IEEE 802.15.1 (Bluetooth)

Sachin Gajjar
sachin.gajjar@nirmauni.ac.in

Reading Material

- DATA COMMUNICATIONS AND NETWORKING, Fourth Edition by Behrouz A. Forouzan, Tata McGraw-Hill
  - Chapter 14 Wireless LANs
- Computer Networks by Andrew Tanenbaum
  - Chapter 4 , Topic 4.6
- https://www.bluetooth.com/

Introduction

- Wireless PAN standard to connect electronic devices of with different functions
- An ad hoc network, network is formed without infrastructure
- Devices, find each other and form a network
- PAN can be connected to Internet if one of the device has this capability

Bluetooth History

- Originally started as a project by Ericsson
- Ericsson wanted to connect devices to mobile phone without cables
- Named after Harald Blaatand, king of Denmark (940-981) who united Denmark and Norway
- Blaatand in Danish translates to Blue-tooth in English
- Defined by IEEE 802.15.1 standard

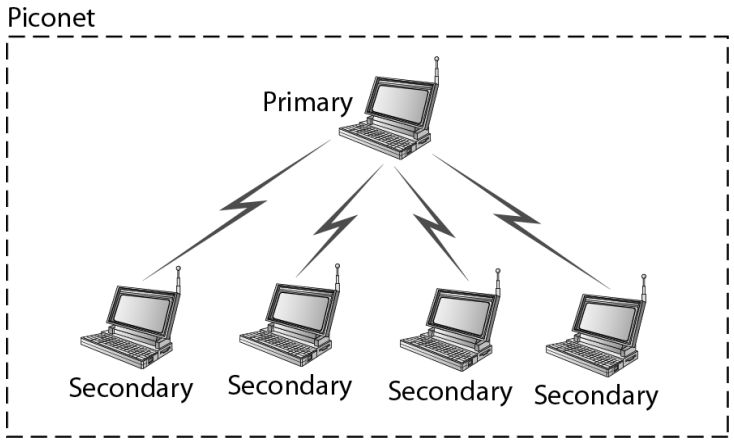
Architecture

- Bluetooth defines two types of networks:

1. Piconet
2. Scatternet

Piconets

- Can have up to eight stations, one is called primary; rest are called secondaries
- Secondary stations synchronize their clocks and frequency hopping sequence with the primary
- A piconet can have only one primary station
- Communication between primary and secondary can be one-to-one or one-to-many
- Primary - Master
- Secondary - Slave

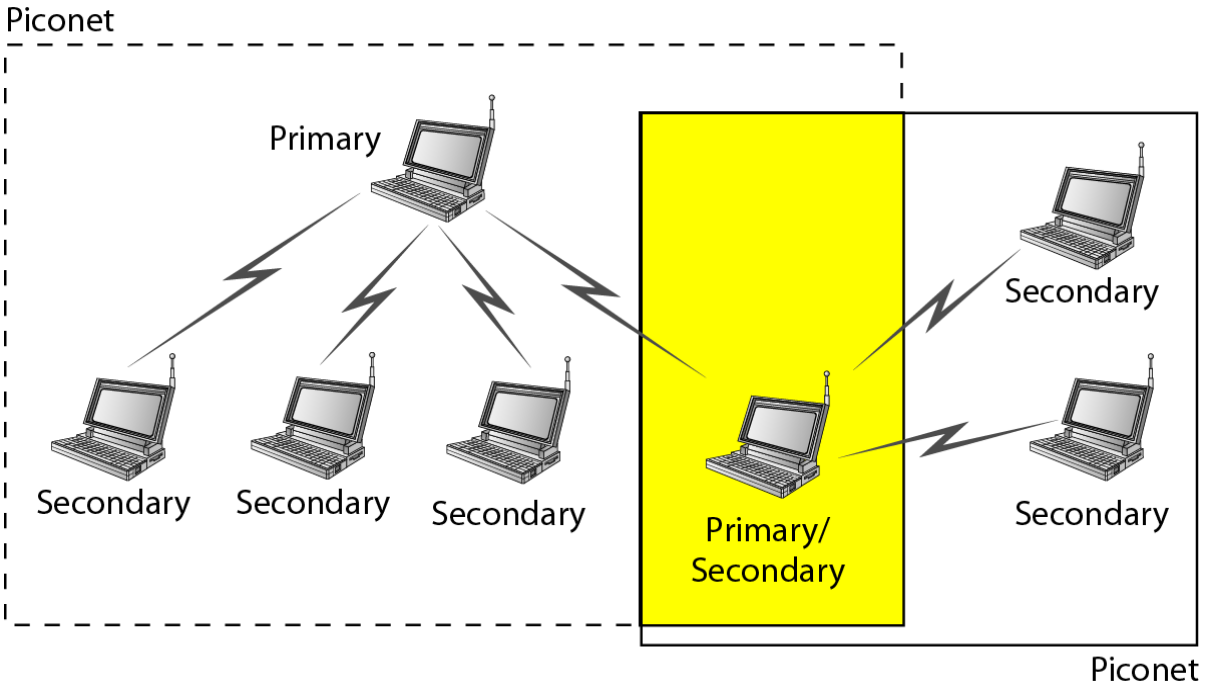


Piconets

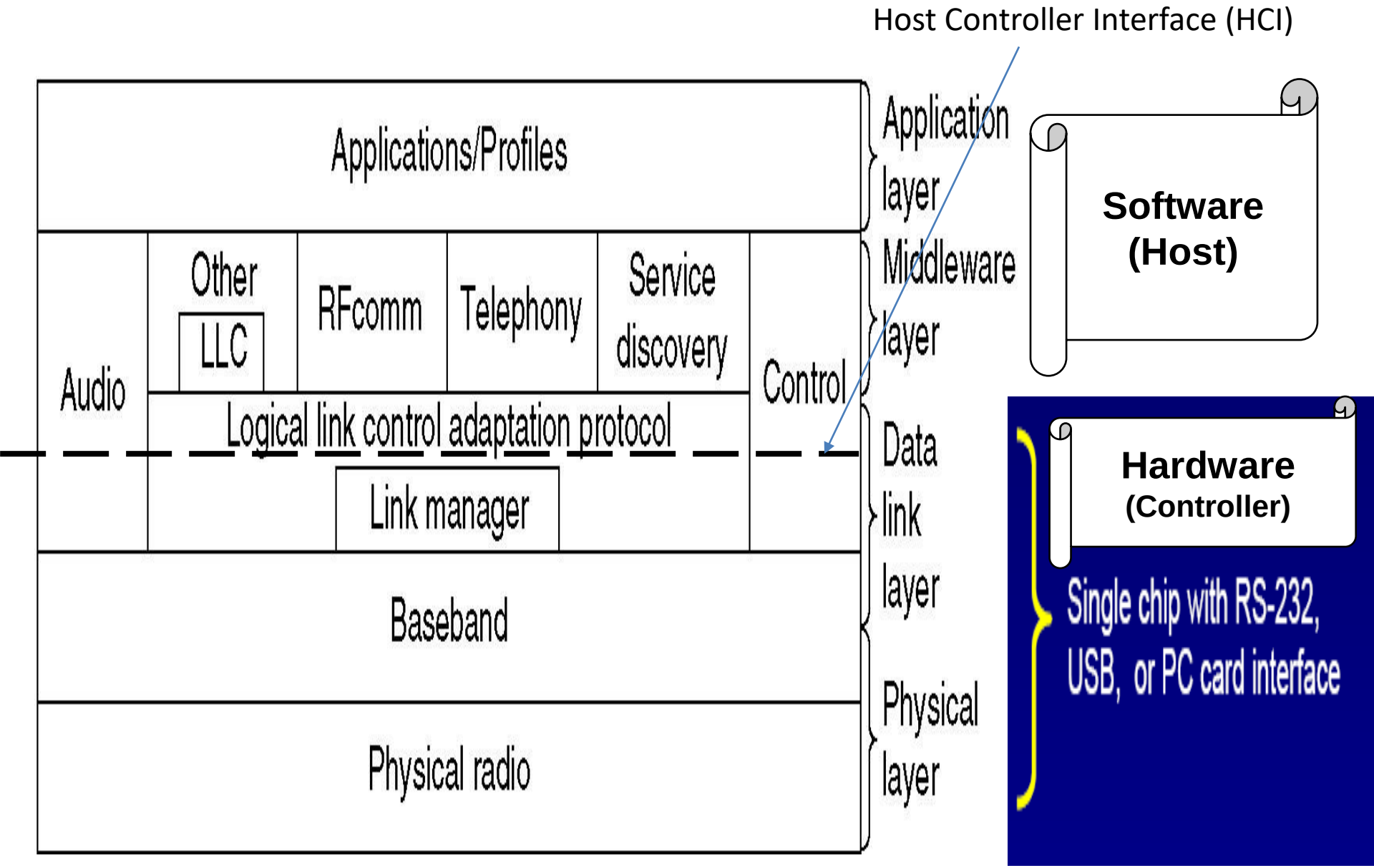
- An additional 8th secondary can be in *parked state*
- Secondary in parked state is synchronized with primary, but cannot take part in communication until it is moved from parked state
- Only eight stations can be active in a piconet
- Activating a station from parked state means that an active station must go to parked state

Scatternet

- Piconets can be combined to form a Scatternet
- Secondary station in one piconet can be primary in another piconet
- Receives messages from primary in first piconet (acts as secondary) and, delivers to secondary in second piconet (acts as a primary)
- A station can be a member of two piconets
- Primary - Master
- Secondary - Slave



Bluetooth Layers



Physical Radio Layer

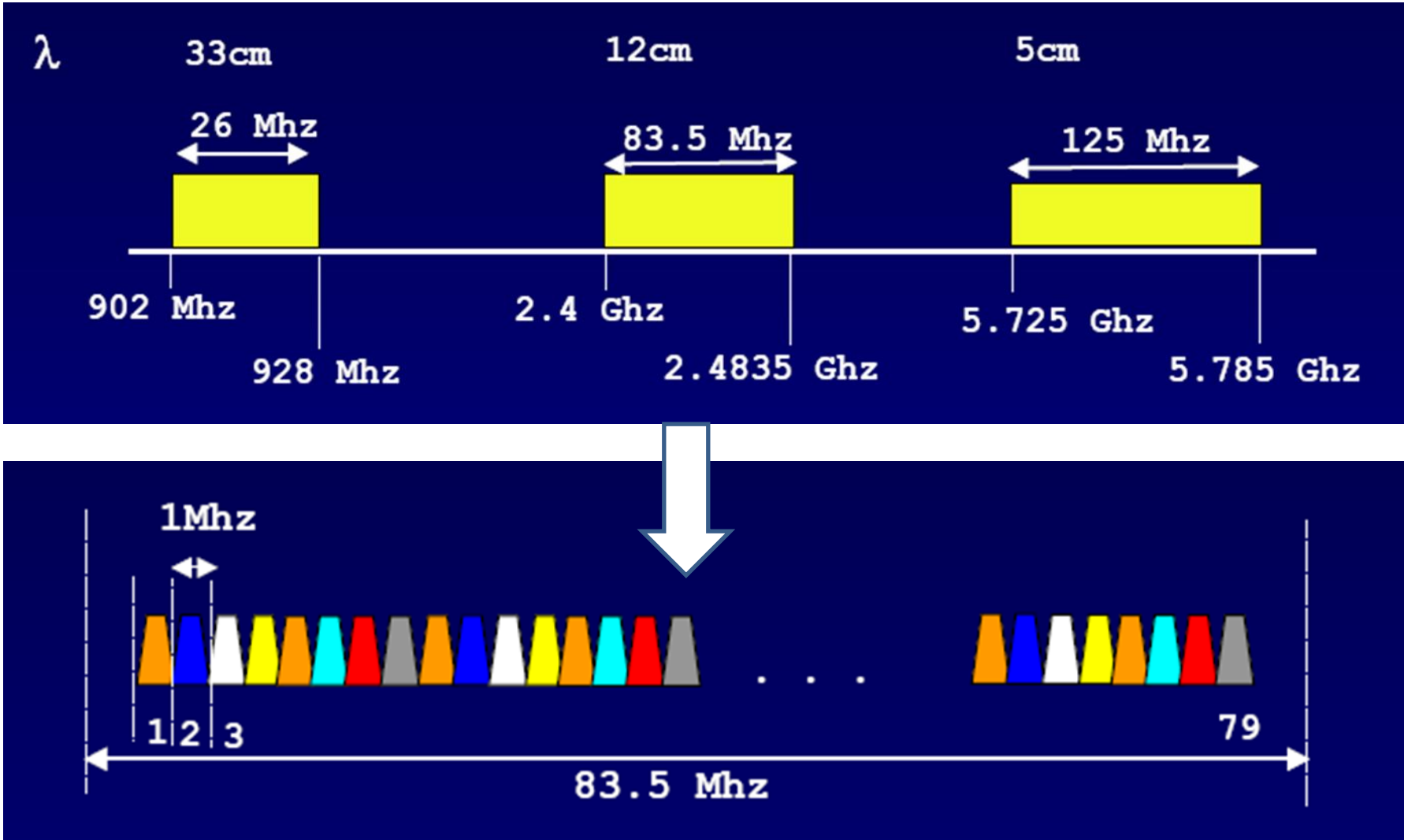
- Roughly equivalent to physical layer of TCP/IP
- Bluetooth devices are low-power and have a range of 10 m to 400 m

Major Bluetooth Versions

	BLUETOOTH V2.1	BLUETOOTH 4.0 (LE)	BLUETOOTH 5 (LE)
Range	Up to 100 m	Up to 100 m	Up to 400 m
Max range (free field)	Around 100 m (outdoors)	Around 100 m (outdoors)	Around 1,000m (outdoors)
Frequency	2.402 – 2.481 GHz	2.402 – 2.481 GHz	2.402 - 2.481 GHz
Topologies	Point-to-point	Point-to-point, mesh network	Point-to-point, mesh network

Band

- Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each



FHSS (frequency-hopping spread spectrum)

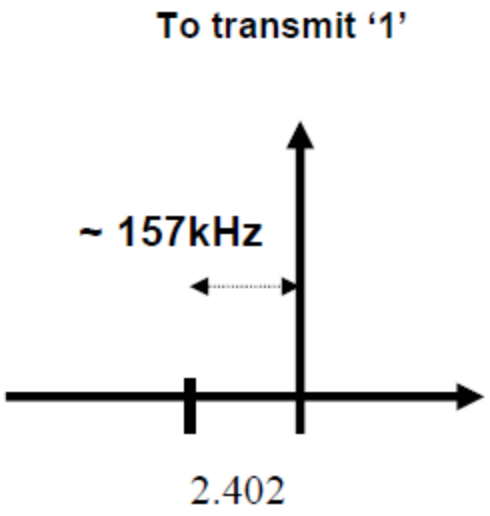
- Uses FHSS in physical layer to avoid interference from other devices/other networks
- Hops carrier frequency 1600 times per second, i.e. each device changes its modulation frequency 1600 times per second
- Pseudo-random hopping sequence dictated by primary
- Device uses a frequency for only 625 μs (1/1600 s) before it hops to another frequency; dwell time is 625 μs

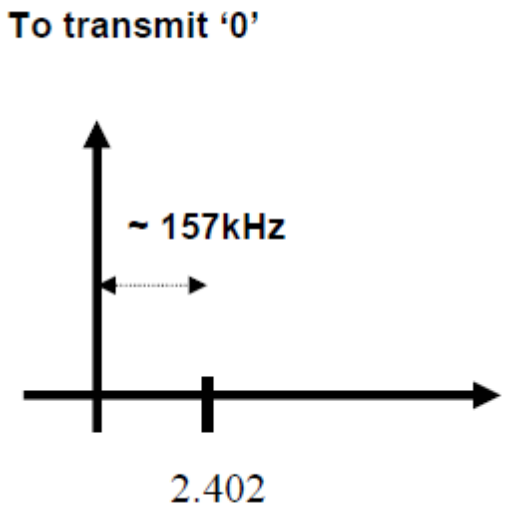
Modulation

- To transform bits to a signal, Bluetooth uses GFSK (FSK with Gaussian bandwidth filtering)
- GFSK has a carrier frequency
- Bit 1 is represented by a frequency deviation above carrier
- Bit 0 is represented by a frequency deviation below the carrier
- Frequencies, in megahertz, are defined according to following formula for each channel:

$$f_c = 2402 + n \quad (n = 0, 1, 2, 3, \ldots, 78)$$

- For example, first channel uses carrier frequency 2402 MHz (2.402 GHz), and the second channel uses carrier frequency 2403 MHz (2.403 GHz)





Baseband Layer

- Equivalent to MAC sublayer in LANs
- Frequency hop selection, connection creation, MAC
- The access method is TDMA
- The primary and secondary communicate with each other using time slots
- The length of a time slot is same as dwell time, 625 μs

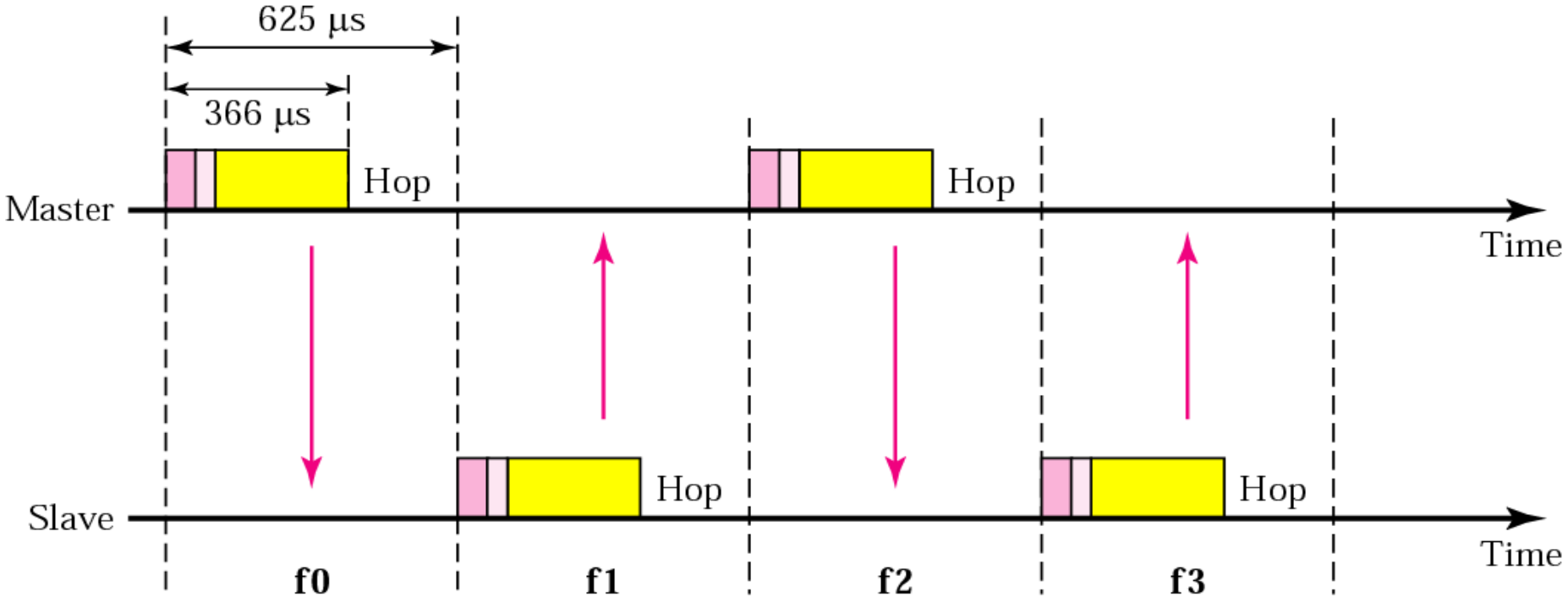
TDD-TDMA

- Uses a form of TDMA that is called TDD-TDMA (time division duplex TDMA)
- TDD-TDMA is a kind of half-duplex communication
- Secondary and primary send and receive data, but not at the same time
- Communication for each direction uses different slots
- Similar to walkie-talkies using different carrier frequencies

Single-Secondary Communication

- If the piconet has only one secondary, the TDMA operation is very simple
- The time is divided into slots of 625 μs
- The primary uses even numbered slots (0, 2, 4, ...)
- the secondary uses odd-numbered slots (1, 3, 5, ...)
- TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode
- In slot 0, primary sends, and secondary receives
- In slot 1, secondary sends, and primary receives
- The cycle is repeated

Single-Secondary Communication

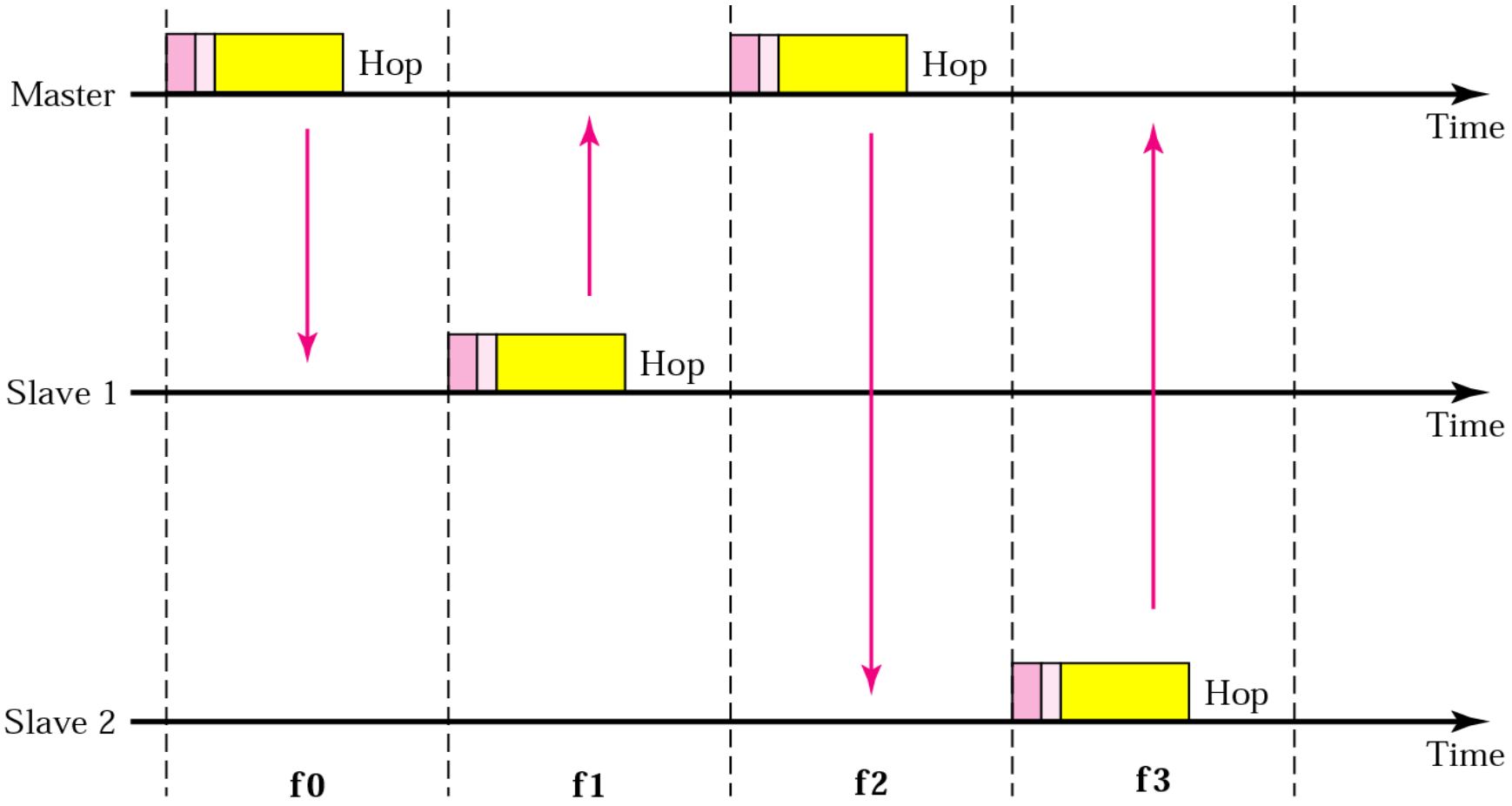


The primary uses even numbered slots (0, 2, 4, ...);
the secondary uses odd-numbered slots (1, 3, 5, ...)

Multiple-Secondary Communication

- More than one secondary in the piconet
- Primary uses even-numbered slots, but a secondary sends in next odd-numbered slot if the packet in the previous slot was addressed to it
- All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot
- Thus it is a poll/select operation with reservations

Multiple-Secondary Communication



All secondaries listen on even-numbered slots, but only one secondary (who is polled by primary) sends in any odd-numbered slot

- As in the figure.
  1. In slot 0, the primary sends a frame to secondary 1.
  2. In slot 1, only secondary 1 sends a frame to the primary because the previous frame was addressed to secondary 1; other secondaries are silent
  3. In slot 2, the primary sends a frame to secondary 2
  4. In slot 3, only secondary 2 sends a frame to the primary because the previous frame was addressed to secondary 2; other secondaries are silent
  5. The cycle continues
- This access method is similar to a poll/select operation with reservations
- When the primary selects a secondary, it also polls it
- Next time slot is reserved for the polled station to send its frame
- If the polled secondary has no frame to send, the channel is silent

Physical Links

- Two types of links can be created between a primary and a secondary:

1. Synchronous Connection Oriented (SCO) links
2. Asynchronous Connectionless (ACL) links

Synchronous Connection Oriented (SCO) links

- Used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery) eg. audio
- A physical link is created between the primary and a secondary by reserving specific slots at regular intervals
- The basic unit of connection is two slots, one for each direction
- If a packet is damaged, it is never retransmitted
- A secondary can create up to three SCO links with the primary, sending digitized audio (PCM) at 64 kbps in each link

Asynchronous Connectionless (ACL) links

- Used when data integrity is more important than avoiding latency eg. file transfer
- if a payload encapsulated in the frame is corrupted, it is retransmitted
- ACL can use one, three, or five slots and can achieve a maximum data rate of 721 kbps

Each transmission slot in Bluetooth is 625 μs long. A voice data of type HV3 takes one slot every 3.75 ms (625 μs x 6, i.e. takes every 6^{th} slot) for transmission and consists of 30 bytes of data with no error correction. Calculate the time taken to transmit 300 bytes of voice data over this configuration

Data: Time
30 bytes : 3.75 ms
300 bytes : ?

300 Byte transmission will take = $3.75ms \times 300/30 = 37.5\ ms$

Logical Link Control and Adaptation Protocol (L2CAP)

- Roughly equivalent to the LLC sublayer in LANs
- It is used for data exchange on an ACL link
- SCO channels do not use L2CAP – why waste time?
- Does multiplexing, framing, segmentation and reassembly, quality of service (QoS), group management

Multiplexing

- At sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer
- At receiver site, it accepts a frame from the baseband layer, extracts data, and delivers them to appropriate protocol layer
- Creates a virtual channel

Segmentation and Reassembly

- Maximum size of the payload field in the baseband layer is 2774 bits or 343 bytes
- This includes 4 bytes to define the packet and packet length
- Therefore, size of packet that can arrive from an upper layer can only be 339 bytes (343-4)
- However, application layers sometimes need to send a data packet that can be up to 65,535 bytes (Internet packet)
- L2CAP divides these large packets into segments and adds extra information to define location of segments in original packet
- The L2CAP segments the packet at the source and reassembles them at the destination

Quality of Service (QoS)

- Bluetooth allows the stations to define a quality-of-service level
- QoS parameters are: peak bandwidth, latency, delay variation when link is established between two devices
- If no quality-of-service level is defined, Bluetooth defaults to - *best-effort service; it will do its best* under the circumstances

Group Management

- allow devices to create a type of logical addressing between themselves
- similar to multicasting
- two or three secondary devices can be part of a multicast group to receive data from primary

Link Manager Protocol

- Power management
- Modes of operation
- Active mode
  - Bluetooth device actively participates in piconet
  - Active slaves are polled by master for transmission

Link Manager Protocol

- Sniff mode
  - Low power mode
  - Listening activity of slave is reduced
  - Master sends commands to slave to enter sniff mode & gives sniff interval
  - Slave listens for transmission at these fixed intervals

Link Manager Protocol

- Hold mode
  - –Slave temporarily does not support ACL packets in channel
  - –SCO links (real time transmission) still be supported

Link Manager Protocol

- Park mode
  - Low power mode
  - Slave gives Active Member address
  - Given an 8 bit Parked address
  - Slave remains in synchronization to channel
  - receives message send through broadcast channel (address = all 0s)
  - To have more than 7 slaves

Host Controller Interface

- Optional interface layer, for accessing Bluetooth hardware capabilities
- Host (gives command to controller)->HCI->Bluetooth controller
- Whenever the higher layers are implemented on the motherboard of a host device, this layer is needed.
- Acts as a Bluetooth device/controller translator for host (eg. PC)
- The specification defines details such as
  - Command packets used by host (eg. PC) to control device/controller
  - Event packets used by device to inform host of changes, and data packets

Middleware Protocol Group

- Applications use application programming interfaces (APIs) or higher level functions provided by middleware protocols
- Applications need not know the transport layer complexities
  - RFCOMM
  - Service Discovery Protocol (SDP)
  - IrDA interoperability protocols
  - Telephony control specification (TCS)
  - Audio

RFCOMM

- RFCOMM layer presents a virtual serial port to applications using the serial interface.
- Application that uses serial interface ->RFCOMM ->Bluetooth lower layers (L2CAP, Link Manager, Baseband, Radio)
- Any application which is using the serial port can work seamlessly on Bluetooth devices.

Service Discovery Protocol (SDP)

- In Bluetooth devices services offered by other devices have to be discovered.
- This is achieved by using service discovery protocol (SDP) of the Bluetooth protocol stack.
- Service discovery makes the device self-configured without manual intervention.

IrDA

- IrDA interoperability protocol is for the existing IrDA applications to work on Bluetooth devices without any changes
- IrDA application -> IrOBEX/IrMC -> Bluetooth controller
- Main protocols set are:
  - IrOBEX (IrDA object exchange) for exchanging objects between two devices
  - IrMC (infrared mobile communications) for synchronization.

Audio

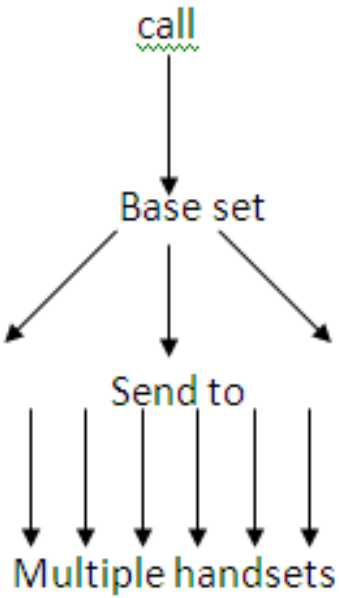
- Audio is given highest priority and is directly carried over baseband at 64 Kbps so that a very good quality of voice is provided.
- Audio is not a layer of protocol stack, but a specific packet format that can be transmitted directly over SCO links of the baseband layer.

Telephony control specification binary (TCS-BIN)

- Telephony control is implemented using the telephony control specification binary (TCS-BIN) protocol.
- TCS defines three major functional areas: call control, group management, connectionless TCS.
- Call control is used to set up calls which can be subsequently used to carry voice and data traffic.
- TCS operates in both point-to-point and point-to-multipoint configurations.

Telephony Control Specification Binary (TCS-BIN)

- Group management enables multiple telephone extensions, call forwarding, and group calls.
- Example, multiple handsets and a single base set.
- When a call comes in to the base set, all the multiple handsets can receive this call.

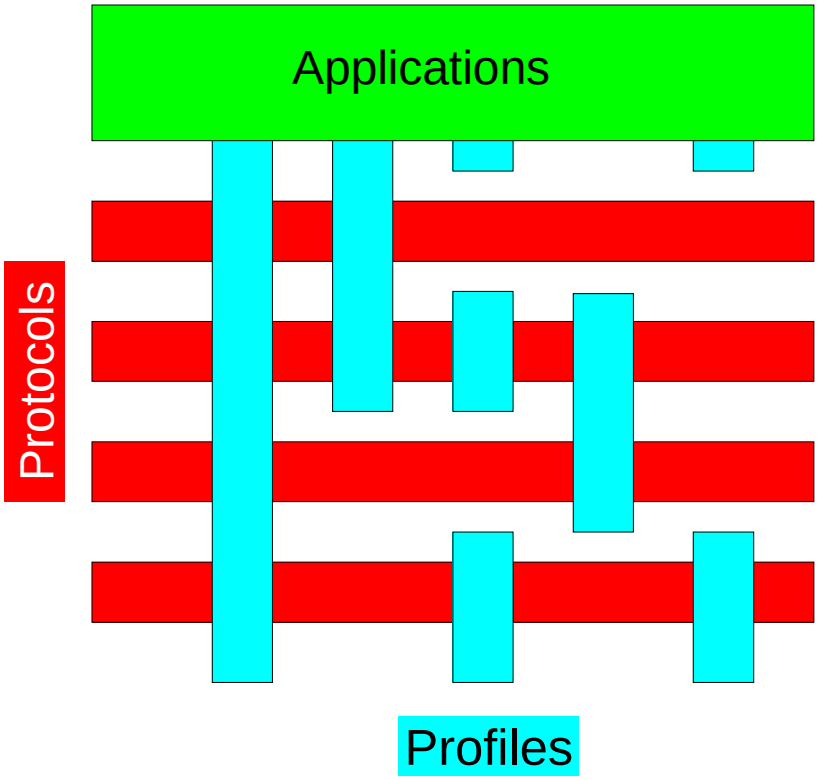


Bluetooth profiles

- Profiles are developed to promote interoperability among the many implementations of the Bluetooth protocol stack.
- Each profile specification provides a clear and transparent standard to implement a specific user end function.
- Two Bluetooth devices can achieve a common functionality only if both devices support identical profiles.

Interoperability & Profiles

- Represents default solution for a usage model
- Vertical slice through the protocol stack
- Basis for interoperability and logo requirements
- Each Bluetooth device supports one or more profiles

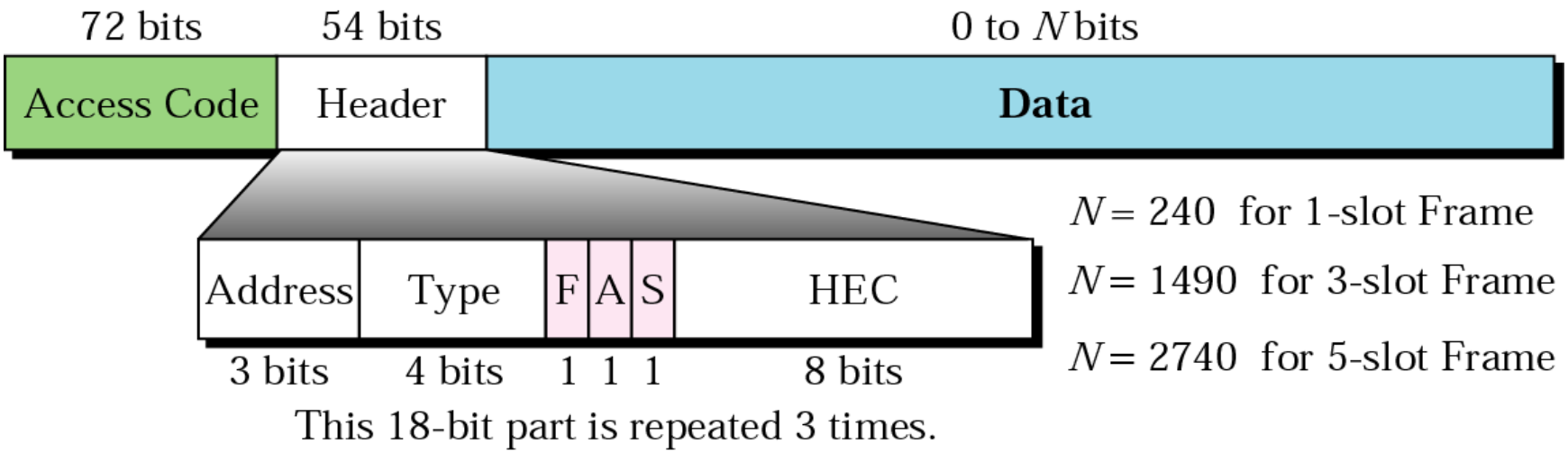


Bluetooth profiles

Name	Description
Generic access	Procedures for link management
Service discovery	Protocol for discovering offered services
Serial port	Replacement for a serial port cable
Generic object exchange	Defines client-server relationship for object movement
LAN access	Protocol between a mobile computer and a fixed LAN
Dial-up networking	Allows a notebook computer to call via a mobile phone
Fax	Allows a mobile fax machine to talk to a mobile phone
Cordless telephony	Connects a handset and its local base station
Intercom	Digital walkie-talkie
Headset	Intended for hands-free voice communication
Object push	Provides a way to exchange simple objects
File transfer	Provides a more general file transfer facility
Synchronization	Permits a PDA to synchronize with another computer

Frame Format

- Format of three frame types



Frame Format

- Access code (72-bit) contains synchronization bits & identifier of primary to distinguish frame of one piconet from another.
- Header (54-bit) is a repeated 18-bit pattern.
- Each pattern has following subfields:

1. Address (3-bit) can define 7 secondaries (1 to 7). If address is zero, it is used for broadcast
2. Type: 4-bit type subfield defines type of data coming from upper layers.

Frame Format

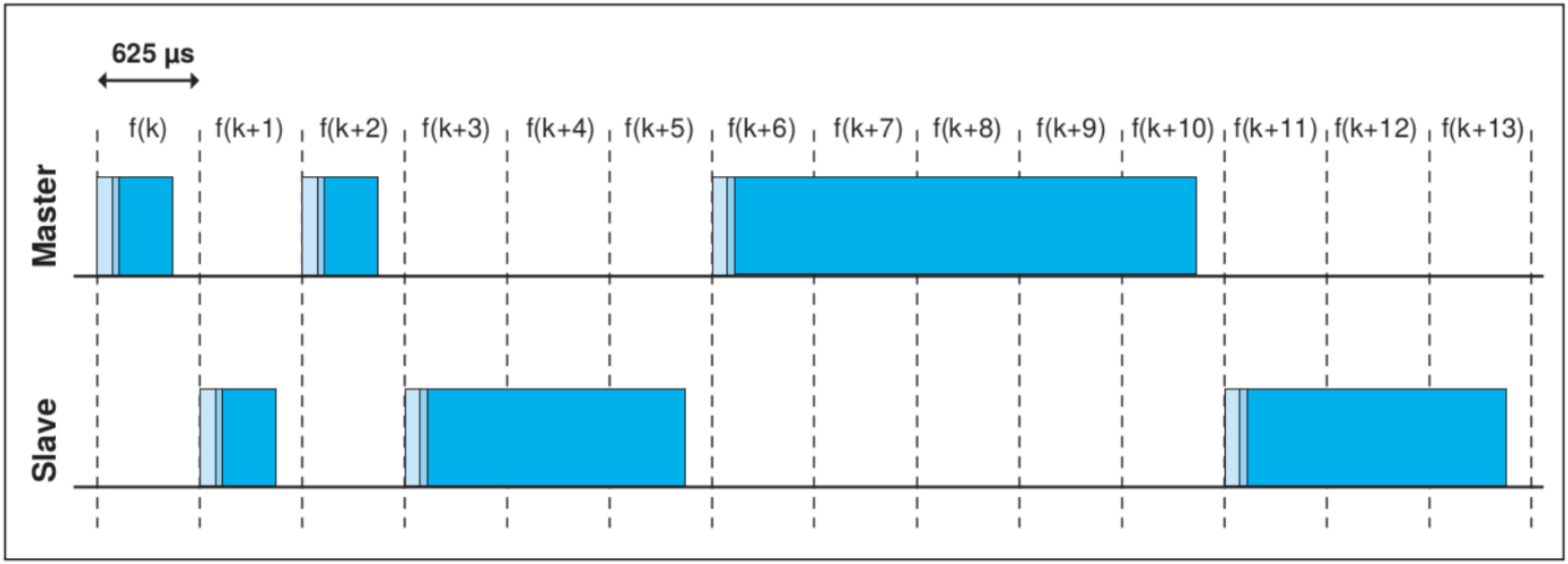
3. F (1-bit) for flow control. Value 1 indicates device is unable to receive more frames (buffer full)
4. A (1-bit) for acknowledgment, BT uses Stop-and-Wait ARQ
5. S (1-bit) holds sequence number
6. HEC (8-bit) header error correction- a checksum to detect errors in each 18-bit header section

Frame Format

- The header has three identical 18-bit sections (54 bits)
- The receiver compares these three sections, bit by bit
- If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules
- This is a form of forward error correction (for the header only)
- This double error control is needed because the nature of the communication, via air, is very noisy
- Note that there is no retransmission in this sublayer
- Payload (0 to 2740 bits) contains data or control information coming from the upper layers

Slot Duration and frame transmissions

- Slot duration: 625 μs
- A frame may be transmitted by device in total 1, 3, or 5 slots



Secondary – even slots
Primary- odd slots

- A secondary wants to transmit 450 bytes of information using Classic Bluetooth with basic rate at 1Mbps. How long will it take?
- Packet length: 72b (access code) + 54b (header) + 450*8b (payload-data to be transmitted) = 3,726b
- Data : Time
- 1000000b : 1 (data rate - 1Mbps)
- 3726b : ?
- It will take 3,726 μs

- Slot size is 625 μs, Slave can get 1, 3, or 5 slots to transmit
- Thus it can get 625 μs (625x1), 1875 (625x3) μs, or 3125 (625x5) μs slot time to transmit
- Our Slave needs 3726 μs to transmit
- Slave cannot fit the data in available 5 slots (i.e. 3125 μs)
- How much data can be send in 5 slots then?
- With 1 Mbps
  - Data : Time
  - 1000000b: 1 s
  - 1b:?
  - 1/1000000=1 μs
  - 1 bit requires 1 μs to transmit
- 3125b can be transmitted in 3125 μs
- 3,125b (available)– 72b (access code) – 54b (header) = 2,999b (data bits that can be transmitted in 3125 μs)
- BUT max payload can be of 2740b
- With first transmission of 5 slots slave can transmit 2740b

- Data yet to be transmitted = 450*8b – 2740 = 860 b
- 860b (payload) + 72b (access code) + 54b (header) = 986b
- 986b is more than 1 slot (625b) but less than 3 slots (1875b)
- Data that can be put in one slot = 625 b (available)– 72b (access code) – 54b (header) = 499 b

- So we have
- First transmission by slave of 5 slots carrying 2,740b data in 3,125 μs
- Master polls and takes 625 μs
- Second transmission by slave of 1 slot carrying 499b data in 625 μs
- Master polls and takes 625 μs
- Third transmission by slave 450*8b (total data to be transmitted)-2740b (data in 1st transmission) -499b (data in 2nd transmission) = 361 b
- 361b (payload) + 72b (access code) + 54b (header) = 487b
- 487b requires 487 μs and can be transmitted in one slot (625 μs)
- Thus total transmission time required = 3125 μs + 625 μs + 625 μs + 625 μs + 487 μs = 5487 μs
- Actual rate: $450*8/5487 * 10^{-6}$ = 656 kbps

Bluetooth Versions and Data Rate

Bluetooth Version	Release Date	Max. Data Transfer Rate	Important Innovations
Bluetooth 1.0a	July 1999	732.2 kbit/s	First official version
Bluetooth 1.0b	December 1999	732.2 kbit/s	General improvements
Bluetooth 1.1	February 2001	732.2 kbit/s	Resolved connection and security issues. First marketable product version. Encryption. Supports up to seven connections simultaneously.
Bluetooth 1.2	November 2003	1 Mbit/s	Backwards compatibility with Bluetooth 1.1. Less prone to interference as a result of AFH (Adaptive Frequency Hopping).
Bluetooth 2.0 + EDR	November 2004	2.1 Mbit/s	Enables three times the data transfer rate as a result of EDR (Enhanced Data Rate). Various energy-saving techniques. Adds use of NFC (Near Field Communication) for pairing.

Bluetooth Versions and Data Rate

Bluetooth 2.1 + EDR	August 2007	2.1 Mbit/s	Connects automatically without using a PIN through Secure Simple Pairing.
Bluetooth 3.0 + HS	April 2009	24 Mbit/s	Additional high-speed channel (HS) based on WLAN and UWB (ultra-wide band).
Bluetooth 4.0 LE (or Bluetooth SMART)	December 2009	24 Mbit/s	Low energy (LE) protocol stack for various energy-saving techniques (e.g. GATT profile) for small devices. Improved error correction. 128-bit encryption.
Bluetooth 4.1	December 2013	25 Mbit/s	Small devices no longer require an intermediary. IPv6.
Bluetooth 4.2	December 2014	25 Mbit/s	General improvements
Bluetooth 5	December 2016	50 Mbit/s	Significant increase in range and data transfer rate.
Bluetooth 5.2 .	January 2020	50 Mbit/s	Feature that allows transmitter to adjust its transmission power by itself or can be requested to change its transmission power by a peer device

Thank You