Security of ZigBee protocol

Brief introduction

ZigBee is kind of wireless technology which is open-source. It is always used to low-powered radio system. ZigBee is based on IEEE 802.15.4 standard. The efficient radius of ZigBee is up to 500 meters. But it is used between 10 - 100 meters in general.

Function

ZigBee system includes three types of devices, each has a specific role as Figure F.1. ZigBee stack layer as Figure F.2.

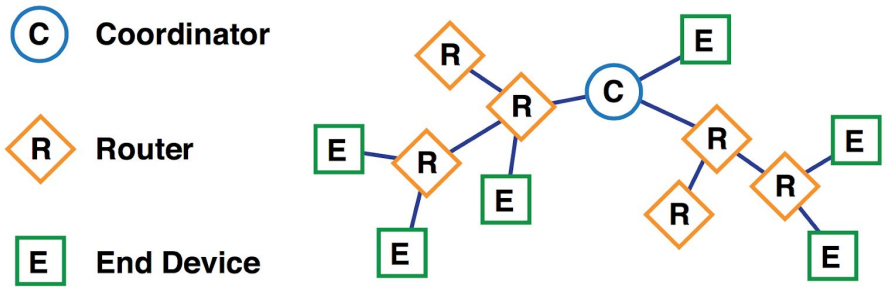


Figure F.1

ZigBee Coordinator: is a device responsible for establishing, executing, and managing the overall ZigBee network. **ZigBee Router:** is an intermediate node device responsible for routing packets between end devices or between an end device and the coordinator. **ZigBee End Device:** is a sensor node device of the Zigbee network, and it is often low-power or battery-power. For example, the distance sensor of autopilot car.

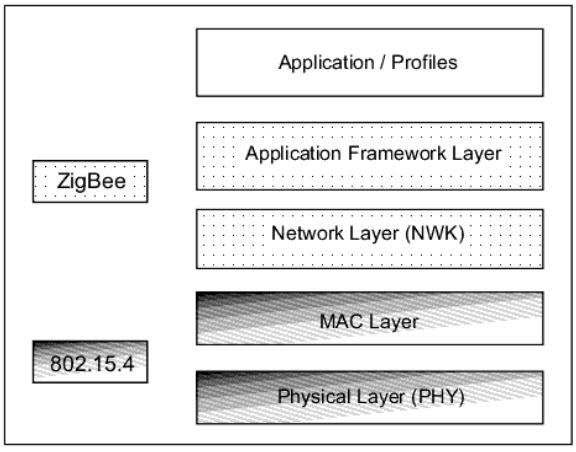


Figure F.2

Security Models

ZigBee provides two different security: Distributed security mode and Centralized security network mode. **Distributed security mode** is a kind of simple and nonsecure mode. This model is used for router and end device. Routers form distributed network and issue network keys which is used to encrypt messages to newly joined routers and end devices. All nodes use same network key and pre-configured (factory installation and only for unique trust center link key) with a link key which is used to encrypt network key before being added in ZigBee network. **Centralized security network mode** is more complex than last one. And it contains the most secure functions of ZigBee. It involves a third party; the trust center (coordinator). The function of trust center includes; Configuring and authenticating routers and end devices that join the network. Generating network key for encrypting communication across the network. Periodically or as required generating a new network key. If an attacker gets a network key, it will be useless after expiring. Establishing a unique Trust Center link key for each device for communicating to Trust Center.

Security Keys

There are three types of symmetric key (128-bit length) used in ZigBee standard. **Network key** is used in broadcast communication and applied by NWK and APL of ZigBee. Every node needs it to communicate with other devices on the network. A device on the network acquires a network key by key-transport (link key encrypted and send) or pre-installation. There are two different types of network keys: standard (sending network key in the open), and high-security (network key is encrypted). **Link key** is used in unicast communication and applied by the APS of the ZigBee stack. A device gets link keys either from key-transport (master key generates it and send), key-establishment (a local method of generating link keys based on the master key), or pre-installation (The manufacturer installs the key into the device itself). **Master key** is the basis for long-term security between two devices and is used only by the APS.

ZigBee Stack Security Measures

IEEE 802.15.4 uses AES (Advanced Encryption Standard) with a 128-bit key length (16 Bytes) for: **Data Confidentiality** which is performed by encrypting the data payload. **Data**

Integrity which is achieved using a Message Integrity Code (MIC)or Message Authentication Code (MAC). It is created by encrypting parts of the IEEE MAC frame using the 128-bit key.

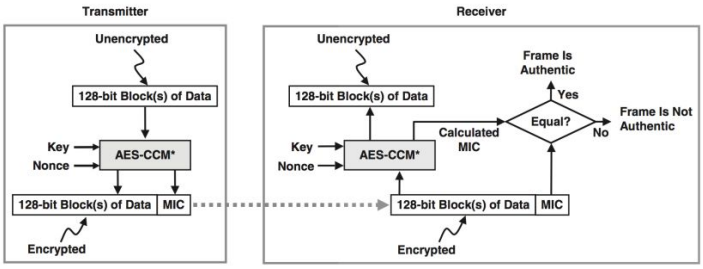
In IEEE 802.15.4 MAC frame, the Auxiliary Security Header has 3 fields and is only enabled if the Security Enabled subfield of the Frame Control Field is turned on. **Security Control** Specifies the type of protection provided by the network. ZigBee defines 8 different security levels available to the NWK and APS Layer as Figure F.3. **Frame Counter** is a counter given by the source of the current frame in order to protect the message from replaying attack. **Key Identifie**r specifies the information needed to know the type of key used by the node for communication.

Security Level Identifier	Security Attributes	Data Encryption	Frame Integrity (length of MIC)
0x00	None	OFF	NO (M = 0)
0x01	MIC-32	OFF	YES (M=4)
0x02	MIC-64	OFF	YES (M=8)
0x03	MIC-128	OFF	YES (M=16)
0x04	ENC	ON	NO (M = 0)
0x05	ENC-MIC-32	ON	YES (M=4)
0x06	ENC-MIC-64	ON	YES (M=8)
0x07	ENC-MIC-128	ON	YES (M=16)

Figure F.3

Encryption/decryption: ZigBee frames can be optionally protected with the security suite AES-CCM* to provide data confidentiality, data authentication and data integrity. AES-CCM* is a modified method of AES (Advanced Encryption Standard) with a modified CCM mode (Counter with CBC-MAC). As Figure F.4.

Figure F.4



Reference

[1] "ZigBee Security: Basics (Part 1)." The Latest News from Research at Kudelski Security. January 23, 2018. Accessed May 27, 2019. https://research.kudelskisecurity.com/2017/11/01/zigbee-security-basics-part-1/.

[2] "About ZigBee Protocol - XBEE Tutorial." Google Sites. Accessed May 27, 2019. https://sites.google.com/site/xbeetutorial/xbee-introduction/zigbee.

[3] 15.4-2011 – IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) <http://standards.ieee.org/findstds/standard/802.15.4-2011.html>