Internet of Things
Wireless Networks

Tullio Facchinetti
<tullio.facchinetti@unipv.it>

24 novembre 2023

http://robot.unipv.it/toolleeo

Basic features of WSN

WSN = **W**ireless **S**ensor **N**etwork

- Self organizing capabilities
- Short range broadcast applications
- Multihop routing
- Dense deployment
- Corporative effort
- Changing of topology
- Limitation in energy, memory and computing capabilities

Basic features of WSN

Fault-tolerant Authentication

- If base station fails, use backup controller in the immediate neighborhood.
- Hierarchy of base stations with multiple keys can be used.

Denial of Service Attacks and Intruder Identification

- Flooding by a malicious host, impersonation, gang attack, Byzantine behavior.
- Suspicion lists, black list can be created to ignore sensors.

Privacy and Anonymity

- Location of sensor.
- Source of data.
- False accusation.
- HIPPA regulations for medical data.
- Limited access and disclosure.

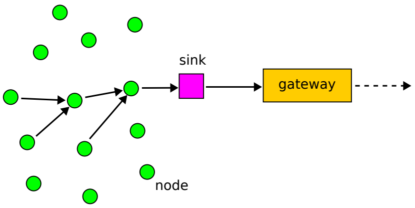
Energy Conservation

- Aggregation of data and pattern identification.
- Routers need to be computationally efficient for energy.

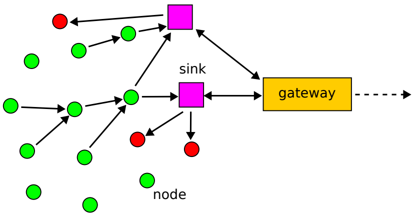
Node roles

- Sensors can be a data originator or a data router.
- Power conservation and power management are important.
- Power aware communication protocols must be developed.

Types of WSNs



The simplest case may consist of a network of sensors distributed in the environment, where the measurements are sent to a single node.



The situation may be complicated further by introducing additional nodes and actuators (bidirectional) data collection and distribution.

Characteristics of Wireless Sensor

- **Requirements**: small size, large number, tether-less, and low cost; constrained by energy, computation, and communication.
- Small size implies small battery.
- Low cost & energy implies low power CPU, radio with minimum bandwidth and range.
- Ad-hoc deployment implies no maintenance or battery replacement.
- To increase network lifetime, no raw data is transmitted.

Ad Hoc Wireless Networks

- Large number of self-organizing static or mobile nodes that are possibly randomly deployed
- Near(est)-neighbor communication
- Wireless connections
  - Links are fragile, possibly asymmetric
  - Connectivity depends on power levels and fading
  - Interference is high for omnidirectional antennas

Sensor Networks and **Sensor-Actuator Networks** are a prominent example

WSN vs ad hoc networks

Wireless Sensor Networks (WSNs) are ad hoc networks with wireless nodes that self-organize into an infrastructureless network

BUT, in contrast to other ad hoc networks:

- Sensing and data processing are essential.
- WSNs have many more nodes and are more densely deployed.
- Hardware must be cheap; nodes are more prone to failures.
- WSNs operate under very strict energy constraints.
- WSN nodes are typically static.
- The communication scheme is many-to-one (data collected at a base station) rather than peer-to-peer.

Data Collection

- Centralized data collection puts extra burden on nodes close to the base station; clever routing can alleviate that problem.
- **Clustering**: data from groups of nodes are combined before being transmitted, so that fewer transmissions are needed.
- Often getting measurements from a particular area is more important than getting data from each node.
- Security and authenticity should be guaranteed; however, the CPUs on the sensing nodes cannot handle fancy encryption schemes.

Data dissemination scheme

Direct communication with the base station

- Sensor nodes communicate with the base station directly.
- Energy consuming.

Multi-hop scheme

- Transmit through some other intermediate nodes.
- Energy consuming.

Architecture for a WSN

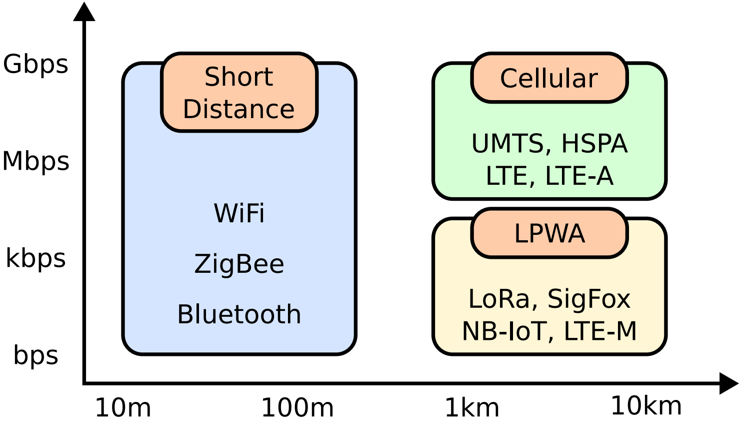
Special addressing requirement

- Local unique addresses.
- Data-centric.
- *Example*: each node is associated to an unique numeric ID.

Attribute-based naming architecture

- Data is named by one or more attributes.
- *Example*: each node is distinguished by an attribute - GPS sensors are practical for this.

Classification by range and bandwidth



LPWA = Low Power Wide Area

Classification

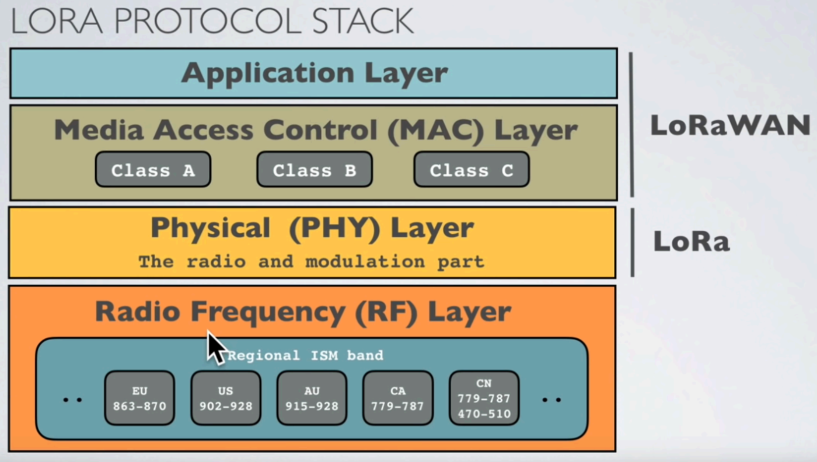
	LPWA (Low Power Wide Area)					
	Cellular IoT (3GPP Standard based)				Non-Cellular IoT	
	LTE-M			NB-IoT (Rel. 13)	LoRa	SigFox
	Cat 1 (Rel. 8)	Cat 0 (Rel. 12)	Cat M (Rel. 12)			
Coverage	Same as LTE coverage (Cat-M deeper penetration)			+20db LTE <20km	<14km	<17km
Spectrum	LTE In-Band Only			LTE In-BAnd Guard Band Standalone	Unlicensed band	
Signal BW	20MHz	1.4MHz	1.08MHz	180KHz	125KHz	0.1KHz
Data Rate	10 Mbps	1 Mbps	1 Mbps	200 Kbps	10 Kbps	100 bps
Battery Life	10 years			10 years	10 years	

Non-standard based: LoRa

LoRa and LoRaWAN

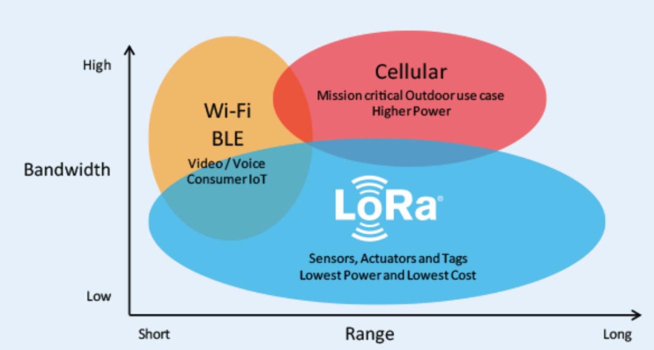
- **LoRa** contains only the link layer protocol.
- Initially developed by Cycleo 2010 (acquired by SEMTEC in 2012) provided interface to IP networks.
- **LoRaWAN** includes the network layer too so it is possible to send the information to any Base Station already connected to a Cloud platform. LoRaWAN modules may work in different frequencies by just connecting the right antenna to its socket. Developed by SEMTEC in 2013.
- Since 2015 **LoRa Alliance** is acting as reference forum to provide open standards for introperability of IoT devices.
- LoRa positioning in the IoT market.

LoRa stack



From https://lora.readthedocs.io/en/latest/

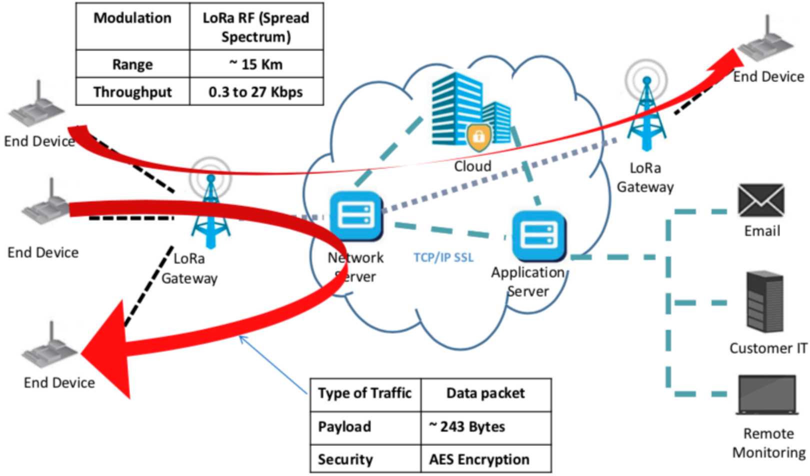
LoRa and LoRaWAN



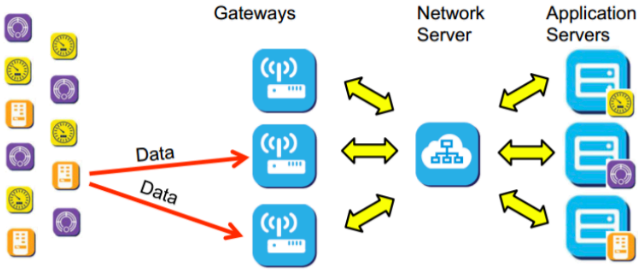
LoRa technology

- LoRaWAN is a Long Range Wide Area Network
- LoRa modulation: a version of Chirp Spread Spectrum (CSS) with a typical channel bandwidth of 125KHz
- High sensitivity (end Nodes: up to -137 dBm, gateways: up to -142 dBm)
- Long range communication (up to 15 Km)
- Strong indoor penetration: with High Spreading Factor, up to 20dB penetration (deep indoor)
- Occupies the entire bandwidth of the channel to broadcast a signal, making it robust to channel noise.
- Resistant to Doppler effect, multi-path and signal weakening.

LoRaWAN architecture

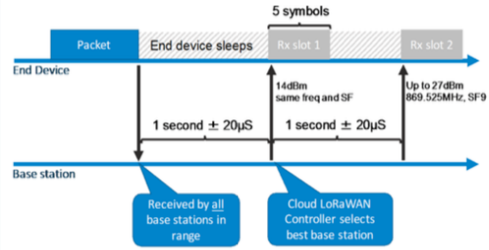


LoRaWAN communication



- A LoRa node transmits in broadcast mode to all gateways in reach.
- All gateways forward to network server.
- Network server selects best packet and forwards to application server.
- ACK is transmitted only via the best gateway.

LoRa duty cycle



- An end node can broadcast a packet at any time.
- After the transmission, the node can sleep to save energy.
- The end node opens two receive slots after given time from the transmission.
- The gateway can respond within the first or the second receive slot, but not both.

based on

ETSI
European Telecommunications Standards Institute

Evolution in 3GPP support for M2M

1. **NB-IoT** (Narrow Band IoT)): New radio added to the LTE platform optimized for the low end of the market.
2. **EC-GSM-IoT** (Extended Coverage – GSM – Internet of Things): EGPRS enhancements in combination with PSM to make GSM/EDGE markets prepared for IoT.
3. **eMTC**: LTE enhancements for MTC, based on Release-12 (UE Cat 0, new PSM).

Legend

Acronym	Extended	Comment
M2M	Machine To Machine (communication)	
MTC	Machine Type Communications	Same as M2M
PSM	Power Saving Mode	
3GPP	3rd Generation Partnership Project	Umbrella term for a number of standards organizations
EGPR	Enhanced General Packet Radio Services	
GSM	Global System for Mobile Communications	
LTE	Long-Term Evolution	Standard for wireless broadband communication for mobile devices and data terminals

Comparison of main features

V • T • E [8][9]	LTE Cat 1	LTE Cat 1 bis	LTE-M				NB-IoT		EC-GSM-IoT
			LC-LTE/MTCe	eMTC					
			LTE Cat 0	LTE Cat M1	LTE Cat M2	non-BL	LTE Cat NB1	LTE Cat NB2	
3GPP Release	Release 8	Release 13	Release 12	Release 13	Release 14	Release 14	Release 13	Release 14	Release 13
Downlink Peak Rate	10 Mbit/s	10 Mbit/s	1 Mbit/s	1 Mbit/s	~4 Mbit/s	~4 Mbit/s	26 kbit/s	127 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Uplink Peak Rate	5 Mbit/s	5 Mbit/s	1 Mbit/s	1 Mbit/s	~7 Mbit/s	~7 Mbit/s	66 kbit/s (multi-tone) 16.9 kbit/s (single-tone)	159 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Latency	50–100 ms		not deployed	10–15 ms			1.6–10 s		700 ms – 2 s
Number of Antennas	2	1	1	1	1	1	1	1	1–2
Duplex Mode	Full Duplex		Full or Half Duplex	Full or Half Duplex	Full or Half Duplex	Full or Half Duplex	Half Duplex	Half Duplex	Half Duplex
Device Receive Bandwidth	1.4–20 MHz		1.4–20 MHz	1.4 MHz	5 MHz	5 MHz	180 kHz	180 kHz	200 kHz
Receiver Chains	2 (MIMO)		1 (SISO)	1 (SISO)	1 (SISO)	1 (SISO)	1 (SISO)	1 (SISO)	1–2
Device Transmit Power	23 dBm	23 dBm	23 dBm	20 / 23 dBm	20 / 23 dBm	20 / 23 dBm	20 / 23 dBm	14 / 20 / 23 dBm	23 / 33 dBm

From `https://en.wikipedia.org/wiki/LTE-M`

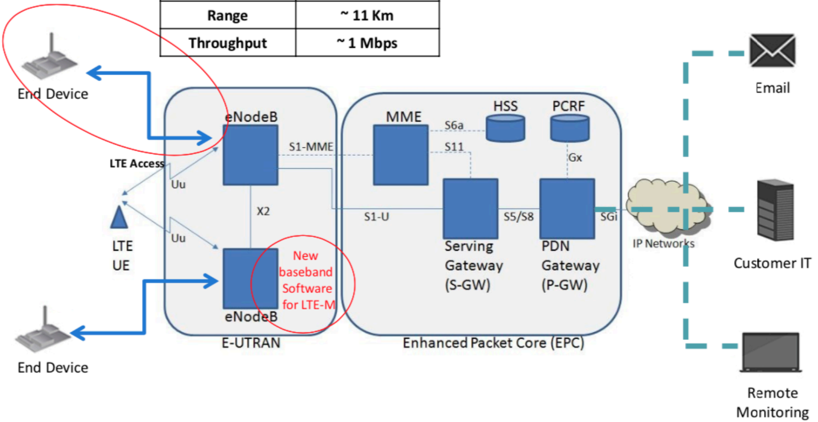
LTE-M

Long-Term Evolution Machine Type Communication
Also know LTE-MTC

- Lower power consumption than LTE
- Easy deployment
- Interoperability with LTE
- Coverage up to 11Km
- Max throughput 1 Mbps

LTE-M architecture

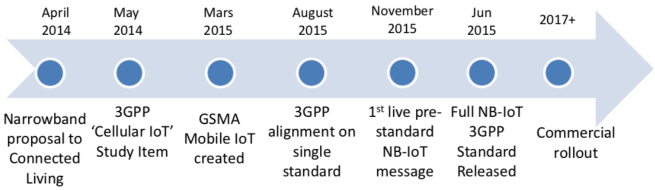
Frequency Band	Narrow Band
Access	LTE-M
Range	~ 11 Km
Throughput	~ 1 Mbps



Note: do not focus on acronyms here but only on the organization of the architecture

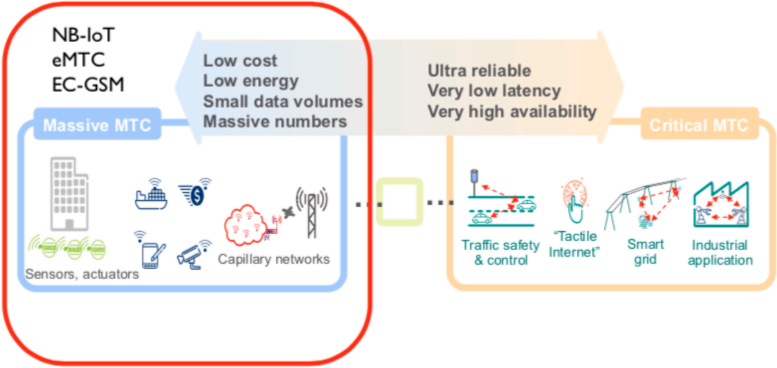
NB-IoT

- Reuses the LTE design extensively: numerologies, DL OFDMA, UL SC-FDMA, channel coding, rate matching, interleaving, etc.
- Reduced time to develop.
- Full specifications.
- NB-IoT products for existing LTE equipment and software vendors.
- June 2016: core specifications completed.
- Beginning of 2017: commercial launch of products and services.

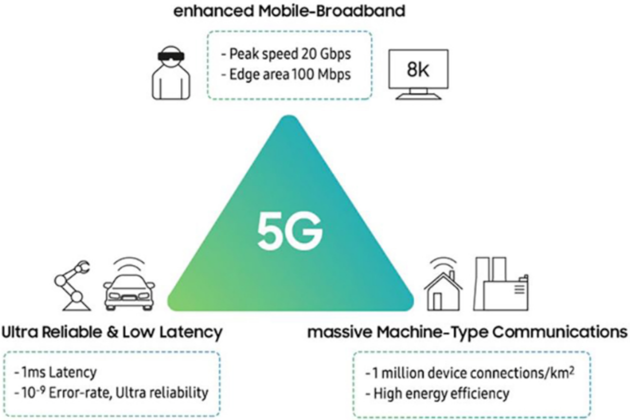


NB-IoT use cases

Suitable for the “lower part” of **5G application triangle**



5G triangle


enhanced Mobile-Broadband
- Peak speed 20 Gbps
- Edge area 100 Mbps
8k
5G
Ultra Reliable & Low Latency
- 1ms Latency
- 10-9 Error-rate, Ultra reliability
massive Machine-Type Communications
- 1 million device connections/km2
- High energy efficiency

NB-IoT design targets

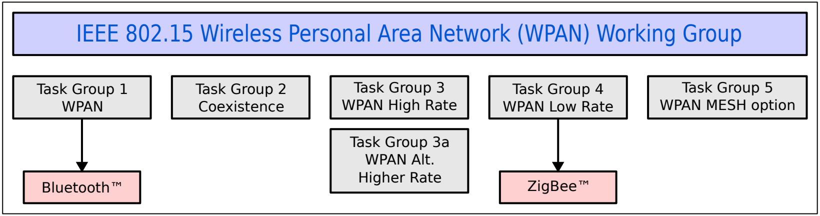
NB-IoT targets the low-end "Massive MTC" scenario

- Low device cost/complexity: $< \$5$ per module.
- Extended coverage: 164 dB MCL, 20 dB better compared to GPRS.
- Long battery life: > 10 years.
- Capacity: 40 devices per household, $\sim 55k$ devices per cell.
- Uplink report latency: < 10 seconds.

An off-the-shelf NB-IoT module

IEEE based

Structure of the IEEE Working Group



- **IEEE 802.15** focuses on the development of consensus standards for Personal Area Networks or short distance wireless networks.
- These WPANs address wireless networking of portable and mobile computing devices such as PCs, PDAs, peripherals, cell phones and consumer electronics.
- The goal is to publish standards, recommended practices, or guides that have broad market applicability and deal effectively with the issues of coexistence and interoperability with other wired and wireless networking solutions.

General network architecture

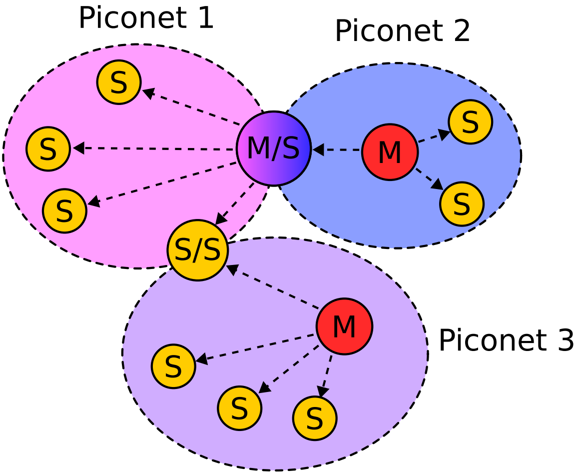
Piconet

- Each piconet has one master and up to N simultaneous slaves.
- **Master**: device that initiates a data exchange.
- **Slave**: device that responds to the master.

Scatternet

- Linking of multiple piconets through the master **or** slave devices.
- Bluetooth devices have point-to-multipoint capability to engage in scatternet communication.

Scatternet



Devices can be slave in one piconet and master of another.

Bluetooth

802.15.1

Physical links

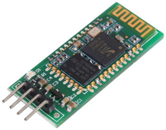
Between master and slave(s), different types of links can be established

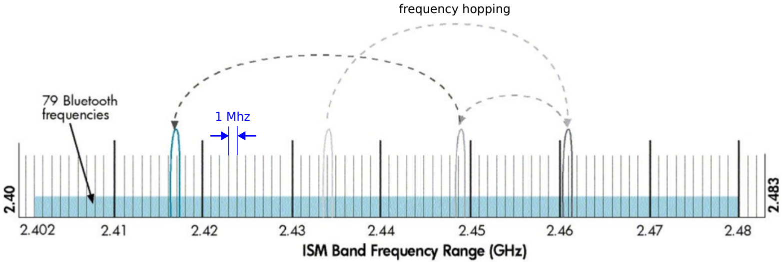
Two link types have been defined:

1. **Synchronous Connection Oriented (SCO)**
    - Support symmetrical, circuit-switched, point-to-point connections.
    - Typically used for voice traffic.
    - Periodic slot reservation.
    - Data rate is 64 kbit/s.
2. **Asynchronous Connection-Less (ACL)**
    - Support symmetrical and asymmetrical, packet-switched, point-to-multipoint connections.
    - Typically used for data transmission.
    - Up to 433.9 kbit/s in symmetric or 723.2/57.6 kbit/s in asymmetric.

Bluetooth Radio

- The lowest defined layer of the Bluetooth specification.
- Operating in the 2,4 GHz ISM Band.
- Accomplishes spectrum spreading by frequency hopping (FHSS) from 2.402 GHz to 2.480 GHz.
- Symbol rate = 1 Ms/s.
- Slotted channel with slot time = 625 ms.
- Time-division duplex (TDD) for full-duplex.





States

Standby
Waiting to join a piconet

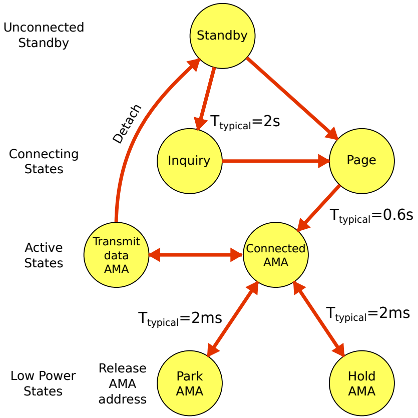
Inquire
Ask about radios to connect to

Page
Connect to a specific radio

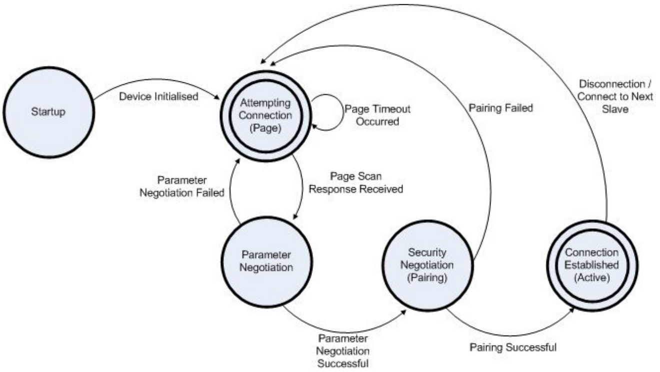
Connected
Actively on a piconet (master or slave)

Park/Hold
Low Power connected states

AMA = Active Member Address
PMA = Parked Member Address

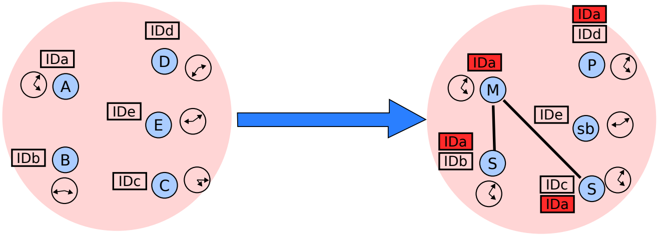


Piconet Master State Diagram



From M. J. Fraser, "Innovative techniques for extending the range and node limits in Bluetooth based wireless sensor networks", Master Degree Thesis, 2006.

The piconet



All devices in a piconet hop together

To form a piconet:

- Master gives slaves its clock and device ID
- Hopping pattern determined by device ID (48-bit)
- Phase in hopping pattern determined by Clock
- Non-piconet devices are in standby

Piconet Addressing:

- Active Member Address (AMA, 3-bits)
- Parked Member Address (PMA, 8-bits)

Bluetooth 4.0: Low Energy (BLE)

Energy usage in traditional Bluetooth

- Traditional Bluetooth is connection oriented: when a device is connected, a link is maintained, even if there is no data flowing.
- Sniff modes allow devices to sleep, reducing power consumption to give months of battery life.
- Peak transmit current is typically around 25mA.
- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough power for coin cells and energy harvesting applications.

Bluetooth Low Energy

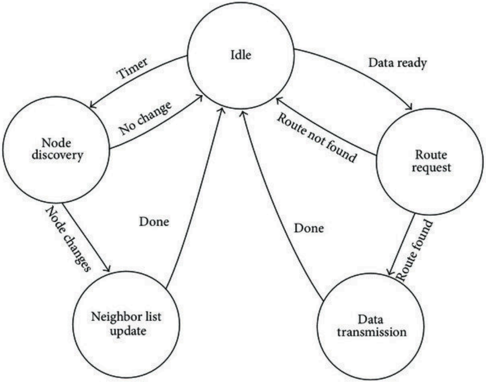
Everything is optimized for lowest power consumption

- Short packets reduce TX peak current.
- Short packets reduce RX time.
- Less RF channels to improve discovery and connection time.
- Simple state machine.
- Single protocol.

Enable coin cell battery use cases

- $<$ 20 mA peak current
- $<$ 5 uA average current

BLE Node State Diagram



From C. Jung et al., “Maximum Power Plus RSSI Based Routing Protocol for Bluetooth Low Energy Ad Hoc Networks”, Hindawi, 2017.

BLE factsheet

Range	∼150 meters open field
Output Power	∼10 mW (10dBm)
Max Current	∼15 mA
Latency	3 ms
Topology	Star
Connections	$>$ 2 billion
Modulation	GFSK @ 2.4 GHz
Robustness	Adaptive Frequency Hopping, 24 bit CRC
Security	128bit AES CCM
Sleep current	∼1µA
Modes	Broadcast, Connection, Event Data Models, Reads, Writes
Data Throughput	Not meaningful for BLE. Streaming is not supported. Data rate of 1Mbps is not optimized for file transfer. It is designed for sending small chunks of data (exposing state).

Estimation of the lifetime of a BLE node (1/3)

Calculation of the energy per transaction

Assumptions

- Upper bound per minimal transaction = 3ms.
- TX power = 15mW (mostly TX power amp for 65nm chips).

$$E = 0.015 \text{ W} \cdot 0.003 \text{ sec} = 45 \ \mu J$$

$$I = 0.015 \text{ W} \cdot 1.5 \text{ V} = 10 \text{ mA}$$

Estimation of the lifetime of a BLE node (2/3)

How long could a sensor last on a battery?

Example battery: Lenmar WC357

- 1.55V
- 180mAh
- $2 – 5

$$T = \frac{180 \text{ mAh}}{10 \text{ mA}} = 18 \text{ Hr} = 64,800 \text{ sec} = 21.6\text{M transactions}$$

Estimation of the lifetime of a BLE node (3/3)

Frequency of messages = 1 msg/min = 1440 msg/day

$$\text{lifetime} = \frac{21.6 \text{ M msg}}{1,440 \text{ msg/days}} = 15,000 \text{ days} > 40 \text{ years}$$

- This far exceeds the life of the battery and/or the product.
- This means that the battery costs more than the electronics.
- This sensor could run on scavenged power, e.g. ambient light.

Frequency of messages = 1 msg/sec = 86,400 msg/day

$$\text{lifetime} = \frac{21.6 \text{ M msg}}{86,400 \text{ msg/days}} = 250 \text{ days} \approx 1 \text{ year}$$

ZigBee

802.15.4

IEEE 802.15.4 - Introduction

- IEEE 802.15.4 is a very commonly used IoT standard for MAC.
- It defines a frame format, headers including source and destination addresses, and how nodes can communicate with each other.
- The frame formats used in traditional networks are not suitable for low power multi-hop networking in IoT due to their overhead.
- In 2008, IEEE802.15.4e was created to extend IEEE 802.15.4 and support low power communication.
- It uses time synchronization and channel hopping to enable high reliability, low cost and meet IoT communications requirements.

IEEE 802.15.4 - Slotframe Structure

IEEE 802.15.4e frame structure is designed for scheduling and telling each node what to do.

A node can sleep, send, or receive information:

- In the **sleep mode**, the node turns off its radio to save power and stores all messages that it needs to send at the next transmission opportunity.
- When **transmitting**, it sends its data and waits for an acknowledgment.
- When **receiving**, the node turns on its radio before the scheduled receiving time, receives the data, sends an acknowledgement, turn off its radio, delivers the data to the upper layers and goes back to sleep.

IEEE 802.15.4 - Scheduling

- The standard does not define how the scheduling is done but it needs to be built carefully such that it handles mobility scenarios.
- It can be centralized by a manager node that is responsible for building the schedule, informing others about the schedule and other nodes will just follow the schedule.

Significant research has been carried out to formulate effective scheduling policies for ZigBee.

IEEE 802.15.4 - Synchronization

Synchronization is necessary to maintain nodes' connectivity to their neighbors and to the gateways.
Two approaches can be used: **acknowledgment-based** or **frame-based** synchronization.

- In acknowledgement-based mode, the nodes are already in communication and they send acknowledgment for reliability guarantees, thus can be used to maintain connectivity as well.
- In frame-based mode, nodes are not communicating and hence, they send an empty frame at pre-specified intervals (about 30 second typically).

IEEE 802.15.4 - Channel Hopping

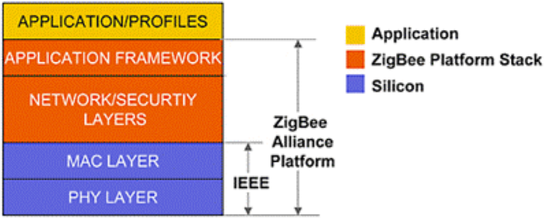
- IEEE802.15.4e introduces channel hopping for time slotted access to the wireless medium.
- Channel hopping requires changing the frequency channel using a pre-determined random sequence.
- This introduces frequency diversity and reduces the effect of interference and multi-path fading.
- Sixteen channels are available, which adds to network capacity as two frames over the same link can be transmitted on different frequency channels at the same time.

IEEE 802.15.4 - Network formation

- Network formation includes advertisement and joining components.
- A new device should listen for advertisement commands and upon receiving at least one such command, it can send a join request to the advertising device.
- In a centralized system, the join request is routed to the manger node and processed there while in distributed systems, they are processed locally.
- Once a device joins the network and it is fully functional, the formation is disabled and will be activated again if it receives another join request.

ZigBee

Suite of communication protocols for high-level compact devices, low-power, low bit rate (20 kbps - 250 kbps), based on IEEE 802.15.4.



ZigBee

- It aims to be a simpler and more cost effective than Bluetooth, while ensuring secure communications.
- It operates in the ISM radio bands (Industrial, Scientific, and Medical).

Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26

General characteristics (theoretical)

- Up to 65,536 network nodes.
- Optimized for time-critical applications and power management.
- Time to join the network: < 30ms.
- Sleeping to active: < 15ms.
- Channel access time: < 15ms.
- Full mesh networking support.

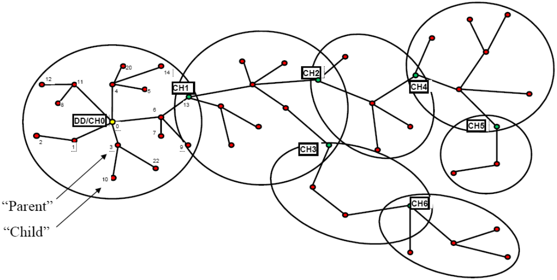
General characteristics (theoretical)

Multi-hop routing

- Ad-hoc On-Demand Distance Vector, neuRFon...

Automatic generation of network

- Mesh or single cluster
- Cluster of clusters (minimizes the overhead to manage the routing of data)



ZigBee devices

1. **ZigBee coordinator** (ZC)
   - The most advanced device, base of the network and acting as bridge to other networks.
   - Exactly one ZigBee coordinator in each network, since it is the one from which the net is controlled.
   - It can store information about the network and can act as a trust centre & repository for keys.
2. **ZigBee Router** (ZR)
   - Not only can act as an application node, but can also may serve as a router, forwarding packets by other nodes.
3. **ZigBee End Device** (ZED)
   - Only basic functionality to communicate with coordinators or routers, but is not able to forward data from other devices.
   - This relationship allows the node to rest for a great deal of time, allowing it to optimize its battery life.
   - Requires less memory and implements less functionality $\Rightarrow$ less expensive to produce and develop than a ZR or ZC.

ZigBee vs BLE (1/3)

Business comparison

- ZigBee is older, it has gone through several iterations.
- ZigBee has market mindshare, but not a lot of shipments yet.
- Market barriers: connectivity - ZigBee is not in PCs or mobile phones yet.

ZigBee vs BLE (2/3)

Technical comparison

- Zigbee is low power; BLE is even lower.
- Detailed analysis depends on specific applications and design detail, not to mention chip geometry.
- ZigBee stack is lightweight; the BLE/GATT stack is even simpler.

ZigBee vs BLE (3/3)

Going forward:

- ZigBee has a lead on developing applications and presence.
- Bluetooth low energy has improved technology, and a pervasive presence in several existing markets: mobile phones, automobiles, consumer electronics, PC industry.
- Replacing “classic Bluetooth” with “dual mode” devices will bootstrap this market quickly.

Protocols and IoT verticals

Key IoT vertical	LPWAN	Cellular	Mesh	BLE	WiFi
Industrial IoT	●	○	○		
Smart Metering	●				
Smart City	●				
Smart Building	●		○	○	
Smart Home			●	●	●
Wearables	○			●	
Connected Car		●			○
Connected Health		●		●	
Smart Retail		○		●	●
Asset Tracking	●	●			
Smart Agriculture	●				

● Highly applicable ○ Moderately applicable

Comparison: applications

	Voice	Data	Audio	Video	State
Bluetooth ACL/HS	✗	✓	✓	✗	✗
Bluetooth SCO/eSCO	✓	✗	✗	✗	✗
Bluetooth low energy	✗	✗	✗	✗	✓
Wi-Fi	(VoIP)	✓	✓	✓	✗
Wi-Fi Direct	✓	✓	✓	✗	✗
ZigBee	✗	✗	✗	✗	✓
ANT	✗	✗	✗	✗	✓

State = low bandwidth, low latency data → Low Power!!