International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 2,Mar-Apr 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Analysis of Security in Zigbee Technology

Shivam Pandey

(Electronics and Communication Engineering Department)

(Maturam Institute of Engineering and Management, Rohtak Haryana India)

(Email: pshivamji@gmail.com)

ABSTRACT:

ZigBee networks have become popular for their low cost, low power, and ease of implementation. The ZigBee protocol has particularly become prevalent for home automation and controlling devices such as door locks and garage door openers. Preventing attacks and reducing vulnerabilities is imperative in cases where there can be high financial losses due to poor security implementations. For systems where low power and cost are desirable, but security is a priority, the application developer must be extremely cautious in the design of their network. ZigBee outlines a new suite of protocols targeted at low-rate, low-power devices and sensor nodes. ZigBee Specification includes a number of security provisions and options. The security model specified in the Smart Energy Profile seems bound to become the reference security model for most of ZigBee applications.

INTRODUCTION

ZigBee is an emerging standard for low-power, low-rate wireless communication which aims at interoperability and encompasses a full range of devices even including low end battery-powered sensor nodes. ZigBee is built upon the physical layer and medium access control defined in the IEEE 802.15.4 standard (2003 version). ZigBee Specification includes a number of security provisions and options. In particular, ZigBee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames and controlling devices. ZigBee improves the basic security framework defined in IEEE 802.15.4, focusing also on key establishment and distribution. ZigBee Specification provides two security models, Standard Security Mode and High Security Mode. While the former is designed for lower security residential applications, the latter is intended to be used for high security commercial applications. The security model of the Smart Energy Profile is asserting itself as a reference security model for ZigBee applications, since it constitutes a trade-off between the two standard modes. With the development of wireless network technology, the trend of wireless network to replace the wired network is becoming more and more obvious. Due to the properties of low cost, low power consuming, high robust and flexibility, the ZigBee protocol is getting more and more adopted in the applications of short distance communication, daily monitoring and short distance data transferring.

The security of ZigBee protocol is a crucial problem and has got more and more attention. In this paper, the overall security architecture of ZigBee technology is analyzed, in order to promote the further development of ZigBee security technology. According to the definition of the ZigBee protocol, there are three types of logical devices: the coordinator, routers and terminal equipment. According to the different performance, they can be divided into two types: one is the equipment full function device FFD (Full Function Device) as the main equipment, which undertakes the network coordinator function. If the network enabled security mechanisms, network coordinator and can become Center Trust (TC). Another

device which just has simple functions is called RFD (Reduced Function Device). It cannot be used as the network coordinator, and can just communicate with the network coordinator. Zigbee is one of the most widely used standards for wireless communication between different IoT devices and has been adopted by many major companies, like Samsung and Philips. Zigbee is an open standard for low-power, low-cost wireless personal area networks

that interconnect devices primarily for personal uses. The standard aims to provide a two-way and reliable communication protocol for applications with a short range, typically 10-100 meters. Zigbee is implemented with different application standards used in a variety of application areas, including home automation, smart energy, remote control and health care. Even though Zigbee was designed with the importance of security in mind, there have been tradeoffs made to keep the devices low-cost, low-energy and highly compatible. Some parts of the standard's security controls are poorly implemented, which inevitably lead to security risks. This paper highlights the main security risks and results of attempted attacks on a few IoT devices implemented with Zigbee standard.

Device types and operating modes

- ***Zigbee Coordinator (ZC)***: The most capable device, the coordinator forms the root of the network tree and may bridge to other networks. There is precisely one Zigbee coordinator in each network since it is the device that started the network originally (the Zigbee LightLink specification also allows operation without a Zigbee coordinator, making it more usable for off-the-shelf home products). It stores information about the network, including acting as the trust center and repository for security keys.
- ***Zigbee Router (ZR)***: As well as running an application function, router devices can act as intermediate routers, passing data on to other devices. These types of Zigbee products are typically mains-powered so they are always available on the network. Zigbee Router devices are sometimes called Zigbee repeaters or Zigbee range extenders.
- ***Zigbee End Device (ZED)***: Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. These types of Zigbee device products are often battery-powered. A ZED requires the least amount of memory and thus can be less expensive to manufacture than a ZR or ZC.

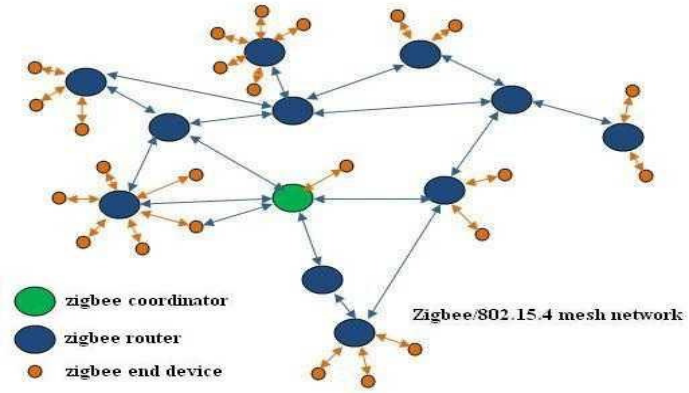

Fig. 1

OVERVIEW

Zigbee is a low-power wireless mesh network standard targeted at battery-powered devices in wireless control and monitoring applications. Zigbee delivers low-latency communication. Zigbee chips are typically integrated with radios and with microcontrollers. Zigbee operates in the industrial, scientific and medical (ISM) Radio bands: 2.4 GHz in most jurisdictions worldwide; though some devices also use 784 MHz in China, 868 MHz in Europe and 915 MHz in the US and Australia, however even those regions and countries still use 2.4 GHz for most commercial Zigbee devices for home use. Data rates vary from 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band). ZigBee is a specification for a suite of high-level communication protocols, intended for devices equipped with small and low-power digital radios based on the IEEE 802.15.4 standard. As reported in ZigBee and IEEE 802.15.4 are standards-based protocols which provide the network infrastructure required for wireless sensor network applications. The IEEE 802.15.4 MAC layer provides reliable communications between a node and its immediate neighbors, addressing collision avoidance and improving efficiency. The MAC layer also assembles and decomposes data packets and frames, while the physical layer provides the interface to the physical transmission medium (e.g., radio).

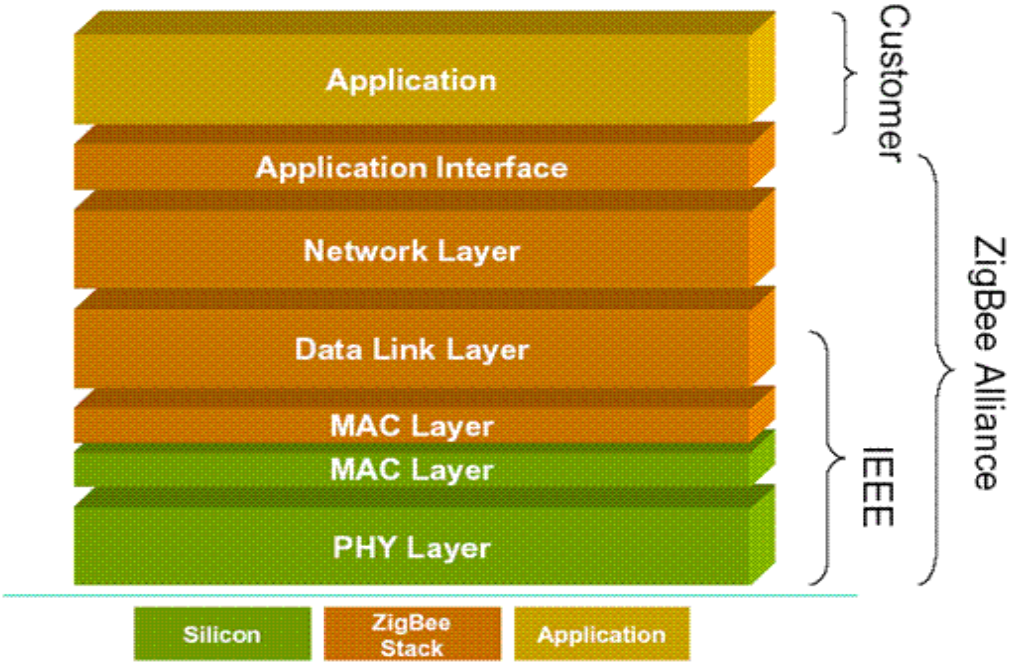

Fig. 2

Security Features

ZigBee technology in the security is specifically expressed in the following features:

1) *ZigBee provides sequential freshness*. Sequential freshness is a security service that uses an ordered sequence of inputs to reject frames that have been replayed. It can prevent the forwarding of attack. ZigBee

devices maintain the input and output freshness counter, when there is a new key is created, the counter will reset.

2) *ZigBee provides frame integrity checking function.* It uses a message integrity code (MIC) to protect data from being modified by parties without the cryptographic key. It further provides assurance that data came from a party with the cryptographic key. This feature prevents an attacker to modify the data. The bit-length of the MIC may take the values 0, 32, 64 or 128.

3) *ZigBee provides entity authentication service*. The entity authentication service provides a secure means for a device to synchronize information with another device while simultaneously providing authenticity based on a shared key. The NWK layer authentication is through the use of a active network key. The APS layer authentication is through using the link key between devices.

4) *ZigBee provides data encryption.* Data encryption is a security service that uses a symmetric cipher to protect data from being read by parties without the cryptographic key. Data may be encrypted using a key shared by a group of devices or using a key shared between two peers.

5) *ZigBee defines the role of 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. All members of the network shall recognize exactly one Trust Center, and there shall be exactly one Trust Center in each secure network. 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:

• Trust Manager, to authenticate devices that request to join the network.

• Network Manager, to maintain and distribute network keys.

• Configuration Manager, to enable end-to-end security between devices

6) *ZigBee adopts CCM* encryption algorithm*. CCM* is a minor modification of CCM. It includes all of the features of CCM and additionally offers encryption-only and integrity only capabilities. These extra capabilities simplify security by eliminating the need for CTR and CBC-MAC modes. Also, unlike other MAC layer security modes which require a different key for every security level, the use of CCM* enables the use of a single key for all CCM* security levels. With the use of CCM* throughout the ZigBee stack, the MAC, NWK, and APS layers can reuse the same key.

ZIGBEE SECURITY ELEMENTS

A. Security services

802.15.4 IEEE standard provides the ZigBee protocol stack MAC layer can provide basic security services and interoperability between devices. Among them, the basic security services include: maintaining an access control list (Control List Access, ACL); the use of symmetric encryption algorithm to protect the transmission of data. The upper layer of the MAC determines whether the MAC layer uses security measures, and provides the key information necessary for the security measures. In addition, the

upper layer is also responsible for the management of key, the identification of the device and the protection of the data, updates, etc. Its main security services are:

Access control - each device controls the access to its own by maintaining an access control table (ACL).

Data encryption - based on 128 bit AES algorithm, the symmetric key method is used to protect the data. In the ZigBee protocol, the net load of the beacon frame, the net load of the command frame and the net load of the data frame should be encrypted.

Data integrity - integrity of the data using the message complete code MIC (Integrity Code Message), you can prevent the illegal modification of information.

Sequential anti replay protection - the use of BSN (beacon serial number) or DSN (data serial number) to reject the replay of the data attacks.

B. Security mode and security components

The MAC layer allows for safe operation of the data, but it is not mandatory for safe transmission, but according to the operational mode of the device and the selected security components, to provide different security services to the device. ZigBee protocol stack provides three security modes: Non secure mode-In the MAC layer, the mode is the default security mode and does not take any security services. Access control (ACL) mode - This mode only provides access control, as a simple filter only allows messages from specific nodes. Safe mode- At the same time using access control and frame load password protection, provides a more perfect security service.

ZigBee Security Background

The ZigBee specification defines security features, such as key establishment, key transport, frame protection, and device authorization. It assumes trust between layers within the ZigBee stack, so cryptographically securing transmission is only done between devices. All services within the network use the same security level once it is decided upon. The specification does not define out-of-band methods for key setup, policy for accepting new devices to the network, policy for expiration and update of keys, or the handling of security errors, loss of counter synchronization, and loss of key synchronization. The coordinator acts as the trust center for the network. As the trust center, it is responsible for managing the security settings and authorizations on the network. It stores the keys for the network, configures other devices with keys, and authorizes devices. All other nodes on the network have full trust with the coordinator to obtain keys and gain access.

There are three different types of keys that can be used: master, link, and network. The master key is used for symmetric-key key establishment (SKKE) to establish link keys. It is either preconfigured or sent in the clear from the trust center. Link keys are shared between two devices on the network, usually between a device and the trust center. It is established dynamically. The network key is shared by all the devices that are on the network. The trust center keeps a set of network keys and the current one is identified by a key sequence number. Network keys are updated by encrypting the new network key with the old network key and broadcasting it to all the network devices. These symmetric keys can be distributed through the

network in three ways, preinstallation, transport, or key establishment. The types of keys used on the network depend on the network topology as well as the security level desired.

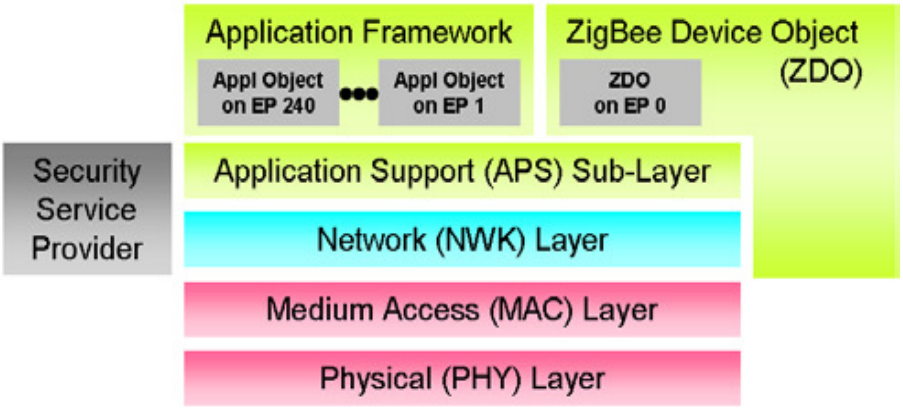

Fig.3

SECURE IMPLEMENTATION OF ZIGBEE

A. *Common safety factor*

ZigBee protocol stack to achieve security, some use a lot of security related features, such as the NWK layer and APS layer are used in the auxiliary frame header, security parameters and the implementation of the policy, etc..

(1) Auxiliary frame header

The auxiliary frame header includes a security control domain, a frame counter domain, a source address field and a key sequence number field. Security domain composed of security level, the key domain identifier, and extend the existing reserved domain. The auxiliary frame counter pillow can provide the frame refresh function, prevent frame retransmission. The security level identifier of the security level sub domain shows which security component is used to protect the output frame and the input frame, and the security component of the security level sub domain.

(2) Security parameter

ZigBee frame protection mechanism using CCM*, AES-128 security operation module. CCM* mode is the expansion of the CCM model, both CCM, but also can be used to separate the CTR and CBC-MAC mode to achieve encryption or authentication. The most important is the CCM* mode for all CCM* security level only using a key, that is, better than CCM* using ZigBee mode, MAC, NWK and APL layer can be reused with the same key. CCM* the current input for the CCM* mode encryption and authentication transfer, but also for the CCM* encryption and authentication transmission.

B. *MAC layer security*

MAC layer is responsible for its own security process, and the upper level should decide which security level to use. In ZigBee network, according to MAC PIB (Personal area network Information Base, a network information database) safety data in the mac Default Security Material and mac ACL Entry Descriptor Set parameters of the two safety process for treatment. The upper (for example: application

layer) and NWK layer should be value from the shared value consensus neighbor device APS LK key mac Default Security Material, set mac ACL Entry Descriptor Set values consistent with the values from the NWK layer of the active network, key counter. The security component should be CCM*, and the security level should be the value of the nwk Security Level identifier in the NIB. For the MAC layer, the LK key should be the first choice, and if you fail to get it, then apply the default key (i.e., the value of the mac Default Security Material ID).

SECURITY CONCERNS AND POSSIBLE SOLUTIONS

In this section we highlight security concerns we have found in the Smart Energy Profile. For each of them we propose a possible approach for a solution.

A. On Supporting Forward Security

In general, a device leaves the network when it has accomplished its mission and thus it is dismissed or when it is momentarily sent to maintenance. Furthermore, a device may be forced to leave the network if it is compromised or suspected to be so. In any case, a device that has left the network must not be able to access any further communication in the network (forward security) or, otherwise, if it ends up into an adversary's hands this could abuse of the keying material still stored in the device. For this reason, the forward security requirement is typically achieved by a proper key revocation and redistribution (rekeying) policy. In this section we argue that the Smart Energy Profile fails to specify a proper rekeying policy so raising security and efficiency concerns. A possible solution consists in revoking the Network Key every time a device leaves and redistributing a new one to all remaining nodes. Rekeying also assures that a device which has left will not be able to perform a secured rejoin, being forced to employ the Key Establishment Cluster procedure to rejoin the network. A possible solution to efficiently and securely managing rekeying could be at the application level so avoiding the security features directly provided by ZigBee. However, as clarified within ZigBee Specification, every application level protocol message requires proper identifiers for the presently considered application profile, cluster and command, each one with its specific payload. Therefore, the introduction of an application level protocol might involve the extension of existing clusters with new commands or, as an alternative, even the definition of a brand-new manufacturer-specific cluster.

B. On Supporting Backward Security

In order to guarantee backward security as well, it would be wise to refresh the current Network Key NK each time a new device i is about to join the ZigBee network. If we exclude the presence of malicious nodes within the network, it is sufficient to broadcast a new Network Key NK+ to all present devices, protecting it via the current Network Key NK. Then every node will start using NK+ as the current Network Key. Once this procedure has been completed, the new device i is allowed to securely join the network and the Trust Center will provide it with the Network Key NK+.

Security Assumptions

Aside from the open trust model between layers, the security of Zigbee ultimately depends on the following assumptions:

1. The safekeeping of symmetric keys. Zigbee assumes that secret keys are not available outside of the device in an unsecured way, meaning that all transmission of keys must be encrypted. An exception to this is during pre-configuration of a new device, in which a single key might be sent unprotected, creating a brief vulnerability. Here, if the keys are stolen because the adversary has physical access to the devices, many information then become available. Zigbee's security policy does not protect against attack to hardware due to its low-cost nature.

2. The protection of mechanism employed. All Router and End Device nodes should support both centralized security and distributed security by adapting to the security scheme employed by the network that they join.

3. The proper implementation of cryptographic mechanism and associated security policies involved. Here, Zigbee developers are assumed to follow the complete protocol in practice. Zigbee also assumes the availability of almost perfect random number generators.

