Security Threats Analysis for ZigBee Home Network Services

Woo Chool Park[1], Myung Soo Lee[1], Myung Hyun Yoon[1], June Jae Yoo[1], Sung Dong Kim[1], Sung Hyun Yang[2]

[1]Ubiquitous Computing Research Center, Korea Electronics Technology Institute,
[2]Ubiquitous Home Network Center, KwangWoon University
{wcpark, leems, yoon}@keti.re.kr

Abstract. ZigBee is a wireless communications standard that provides a short-range cost effective networking capability. It has been developed with the emphasis on lowcost battery powered applications, such as building automation, industrial and commercial controls, marine wireless, personal healthcare and advanced tagging. The IEEE and ZigBee alliance have introduced ZigBee to provide the first general standard for these applications. ZigBee enabled products are rapidly being developed thanks to considerable investment by some market leaders to provide a simple, low cost implementation route. In this paper, we have analyzed IEEE 802.15.4, ZigBee security issues, hacked ZigBee home network system in simulation by NS-2, a real home network system. We highlight places where application designers should exercise care when implementing and using ZigBee devices. ZigBee home network attack scenarios are models and their impacts are evaluated. We urge ZigBee home network implementer to consider security problem.

Keywords: ZigBee, IEEE 802.15.4, Security, Home Network, Ubiquitous Computing

1 Introduction

This paper presents a systematic analysis of the threats faced by IEEE 802.15.4 [1] and the ZigBee Alliance [2]. Attack scenarios are models and their impacts are evaluated. Some security problems within the current ZigBee security architecture are identified and remedies are suggests. And countermeasures of various attacks are also given.

ZigBee is a wireless communications standard that provides a short-range cost effective networking capability. It has been developed with the emphasis on lowcost battery powered applications, such as building automation, industrial and commercial controls, marine wireless, personal healthcare and advanced tagging. The IEEE and ZigBee Alliance have introduced ZigBee to provide the first general standard for these applications. With a tenth of the memory requirements of Bluetooth and a fraction of the processing power needed for 802.11 networking devices, ZigBee is the best solution for low data-rate, short-range communications. ZigBee enabled products

are rapidly being developed thanks to considerable investment by some market leaders to provide a simple, low cost implementation route.

ZigBee also offers:

- Low power consumption - optimized for battery operation
- Licence free operation in the 2.4GHz, 868MHz and 915MHz bands
- Simple protocol definition can be implemented on low-cost microcontrollers
- Hundreds of devices per network
- Network flexibility - star, cluster tree or Mesh configuration [3]

The rest of this paper is structured as follows: In Section 2, we give an overview of security architecture of IEEE 802.15.4 and ZigBee, present a ZigBee security objectives. Then. In Section 3, we introduce our NS-2 based ZigBee simulator and provide some attack modeling results with analyses. In Section 4, we implement a real ZigBee home network services and provide some attack modeling results with analyses. In Section 5, we focus on the design of secure ZigBee home network services. Finally, in Section 6, we conclude with a summary.

2 Security Architecture Defined by IEEE 802.15.4 and ZigBee

IEEE 802.15.4 provides link layer security for LR-WPANs, including access control, confidentiality, message integrity, and optional message freshness, as outlined in Table 1.

Table 1. IEEE 802.15.4 Security Suites

Security suite name	Access Control	Data Encryption	Frame Integrity	Sequential Freshness (optional)
None				
AES-CTR	*	*		*
AES-CCM-128	*	*	*	*
AES-CCM-64	*	*	*	*
AES-CCM-32	*	*	*	*
AES-CBC-MAC-128	*		*	
AES-CBC-MAC-64	*		*	
AES-CBC-MAC-32	*		*	

Access control is supported by all security suites except none and it provides the ability for a device to select the other devices with which it is willing to communicate. For security purpose, each device keeps an ACL in its MAC sublayer PAN Information Base (MPIB). The ACL contains up to 255 entries, one for each destination device. Each ACL entry consists of the destination address (IEEE address and optional logical short address), security suite identifier, and other security materials. By default, security is not enabled in 802.15.4. To enable security, upper layers should specify a security suite other than None in the ACL entry corresponding

to the destination. However, acknowledgment frame is required to always use security suite None and, thus, not protected.

The AES-CTR security suite provided confidentiality protection by encrypting the payload of a frame, using the AES block cipher with counter mode. The AES-CBC-MAC security suite, on the other hand, provides integrity protection, using the CBC-MAC. And the AES-CCM security suite provides both confidentiality and integrity protection, using the CCM. Both AES-CBC-MAC and AES-CCM have three variants depending on the size of the MAC used.

Upon 802.15.4, the ZigBee Alliance defines the NWK and application layer security services, based on CCM*, a minor modification of CCM. Besides all the features of CCM, CCM* additionally offers encryption-only and integrity-only capabilities, thus eliminates the need for CTR and CBC-MAC modes. Also, CCM* allows using a single key for all CCM* security levels. This is different from the MAC sublayer security modes, which require different keys for different security levels. As a result, different layers in ZigBee is to use the so-called open trust mode, in which different layers of the communication stack and all applications running on a single device trust each other.

ZigBee uses a 128-bit link key (more actually its derivatives, see details below) to secure pairwise communications, probably multiple hops away, and a 128-bit Network key to secure broadcast communications. A device can acquire link keys and a Network key via key-transport or preinstallation. Link keys can also be obtained through key-establishment technique, based on a "master" key, which itself can be obtained via key-transport or preinstallation. The ultimate security between devices depends on the secure initialization and installation of these keys.

To avoid security leaks due to unwanted interactions between different security services, ZigBee also uses a one-way function to derive various service-specific keys from the link key, including the key-load key, key-transport key, and data key. The key-load key, key-transport key, and data key are used to protect frames containing transported master keys, frames containing other transported keys, and all other frames that need to be secured, respectively.

Table 2. Security Levels Available in ZigBee.

Security-Level	Security-Attribute	Data Encryption	Frame Integrity
‘000’	None		
‘001’	MIC-32		*
‘010’	MIC-64		*
‘011’	MIC-128		*
‘100’	ENC	*	
‘101’	ENC-MIC-32	*	*
‘110’	ENC-MIC-64	*	*
‘111’	ENC-MIC-128	*	*

ZigBee performs centralized security control via a trust center. There is exactly one trust center in each secure network. The trust center is responsible for distributing and maintaining the Network key to devices as well as binding two applications and enabling end-to-end security between devices (e.g., distributing master keys of link keys). In both IEEE 802.15.4 and ZigBee, a frame counter, which is a monotonically

increasing 4-octet sequence number bound to an encryption key, is used to prevent replay attacks [4, 5, 6].

2.1 Security Objectives of ZigBee Home Network Services

* Confidentiality: The main goal of confidentiality is to ensure that sensitive data are not disclosed to any entities other than the intended receivers. Confidentiality is the basic method to prevent passive attacks.
* Integrity: It is a basic requirement that a message is received as it is transmitted at the sender side. However, because of malicious attacks or due to benign failures such as transmission collisions and radio propagation impairment, a message may be corrupted in transit. Integrity guarantees that a message is transferred as it is, without replacement, deletion, injection, resorting, or any other modifications
* Authentication: Authentication is used by a node to verify the identity of the peer node it is communicating with (entity authentication) or the origin of a message (data origin authentication). Authentication is important in ZigBee, especially in administrative tasks such as association, orphaning, coordinator realignment, superframe setup, beaconing, and the resolution of PAN identifier (ID) confliction.
* Freshness: Unlike most general purpose networks, ZigBee network is normally task specific. Information flowing in an LR-WPAN is often time-sensitive. In such networks, it is not enough to only guarantee confidentiality and authentication. Replaying stable (but secret and authentic) messages can substantially disrupt the network operations and even cause catastrophes. Freshness ensures that the received message is recent and valid in the context of the applications.
* Availability: The goal of availability is to ensure the survivability of network services despite attacks(e.g., denial of service (DOS) attacks) and normal failures (e.g. node failure and link breakdown). As ZigBee network is highly resource constrained networks, they can easily suffer from attacks based on resource consumption.
* Fairness: Fairness ensures that the network resources are used in a fair and efficient way [7, 8, 9].

3 ZigBee Home Network Attack Simulation by NS-2

This simulation is a Sybil attack in the case of ZigBee home network, which is the result of NS-2 on the attacks and the faults of ZigBee [10].

* ZigBee home network attack modeling

A malice node acquires several node identity and registers a normal node to coordinator which takes over system control, happens error action.

* ZigBee home network attack assumption

1. packet sniffing which acquires packet format
2. node capture, sniffing which can acquires network key, mater key
3. could be registered coordinator by acquired mater key
4. No mobility of sensor nodes for Home control/automation service

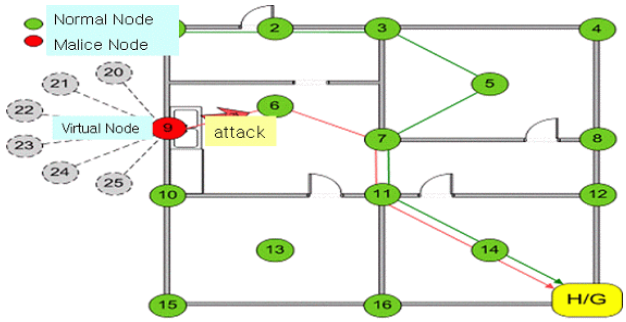

Fig. 1. ZigBee Home Network Attack Scenarios.

* ZigBee home network attack scenarios

1. The 9th node is infected with malice node or malice 9th node is joined by ZigBee network.
2. Every node transmits smoke, thermal data to H/G (Home Gateway, Coordinator)
3. Malice node which has virtual ID requests to join network sending Join_Request messages
4. Malice node can acquire network key value using packet sniffer. H/G considers virtual node as normal node after Join_Confirm
5. Malice node sends different message using several virtual ID to attack ZigBee network.
6. Considering the state of smart home is normal state, H/G is mistaken to happen a fire considering malice node which sends several messages.

The Fig. 2 shows ZigBee home network attack simulation by NS-2, the 6th node sends mistaken messages using several virtual ID to Home Gateway.

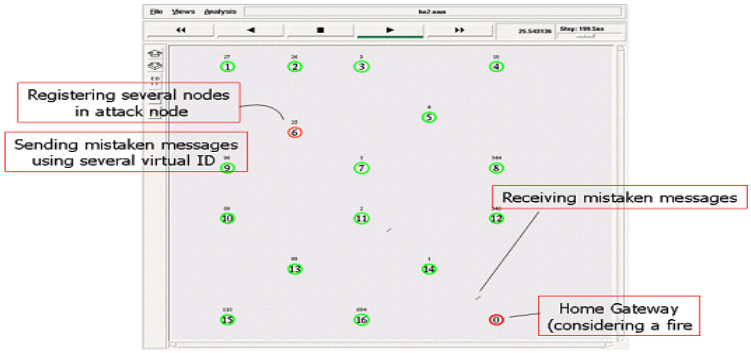

Fig. 2. ZigBee Home Network Attack Simulation by NS-2.

The Fig. 3 shows the information of nodes states and sensing type, the malice node 9th joins the normal ZigBee network.

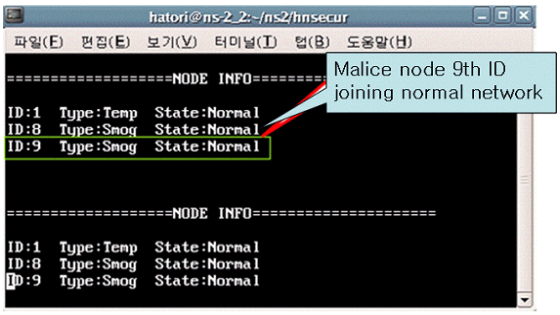

Fig. 3. The malice node 9th joining normal ZigBee Network..

The Fig. 4 shows to registering several virtual ID(20 – 25) nodes send mistaken messages to home gateway.

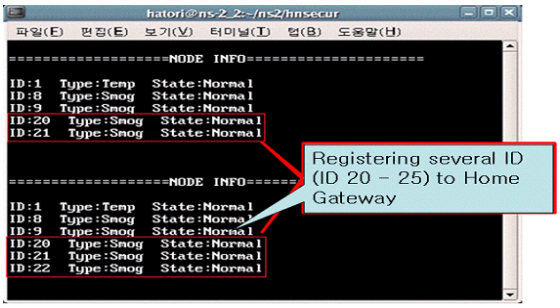

Fig. 4. Several virtual ID nodes send mistaken messages to home gateway.

4 Hacking ZigBee Home Network Service

In this paper, we have implemented ZigBee home network services which are home automation, control. We have demonstrated security threats over ZigBee home network services. We have hacked ZigBee home network service using our ZigBee hacking tool. The Fig. 5 shows 8-bit microcontroller unit (ATmega128), RF data modem is CC2420. The total number of passives required is generally under a dozen, mainly capacitors, and one crystal.

Fig. 5. ZigBee Device (including antenna, RF data modem, application processor, all necessary passives and 16MHz crystal, I/O port flex connector, 4-layer circuit board, about 15*40mm).

The Fig. 6 shows our smart home architecture over ZigBee home network service which is home automation, control service. There are 10 ZigBee devices, coordinator device collects data from 9 ZigBee devices.

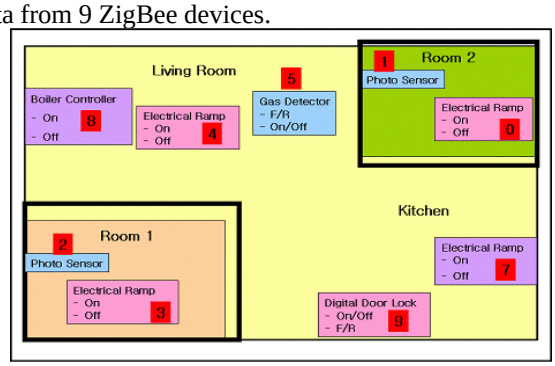

Fig. 6. The smart home architecture over ZigBee home network service.

ZigBee hacking tool sniffs the packets in the zigbee network. This figure shows the sniffing of packet data. In the Information of the selected node it can read FCF, PAN ID, Dst Addr, Src Addr, Seq no. Key value, ZigBee Mac frame format. In the command part it consist of selecting serial port, connected to serial port and ZigBee node. The packets of ZigBee nodes can be sniffed to serial port, try to Dos attack by Attack Command. The pattern of Dos attack is to modify SIFS interval of MAC layer of CSMA/CA.

It is continuously transmitted to a volume of messages. According to Dos Attack the state of normal node do not act normal performance, it transmits a abnormal sensing messages to H/G (Home Gateway, Coordinator) supposing abnormal node to normal node.

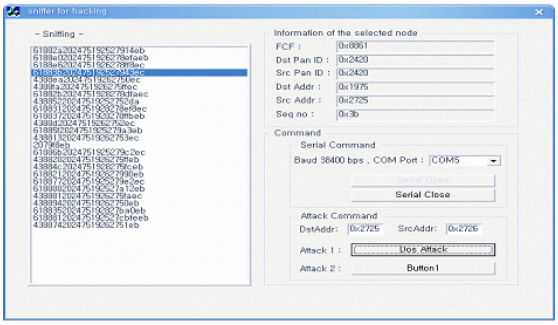

Fig. 7. ZigBee hacking tool for smart home service.

The Fig. 8 shows intrusion detection monitoring tool. It can receive data by serial port connecting ZigBee devices. There are 0 - 7th nodes, the coordinator node receives sensing data. It can monitor the state of hacking considering the receiving data pattern to abnormal data pattern by intrusion detection engine.

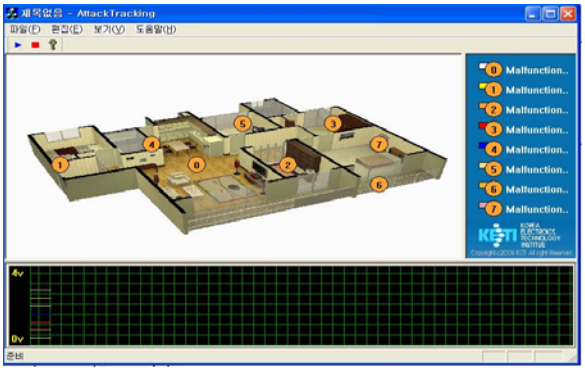

Fig. 8. Intrusion detection monitoring tool for ZigBee home network service.

5 Improving the Security of ZigBee Home Network Services

Attacks such as jamming and collision are closely related to PHY layer and are difficult to cope with. Normally there is no way for a node under such attacks to flight back automatically. Securing the PHY layer in wireless environments is a challenging task due to the feature of open media. For some applications like battle field communications where high reliability and strong security are required, spread spectrum techniques will play an important role. For other applications, we can selectively equip some important devices. (coordinators, other devices in charge of network management) with spread spectrum function module so that they can effectively reject inferences. Although the whole network is not protected devices will be able to perform critical management functions, for example, monitor the behavior

of network and request for human interventions when needed. The availability of multiple frequency bands and channels also provides some protection against those attacks.

Sybil attack that is related to association can be prevented by authenticating sensitive information such as source address and tree level. This in general requires the use of some public key scheme and certificate services. We suggest the simple key management scheme which ZigBee devices have original key value for ZigBee network and exchanges key value with coordinator.

6 Conclusion

ZigBee home network service is expected to fill every aspect of our lives and play increasingly important roles. This paper focuses on the security problems in ZigBee home network service. We present the security of IEEE 802.15.4 and ZigBee and security objectives for ZigBee home network service. A simulator is developed for modeling attack and some experimental results are presented. We have implemented a real ZigBee home network system to demonstrate security problems. Some problems are identified and remedies are suggested. We urge ZigBee home network implementer to consider security problem.

References

[1] IEEE 802.15.4, Draft Standard: Low Rate Wireless Personal Area Networks, Feb. 2003

[2] ZigBee Alliance, http://www.zigbee.org. 2006.

[3] ZigBee Network Specification, V 1.0, Dec. 2004.

[4] ZigBee Security Services Specification, V1.0, Dec. 2004.

[5] FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Dept. of Commerec/N.I.S.T, Nov. 2001.

[6] D. Whiting, R. Housley, and N. Ferguson, “Counter with CBC-MAC (CCM), “RFC 3610, SPT. 2003.

[7] Jianliang Zheng, Myung J. Lee, Michael Anshel, “Toward Secure Low Rate Wireless Personal Area Networks”, IEEE Transactions on Mobile Computing, Vol.5, No.10, OCT. 2006

[8] N. Sastry and D. Wagner, “Security Considerations for IEEE 802.15.4 Network,” Proc. 2004 ACM Workshop Wireless Security, Oct. 2004.

[9] A. Perrig, R. Szewczyk, V.Wen, D.Culler, and J.D.Tygar, “SPINS: Security Protocols for Sensor Networks,” Wireless Networks J., Sept. 2002.

[10] USC Information Sciences Institute, Network Simulator-NS2, http://www.isi.edu/nsnam/ns, 2006.