ZigBee Security

By Naveen PS

MAKERDEMY
LEARN EXPLORE MAKE

ZigBee Security

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 policy 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.

THE END