Bluetooth: IEEE 802.15.1

→ PAN (personal area network)

Features:

• overlapping 2.4 GHz ISM frequency band
  → 2.402–2.480 GHz

• divide into 79 carrier frequencies (i.e., channels)
  → 1 MHz bandwidth each

• target range ∼10 m

• bandwidth range 125 Kbps–2 Mbps
  → between WLAN and IoT (Internet of Things)
  → has become key IoT enabling technology
Centralized master/slave architecture:

→ 1 master \((M)\), up to 7 slave \((S)\) devices

→ polling based MAC protocol

→ contention-free

Bluetooth MAC:

• \(M\) selects \(S\) to communicate with
  → round-robin

• frequency hopping
  → 1600 hops per second

• TDMA with 625 \(\mu\)sec time slots

• TDD: \(M\) even slots, \(S\) odd slots

• adaptive
  → avoid crowded frequencies
  → channel map
Operation:

- two modes
  - SCO (synchronous connection oriented): isochronous streaming, no retransmission
  - ACL (asynchronous connectionless): interactive, retransmission
- nominal bandwidth: 1 Mbps (version 1.2), up to 2 Mbps (versions 3–5)
  - enhanced data rate: 24 Mbps (3.x–4.x), 50 Mbps (5.x)
- pairing: shared private key
  - PIN based
  - incorporation of cryptographic primitives
BLE (Bluetooth Low Energy):

→ Bluetooth versions 1.x–3.x: speed

→ 4.x: focus on reducing energy consumption

→ v5.x (v5.4): power efficiency, reliability, security

→ applications: smart phones + IoT and variants

→ e.g., automobiles (e.g., smart phone instead of fob as key, TPMS), home automation (e.g., light bulbs, doorlocks, security cams)

Operate at lower data rate

→ e.g., 125 Kbps–2 Mbps

→ event-driven by slave device: interrupt vs. polling

→ initiation through advertisement packets

→ focus: minimize energy consumption at slave devices
Device initiated advertisement:

- 40 channels vs. 79 for classic Bluetooth
- 3 used for advertisement
- advertisement interval: configurable 20 ms–10.24 s
- central device monitors channel activity: discovery
- responds to establish connection for data transfer
- initiated by central device, peripheral device passive

Increasing advertisement interval decreases energy consumption

→ application dependent
→ asymmetry assumption: peripheral vs. central device
→ central device: large battery capacity or connected power source
ZigBee: IEEE 802.15.4

→ low bit rate: 250 Kbps

Features

• 2.4 GHz ISM
  → 16 channels
  → plus 868 MHz and 915 MHz bands

• uses CSMA MAC protocol
  → data, ack, beacon, control frames

• both short- and long-range
  → 10 m (PAN) and 100+ m (e.g., sensor networks)

In practice, functional overlap with Bluetooth and WLAN
→ future uncertain
Control Area Network (CAN): ISO 11898
→ dominant standard for vehicular networks

CAN is dominant but on-going developments driven by changing needs.

→ CAN, LIN, Ethernet, MOST, etc.
→ intra- vs. inter-vehicle
CAN architecture:

- twisted pair copper with differential coding
  → similar to FastEthernet and telephone wires
- maximum bandwidth 1 Mbps
  → 5 Mbps on CAN-FD (flexible data-rate)
- connect tens of ECUs (electronic control units) in vehicles
  → engine, transmission, brake, suspension, sensors, lights, battery, navigation, infotainment, etc.
  → some more critical than others
  → real-time constraints
- MAC protocol: CSMA/CD
  → what’s going on?
  → non-destructive arbitration (NDA)
CAN data frame format

→ 1-bit SOF (start-of-frame)

→ 11-bit identifier (CAN 2.0A)

→ 29-bit identifier (CAN 2.0B)

→ control, payload, CRC, EOF (end-of-frame) bits

Role of 11-bit identifier field

→ packet priority

→ 00000000000: highest priority

→ 11111111111: lowest priority
Example: captured CAN frame

CAN HI (red) signal:
→ high voltage bit value 1
→ low voltage bit value 0
CSMA/CD with NDA example:

- bus arbitration method: wired-AND
- collision does not lead to frame destruction
  \[\rightarrow\] TDMA time slots are not wasted
CSMA/CD with NDA: works as long as there is one clear winner

→ one highest priority (i.e., identifier) frame
→ careful design and operation

Suffers under weakness of priority scheduling

→ delay of lower priority frames
→ potential starvation
→ lower priority does not imply unimportant

Scalability.

Works underway for implementing generalized real-time packet scheduling.
RFID (Radio Frequency Identification) and NFC (Near Field Communication):

→ low-bit rate, short-distance wireless communication

→ NFC: close proximity (inches)

→ inductive/magnetic coupling

Device: two types

• reader/writer

• tag

Frequency band

• 125 KHz (unregulated): RFID

• 13.56 MHz (ISM): RFID, NFC

• others (e.g., 433.92 MHz, 915 MHz ISM)
Bandwidth

→ from 4 Kbps up to 848 Kbps

→ ISO 14443, 18000-x

→ NFC Forum

Tag has battery power:

• yes: active

• no: passive

→ requires specialized techniques

→ focus
Passive: inductive coupling enabled communication

- reader energizes tag
  - → primary function
- clock synchronization
- backscatter
  - → tag modulates reader’s signal: e.g., AM
  - → full duplex
- capacitor
  - → transient energy store
  - → half duplex
MAC protocol: polling
→ multiple tags: collision
→ e.g., inventory systems

Reader detects collision
• instruct tags to randomize
  → tags inject pseudo-random delay: i.e., CA
• tree walking
  → binary search

Three operating modes in NFC
• reader/writer
• card emulation
  → e.g., smartphone acts as tag
• peer-to-peer
  → symmetric