Wireless Networks for Mobile Applications

Prof. Claudio Palazzi
cpalazzi@math.unipd.it

Università degli Studi di Padova

Bluetooth

Where does the name come from?

Harald Blaatand “Bluetooth” II
King of Denmark 940-981

- Harald christianized the Danes
- Harald controlled Denmark and Norway

Bluetooth working group history

- February 1998: The Bluetooth SIG is formed
  - promoter company group: Ericsson, IBM, Intel, Nokia, Toshiba
- May 1998: Public announcement of the Bluetooth SIG
- July 1999: 1.0A spec (>1,500 pages) is published
- December 1999: ver. 1.0B is released
- December 1999: The promoter group increases to 9
  - 3Com, Lucent, Microsoft, Motorola
- March 2001: ver. 1.1 is released
- Aug 2001: There are 2491+ adopter companies
- Today: almost all connected devices have Bluetooth

What does Bluetooth do for you?

Synchronization

- Automatic synchronization of calendars, address books, business cards
- Push button synchronization
- Proximity operation

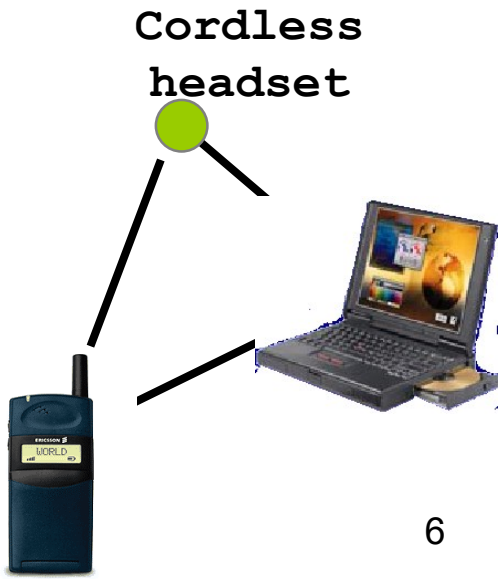
Cordless Headset

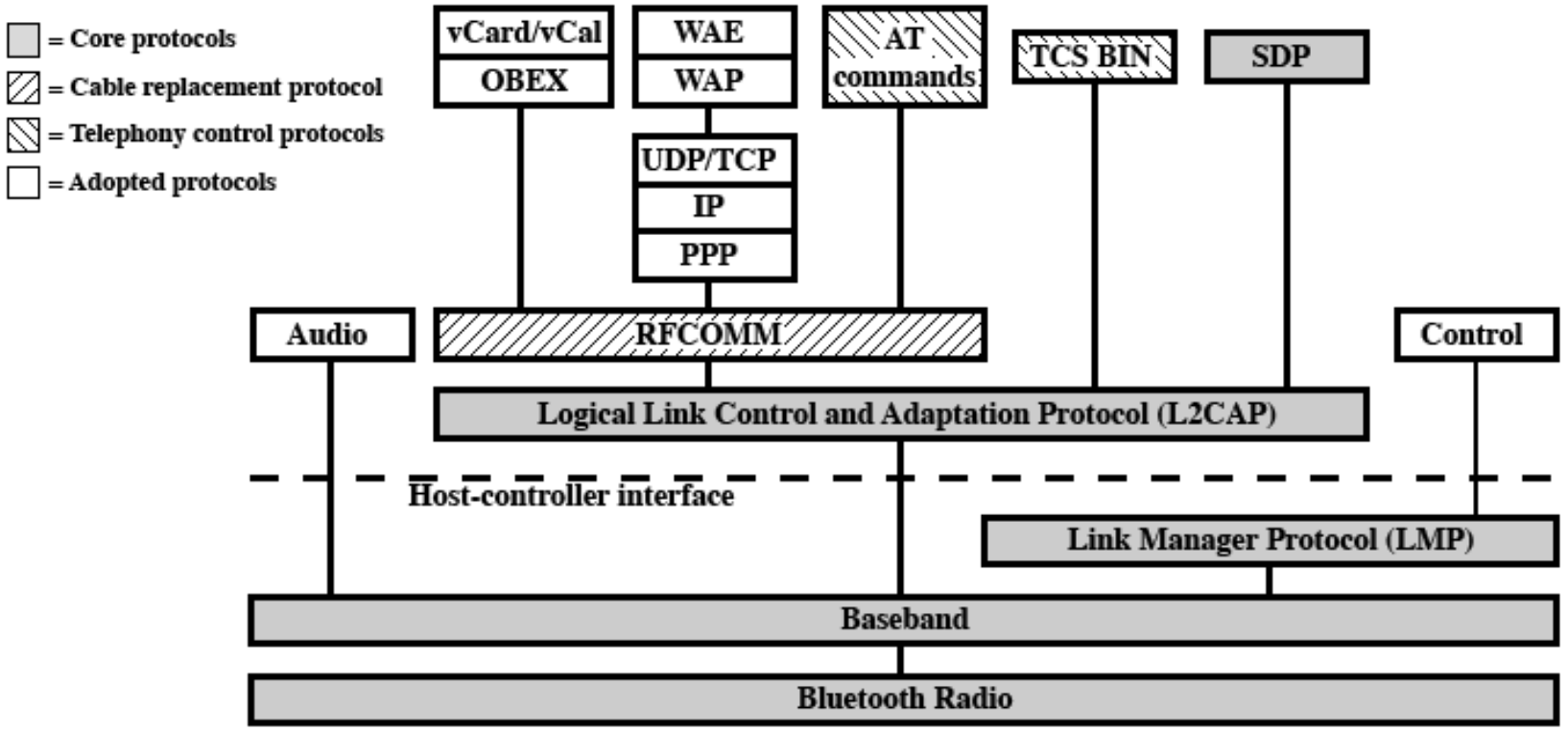
User benefits

- Multiple device access
- Cordless phone benefits
- Hands free operation

Examples of use

- Cordless Headset
- Portable PC speakers
- Cordless printer, scanner, keyboard, mouse, LAN
- Synchronization among devices
- Internet bridge
- Direct file sharing among devices
- Ad hoc networking
- IoT
- …





AT	=	attention sequence (modem prefix)	TCS BIN	=	telephony control specification - binary
IP	=	Internet Protocol	UDP	=	User Datagram Protocol
OBEX	=	Object exchange protocol	vCal	=	virtual calendar
PPP	=	Point-to-Point Protocol	vCard	=	virtual card
RFCOMM	=	radio frequency communications	WAE	=	wireless application environment
SDP	=	service discovery protocol	WAP	=	wireless application protocol
TCP	=	transmission control protocol			

Bluetooth Protocol Stack

Protocol Architecture

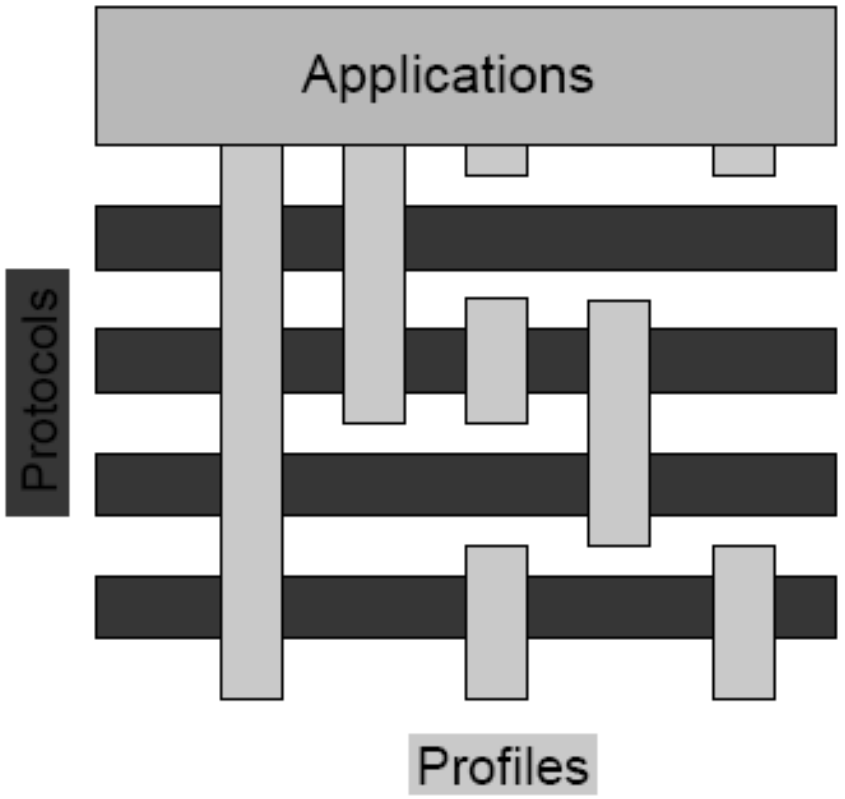
- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
    - Details of air interface (frequency hopping, modulation, tx power)
  - Baseband
    - Connection establishment in Piconet, pckt format, timing, addressing
  - Link manager protocol (LMP)
    - Setup between Bluetooth devices, security aspects, authentication, encryption
  - Logical link control and adaptation protocol (L2CAP)
    - Adapts upper-layer protocols with Baseband
  - Service discovery protocol (SDP)
    - Device information, services
    - To establish a connection between two or more bluetooth devices

Protocol Architecture

- Cable replacement protocol
  - RFCOMM (virtual serial port)
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols (use existing protocols and invent new ones only when necessary)
  - PPP (Point-to-Point protocol, IP datagrams over a point-to-point link)
  - TCP/UDP/IP
  - OBEX (Object Exchange protocol, defines objects and operations)
    - Defined by Infrared Data Association (IrDA)
  - WAE/WAP (Wireless Application Environment/Protocol)

Interoperability and Profiles

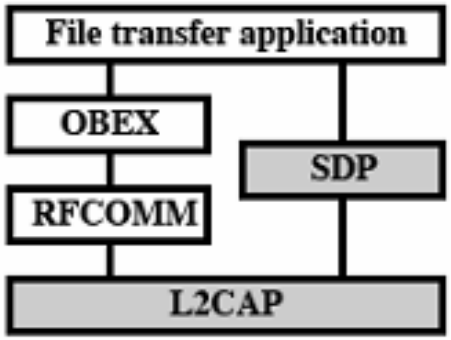
- Represents default solution for a usage model
- Vertical slice through the protocol stack
- Basis for interoperability and logo requirements
- Each Bluetooth device supports one or more profiles



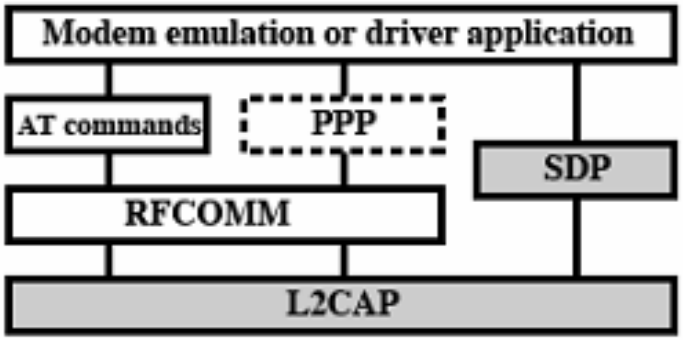
Bluetooth Usage Models

- File transfer
- Internet bridge
- LAN access
- Synchronization
- Three-in-one phone
- Headset

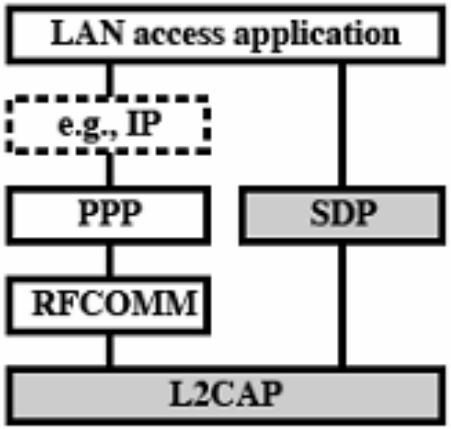
Bluetooth Usage Model



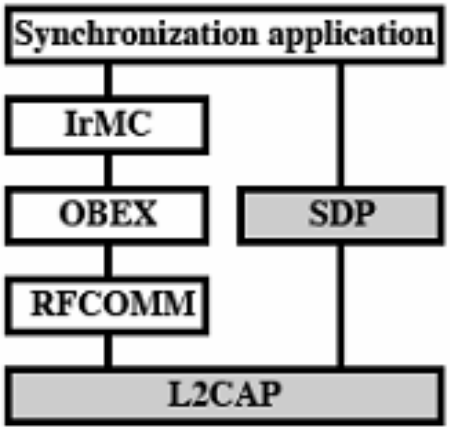
(a) File transfer



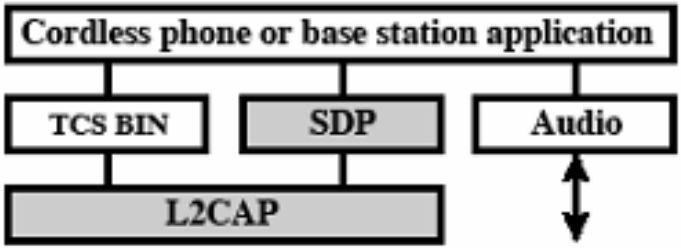
(b) Dial-up networking



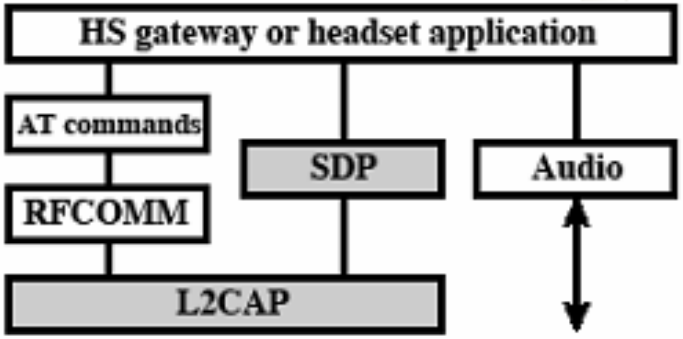
(c) LAN access



(d) Synchronization



(e) Cordless phone and intercom



(f) Headset

Bluetooth Radio and Baseband Parameters

- Topology: up to 7 simultaneous links in a logical star
- Peak data rate: 1 Mbps
- RF Band: 2.4 GHz
- Frequency allocations (in US and EU): 2.4 to 2.4835 GHz
- RF Channels: 2.402 GHz + n MHz (n = 0, …, 78)
- Carrier Spacing: 1 MHz
- Transmit power: 0.1 mW
- Piconet access: FH-TDD-TDMA
- Scatternet access: FH-CDMA
- Hop Rate: 1600 hops per second (625us duration per hop)

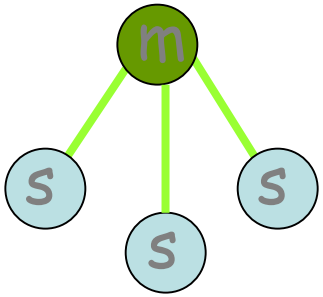
What is a Piconet?

- A collection of devices connected in an ad-hoc fashion.
- One unit will act as a master and the others as slaves for the duration of the piconet connection.
- Master sets the clock and hopping pattern.
- Each piconet has a unique hopping pattern/ID
  - Pseudo-randomly chosen
- Each master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet

Bluetooth Physical link

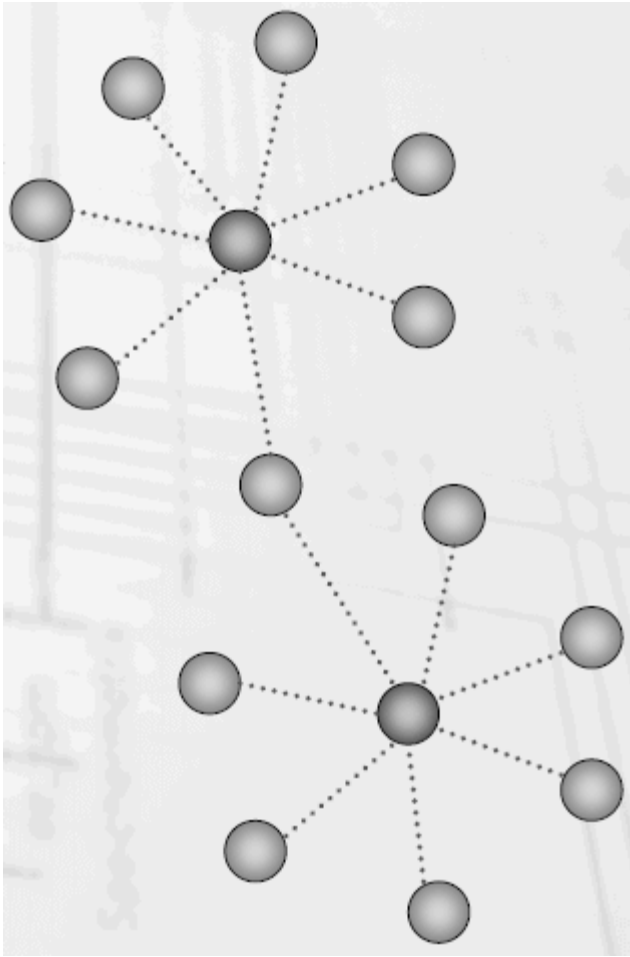
- Point to point link
  - master - slave relationship
  - nodes can function as masters or slaves

- Piconet
  - Master can connect to 7 slaves
  - Each piconet has max capacity =1 Mbps
  - hopping pattern is determined by the master



Bluetooth Physical link

- **Interconnected piconets**
- **One master per piconet**
- **Few devices shared between piconets**
  - Master/Slave
  - Slave/Slave
  - Need special features
- **No central network structure**
  - “Ad-hoc” network



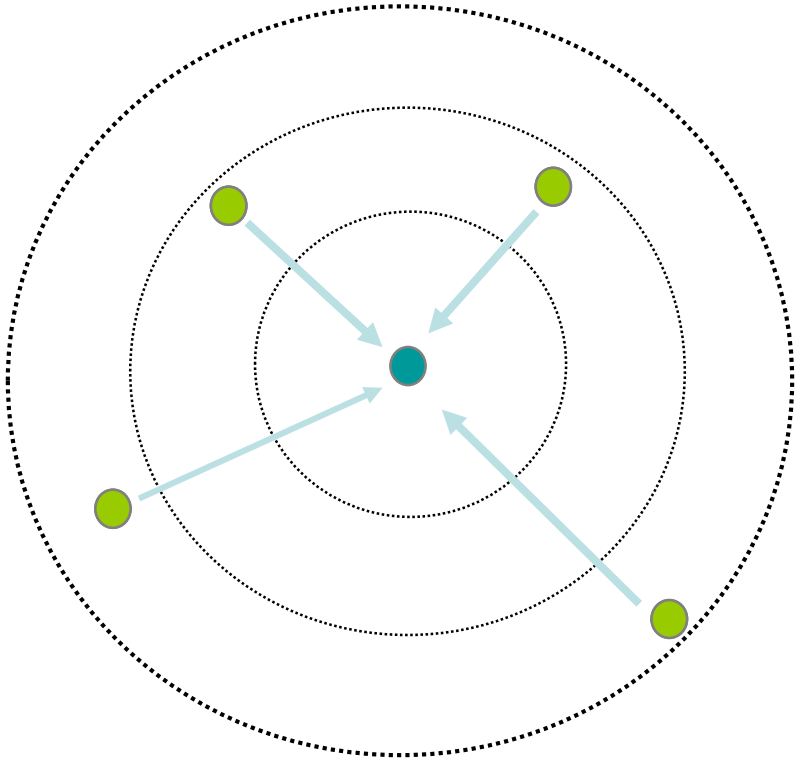
Piconets and Scatternets

- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase

- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth

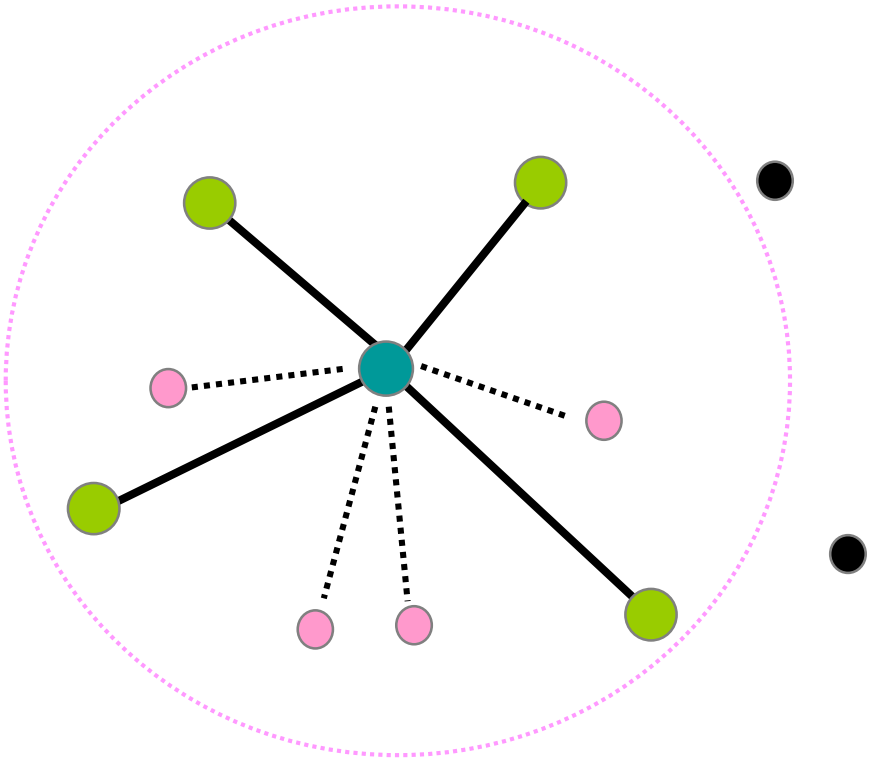
Connection Setup

- Inquiry - scan protocol
  - to learn about the clock offset and device address of other nodes in proximity



Piconet formation

- Page - scan protocol
  - to establish links with nodes in proximity

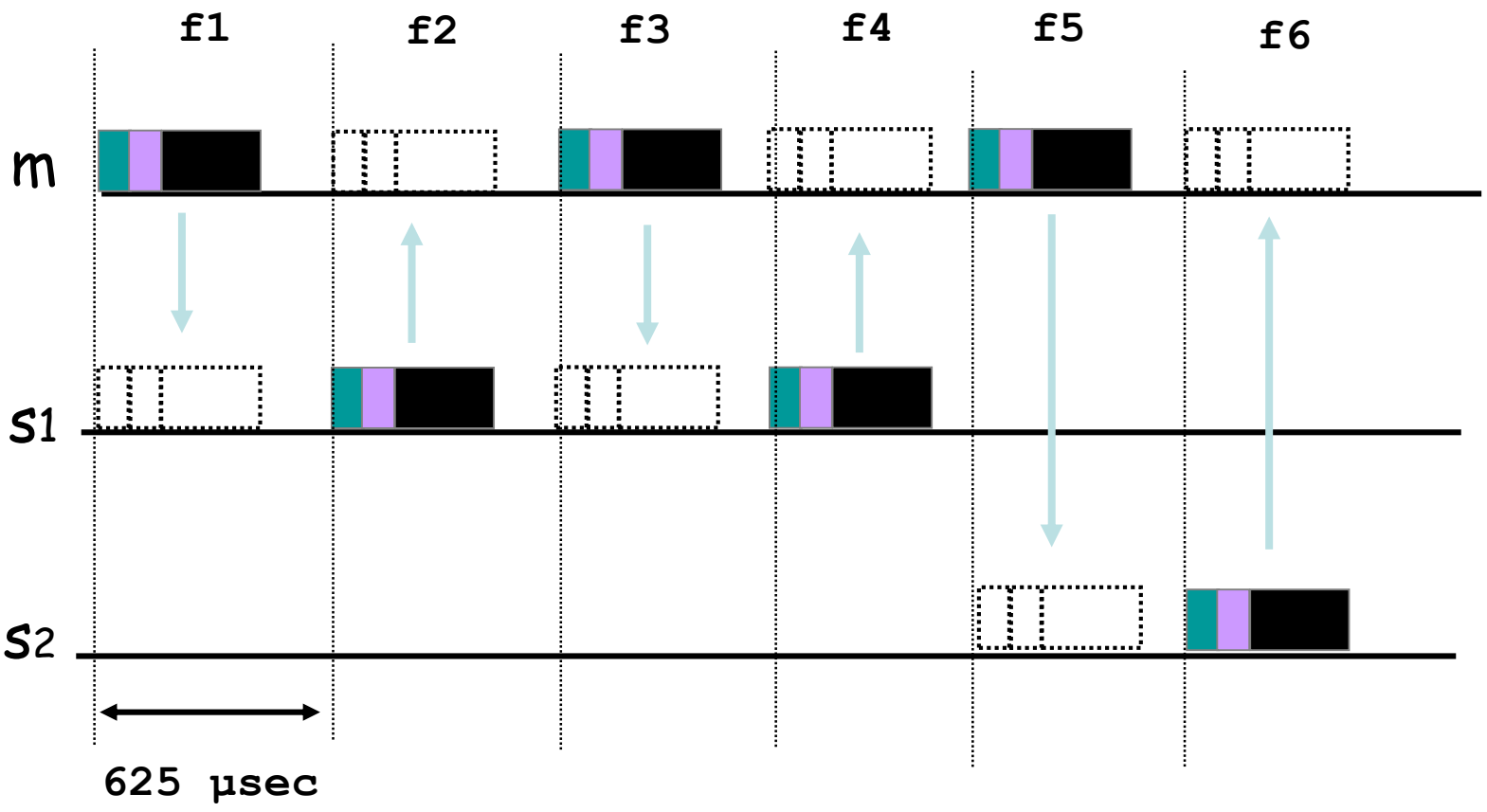


Addressing

- Bluetooth device address (BD_ADDR)
  - 48 bit IEEE MAC address
- Active Member address (AM_ADDR)
  - 3 bits active slave address
  - all zero broadcast address
- Parked Member address (PM_ADDR)
  - 8 bit parked slave address

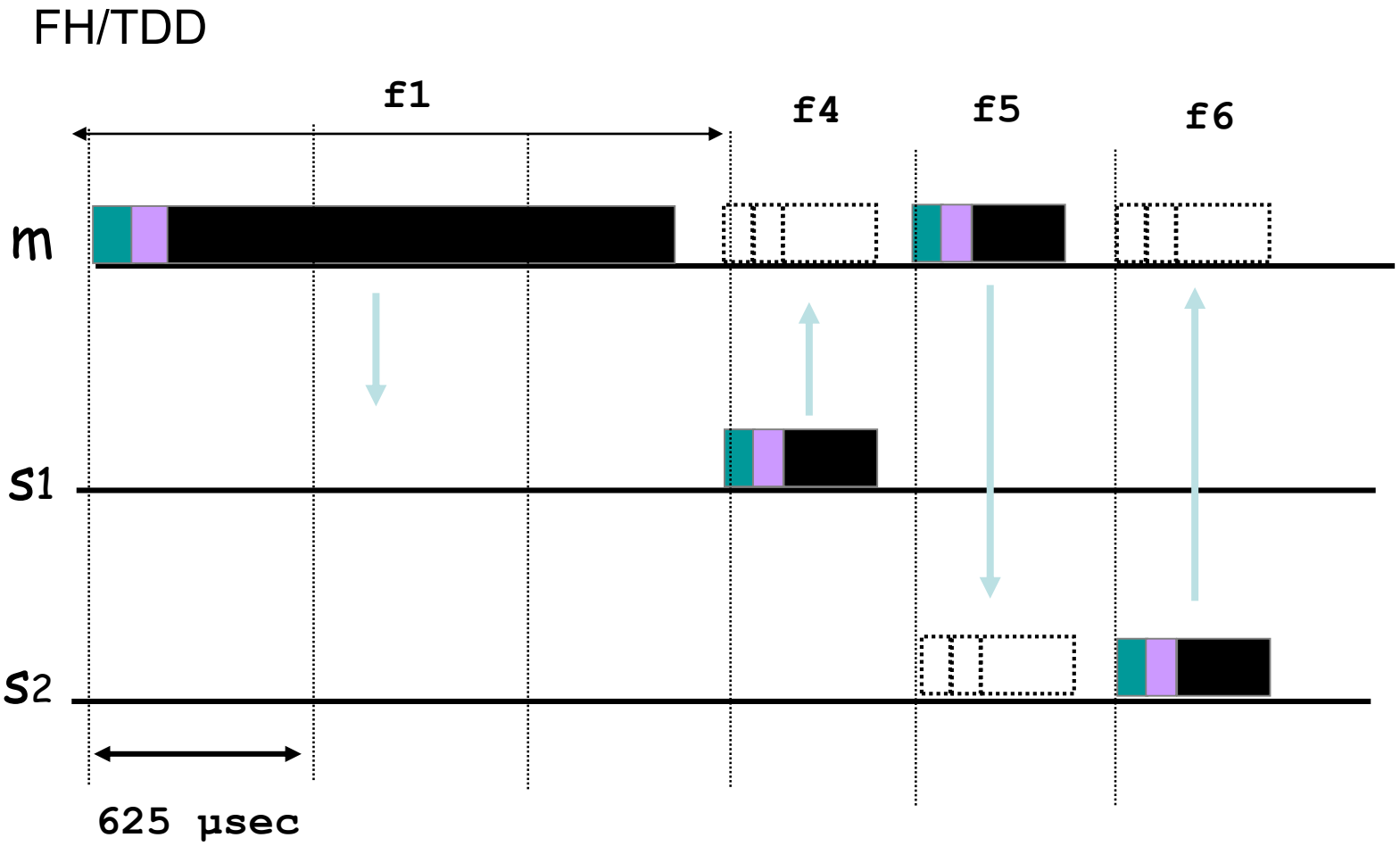
Piconet MAC protocol: Polling

FH/TDD



1600 hops/sec

Multi slot packets



Data rate depends on type of packet

Error Correction Schemes

- 1/3 rate FEC (forward error correction)
  - Used on 18-bit packet header, voice field in HV1 packet
- 2/3 rate FEC
  - Used in DM packets, data fields of DV packet, FHS packet and HV2 packet
- ARQ
  - Used with DM and DH packets

ARQ Scheme Elements

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgment
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits

Many Versions

- Bluetooth 1.0
- Bluetooth 1.1
- Bluetooth 1.2
- Bluetooth 2.0 (up to 3 Mbps and reduced latency)
- Bluetooth 2.1
- Bluetooth 3.0 (improved speed and cooperation with Wi-Fi)
- Bluetooth 4.0
  - LE: Low Energy (speed up to 1Mbps)
  - UWB: Ultra Wideband
- Bluetooth 4.1 (improved interaction with 4G LTE)
- Bluetooth 4.2 (improved interaction with IoT)
- Bluetooth 5.0 (improved range, speed and interference avoidance)

IEEE 802.15.4 ZIGBEE

Meeting market needs

- No new wires
- Easy to install and maintain (mesh, self-organizing)
- Reliable (mesh, multiple channels, proven interference tolerance)
- Secure (AES 128)
- Scalability (hundreds of thousands of devices)
- Low power consumption (can sleep most of the time on, can last years on batteries)
- Low cost (small footprint)

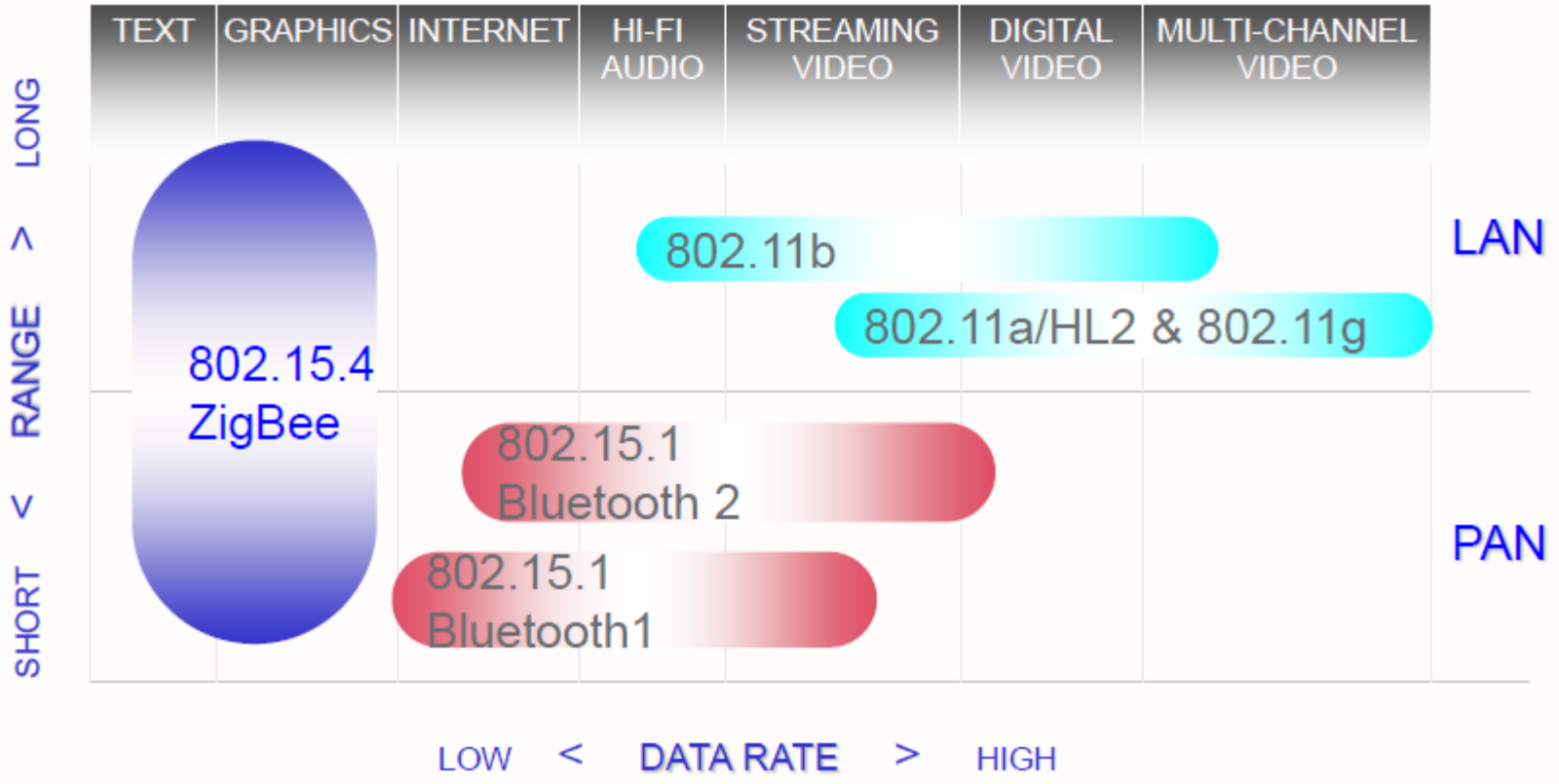
ZigBee Technology Profile

- High level communications protocol
  - Uses small, ultra low-power digital radio based on IEEE 802.15.4 wireless standard
- Targeted applications
  - secure networking
  - long battery life
  - low data rate
- RF bands
  - 2.4 GHz with 16 channels for global use
  - 915 MHz with 10 channels for NA, Australia +
  - 868 MHz with 1 channel for EU

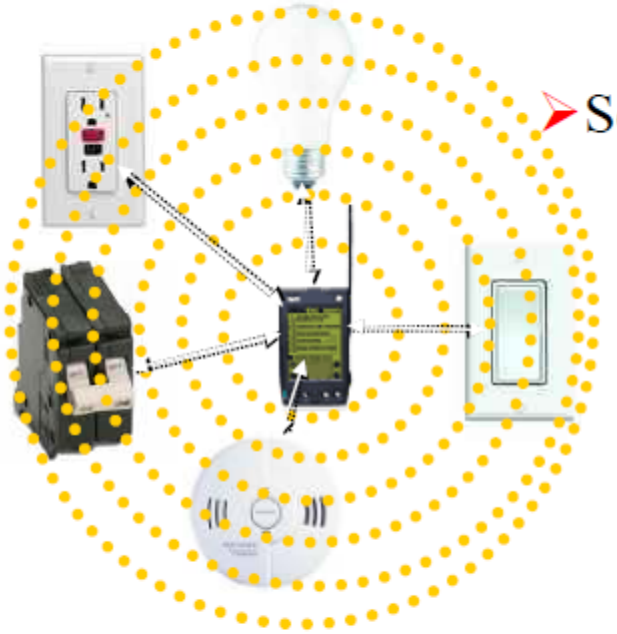
How does ZigBee compare?

ZigBee	Bluetooth	WiFi
802.15.4 standard	802.15.1 standard	802.11 standard
250 kbps	1 Mbps	< 54 Mbps
TX: 35 mA	TX: 40 mA	TX: 400+ mA
Standby: 3 uA	Standby: 200 uA	Standby: 20mA
32-60 KB memory	100+ KB memory	100+ KB memory
Lighting, sensors, RC peripherals	Telecom audio, cable replacement	Enterprise, home access points
Mesh networking	Pt-Mpt	Pt-Mpt

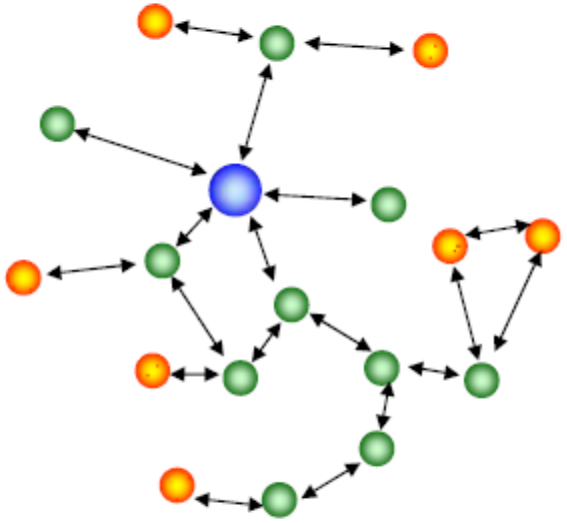
Applications



802.15.4 Application Space

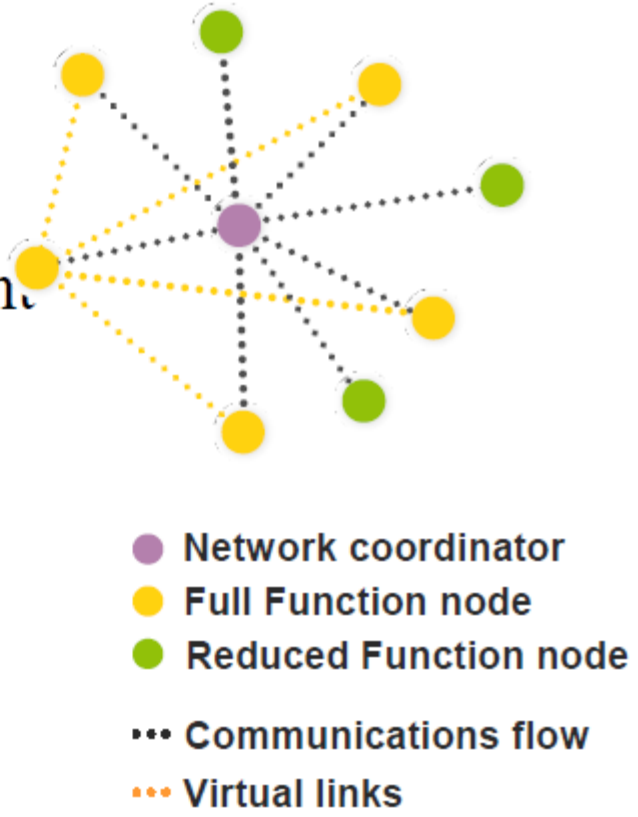


- Sensors & Controls:
  - Home Automation
  - Industrial Automation
  - Remote Metering
  - Automotive Networks
  - Interactive Toys
  - Medical

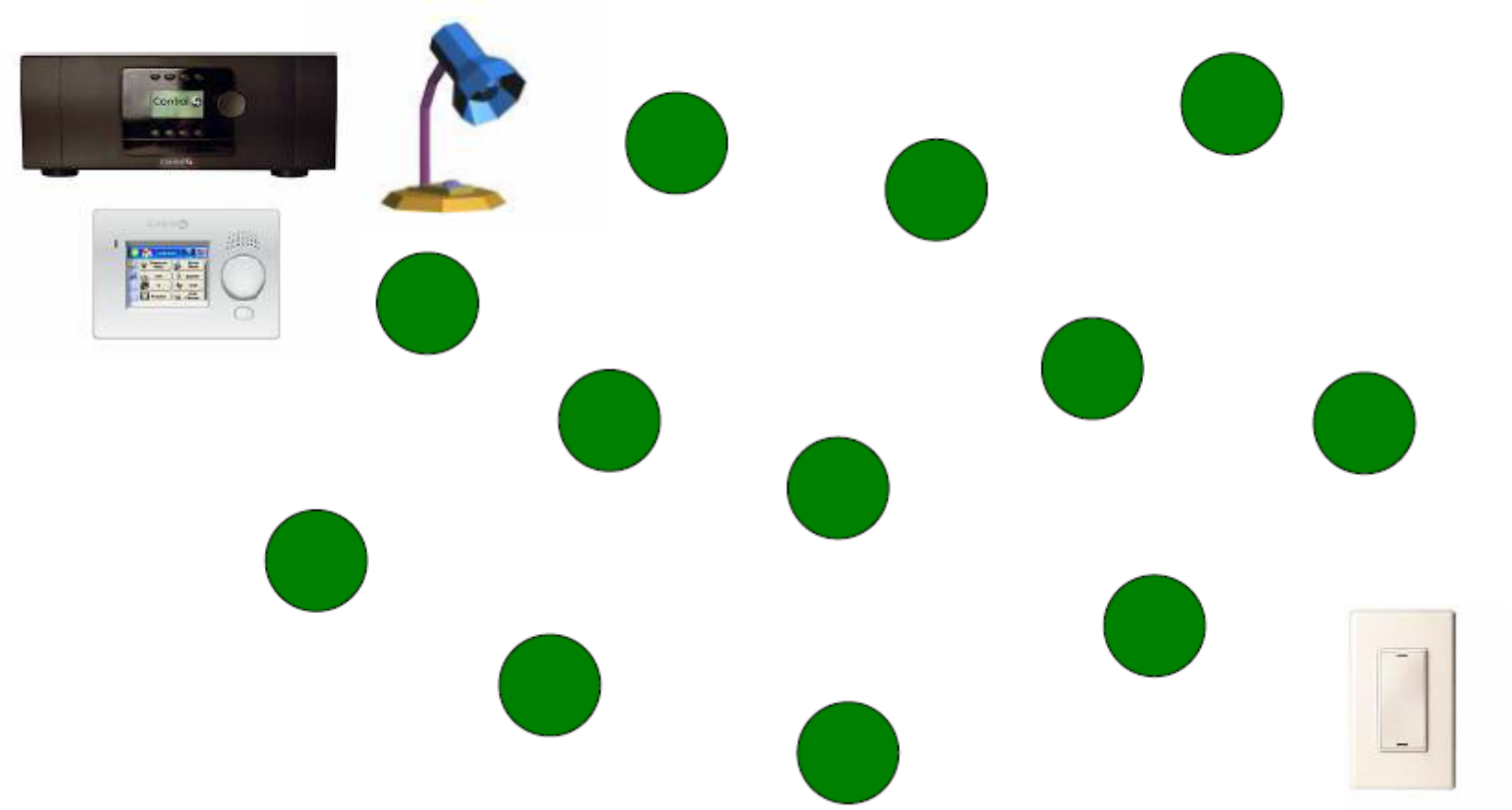


Basic Network Characteristics

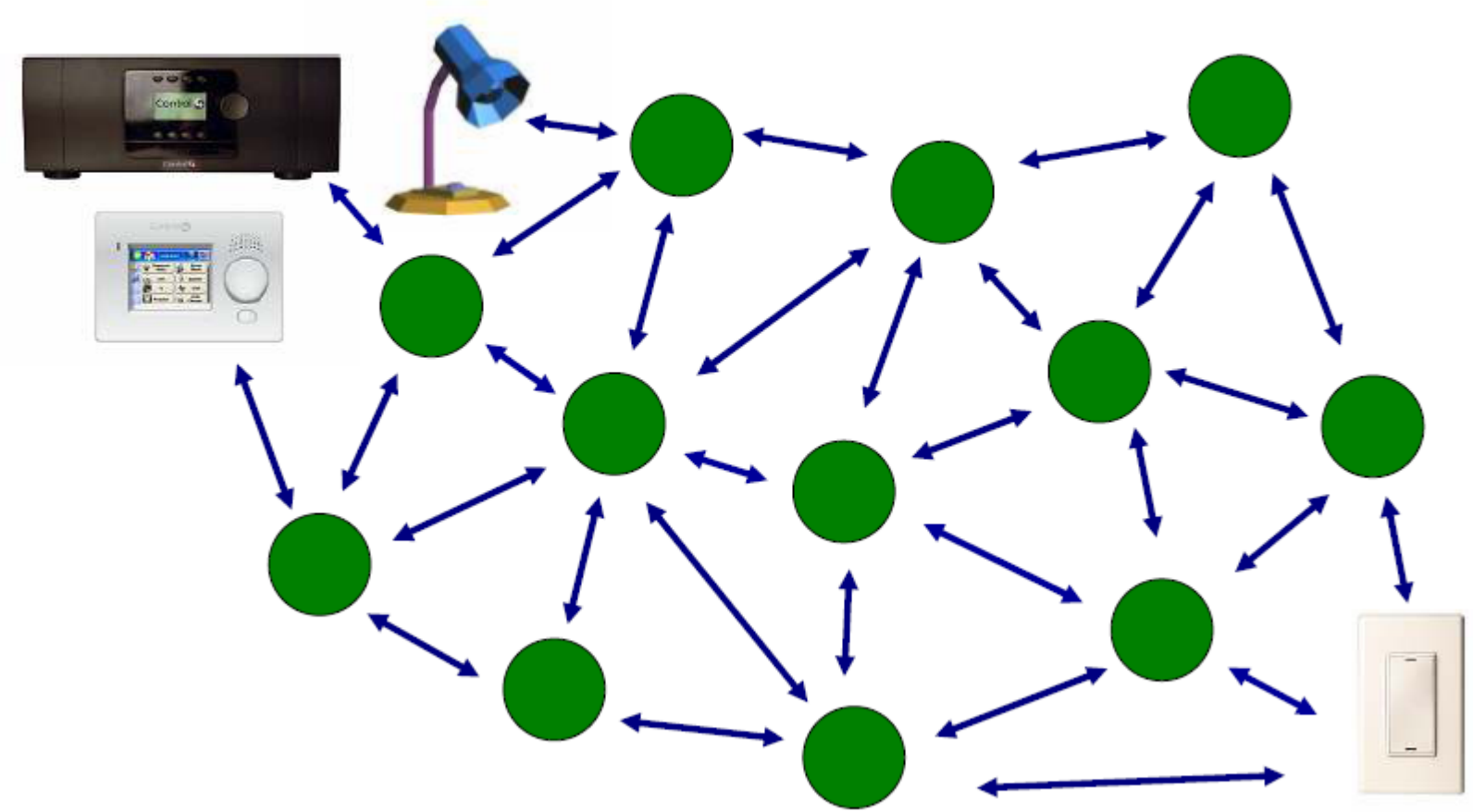
- 65,536 network (client) nodes
- Optimized for timing-critical applications and power management
  - Time to Join Network: <30ms
  - Sleeping to active: <15ms
  - Channel access time: <15ms
- Full Mesh Networking Support



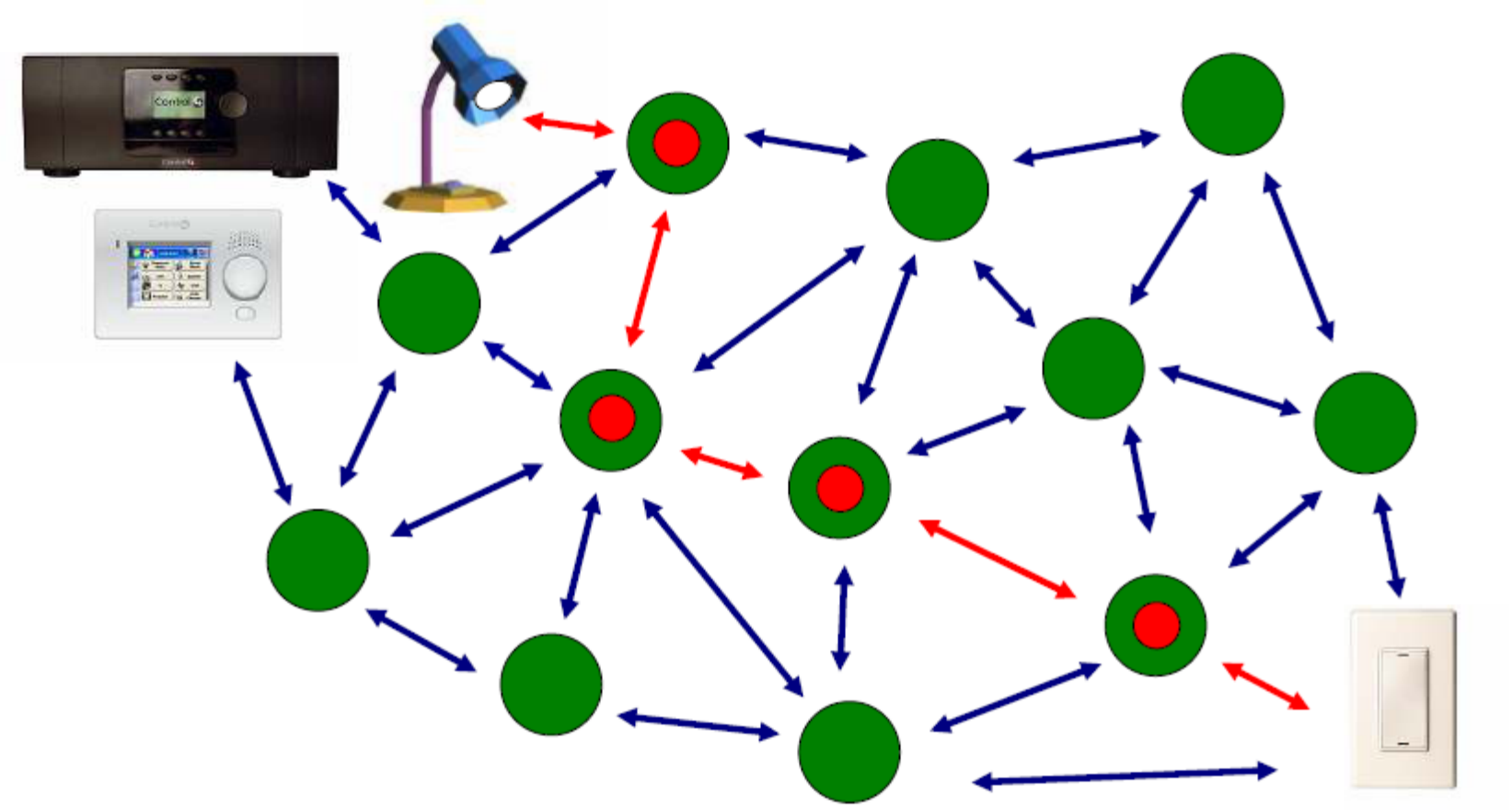
ZigBee Mesh Networking



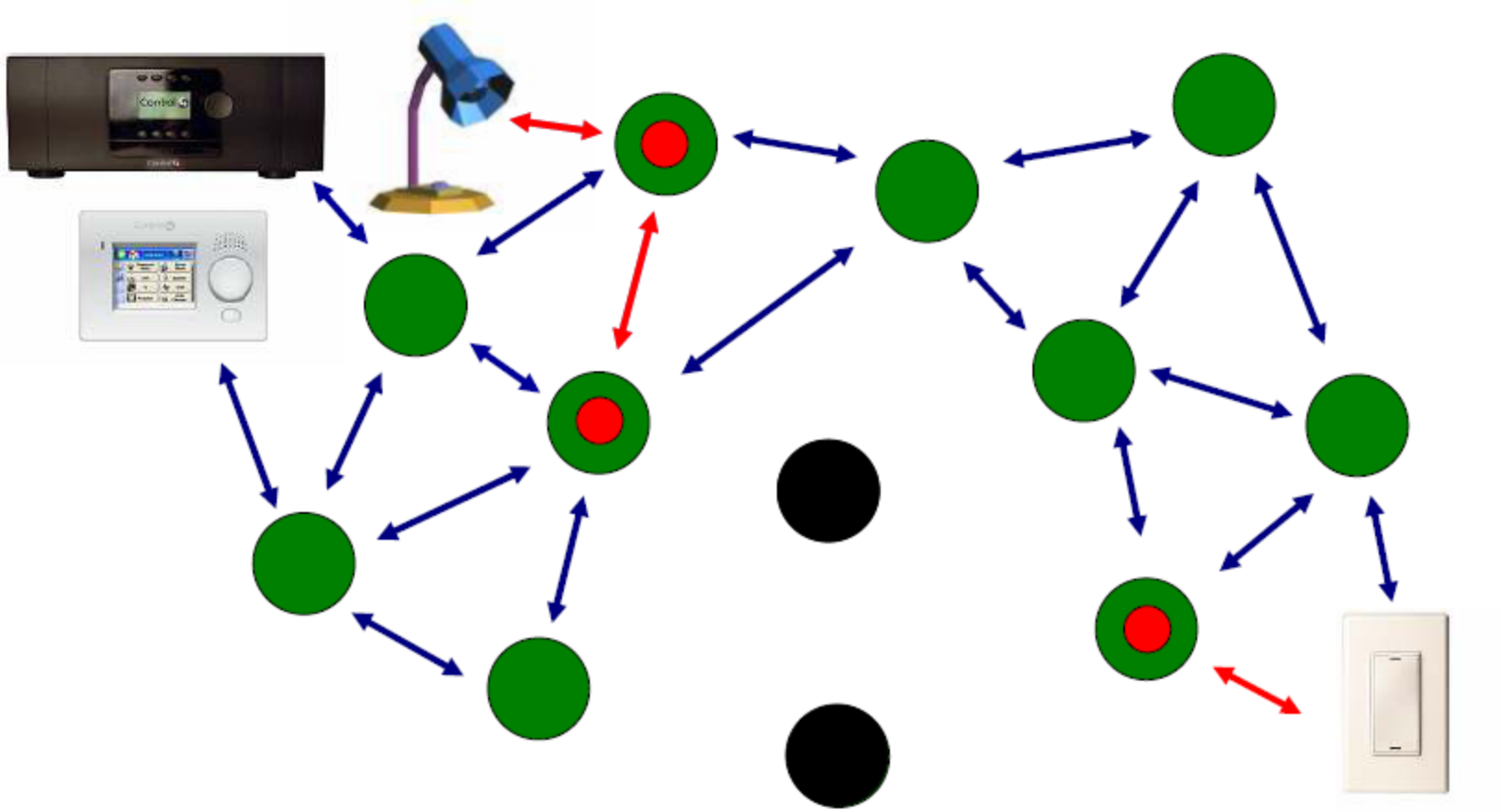
ZigBee Mesh Networking



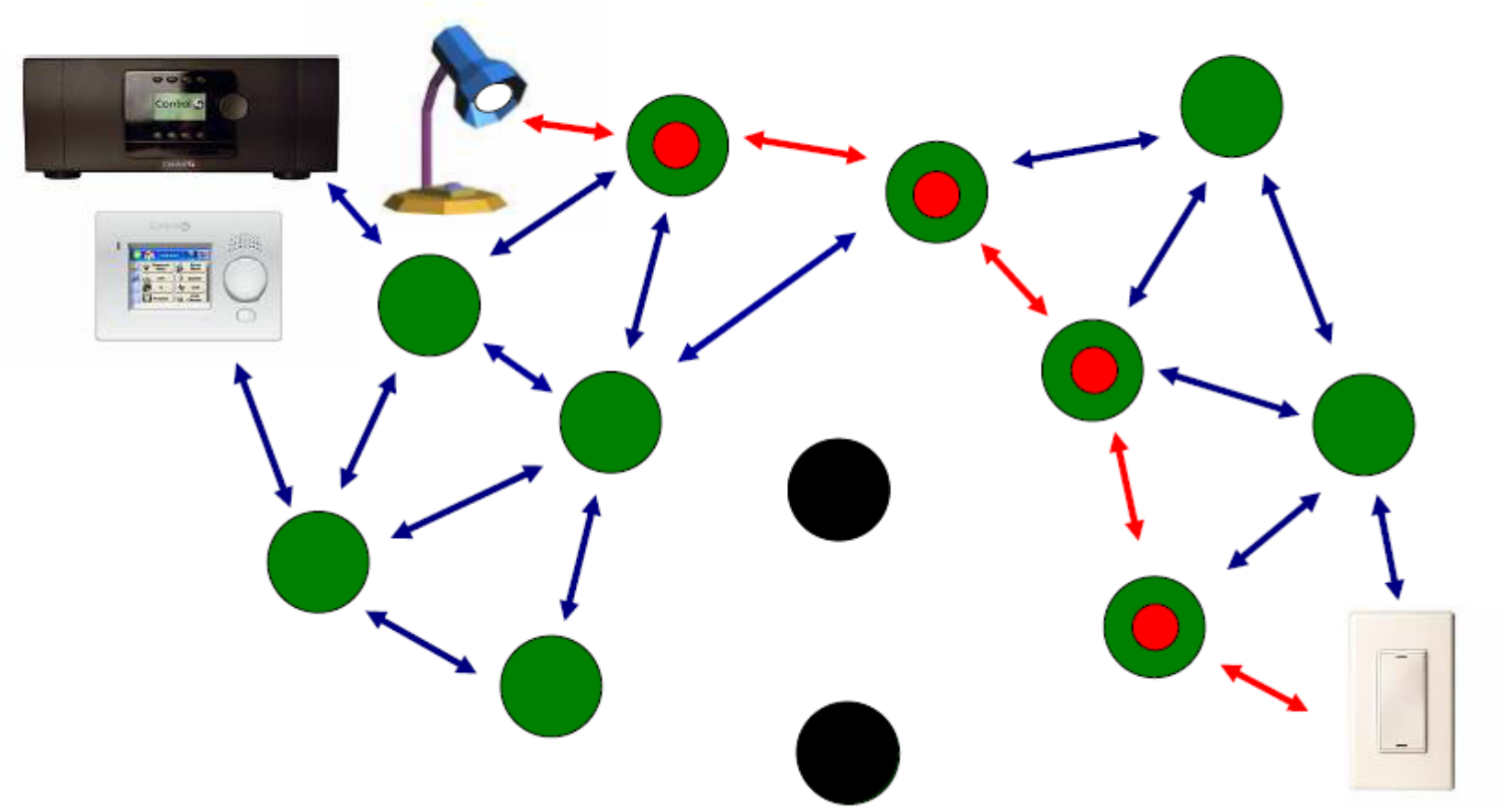
ZigBee Mesh Networking



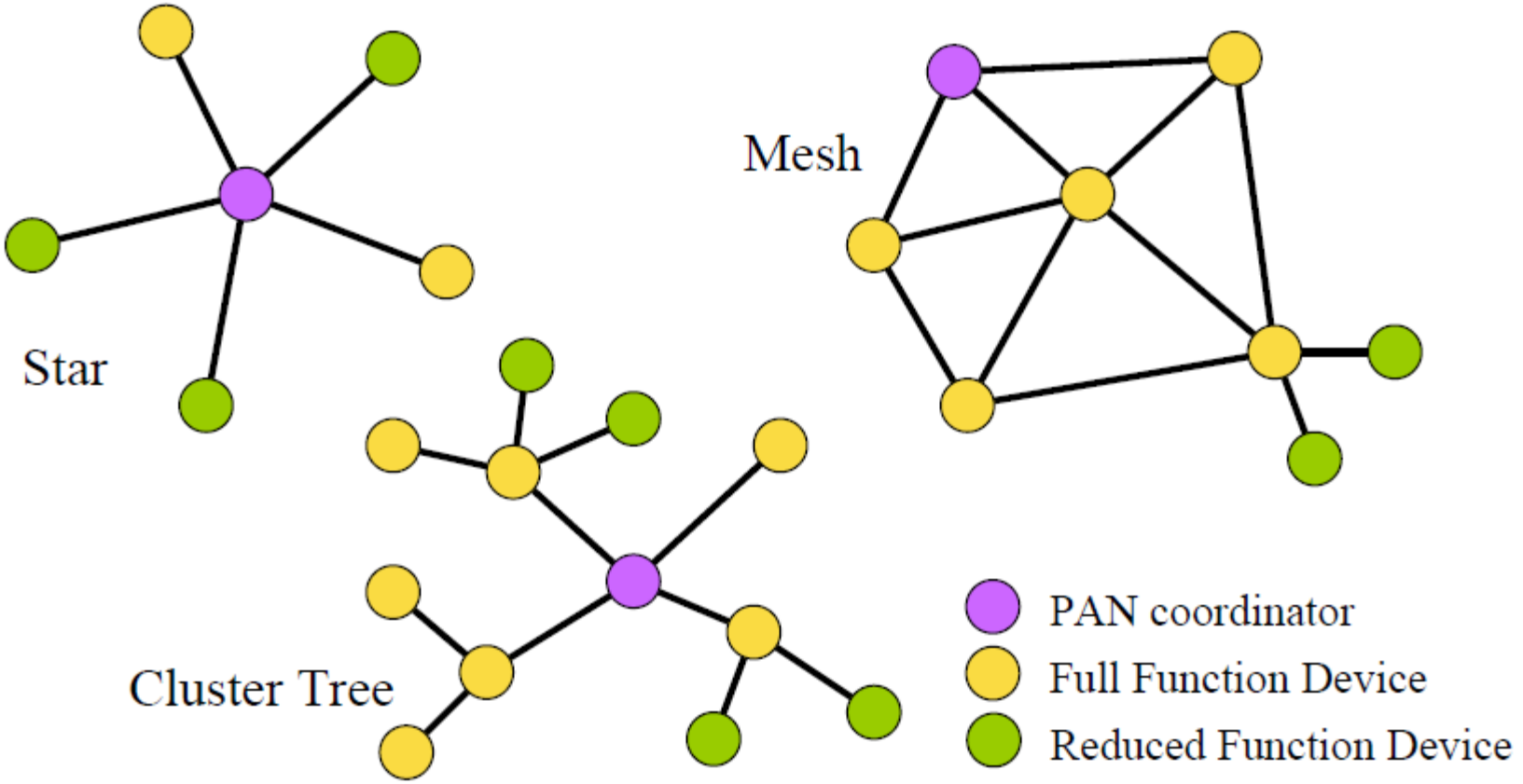
ZigBee Mesh Networking



ZigBee Mesh Networking



ZigBee Network Topologies



ZigBee Device Types

- ZigBee Coordinator (ZC)
  - One and only one required for each ZB network.
  - Initiates network formation.
  - Acts as 802.15.4 2003 PAN coordinator (FFD).
  - May act as router once network is formed.
- ZigBee Router (ZR)
  - Optional network component.
  - May associate with ZC or with previously associated ZR.
  - Acts as 802.15.4 2003 coordinator (FFD).
  - Participates in multihop routing of messages.
- ZigBee End Device (ZED)
  - Optional network component.
  - Shall not allow association.
  - Shall not participate in routing.

General Advantages of ZigBee

- Reliable and self healing
- Supports large number of nodes
- Easy to deploy
- Very long battery life
- Secure
- Low cost
- Can be used globally

The Inevitable Question is whether ZigBee and Bluetooth are competitors or complements?

Bluetooth seems best suited for:

- Synchronization of cell phone to PDA
- Hands-free audio
- PDA to printer

While ZigBee is better suited for:

- Controls
- Sensors
- Lots of devices
- Low duty cycle
- Small data packets
- Long battery life is critical

Timing Considerations

ZigBee

- New slave enumeration = 30ms typically
- Sleeping slave changing to active = 15ms typically
- Active slave channel access time = 15ms typically

Bluetooth

- New slave enumeration = >3s, typically 20s
- Sleeping slave changing to active = 3s typically
- Active slave channel access time = 2ms typically

Conclusion:

ZigBee devices can quickly attach, exchange information, detach, and then go to deep sleep to achieve a very long battery life. Bluetooth devices require about ~100X the energy for this operation.

Power Considerations

ZigBee

- 2+ years from 'normal' batteries
- Designed to optimize slave power requirements

Bluetooth

- Power model as a mobile phone (regular daily charging)
- Designed to maximize ad-hoc functionality

Bluetooth - Wibree

- The “Bluetooth consortium” (e.g. Nokia) has been working a low power consumption version of Bluetooth since 2001
- Wibree
  - Performance similar to ZigBee
  - Bluetooth without frequency hopping and with the possibility for nodes to be asleep most of the time
- Wibree has been adopted into Bluetooth specifications
  - It will use the same hardware as Bluetooth (shared antenna)

	Bluetooth	Wibree	ZigBee
Band	2.4GHz	2.4GHz	2.4GHz, 868MHz, 915MHz
Antenna/HW	Shared		Independent
Power	100 mW	~10 mW	30 mW
Target Battery Life	Days - months	1-2 years	6 months - 2 years
Range	10-30 m	10 m	10-75 m
Data Rate	1-3 Mbps	1 Mbps	25-250 Kbps
Component Cost	$3	Bluetooth + 20¢	$2
Network Topologies	Ad hoc, point to point, star	Ad hoc, point to point, star	Mesh, ad hoc, star
Security	128-bit encryption	128-bit encryption	128-bit encryption
Time to Wake and Transmit	3s	TBA	15ms