ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Security Issues in ZigBee Networks during Data Broadcasting in Wireless Mesh Network

Kuber Singh
Department of Computer Science & Engineering
B. T. Kumaon Institute of Technology,
Dwarahat, Almora, Uttarakhand, INDIA
spritekuber@gmail.com

Vinod Kumar Mishra*
Department of Computer Science & Engineering
B. T. Kumaon Institute of Technology,
Dwarahat, Almora, Uttarakhand, INDIA
vkmishra2005@gmail.com

Meenakshi
Department of Computer Science & Engineering
B. T. Kumaon Institute of Technology,
Dwarahat, Almora, Uttarakhand, INDIA
meenakshisngh06@gmail.com

Abstract: In this paper, we investigate the principal security issues for wireless ZigBee networks and focuses on the security service provider part of the ZigBee specification, which interacts with the network and applications layers. We study the security threats that a ZigBee networks faces & the security goals to be achieved by ZigBee network and we identify the new challenges and opportunities posed by this new networking environment and explore approaches to secure its communication.

Keywords: ZigBee protocol; ZigBee network; Security issues of ZigBee; Security architecture; security mechanism and security modes.

I. INTRODUCTION

ZigBee technology was developed for a wireless personal area networks (PAN), aimed at control and military applications with low data rate and low power consumption. ZigBee is a low-cost, low-power, and highly reliable wireless mesh networking standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries and the mesh networking provides high reliability & more extensive range [1], [2].

ZigBee is a new standard developed by the ZigBee Alliance for personal-area networks (PANs). Consisting of more than 270 companies (including Free scale, Ember, Mitsubishi, Philips, Honeywell, and Texas Instruments), the ZigBee Alliance is a consortium that promotes the ZigBee standard for a low-rate/low-power wireless sensor and control network. The ZigBee protocol stack is built on top of IEEE 802.15.4, which defines the Media Access Control (MAC) and physical layers for low-rate wireless personal-area network (LR-WPAN) [3]. The ZigBee standard offers a stack profile that defines the network, security, and application layers. Developers are responsible for creating their own application profiles or integrating with the public profiles that were developed by the ZigBee Alliance. The ZigBee specification is an open standard that allows manufacturers to develop their own specific applications that require low cost and low power. The ZigBee specification has undergone multiple modifications. The major milestones in its revision history are as follows [4]:

In 2004, the ZigBee Alliance published its first specification, which supported a home control lighting profile. However, the ZigBee Alliance no longer supports the 2004 specification. In February 2006, the ZigBee Alliance published the ZigBee Stack 2006, which contained modifications to ZigBee 2004. In October 2007, the ZigBee Alliance published two feature sets called ZigBee and ZigBee PRO. The ZigBee feature set is inter-operable with ZigBee PRO. If a network is based on the ZigBee PRO stack, devices from the ZigBee feature set stack can join the network as end devices. Likewise, if a network is based on the ZigBee stack, ZigBee PRO devices can join the network as end devices.

A. ZigBee Network (Device Types):

A ZigBee network consists of ZigBee nodes (devices). A node consists of a microcontroller, a transceiver, and an antenna. A ZigBee node uses stack profiles, which are developed by software. A node can be used for a wide variety of applications for example, lighting control, smoke-detector, and home-security monitoring. Therefore, a node can support multiple subunits, and each subunit has an application object that describes the subunit function. A node can operate as either a full function device (FFD) or reduced function device (RFD). An FFD can perform all the tasks that are defined by the ZigBee standard, and it operates in the full set of the IEEE 802.15.4 MAC layer. An RFD performs only a limited number of tasks. There are five types of ZigBee network devices [4]:

- ***a. Coordinator:*** A coordinator is an FFD and responsible for overall network management. Each network has exactly one coordinator. The coordinator starts the network, selects the channel to be used by the network, assigns how addresses are allocated to nodes or routers, permits other devices to join or leave the network, holds a list of neighbors & routers and transfers application packets.
- ***b. End Device:*** An end device can be an RFD. An RFD operates within a limited set of the IEEE 802.15.4 MAC

layer, enabling it to consume less power. The end device (child) can be connected to a router or coordinator (parent). It also operates at low duty cycle power, meaning it consumes power only while transmitting information. Therefore, ZigBee architecture is designed so that an end device transmission time is short. The end device Joins or leaves a network and transfers application packets.

c. ***Router:*** A router is an FFD. A router is used in tree and mesh topologies to expand network coverage. The function of a router is to find the best route to the destination over which to transfer a message. A router performs the function similar to a coordinator except the establishing of a network.

d. ***Zigbee Trust Center (ZTC):*** The ZigBee trust center is a device that provides security management, security key distribution, and device authentication.

e. ***Zigbee Gateway:*** The ZigBee gateway is used to connect the ZigBee network to another network, such as a LAN, by performing protocol conversion.

II. CHARACTERISTICS AND APPLICATION OF ZIGBEE NETWORKS

Several standards currently exist for wireless networks, including Bluetooth, WiFi, and WiMax. ZigBee is a new standard for wireless sensor and control networks. The following characteristics make the ZigBee network more useful [5].

a. Low battery consumption. A ZigBee end device should operate for months or even years without needing its battery replaced.
b. Low cost.
c. Low data rate. The maximum data rate for a ZigBee device is 250Kbps.
d. Easy to implement.
e. Supports up to 65,000 nodes connected in a network.
f. ZigBee can automatically establish its network.
g. ZigBee uses small packets compared with WiFi and Bluetooth.
h. Max throughput 250 Kbps.
i. Small, lightweight stack (120 KB).
j. Built-in star or mesh topology support.
k. Range commonly 10-100 meters.

A. Application of Zigbee Network:

The ZigBee Alliance developed the following application profiles [6]-[7]:

a. ***Smart energy:*** ZigBee can be used to quickly read electrical, gas, and water meters. The ZigBee smart energy network enables wireless communication between the advanced metering infrastructure (AMI) and the home-area network.

b. ***Commercial building automation:*** In a commercial building, ZigBee can be an integral tool in building maintenance. ZigBee wireless can be used to monitor smoke-detector operation and fire-door position.

c. ***Home automation:*** ZigBee home automation profile defines devices that are used for residential and commercial applications. ZigBee can be used to remotely control lighting, heating, cooling, and door-locking mechanisms.

d. ***Personal, home, and hospital care (PHHC):*** This profile is used for monitoring the personal health of a patient at home without limiting a patient's mobility. For example, it can remotely monitor blood pressure and heart rate.

e. ***Telecom applications:*** Embedding a ZigBee device into a mobile phone or PDA creates a new device called a ZigBee mobile device. A ZigBee mobile device can be used to communicate with other ZigBee devices.

B. Remote control for consumer electronics (ZigBee RF4CE):

Currently, most remote controllers are using infrared (IR) technology, which requires line of sight; ZigBee RF4CE is a protocol that uses radio frequency (RF) to replace IR technology for remote controllers used in consumer electronics [8].

III. SECURITY ISSUES IN ZIGBEE NETWORK

As one of its defining features, ZigBee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames and controlling devices. It builds on the basic security framework defined in IEEE 802.15.4. This part of the architecture relies on the correct management of symmetric keys and the correct implementation of methods and security policies. Security and data integrity are key benefits of the ZigBee technology. ZigBee leverages the security model of the IEEE 802.15.4 MAC sublayer which specifies four security services [4]:

a. ***Access Control-*** The device maintains a list of trusted devices within the network.
b. ***Data Encryption*** **-** This uses symmetric key 128-bit advanced encryption standard.
c. ***Frame Integrity-***To protect data from being modified by parties without cryptographic keys.
d. ***Sequential Freshness-***To reject data frames that have been replayed the network controller compares the freshness value with the last known value from the device and rejects it if the freshness value has not been updated to a new value

Security issues for Zigbee networks are basically identical to security requirements for any other communication system, and include following attributes:

A. Attacks against ZigBee:

ZigBee wireless attacks and security has attracted a lot of interest by government and industry security professionals as well as the hacker community. Each is looking at the security capabilities of the 802.15.4 protocol as well as how manufacturers are implementing the ZigBee radios into products and equipment. Often it is the "implementations" part of the equation that is causing most of the security risks. This is clearly evident in the types of attacks used against the devices. ZigBee and the 802.15.4 framework it rides on were

designed with security in mind, but as we have all learned, security is only effective if it's implemented properly. While there are numerous types of attacks that have been successfully leveraged against ZigBee devices, they generally fall into three categories: Physical attacks, Key attacks, and Replay and Injection attacks:

a) ***Physical Attacks-*** If a knowledgeable attacker can gain physical access to a device containing a ZigBee radio; chances are good that they can compromise it. What makes physical attacks so effective is being able to interact physically with the device to obtain an encryption key used by the target ZigBee network. Many ZigBee radios use a hard-coded encryption key that is loaded in RAM memory when the device is powered. Since these keys are typically written (flashed) on all the devices in a ZigBee network, it's highly unlikely that the keys will ever be changed. Knowing this, attackers can utilize special serial interfaces on the ZigBee device to attempt to capture the encryption keys as those keys are moved from flash to RAM during power up [9].

b) ***Key Attacks-*** Other forms of key attacks are possible by utilizing remote means to obtain encryption keys. ZigBee radios often use one of two encryption key methodologies to ensure that devices have the appropriate keys to talk to each other. These methodologies are known as pre-shared keying and Over the Air (OTA) key delivery. Larger, more sophisticated ZigBee networks will typically utilize OTA for security and ease of updating.

c) ***Replay and Injection Attacks-*** One final type of attack we'll discuss can utilize key-based attacks blended with packet replay and/or injection attacks to trick the ZigBee device into performing unauthorized actions. ZigBee radios are susceptible to these types of attacks because of the lightweight design of the protocol, which has very minimal replay protection.

IV. ZIGBEE SECURITY ARCHITECTURE

ZigBee uses 128-bit keys to implement its security mechanisms. A key can be associated either to a network, being usable by both ZigBee layers and the MAC sublayer, or to a link, acquired through pre-installation, agreement or transport. Establishment of link keys is based on a master key which controls link key correspondence. Ultimately, at least the initial master key must be obtained through a secure medium (transport or pre installation), as the security of the whole network depends on it. Link and master keys are only visible to the application layer. Different services use different one way variations of the link key in order to avoid leaks and security risks [9], [10].

ZigBee is built on the Physical layer (PHY) and the Medium Access Control layer (MAC), both defined by the IEEE 802.15.4 standard. The PHY layer can operate in two separate frequency ranges: lower 868(European)/915(United States, Australia, etc.) MHz and higher 2.4 GHz (worldwide). The MAC layer controls access to the radio channel using a CSMA-CA mechanism. Upon this structure, ZigBee builds the Network layer (NWK) and the Application layer (APL) which consists of the Application Support sublayer (APS) and the ZigBee Device Object (ZDO). Fig-1 shows the ZigBee stack architecture, including the end manufacturer defined part in dashed box. The security architecture is distributed among the network layers as follows:

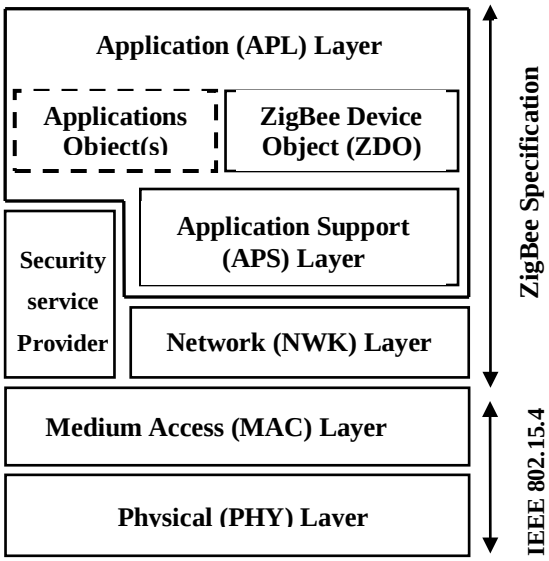

Figure-1 (Zigbee Architecture)

The MAC sublayer is capable of single hop reliable communications. As a rule, the security level it is to use is specified by the upper layers.

The network layer manages routing, processing received messages and being capable of broadcasting requests. Outgoing frames will use the adequate link key according to the routing, if it is available; otherwise, the network key will be used to protect the payload from external devices.

The application layer offers key establishment and transport services to both ZDO and applications. It is also responsible for the propagation across the network of changes in devices within it, which may originate in the devices themselves (for instance, a simple status change) or in the trust manager (which may inform the network that a certain device is to be eliminated from it). It also routes requests from devices to the trust center and network key renewals from the trust center to all devices.

V. SECURITY MECHANISM IN ZIGBEE NETWORKS

ZigBee security, which is based on a 128-bit AES algorithm, adds to the security model provided by IEEE 802.15.4. ZigBee's security services include methods for key establishment and transport, device management, and frame protection [7].The ZigBee specification defines security for the MAC, NWK and APS layers. Security for applications is typically provided through Application Profiles [11], [12].

A. ZigBee Protocol Stack:

The ZigBee stack architecture is made up of a set of blocks called layers. Each layer performs a specific set of services for the layer above, including a data entity that provides a data transmission service and a management entity that provides all other services. Each service entity exposes an interface to the

upper layer through a service access point (SAP), and each SAP supports a number of service primitives to achieve the required functionality.

The ZigBee stack architecture, is based on the standard open systems interconnection seven-layer model, but defines only those layers relevant to achieving functionality in the intended market space. The IEEE 802.15.4 defines specifications of the physical layer and MAC layer for supporting simple devices that consume minimal power and typically operate in a personal operating space. The ZigBee Alliance builds on this foundation by providing the network layer and the framework for the application layer, which includes the application support sub-layer (APS), the ZigBee device object (ZDO), and the manufacturer-defined application objects.

B. *Trust Center:*

The Trust Center decides whether to allow or disallow new devices into its network. The Trust Center may periodically update and switch to a new Network Key. It first broadcasts the new key encrypted with the old Network Key. Later, it tells all devices to switch to the new key. The Trust Center is usually the network coordinator, but is also able to be a dedicated device. It is responsible for the following security roles -:

a. Trust Manager, to authenticate devices that request to join the network.
b. Network Manager, to maintain and distribute network keys.
c. Configuration Manager, to enable end-to-end security between devices.

C. *Security Keys:*

ZigBee uses three types of keys to manage security: Master, Network and Link.

a. Master Keys- These optional keys are not used to encrypt frames. Instead, they are used as an initial shared secret between two devices when they perform the Key Establishment Procedure (SKKE) to generate Link Keys. Keys that originate from the Trust Center are called Trust Center Master Keys, while all other keys are called Application Layer Master Keys.

b. Network Keys- These keys perform Network Layer security on a ZigBee network. All devices on a ZigBee network share the same key. High Security Network Keys must always be sent encrypted over the air, while Standard Security Network Keys can be sent either encrypted or unencrypted. Note that High Security is supported only for ZigBee PRO.

c. Link Keys- These optional keys secure unicast messages between two devices at the Application Layer. Keys that originate from the Trust Center are called Trust Center Link Keys, while all other keys are called Application Layer Link Keys.

D. *Network Layer Security:*

The Network (NWK) layer provides functionality to ensure correct operation of the MAC layer and also provides suitable service interface to the APL layer. When a NWK layer frame needs to be secured, the NWK layer secures it by using AES encryption/ authentication in the Enhanced Counter with CBC-MAC (CCM) mode of operation. The NWK layer processes outgoing/incoming frames in order to securely transmit/receive them.

The upper layers control the security processing operations by setting up the security keys, frame counters and the security level [13].

E. *Application Layer Security:*

Application (APL) Layer is composed of the APS sub layer, ZDO and manufacturer defined application objects. A maximum of 240 distinct application object scan be defined. ZDO is responsible for initializing APS, NWK, Security Service Provider, and assembling the information from applications. ZDOs are applications that employ NWK and APS primitives to implement ZigBee End Devices, ZigBee Routers and ZigBee Coordinators. When an APL layer frame needs to be secured, the APS sublayer handles security.

F. *Security Modes:*

ZigBee PRO offers two different security modes: Standard and High.

a. Standard Security Mode - In Standard Security mode, the list of devices, master keys, link keys and network keys can be maintained by either the Trust Center or by the devices themselves. The Trust Center is still responsible for maintaining a standard network key and it controls policies of network admittance. In this mode, the memory requirements for the Trust Center are far less than they are for High Security mode.

b. High Security Mode - In High Security mode, the Trust Center maintains a list of devices, master keys, link keys and network keys that it needs to control and enforce the policies of network key updates and network admittance. As the number of devices in the network grows, so too does the memory required for the Trust Center.

The additional security capabilities inherent in ZigBee PRO are critical as ZigBee is used in increasingly important applications like control of critical systems infrastructure, whether in a commercial building, utility grid, industrial plant or a home security system must not be compromised.

VI. POSSIBLE SOLUTIONS FOR ZIGBEE NETWORKS

A. *Solution for Network Discovery and Location Tracking Attack:*

The hacking tool that is used to discover the ZigBee network uses the same mechanism that is used by ZigBee devices. There is no solution for this attack since the network discovery process can't be disabled by any means as it is part of the ZigBee mechanism. However, it is helpful to understand the impact of this attack and evaluate the ZigBee network accordingly [3].

B. *Solution for Packet and Key Sniffing:*

Packet sniffing or eavesdropping in general is one of the well known attacks. The only mechanism that is used to avoid

such attack is the CCM* integrity algorithm that provides encryption for the data being transmitted. So, in order to avoid this attack, the network administrator should ensure that a strong key is selected to avoid data leakage.

C. Solution for Replay Attack:

In order to avoid the replay attack, the ZigBee stack should be able to identify the frames by a sequence number and make sure that the received number is greater than that previously received frame. However, ZigBee stack has only 8 bits of network sequence numbers in which an attacker can take advantage of and retransmit the frame after waiting 255 frames.

D. Benefits of Using Cognitive Radio:

The advantage of using cognitive radio is its ability to use software in processing the signal, which results in higher cycle rates when compiling. In addition, it is easier and more efficient to program the modulation and the demodulation of the signal while during experiments. There is no need for additional hardware circuitry to be developed. So using CR as a spectrum analyzer gives us the ability to scan the spectrum and analyze received ZigBee packets passively.

VII. CONCLUSION

ZigBee is an emerging wireless network standard with low resource requirements. The latest version of the ZigBee Specification, ZigBee-2007, enhances the security of ZigBee. In this paper we presented a high level self-contained overview of the ZigBee-2007 security. We explained the key points of the specification such as security in different layers, computations behind key establishment and authentication schemes. We analyze the security issues in zigbee protocol and their possible solutions.

VIII.REFERENCES

[1] Tulin Mangir, Lelass Sarakbi, Harvy Younan “Analyzing the Impact of Wi-Fi Interference on ZigBee Networks Based on Real Time Experiments” in International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.4, pp. 1-10, (2011).

[2] Muhammad Shoaib Siddiqui, Choong Seon Hong‘’Security Issues in Wireless Mesh Networks’’ in International Conference on Multimedia and Ubiquitous Engineering(MUE), pp.1-6, September 2007.

[3] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[4] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks" in ACM/Kluwer International Journal of Wireless Networks (ACM WINET), Vol. 9, No. 5, September 2003.

[5] N. B. Salem and J-P Hubaux, “Securing Wireless Mesh Networks”, in IEEE Wireless Communication, Volume 13, Issue 2, pp.50 – 55, April 2006.

[6] Jin-Shyan Lee, Yu-Wei Su, and Chung-ChouShen “A Comparative Study of Wireless Protocols: Bluetooth, UW, ZigBee, and Wi-Fi” in The 33rdAnnual Conference of the IEEE Industrial Electronics Society (IECON) Nov. 5-8, pp. 46-51, (2007).

[7] Lee-Chun Ko and Jin-Shyan Lee“ZigBee Security for Residential Sensor Networks” inSmart Computing Review, vol.1, no.2, pp.95-103, December 2011.

[8] Tulin Mangir, Lelass Sarakbi, Harvy Younan “Detecting Malicious Activities in ZigBee Networks using Cognitive Radio” in International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, pp.51-62, (2011).

[9] Li Quan-Xi, Li Gang “Design of remote automatic meter reading systembased on ZigBee and GPRS” in Third International Symposium on Computer Science and Computational Technology(ISCSCT’10)14-15, pp.186-189,(2010).

[10] Li-Hsing Yen, Yee Wei Law, and Marimuthu Palaniswami ‘’Risk-Aware Distributed Beacon Schedulingfor Tree-Based ZigBee Wireless Networks’’in IEEE Transactions On Mobile Computing, Vol. 11, No. 4, pp. 692-703, April 2012.

[11] Gang Ding, Zafer Sahinoglu, Philip Orlik, , Jinyun Zhang, and Bharat Bhargava‘’Tree-Based Data Broadcast inIEEE 802.15.4 and ZigBee Networks’’in IEEE Transactions On Mobile Computing, Vol. 5, No. 11, pp.1561-1574, November 2006.

[12] Taehong Kim, Daeyoung Kim, Noseong Park, Seong-eun Yoo, Tomás Sánchez López “Shortcut Tree Routing in ZigBee Networks’’ in International Symposium on Wireless Pervasive Computing ISWPC-07, pp.42-47, August 2007.

[13] Helena Fernández-López , José A. Afonso, J.H. Correia , Ricardo Simoes “Towards the design of efficient nonbeacon-enabled ZigBee networks’’ in International Journals of Computer Networks, vol. 23, pp.1-12, April 2012.