

Key types	Master key	Link key	Network key
Key-transport	Yes	Yes	Yes
Pre-installation	Yes	Yes	Yes
Key-establishment	No	Yes	No

ZigBee network security: ZigBee network as a wireless sensor network is more vulnerable to security attacks compared to a wire network, hence, encryption is necessary for a data transmission. However, the consisting parts of ZigBee network can be used for their original purposes, yet, they are lack in resources to conduct high-degree encryption procedures. To resolve the problem, the system is equipped with a security system which is relatively efficient. The security vulnerability during a removal process of a device that is accessed to ZigBee network, however can cause a serious problem that can collapse the entire network system (Bonghwan, 2014).

Master Key (MK), Link Key (LK) and Network Key (NK) are the keys for ZigBee network security. MK is used for LK generation. LK is to protect the frame at the application layer and transmitted via unicast between two devices. NK is a type of group-key shared by TC and all other devices in ZigBee network and is used to protect the frame at all network layers. MK and LK, shared by TC and another specific device are regarded as TC-MK and TC-LK and MK and LK shared between all devices are regarded as AP-MK and AP-LK (Oh *et al*., 2012).

The key for security can be acquired by three ways. First of all, the key can be received from other devices, so-called, key-transport. It is the most common method, however, requires encryption during key-transport processes as the key can be exposed if any tapping is practiced during the transmission process. Second, it is per-installation, a way to pre-store a usable key in devices in the network. Third, it is key-establishment, a way to generate a new key using mutually exchanged data during the authentication process after securement of reliability via. mutual-authentication between two devices in advance (Kim *et al*., 2012; Bonghwan, 2014). The three ways of acquiring the security key can be describe as in Table 1.

Security mode of ZigBee network comprised of standard security mode and high security mode. Standard security mode, designed for low level security, fundamentally only utilizes NK and high security mode, designed for high level security utilizes all MK, LK and NK (Oh *et al*., 2012).

ZigBee network authentication protocol: In ZigBee network, for generation of a new key between devices or to identify whether devices share the same key, two authentication protocols are used.

First of all, SKKE (Symmetric-Key Key Establishment protocol) authentication protocol generates and identifies LK_B(TC-LK) based on MK_B(TC-MK) and its equation as:

$$LK_B = Kdf(TC, B, RN_{TC}, RN_B, MK_B)$$

Kdf() is a function that generates a new key by using the value of () and TC and B are the ID of each device and RN_{TC} and RN_B are the random numbers generated to prevent any command duplication in each device (Bonghwan, 2014).

Second, MEA (Mutual Entity Authentication) is an authentication protocol to identify each device as properly accessed entity to the network by using NK. By using ID, RN and NK which are transferrable between devices, authenticator is generated and transferred to others and whether the NK being used in the current network has been properly acquired can be indirectly confirmed if the received value and the self-generated authenticator value of the receiving device are identical.

MATERIALS AND METHODS

Proposal for improvement of problems during device removal process from ZigBee network

Device removal process from ZigBee network: Device removal from ZigBee network is differentiated into two types based on its proceeding direction of removal process.

First of all, a device removal process proceeding from TC to ZB starts by TC transmitting a remove-dive command to ZA. ZA transmits a leave command to ZB and remove ZB from the network at the same time after identifying which device to be removed by receiving the command and then, TC which transmitted remove-device command to ZA, removes ID of ZB from the device management list. TC and ZA delete the shared key with ZB. At this point, the remove-device command sent from TC to ZA is encrypted by LK_A shared by TC and ZA, however, the leave command sent from ZA to ZB is not encrypted.

The second device removal process proceeds from ZB to TC. ZB sends a leave command to ZA in order for its removal from the network, then deletes all the keys shared with other devices. ZA identifies the leave command received from ZB and transmits an update-device command to TC notifying the removal command of ZB. TC which received the update-device command deletes the shared key with ZB and the ID of ZB from the device management list. ZA deletes the shared key with ZB as well. Leave command from ZB is encrypted by NK and update-device command sent from ZA to TC is encrypted by LK_A shared between TC and ZA.

Proposed method: A security vulnerability during the device removal process from ZigBee network is that some of the transmitted command during the removal process is not encrypted, hence, any counterfeit and falsification of the command is easily available and identification of a sender is difficult to be practiced.

If a device removal process proceeds from TC to ZB, the remove-device command transmitted from TC to ZA is encrypted by LK_A. Being encrypted by LK_A allows identification of the sender as TC as it means that TC which is shared between ZA and LK_A can exclusively encrypt the command. Furthermore, that is descrambling remove-device command is only available by ZA so that any counterfeit and falsification are securely prevented. However, the leave command from ZA to ZB is not encrypted, hence, anyone can monitor and produce it. For that reason, no response or action can be practiced upon any counterfeit of leave command by a device disguising itself as ZA.

If a removal proceeds from ZB to TC, the leave command from ZB to ZA is encrypted by NK which is a group-key. Being encrypted by NK means that any counterfeit of leave command by a device disguising itself as ZB cannot be prevented.

Accordingly, the thesis would like to propose a method to cope with security problems that may occur during a device removal process from ZigBee network. First of all, in case of a device removal process starting from TC, TC includes MIC(LK_B) in a remove-device command that will be sent to ZA for the removal of ZB, then descramble the command with LK_A. The remove-device command encrypted by LK_A can only be descrambled by ZA which shares LK_A with TC, hence, it becomes identifiable that the remove-device command has not been counterfeited by any other devices and that the sender of the command is TC.

After ZA which received the remove-device command identifies the command, it makes the leave command which will be sent to ZB, the device to be removed include MIC(LK_B) received from TC. Then, encryption of the leave command by LK_{AB} is practiced. It makes ZB identifiable that TC is the device that started the device removal process and being encrypted by LK_{AB} makes it identifiable that the sender of the leave command is ZA and that the leave command has not been counterfeited by any other devices. The proposed improved process as:

- TC encrypts the ID of ZB to be removed and the remove-device command having MIC(LK_B) by LK_A, then transmits them to ZA
- TC deletes ZB from the management list and deletes all keys shared with ZB
- ZA encrypts the leave command having MIC(LK_B), then sends the command to ZB. ZA deletes all shared keys with ZB
- ZB descrambles the leave command by LK_{AB}. When contents are identified, ZB deletes all keys shared with other devices

In case of a device removal process starting from ZB, ZB makes MIC(LK_B) included in the leave command that will be sent to ZA and then makes the command be encrypted by LK_{AB}. If the leave command is encrypted by LK_{AB}, the command can only be descrambled by ZA which shares LK_{AB}. That is, it is identifiable that the device requesting for a removal is ZB and that the command has not been counterfeited by any other devices. Furthermore, by including MIC(LK_B) in an update-device command which will be transmitted from ZA to TC, it becomes identifiable that device requested for a removal to TC is ZB. The improved device removal process starting from ZB is as:

- ZB encrypts the leave command having MIC(LK_B) by LK_{AB}, transmits the command to ZA and then, deletes all keys shared with other devices in the network
- ZA descrambles the leave command by LK_{AB} and identifies ZB, the devices requested for a removal
- ZA encrypts the update-device command having MIC(LK_B) by LK_A and transmits the command to TC. After the transmission of the command, all keys shared with ZB are deleted

TC which received an update-device command from ZA, identifies that the command has been transmitted from ZA by descrambling the command by LK_A and that the device which requested for a removal is ZB by identifying MIC(LK_B). Then, it deletes ZB from the device list and deletes all keys shared with ZB.

RESULTS AND DISCUSSION

Safety analysis: This study analyzes the safety of the proposed method to cope with problems that may occur during a device removal process from ZigBee network.

A security problem during a device removal process proceeding from TC is that the remove-device command transmitted from TC to ZA is encrypted by LK_A, however, the leave command transmitted from ZA to ZB is not encrypted, hence, a device disguising itself as ZA can counterfeit a remove-device command, then, transmit it to ZB. Therefore, the proposed method from this thesis is to include MIC(LK_B) in a remove-device command sent from TC to ZA and to encrypt the command by LK_A for transmission. When ZA receives the remove-device command, descrambles the command with LK_A for an acquisition of MIC(LK_B). ZA includes MIC(LK_B) in the leave command, encrypt the command with LK_{AB} then, transmits it to ZB.

ZB which received a leave command having MIC(LK_B) encrypted by LK_{AB}, descrambles the command with LK_{AB} shared with ZA and identifies whether the sender of the command is ZA. It allows identification of that the leave command has not been counterfeited by a device which does not have LK_{AB}. Furthermore, by identifying MIC(LK_B) included in a leave command whether the sender of the remove-device command transmitted to ZA is TC can be identified.

A security problem that may occur during a device removal process proceeding from ZB is that the leave command sent from ZB to ZA is encrypted by NK, hence, any device disguising itself as ZB in the network can counterfeit a leave command and send it to ZA. Therefore, the proposed method from this thesis is to encrypt the leave command having MIC(LK_B) transmitted from ZB to ZA by LKAB.

If a leave command that is sent from ZB is encrypted by LK_{AB}, descrambling the command can be only practiced by ZA which shares LK_{AB}. That is, it is identifiable that the leave command has been sent from ZB and that the leave command has not been counterfeited by any other devices. Furthermore, if MIC(LK_B) is included in an update-device command that is transmitted from ZA to TC it becomes identifiable by TC that the devices requested for a removal is ZB.

CONCLUSION

Devices in the network are included in the device management list through application and authentication procedure and deleted from the list through removal procedures. Device removal processes from the ZigBee network is divided into two types based on the proceeding direction of the device removal processes.

The device removal processes starting from TC starts with a transmission of a remove-device command from TC to ZA for a removal of ZB. The remove-device command from TC to ZA is encrypted by LK_A, hence, the sender can be identified and it is recognizable that other devices cannot counterfeit the remove-device command as

descrambling of the command is only practicable by ZA which shares a LK_A. However, the leave command sent from ZA which received a remove-device command, to ZB is not encrypted any device disguising itself as ZA can counterfeit the leave command, therefore, security problems may occur.

Accordingly, the thesis makes $MIC(LK_B)$ be included in a remove-device command and suggested a method to encrypt the leave command with a shared key between two devices during a command transmission. ZA which received a remove-device command, counts $MIC(LK_B)$ in the received command into a leave command, then transmits the command after encryption with LK_{AB}. The leave command encrypted by LK_{AB} can be identified with the sender, ZA which shared LKAB and $MIC(LK_B)$ included in the leave command allows an identification of the sender of the remove-device command as TC.

The deice removal process starting from ZB gets initiated when a leave command is sent from the device ZB desiring for its removal to ZA. However, as the leave command from ZB is encrypted with NK that is shared by all devices in the network, any counterfeit of the leave command by a disguised device as ZB cannot be prevented.

Hence, this thesis proposed a method to encrypt the leave command having $MIC(LK_B)$ with LK_{AB} shared with ZA, then to transmit the command from ZB desiring for its removal to ZA.

If a leave command from ZB is encrypted by LK_{AB}, it allows an identification by ZA that the leave command has been sent from ZB. Furthermore, as letting ZA include $MIC(LK_B)$ originally included in the leave command into an update-device command heading to TC, ZA can allow TC to identify that the device requesting for a removal is ZB.

The improved method of device removal process from ZigBee, proposed in this thesis, it assumes that there is already a safely shared TC-MK between TC and devices. If TC-MK is exposed to malicious devices, any counterfeit and falsification of a leave command by the devices becomes available, moreover, their disguises as other devices becomes available. Therefore, researches on safe storage and management of pre-shared TC-MK is necessary.

REFERENCES

Back, M.K., H.J. Yim and K.C. Lee, 2014. Zigbee adaptor for two-way data-event-service interoperation in internet of things. KIPS. Trans. Comput. Commun. Syst., 3: 107-114.

Bonghwan, K., 2014. Secure and efficient key established protocol in ZigBee network. Master Thesis, Dankook University, Yongin, South Korea.

IEEECS., 2012. IEEE standard for information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements part 11. IEEE Computer Society, Washington, D.C., USA.

Jang, B.I. and C.S. Kim, 2014. A study on the security technology for the internet of things. J. Secur. Eng., 11: 429-438.

Jihoon, C., 2010. A study on the safe authentication and key management mechanism in the HAN environment based on Zigbee. MBA Thesis, Soongsil University, Seoul, South Korea.

Kim, B.H. and C.S. Park, 2013. Secure membership protocol for ZigBee network. J. Korea Inst. Inf. Secur. Cryptology, 23: 405-416.

Kim, B.H., J.M. Lim and C.S. Park, 2012. Analysis of ZigBee security mechanism. J. Secur. Eng., 9: 417-728.

Oh, S.M., S.K. Choi, Y.J. Kwon and C.S. Park, 2012. Secure key distribution protocol for ZigBee wireless sensor network. J. Korea Inst. Inf. Secur. Cryptology, 22: 745-759.

ZigBee Alliance, 2008. ZigBee-2007 specification: ZigBee document. Zigbee Alliance, Davis, California.