# Intrusion in IoT Devices

## Basics of Bluetooth

Abir, Aditya, Dhruv, Mihir, Mohak, Rajat

# Content Covered

1. **What is Bluetooth ?**
2. **Working of Bluetooth**
3. **Payload and Protocol Stack**
4. **Security**

# Bluetooth Basics - What is Bluetooth?

- An interface that allows device to communicate without cables
- It was built to connect the telecommunications protocol under one universal standard
- It is used for short range wireless communications and transmissions
- Simplifying communications between:
  - devices and the internet
  - data synchronization
- Omni directional, no requiring line of sight (which is needed in infrared)
- Bluetooth offers data speeds of up to 1 Mbps up to 10 meters (Short range wireless radio technology)
- The key limitations of Bluetooth are security and interference with wireless LANs.

# Bluetooth Networks

## PICONET

1. A piconet is a network created by connecting multiple wireless devices using Bluetooth technology. In a piconet network a master device exists.
2. It supports maximum 8 nodes i.e,1 master & 7 slaves.
3. It Allows less efficient use of Bluetooth bandwidth
4. It is a smaller coverage area

## SCATTERNET

1. Scatternet is a network which connects multiple piconets using Bluetooth and it acts as a master and another type of piconet acts as a slave.
2. It supports more than 8 nodes.
3. It Allows more efficient use of Bluetooth channel bandwidth.
4. It is a larger coverage area.

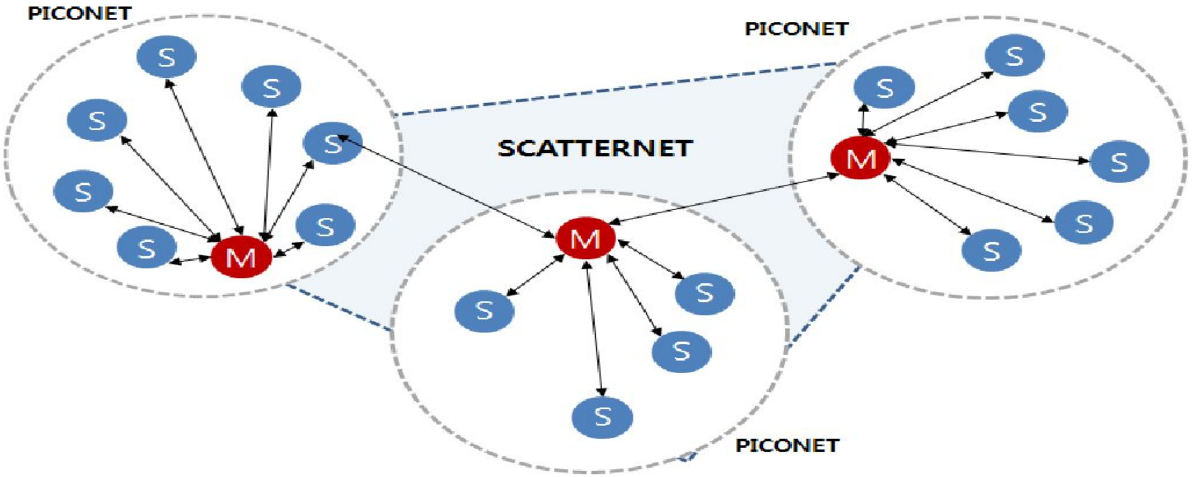
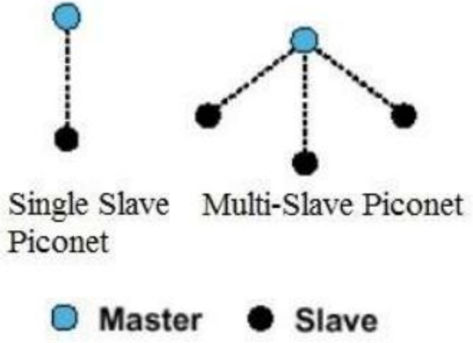


Figure 1. Bluetooth Piconet & Scatternet



# Encoding information (Quantization)

- Any information, say an analog ***<u>sound</u>*** waveform, can be encoded into ***<u>bits</u>***.

- Y-axis of waveform is divided into 2^(bit-depth) number of divisions, each corresponding to a particular range of displacements (which is the information we desire to transmit).

- Hence, each piece of information / each point on waveform ⇔ A binary number. High quality => higher bit depth.

- Discrete points are chosen at regular intervals on the waveform, and mapped onto one of the 2^(bit-depth) levels closest to it, and hence the waveform is encoded into many packets of (0s and 1s).

- Now, how are these strings of 0s and 1s transferred?

# How is information transferred? - Bluetooth Radio Layer

- These packets of 0s and 1s are sent via a particular ***channel*** to the receiver, where they are decoded to retrieve information.
- Each channel has 2 set frequencies - a higher f1 => "1", and a lower f2 => "0". The master sends out a wave of freq f1, in case a "1" has to be transferred.
- Usually, a ***master wave*** is sent out, whose frequency is slightly raised to f1, or, slightly decreased to f2. This is known as frequency "modulation".
- Typically, the band **2.4GHz - 2.4835Ghz** is divided into 79 smaller "channels" to transmit information.
- Packets need not be transferred through only a single channel. The entire bandwidth can be effectively used. The master decides the channel for each time slot, and conveys this to the slave. This is known as ***frequency hopping.***
- Frequency hopping helps prevent noise, makes the process more secure and reliable. A device could hop over 1600 times / sec between the channels.

# What exactly is transferred? - Access codes, Headers and Payload

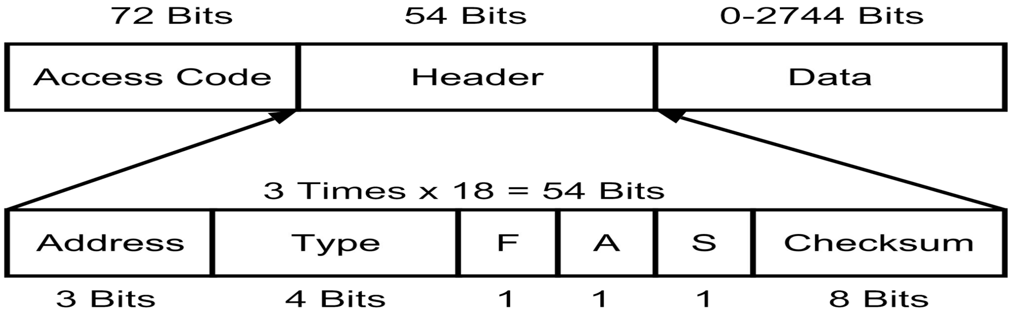
- The first 72 bits of each packet comprise the ***Access Code***, which makes sure the master is paired to the correct slave. Could be thought of as the “address” on a letter to be delivered.

- The next 54 bits comprise the ***header***, which contains the details of the incoming payload.

- The remaining bits in the packet are the actual data that has to be transferred, known as the ***payload***. The payload could be anywhere upto 2744 bits, depending on the size of information.

- The payload is decoded back to the original information by the receiver.

# Bluetooth Frame Format



72 Bits | 54 Bits | 0-2744 Bits

Access Code | Header | Data

3 Times x 18 = 54 Bits

Address | Type | F | A | S | Checksum

3 Bits | 4 Bits | 1 | 1 | 1 | 8 Bits

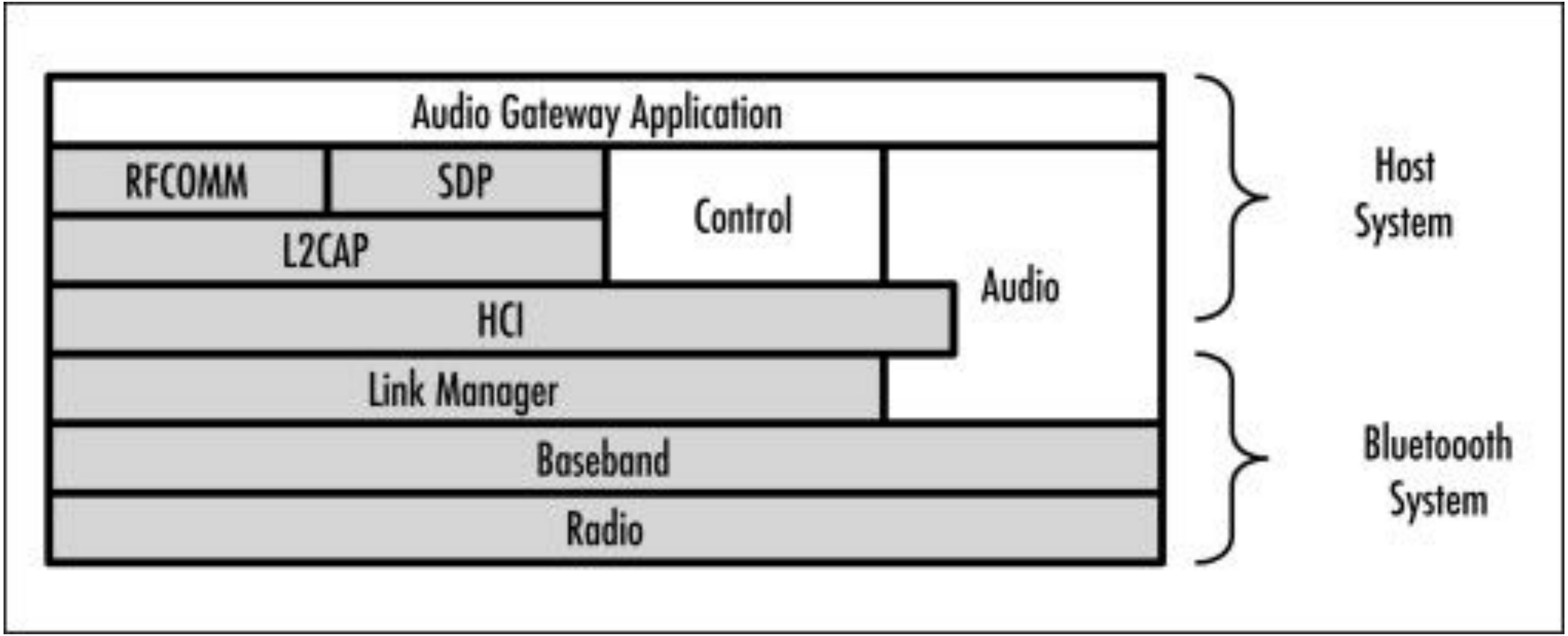
Bluetooth Frame Format

The various fields of bluetooth frame format are:

1. **Access Code**: It is 72 bit field that contains synchronization bits. It identifies the master.
2. **Header**: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time. The header field contains following subfields:
   a. **Address**: This 3 bit field can define upto seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.
   b. **Type**: This 4 bit field identifies the type of data coming from upper layers.
   c. **F**: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.
   d. **A**: This bit is used for acknowledgement.
   e. **S**: This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.
   f. **Checksum:** An 8-bit field containing checksum for error detection.

3. **Data**: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers

# Bluetooth Protocol Stack



# Bluetooth Protocol Stack

**Physical Radio(RF) Layer:** It performs modulation/demodulation of the data into Radio Signals. It defines physical attributes of bluetooth transceiver. This protocol specification defines air interface, frequency bands, frequency hopping specifications, modulation technique used and transmit power classes.
**Baseband Link Layer:** Addressing scheme, packet frame format , timing and power control algorithms required for establishing connection between bluetooth devices within piconet defined in this part of protocol specification.
**Link Manager protocol layer:** It performs the management of the already established link. It also includes authentication and encryption processes.Negotiation of packet sizes between devices can be taken care by this.
**Logical Link Control and Adaptation Layer (L2CAP):** It is the heart of bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers.
It also performs Segmentation and Multiplexing.

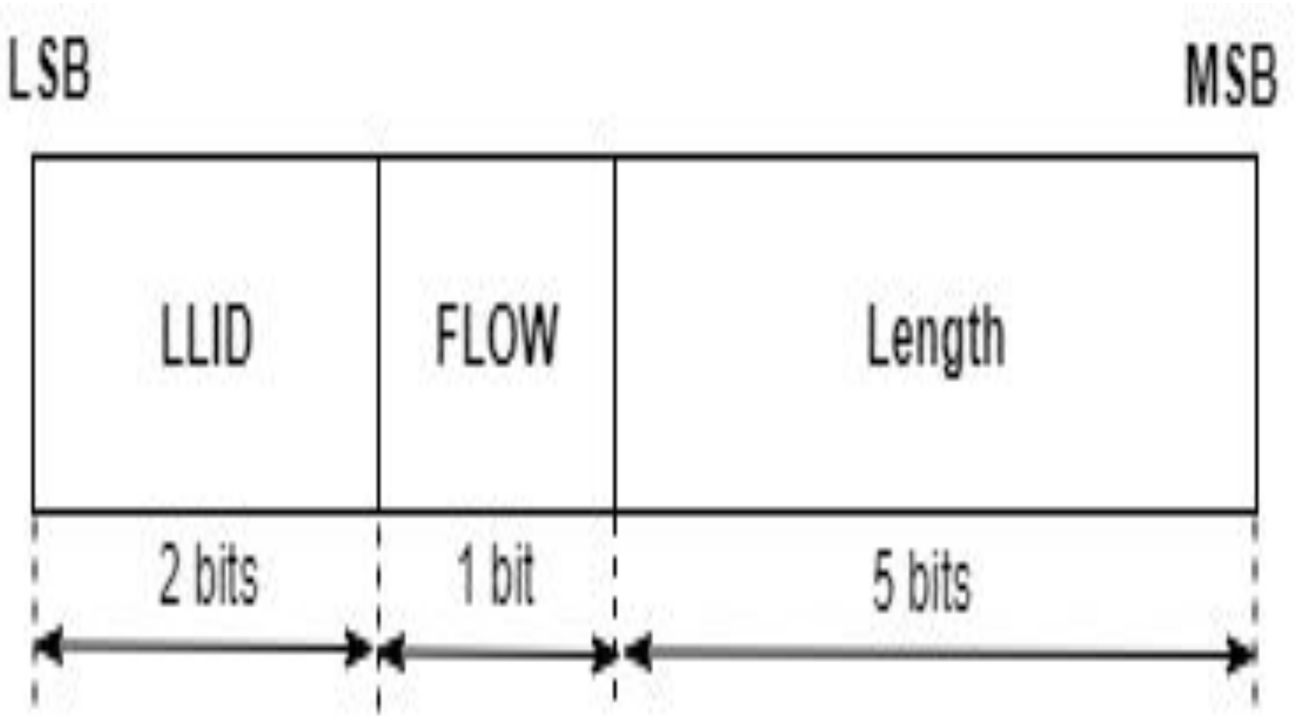
# Bluetooth Protocol Stack

**RFcomm Layer:** It is short for Radio Frequency Communication. It provides serial interface with WAP( Wireless Application Protocol) and OBEX( Object Exchange Protocol).
**OBEX:** It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.
**WAP:** It is short for Wireless Access Protocol. It is used for internet access.
**TCS:** It is short for Telephony Control Protocol. It provides Telephony services.
**SDP Layer:** It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device.
**Application Layer:** It allows the user to interact with the application.

# Payload Format

- The Bluetoot ı field
  (for ACL pack 'oice or
  DV packets c
- **Synchronous** ıous
  data field cor :.
- **Asynchronou**
  consisting of CRC
  (Cyclic Redur

This figure shows t : ACL
packets.



# VARIETY OF BLUETOOTH HACKING TECHNIQUES

- **BlueSmacking** BlueSmacking is a way to execute a Denial of Service attack against a Bluetooth-enabled device. It’s when a target such as a server or device gets way more data packets or oversized data packets than it’s designed to handle. The target gets overwhelmed, so it shuts down. Thankfully Denial of Service attacks are relatively minor as far as cyber attacks in general are concerned. You can usually recover from one by rebooting the targeted device. To get technical, a BlueSmack attack uses the L2CAP layer of Bluetooth’s networking stack to send a really oversized data packet.

- **Bluejacking**: This type of cyberattack on Bluetooth connection lies in sending spam messages via Bluetooth. One Bluetooth-enabled device hijacks another and sends spam messages to the hijacked device. The messages may contain a link that will lead to a website that is designed to steal your personal information and compromise you.

# VARIETY OF BLUETOOTH HACKING TECHNIQUES

- **Bluesnarfing:** During these hijacking attempts, hackers can not only send spam messages to one’s phone, but also collect some private information like chat messages, photos, documents, or even credentials from the victim’s device.
- **Bluebugging:** This is the most dangerous type of Bluetooth hijacking. Hackers use your device to establish a secret Bluetooth connection. This connection is then used to acquire backdoor access to your device. Once inside, they can monitor your activities, gain your personal information, and even use your personality on your device's apps, including those used for online banking.