ZigBee Security

Robert Cragie
Chair, ZigBee Alliance ZARC Security Task Group
Principal Engineer, Jennic Ltd.
Security in the ZigBee stack
The specification assumes an 'open trust' model where the protocol stack layers trust each other

- This is not unreasonable for the type of devices ZigBee is aimed at, e.g. single-chip wireless microcontrollers executing the whole stack on a single CPU

This implies that cryptographic protection only occurs between devices

The same security suite level is used for all services
Security services provided

The ZigBee Security Services provided in the specification are:
- Key establishment
- Key transport
- Frame protection
- Device authorization
To function securely in a network, a device must have a counterpart device which it can trust to obtain keys and which controls access.

ZigBee therefore introduces the concept of the Trust Center, which:

- Stores the keys for the network
- Uses the security services to configure a device with its key(s)
- Uses the security services to authorize a device onto the network

The ZigBee Coordinator is usually designated the Trust Center.
ZigBee security is based on symmetric keys

Both originator and recipient of a protected transaction need to share the same key

That key is used directly in the security transformation

How does this key get to both ends?

Three basic methods

- Pre-installation
- Transport
- Establishment
Distribution methods

- Pre-installation is where keys are placed into device using out-of-band method, e.g. commissioning tool
- Transport is where the Trust Center sends the key (securely wherever possible) to the device
- Establishment is where the device negotiates with the Trust Center and keys are established at either end without being transported
  - SKKE (Symmetric Key Key Establishment)
  - CBKE (Certificate-based Key Establishment)
  - ASKE (Alpha-secure Key Establishment)
There are three key types:
- Master key
  - Shared key for SKKE only
- Link key
- Network key
Key which is uniquely shared between two and only two devices for protecting frames at the APS layer

One of those devices is normally the Trust Center

Usually dynamically established using key establishment service

Can also be pre-installed or transported from the Trust Center
Global key which is used by all devices in the network

A set of network keys is held by the Trust Center and current network key is identified by a key sequence number

Usually transported from the Trust Center

Can also be pre-installed

Two stage update mechanism
  – Update new key and associated key sequence number
  – Switch to new key sequence number
Some confusion due to flexibility in specification

A *common security model* was developed

Use of network key with pre-configured Trust Center link keys

Pre-configured TC link key protects the transport of the network key

Additional link keys can be transported or established using higher-layer mechanism
  - Secure communication cluster in SE/HC profile
The security suite used is AES-CCM*

The security level used in ZigBee (level 5) means AES_CCM* is the same as AES-CCM

AES-CCM is NIST special publication 800-38C

Low-cost implementation in terms of resources

Some wireless microcontrollers have hardware support for AES-CCM or AES-CCM*

Two parts to protection
  – Encryption
  – Integrity protection

ZigBee security uses level 5 in the AES-CCM* suite
  – Encrypted
  – MIC length 4 octets
Encryption and Integrity protection

- Encryption scrambles the original data (called plaintext in 'security speak') into ciphertext.
- Encryption prevents an eavesdropper from being able to interpret frame payload.
- Integrity protection adds a Message Integrity Code (MIC) to be transported along with the data to be protected.
- The MIC 'signs' the data and allows the recipient to verify that the data has not been tampered with.
- The MIC is also bound to the identity (IEEE address) of the originator and thus provides origin authenticity.
- Without integrity protection, a rogue device could modify a transmitted frame and the modification may not be detected by the recipient.
Protecting at NWK layer

- **Sync**
- **PHY HDR**
- **MAC HDR**
- **Plaintext MAC Payload**
- **FCS**

- **Unsecured NWK PDU**
- **NWK HDR**
- **Plaintext NWK Payload**

- **Secured NWK PDU**
- **NWK HDR**
- **Auxiliary Header**
- **Ciphertext NWK Payload**
- **MIC**
Protecting at APS Layer

- **PHY PDU**
  - SYNC
  - PHY HDR
  - MAC HDR
  - Plaintext MAC Payload
  - FCS

  **Unsecured NWK PDU**
  - NWK HDR
  - Plaintext NWK Payload

  **Unsecured APS PDU**
  - APS HDR
  - Plaintext APS Payload

- **PHY PDU**
  - SYNC
  - PHY HDR
  - MAC HDR
  - Plaintext MAC Payload
  - FCS

  **Unsecured NWK PDU**
  - NWK HDR
  - Plaintext NWK Payload

  **Secured APS PDU**
  - APS HDR
  - Auxiliary Header
  - Ciphertext APS Payload
  - MIC
Protecting at NWK and APS layer

PHY PDU

SYNC | PHY HDR | MAC HDR | Plaintext MAC Payload | FCS

Unsecured NWK PDU

SYNC | PHY HDR | MAC HDR | Plaintext NWK Payload

Unsecured APS PDU

SYNC | PHY HDR | MAC HDR | Plaintext APS Payload

PHY PDU

SYNC | PHY HDR | MAC HDR | Plaintext MAC Payload | FCS

Secured NWK PDU

SYNC | PHY HDR | MAC HDR | Ciphertext NWK Payload | MIC

Secured APS PDU

SYNC | PHY HDR | MAC HDR | Ciphertext APS Payload | MIC
Joining scenario

- ZigBee Coordinator normally acts as Trust Center
- Walk through device without network key and with pre-configured TC link key
  - Common security model

Coordinator
Router
End Device
Mesh link
End device star link
Joining scenario walkthrough

1: Device does unsecured join

2: Router sends device update to TC for authorization

3: TC prepares network key transport for joining device secured with pre-configured TC link key shared between TC and joining device and tunnels it to router

4: Router unpacks tunneled network key transport and sends to device unsecured at network layer

5: Device retrieves network key from network key transport using pre-configured TC link key
ZigBee SE 2.0 security requirements

- SE 2.0 requires a more flexible security implementation
- Both federated and end-to-end models need to be considered
- Existing standards from IETF, IEEE, IEC etc. need to be used
- Multiple sources for implementation and multiple CAs required
ZigBee SE 2.0 security initial technical requirements

- Link layer security provided by 802.15.4-2006 frame protection
- EAP (Extensible Authentication Protocol) used for network admission
  - Certificates
  - Passphrases
  - PINs
- TLS (Transport Layer Security) used for secure associations at application level
  - Locally within HAN
  - Across the wider network to utility
- TRD available on ZigBee/Homeplug document server