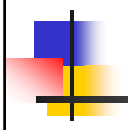


WSN Protocols

Piero Zappi
pzappi@deis.unibo.it

Outline

- Wireless Sensor Networks overview
  - Motivations
  - Application
  - Design objectives
- WSN Protocols
  - Impact on WSN
  - OSI layers
  - Security
- Examples
  - IEEE 802.15.4/ZigBee
  - T-MAC S-MAC
  - Bluetooth & ZigBee

WSN Motivations

New solution to collect information from environment

Flexible	▪ The environment may change ▪ Nodes may fall ▪ The information required may grown
Efficient	▪ Real time ▪ Reliable ▪ Deeply integrated with the environment
Cheap	▪ Wide market

WSN Protocols

WSN protocol strongly impact on system performance

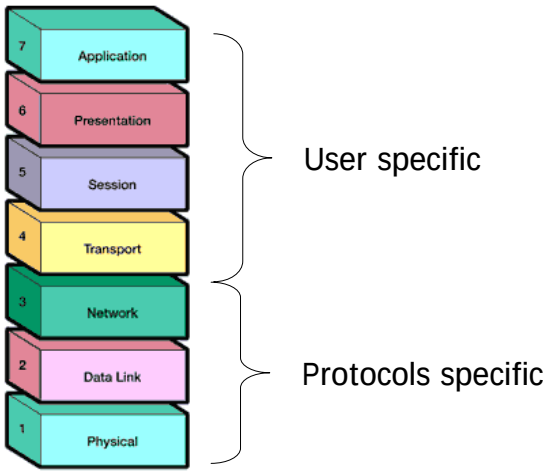
Choosing the wrong protocol may cause severe inefficiency and prevent the WSN to accomplish user need.

The protocol affect:
- Energy dissipation
- System cost
- Latency
- Security

Protocol layers

WSN protocols define lower level
- Physical
- Data Link (MAC)
- Network

User application, usually, are built over Network layer



Protocols PHY layer

A communication protocol physical layer

... provides mechanical, electrical, functional, and procedural characteristics to establish, maintain, and release physical connections (e.g., data circuits) between data link entities

Two main metrics are used to evaluate the physical layer

Cost

Power

Protocols PHY layer - Cost

Largely due to hardware

- Transceiver and antennas
  - Channel filtering
- Cristals

Digital approach
- dimension and cost fall as technology advance

Analog approach
- dimension and cost almost constant as technology advance

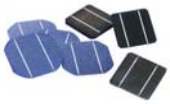
...but also due to market
- Use of world-wide available free ISM band

Protocols PHY layer – Power

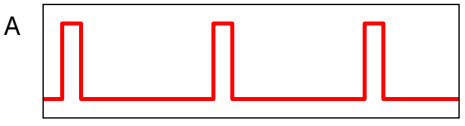
Power source point of view

Wireless Sensor Node has low power consumption

Unconventional power sources may be used
- Solar
- Vibration
- Human movement



Charge recovery effect for battery



low duty cycle

Protocols PHY layer – Power

Power consumption point of view

$$I_{avg} = I_{on} \cdot T_{on} + I_{stby} \cdot (1 - T_{on})$$

$$I_{stby} << I_{on}$$

- Keep the transceiver in low power states as long as possible
  - Minimize T_{on}
  - High data Rate
- Low symbol rate
  - Minimize I_{on}
  - Send more than one bit per symbol

Protocols PHY layer Modulation

DSSS – Direct Sequence Spread Specrum

- Fixed Carrier Frequency
- Signal spread over a wide band using PN sequences
- Redundancy factor

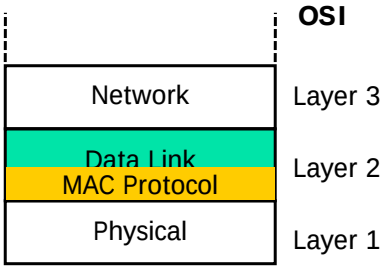
ZigBee™ Alliance

FHSS – Frequency Hop Spread Specrum

- Pseudo casual jumps between several carrier frequency
- Narrow signal band
- Harder synchronization

Bluetooth

Protocols Data link layer (MAC)



Data link layer:
- Mapping network packets
  - radio frames
- Transmission and reception of frames over the air
- Error control
- Security

Protocols MAC layer

Control access to the shared medium (radio channel)
- Avoid interference between transmissions
- Mitigate effects of collisions (retransmit)

Approaches
- Contention-based: no coordination
- Schedule-based: central authority (access point)

Less used approaches:
- Frequency division
- Code division

Protocols MAC layer

Contention based protocols

...listen before send

Objective: Multiple Access with Collision Avoidance (MACA)

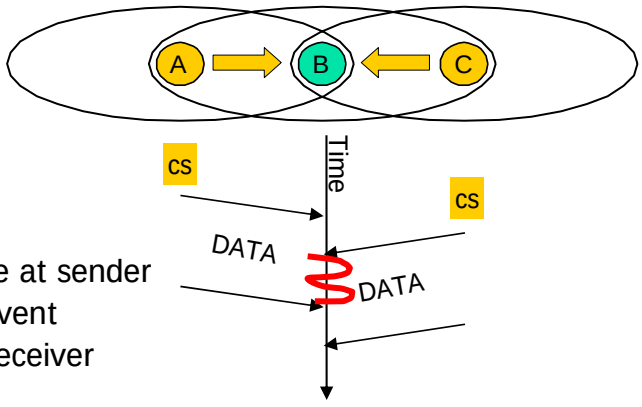
Node sense the medium for special packets or energy in order to understand when there are no communication.

Carrier Sense Multiple Access (CSMA)

- How long device sense the channel?
- How long device remain in idle listening State?

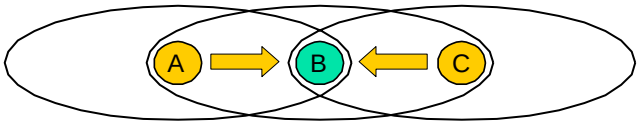
Hidden terminal problem

A and B are out of range



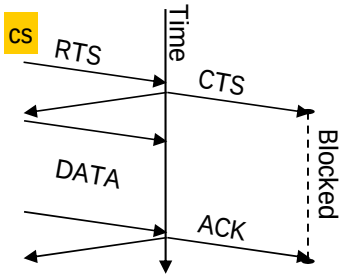
Carrier sense at sender may not prevent collision at receiver

Hidden terminal problem

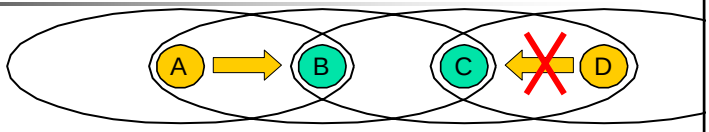


MACA:

- Request To Send
- Clear To Send
- DATA
- Acknowledge

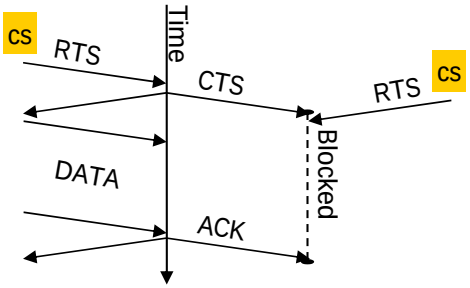


Exposed terminal problem



Parallel CSMA transfers are synchronized by CSMA/CA

Collision avoidance can be too restrictive!



Protocols MAC layer

Schedule based protocols

Communication is scheduled in advance

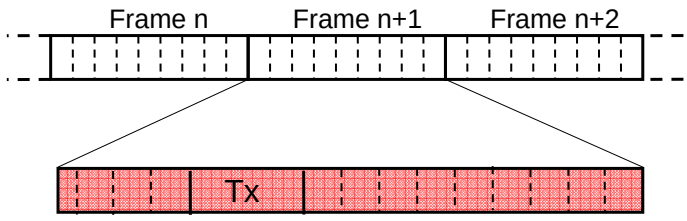
- No contention
- No overhearing

Time-Division Multiple Access

- Time is divided into slotted frames
- Access point broadcasts schedule
- Coordination between cells required
- Need of global clock

} Hard with WSN constraints

Protocols MAC layer



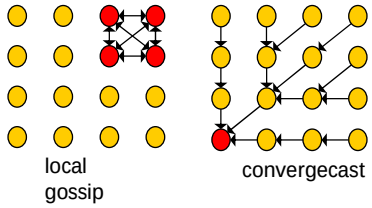
- Dedicated slot for transmission (no contention)
- Eventually low power period when no transmission is expected
- Synchronization hard if number of nodes explodes

MAC Design guidelines

- Switch radio off when possible (duty cycle)
- AND, minimize number of switches

- Low complexity (memory)

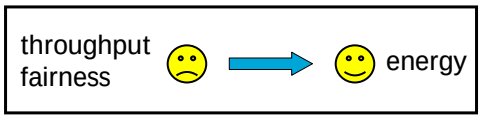
- Trade off performance for energy
- Optimize for traffic patterns



Energy efficient MAC

Performance/Cost trade-off
- latency
- throughput
- fairness
- energy consumption

Organizational/Flexibility trade-off
- contention-based
- schedule-based



Energy efficient MAC

- idle listening (to handle potentially incoming messages)
- collisions (wasted resources at sender and receivers)
- overhearing (communication between neighbors)
- protocol overhead (headers and signaling)
- traffic fluctuations (overprovisioning and/or collapse)
- scalability/mobility (additional provisions)

Protocols Network layer

A communication protocol network layer

Provides functional and procedural means to exchange network service data units between two transport entities over a network connection. It provides transport entities with independence from routing and switching consideration

Easy flow control (few data to send)
Hard routing (low duty-cycle, topology change)

Network – Structure

Not always predictable but can follow logical structure

Examples:

- PRNET – Packet Radio Network (DARPA)
  - Special packet are sent every 7.5 s in order to update neighbor tables
  - →**Not Scalable!**
- LCA – Linked Cluster Architecture
  - Nodes are organized in subgroup (cluster)
  - Each cluster has a cluster head and one or more gateway
  - →**Need a global clock to synchronize clusters**
  - →**Optimal clustering NP-hard problem (heuristic algorithm)**
- LEACH – Low Energy Adaptive Clustering Hierarchy
  - Clustering based on signal energy strength

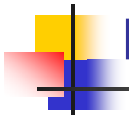
Network – Routing

Hard, due to node failure and mobility

→Balance between low duty cycle and frequent path updates

Routing algorithm can be classified in three group

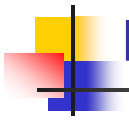
- Connect dominating
  - Try to find the shorter path to the destination
- Energy dominant
  - Life of network can be longer if energy consumption is balanced among nodes
- Biological model
  - Ants communication paradigm



Protocols – Security (1)

Security Concerns:

- Integrity - Ensure that information is accurate, complete, and has not been altered in any way.
- Availability - Ensure that a system can accurately perform it's intended purpose and is accessible to those who are authorized to use it.
- Confidentiality - Ensure that information is only disclosed to those who are authorized to see it.



Protocols – Security (2)

Possible threats:

- Passive threats
  - Eavesdrop
- Active threats
  - Bogus Routing (against routing information exchanged between nodes)
  - Selective forwarding (stop messages propagation)
  - Sink hole (attract messages from neighbor)
  - Sybil attack (forge multiple identities)
  - Wormhole (send wrong information about distance in order to force different routing path)
  - HELLO floods (send packet with higher energy, attract communication)
  - Acknowledge Spoofing (send fake ack messages to encourage communication)

Protocols – Security (3)

Traditional security techniques cannot be applied due to system constraints

- Power
- Bandwidth
- Computation

Secure protocols uses:

- Encription
- Data authentication
- Data freshness

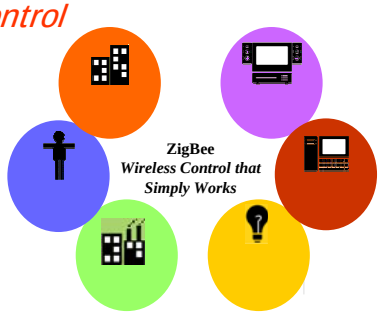
IEEE 802.15.4 – ZigBee

Motivation:

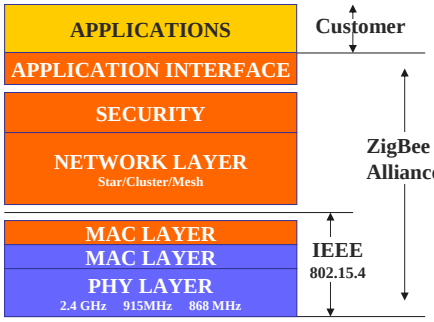
define a *complete* open *global standard* for reliable, cost-effective, low-power, wirelessly networked products addressing *monitoring and control*

Applications:

- Building automation
- Consumer electronics
- Personal health care
- Industrial control
- Commercial control



IEEE 802.15.4 – ZigBee



IEEE 802.15.4™

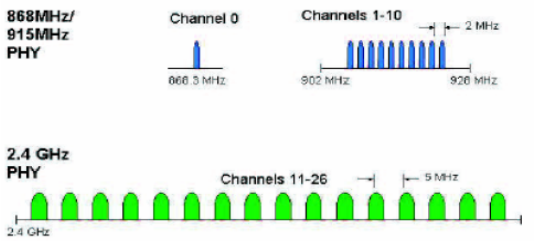
- Physical layer
- Media Access Control layers

ZigBee Alliance

- Network layer
- Security
- Standard interface to the application

IEEE 802.15.4 – PHY layer

Communication over 26 channel in 3 ISM band



DSSS modulation:

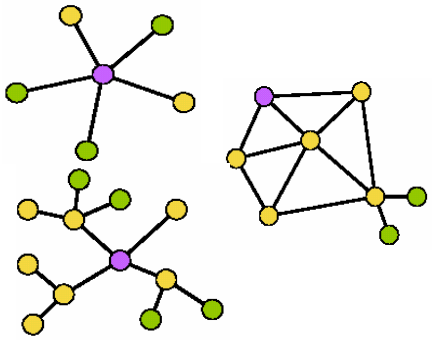
- B-PSK: 20 kb/s (868MHz), 40kb/s(915MHz)
- Q-PSK: 250 kb/s (2.4GHz)

IEEE 802.15.4 – MAC layer

Define two device type:
- Reduced Function Device (RFD)
- Full Function Device (FFD)

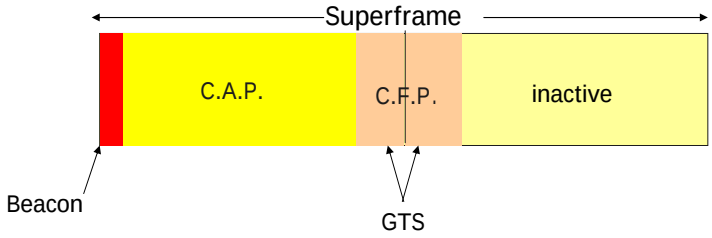
Define two roles:
- Coordinator
- Associated Device

Three available topologies:
- Star
- Mesh
- Cluster tree



IEEE 802.15.4 – MAC layer

Hybrid contention and scheduled based MAC



Security suite:
- Encryption: Advanced Encryption Standard (AES) 128bit
- ACL, Access Control List

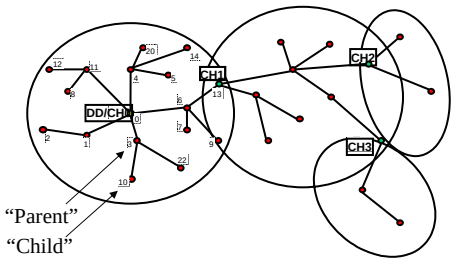
ZigBee – Network

Three roles:

- ZigBee Coordinator (ZC)
- ZigBee Router (ZR)
- ZigBee End Device (ZED)

Maintain the device types, network topologies and beacon/non beacon structure.

- Description based service discovering
- Employ multi-hop routing
- Can be very large (255 cluster of 254 nodes), and span over wide areas
- Mesh and Cluster tree provides redundant routes
- Automatic retries and acknowledge



ZigBee – Application

- Devices are modeled through *Application Objects*
- Application Objects communicate through the exchange of *Attributes*
- Attributes are sent either
  - Directly to destination application objects (thereby to target device)
  - To ZigBee coordinator, ZigBee coordinator reflects Attributes to single or multiple target objects
- Generic ZigBee device functions are provided through *ZigBee Device Objects* (ZDO)

Two new definition:

- **Endpoint**: an extension of the address which permits to support multiple application
- **Profiles**: an agreement on a series of messages defining an application

ZigBee – Security

Security is obtained using special key to encrypt messages

- Master Key, provided by a trust center (usually the coordinator).
- Network Key, used for all Network commands from any device.
- Link Keys, used for each pair of communicating devices.

Features:

- Authentication and Encryption
- Freshness (frame counters)
- Message Integrity

Slotted Protocols

Contention based protocols suffer for:

- Collision
- Over-hearing
- Idle listening

Solution: coordinated sleeping

- Synchronize nodes
- Sleep periodically

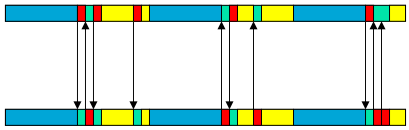
Slotted protocols

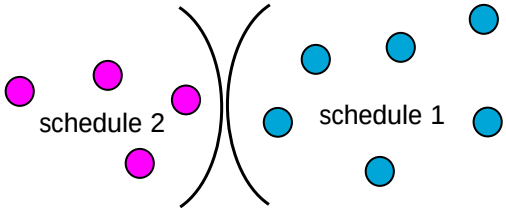
- T-MAC
- S-MAC

S-MAC

Slotted MAC

- Periodic listen and sleep
- Message passing



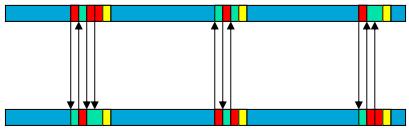


- Periodic broadcast of schedule
- Border nodes follow both schedules

T-MAC

Time Out MAC

- fixed frames
- variable active period



Advantages:

- Low duty cycle
- Automatic adaptation
- Handle traffic fluctuation

} Not possible with S-MAC

Bluetooth

Bluetooth is a short-range wireless network originally intended to replace the cable(s) connecting portable and/or fixed electronic devices.

Two main field of application:

- Voice
  - Phone
  - Head set
- Data
  - Internet bridge
  - Synchronizer

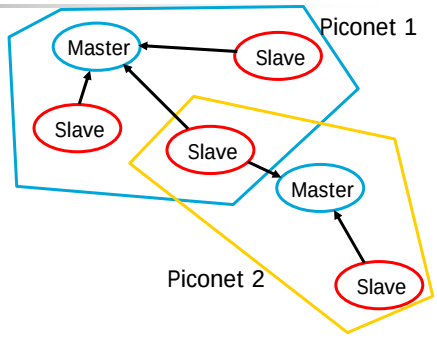
Bluetooth PC Card

Bluetooth Technical overview

Basic network, Piconet:

- At most 7 slaves
- 1 master

A set of piconet form a scatternet



All devices are identical:

- Data rate 720 kb/s
- Range 10-100 meters
- FHSS (Gaussian Frequency Shift Keying) on 2.4GHz ISM band
- 48 bit identifier
- Every device can be either slave or master
- Dynamic environment

Bluetooth

Designed to be:

- Simple and robust
- Low power
  - 30-100mA active current
  - Low power states available
- (Relatively) Low cost

...but not enough for many WSN applications

Limits:

- Battery life too short: 1-7gg
- System resources high: 250kB+ memory
- Network size small: 7 devices
- Slow to react at changes

Summary

- WSN are a flexible, low cost and efficient solution to collect information from the environment
- WSN requires ad-hoc protocols in order to archive goals as
  - Low power
  - Low cost
  - Flexibility
  - Security
- This specific must be kept in mind at every level of design: PHY, Data Link, Network
- Many protocols are been designed to meet WSN need:
  IEEE 802.15.4, ZigBee, Bluetooth, T-MAC, S-MAC

...and tomorrow?

WSN will be everywhere to meet user needs

WSN protocols must:

- Follow a common standard
- Respect countries norms
  - Use world-wide free ISM band
  - Be EMC complaint
- Be flexible and robust
- Secure

Thank you