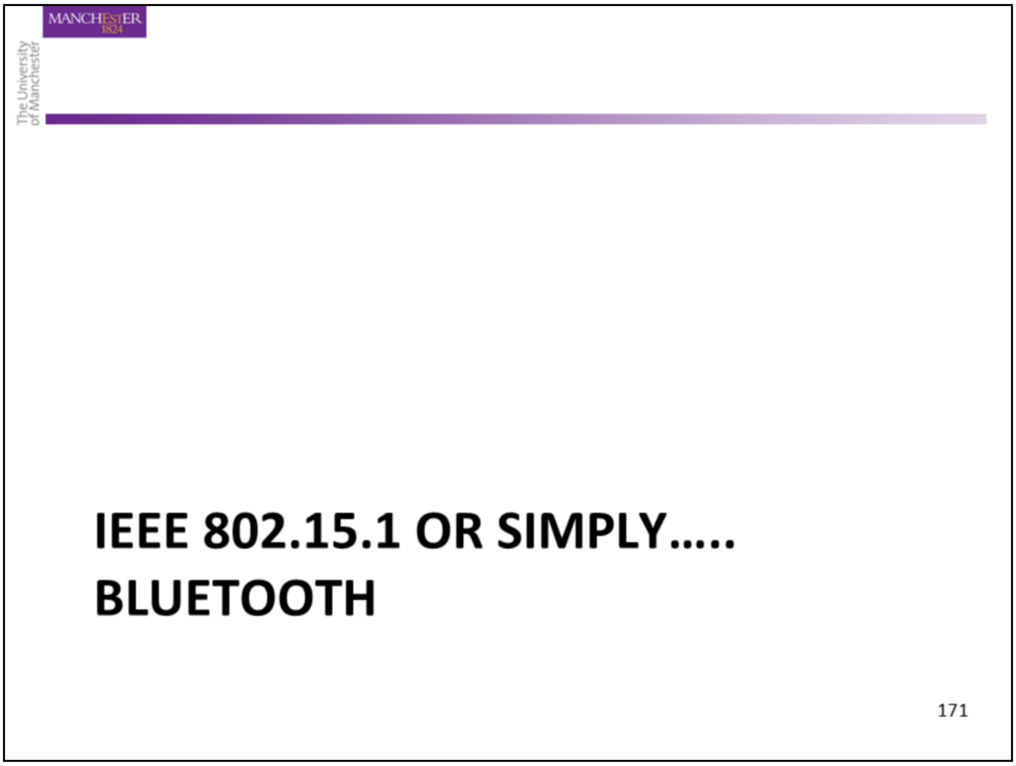
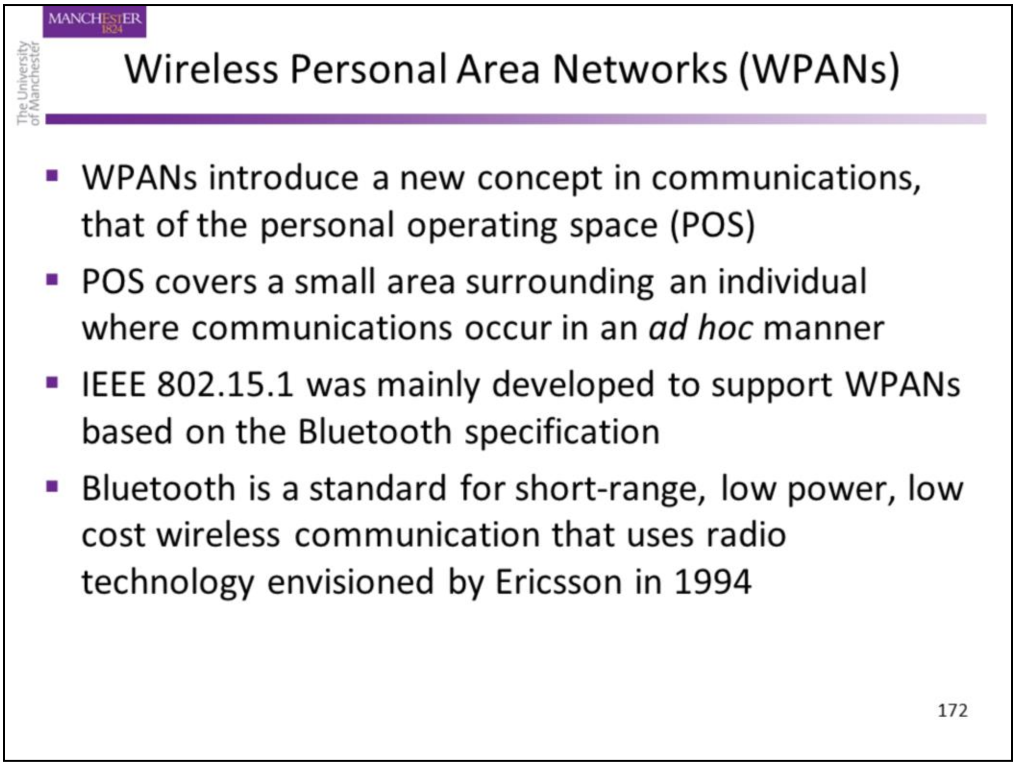


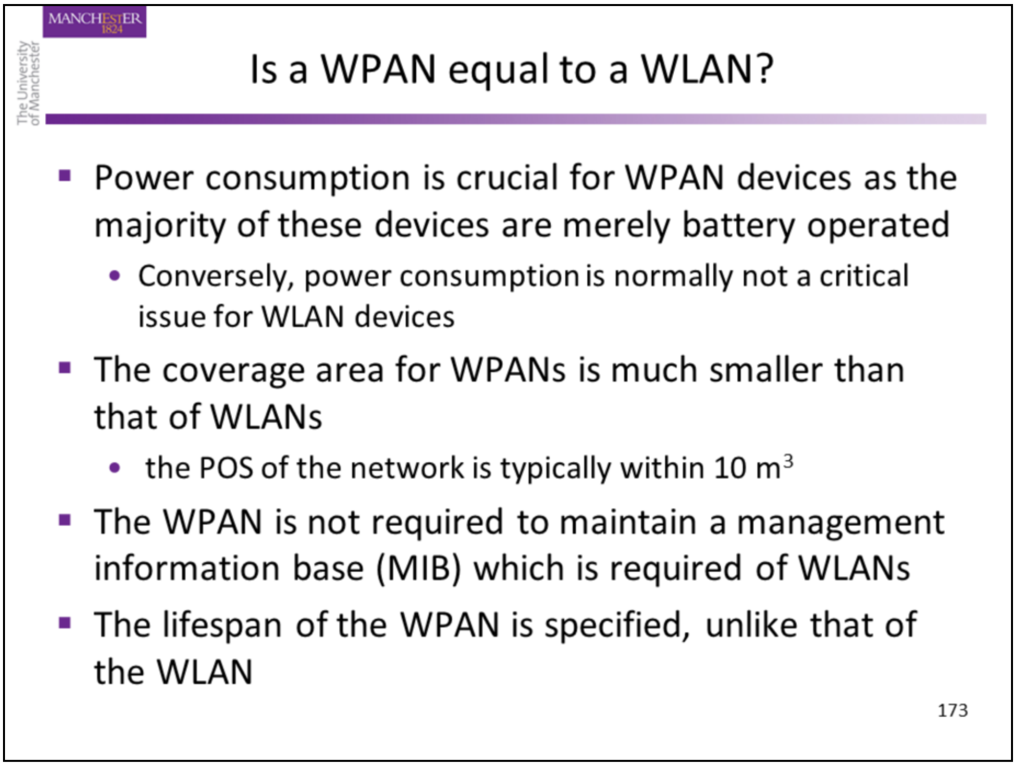
IEEE 802.15.1 OR SIMPLY….. BLUETOOTH



Wireless Personal Area Networks (WPANs)

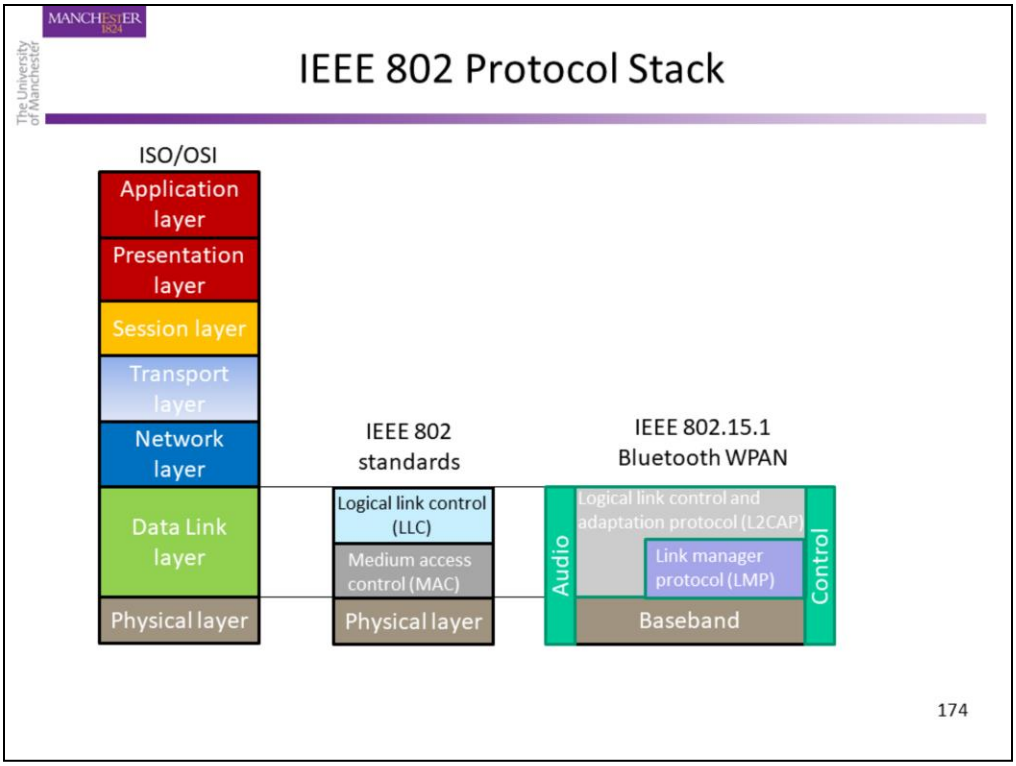
- WPANs introduce a new concept in communications, that of the personal operating space (POS)
- POS covers a small area surrounding an individual where communications occur in an *ad hoc* manner
- IEEE 802.15.1 was mainly developed to support WPANs based on the Bluetooth specification
- Bluetooth is a standard for short-range, low power, low cost wireless communication that uses radio technology envisioned by Ericsson in 1994

- WPANs primarily target the consumer market and are used for ease of connectivity of personal wearable or hand-held devices.
- Bluetooth is today supported by myriads of devices for a multitude of applications including cell phones, personal computers, peripherals such as mice and keyboards, local area network (LAN) access points, audio peripherals including headsets and speakers, and embedded applications comprising automobile power locks, grocery store updates, etc.
- Ericsson joined forces with Intel, International Business Machines (IBM), Nokia, and Toshiba to form the Bluetooth special interest group (SIG) in early 1998. 3Com, Lucent/Agere Technologies, Microsoft, and Motorola joined the group in late 1999.



Is a WPAN equal to a WLAN?

- Power consumption is crucial for WPAN devices as the majority of these devices are merely battery operated
  - Conversely, power consumption is normally not a critical issue for WLAN devices
- The coverage area for WPANs is much smaller than that of WLANs
  - the POS of the network is typically within 10 m^3
- The WPAN is not required to maintain a management information base (MIB) which is required of WLANs
- The lifespan of the WPAN is specified, unlike that of the WLAN



IEEE 802 Protocol Stack

ISO/OSI

Application layer

Presentation layer

Session layer

Transport layer

Network layer

Data Link layer

Physical layer

IEEE 802 standards

Logical link control (LLC)

Medium access control (MAC)

Physical layer

IEEE 802.15.1 Bluetooth WPAN

Audio

Logical link control and adaptation protocol (L2CAP)

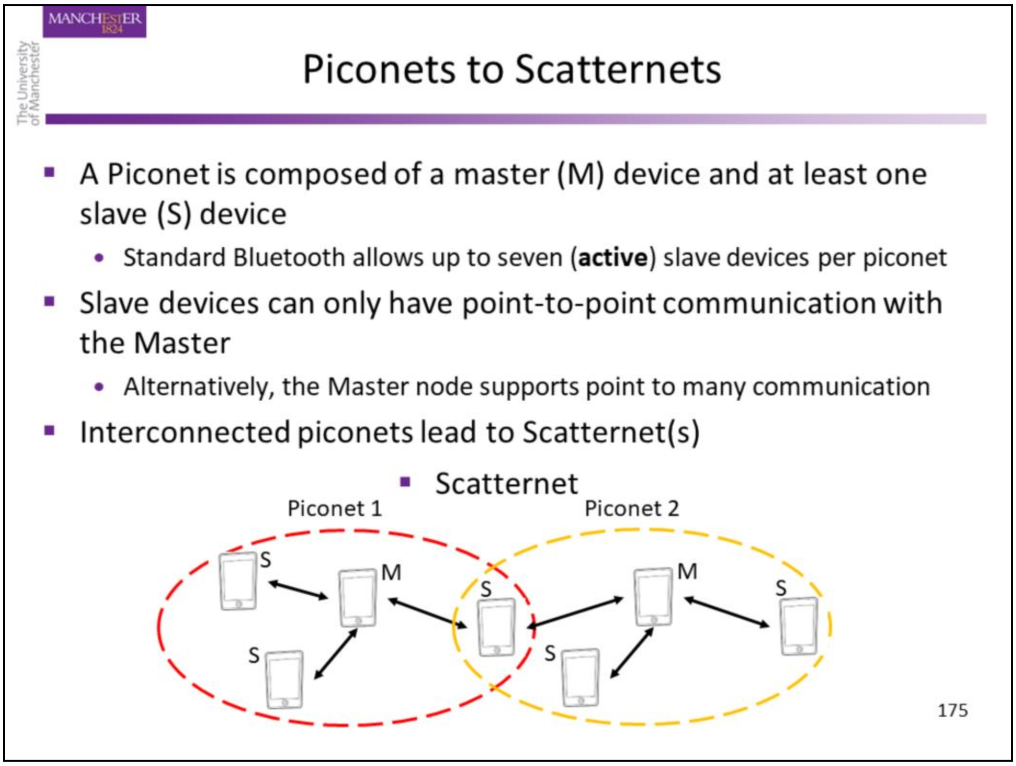
Link manager protocol (LMP)

Control

Baseband

174

- Note that the application, presentation, session, transport, and network layers are not within the scope of the IEEE 802 standards.
- The data link layer of the open systems interconnection (OSI) seven-layer model is mapped directly to the logical link control (LLC) and MAC layers.



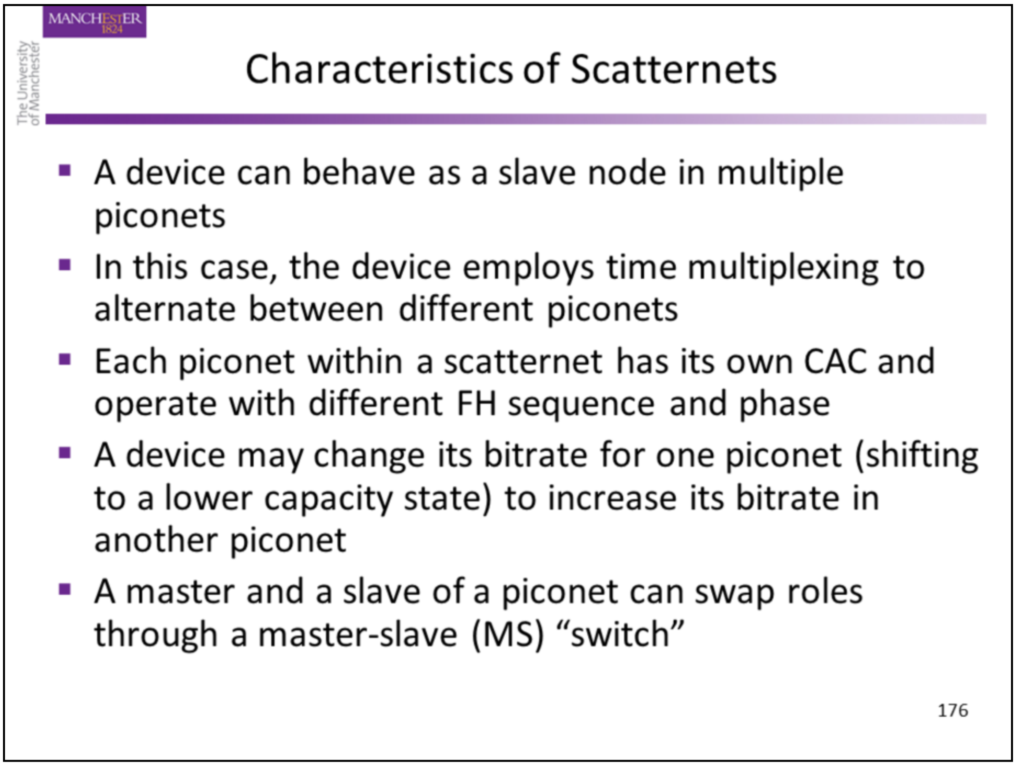
Piconets to Scatternets

- A Piconet is composed of a master (M) device and at least one slave (S) device
  - Standard Bluetooth allows up to seven (**active**) slave devices per piconet
- Slave devices can only have point-to-point communication with the Master
  - Alternatively, the Master node supports point to many communication
- Interconnected piconets lead to Scatternet(s)

- Scatternet

175

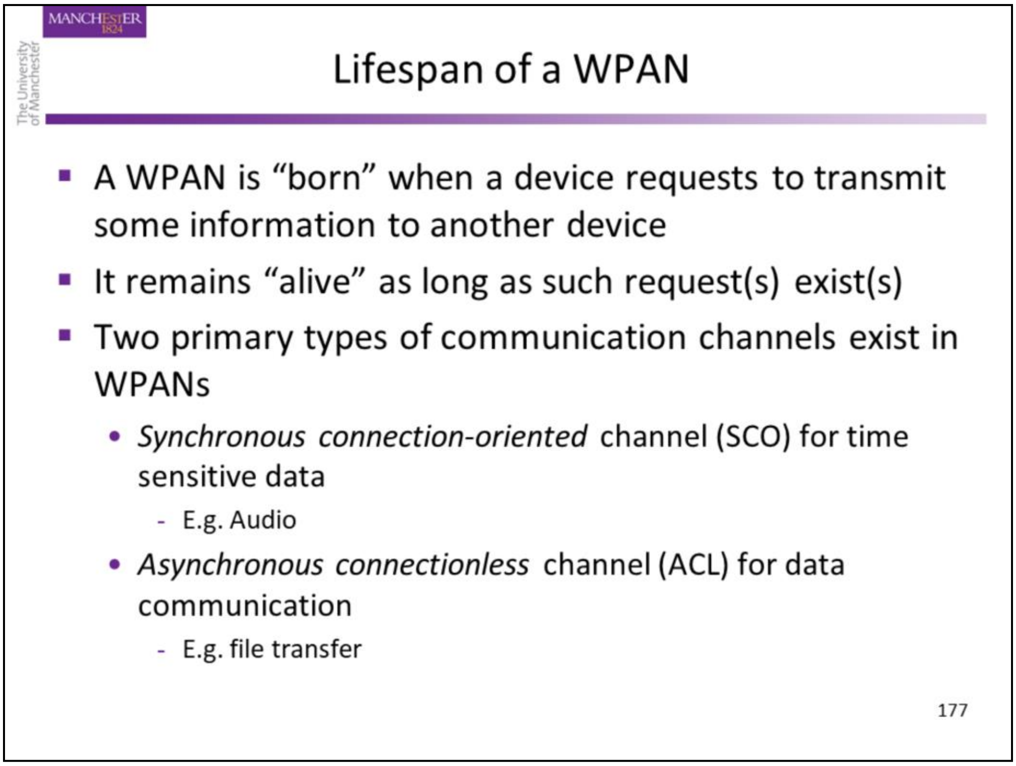
- The master node can communicate with more than one slave node at a given time instance. On the other hand, slave nodes are only allowed to communicate directly with the master node by point-to-point communication.
- A device can be a **slave node** in multiple piconets (not simultaneously though) but can be a **master node** in only one piconet. Also, a device might be a slave node in one piconet and a master node in another piconet.
- A piconet can access another network, e.g., LAN, with the help of an attachment gateway (AG).



Characteristics of Scatternets

- A device can behave as a slave node in multiple piconets
- In this case, the device employs time multiplexing to alternate between different piconets
- Each piconet within a scatternet has its own CAC and operate with different FH sequence and phase
- A device may change its bitrate for one piconet (shifting to a lower capacity state) to increase its bitrate in another piconet
- A master and a slave of a piconet can swap roles through a master-slave (MS) “switch”

- The device must maintain synchronization between two different masters, each with their own drift, such that the device must update its offset frequently.
- The device may also go to a lower capacity mode, such as sniff, hold, or park, in one piconet to increase its capacity in another piconet.
- The role of MS switching is needed in a few different situations, e.g., when a device pages the master of a piconet that it wants to join.
- This MS switch consists of a TDD switch followed by a piconet switch between the master and slave.
- This process is followed by a piconet switch between the new master and each old slave that wishes to be a part of the new piconet.



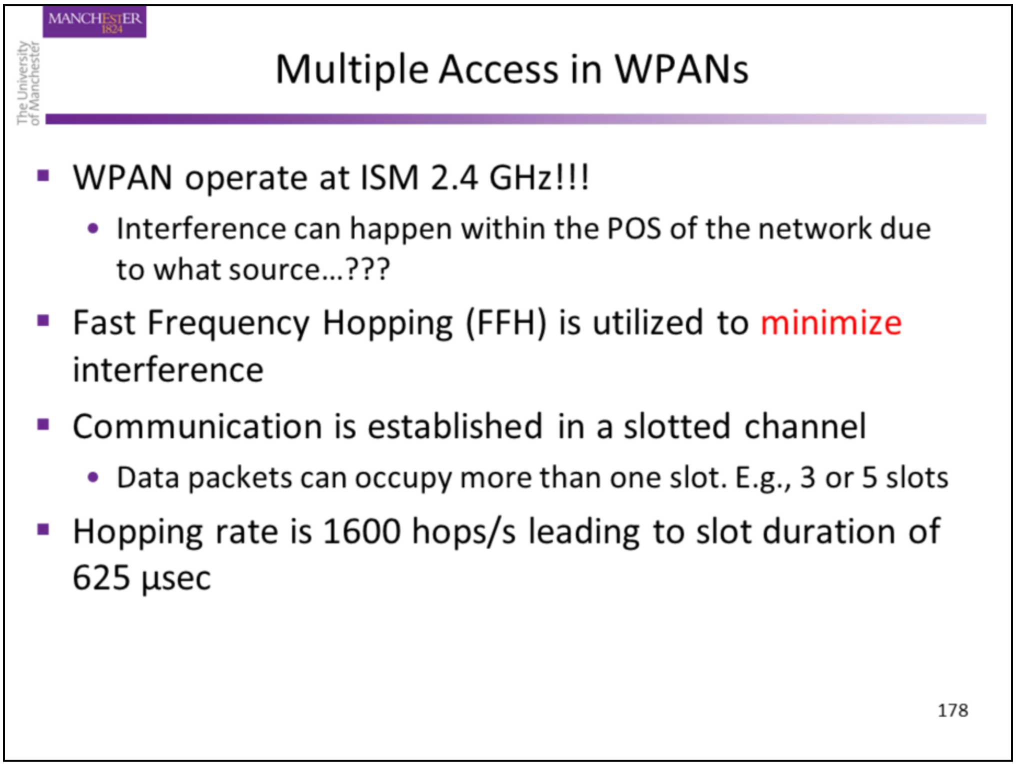
MANCHESTER 1824

The University of Manchester

Lifespan of a WPAN

- A WPAN is “born” when a device requests to transmit some information to another device
- It remains “alive” as long as such request(s) exist(s)
- Two primary types of communication channels exist in WPANs
  - *Synchronous connection-oriented* channel (SCO) for time sensitive data
    - E.g. Audio
  - *Asynchronous connectionless* channel (ACL) for data communication
    - E.g. file transfer

- Each SCO channel is a one-to-one link between a master and a slave node. This type of communication link is usually reserved for only audio communication and more broadly for time-sensitive information.
- Alternatively, an ACL channel is a one-to-many link between the master and all slaves. The ACL supports transmission of time-insensitive communication. As such, data packet retransmission, which is not available in communications through SCO, is utilized to avoid packet corruption during information exchange. ACL packets can be addressed either to a single slave node or to all slave devices with the absence of a particular address.



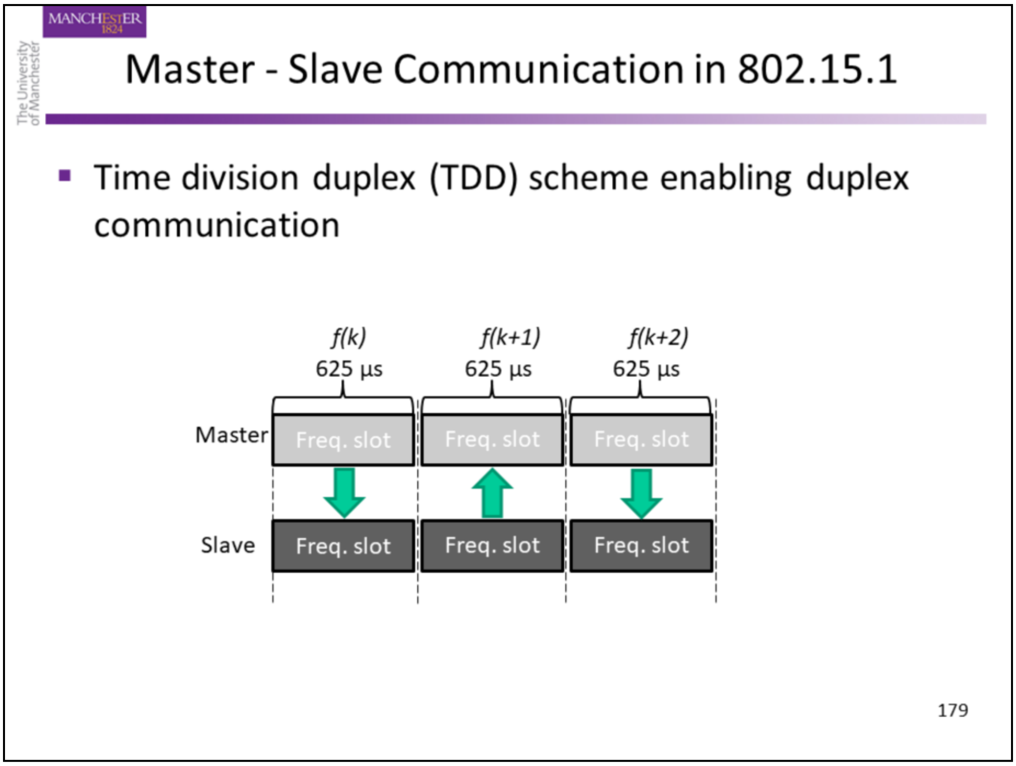
Multiple Access in WPANs

- WPAN operate at ISM 2.4 GHz!!!
  - Interference can happen within the POS of the network due to what source…???
- Fast Frequency Hopping (FFH) is utilized to minimize interference
- Communication is established in a slotted channel
  - Data packets can occupy more than one slot. E.g., 3 or 5 slots
- Hopping rate is 1600 hops/s leading to slot duration of 625 μsec

- Packets for (different) destinations are propagated on narrow frequency bands determined by the hopping sequence.
- Frequencies within the ISM 2.4 GHz band are used by IEEE 802.15.1

Geographical region	Regulatory range (GHz)	RF channel slots (MHz)
USA, Europe, and most other countries	2.4000 – 2.4835	f = 2401 + k (k = 0, ……., 78)
Spain	2.4450 – 2.4750	f = 2449 + k (k = 0, ……., 22)
France	2.4465 – 2.4835	f = 2454 + k (k = 0, ……., 22)

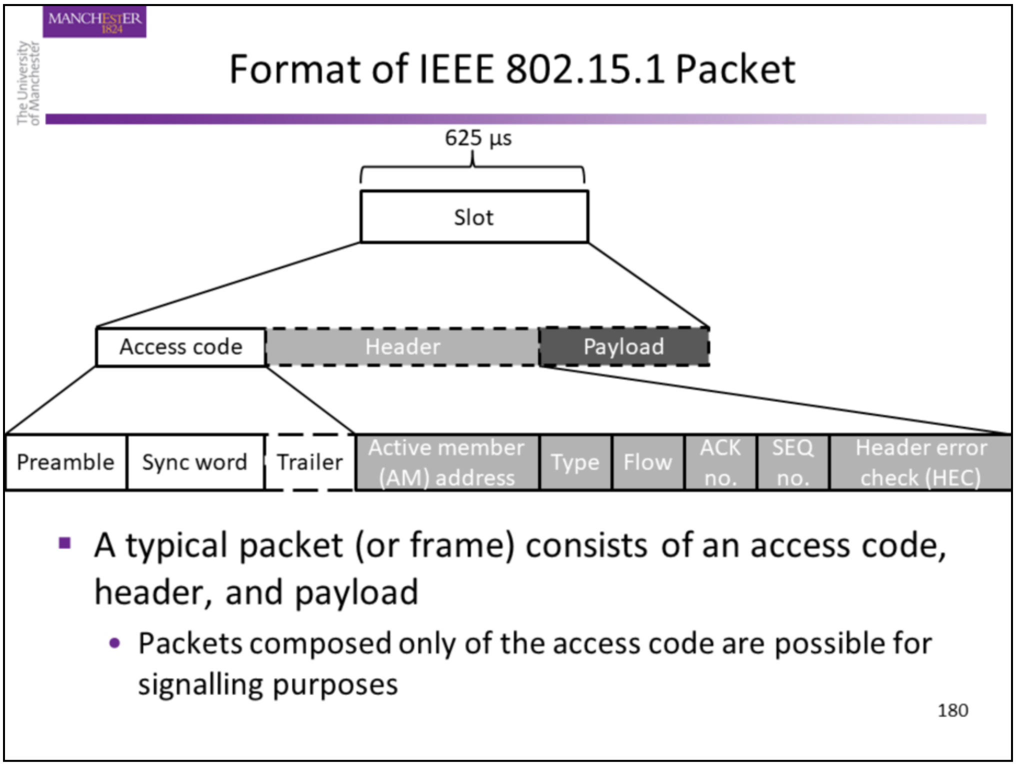
- Note that products implementing the reduced frequency band will not work with products implementing the full band.



Master - Slave Communication in 802.15.1

- Time division duplex (TDD) scheme enabling duplex communication

- The duration of the slots is kept small to also lead to efficient duplex communication.
- There are 2^{27} slots which are repeated once the slot 2^{27} - 1 is reached.
- The master and slave devices transmit on alternating numbered slots. The master node transmits only on even-numbered slots while slave nodes deliver their packets only on odd-numbered slots.
- The rule of transmission on either even or odd slots is followed even when a packet extends to three or five slots in length. In these cases, depending on whether the delivered packet extends to three or five slots, the regular transmission slot(s) will simply be skipped.
- Slaves are only allowed to communicate with the master, and only in slots following a slot in which their AM_ADDR (see corresponding slide on Addressing for the definition of this term) was in the header sent by the master.
- For an SCO slot, the slave is allowed to transmit in its designated slot as long as another slave device's AM_ADDR is not addressed in the preceding packet header sent by master node.



Format of IEEE 802.15.1 Packet

625 µs

Slot

Access code | Header | Payload

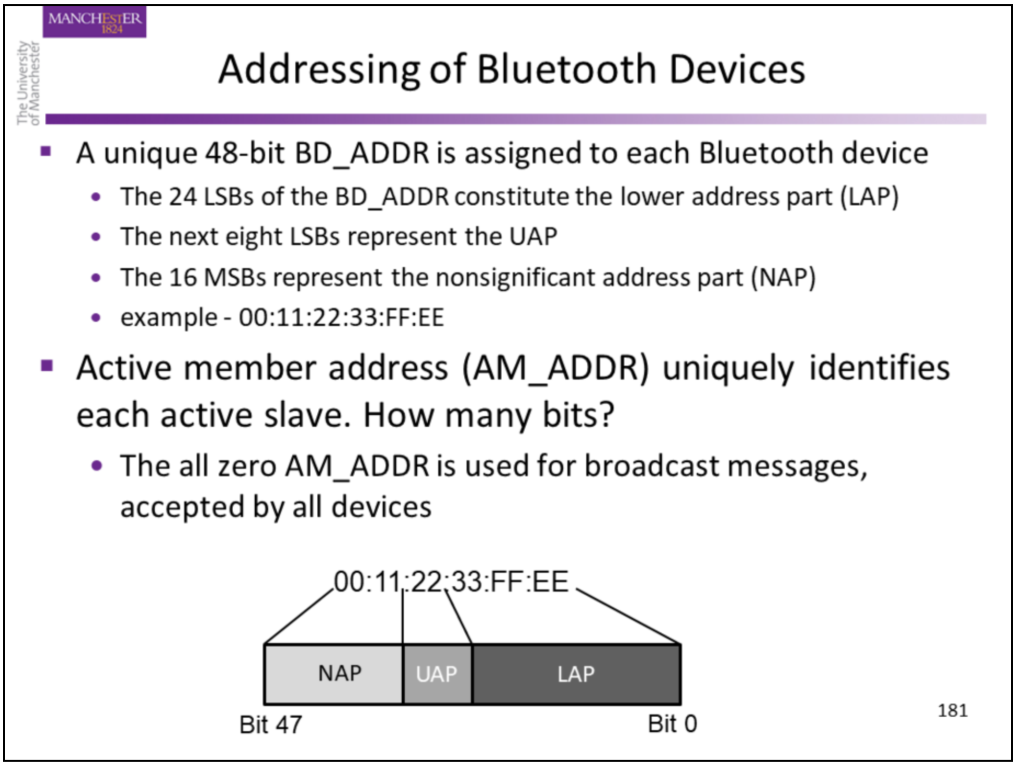
Preamble | Sync word | Trailer

Active member (AM) address | Type | Flow | ACK no. | SEQ no. | Header error check (HEC)

- A typical packet (or frame) consists of an access code, header, and payload
  - Packets composed only of the access code are possible for signalling purposes

180

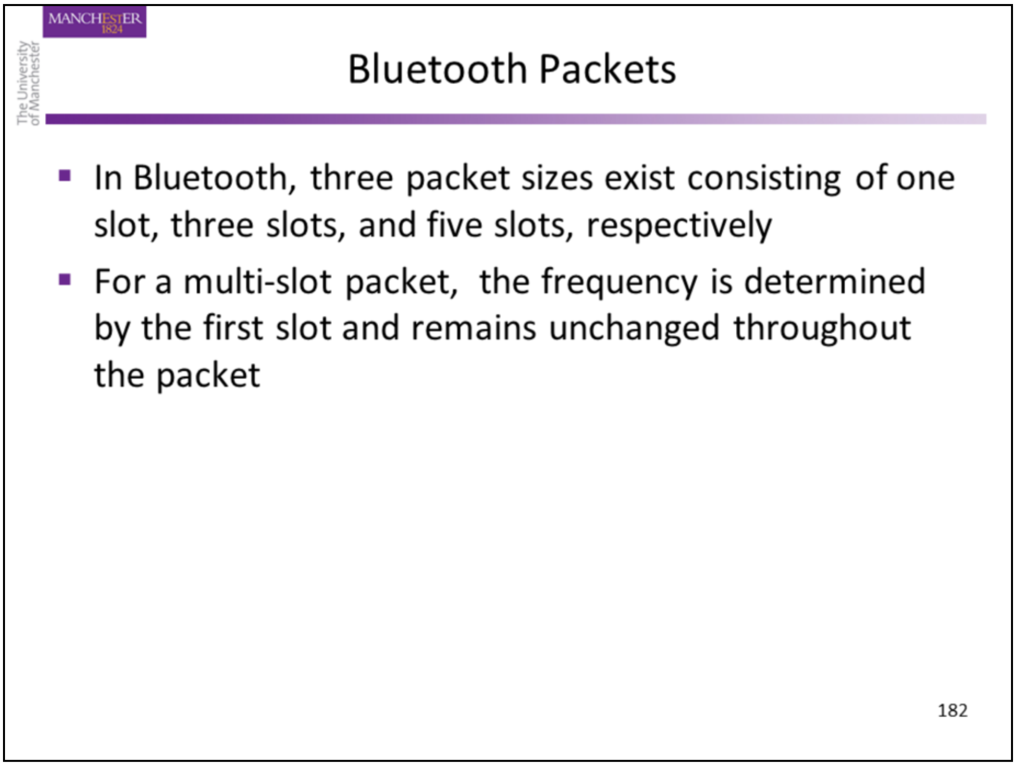
- Packets are sent with the least significant bit (LSB) being transmitted first.
- The field of the access code is used to identify particular WPANs from each other.
- The header part is used for packet transmission management. Header data is encoded reaching 54 bits from 18 bits of real information.
- The payload carries the information transmitted.
- The access code comes in one of three types: channel access code (CAC) used for piconet identification, device access code (DAC) exploited for paging, and inquiry access code (IAC) utilized for discovering compatible devices located within the piconet's POS. These access codes consist of a *preamble*, *sync word*, and a *trailer* if there is a header.
- The *preamble* will be 0101 if the LSB of the sync word is 0; otherwise, it will be set to 1010. The trailer is 1010 if the most significant bit (MSB) of the sync word is 0, else, it will be 0101.
- The *sync word* is a 64-bit word that is based upon a 24-bit address. This address is called the lower address part (LAP) and is used by the master for CAC, the slave for DAC, or a dedicated LAP for IAC.
- The *header* has six fields: The **active member address (AM_ADDR)** field is used to identify active members of a piconet. The type field is used to indicate the packet type, such as SCO versus ACL. The flow field is used to determine overflow. The acknowledgment request notification (ARQN) field acknowledges successful transmissions. The sequence (SEQN) field enables appropriate merging of large data files that were segmented for transmission over the air interface. The header error check (HEC) field ensures data integrity.
- There are several types of packets, for example high quality audio packets (HV1, HV2, HV3), and data – voice packets that combine audio and data in a single packet.



Addressing of Bluetooth Devices

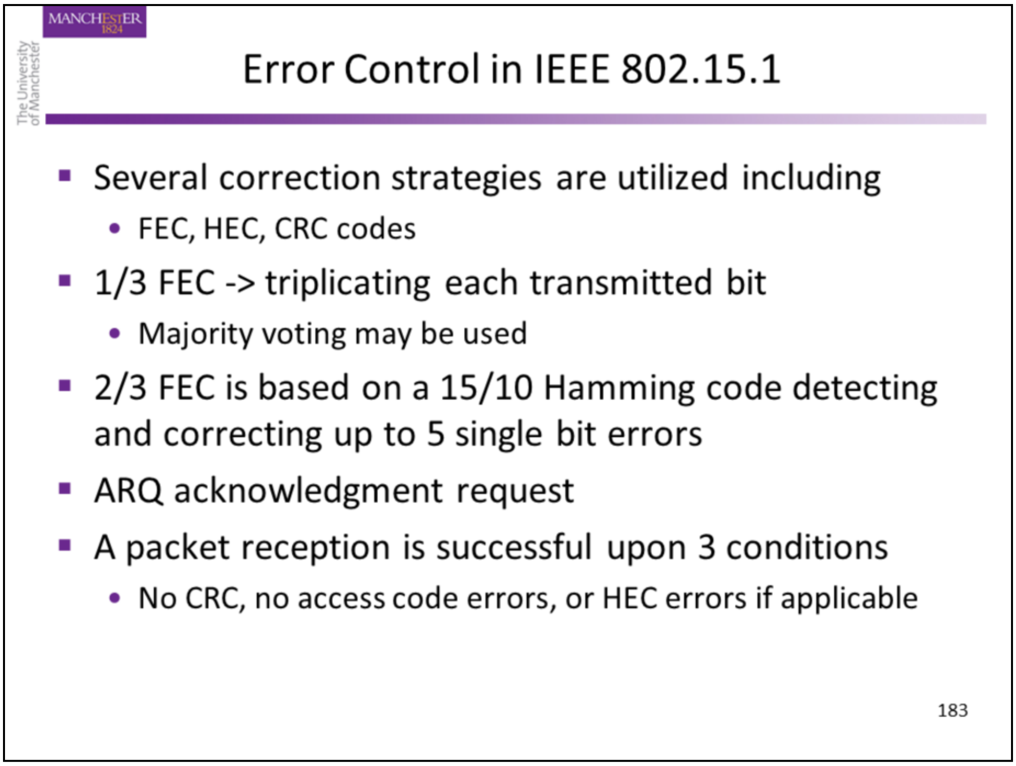
- A unique 48-bit BD_ADDR is assigned to each Bluetooth device
  - The 24 LSBs of the BD_ADDR constitute the lower address part (LAP)
  - The next eight LSBs represent the UAP
  - The 16 MSBs represent the nonsignificant address part (NAP)
  - example - 00:11:22:33:FF:EE
- Active member address (AM_ADDR) uniquely identifies each active slave. How many bits?
  - The all zero AM_ADDR is used for broadcast messages, accepted by all devices

- There are three access codes used in the IEEE 802.15.1 standard.
- These are channel address code (CAC), device access code (DAC), and inquiry address code (IAC). All of these codes are derived from the BD_ADDR’s LAP.
- The CAC is generated from the master’s BD_ADDR LAP and is used in the preamble of every packet exchanged in the piconet.
- The NAP and UAP combined determine the Organizationally Unique Identifier (OUI) of the device.



Bluetooth Packets

- In Bluetooth, three packet sizes exist consisting of one slot, three slots, and five slots, respectively
- For a multi-slot packet, the frequency is determined by the first slot and remains unchanged throughout the packet



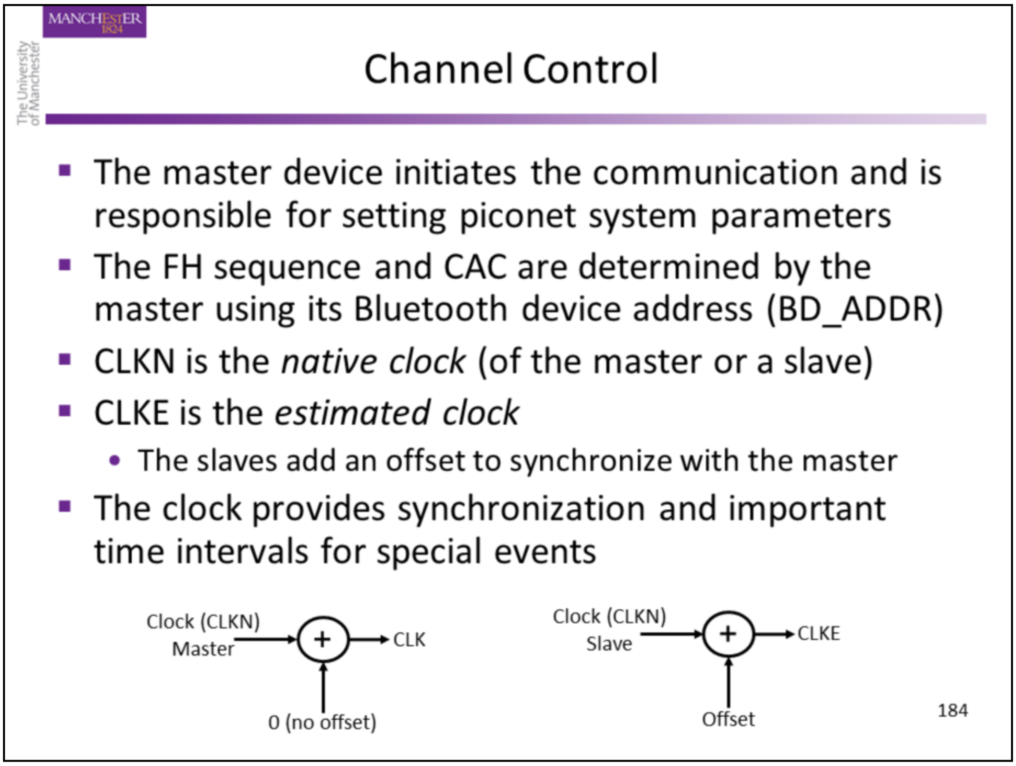
MANCHESTER 1824

The University of Manchester

Error Control in IEEE 802.15.1

- Several correction strategies are utilized including
  - FEC, HEC, CRC codes
- 1/3 FEC -> triplicating each transmitted bit
  - Majority voting may be used
- 2/3 FEC is based on a 15/10 Hamming code detecting and correcting up to 5 single bit errors
- ARQ acknowledgment request
- A packet reception is successful upon 3 conditions
  - No CRC, no access code errors, or HEC errors if applicable

- 2/3 FEC can also detect double bit errors but these cannot be corrected through this code.
- If ARQ is not received, packets are continually retransmitted until an ARQ is received or a time out period is reached.
- The CAC of a received packet is initially checked to ensure that this packet originates from the appropriate piconet (in case multiple piconets exist in the POS of a slave).
- Subsequently, the HEC is checked for errors in the header field and finally the CRC is checked for errors in the payload.
- Typically, the HEC and CRC codes are generated using 8- and 16-bit linear feedback shift register (LFSR) circuits, respectively.

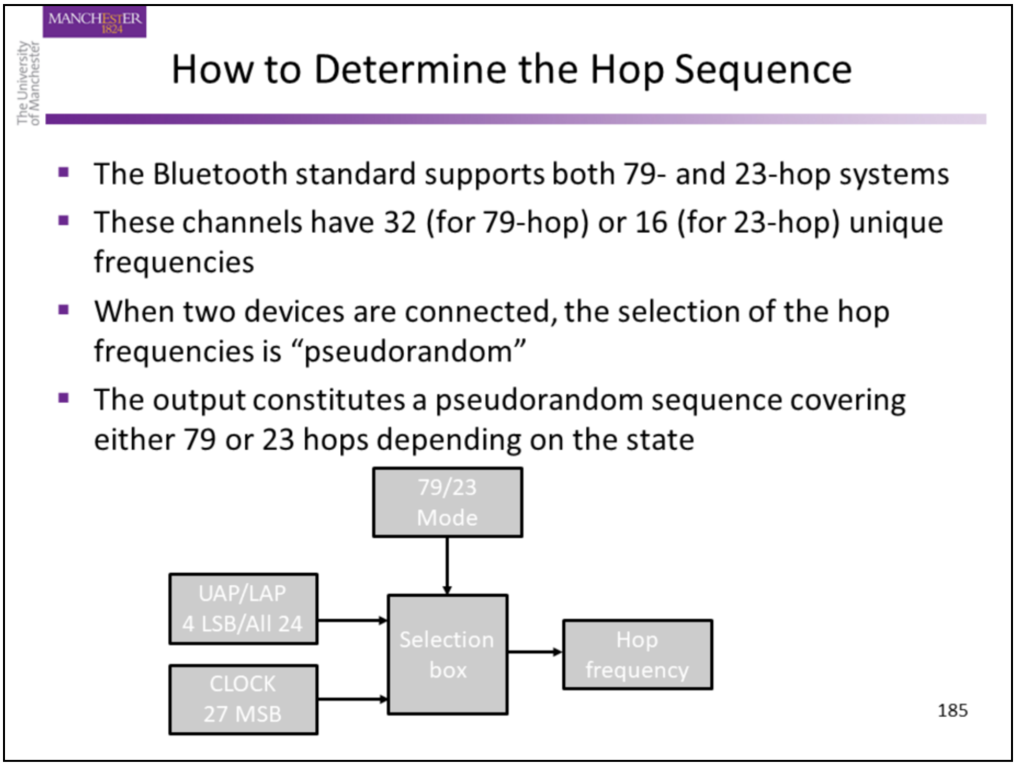


Channel Control

- The master device initiates the communication and is responsible for setting piconet system parameters
- The FH sequence and CAC are determined by the master using its Bluetooth device address (BD_ADDR)
- CLKN is the *native clock* (of the master or a slave)
- CLKE is the *estimated clock*
  - The slaves add an offset to synchronize with the master
- The clock provides synchronization and important time intervals for special events

- Every Bluetooth unit has a free-running internal clock which is used for timing and frequency regulation of each transceiver.
- Bits [0:27] used in the free running clock to produce the required timings. In the table below, only the bits related to the timings of the standard are depicted.

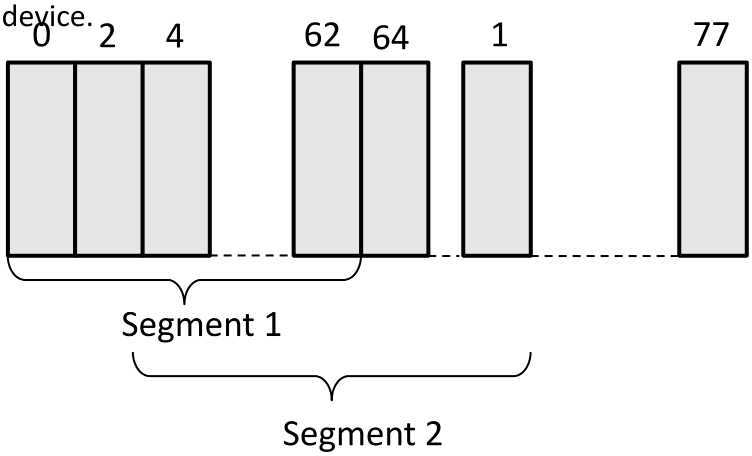
CLK 3.2 KHz						
27	26-13	12	11-3	2	1	0
MSB	Non critical	1.28 sec	Non critical	1.25 msec	625 μsec	312.5 μsec

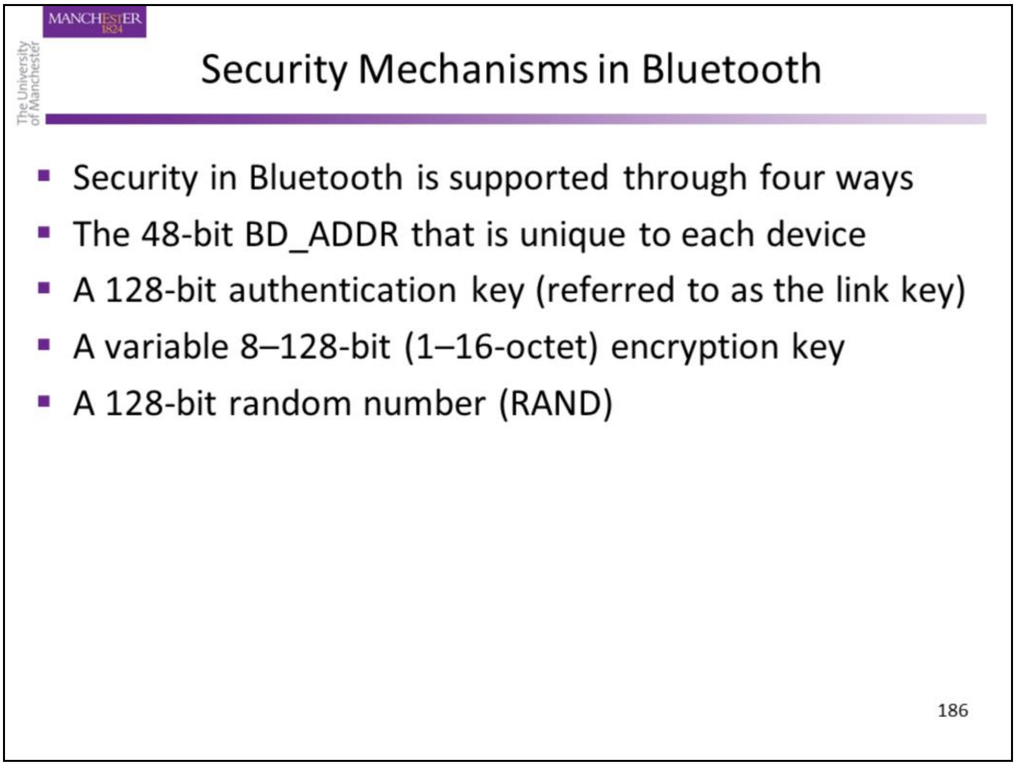


How to Determine the Hop Sequence

- The Bluetooth standard supports both 79- and 23-hop systems
- These channels have 32 (for 79-hop) or 16 (for 23-hop) unique frequencies
- When two devices are connected, the selection of the hop frequencies is “pseudorandom”
- The output constitutes a pseudorandom sequence covering either 79 or 23 hops depending on the state

- In addition, there is also a long period channel-hopping sequence used to distribute the hop frequencies equally over the available bandwidth.
- The output constitutes a pseudorandom sequence covering either 79 or 23 hops depending on the state of the device. These segments and their overlap are illustrated in the Figure below.
- The segments are listed in order with all even hop frequencies listed together followed by all odd hop frequencies. This approach allows for better distribution of hop frequencies within a given segment.
- Each piconet has a unique hop sequence that is determined by the clock and address of the master device.

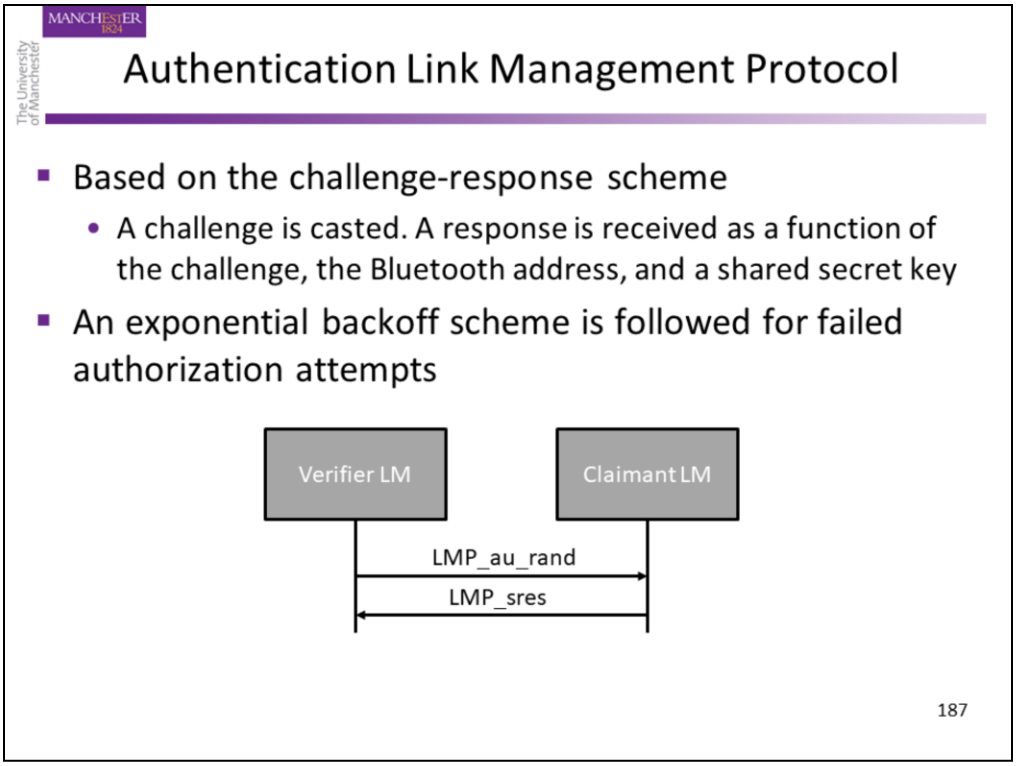




Security Mechanisms in Bluetooth

- Security in Bluetooth is supported through four ways
- The 48-bit BD_ADDR that is unique to each device
- A 128-bit authentication key (referred to as the link key)
- A variable 8–128-bit (1–16-octet) encryption key
- A 128-bit random number (RAND)

- The link key is an 128-bit randomly generated number which is used for authentication as well as encryption key generation.
- There are four types of link keys: combination key (KAB), unit key (KA), temporary key (Kmaster), and initialization key (Kinit). There is also an encryption key (Kc).



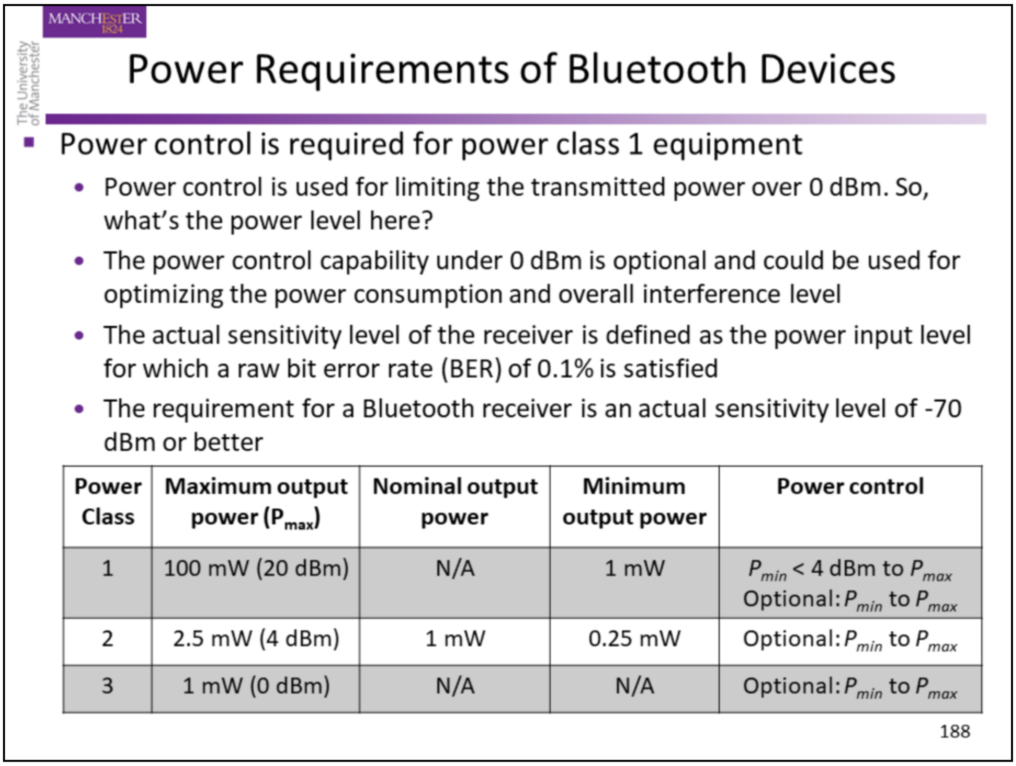
Authentication Link Management Protocol

- Based on the challenge-response scheme
  - A challenge is casted. A response is received as a function of the challenge, the Bluetooth address, and a shared secret key
- An exponential backoff scheme is followed for failed authorization attempts

Verifier LM
Claimant LM
LMP_au_rand
LMP_sres

187

- The verifier sends a protocol data unit (PDU) packet with a randomly generated authentication number, LMP_au_rand.
- The claimant calculates a response, LMP_sres, and sends it back to the verifier.
- Authentication is granted only if the response is correct; otherwise, authentication is denied.
- The response is a function of the challenge, the claimant’s BD_ADDR, and their shared secret key.



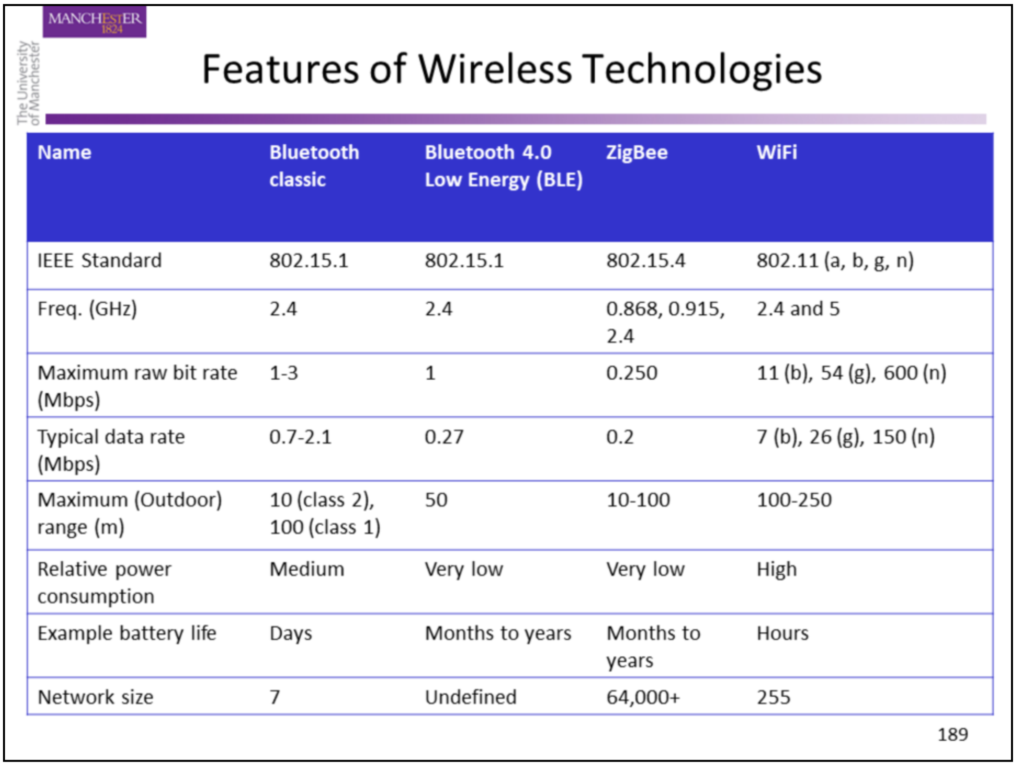
Power Requirements of Bluetooth Devices

- Power control is required for power class 1 equipment
  - Power control is used for limiting the transmitted power over 0 dBm. So, what's the power level here?
  - The power control capability under 0 dBm is optional and could be used for optimizing the power consumption and overall interference level
  - The actual sensitivity level of the receiver is defined as the power input level for which a raw bit error rate (BER) of 0.1% is satisfied
  - The requirement for a Bluetooth receiver is an actual sensitivity level of -70 dBm or better

Power Class	Maximum output power (P_{max})	Nominal output power	Minimum output power	Power control
1	100 mW (20 dBm)	N/A	1 mW	P_{min} < 4 dBm to P_{max} Optional: P_{min} to P_{max}
2	2.5 mW (4 dBm)	1 mW	0.25 mW	Optional: P_{min} to P_{max}
3	1 mW (0 dBm)	N/A	N/A	Optional: P_{min} to P_{max}

188

- The power steps should form a monotonic sequence with a maximum step size of 8 dB and a minimum step size of 2 dB.
- Class 1 equipment with a maximum transmit power of +20 dBm must be able to control its transmit power down to 4 dBm or less.
- Link Management Protocol commands optimize the output power for devices with power control capability.



Features of Wireless Technologies

Name	Bluetooth classic	Bluetooth 4.0 Low Energy (BLE)	ZigBee	WiFi
IEEE Standard	802.15.1	802.15.1	802.15.4	802.11 (a, b, g, n)
Freq. (GHz)	2.4	2.4	0.868, 0.915, 2.4	2.4 and 5
Maximum raw bit rate (Mbps)	1-3	1	0.250	11 (b), 54 (g), 600 (n)
Typical data rate (Mbps)	0.7-2.1	0.27	0.2	7 (b), 26 (g), 150 (n)
Maximum (Outdoor) range (m)	10 (class 2), 100 (class 1)	50	10-100	100-250
Relative power consumption	Medium	Very low	Very low	High
Example battery life	Days	Months to years	Months to years	Hours
Network size	7	Undefined	64,000+	255