CMP4204
Wireless Technologies

Lecture 07

Personal Access Network (PAN)

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

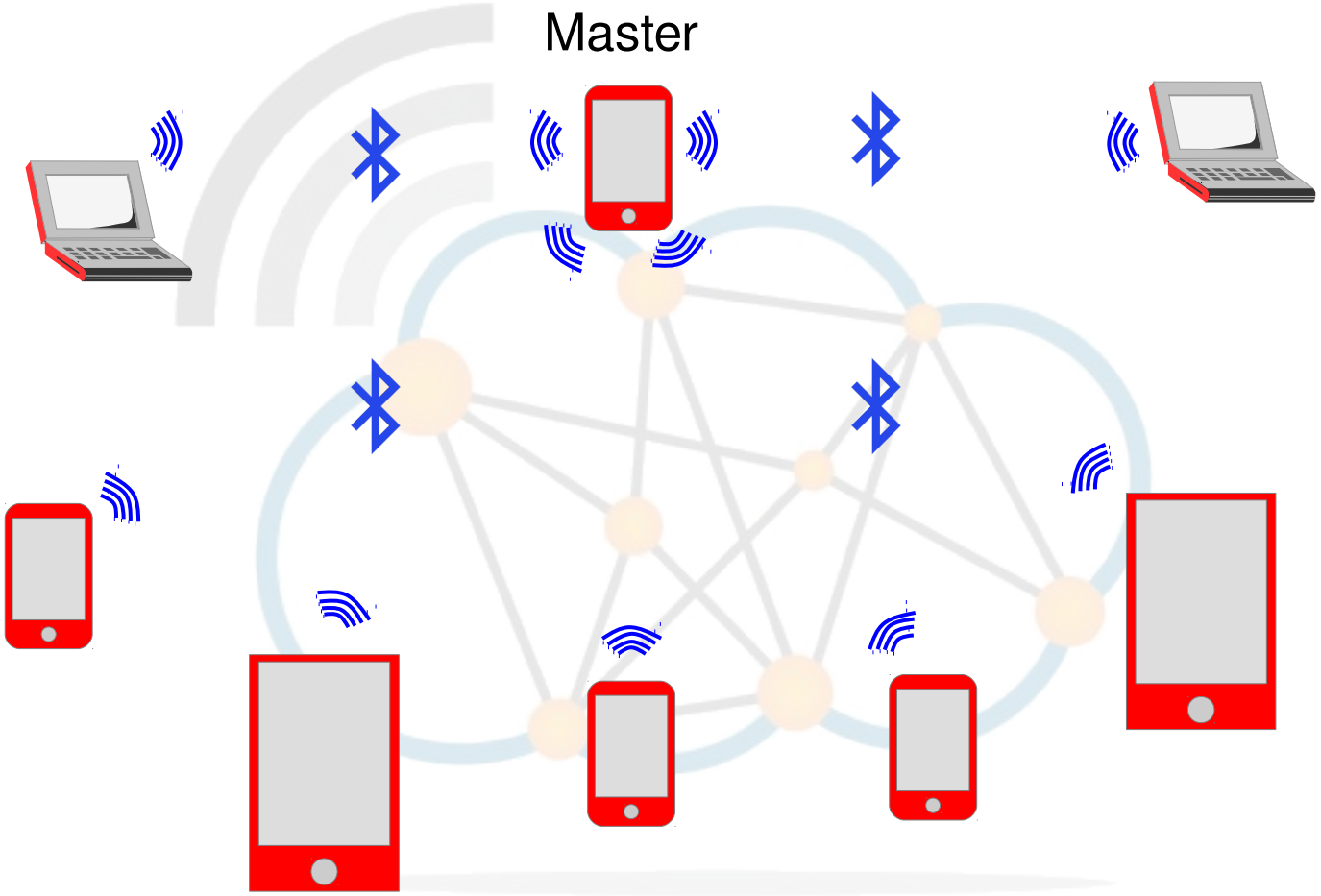
Wireless Personal Access Network (PAN)

- A Wireless PAN (WPAN)
  - Short-distance wireless network 10m - 100m
  - Support portable and mobile computing devices
    - smartphones, laptops, wireless printers, etc..
- Bluetooth is a WPAN
  - ad-hoc wireless networks for the exchange information.
- Smartphones
  - Cellular mobile
  - WLAN
  - WPAN.

Usage Scenarios Examples

- Data Access Points.
- Synchronisation.
- Headset.
- Conference Table.
- Cordless Computer.
- Business Card Exchange.
- Instant Postcard.
- Computer Speakerphone.

Piconet



Piconet

- A Bluetooth WPAN is called a piconet,
  - Up to 8 active devices (255 in parked mode)
  - master-slave relationship.
  - 1st bluetooth device master
  - Subsequent devices are slaves
  - that communicate with the master.

Piconet controller

- One device assumes controller role for piconet initialisation
  - Mediates communication within the piconet
  - Broadcasts a beacon for all devices to synchronise
  - Allocates Time Slots (TS) for the devices.
- Devices join by requesting a TS from the controller.
  - Controller authenticates the device
  - Assigns TS.
- Device can communicate using:
  - Piconet destination address, to all devices
  - Directed address to a particular device.

IEEE 803.15 WPAN working groups

- 802.15.3
  - High-bandwidth (about 55 Mb/s)
  - Low-power MAC and PHYsical layers.
- 802.15.4
  - Low-bandwidth (about 250 kb/s)
  - Extra-low power MAC and PHYsical layers.

IEEE 803.15 WPAN

- Original functional (1998) specified devices with:
  - Power management: low current consumption
  - Range: 0 - 10 m
  - Speed: 19.2 - 100 kb/s
  - Small size: 12mm³ without antenna
  - Low cost relative to target device
  - Should allow overlap of multiple networks in the same area
  - Networking support for a minimum of 16 devices.

IEEE 803.15 WPAN Task groups

- Task group 1
  - Based on Bluetooth. Defines PHY and MAC for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space.
- Task group 2
  - Focused on coexistence of WPAN and 802.11 WLANs.
- Task group 3
  - PHY and MAC layers for high-rate WPANs (> 20 Mb/s).
- Task group 4
  - Ultra-low complexity, ultra-low power consuming, ultra-low cost PHY and MAC layer for data rates of up to 200 kb/s.

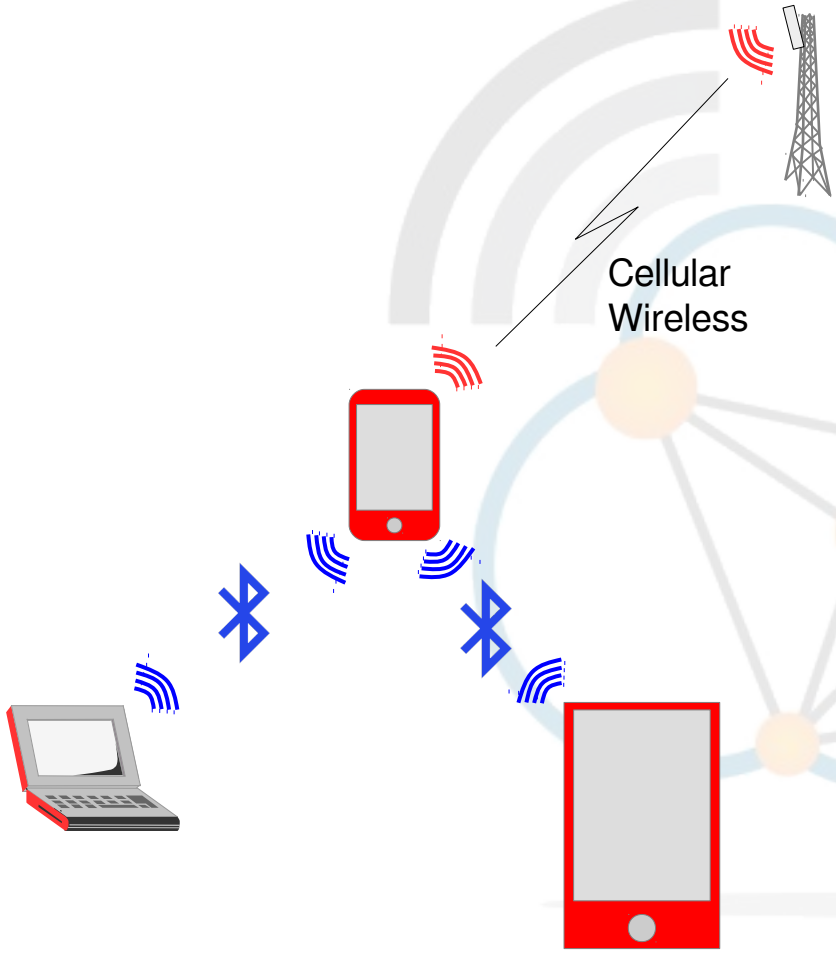
Bluetooth

- Universal radio interface for ad-hoc wireless connectivity.
- Interconnecting computer and peripherals.
- Replacement of IrDA.
- Embedded in other devices
  - €5 (20,000 UGX) / device
  - €50 (200,000 UGX) / USB Bluetooth.
- Short range (10m).
- Low power consumption.
- SRD ISM band: 2.45 GHz.
- Voice and data tx gross data rate 1 Mb/s.

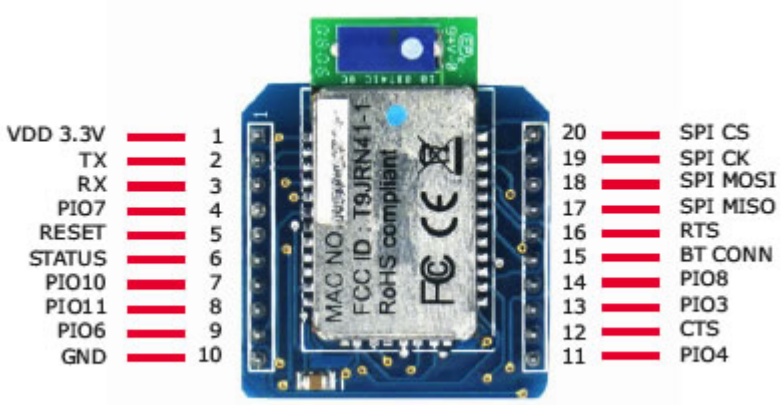
Interference Between Bluetooth and 802.11

- The WLAN industry specified three levels of overlapping:
  - **Interference**: co-location causes performance degradation.
  - **Coexistence**: if co-located without significant impact on performance.
  - **Interoperation**: an environment with multiple wireless systems to perform a given task using a single set of rules.

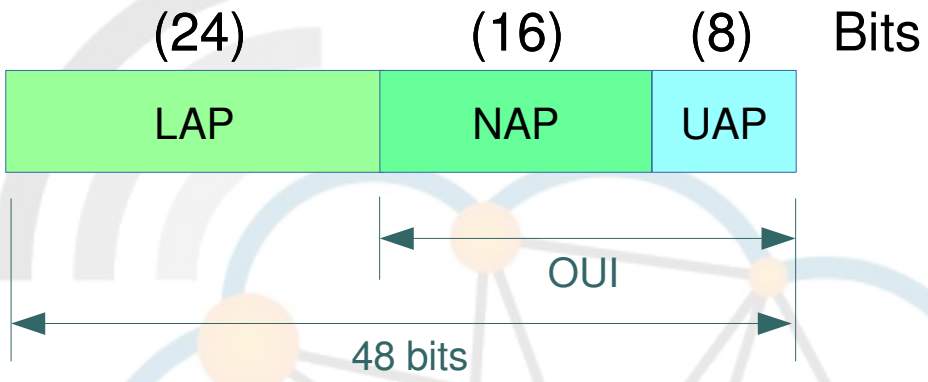
Bluetooth application



Bluetooth module



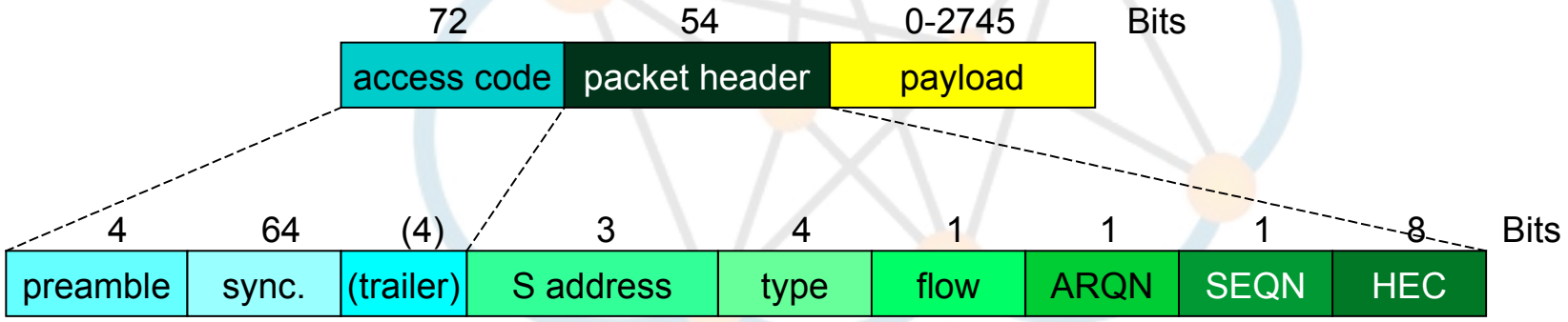
Bluetooth address (BD_ADDR)



- Uniquely identifies a bluetooth device
- Lower, Upper and Non-signifiant address parts
- Used to determine frequency hopping sequence.

Frame Format of Bluetooth Packets

- The 48 bit address unique to every Bluetooth device is used as the seed to derive the sequence for hopping frequencies of the devices.



Overall Frame Format of Bluetooth Packets

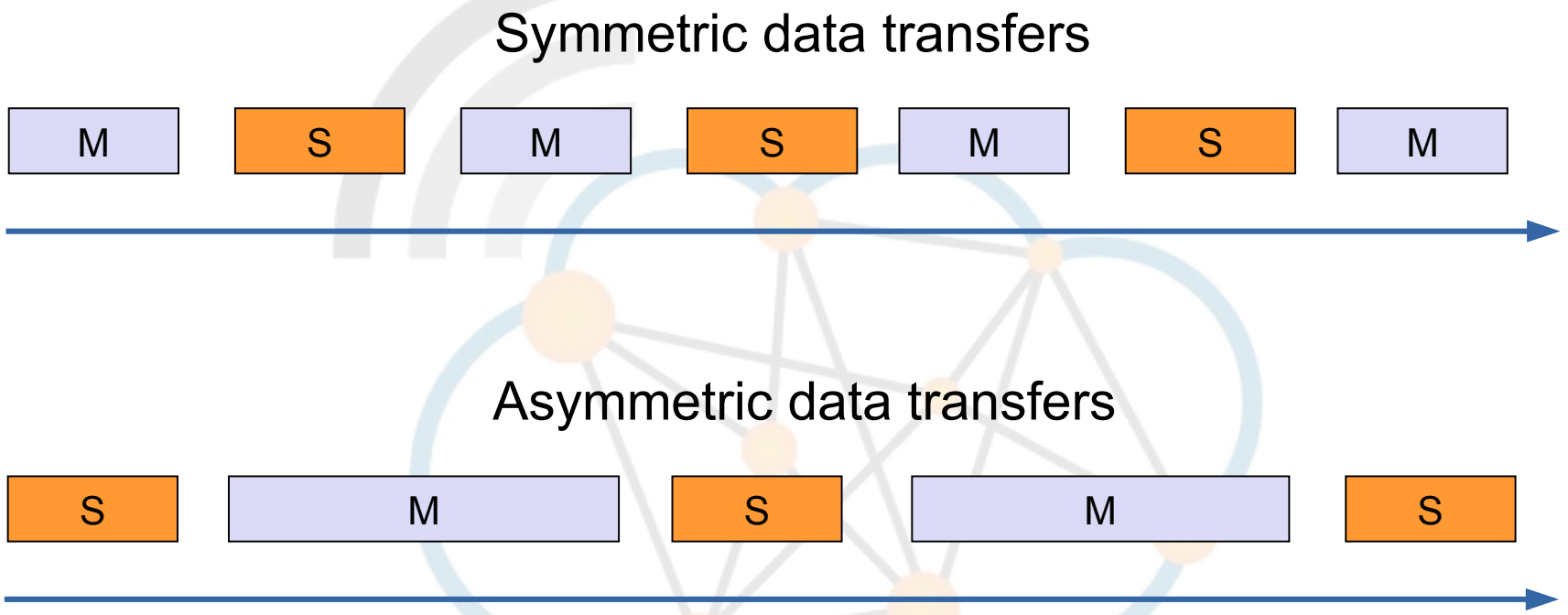
Type 1: Master terminal addr
Type 2: Slave terminal addr
Type 3: Fixed access code
(inquiry process)
Type 4: Dedicated access
(ID specific devices)

S-address
4 bit packet type (16 options)
6 ACL, for packet data communication
3 SCO, for voice communications
1 integrated voice SCO and data ACL
4 are control packets common for SCO & ACL

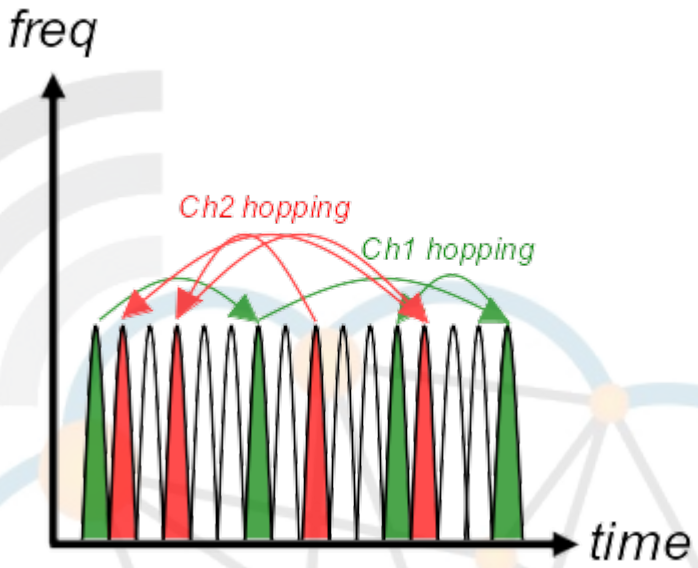
Control Packets

- **ID**
  - Carries the access code.
- **NULL**
  - Used to ACK signalling, and there is no ACK for it.
- **POLL**
  - Similar to the NULL, but it has an ACK.
- **FHS**
  - Carries all the information necessary to synchronise two devices in terms of access code and hopping timing.

Data transmission

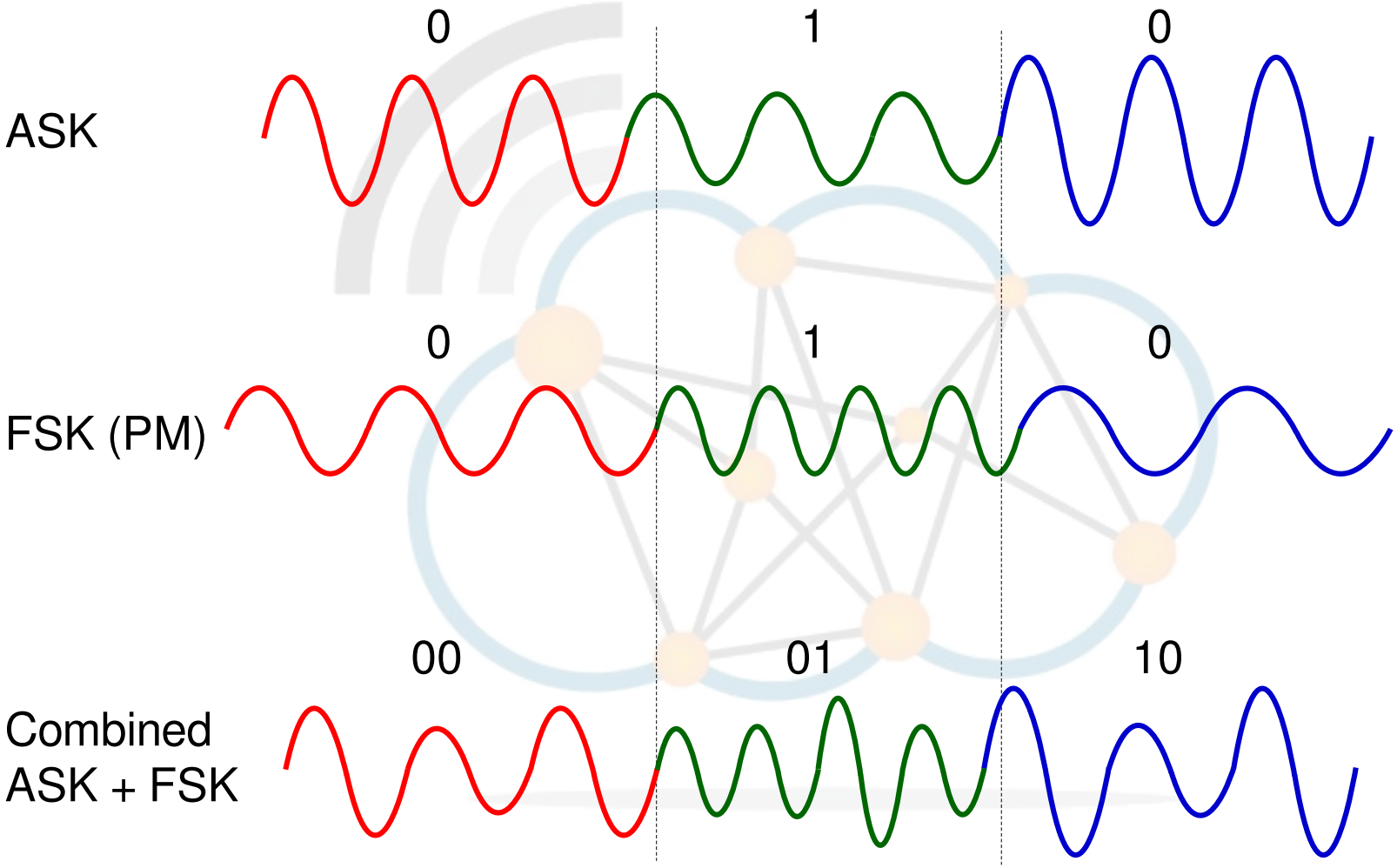


Frequency Hopping Spread Spectrum

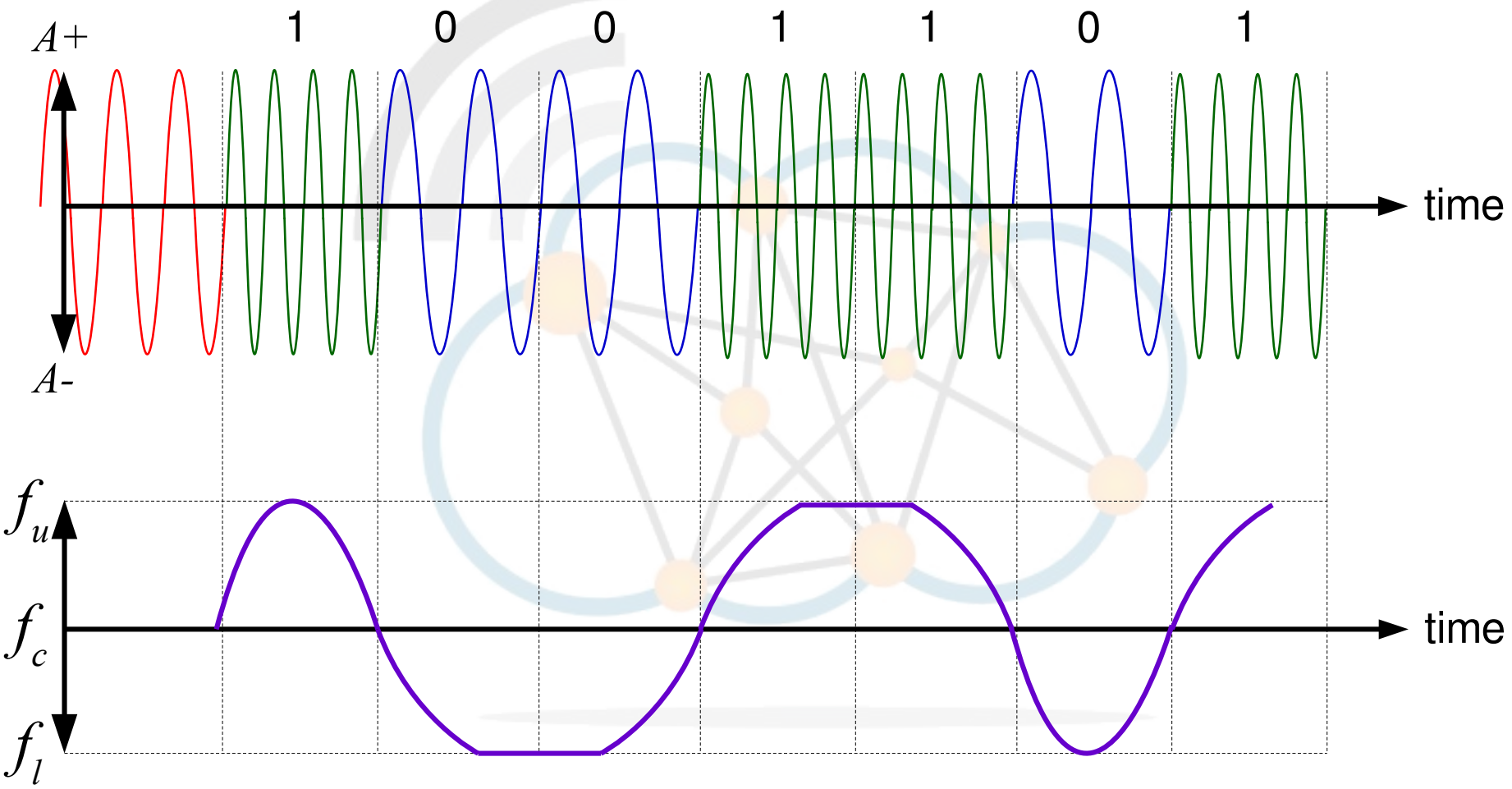


- 79 communication channels can be used.
- In the face of interference the bluetooth devices will automatically change its hopping pattern to avoid the interference.

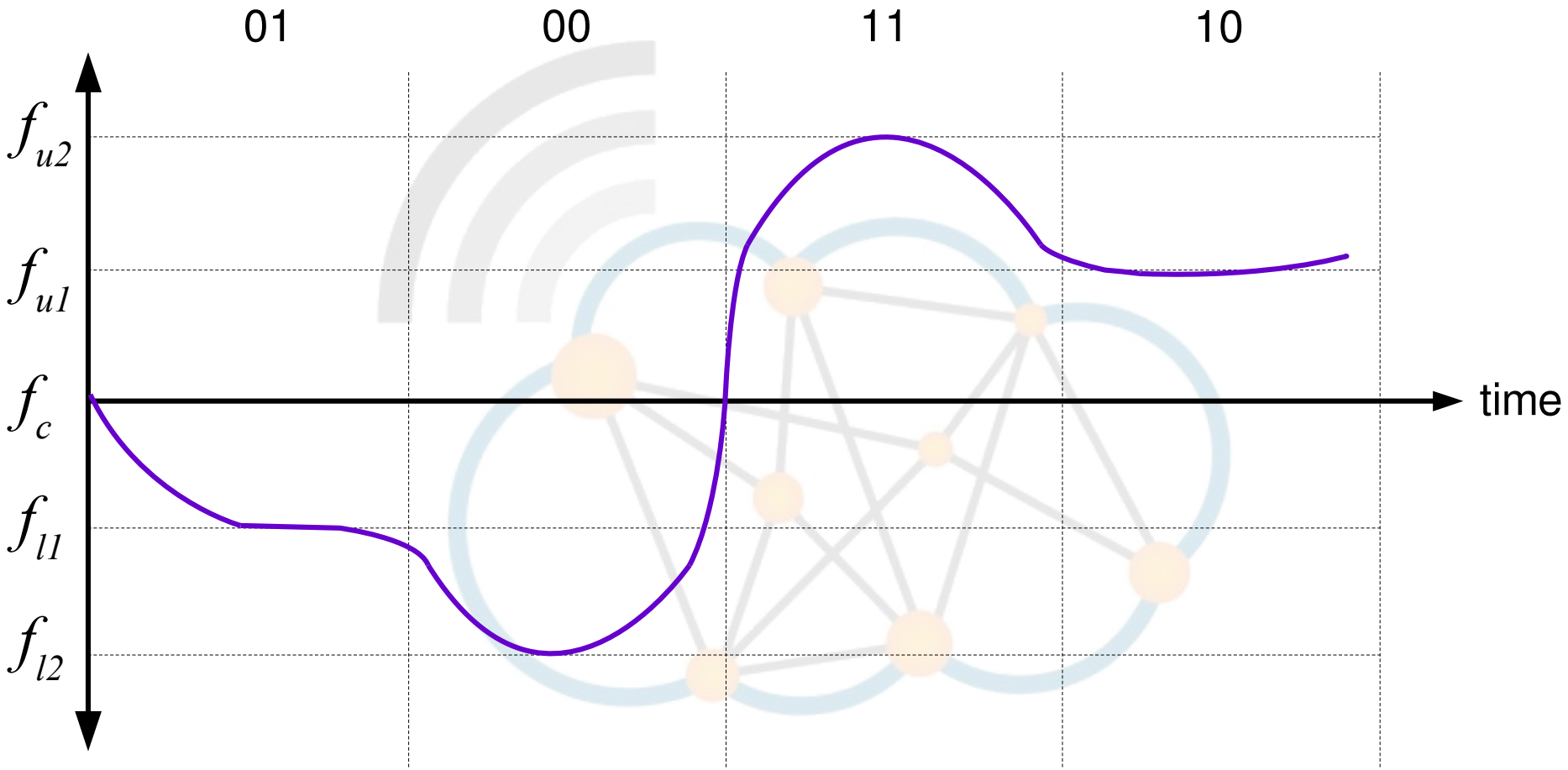
Modulation



Modulation - 2GFSK



Modulation - 4GFSK



Modulation from Bluetooth v2.0

- Bluetooth v1.0
  - Gaussian FSK (GFSK)
- Bluetooth v2.0
  - GFSK
  - $\pi/4$ QPSK
  - D8PSK

Bluetooth power classes

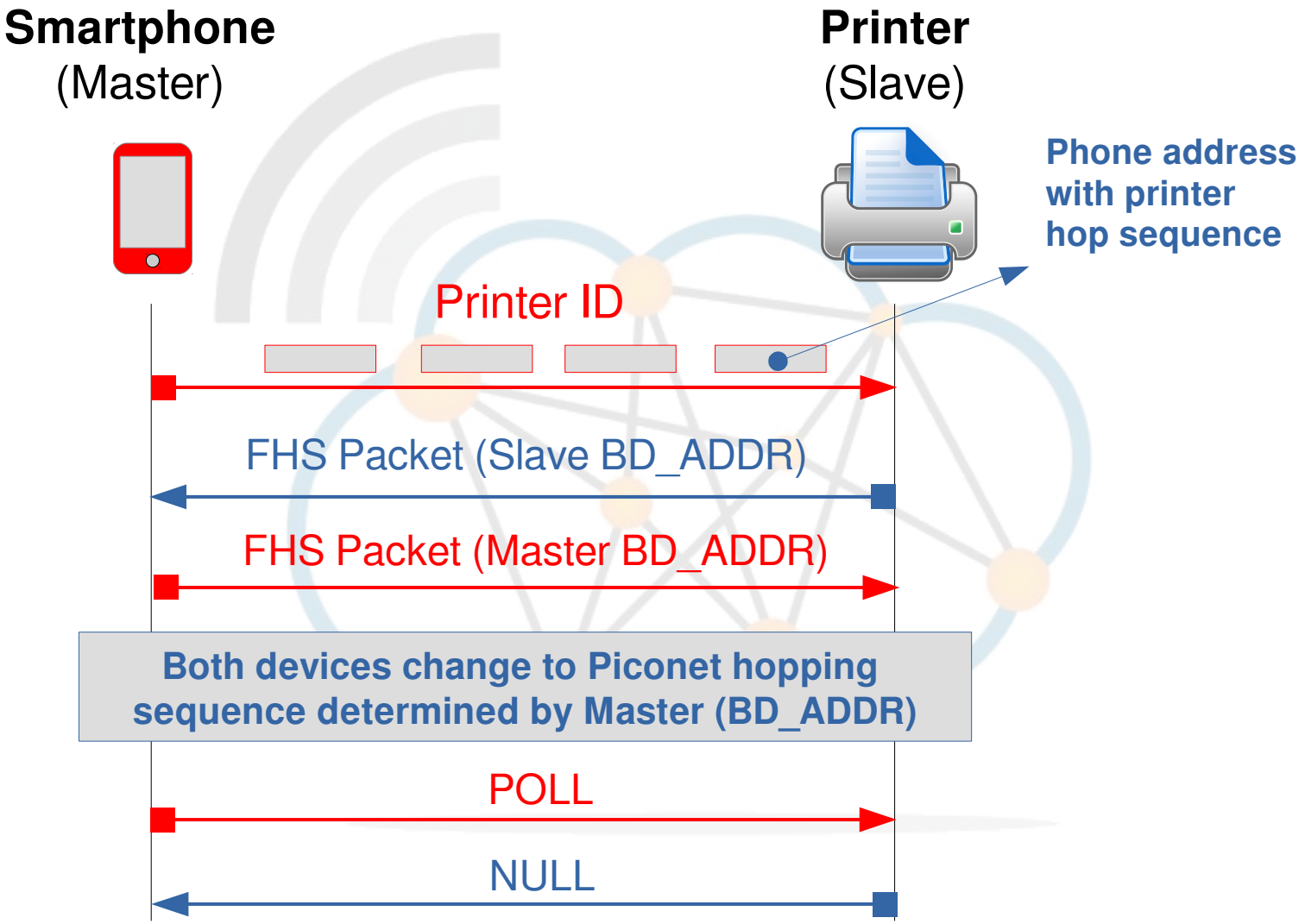
- 3 RF power classification levels.
- Dynamic power control that automatically is reduced when enough signal strength is available between Bluetooth devices is a requirement for Class 1.

Class	Max power (W/dBm)	Range (m)
1	100 mW	100
2	2.5 mW	10
3	1 mW	1

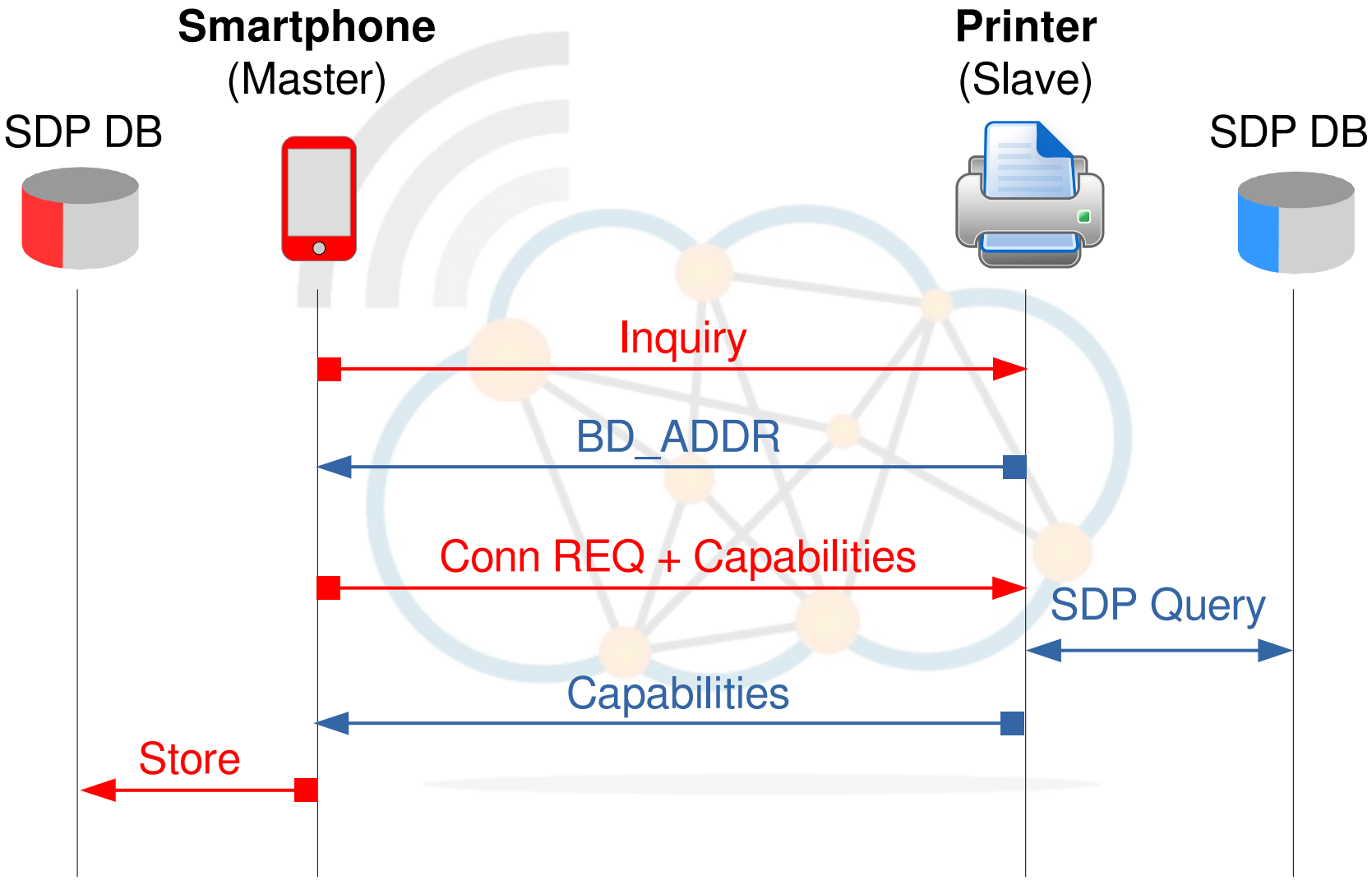
Operation

- Device Discovery
- Device Connection
- Bluetooth Pairing
- Logical Channels
- Service Discovery

Device connect



Service Discovery



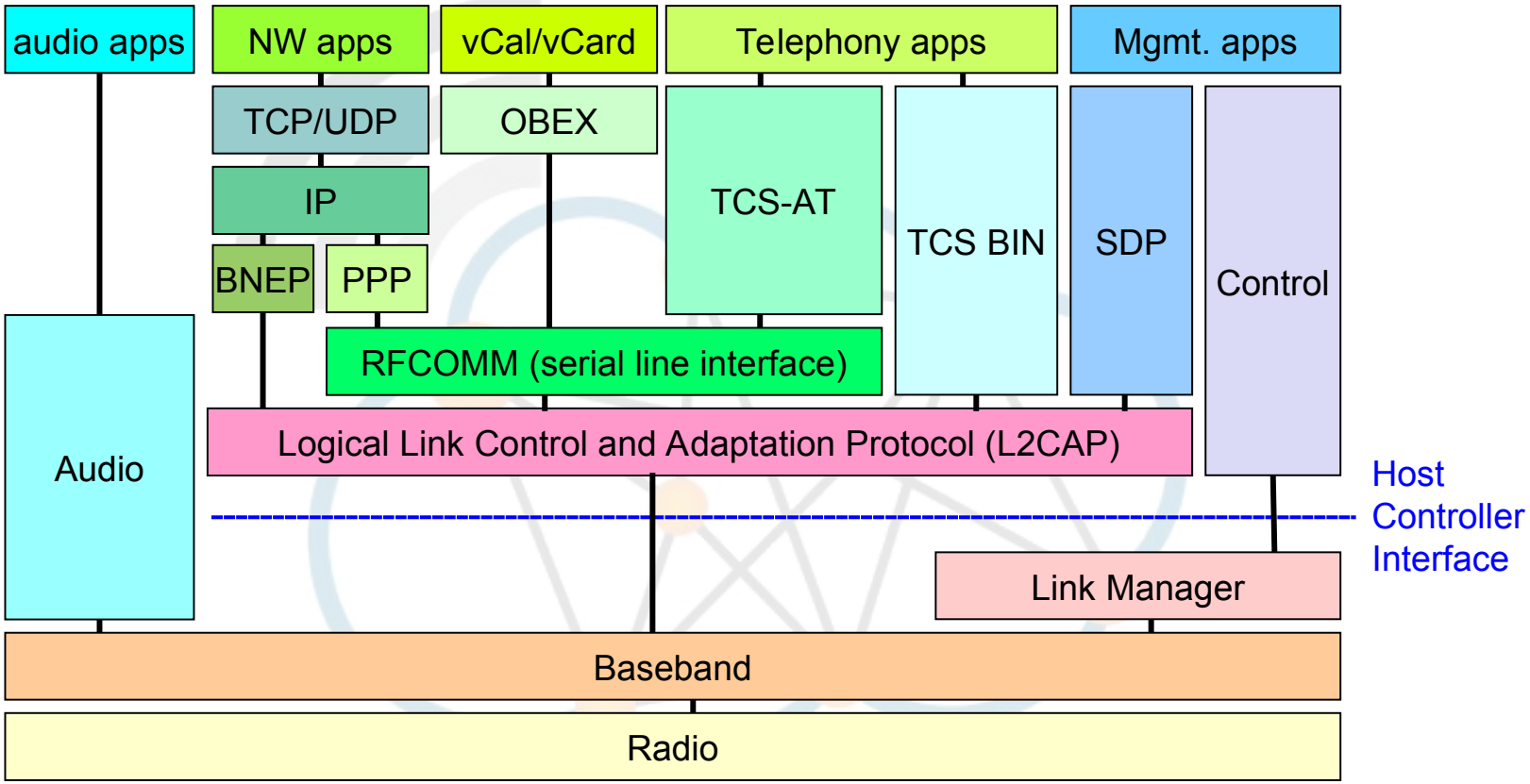
Address types

- Active Member Address (AMA)
  - 3 bit (limits to 7 devices)
- Parked Member Address (PMA)
  - 8 bit (limited to 255 devices)

Modes of operation

Purpose	Mode	Addressing	State	Power	Master to Slave Access Time
Active mode enables master/slave communications in any given frame.	Active	AMA	Connected	High	Any given frame (1250 ms)
Hold mode frees a slave for a predetermined one time hold period.	Hold	AMA	Connected	Low	At end of hold duration (T hold)
Sniff mode frees a slave for predetermined, recurring, fixed time periods.	Sniff	AMA	Connected	Low	At end of sniff intervals (T sniff)
Parking mode enables a master to connect to as many as 255 parked devices in addition to its 7 active devices	Park	PMA	Parked	Lower	At beacon time intervals (T beacon) plus some reconnection overhead
Standby mode is the default mode for any Bluetooth device	Standby	None	Standby	Lowest	Paging cycle or Inquiry & Paging cycle (2-10s)

Bluetooth Protocol Stack



AT: ATtention sequence
TCS AT: Telephony Control Specification – Attention
TCS BIN: Telephony Control Specification – Binary
BNEP: Bluetooth Network Encapsulation Protocol

OBEX: OBject EXchange
SDP: Service Discovery Protocol
RFCOMM: RF communications

Bluetooth Protocol Stack

- **Link Manager** (LM)
  - Carries out link setup, authentication, link configuration, and other protocols.
- **Link Manager Protocol** (LMP)
  - Link setup and control. LMP messages are interpreted and filtered out by LM.
- **Host Controller Interface** (HCI)
  - Application layer providing command interface to the LM Baseband layers.
- **Logical Link Control Applications Protocol** (L2CAP)
  - Supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.
- **RF COMMunications protocol** (RFCOMM),
  - Serial Cable Emulation Protocol.
- **OBject EXchange** (OBEX)
  - Communications protocol that facilitates the exchange of binary objects between devices like business cards, data, even applications.

Bluetooth Protocol Stack

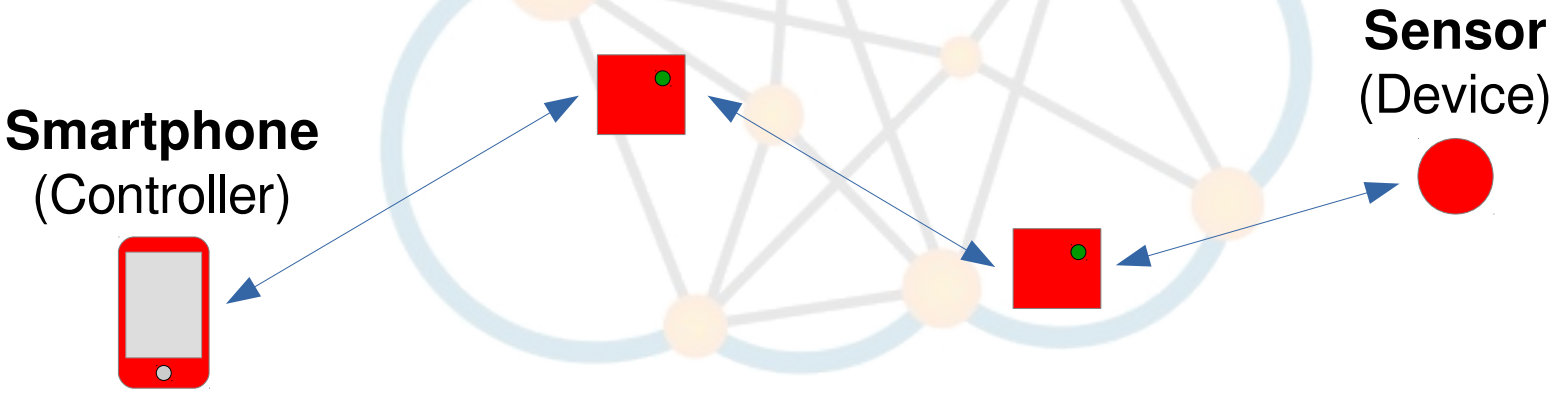
- **Telephony Control Specification - ATtention** (TCS-AT)
  - Commands by which a mobile phone and modem can be controlled in the multiple usage models. It is also used for fax services, dial-up networking and headset profiles.
- **TCS-BIN** (Binary)
  - Bluetooth Telephony Control protocol used for cordless telephony profiles.
- **Service Discovery Protocol** (SDP)
  - Protocol for applications to discover which services are available and to determine the characteristics of those available services.
- **Bluetooth Network Encapsulation Protocol** (BNEP)
  - Used in Personal Area Networking Profile (PAN) to transport common networking protocols over bluetooth media such as IPv4 and IPv6.
  - Its packet format is based on Ethernet framing as defined by IEEE 802.3. It runs on L2CAP.

Bluetooth Low Energy (BLE)

- Wireless PAN technology introduced in Bluetooth v4.0.
- Applications in the healthcare, fitness, beacons, security, and home entertainment industries.
- Considerably reduced power consumption and cost compared to Classic Bluetooth.
- It is predicted that by 2018 more than 90% of Bluetooth-enabled smartphones will support BLE.
- Not backward-compatible with Classic Bluetooth.
- Bluetooth v4.0 permits devices to implement either or both of the BLE and Classic systems.
- Single antenna for dual mode as BLE and Classic use 2.4 GHz.

Bluetooth Mesh networks

- Greater range through bluetooth device relay.
- Controller communicates with the closest device within the mesh and the messages are relayed to and from the device.



Bluetooth Versions

Version	Modulation	Max speed	Max range
1	GFSK	1 Mb/s	10 m
2	GFSK, π/4-DQPSK, 8DPSK	3 Mb/s	10 m
3	GFSK, π/4-DQPSK, 8DPSK (802.11g)	24 Mb/s	10 m
4	GFSK, π/4-DQPSK, 8DPSK (802.11n)	24 Mb/s	60 m
5	GFSK, π/4-DQPSK, 8DPSK (802.11n)	50 Mb/s	240 m

Thank You

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com