Internet of Things Security

Lecture 05: Low Power Networks and Security Challenges

Mehmoona Jabeen

Mehmoona.jabeen@au.edu.pk

Department of Cyber Security, Air University

Lecture Outlines

- Introduction to RFID Protocol
- Security Challenges in RFID
- Introduction to ZigBee Protocol
- Security in Zigbee
- Introduction to Bluetooth Protocol
- Security Challenges in Bluetooth

RFID

- Identification is one of the key requirements for the implementation of IoT.
- The RFID development community used the term Internet of Things to refer to the possibility of discovering information about a tagged object by browsing an Internet address or database entry that corresponds to a particular RFID tag.
- This provides the foundation of Web 4.0; Web of Things
- RFID stands for Radio Frequency Identification. It is a technology that uses radio waves to identify and track objects.
- RFID works by using a small electronic device called a tag or transponder, which contains a microchip and an antenna.
- The tag is attached to an object, and when it comes into range of an RFID reader, the reader sends out radio waves that power the tag and read its unique identifier.
    - Src: https://www.theguardian.com/technology/2003/oct/09/shopping.newmedia

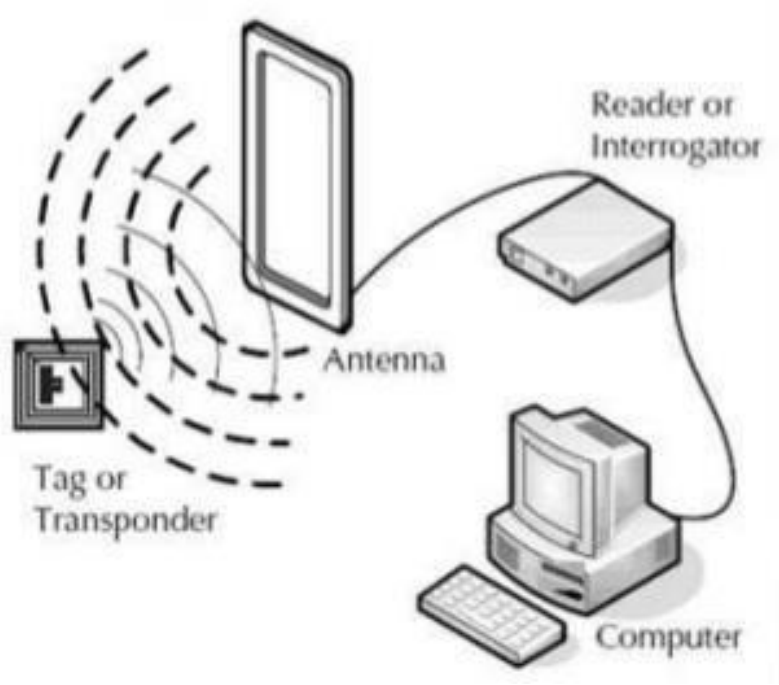
RFID architecture

RFID consists of

1. Tags (transmitters / responders) : The tag is a microchip connected with an antenna, which can be attached to an object as the identifier of the object.

2. Readers (transmitters / receivers) : The RFID reader communicates with the RFID tag using radio waves.

3. Controller/host : PC/workstation running database and control (middleware).



RFID Spectrum

- Tag wirelessly sends bits of data when it is triggered by a reader
- Power source not required for passive tags… a defining benefit
- Superior capabilities to barcode:
  - Non Line of Sight
  - Hi-speed, multiple reads
  - Can read and write to tags
  - Unit specific ID

	Frequency	Distance	Example Application
LF	125khz	Few cm	Auto-Immobilizer
HF	13.56Mhz	1m	Building Access
UHF	900Mhz	~7m	Supply Chain
µwave	2.4Ghz	10m	Traffic Toll

How it works?

Near field (LF, HF): inductive coupling of tag to magnetic field circulating around antenna (like a transformer)

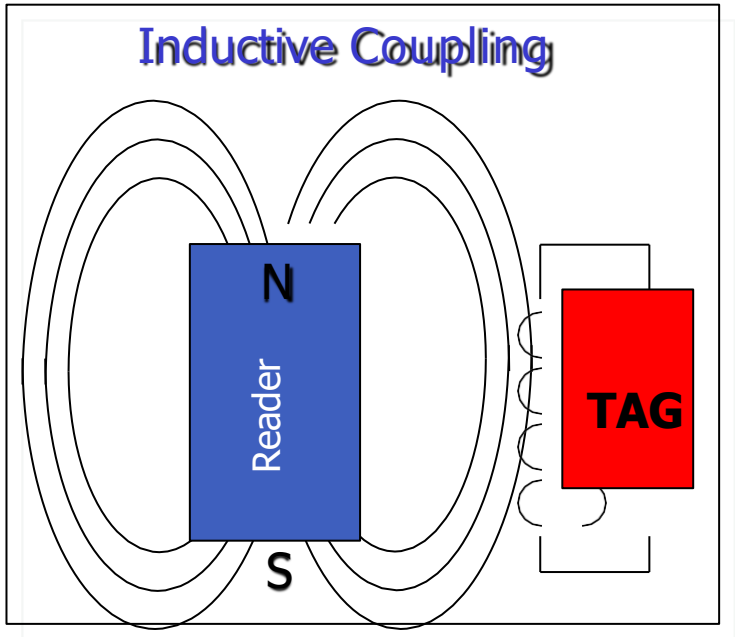
- Varying magnetic flux induces current in tag. Modulate tag load to communicate with reader
- field energy decreases proportionally to 1/R3 (to first order)

Far field (UHF, microwave): backscatter.

- Modulate back scatter by changing antenna impedance
- Field energy decreases proportionally to 1/R

Boundry between near and far field:

- R = wavelength/2 pi
- so, once have reached far field, lower frequencies will have lost significantly more energy than high frequencies



RFID Standards

Standard	Description	Frequency Band	Read Range	Application
EPCglobal Class 1 Gen 2	Standard for UHF RFID tags and readers widely used in supply chain management and inventory control.	860-960 MHz	Up to 30 feet	Supply chain management, inventory control
ISO 15693	Standard for HF RFID tags and readers used in access control, library systems, and asset tracking.	13.56 MHz	Up to 3 feet	Access control, library systems, asset tracking
ISO 14443	Standard for NFC RFID tags and readers used in mobile payments, transit, and access control.	13.56 MHz	Up to 4 inches	Mobile payments, transit, access control
ISO 18000-6C	Standard for UHF RFID tags and readers used in asset tracking, logistics, and vehicle identification.	860-960 MHz	Up to 30 feet	Asset tracking, logistics, vehicle identification

EPC(Electronic Product Code)

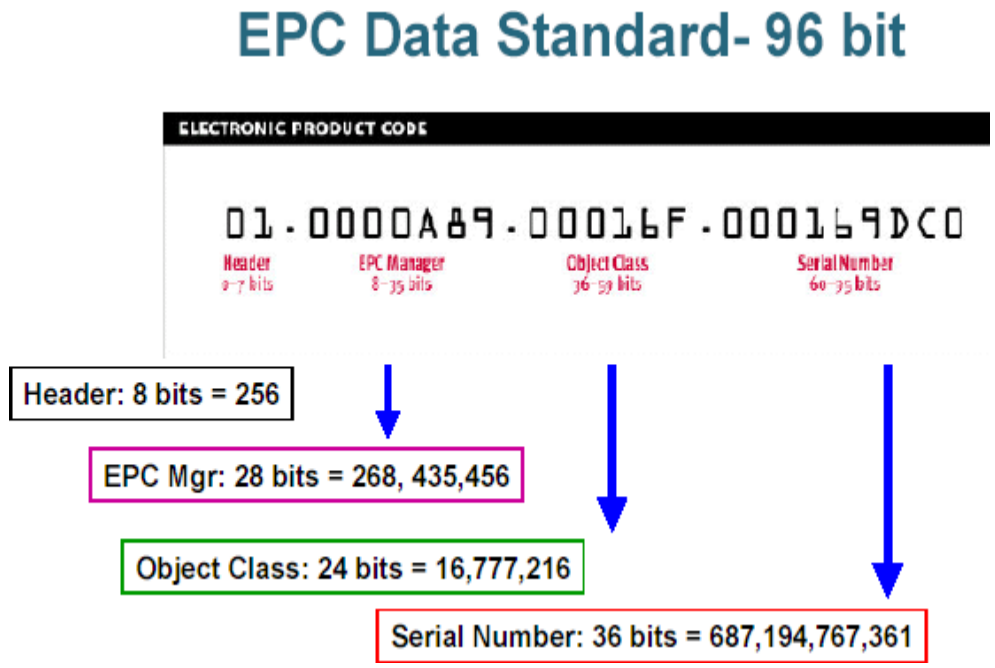
Header - Tag version number

EPC Manager - Manufacturer ID

Object class - Manufacturer's product ID

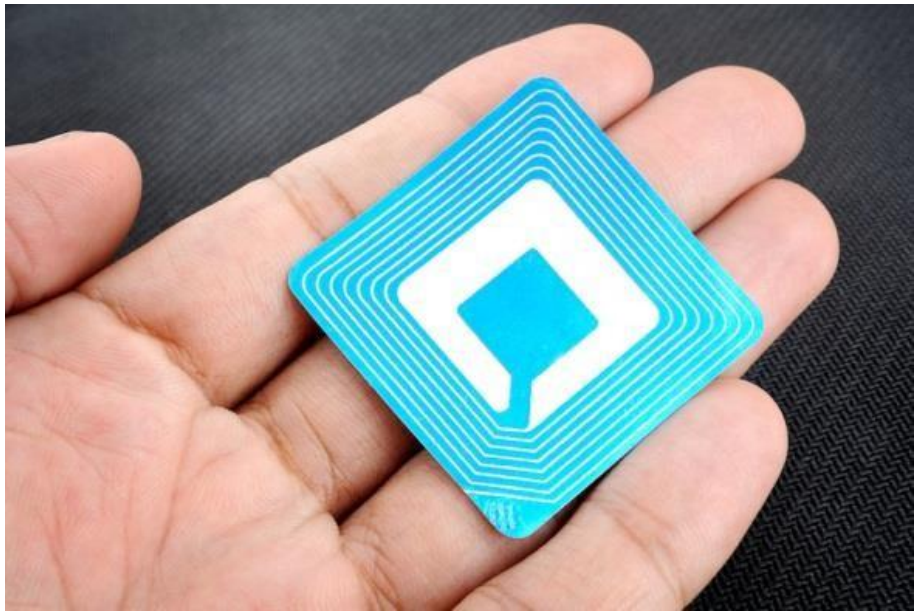
Serial Number - Unit ID

With 96 bit code, 268 million companies can each categorize 16 million different products where each product category contains up to 687 billion individual units



Types of RFID?

- Passive Tags
- Passive tags have limited computational capacity, no ability to sense the channel, detect collisions, and communicate with each other.
- They respond only at reader commands.
- Passive RFID tags have an integrated circuit and antenna.
- Semi-passive have on-board power source that can be used to energize their microchip.



Types of RFID?

- Active Tags

- The term “active” means the transponder has a power source, usually a battery.

- Energy can also be captured from light via photovoltaic cells or other source.

- Active tag can broadcast its own signals, like a cell phone.

- It has longer range as compared to passive tags.

RFID Security Challenges

- Unauthorized access: RFID signals can be intercepted by unauthorized individuals, potentially allowing them to access sensitive data or track the movement of objects or individuals.
- Data tampering: RFID data can be manipulated or altered, which could result in the tracking of false information or the misidentification of objects.
- Denial of service: RFID systems can be disrupted by jamming the radio signals or blocking the antennas, preventing the system from functioning properly.
- Eavesdropping: RFID signals can be monitored and captured by attackers, who can then use the information to gain unauthorized access or track the movement of objects or individuals.
- Malicious attacks: RFID systems can be attacked by hackers who attempt to gain access to the system, steal data, or cause other disruptions.
- Cloning
- Tracing
- Data forging

Security of RFID?

- IPSec Security

- Internet Protocol Security has been jointly defined with the IPv6 standard to provide end-to-end security for Internet connections. IPsec itself is mandatory in IPv6 and must be supported by all IPv6 implementations but is optional for IPv4. It has been standardized by the Internet Engineering Task Force in several RFCs .

- The security services of IPsec can be provided between a pair of communicating nodes, between a pair of communicating security gateways, or between a security gateway and a node.

Security of RFID?

- IPSec Security Methods
- Authentication headers
- The Authentication Header (AH) protocol of IPsec provides origin authentication and integrity of the IP datagrams. In addition, it can also prevent from replay attacks of IP datagrams.
- Encapsulating security payloads
- In addition to AH, it is also possible to use ESP protocol, which also provides confidentiality for IP datagrams. In contrast to AH, ESP does not provide protection for the IP header. However, it is possible to use the tunnel mode of operation where the original IP datagram is encapsulated in a new datagram. Thus, the whole inner datagram is protected by ESP, including the header.

Security of RFID?

- Cryptography-Cloning

- In principle, symmetric-key cryptography can go far toward eliminating the problem of tag cloning. With a simple challenge response protocol like the following, a tag can authenticate itself to a reader with which it shares the key .

  - 1) The tag identifies itself by transmitting the value .
  - 2) The reader generates a random bit string (often called a nonce) and transmits it to the tag.
  - 3) The tag computes , and transmits .
  - 4) The reader verifies that .

Privacy of RFID?

- **"**Killing" and "Sleeping**":** EPC tags address consumer privacy with a simple and draconian provision: Tag "killing." When an EPC tag receives a "kill" command from a reader, it renders itself permanently inoperative. To prevent wanton deactivation of tags, this kill command is PIN protected. To kill a tag, a reader must also transmit a tag-specific PIN (32 bits long in the EPC Class-1 Gen-2 standard).

- Renaming Approach**:** Even if the identifier emitted by an RFID tag has no intrinsic meaning, it can still enable tracking. For this reason, merely encrypting a tag identifier does not solve the problem of privacy. An encrypted identifier is itself just a meta-identifier. It is static and, therefore, subject to tracking like any other serial number. To prevent RFID-tag tracking, it is necessary that tag identifiers be suppressed, or that they change over time.

Privacy of RFID?

- Relabeling: Consumers be equipped to relabel tags with new identifiers, but that old tag identifiers remain subject to reactivation for later public uses, like recycling. By peeling off one of these two tags, a consumer can reduce the granularity of tag data.

- "Minimalist" cryptography: a "minimalist" system in which every tag contains a small collection of pseudonyms; it rotates these pseudonyms, releasing a different one on each reader query. An authorized reader can store the full pseudonym set for a tag in advance and, therefore, identify the tag consistently. An unauthorized reader, however, that is, one without knowledge of the full pseudonym set for a tag, is unable to correlate different appearances of the same tag. To protect against an adversarial reader harvesting all pseudonyms through rapid-fire interrogation.

Standards Challenges

- Standards and specifications by international forums are the foremost requirement in order to see IoT in its desired shape. Although European communities have been investing significant efforts towards IoT mission, a collective effort by IEEE, NIST, ITU, ISO/IEC, IETF could probably make this mission effective, implementable and deliverables.
  - ISO/IEC 29167-11:2023: Information technology —Automatic identification and data capture techniques —Part 11: Crypto suite PRESENT-80 security services for air interface communications
  - ISO/IEC 29167-10:2017: Information technology —Automatic identification and data capture techniques —Part 10: Crypto suite AES-128 security services for air interface communications

- While integrating trillions of objects in IoT infrastructure, managing identities would become a major task in IoT. Both addressing and uniqueness issues have to be resolved suitably. Some existing technologies such as smart cards, RFID tags, IPv6, are going to play important roles for identifying objects in IoT infrastructure.

Technical Challenges

- Certain products (especially those containing metal and liquids) can pose serious obstacles for automatic read outs. This can limit the feasibility of some sales floor applications to certain product types.

- Further challenges can arise when multiple readers are operated in close proximity. This is especially the case for smart shelves. Close physical proximity can result in false reads where a shelf captures RFID tags in the adjacent shelf.

- Simultaneously operated readers can distort each other. Addressing these 132 RFID in Retail challenges requires an advanced middleware to coordinate reads and to associate reads with the correct shelf.

How RFID Secure

- RFID security can be achieved through a combination of technical and procedural measures. Here are some ways in which RFID security can be enhanced:
- Authentication: RFID systems can use authentication protocols to ensure that only authorized tags are allowed to access the system. This can be achieved by using encrypted data transmissions or by requiring a password or key to access the system.
- Encryption: RFID systems can use encryption to protect the data being transmitted between the tag and the reader. This can help to prevent unauthorized access and data tampering.
- Access control: Physical access to RFID systems can be restricted to authorized personnel only. This can be achieved by using access cards or biometric authentication systems.

RFID Hacking Tools

1. Proxmark3 ID DEV Kit:
   - Multi-purpose research and development hardware tool for RFID securit analysis. It can sniff, read, analyse and emulate RFID (Radio Frequency Identification) tags.

2. Flipper Zero
   - The Swiss army knife that contains multiple tools for pentesting such as RFID, RF, Infrared, HID emulation, GPIO, Hardware debugging, 1-Wire, Bluetooth, Wifi and more.

3. ESP RFID Tool
   - Data logger that captures data from a standard Wiegand Interface.
   - You can use this device to log the credentials for access control systems, RFID card readers, pin pads, magnetic stripe systems, some biometric readers and any other device that utilizes a Wiegand Interface.

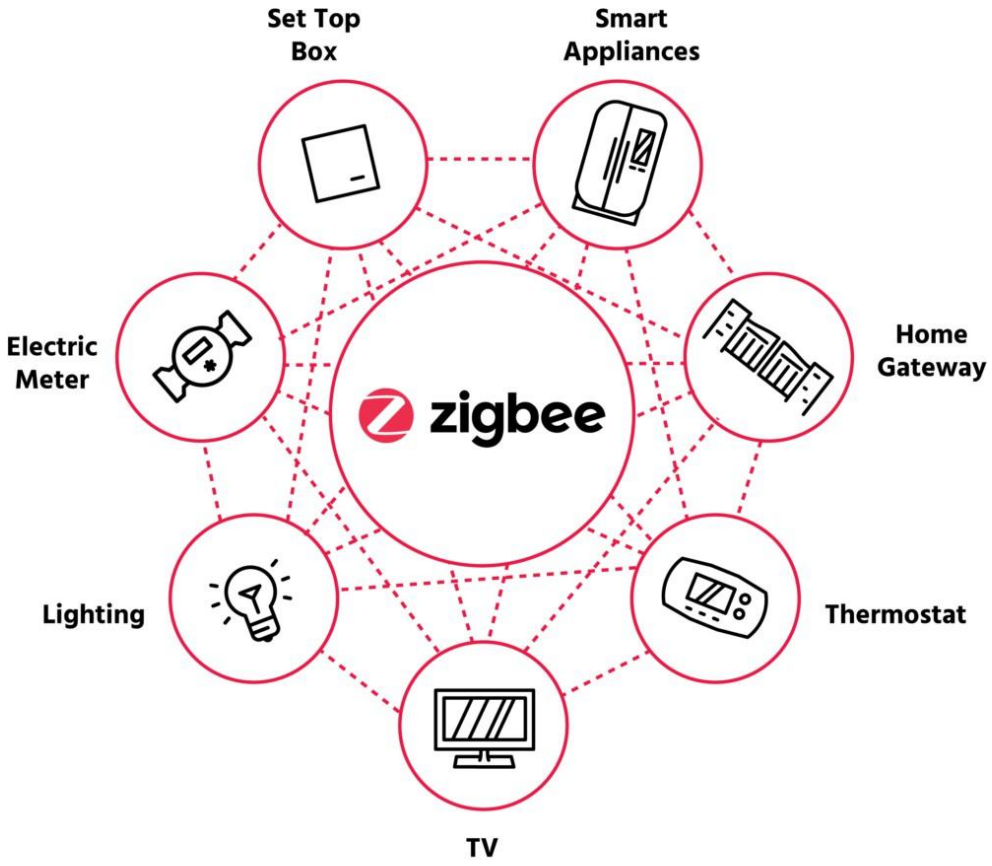
Source: github.com/rfidtool/ESP-RFID-Tool

Readings

1. **M. Hosseinzadeh *et al*., "An Enhanced Authentication Protocol for RFID Systems," in *IEEE Access*, vol. 8, pp. 126977-126987, 2020**
2. Ju Wang, Omid Abari and Srinivasan Keshav, "Challenge: RFID Hacking for Fun and Profit", IEEE MobiCom, 2018.
3. P. Gope, J. Lee and T. Q. S. Quek, "Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831-2843, Nov. 2018
4. B. Song, J. Y. Hwang and K. -A. Shim, "Security Improvement of an RFID Security Protocol of ISO/IEC WD 29167-6," in *IEEE Communications Letters*, vol. 15, no. 12, pp. 1375-1377, December 2011, doi: 10.1109/LCOMM.2011.103111.111816.

What is ZigBee?

- A standard for mesh networking
  - Built on the IEEE 802.15.4 standard
  - Reliability through meshed connectivity
- Designed for low power applications
  - Very long battery life
- Low data rate
  - 20-250Kb/sec (depending on band)
- Very Secure
  - AES-128 encryption available
- Self configuring
  - Allows ad hoc networks
  - Ease of installation and configuration



Smart Home

ZigBee/IEEE 802.15.4 Market Feature

- Low power consumption
  - Transmit between 10 to 100 milliwatts (mW), which is 10 to 100 times less than traditional Bluetooth.
- Low cost, available upto 3$
- Low offered message throughput
- Supports large network orders (<= 65k nodes)
- Low to No-QoS guarantees
- Flexible protocol design suitable for many applications

IEEE 802.15.4 Basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - Channel Access is via Carrier Sense Multiple Access with collision avoidance and optional time slotting
  - Message acknowledgement and an optional beacon structure
  - Works well for
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
  - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries

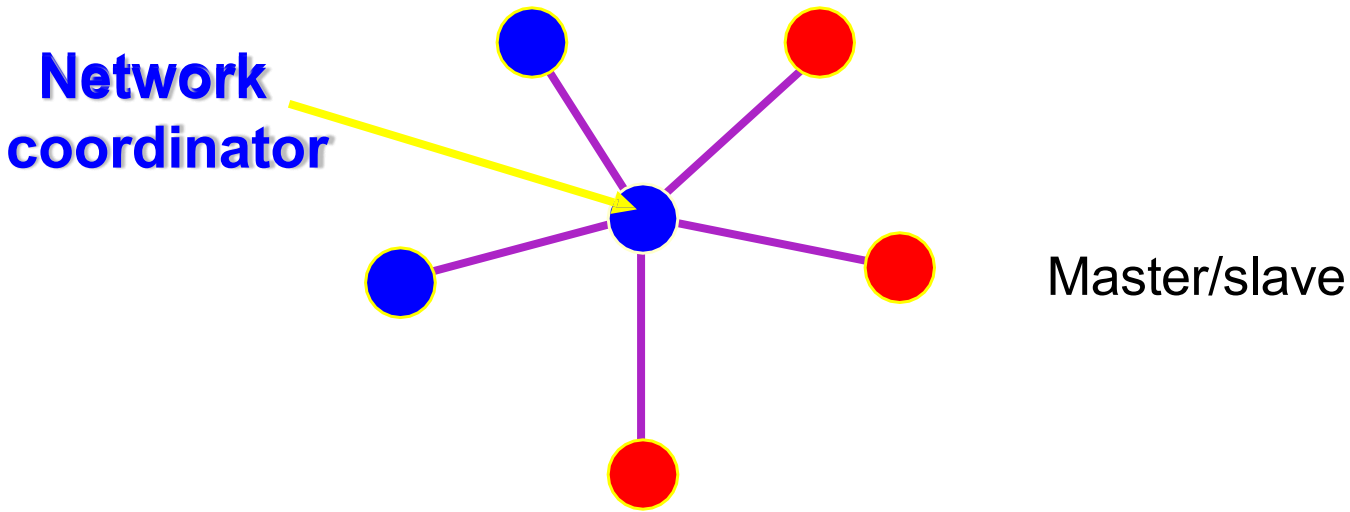
IEEE 802.15.4 Device Types

- There are two different device types :
  - A full function device (FFD)
  - A reduced function device (RFD)
- The FFD can operate in three modes serving
  - Device
  - Coordinator
  - PAN coordinator
- The RFD can only operate in a mode serving:
  - Device

FFD vs RFD

- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

Star Topology

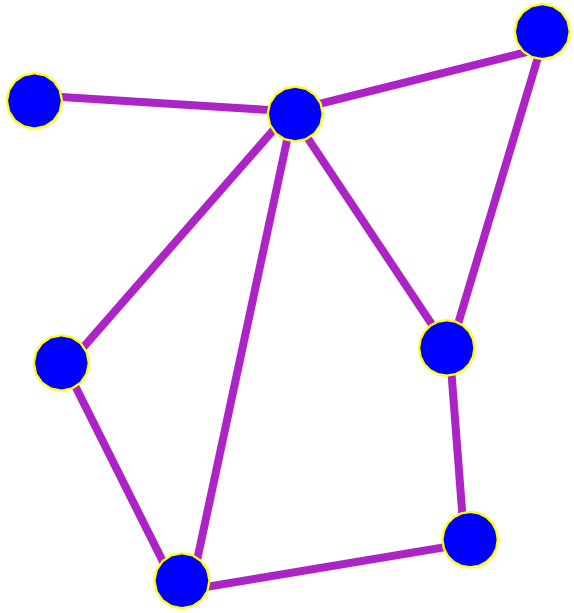


Full Function Device (FFD)

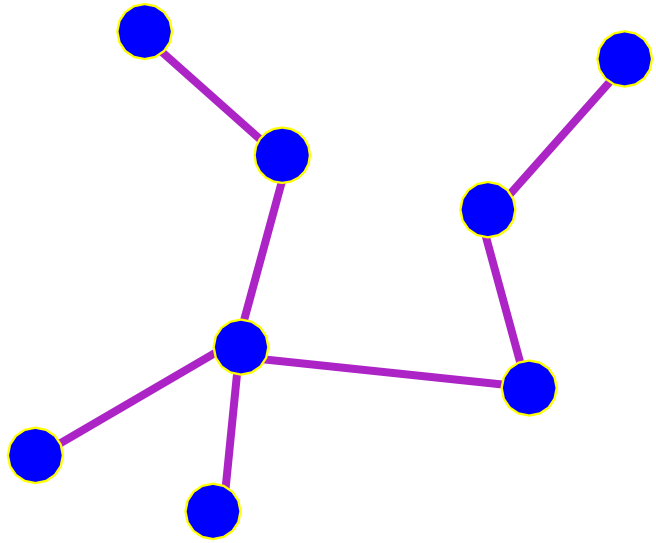
Reduced Function Device (RFD)

Communications Flow

Peer-Peer Topology



Point to point

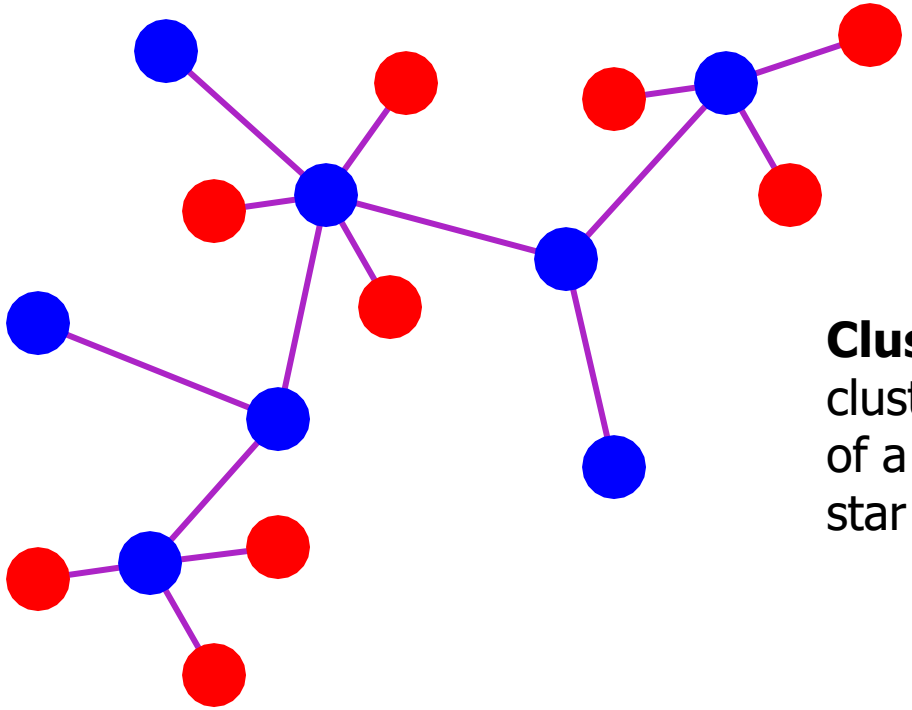


Tree

Full Function Device (FFD)

Communications Flow

Combined Topology



Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

Full Function Device (FFD)

Reduced Function Device (RFD)

Communications Flow

Device Addressing

- Each independent PAN will select a unique PAN identifier
- All devices operating on a network shall have unique 64-bit extended address. This address can be used for direct communication in the PAN
- A member can use a 16-bit short address, which is allocated by the PAN coordinator when the device is associated.
- Addressing modes:
  - star: Network (64 bits) + device identifier (16 bits)
  - peer-to-peer: Source/destination identifier (64 bits)
  - cluster tree: Source/destination cluster tree + device identifier (unclear yet)

Channel Access Mechanism

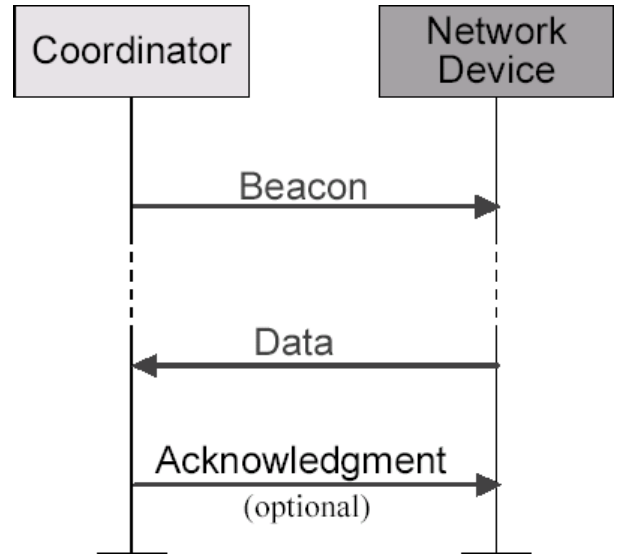
- Two type channel access mechanism, based on the network configuration:
  - In non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism
  - In beacon-enabled networks → slotted CSMA/CA channel access mechanism
    - The superframe structure will be used.
- The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator
  - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
- The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period

CSMA/CA Algorithm

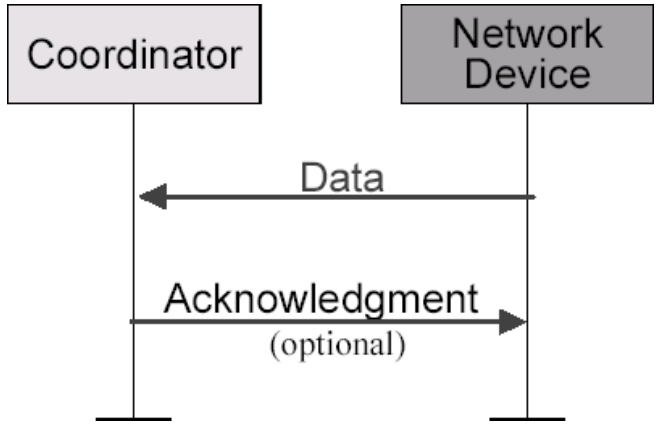
- Each device shall maintain three variables for each transmission attempt
  - NB: number of slots the CSMA/CA algorithm is required to backoff while attempting the current transmission.
  - BE: the backoff exponent which is related to how many backoff periods a device shall wait before attempting to assess a channel
  - CW: (a special design)
    - Contention window length, the number of backoff slots that needs to be clear of channel activity before transmission can commence.
    - It is initialized to 2 and reset to 2 if the channel is sensed to be busy.
      - So a station has to detect two CCA before contending.

Data Transfer Model

- Data transferred from device to coordinator
  - In a beacon-enable network, device finds the beacon to synchronize to the superframe structure. Then using slotted CSMA/CA to transmit its data.
  - In a non beacon-enable network, device simply transmits its data using unslotted CSMA/CA



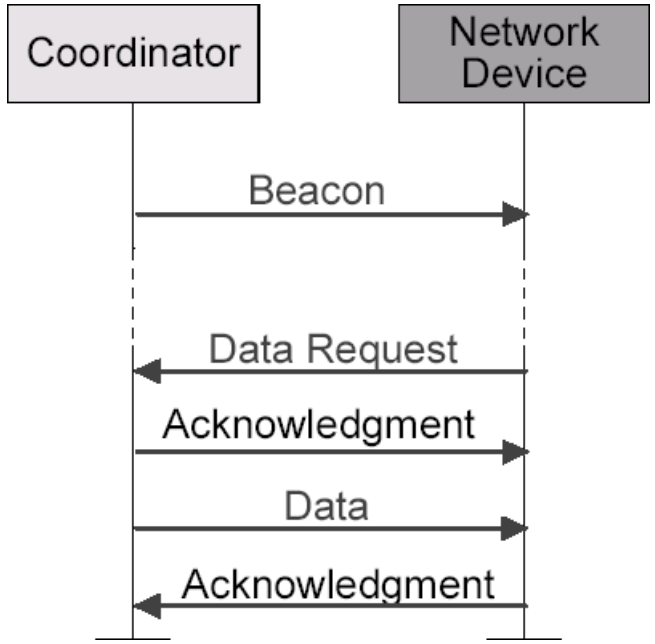
Communication to a coordinator



Communication to a coordinator
In a non beacon-enabled network

Data Transfer Model

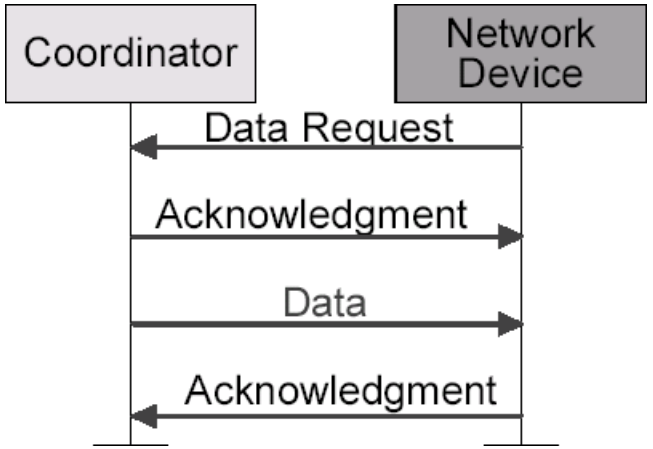
- Data transferred from coordinator to device
  - In a beacon-enable network, the coordinator indicates in the beacon that "data is pending."
  - Device periodically listens to the beacon and transmits a MAC command request using slotted CSMA/CA if necessary.



Communication from a coordinator
In a beacon-enabled network

Data Transfer Model

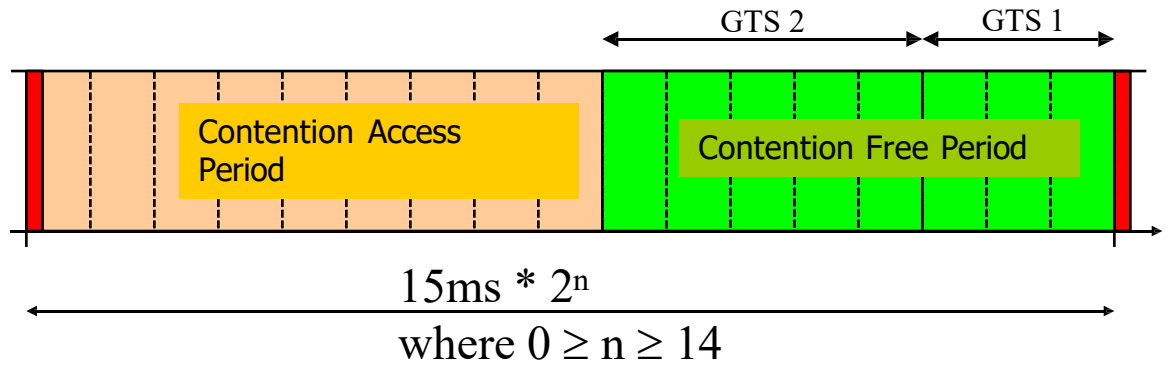
- Data transferred from coordinator to device
  - In a non beacon-enable network, a device transmits a MAC command request using unslotted CSMA/CA.
  - If the coordinator has its pending data, the coordinator transmits data frame using unslotted CSMA/CA.
  - Otherwise, the coordinator transmits a data frame with zero length payload.



Communication from a coordinator in a non beacon-enabled network

Superframe

- A superframe is divided into two parts
  - Inactive: all stations sleep
  - Active:
    - Period divided into 16 slots
    - 16 slots can further divided into two parts
      - Contention access period
      - Contention free period
      - (These slots are "MACRO" slots.)



Network beacon — Transmitted by network coordinator. Contains network information, frame structure and notification of pending node messages.

Contention period — Access by any node using CSMA-CA

Guaranteed Time Slot — Reserved for nodes requiring guaranteed bandwidth

Superframe Structure (cont.)

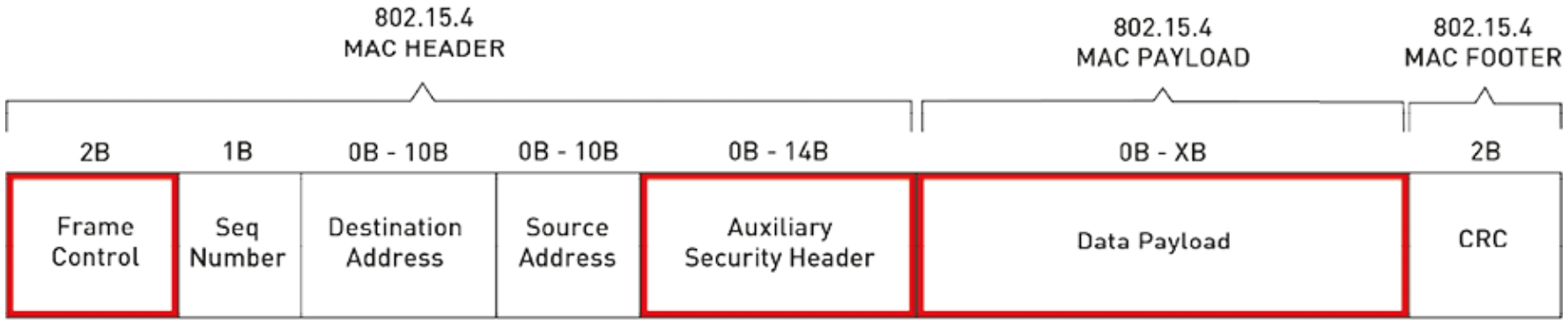
- There are two parameters:
  - SO(Superframe order): to determine the length of the active period
  - BO (Beacon order): to determine the length of the beacon interval.
- In CFP (contention free period), a GTS may consist of multiple slots, all of which are assigned to a single device, for either transmission (t-GTS) or reception (r-GTS).
  - GTS = guaranteed time slots
- In CAP, the concept of slots is not used.
- CAP= contention access period
  - Instead, the whole CAP is divided into smaller "contention slots".
  - Each "contention slot" is of 20 symbols long.
    - This is used as the smallest unit for contention backoff.
  - Then devices contend in a slotted CSMA/CA manner.

Security Models

- Centralized Security model: is complex but, the most secure model and involves a Trust center (network coordinator). The Trust center is responsible for:
  - Configuring and authenticating routers and end devices that join the network,
  - Generating network key to be used for encrypted communication across the network,
  - Periodically or as required switching to a new network key. Thus, if an attacker acquires a network key, it will have a limited lifetime before expiring,
  - Establishing a unique Trust Center link key for each device as they join the network to securely communicate with the Trust Center, and
  - Maintaining the overall security of the network.
- Distributed security model: is simple, but less secure.
  - This model supports only routers and end devices.
  - Routers form the distributed network are responsible for enrolling other routers and end devices.
  - Routers issue network keys (used to encrypt messages) to newly joined routers and end-devices.
  - All the nodes in the network use the same network key for encrypting messages. Also, all nodes are pre-configured with a link key (used to encrypt the network key) prior to being enrolled in the network.

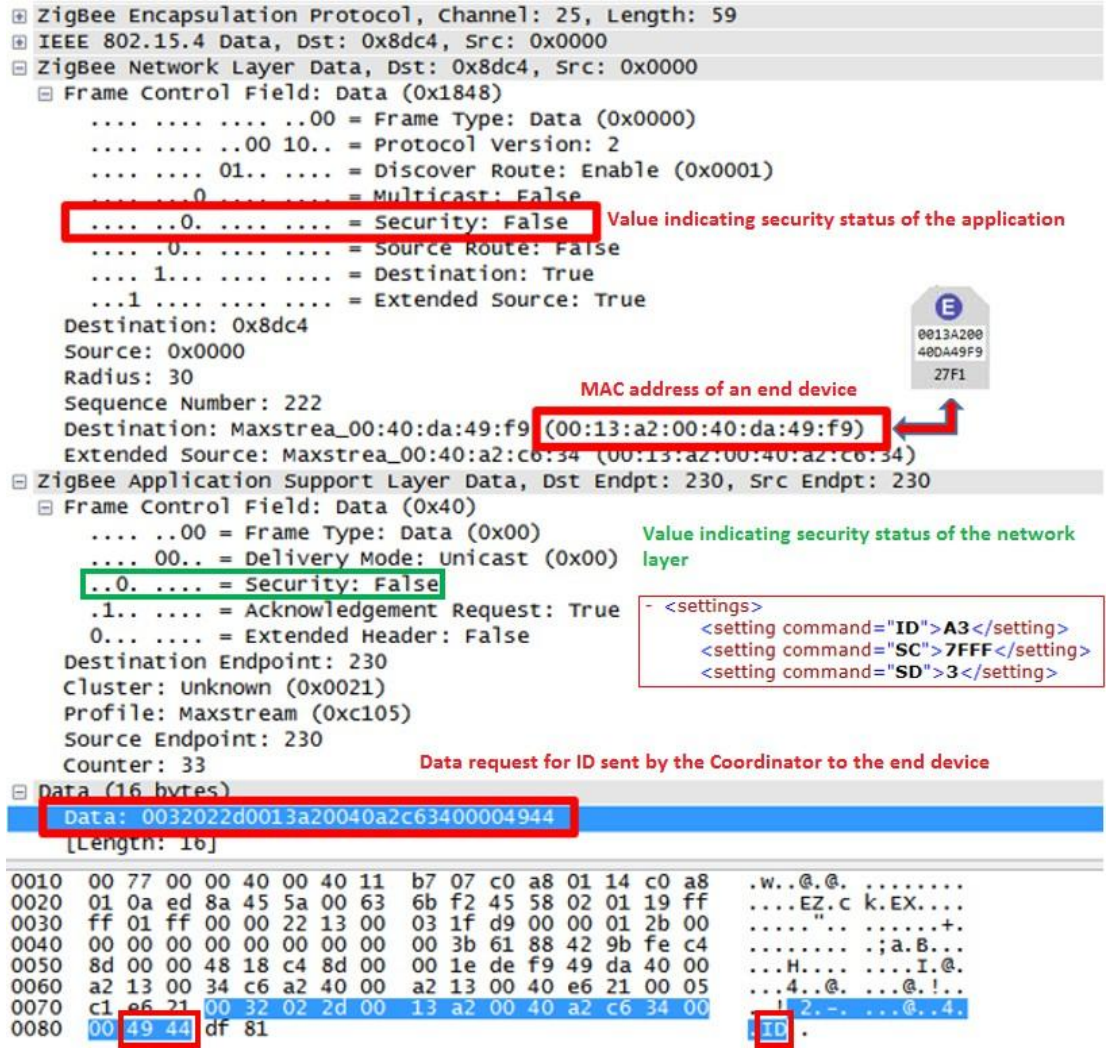
Data Encryption in ZigBee

- ZigBee security and data encryption is based on security defined in 802.15.4 protocol.
- ZigBee uses AES with a 128 bit key length (16 Bytes) for data encryption.
- AES based Message Authentication Code (MAC) is appended to the message. This code ensures integrity of the MAC header and payload data attached.
- The MAC can have different sizes: 32, 64, 128 bits, however it is always created using the 128 bit AES algorithm.
- The Auxiliary Security Header is only enabled if the Security Enabled subfield of the Frame Control Field is turned on.

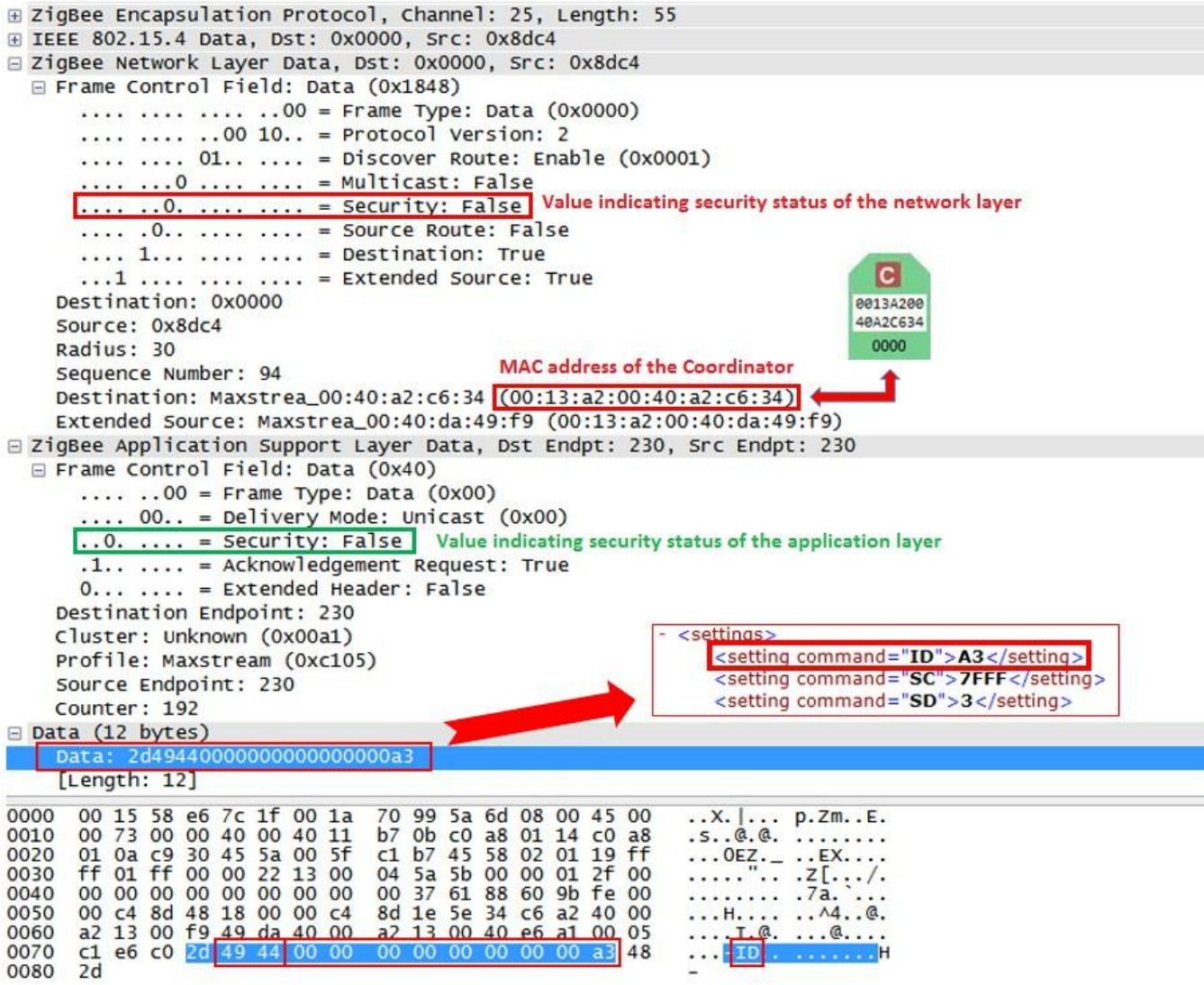


Wireshark capture

Coordinator Request to End Device



End Device to Coordinator



Security Keys

- There are three types of symmetric keys (each of length 128-bit) used in the ZigBee standard.
- Network key: is used in broadcast communication and applied by NWK and APL of ZigBee.
  - The trust center generates the network key and distributes it to all the devices on the network.
  - A device on the network acquires a network key via key-transport (used to protect transported network keys) or pre-installation.
  - There are two different types of network keys: standard (sending network key in the open), and high-security (network key is encrypted).
  - The type of network key controls how a network key is distributed.
- Link key: is used in unicast communication
  - A device acquires link keys either via key-transport, key-establishment (based on the "master" key and other network parameters), or pre-installation (for example, during factory installation).
  - Usually, link keys related to the Trust Center are pre-configured using an out-of-band method, for instance, QR code in the packaging, whereas the link keys between nodes are generated by the Trust Center and encrypted with the network key before sending it to the node.

Security Keys Contd.

- Each node may also have the following pre-configured link keys which would be used to derive a Trust Center link key
  - A default global trust center link key defined by the ZigBee Alliance has a default value of 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39 (ZigBeeAlliance09) and is used or supported by the device if no other link key is specified by the application at the time of joining.
  - A distributed security global link key, a manufacturer specific key used for interaction between devices from the same manufacturer.
  - Install code (All ZigBee devices can contain a unique install code) is a preconfigured link key, a random 128-bit number protected by a 16-bit cyclic redundancy check (CRC).
  - The Trust Center may require that each new device use a unique install code to join a centralized security network and the install code must match a code previously entered into the Trust Center out-of-band (i.e., QR code).
  - Once the install code is verified, the joining device and the Trust Center derive a unique 128-bit Trust Center Link Key from the install code using the Matyas-Meyer-Oseas (MMO) hash function
- Master key: It forms the basis for long-term security between two devices and is used only by the APS.
  - Its function is to keep the link key exchange between two nodes in the Symmetric-Key Key Establishment protocol (SKKE) confidential.
  - A device acquires a master key via key-transport, pre-installation or user-entered data such as PIN or password.

Key Management

- Pre-installation:
  - The manufacturer installs the key into the device itself. The user can select one of the installed keys by using a series of jumpers in the device (in devices where more than one key is preinstalled).
- Key establishment:
  - This is a local method of generating link keys based on the master key.
  - Different security services of the ZigBee Network use a key derived from a one-way function (with link key as the input) to avoid security leaks due to unwanted interactions between the services.
- Key transport:
  - The network device makes a request to the Trust Centre for a key to be sent to it.
  - This method is valid for requesting any of the three types of key in commercial mode
  - The key-load key is used by the Trust Center to protect the transport of the master key.
- Additionally, in the centralized model, keys can be distributed using Certificate-Based Key Establishment protocol (CBKE).

Vulnerabilities in ZigBee

- Vulnerabilities in the ZigBee network categorized into two categories
  - Protocol vulnerabilities
  - Poor implementation of protocol during product development.

Src: https://payatu.com/blog/zigbee-security-101/

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

- 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.

Protocol Vulnerabilities

- 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.

Bluetooth

- Bluetooth technology is a wireless communication standard that enables devices to communicate with each other over short distances.
- Bluetooth uses radio waves to transmit data between devices, typically over a range of up to 10 meters (33 feet).
- It is designed to be a low-power, low-cost communication protocol that can be used in a wide range of devices, from smartphones and laptops to smart home devices and wearables.
- Why this name?
  - It was taken from the 10th century Danish King Harald Blatand who unified Denmark and Norway.
- When does it appear?
  - 1994 – Ericsson study on a wireless technology to link mobile phones & accessories.
  - 5 companies joined to form the Bluetooth Special Interest Group (SIG) in 1998.
  - First specification released in July 1999.

Bluetooth Versions

- Bluetooth technology has evolved over the years, and several versions of the Bluetooth standard have been released, each with its own set of features and capabilities. Some of the most significant versions of Bluetooth are:
- Bluetooth 1.x: The first version of Bluetooth, released in 1999, provided basic wireless connectivity for devices such as phones, headsets, and computers. It had a limited range and data transfer rate.
- Bluetooth 2.x: Released in 2004, Bluetooth 2.x introduced Enhanced Data Rate (EDR) technology, which increased the maximum data transfer rate to 3 Mbps. It also added support for additional profiles such as A2DP and HFP.
- Bluetooth 3.x: Released in 2009, Bluetooth 3.x introduced High-Speed Bluetooth (HSB) technology, which allowed for faster data transfer rates up to 24 Mbps. It also added support for streaming multimedia content.

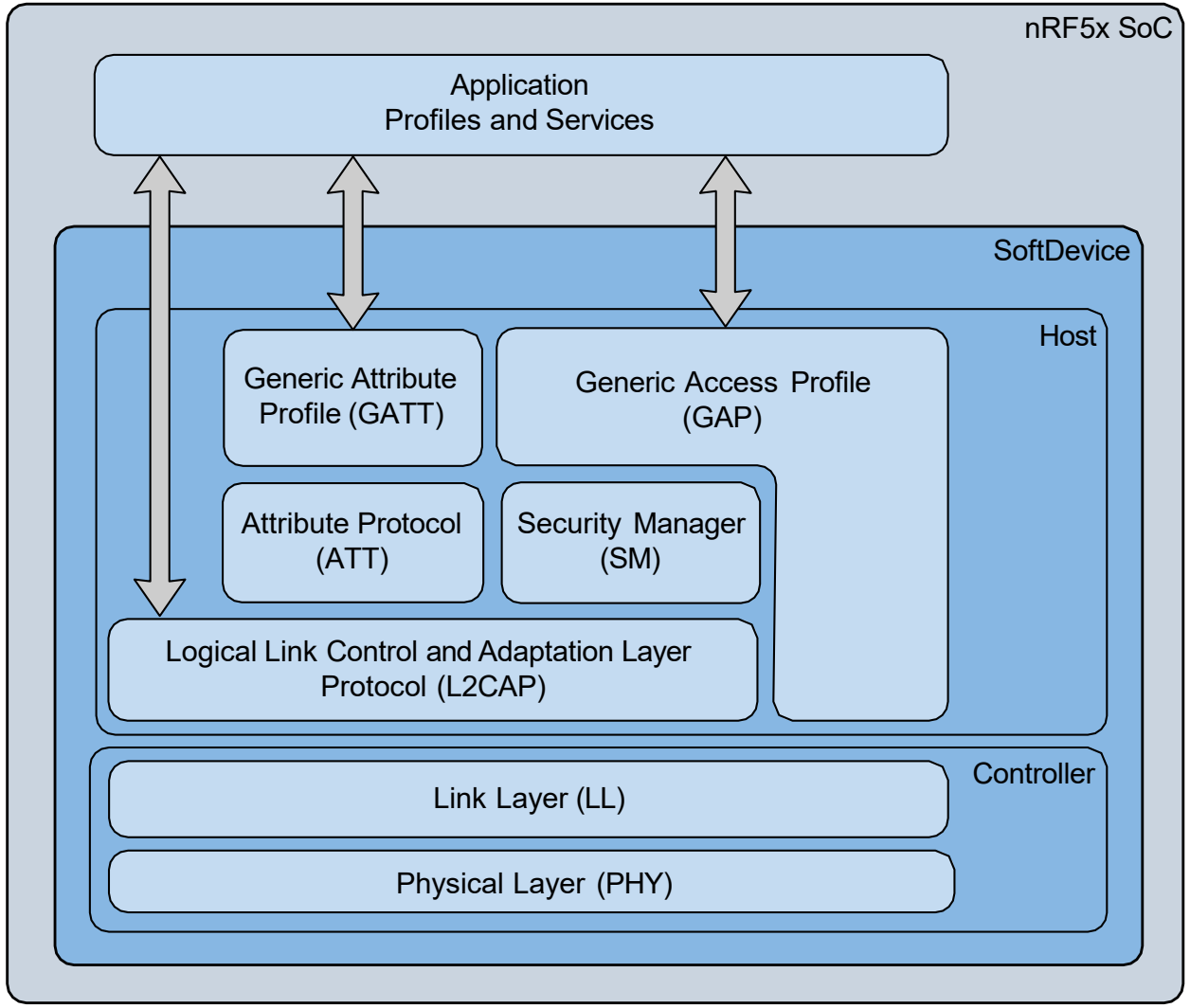
Bluetooth Versions

- Bluetooth 4.x: Released in 2010, Bluetooth 4.x introduced Bluetooth Low Energy (BLE) technology, which enables devices to operate on lower power and provides longer battery life. BLE is ideal for applications such as wearables, health monitoring, and smart home devices.
- Bluetooth 5.x: Released in 2016, Bluetooth 5.x introduced several improvements, including longer range, higher data transfer rates, and improved interoperability with other wireless technologies. Bluetooth 5.2 introduced features such as LE Audio and Bluetooth Mesh networking. The latest Bluetooth version is Bluetooth 6.0.
- The latest versions of Bluetooth provide faster data transfer rates, longer range, and improved battery life, making Bluetooth an essential technology for a wide range of applications, from smartphones and laptops to wearables and IoT devices.

Frequency Band

- Bluetooth technology uses the 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band for wireless communication.
- Within the 2.4 GHz ISM frequency band, Bluetooth technology uses a frequency hopping spread spectrum (FHSS) technique to avoid interference with other wireless technologies that also use the same frequency band, such as Wi-Fi and microwave ovens.
- The Bluetooth protocol divides the 2.4 GHz ISM frequency band into 40 channels, each with a bandwidth of 1 MHz The Bluetooth transceiver uses FHSS to hop between these 40 channels at a rate of 1600 hops per second

Bluetooth Architecture



Bluetooth Profiles

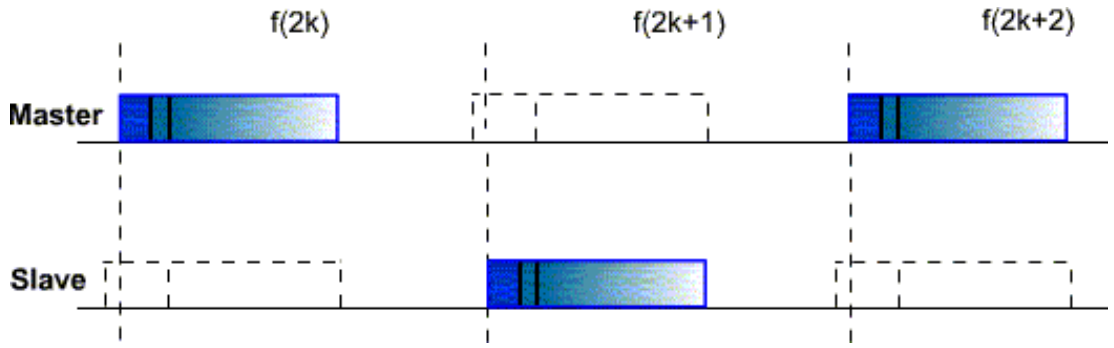
- Bluetooth profiles are standardized protocols that define how Bluetooth devices communicate with each other. Bluetooth profiles enable interoperability between different devices and applications, ensuring that devices can communicate with each other seamlessly.
- Some common Bluetooth profiles include:
  - Advanced Audio Distribution Profile (A2DP): A2DP is used for streaming high-quality audio from one device to another, such as streaming music from a smartphone to wireless headphones.
  - Hands-Free Profile (HFP): HFP is used for making and receiving phone calls wirelessly. It allows users to control their phone's call features, such as answering or ending a call, using buttons on a Bluetooth headset.
  - Human Interface Device (HID): HID is used for connecting input devices such as keyboards, and game controllers to computers or other devices wirelessly.
  - Object Push Profile (OPP): OPP is used for sending and receiving files between Bluetooth devices, such as photos or documents.
  - Serial Port Profile (SPP): SPP is used for establishing a virtual serial port between two Bluetooth devices, enabling serial communication between them.
  - Generic Attribute Profile (GATT): GATT is used in Bluetooth Low Energy (BLE) devices to exchange data between devices. It defines a hierarchical data structure that is used to organize data and services in a BLE device.

Key Functions in Bluetooth

- **Pairing:** The first step in using Bluetooth is to pair two devices together. This involves creating a secure link between the devices, so that they can communicate with each other.
- **Discovery:** Once two devices are paired, they can discover each other and establish a connection. This involves sending out radio signals to search for nearby devices that are also Bluetooth-enabled.
- **Connection:** After discovering each other, the two devices can establish a connection. This involves creating a communication channel between the devices, so that they can exchange data.
- **Data Transmission:** Once a connection is established, data can be transmitted between the devices. This can include audio, video, or any other type of data that is supported by the Bluetooth protocol.
- **Disconnection:** Finally, when the data transmission is complete, the devices can disconnect from each other. This involves terminating the communication channel and ending the Bluetooth connection.

Transmission and Networking in Bluetooth

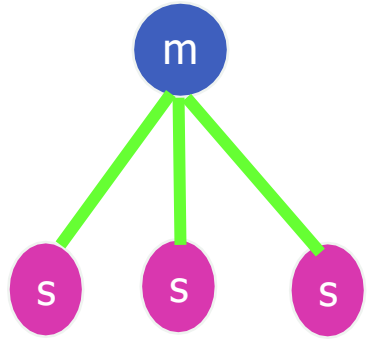
- Channel is divided into consecutive slots (each 625 μs)
- One packet can be transmitted per slot
- Subsequent slots are alternatively used for transmitting and receiving
  - Strict alternation of slots between the master and the slaves
  - Master can send packets to a slave only in EVEN slots
  - Slave can send packets to the master only in the ODD slots



Transmission and Networking in Bluetooth

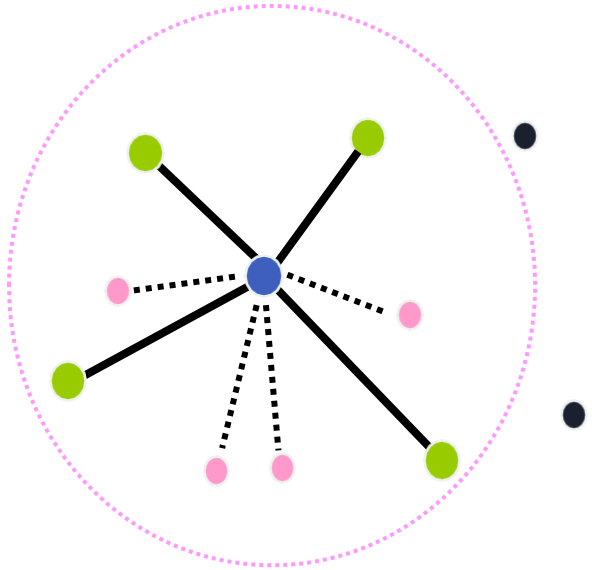
- Bluetooth will support wireless point-to-point and point-to-multipoint (broadcast) between devices in a piconet.
- Point to Point Link
  - Master - slave relationship
  - Bluetooth devices can function as masters or slaves

- Piconet
  - It is the network formed by a Master and one or more slaves (max 7)
  - Each piconet is defined by a different hopping channel to which users synchronize to
  - Each piconet has max capacity (1 Mbps)



Transmission and Networking in Bluetooth

- All devices in piconet hop together.
- Master's ID and master's clock determines frequency hopping sequence & phase.



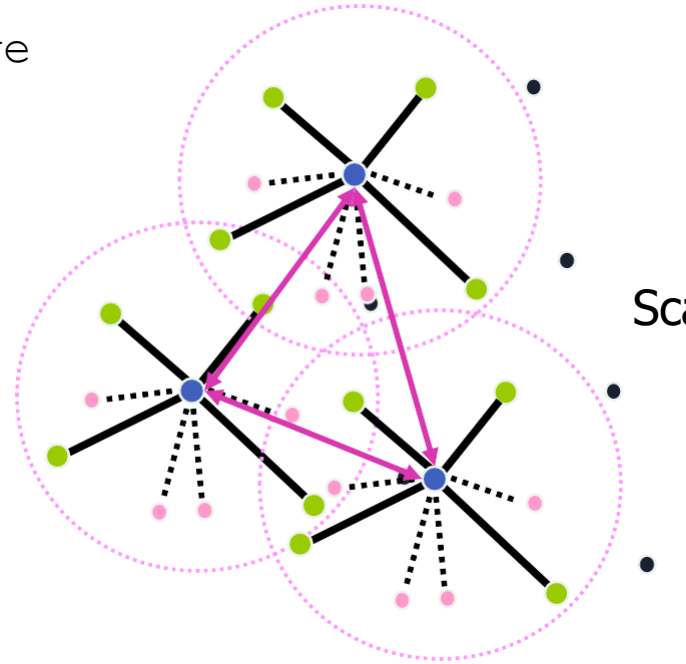
Piconet

Master

Active Slave

Parked Slave

Standby



Scatternet

Bluetooth VS Other Wireless Technology

Specifications	Bluetooth	RFID
Range	Up to 100m	A few cm to a few m
Data transfer rate	Up to 24 Mbps	Up to 424 Kbps
Power consumption	Requires battery	Lower power consumption, can be powered by reader
Cost	More expensive	Less expensive
Applications	Wireless audio, smartphone accessories, smart home devices	Asset tracking, inventory management, access control

Bluetooth VS Other Wireless Technology

Specifications	Bluetooth	WIFI
Range	Up to 100m	Up to 100m (depending on the protocol)
Data transfer rate	Up to 24 Mbps	Up to several Gbps
Power consumption	Lower power consumption	Higher power consumption
Security	Lower security compared to Wi-Fi	Higher security compared to Bluetooth
Cost	Generally less expensive	Generally more expensive
Applications	Wireless audio, smartphone accessories, smart home devices	High-speed internet access, streaming, file sharing, VoIP, gaming, etc.

Bluetooth VS Other Wireless Technology

Specifications	Bluetooth	NFC
Range	Up to 100m	Up to 10cm
Data transfer rate	Up to 24 Mbps	Up to 424 Kbps
Power consumption	Requires battery	Lower power consumption, can be powered by reader
Security	Higher security compared to NFC	Lower security compared to Bluetooth
Cost	Generally more expensive	Generally less expensive
Applications	Wireless audio, smartphone accessories, smart home devices	Mobile payments, access control, data sharing between mobile devices

Bluetooth Security

- Bluetooth security is designed to ensure that data transmitted wirelessly over Bluetooth is protected against unauthorized access or interception. Some key security features of Bluetooth technology include:
- Pairing: Bluetooth devices must be paired before they can communicate with each other. Pairing involves exchanging a security key between the two devices, which is used to encrypt all data transmitted between them.
- Encryption: Bluetooth uses strong encryption algorithms AES to protect data transmitted wirelessly. The encryption ensures that data can only be decoded by the intended recipient and prevents eavesdropping or data interception.
- Bluetooth Security Levels
  - **Security Level 1** supports communication without security at all, and applies to any Bluetooth communication, but think of it as applying to unpaired communications.
  - **Security Level 2** supports AES-CMAC encryption (aka AES-128 via RFC 4493, which is FIPS-compliant) during communications when the devices are unpaired.
  - **Security Level 3** supports encryption and requires pairing.
  - **Security Level 4** supports all the bells and whistles, and instead of AES-CMAC for encryption, ECDHE (aka Elliptic Curve Diffie-Hellman aka P-256, which is also FIPS-compliant) is used instead.

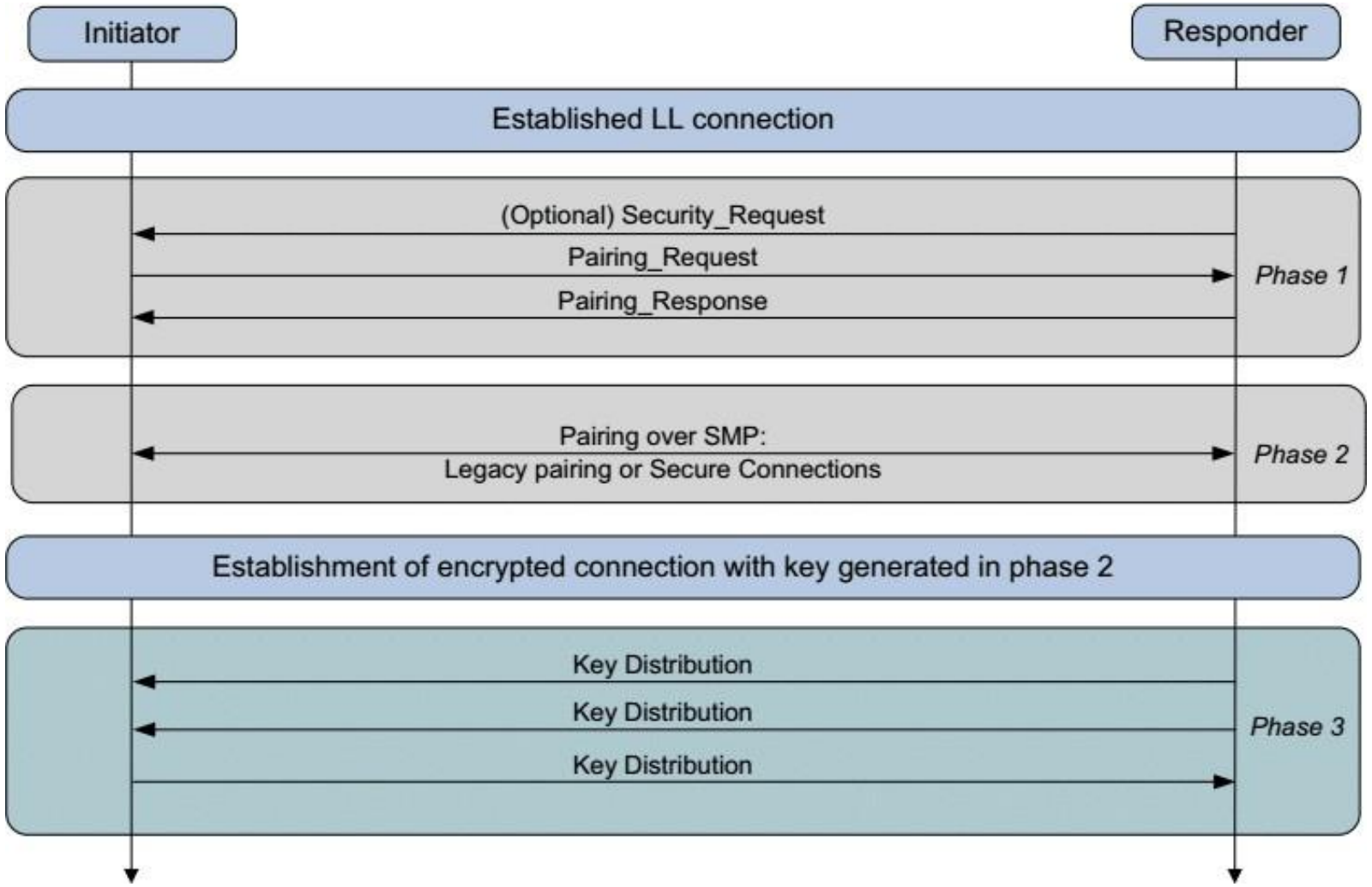
Bluetooth Security

- Authentication: Bluetooth devices must authenticate themselves to each other before data can be transmitted. Authentication involves verifying the identity of the device and ensuring that it has the necessary permissions to access the data.
- Authorization: Bluetooth devices can be configured to allow or deny access to specific services or data. Authorization ensures that only authorized devices can access sensitive data or services.
- Secure Simple Pairing (SSP): SSP is a feature introduced in Bluetooth v2.1 that enhances the security of pairing by using an out-of-band channel to exchange security keys. This approach ensures that the security key is not intercepted or compromised during the pairing process.
- There are two security modes: LE Security Mode 1 and LE Security Mode 2. You can mix levels and modes. there are two additional security modes named Mixed Security Mode and Secure Connection Only Mode.
  - **Security Mode 1** is those levels without signing of data
  - **Security Mode 2** is those same levels with signing of data, including both paired and unpaired communications.
  - **Mixed Security Mode** is when a device is required to support both Security Mode 1 and 2, i.e., it needs to support signed and unsigned data.

Bluetooth Pairing Phases

- Its purpose is to determine what the capabilities are on each end of the two devices getting ready to pair and then to get them actually talking to each other. The pairing process happens in three phases
- **Phase One**
  - The two devices let each other know what they are capable of doing. The values they are reading are Attribution Protocol (ATT) values. They determine the pairing method to be used in phase two.
- **Phase Two**
  - Purpose is to generate a Short Term Key (STK). This is done with the devices agreeing on a Temporary Key (TK) mixed with some random numbers which gives them the STK. With STK, this is commonly known as LE legacy pairing.
  - However, if the Secure Connection Only Mode is being used, a Long Term Key (LTK) is generated at this phase (instead of an STK), and this is known as LE Secure Connections.
- **Phase Three**
  - The key from phase two is used to distribute the rest of the keys needed for communications.
  - If an LTK wasn't generated in phase two, one is generated in phase three.
  - Data like the Connection Signature Resolving Key (CSRK) for data signing and the Identity Resolving Key (IRK) for private MAC address generation and lookup are generated in this phase.

Pairing Process



Pairing Methods

- There are four different pairing methods:
- **Numeric Comparison.**
  - Both devices display the same six digit value on their respective screens or LCD displays, and you make sure they match and hit or click the appropriate button on each device.
- **Just Works**
  - Not all devices have a display, such as headphones or a speaker.
  - The six-digit value is set to all zeros. While Numeric Comparison requires some on-the-fly math if you are performing a MITM attack, there is no MITM protection with Just Works.
- **Passkey Entry**
  - With Passkey Entry, a six-digit value is displayed on one device, and this is entered into the other device.
- **Out Of Band (OOB)**
  - A communication method outside of the Bluetooth communication channel is used.
  - The Apple Watch is a good example of this workflow. During the Apple Watch pairing method, a swirling display of dots is displayed on the watch face, and you point the pairing iPhone's camera at the watch face while (according to Apple) bits of information are transmitted via this process.
  - Another example is using Near Field Communication (NFC) between NFC-capable headphones and a pairing phone.

Bluetooth Vulnuerabilities

- Some of the most common Bluetooth security vulnerabilities today.
- Bluejacking
  - This type of cyber attack involves one Bluetooth-enabled device hijacking another and sending spam messages to the hijacked device.
  - Mostly it is an annoyance, but if a recipient falls for such a phishing attempt and clicks on a link in one of these spam messages, personal information is stolen or malware is installed.
- Bluesnarfing
  - A bluesnarfing attack is similar to bluejacking but more sinister. It also extracts information from your device. Data like text messages, photos, emails etc.
- Bluebugging
  - Hackers establish a surreptitious Bluetooth connection with your phone or laptop.
  - They then use this connection to gain backdoor access to your device.
  - Once in, they can spy on your activity, access your sensitive information, and even use your device to impersonate you on any apps on your device, including the apps you use for online banking.

Bluetooth Vulnuerabilities

- BlueFrag Leak (2020)
  - In 2020, ERNW discovered that on Android 8.0 to 9.0, an attacker in proximity to the targeted device could silently execute arbitrary code on the phone through Bluetooth as long as it was enabled. The vulnerability allowed hackers to steal personal data or spread a worm virus. The issue was patched in a security update by Google in February 2020.
- Bluewave Zero-Click Bugs (2020)
  - In 2020, a collection of security vulnerabilities in Apple's macOS Bluetooth system allowed hackers to take over devices through Bluewave Zero-Click Bugs. This means they were able to compromise a device even if the user didn't open a malicious link or attachment and even without contact with the device.
  - Apple released a security patch in 2020 and awarded the research team an award of $75,000 for discovering and reporting the vulnerabilities.
- BleedingTooth (2020)
  - In 2020, a researcher at Google discovered a set of Zero-Click vulnerabilities in the Linux Bluetooth subsystem called BlueZ. The vulnerability allowed a malicious actor in close proximity to execute arbitrary code with kernel privileges on vulnerable devices. Essentially taking over the device without the user's knowledge.
  - The Google researcher informed both BlueZ and the Linux Bluetooth Subsystem maintainers (Intel). Who later released security patches and integrated them into the Linux Kernel.

Bluetooth Vulnuerabilities

- Bluesmacking
  - Bluesmacking is a denial of service (DoS) attack designed to overwhelm your device and force a shutdown. Cybercriminals attack your device by sending oversized packets of data. Hackers will use bluesmacking as a gateway for more severe attacks once your device is shut down. In many cases, your device will return to normal once rebooted.
- Car whispering
  - Car whispering is a Bluetooth security vulnerability that targets car radios with Bluetooth capabilities. Hackers use this attack to eavesdrop on conversations and phone calls that take place inside the car. In other cases, the hackers may use the connection to inject audio into the car, oftentimes with malicious intent.
- Privacy Breach
  - Your location can be tracked using Bluetooth
  - When you turn off Bluetooth on your device's settings, it stops transmitting but still recognizes nearby Bluetooth signals. App makers use these Bluetooth signals to pinpoint your location.

Bluetooth Hacking Tools

- **Kali** once had several Bluetooth hacking tools built-in. In Kali 2020 we are down to just one, spooftooth. You can install others
  - **Bluelog:** A bluetooth site survey tool. It scans the area to find as many discoverable devices in the area and then logs them to a file.
  - **Bluemaho:** A GUI-based suite of tools for testing the security of Bluetooth devices.
  - **Blueranger:** A simple Python script that uses i2cap pings to locate Bluetooth devices and determine their approximate distances.
  - **Btscanner:** This GUI-based tool scans for discoverable devices within range.
  - **Redfang:** This tool enables us to find hidden Bluetooth device.
  - **Spooftooph:** This is a Bluetooth spoofing tool.