F-Secure

ZIGBEE NETWORKS AN OVERVIEW

A guide for implementers and security testers

An F-Secure Consulting Whitepaper

CONTENTS

1. WHAT IS ZIGBEE? 2

1.1. ZIGBEE VERSIONS 2

2. HOW DOES ZIGBEE OPERATE? 3

2.1. THE ZIGBEE STACK 3

2.2. ZIGBEE NODE TYPES 5

2.3. ZIGBEE TOPOLOGY 6

2.3.1. STAR 6

2.3.2. TREE 7

2.3.3. MESH 8

2.3.4. HARDWARE DEVICE TYPES 8

2.4. ADDRESSING AND IDENTITY IN A ZIGBEE NETWORK 9

2.4.1. DEVICE IDENTITY 9

2.4.2. NETWORK IDENTITY 10

2.4.3. APPLICATION LEVEL ADDRESSING 10

2.5. HOW ZIGBEE MESSAGES PROPOGATE 11

2.5.1. SERVICE DISCOVERY AND BINDING 13

2.6. ENCRYPTION, INTEGRITY AND AUTHENTIFICATION 14

3. CONCLUSION 19

1. WHAT IS ZIGBEE?

ZigBee is a standard for low-power Wireless Personal Area Networks (WPANs) - wireless networks with a short range, typically 10-100 meters. It's commonly used for wireless control and monitoring applications such as:

- Wireless sensor networks (WSNs)
- Industrial plant monitoring
- Building control
- Hospitals
- Smart metering
- Home automation

There are actually public profiles defined in the ZigBee specification for many of these use cases.

It operates in the Industrial, Scientific, and Medical (ISM) radio bands but the exact frequency will depend on where you are in the world. It can use the 868 MHz band in much of Europe, 915 MHz in the USA, and 2.4 GHz in many other locations. The 2.4 GHz band is very common as many of the available chipsets use it. The speeds available depend on which band you're using, but the maximum is 250 Kbps. Although slower than other popular wireless technologies, such as WiFi, it's cheaper.

1.1 ZIGBEE VERSIONS

Since the original ZigBee 2004 specification, there have been several updates. So you may see references to both "ZigBee 2006" and "ZigBee PRO", with the latter also referred to as ZigBee 2007.

ZigBee PRO allows for more complex routing and dynamic channel switching if interference is detected. It's also backwards compatible with ZigBee 2006 - however, there are some limitations. Specifically, a ZigBee PRO device on a ZigBee 2006 network must operate as an End Device. The same goes for a ZigBee 2006 device on a ZigBee PRO network.

Many people consider pre-ZigBee PRO to be "legacy" but it's important for those concerned with the security of ZigBee networks to understand older versions. Being the newer version, some of this article discusses ZigBee PRO concepts, although much of it will apply to all versions.

2. HOW DOES ZIGBEE OPERATE?

ZigBee is built on top of the 802.15.4 specification which defines the Physical (PHY) and Media Access Control (MAC) layers for low-rate WPANs (LR-WPANs). It adds layers on top of this to add more network and application intelligence.

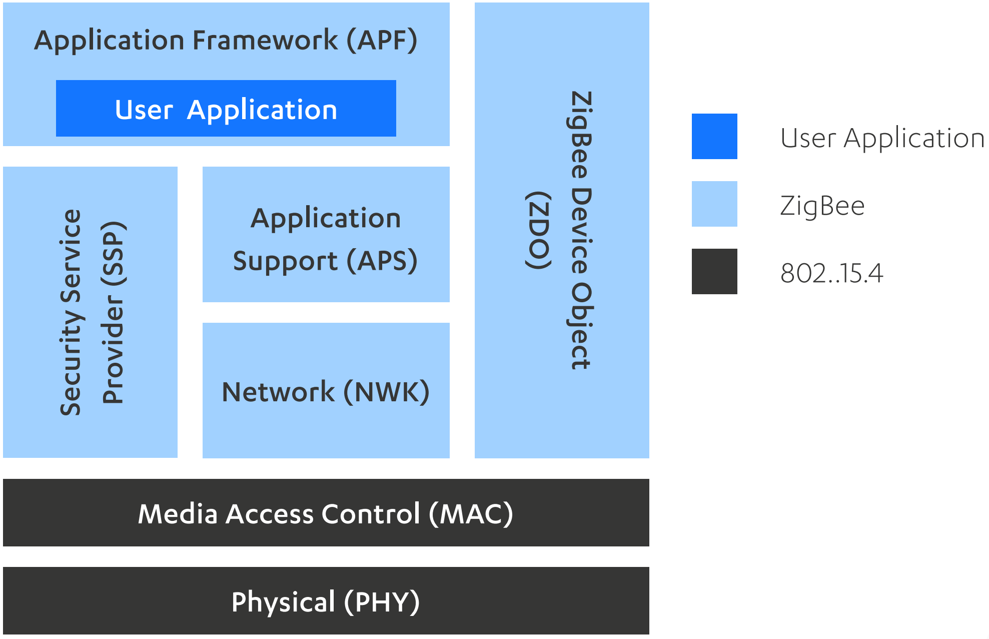
> **802.15.4** is the basis for ZigBee and many other industrial wireless protocols, so understanding it can be very useful to a security consultant.

A ZigBee network allows a set of devices to communicate wirelessly via one of several possible topologies. Packets of data can be sent between nodes, and may be routed by intermediary devices to more distant nodes that would otherwise be out of range. Each device has both a MAC address and a ZigBee network address, while the entire network has its own PAN ID shared by all devices.

Packets can be protected by encryption - but all nodes need a key for this to work, and there can be issues around how they're deployed to devices.

2.1 THE ZIGBEE STACK

A simplified view of the ZigBee stack looks like this:


Application Framework (APF)
User Application
Security Service Provider (SSP)
Application Support (APS)
Network (NWK)
ZigBee Device Object (ZDO)
Media Access Control (MAC)
Physical (PHY)
User Application
ZigBee
802..15.4

PHY – Defined by 802.15.4, the PHY layer is responsible for the modulation, demodulation, and physical transmission of packets over the air. It handles various things needed for robust radio transmission in noisy, interference prone environments.

MAC – Also defined by 802.15.4 and similar to MAC layers in other protocols, ZigBee doesn't actually use all of its features. This layer performs functions such as CSMA/CA to avoid collisions when transmitting frames, and defines a frame format with things like MAC addresses. The MAC layer also defines network topologies which ZigBee builds upon and enhances at higher levels of the stack.

NWK – One of the more complex ZigBee layers that builds on 802.15.4, this provides the ability to discover and join networks. It also expands on the topologies defined by 802.15.4 at the MAC layer to allow mesh networking - a popular feature of ZigBee. The NWK layer also determines routes through the ZigBee network and supports ZigBee addresses different to the MAC addresses present at the MAC layer.

APS – This ZigBee layer implements features needed by ZigBee applications and acts as an interface to the NWK layer. It filters some duplicate packets from the NWK layer and maintains a binding table of nodes in the network.

SSP – Provides ZigBee security services to the NWK and APS layers including key establishment and transport, device management, and frame protection.

ZDO – Responsible for the overall management of the ZigBee device. The ZDO initializes the APS and NWK layer, allows device discovery, manages binding requests, and defines the device mode (coordinator, router, or end device).

APF – This is an execution environment for ZigBee user applications, helping them send and receive data. It also provides an Endpoint for each application, with Endpoint 0 being reserved for the ZDO and Endpoint 255 for a broadcast address. Applications themselves implement the function of the ZigBee device (e.g. a sensor).

2.2 ZIGBEE NODE TYPES

A device can act as one of three node types within a ZigBee network. Whatever node a device is acting as, it can also be doing some useful work, such as acting as a sensor. Node types are only relevant to the topology of the ZigBee network and how devices help to route messages. The available node types are:

- **Coordinator** – Every ZigBee network must have a single Coordinator, the first node to start up. It initializes the rest of the network, selects the frequency to use, the PAN ID of the network, and allows other nodes to join the network. Not only that, it acts as the parent to nodes that use it to connect to the network.

  The Coordinator often runs other services such as routing and certain security services. However, many of these services are options and some can be run on separate dedicated nodes.

- **Router** – Routers aren't necessarily required, but are commonly found in all ZigBee topologies. They're responsible for relaying messages to other nodes. Nodes can also join the network via a Router, with the Router becoming their parent node - this can include one Router being the parent of another Router.

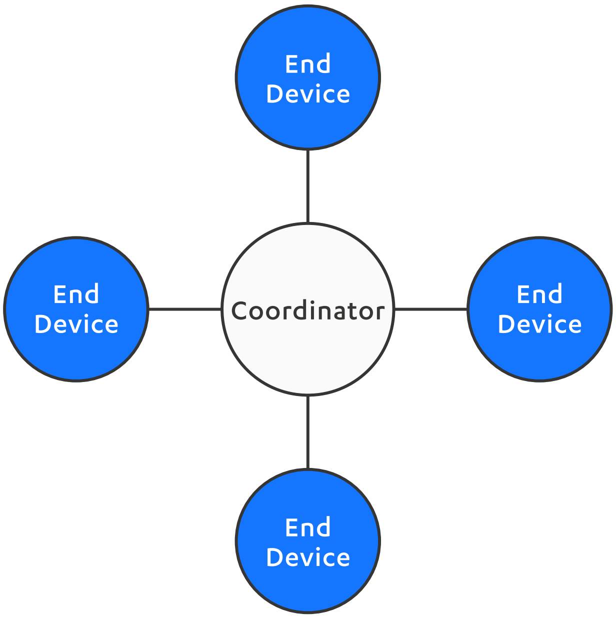
- **End Device** – An End Device is a node that simply sends and receives messages. It doesn't perform any other special function in the network, and nodes can't join the network through them. End Devices are the only nodes that can sleep, according to the ZigBee specification with the parent node (a Router or Coordinator). It will buffer messages until it wakes up again.

2.3 ZIGBEE NETWORK TOPOLOGY

For every network topology, there will be a parent node. All other nodes that connect to this are considered a child node. ZigBee networks can have one of three different topologies which affect how messages are routed devices communicate. These topologies are shown below:

2.3.1 STAR

This is the simplest, most limited topology available to ZigBee. All devices connect to a single Coordinator node and all communication goes via this. It's interesting to note this topology is actually defined by the underlying 802.15.4 specification which ZigBee builds on.

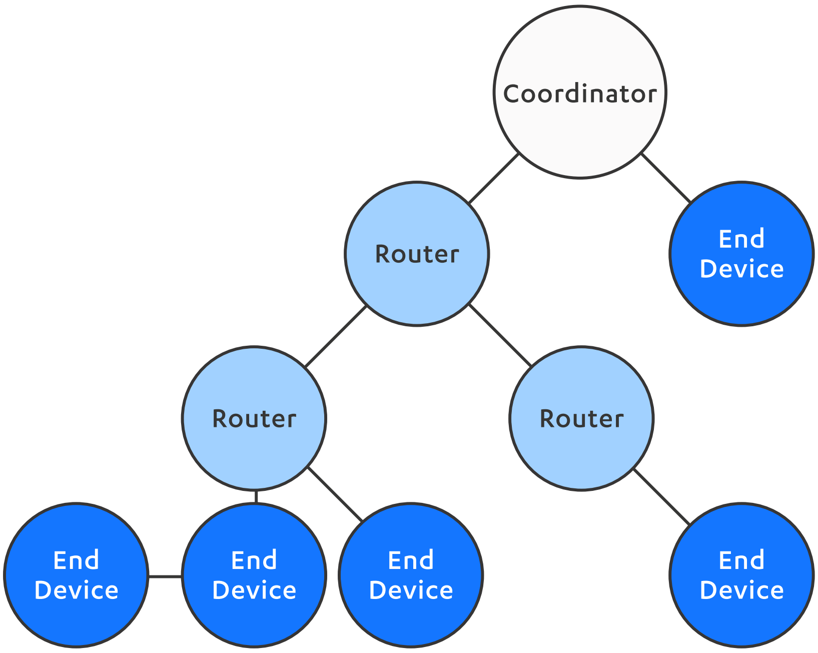


Child nodes can also be Routers, although they won't perform any routing functionality and will act as an End Device.

With Star topology, the throughput of the network is limited by the Coordinator. If the Coordinator fails, the whole network fails. The range of the network is also limited to the range of the Coordinator itself.

2.3.2 TREE

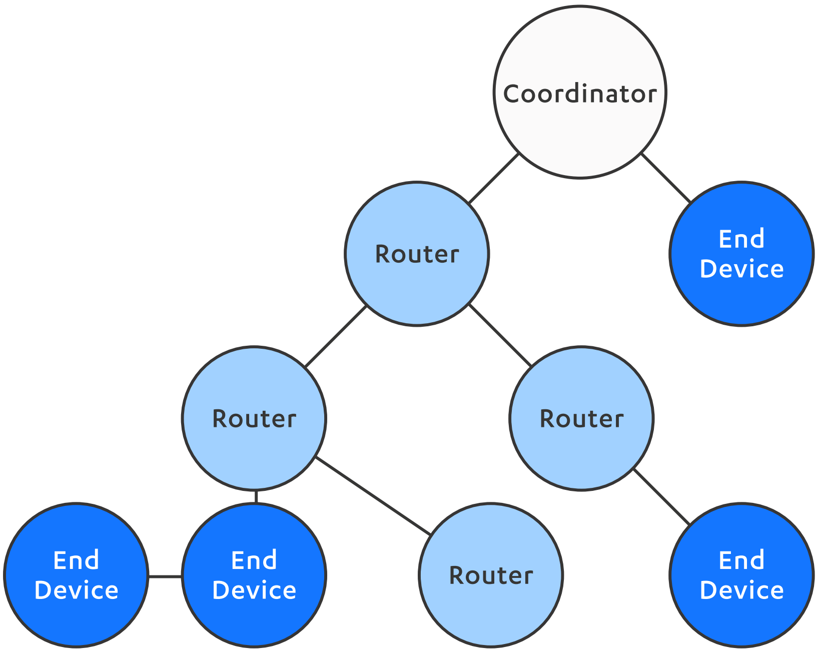
The Coordinator forms the root node of a tree of child nodes. End Devices are leaf nodes (although a Router could also be a leaf if no children have joined it yet) and intermediate nodes are Routers. Direct communication can only occur between a child node and its parent. However, all nodes can communicate together by messages moving up the tree towards the target node.



In this topology, Routers can extend the range of the network beyond any single device-to-device link. So if a Router fails there's no alternative route, meaning portions of the network can become disconnected.

2.3.3 MESH

Mesh topology is one of the most flexible offered by ZigBee. It's similar to Tree topology but doesn't follow the rigid tree structure. In this topology, a Router can communicate directly with any other Router or the Coordinator if it's in range. There can be many routes through the network to a given node, and ZigBee has a route discovery feature to find the best one, making it "self-healing".



2.3.4 HARDWARE DEVICE TYPES

A device can be classified as a Full Function Device (FFD) or a Reduced Function Device (RFD). These classifications relate to the physical capabilities of the hardware and come from the 802.15.4 specification. RFDs are often battery powered and sleep between transmissions to save power - FFDs are usually the opposite.

In a ZigBee network, an RFD must be an End Device and not a Router or Coordinator. This is because the latter two can't perform their functions correctly if they go to sleep.

2.4 ADDRESSING AND IDENTITY IN A ZIGBEE NETWORK

2.4.1 DEVICE IDENTITY

Individual devices in a ZigBee network have two addresses - a MAC address and a Network Address (NwkAddr). The MAC address comes from the underlying 802.15.4 protocol whereas the NwkAddr is actually part of the ZigBee layer itself. The difference between these addresses is detailed below:

- **MAC Address** – Sometimes referred to as the "extended address", this is a 64-bit address (like the MAC addresses you may be used to in the world of Ethernet). It's meant to be assigned to the device at the time of manufacture and should never change. No other device in the world should ever have the same address. The MAC address is an important part of 802.15.4, used for low level packet delivery.

  At the ZigBee layer the MAC address is rarely used, except in certain cases such as binding when the mapping between the MAC address and NwkAddr is needed.

- **Network Address (NwkAddr)** – Also called the "short address", this is a 16-bit address that's unique only within an individual ZigBee network. The NwkAddr is assigned when a device joins the network and can change if it leaves and re-joins the network. The Coordinator always has the NwkAddr 0x0000.

  Depending on the version or configuration of ZigBee, stack addresses will either be assigned according to a devices position in a Tree topology or randomly assigned by the Coordinator. In the latter case, a Device Announcement will be broadcast at the time of assignment to allow an Address Conflict to be sent by any device that already has the selected address.

As translation between the MAC address and NwkAddr is necessary to deliver packets correctly, ZigBee provides a mechanism to allow the NwkAddr to be discovered. You can superficially compare this to the way ARP resolves MAC addresses to IP addresses in IP networks.

It's also possible to configure group addresses which allow message sending to a specific group of nodes subscribed to that address.

2.4.2 NETWORK IDENTITY

There are two identifiers that can be used to identify a ZigBee network - the Personal Area Network Identifier (PAN ID) and the Extended PAN ID (EPID).

- **PAN ID** – SPart of 802.15.4, the PAN ID is a 16-bit identifier selected at random by the Coordinator when the network starts up. It's used by the MAC layer to filter out packets that aren't part of the same network.
- **EPID** – A ZigBee concept, the EPID is a 64-bit identifier which can be used for more fine grained uniqueness and identification of the ZigBee network. This isn't sent in all packets but can be used in some situations such as when resolving PAN ID conflicts.

2.4.3 APPLICATION LEVEL ADDRESSING

A single ZigBee node may run one or more applications. 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 be sent to all applications on a given node.

Although not technically an address, messages can also be sent to a specific part of an application by specifying a **Cluster ID**. Clusters provide context or meaning to an application and allow commands and data to be exchanged in a certain way.

They're divided into **Input/Server** and **Output/Client** clusters. Input Clusters store attributes and allow them to be manipulated by incoming messages. Messages are sent from an Output Cluster to manipulate attributes in an Input Cluster, and receive responses to those messages.

ZigBee applications also run in the context of a particular profile. They define a set of Clusters with particular attributes and commands, allowing devices to be compatible out of the box in a specific domain. There are a number of public profiles, including Home Automation, Telecom Applications, Industrial Plant Monitoring, and more. These allow devices designed for a specific purpose to all interact together in a meaningful, standardized way. Private profiles can also be defined for custom behaviour not present in the public profiles.

2.5 HOW ZIGBEE MESSAGES PROPAGATE

ZigBee messages can be sent to a specific node, a group of nodes, or broadcast to (potentially) all nodes - they can even be sent between ZigBee networks with different PAN IDs. Here's an overview of all these scenarios:

Broadcast – 802.15.4 has its own broadcast mechanism, but ZigBee builds on this. When a broadcast is sent, any Coordinator or Router in range will retransmit it - unless it's reached the maximum number of retransmissions. This means a broadcast can only propagate a certain number of hops before it stops being sent.

A process of passive acknowledgement is used to provide a level of reliability without requiring additional messages to be sent. When a device transmits or re-transmits a broadcast, it listens to its neighbours to be sure they re-transmitted the broadcast within a certain period of time. If they don't, it sends it again.

Broadcast messages are identified by the Network Address being set to one of the predefined broadcast addresses. These are:

0xFFFF – Broadcast to all devices (most common)

0xFFFD – Broadcast to all devices with receiver turned on permanently

0xFFFC – Broadcast to all Routers and Coordinators

0xFFFB – Broadcast to Low Power Routers

Unicast – Unicast messages are directed towards a single node. Not all nodes can communicate directly, based on transmission range and network topology. So messages often pass through multiple nodes to reach their final destination. To automatically discover a route, you can use a route discovery algorithm.

At the Network level, a Network ACK is returned to the original node once the messages reach their destination. At the MAC level, a MAC ACK is sent between each hop as the message propagates.

Group Multicast – This is used to send a message to a group of nodes simultaneously. Messages are sent with a group address (basically a Network Address), just like broadcasts. Each node checks if it has Endpoints in the group before processing the message.

Bound Transfer – This is when a message is sent to Endpoints which the sender has been bound to. More information on this is given in the upcoming Service Discovery and Binding section.

Inter-PAN Transfer – Refers to a message being sent to a node in a different network with a different PAN ID.

802.15.4 supports inter-PAN addressing and, while not really a part of ZigBee, some devices support this. Usually these messages aren't forwarded or routed through the network – they're sent directly to an out-of-network device in range of the sender. This can allow some data transfer to other devices that may not be compatible with the whole network.

Importantly, such transmissions aren't encrypted as they're destined to a foreign network outside of the normal security framework. However, it could be possible for developers to add application level encryption using a shared key or similar.

For messages passing through several nodes to reach their final destination, two address fields are used - "next hop" and "final destination". The next hop is determined by a routing table maintained by each Router or Coordinator node and is filled in each time one of these nodes forwards a packet on. The route discovery mechanism uses a route discovery broadcast if no routing table entry is found.

2.5.1 SERVICE DISCOVERY AND BINDING

Depending on the purpose of the ZigBee network, nodes must be able to identify the service they're interacting with on other nodes to allow meaningful communication. There are two main ways to accomplish this - Service Discovery and Binding.

With Service Discovery, a node sends a broadcast requesting a certain service. Nodes with that service then respond with their address. A node can store this information and communicate with the other nodes services with "direct addressing" using the Network Address, Endpoint, and Cluster ID.

Rather than using discovery and direct communication, nodes can also make use of the binding mechanism. When nodes are bound, it allows messages to be automatically routed without specifying the destination address and Endpoint. Binding can be one-to-one, one-to-many, or many-to-one.

2.6 ENCRYPTION, INTEGRITY AND AUTHENTICATION

As with any wireless network where security's a concern, encryption plays an important part. There are a number of security options that can be configured, affecting encryption in a ZigBee network. The way keys are handled and exchanged can be partly defined by the Application Profile being used. Also whether the network is using Standard Security Mode (Residential Mode in ZigBee 2006) or High Security mode (Commercial Mode in ZigBee 2006).

Ultimately, encryption can be applied at three different levels; the MAC layer, Network (NWK) layer, and the Application Support (APS) layer. A ZigBee frame will contain fields from all of these layers encapsulated within one another, and each can later encrypt its data payload.

In fact, the underlying 802.15.4 specification allows for encryption of frames at the MAC layer but doesn't specify important things, such as key management and authentication schemes. ZigBee implements these controls at the NWK and APS layers.

All encryption in a ZigBee network uses AES-128, including at the 802.15.4 level. This allows hardware designed for use with 802.15.4 containing optimized AES components to be used throughout a ZigBee implementation. AES provides symmetric encryption meaning both sides must share a key.

How nodes obtain these keys is an important security concern. There are three main methods:

Pre-installation – Keys are placed on devices out-of-band (e.g. physically programmed in before deployment).

Transport - Keys are transported over the network to the device.

Establishment – Through a negotiation process, keys are established without ever actually sending them over the network. Three methods of Establishment are:

- Symmetric-Key Key Establishment (SKKE)
- Certificate-Based Key Establishment (CBKE)
- Alpha-Secure Key Establishment (ASKE)

Where keys aren't pre-installed there must be a device which can store and distribute or negotiate keys. This is known as the **Trust Center** and is often the Coordinator of the network. However, it doesn't have to be for ZigBee PRO.Tthe Trust Center also authenticates devices onto the network.

It can be possible to distribute some keys securely where multiple keys are used, but there are situations where ZigBee can be configured so keys will be sent unencrypted over the network which introduces a short period of vulnerability.

Depending on configuration and profile ZigBee can actually use a number of keys. Keys can be used by different layers in the stack but all have unique purposes. Keys that can be present are:

Link Key – This is uniquely shared between two devices and can be used to encrypt unicast messages between them. If a device shared a Link Key with the Trust Center (known as a Trust Center Link Key), it can be used to encrypt the transfer of the Network Key to a node joining the network. Other Link Keys operate at the APS layer and are known as Application Layer Link Keys.

Network Key – Shared between every device on the network, this can be used for NWK layer encryption and protecting broadcast traffic. A set of Network keys are stored on the Trust Center and identified by a key sequence number. They can be pre-installed on devices or transported from the Trust Center. Such transport will only be encrypted if another key's available to be used as a key-transport key, such as the Trust Center Link Key.

Master Key – Used for SKKE Establishment of Link Keys. Usually pre-installed, some mechanisms may use a "key- load key" to help securely transfer a Master Key from the Trust Center to a device.

These keys also provide the basis for authentication through a challenge response mechanism. ZigBee PRO also supports Mutual Symmetric-Key Entity Authentication between any devices, as well as simple authentication to the network as a whole.

A frame counter is also used which is incremented with each transmission. This helps prevent replay attacks and forms part of a nonce value which ensures the freshness of the frame with regards to cryptography. If a device receives a frame with a frame counter lower than the previous value it will reject it.

The frame counter is also associated with the current Network Key. The Trust Center will periodically change the Network Key and reset the frame counter to zero to avoid locking the network up when the counter reaches its maximum value. The Network Key must be changed to reset the frame counter.

While encryption can provide confidentiality of data being transmitted and allow authentication to occur, it can also be used to provide assurances over message integrity. This is achieved by the Message Integrity Code (MIC), also referred to as the Message Authentication Code (MAC) - not to be confused with the MAC layer in the protocol stack. The MIC uses AES to effectively sign the message to assure the contents hasn't been tampered with.

ZigBee can operate in a number of configurations with regards to encryption level. This can enable or disable encryption and the MIC independently, depending on the Security Level. This level also specifies things such as how many bits the MIC contains, with a longer MIC considered more secure and more difficult for an attacker to forge or guess. The MIC can be 32, 64, or 128 bits.

It's important to remember any Inter-PAN messages between networks won't be encrypted as they're outside the normal key management processes within a ZigBee network.

Proper key management is important in maintaining the security of a ZigBee network. As such, implementers should be aware there are situations where keys may be transmitted in the clear which opens a clear window of vulnerability to the network.

3. CONCLUSION

ZigBee networks can be configured and operate in many different and often subtle ways. Sometimes the exact way a given aspect of the network will operate is based on the manufacturer of the ZigBee chipset. What's more, ZigBee networks can be highly flexible with devices sleeping and waking up, connecting and disconnecting, altering the layout of the mesh network, switching channel or PAN ID and so on. To deploy these networks securely, or to analyse such a network as a security tester or researcher, it's important to understand all these core concepts.

F-Secure.