Payatu

IoT Security – Part 6 (ZigBee Security - 101)

Dattatray

11-June-2020

ZigBee Security 101

This blog is part of the "IoT Security" Series. If you haven't read the previous blogs (parts 1 - 5) in the series, I urge you to go through them first unless you are already familiar with those concepts and want to only read about the current topic.

IoT Security – Part 1 (101 – IoT Introduction And Architecture)

IoT Security – Part 5 (ZigBee Protocol - 101)

In this blog, we will discuss the security architecture of ZigBee protocol and security issues present in ZigBee devices and networks.

ZigBee Security Architecture (Open Trust)

The security architecture in ZigBee complements or enhances the security service of the IEEE 802.15.4 layers. It is an "open trust" model based on certain assumptions which are described below:

- Different layers and applications are running on a single device trust each other.
- The communication between different stack layers on the same device is not encrypted.
- A device will not intentionally or inadvertently transmit keys to other devices unless protected, such as during key-transport.
- The communication between the two devices is cryptographically encrypted and secured.
- Random number generators are working as expected by the cryptographic engine
- Hardware is tamper-resistant

ZigBee security architectural design principle:

- The layer that originates a frame is responsible for initially securing it.
- Only a device with an active network key can communicate to more than one hop across the network.
- Both the APS layer and NWK layer can use the same active network key to secure the frames. Re-use of keys helps reduces storage overhead.
- End to End message security, i.e., the only source and destination devices, can decrypt the messages protected by a shared key, and the routing mechanism is out of trust considerations.
- A device that forms a network is responsible for base security level, security policies, and authentication of nodes in the network. The application layer can provide additional application level security if required between two devices.

Trust Center

The Trust Center is an application that runs on a device trusted by other devices within a ZigBee network to distribute keys for network and potentially end-to-end application configuration management. Only one trust center can exist per network, and it can be a coordinator or a device designated by the coordinator, and all member nodes recognize this device as a trust center. Trust center is responsible for * Configuring and maintaining network security policies * Establishing end-to-end application keys. * Generation of keys by using some key establishment protocol

Security Modes in ZigBee

- ### Distributed Security Mode

  The distributed Security Mode, unique Trust Center, is not required in the network, and routers are responsible for end device authentication. The link key is pre-configured on the device, and the network key is issued by a router when the device joins the network. Network key remains the same for all nodes in the network; this makes distributed security mode less secure.

- Centralized Security Mode

  The centralized security mode used in applications, a trust center control, and maintain centralized security policy for network and device. In this mode, the trust center is responsible for

- Maintaining security and security configuration for the entire network
- Authentication of devices and maintaining a list of devices on the network
- Maintaining Link keys and Network keys with all the devices in the network

ZigBee Security Keys

ZigBee standard defines two types of symmetric keys, each of 128-bit length used for encrypted communication.

- Network Key

  128-bit Network key used in broadcast communication and any network layer communications. Each node requires the network key to communicate securely with other devices on the network. A device on the network acquires a network key via key transfer on the network, i.e., key-transport. There is only one type of network key; however, it can use in either distributed or centralized security models. The security model controls how a network key is distributed and may control how network frame counters initialized. The security model does not affect how messages are secured.

- Link Key

  A 128-bit unique Link key shared by two devices, used in unicast communication between APL peer entities. A device can get link keys either via key-transport service over the network, or pre-installation There are two different types of trust center link keys: global and unique. The type of trust center link key in use by the local device determines how the device handles various trust center messages (APS commands), including whether to apply APS encryption or not. Each node may also have the following pre-configured link keys, which would use to derive a Trust Center link key.

Sr. No.	Key Name	Description
1	Centralized security global trust center link key	Link key used for joining centralized security networks. The default value for the centralized security global trust center link key is ZigBeeAlliance09, i.e. (“5A 69 67 42 99 23 65 65 41 6C 6C 69 61 6E 63 65 30 39”) and is used or supported by the device if no other link key is specified by the application at the time of joining
2	Distributed security global link key	Link key used for joining distributed security networks
3	Install code link key	Link key derived from install code from joining device to create unique trust center link key for joining

Sr. No.	Key Name	Description
4	Application link key	Link key used between two devices for application layer encryption
5	Device Specific trust center link key	Link key used between the trust center and a device in the network. Used for trust center commands and application layer encryption.

Key Management

ZigBee specification mentions three different key management mechanisms

- Pre-installation – Keys are configured or install on devices out-of-band
- Key Transport – The Trust center sends security keys over the network to the device.
- Key Establishment – Trust center and end device negotiate on keys, and keys are established without ever actually sending any key over the network. This key establishment is based on the Symmetric-Key Key Establishment (SKKE) protocol.

ZigBee Protocol Security

Auxiliary Security Header

ZigBee NWK layer and APS layer can use the Auxiliary Security Header for secure communication if security control bit in the NWK frame control field set to 1. Auxiliary Security Header has the following fields

Octets: 1	Octets: 4	Octets: 0 or 8	Octets: 0 or 1
Security Control	Frame Counter	Source Address	Key Sequence Number

Below is sample snapshot of ZigBee packet with security field in NWK frame control set to true (1) and Security header is set with corresponding security control fields, and Message Integrity Code (MIC)

```
> Frame 3383: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface 0
> IEEE 802.15.4 Data, Dst: Broadcast, Src: 0x0000
v ZigBee Network Layer Command, Dst: Broadcast, Src: 0x0000
  v Frame Control Field: 0x1209, Frame Type: Command, Discover Route: Suppress, Security, Extended Source Command
      .... .... .... ..01 = Frame Type: Command (0x1)
      .... .... ..00 10.. = Protocol Version: 2
      .... .... 00.. .... = Discover Route: Suppress (0x0)
      .... ...0 .... .... = Multicast: False
      .... ..1. .... .... = Security: True
      .... .0.. .... .... = Source Route: False
      .... 0... .... .... = Destination: False
      ...1 .... .... .... = Extended Source: True
      ..0. .... .... .... = End Device Initiator: False
    Destination: 0xfffc
    Source: 0x0000
    Radius: 1
    Sequence Number: 23
    Extended Source: 0b:01:0e:09:ec:77:bf:ec (0b:01:0e:09:ec:77:bf:ec)
  v ZigBee Security Header
    v Security Control Field: 0x28, Key Id: Network Key, Extended Nonce
        ...0 1... = Key Id: Network Key (0x1)
        ..1. .... = Extended Nonce: True
      Frame Counter: 22552
      Extended Source: 0b:01:0e:09:ec:77:bf:ec (0b:01:0e:09:ec:77:bf:ec)
      Key Sequence Number: 0
      Message Integrity Code: 43cce9d6
    > [Expert Info (Warning/Undecoded): Encrypted Payload]
  > Data (2 bytes)
```

Security control

8 Bit security control field consists of a security level, a key identifier, and an extended nonce sub-field as shown below

Bit	0 - 2	3 - 4	5	6 - 7
Description	Security Level	Key Identifier	Extended nonce	Reserved

- Security Level

The security level identifier indicates how an outgoing frame is to be secured, how an incoming frame purportedly has been secured. It also indicates whether or not the payload is encrypted and to what extent data authenticity over the frame provided, as reflected by the length of the message integrity code (MIC). The bit-length of the MIC may take the values 0, 32, 64, or 128 and determines the probability that a random guess of the MIC would be correct. The security properties of the security levels listed in below

Security Level Identifier	Security Attributes	Data Encryption	Frame Integrity (length M of MIC, in Number of Octets)
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)

- Key Identifier

The key identifier sub-field consists of two bits used to identify the key used to encrypt the frame.

Key Identifier	Description
0x00	A data key
0x01	A network key
0x02	A key-transport key
0x03	A Key-load key

- Extended nonce

When set to 1, the extended nonce sub-field indicates the sender address field is present in the auxiliary header. Otherwise, it set to 0.

Frame counter

The counter field used to provide frame freshness and to prevent the processing of duplicate frames.

Source address

The source address field in security control is the extended 64-bit address of the source device and present when the extended nonce sub-filed of the security control field set to 1.

Key sequence number

The key sequence number present in the auxiliary security header indicates the key sequence number of the network key used to secure the frame. The key identifier subfield from the security control field, when set to 1 (i.e., a network key), indicates a key sequence number present in the auxiliary security header.

ZigBee Vulnerabilities

> **Security between devices depends on secure initialization and installation of security keys**

Vulnerabilities in the ZigBee network categorized into two categories as protocol vulnerabilities and poor implementation of protocol during product development. Below are some common vulnerabilities:

Implementation vulnerabilities

Security keys stored insecurely

ZigBee protocol expects all security keys (network, Link) stored secularly on the device. Keys can identify by reverse-engineering the firmware binary to find the location of the keys if they are not stored securely.

Over-The-Air insecure key transportation

In some implementations, when a node joins a ZigBee network for the first time, the node obtains its keys over-the-air, mostly in a clear-text format from the coordinator. Thus a sniffer device network sniper or rough device can obtain keys from the coordinator and can compromise the entire network.

Energy Depletion Attack

Below are two very common energy depletion attacks

- Invalid security header

  In such attacks, an attacker sends bursts of packets with invalid security headers in frame with the intention that the device has to spend some amount of energy to verify frame integrity, leading to faster battery depletion of the target device.

- Polling Rate

  In such attacks, attackers send packets to the end device faster than the configured polling rate of the network, leading to faster battery depletion of the target device.

Protocol vulnerabilities

Network Jamming Vulnerability

IEEE802.15.4/ZigBee standards provide certain protection mechanism against radio and network interference, but there are certain techniques by which an attacker can jam the network

Below are two types of jamming attacks possible in the ZigBee network:

- Radio Jamming

  In such attacks, the attacker increases the radio signal's emission for a given channel, leading to a decrease in Signal to Noise Ratio of the radio channel.

- Link Layer Jamming

  In such attacks, the attacker targets the MAC layer by transmitting bursts of random ZigBee frames with useless data on the network either at the random interval or specific interval targeting specific node and thus leading to packet drop and DoS attack in the network.

Link key vulnerability

ZigBee standard has an open-trust model for security and below vulnerabilities in standard leads to Link key related attack

- Default Link Key

ZigBee standard provides a default value for link key to ensure interoperability between ZigBee devices from different manufacturers; thus, an attacker can use a rogue device to join the network with the default network key.

- Unencrypted Link-Key

  When a device without pre-configured key tries to join the network, in such cases trust center sends a single key (default link key) unencrypted to the device and can be obtained by an attacker by sniffing the network communication leading to ZigBee network compromise.

- Re-using Link key

  ZigBee standard permits the re-use of link keys for rejoining the network; in such cases, an attacker can clone the legitimate device and spoof the network layer of Trust Center by pretending to be previously connected device that wants to rejoin the network. Thus Trust Center then sends the keys encrypted with the previously used link key.

Unauthenticated ACK frame vulnerability

Acknowledgment frame is a part of network layer in IEEE 802.15.4/ZigBee standards but limited to confirmation of frame transmission at the network layer and does not provide frame integrity and confidentiality protections for acknowledgment packets. Below are some common ACK attacks in the ZigBee network. Both required Link Layer jamming.

- ACK Spoofing

  In such attacks, attackers jam the network such that the legitimate device does not receive frames, and then the attacker sends the ACK frame with the correct sequence number to the sender, leading to data loss in the network.

- ACK Dropping

  In such attacks, attacker jams the network such that only ACK frame from receiver to the sender jammed, forcing the sender to retransmit data till the maximum number of retransmissions, depletes the network bandwidth and device battery power.

Replay-protection vulnerability

An IEEE 802.15.4 has replay-protection mechanisms. It mentions that a node can drop the received frame if the frame sequence number is equal to or less than the sequence number of the preceding frame received from the same source node. In such attacks, an attacker can send frames with large sequence numbers to the target node, forcing the target node to drop the frame with a smaller sequence number.

Conclusion

We hope this blog gives you a brief insight into the security architecture of ZigBee protocol. The vulnerabilities covered in this blog are either due to a lack of secure design and implementation or due to inherent vulnerabilities of ZigBee protocol.

Continue to the next part - IoT Security - Part 7 (Reverse Engineering An IoT Firmware)

Reference

- **802.15.4-2020 - IEEE Approved Draft Standard for Low-Rate Wireless Networks**
- **ZigBee specification - 05-3474-21, August 5, 2015**
- **The ZigBee Alliance**
- **IEEE 802.15.4 Wikipedia**
- **ZigBee Wikipedia**