Payatu

IoT Security – Part 5 (ZigBee Protocol - 101)

Dattatray

11-June-2020

ZigBee Protocol 101

This blog is part of the "IoT Security" Series. If you haven't read the previous blogs (part 1- 4) 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 4 (bluetooth low energy-101)

In this blog, we are going to discuss ZigBee specification and ZigBee protocol architecture in detail. The next blog will cover the security architecture of ZigBee protocol and security issues present in ZigBee devices and networks.

History

ZigBee – developed as an ad-hoc digital radio network during the 1990s and alternate to the wired network. Unlike Wi-Fi or Bluetooth, ZigBee is more suitable for applications in industrial automation and control systems (IACS) where end nodes are required to transmit a low amount of data periodically and be low on power consumption and have a short distance of transmission from a centralized monitoring system. Nowadays, ZigBee Low-Rate, Wireless Personal Area Network (LR-WPAN) widely used in control and monitoring applications that require a low data rate, long battery life, self-healing, and secure network in noisy RF environments. Below are some industries that use ZigBee standard for networking solution in their products

- Wireless sensor networks(WSNs)
- Industrial Automation
- Building Automation
- Home Automation
- Smart Energy metering
- Hospitals and Health Care Automation

ZigBee Overview

In 2000 IEEE 802.15 working group was formed to work on or standard for wireless personal area networks (WPAN) characterized by a short-range, high level of simplicity, allowing for low cost and low power implementations. The First edition of IEEE 802.15.4 standards was released in 2003, i.e., IEEE 802.15.4-2003 (LR-WPAN), and defined the physical layer and data-link layer of the OSI model. In 2002 ZigBee Alliance was established and working together with IEEE 802.15.4 working group, announced ZigBee v.1.0 draft ratified ZigBee 2004 Specification in December 2004. ZigBee standard is built on top of IEEE 802.15.4-standards, where IEEE 802.15.4 defines first two layers, i.e., Physical (PHY) layer, Medium access control (MAC) layer for low-rate wireless personal area network (LR-WPAN), and ZigBee standard provides Network layer (NWK), Application layer (APL) and security features – as shown in the figure below

Following sections will illustrate the different components of ZigBee standard in more details

IEEE 802.15.4 Protocol

PHY Layer

IEEE 802.15.4 PHY layer provides modulation-demodulation of data, transmission, and reception management services and operates in two separate frequency ranges, low frequency $^{868}/_{915}$ MHz and high frequency 2.4 GHz. PHY layer is responsible for Radio controls (enable/disable), Link Quality Indication of received packets (LQI), Energy Detection (ED), and Clear Channel Assessment (CCA)

PHY	Frequency	Channels	Regions
Low Frequency PHY	868.0-868.6 MHz	1	Europe
Low Frequency PHY	902-928 MHz	30	United States and Australia
High Frequency PHY	2400-2483.5 MHZ	16	Worldwide

MAC Layer

IEEE 802.15.4 MAC layer controls access to the radio channel using a CSMA-CA mechanism. MAC layer is responsible for Beacon transmission (when the device is a coordinator), implementation of carrier sense multiple access with collision avoidance (CSMA-CA), synchronization using a guaranteed time slot (GTS) mechanism, provide a reliable transmission mechanism for upper layers.

IEEE 802.15.4 Network Model

Node Type

IEEE 802.15.4 standard defines two types of the network node

- Full-Function Device (FFD)

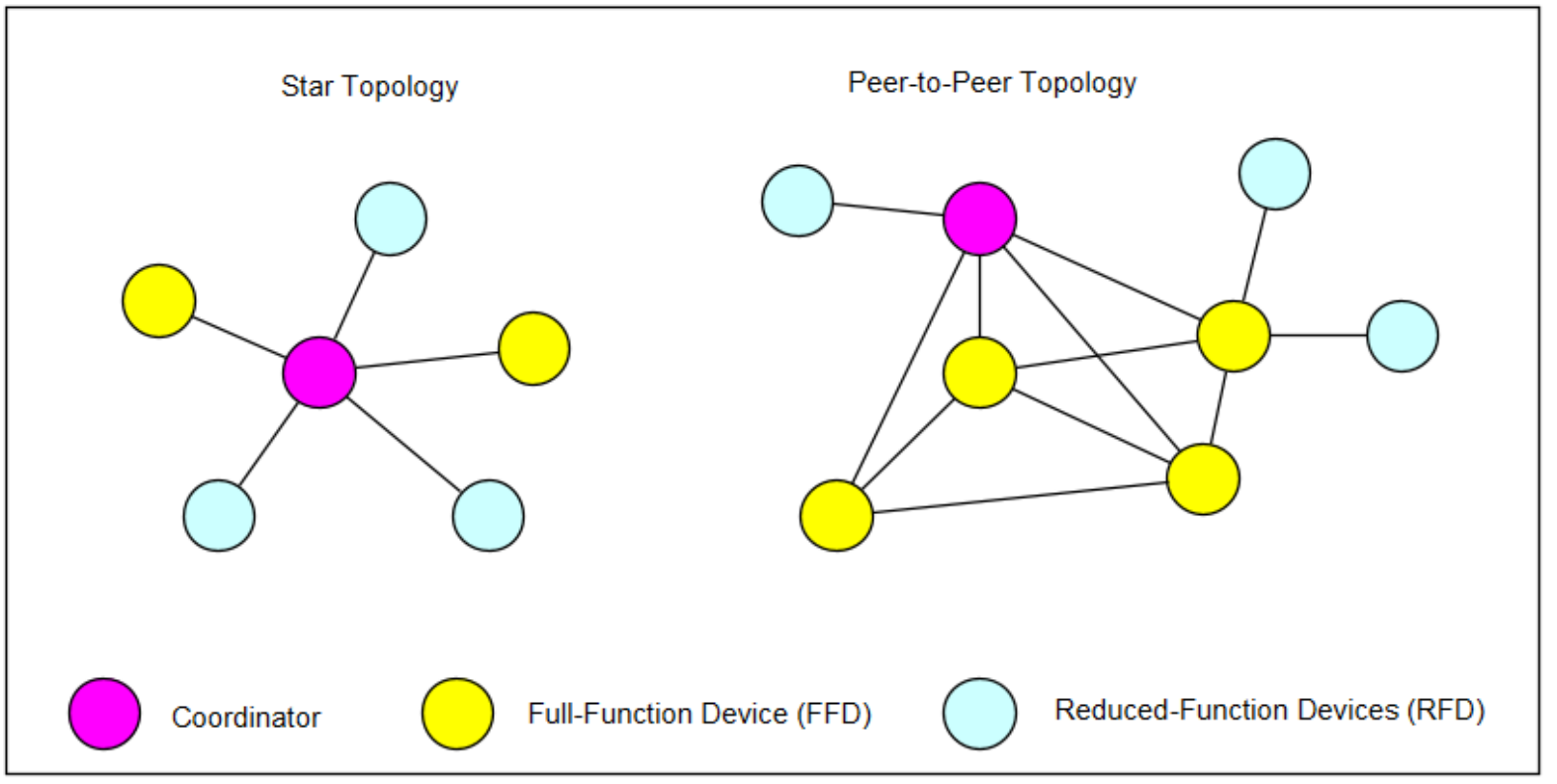
  FFD device is capable of network creation, configuration, and message routing within the PAN network. FFD device is capable of configuring the security model in the PAN network. FFD devices can operate in three operating modes, namely: PAN Coordinator, a Coordinator, and End Device. An FFD device can communicate with any RFD or FFD device in the network.

- Reduced-Function Devices (RFD)

  RFD is often a battery-operated, simple device with very modest resource and communication requirements. RFD devices can only act as an End Device in the PAN network due to a lack of routing capability and can only communicate with FFD devices in the network.

Topologies

IEEE 802.15.4 standard defines two network topologies star or peer-to-peer for LR-WPAN devices. However, every network needs at least one FFD to work as the coordinator of the network.



- Star

  The star network is a more structured network with at least one FFD device in the network act as a coordinator for the entire network. Any FFD device chooses its unique PAN identifier to create its own PAN and declares itself as a PAN coordinator. Once the PAN coordinator becomes active in the network, other end devices can join the network. The end device can only communicate to the central node or coordinator. It mostly used in Home-Automation, personal health monitoring, toys, and game control.

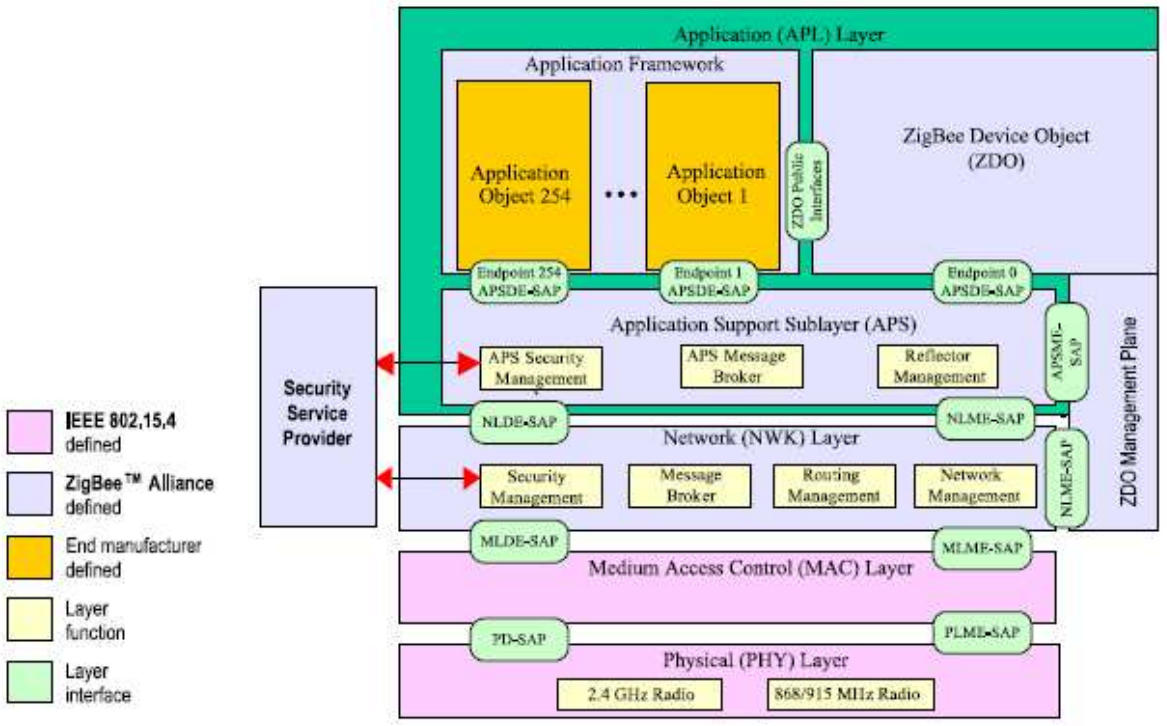
- Peer–to–Peer

  The Peer-to-Peer networks also need one PAN coordinator, but unlike a star network, any device can communicate with any other device within the network range. A peer-to-peer network can be an ad-hoc network capable of self-organization and self-management. It mostly used in industrial control and monitoring systems, wireless sensor networks, inventory management systems.

Node Addressing Modes

Each IEEE 802.15.4 has two addressing modes, short (16-bit), and extended (64-bit) addressing. An IEEE 802.15.4 compliant device gets its 64-bit extended address from the manufacture while a unique 16-bit PAN address assigned by the coordinator when the device associates with a WPAN.

ZigBee protocol



Source: ZigBee Specification Document 05-3474-21 (docs-05-3474-21-0csg-zigbee-specification)

Application Layer

As shown in figure above, the APL layer consists of several sublayers, namely: APS sublayer, service access points (SAP), and the ZigBee Device Object (ZDO) along with ZDO management plane, and the manufacturer defined application objects.

Application Support Sub-Layer (APS)

The APS sub-layer provides an interface between the NWK and APL through a general set of services that are used by both the ZDO and the manufacturer-defined application objects. The APS Data Entity (APS-DE) and APS Management Entity (APS-ME) are two APS entities and provide the below services:

- APS data entity (APS-DE)
- Generation of the Application support sub-layer protocol data unit (APDU)
- Device Binding
- Group address filtering
- Reliable transport
- Duplicate rejection
- Fragmentation

- APS management entity (APM-SE)
- Binding management
- Application Support Layer Information Base (AIB) management
- Security
- Group management

Application Framework

Application Framework provides an execution environment in which application objects are hosted and can send or receive data, up to 254 distinct application objects can be defined, each identified by an endpoint address from 1 to 254. Endpoint 0 and Endpoint 255 are used as ZigBee Device Object (ZDO) address and broadcast address respectively by Application support sub-layer data entity - service access point (APSDE-SAP) Endpoints 241 through 254 reserved by ZigBee Alliance and cannot be used without approval.

- Application Profiles

  Application profiles are agreements for messages, message formats, and processing actions that enable developers to create an interoperable, distributed application employing application entities that reside on separate devices. ZigBee Alliance has published number of public application profiles for applications like Home Automation, Industrial Automation, etc. Device manufactures can also define custom profiles suitable for their end application.

- Clusters

  Clusters are represented as the collection of attributes and application messages. Clusters are divided into two types, i.e., input and output clusters. A cluster identifier is a 16-bit number unique within the scope of a particular application profile.

ZigBee Device Objects (ZDO)

Located between the application framework and APS, the ZigBee device objects (ZDO) represent a base class of functionality that provides an interface between the application objects, the device profile, and the APS. The ZDO is responsible for the following:

- Initializing the application support sub-layer (APS), the network layer (NWK), and the Security Services.
- Assembling configuration information from the end applications to determine and implement discovery, security management (key loading, key establishment, key transport, and authentication), network management (network discovery, leaving/joining a network, resetting a network connection and creating a network), and binding, node, and group management.

Network Layer

The network layer provides a service interface between the 802.15.4 MAC layer and the application layer. The Network Layer Data Entity (NLDE) and Network Layer Management Entity (NLME) are two network layer entities provides below services:

- Network Layer Data Entity (NLDE)
- Generation of the Network level PDU (NPDU)
- Topology-specific routing
- Security

- Network Layer Management Entity (NLME)
- Configuring a new device
- Starting a network
- Joining, rejoining and leaving a network
- Addressing:
- Neighbor discovery
- Route discovery
- Reception control
- Routing

ZigBee Device Type

A ZigBee device can work in three different modes or node types.

- ZigBee Coordinator (ZC)

  A ZigBee coordinator is a FFD device that acts as a central node or parent for other nodes in the network. Only one per network is responsible for the creation, configuration, and management of the ZigBee network. It maintains a list of associated devices, support services like association, disassociation, and orphan scan, rejoin. ZigBee network cannot exist without a ZC; ZC is always active on the network and cannot be put in sleep mode.

- ZigBee Router (ZR)

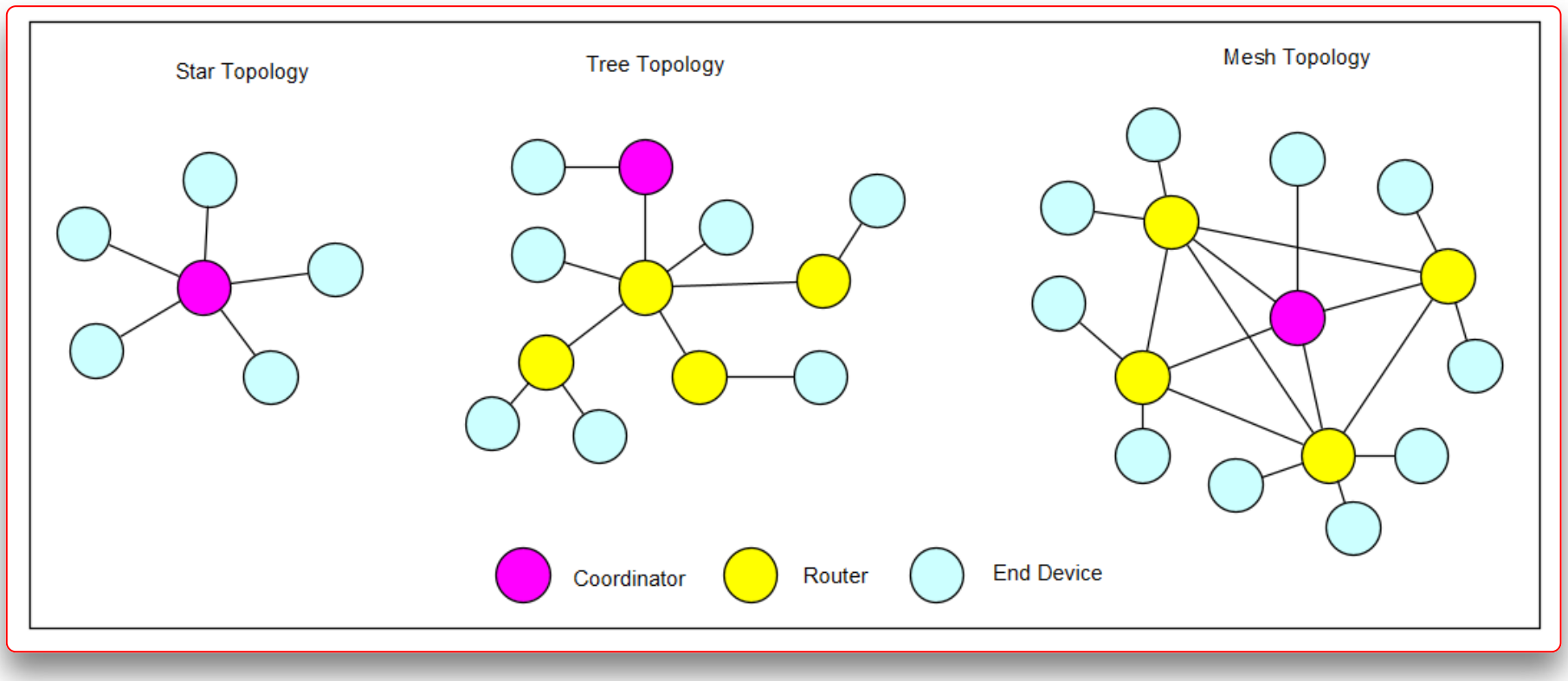
  The ZigBee Router is an intermediate FFD device, responsible for relaying packets between end devices or between an end device and the coordinator. End Device can also join the network through a router, with the ZR acting as a parent for that segment of the network.

- ZigBee End Device (ZED)

Any FFD or RFD device can become End device on ZigBee network, ZigBee End device is a simple device like a sensor responsible for monitoring and collecting data, or take particular action based commands from the user. ZED without any message routing capability can only send and receive data from the parent node. Usually, ZED is are low powered battery operated device and can be put to sleep to save power consumption.

Network Topology

The ZigBee network layer (NWK) supports star, tree, and mesh topologies.



- Star

  A Single ZigBee coordinator device per network, controlling the network, and is responsible for initiating and maintaining the ZigBee network. All other devices, called as end devices, directly communicate with the ZigBee coordinator or other end devices via ZigBee coordinator. In the Star network, the coordinator becomes a bottleneck for message routing, and failure of coordinator leads to network shutdown.

- Tree

  In tree topologies, the ZigBee coordinator is responsible for starting the network and for choosing specific key network parameters, but the network may extend by ZigBee routers. In tree networks, routers route data and control messages through the network using a tree routing strategy. In Tree network, failure of a router can lead to a shutdown of the network segment under the affected router.

- Mesh

  In a mesh topology, the ZigBee coordinator is responsible for creation and configuration, but the network may extend using ZigBee routers. Mesh networks allow full peer-to-peer communication. Mesh network, also called a self-healing network, i.e., failure of coordinator does not result in network failure as end devices communicate with each other and to the router.
  Mesh network is complex and creates a messaging overhead in the network.

Addressing in ZigBee

Device Addressing

Each ZigBee device in a ZigBee network gets two types of addresses - an IEEE address and a Network Address.

- IEEE Address

  A globally unique 64-bit address and assigned by device manufacture during production. Part of IEEE 802.15.4 standard, this address is also referred to as “extended address” used by IEEE 802.15.4 layer for low-level packet delivery and rarely used by the ZigBee layer except for the binding map need to create a binding between IEEE address and Network Address.

- Network Address

  A unique within a ZigBee network, 16-bit Network address is part of the ZigBee layer, also called the “short address”. Network Address is assigned to the end device and used by the network layer for routing messages between devices.

ZigBee Network Identity

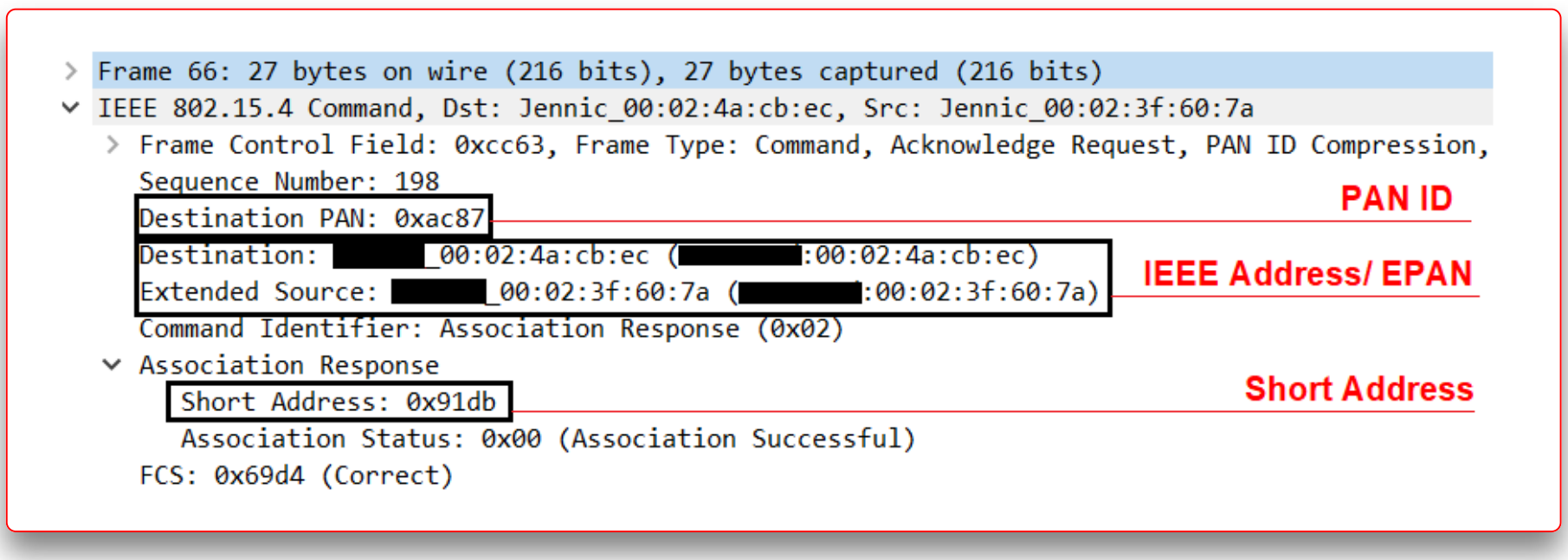
Each ZigBee device in a ZigBee network gets two types of identifiers (ID) - the Personal Area Network Identifier (PAN ID) and the Extended PAN ID (EPID).

- PAN Identifier (PAN ID)

  Part of the IEEE 802.15.4 standard, the PAN identifier (PAN ID) is a 16-bit identifier selected by the PAN Coordinator while setting up the network and communicated to the End devices. MAC layer filter out packets from other networks which are not part of the same network as identified by the specific PANID.

- Extended PAN ID (EPID)

  A globally unique 64-bit identifier of the ZigBee network, EPID identifier should be unique among the PAN overlapping in a given area and is used to avoid PAN ID conflicts between distinct networks. Refer below snapshot of ZigBee packet for more understating of PAN ID, EPAN and short address



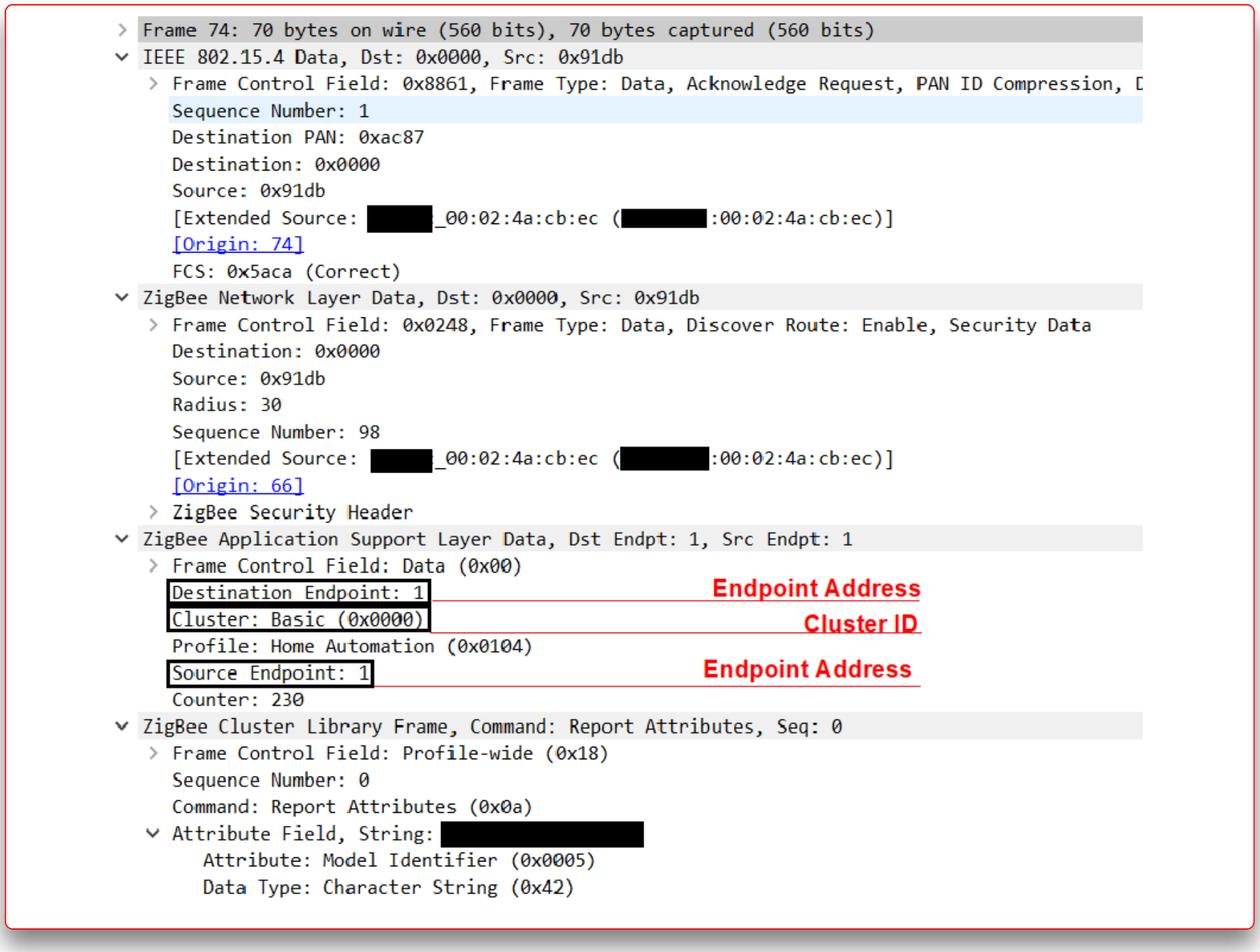
Application level addressing

- End Point Address

  Every ZigBee node may support one or more applications or End Points. To send direct messages to a specific application, Endpoints numbered from 1 to 240 are used - there's also a broadcast Endpoint, 255, which allows messages to send to all applications on a given node.

- Cluster Identifier (Cluster ID)

  The cluster identifier is a 16-bit number unique within the scope of each application profile and identifies a specific cluster. Refer below snapshot of ZigBee packet for more understating of End Point address and Cluster ID



Messaging in ZigBee

ZigBee supports broadcast, unicast, group-multicast, and Inter-PAN messaging.

- Broadcast

  Message initiated by PAN coordinator, intended for all devices in the PAN network and router devices, the router retransmit it for End Node belonging to the same PAN network.

- Unicast

The message directed towards a single End Node in the network and often routed through multiple nodes to reach the destination node. The unicast message requires network level acknowledgment from the final destination device to the source device while MAC level acknowledgment is sent between the MAC layer if the message route through different nodes.

- Group Multicast

  The message intended for every device in a particular PAN network and belonging to a dynamically defined multicast group within a given transmission radius measured in hops.

Inter-PAN Communication

This Message intended for device from different PAN network with different PANID. ZigBee specification defines inter-pan communication as a mechanism whereby ZigBee devices can perform exchanges of information with devices in their local area without having to form or join the same ZigBee network.

Conclusion...

We hope this gives you an introduction and a brief insight into the ZigBee protocol. In the next blog, we will look at the security of the ZigBee protocol and devices.

Continue to the next part in the series - IoT-Security Part-6 (ZigBee Security - 101)

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**