Corso Professionalizzante di Specializzazione (3 CFU)
Ingegneria delle Telecomunicazioni, Ingegneria Informatica,
Ingegneria dei Sistemi di Controllo e dell'Automazione,
Informatica

WSN and VANET Security

Part I: Security Analysis

Lecture I.2

The case of WSN

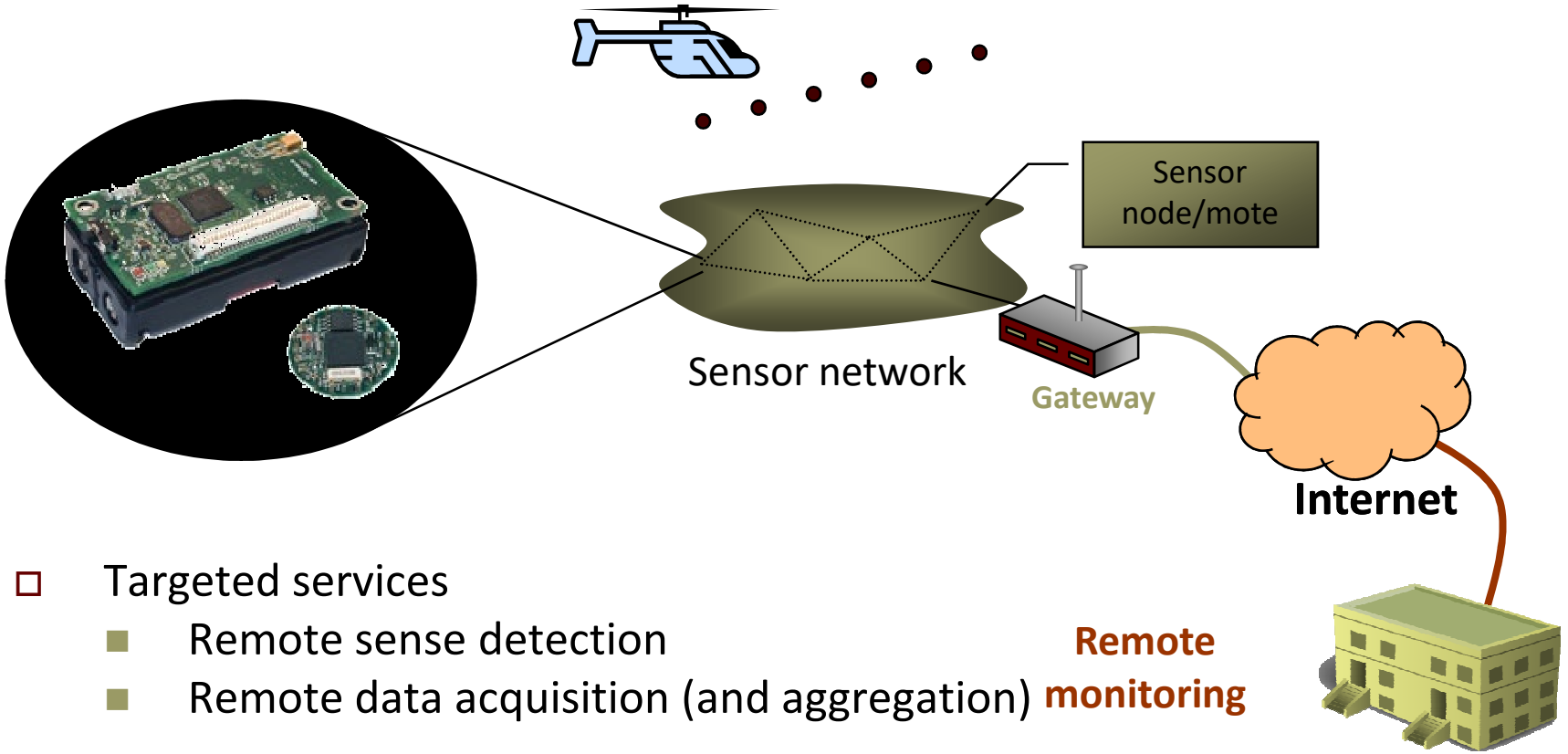
Ing. Marco Pugliese, Ph.D., SMIEEE
Senior Security Manager UNI 10459-2017 ICMQ cert. 25-00238
marco.pugliese@univaq.it
April 11th, 2025

Outline

- Wireless Sensor Network (WSN)
  - Applications
  - Design Issues
  - Reference WSN Architecture
- IEEE 802.15.4

Wireless Sensor Networks

- Wireless sensors + wireless network
- Typically WSN are organized as a tree topology (with redundancy for resilience)
- If hierarchically organized, WSN are clustered with cluster head nodes
- Any node makes data aggregation



- Targeted services
  - Remote sense detection
  - Remote data acquisition (and aggregation)

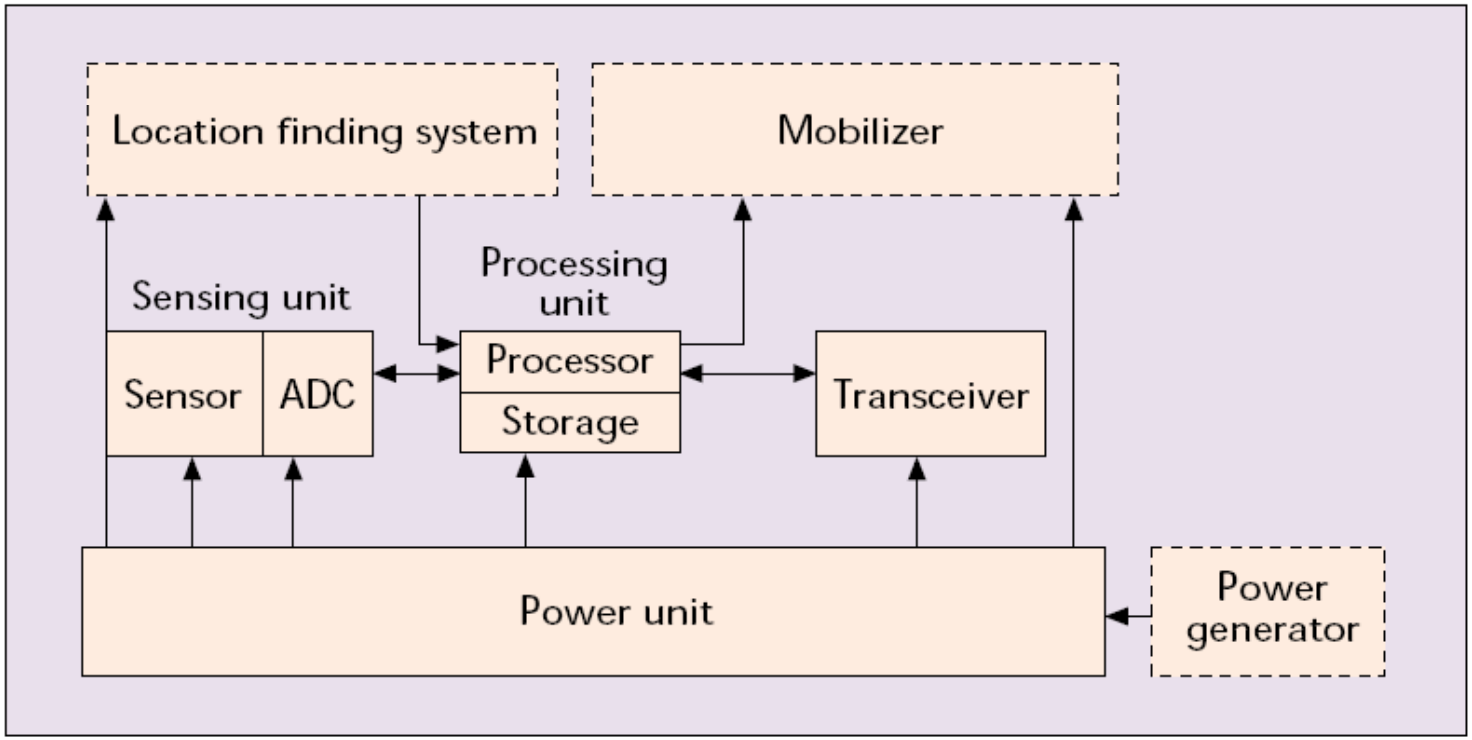
WSN Nodes are Smart Sensors

- Each WSN node is a “smart sensor”.
- A “smart sensor” is a sensor with autonomous processing capabilities
- Processing means “execution of functions”.
- Functions can be: data processing, topology management, routing, …, transmission, resilience management, … , applications.

- Node types in WSN
  - **Ordinary Sensor Node:**
    - Low-power, Low-resource, Low-bandwidth, short-range
    - Implements the base protocol stack of the reference standard
  - **Aggregation Node:**
    - An Ordinary Sensor Node with higher resources for (at least) data aggregation and routing function**: in clustered topologies it denotes the Cluster Head role**.
  - **Base station**
    - An edge unit interfacing the backbone or directly the SOC
    - Usually is not a constrained platform (e.g. electrically feeded)

Sensor Node Architecture

- A sensor node is basically made up of four basic components: sensing unit, processing unit (microcontroller), radio transceiver unit, and power unit.
- They may also have additional application-dependent components such as a location finding system, power generator, and mobilizer.
- Key building blocks for any mote are the microcontroller and radio transceiver that can be used on more platforms.



Berkeley “Motes” (“Smart Dust”)

Mote Evolution

Mote Type	*WeC*	*René*	*René 2*	*Dot*	*Mica*	*Mica2Dot*	*Mica 2*	*Telos*
Year	1998	1999	2000	2000	2001	2002	2002	2004
								
Microcontroller								
Type	AT90LS8535		ATmega163		ATmega128			TI MSP430
Program memory (KB)	8		16		128			60
RAM (KB)	0.5		1		4			2
Active Power (mW)	15		15		8		33	3
Sleep Power (μW)	45		45		75		75	6
Wakeup Time (μs)	1000		36		180		180	6
Nonvolatile storage								
Chip	24LC256				AT45DB041B			ST M24M01S
Connection type	I^2C				SPI			I^2C
Size (KB)	32				512			128
Communication								
Radio	TR1000				TR1000	CC1000		CC2420
Data rate (kbps)	10				40	38.4		250
Modulation type	OOK				ASK	FSK		O-QPSK
Receive Power (mW)	9				12	29		38
Transmit Power at 0dBm (mW)	36				36	42		35
Power Consumption								
Minimum Operation (V)	2.7		2.7		2.7			1.8
Total Active Power (mW)	24				27	44	89	41
Programming and Sensor Interface								
Expansion	none	51-pin	51-pin	none	51-pin	19-pin	51-pin	10-pin
Communication	IEEE 1284 (programming) and RS232 (requires additional hardware)							USB
Integrated Sensors	no	no	no	yes	no	no	no	yes

Iris
2007

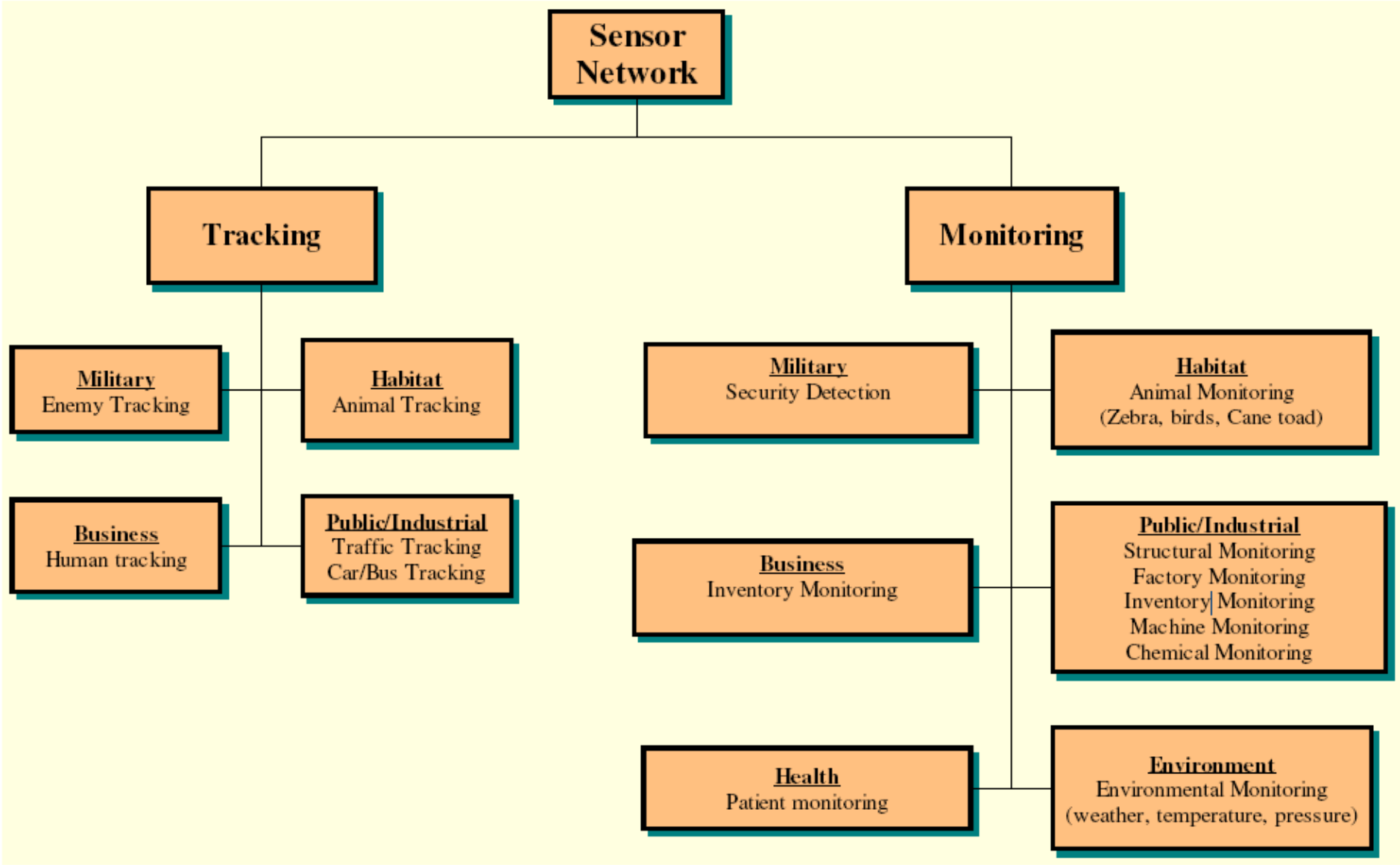
IEEE 802.15.4 compliant

AT86RF230

Outline

- Wireless Sensor Network (WSN)
  - Applications
  - Design Issues
  - Reference WSN Architecture
- IEEE 802.15.4

A Taxonomy for WSN Applications



Outline

- Wireless Sensor Network (WSN)
  - Applications
  - Design Issues
  - Reference WSN Architecture
- IEEE 802.15.4

Design Issues

Integrated design approach of different functions (secure by design)

- **Topology Management Functions**
  - Both cluster-wise and pair-wise topologies
  - Operation continuity (through resilience management, functions redundancies and dynamic assignments)
  - Code management
- **Data processing Functions**
  - Time-driven: for synchronous comms. (data traffic monitoring)
  - Event-driven: for asynchronous comms. (anomaly detection)
- **Transmission Functions**
- **Resource Management**
- **Energy Management**
  - Duty cycle, MAC procedures
- **Security Functions**

$$P = P_c + P_p + P_s \approx P_c + P_p$$

Power Consumption - Data Comm. (P_C)

$$P_c = N_T\,[P_T(T_{on} + T_{st}) + P_{out}(T_{on})] + N_R[P_R(R_{on} + R_{st})]$$

where

P_T is power consumed by transmitter

P_R is power consumed by receiver

P_{out} is output power of transmitter

T_{on} is time for "transmitter on"

R_{on} is time for "receiver on"

T_{st} is start-up time for transmitter

R_{st} is start-up time for receiver

N_T is the number of times transmitter is switched on per unit time

N_R is the number of times receiver is switched on per unit time

$T_{on} = R_{on} = L / R$

L = packet size, R data rate

Power Consumption - Data Proc. (P_p)

$$P_p = C \cdot V^2_{dd} \cdot f + V_{dd} \cdot I_o \cdot \exp\{V_{dd} / V_T\}$$

where

C is the total switching capacitance

V_{dd} is the voltage swing (output from the ADC Sensing Unit)

f is the switching frequency

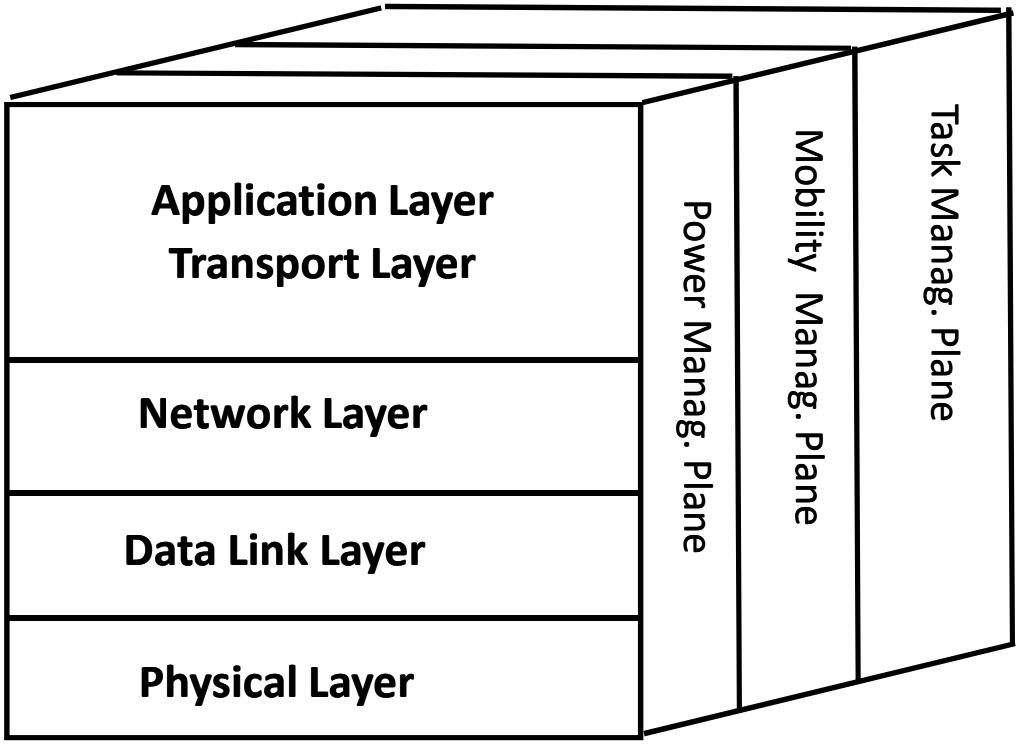
V_T is the threshold voltage in the (non linear) processing devices

I_o is the leakage current in processing devices (the second term indicates the power loss due to leakage currents)

Outline

- Wireless Sensor Network (WSN)
  - Applications
  - Design Issues
  - Reference WSN Architecture
- IEEE 802.15.4

Reference WSN Architecture



Reference WSN Architecture

- Power management plane
  - Manage duty cycles of all active components in the sensor
- Mobility management plane
  - Detects and registers the movement of sensor nodes, so a route back to the user is always maintained.
- Task management plane
  - Balances and schedules the sensing tasks given to a specific region

Reference WSN Architecture

- Physical layer
  - Responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption.
- Data link layer
  - Responsible for the multiplexing of data streams, data frame detection, medium access and error control.
- Network layer
  - Responsible for multi-hop wireless routing protocols between the sensor nodes and the sink node.
- Transport layer
  - Responsible for access by Internet or other external networks.
- Application layer

MAC Protocol Requirements

MAC stands for **Medium Access Control**.

Therefore a MAC protocol manages the access to a shared medium of data frames from different transmitters to different receivers applying predefined polices.

MAC requirements are:

- Energy Efficiency: sources of energy waste are
  - Collision, Idle Listening, Overhearing, and Control Packet Overhead
- Effective Collision Avoidance
  - When and how the node can access the medium and send its data
- Tolerant to changing RF/Networking conditions
- Scalable to large number of nodes

WSN Requirements for MAC Protocols

Medium is the electromagnetic spectrum → radio channels set

Access Control

- Minimize retrasmissions rate (due to collisions)
- Robust to topology changes
- Avoid the need of global clock synchronization
- Avoid the need of global topology information
- Tolerant to changing RF/Networking conditions
- Scalable to large number of nodes

- WSN MAC standard protocol is Carrier Sense Multiple Access (CSMA)
- **CSMA/CA is the MAC algorithm adopted in IEEE 802.15.4 networks**
- Radio coverages determine the detection domains ("Hidden Node Problem").

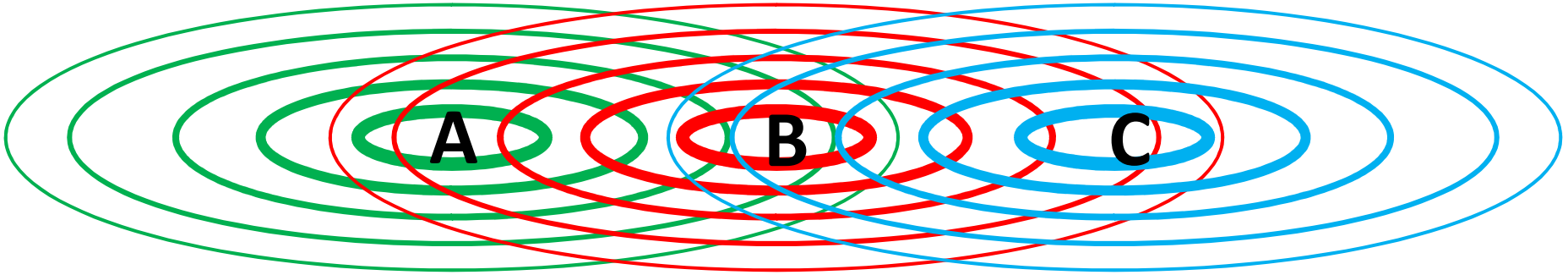
CSMA/CA

- **CSMA with Collision Avoidance (CSMA/CA)**: is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is unreliable due to the *hidden node problem*.
- **Collision Avoidance** is used to improve the performance of the CSMA in radio networks.
  - **Request to Send/Clear to Send (RTS/CTS)**: this handshake is used to mediate access to the shared medium and therefore to avoid the "hidden node problem".
  - **Transmission**: if the medium was identified as being clear *or* the node received a CTS to explicitly indicate it can send, it sends the frame in its entirety.
- However some vulnerabilities are introduced by the Collision Avoidance mechanism (CTS is equivalent to an ACK message).

- **CSMA/CA is the MAC algorithm adopted in IEEE 802.15.4 networks**

CSMA and the "Hidden Node Problem"

- **Carrier Sense Multiple Access (CSMA)**: the sender listens to the channel before transmitting its packet: if the channel is found busy the sender will defer its access by an amount of time which is called *back-off period* otherwise it will send. CSMA gives the recent channel access to the contending node with the smallest back-off value.
- **Radio coverages determine the detection domains.**



- Node A is hidden to node C and vice-versa because A and C **are not in the same detection domain.**
  - A sends to B, C cannot detect A's transmission (CS fails)
  - Collision at B, C cannot detect the collision (CD fails)
  - **A is "hidden" for C**

WSN Routing Protocols

- Clustered WSN (in general clustered ad hoc networks) use **proactive routing protocols**: state-based with routing databases to be periodically updated, e.g. Destination Sequenced Distance Vector (DSDV) or Optimized Link State Routing (OLSR).
  - Hierarchical routing: a simple proactive routing where each node forwards data to its parent node.

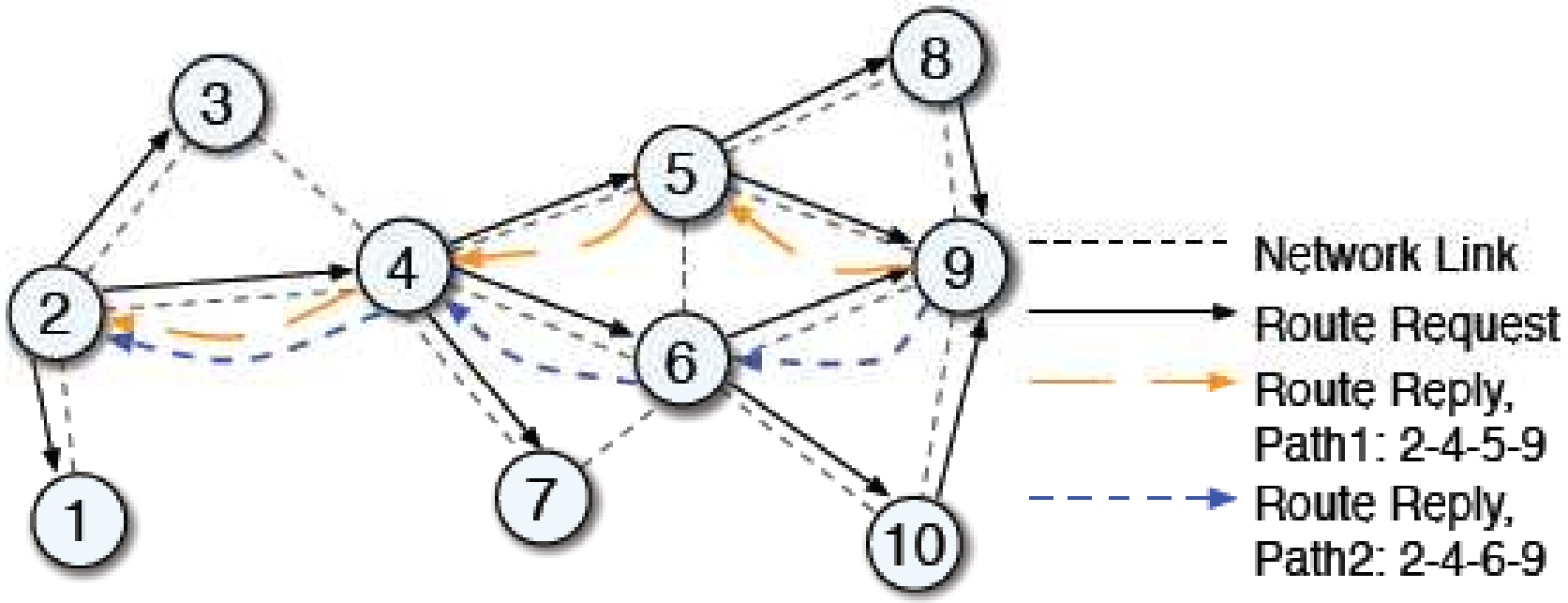
- No clustered WSN (in general no clustered ad hoc networks) use **reactive routing protocols**: state-less, routes are built on-demand, e.g. **Dynamic Source Routing** (DSR)

Reactive Routing: DSR

- Dynamic Source Routing (DSR) is an on-demand source routing protocol
- Nodes maintain routing information in route caches

- Two components:
  - **Route Discovery**
    - used only when source S (e.g. node 2) attempts to send a packet to destination D (e.g. node 9)
    - based on flooding of Route Requests (RREQ) and returning Route Replies (RREP)
  - **Route Maintenance**
    - makes S able to detect route errors (e.g., if a link along that route no longer works)

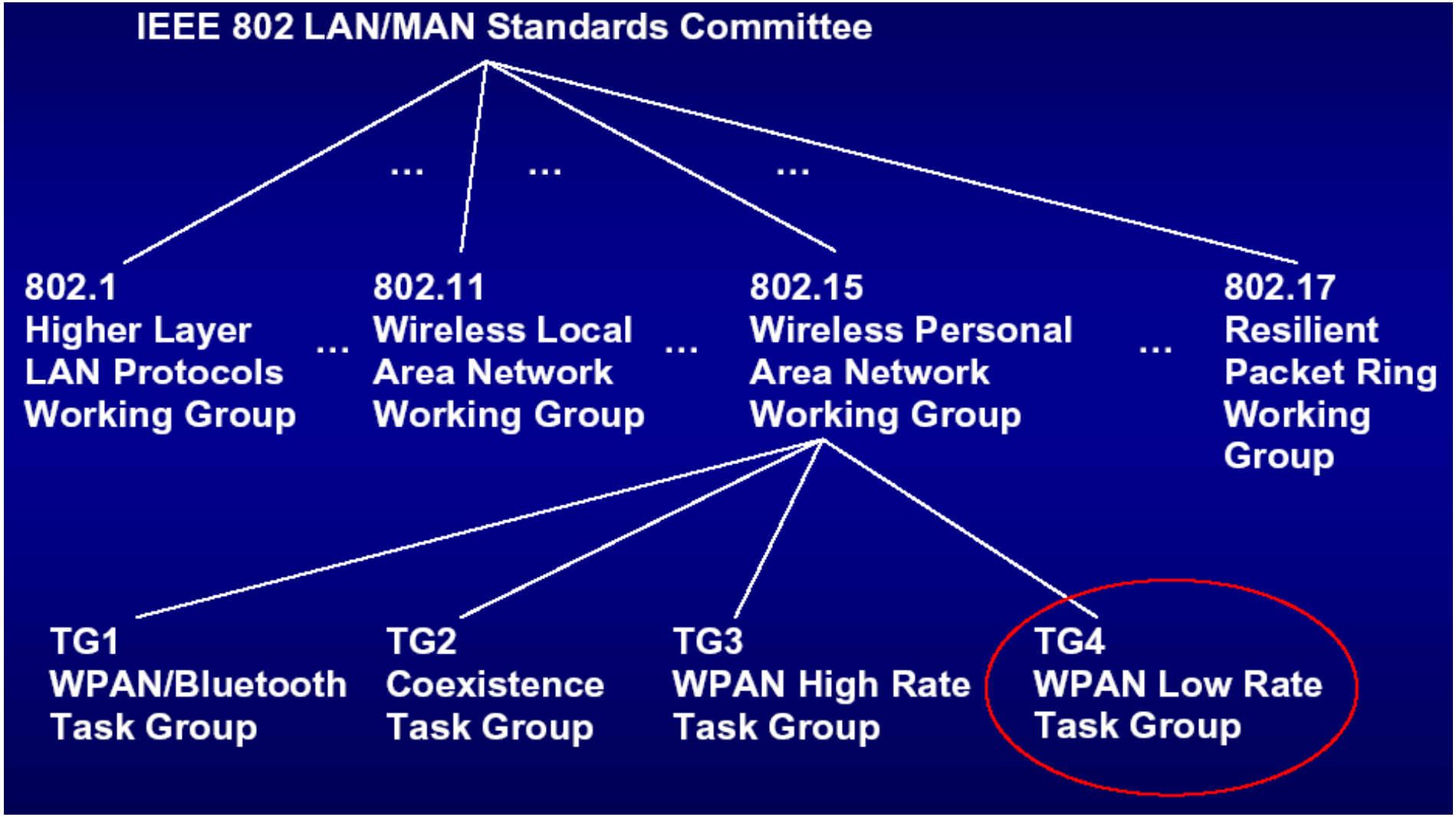
DSR Route Discovery illustrated



Outline

- Wireless Sensor Network (WSN)
  - Applications
  - Design Issues
  - Reference WSN Architecture
- IEEE 802.15.4

IEEE 802.15.4 Working Group



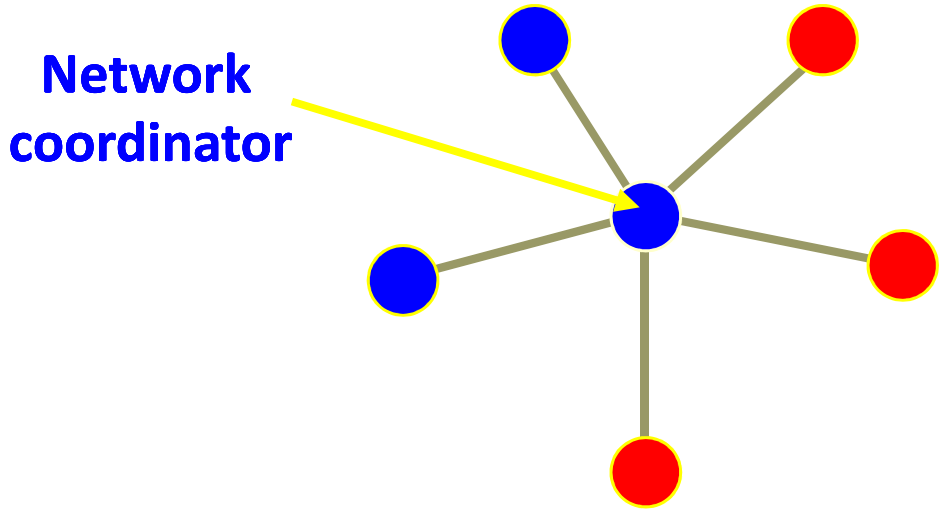
IEEE 802.15.4 Main features

- Current version: IEEE 802.15.4-2020
- It manages the physical layer (PHY) and medium access control (MAC) sublayer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements are defined in this standard. In addition, the standard provides modes that allow for precision ranging. PHYs are defined for devices operating in a variety of geographic regions.
  - Low power consumption (extremely low duty-cycle <0.1%)
  - Data rates of 250 kbps, 40 kbps, and 20 kbps.
  - Two addressing modes; 16-bit short and 64-bit IEEE addressing.
  - Support for critical latency devices
  - CSMA-CA channel access
  - Automatic network establishment by the coordinator
  - Fully handshaked protocol for transfer reliability
  - Power management to ensure low power consumption
- IEEE 802.15.4e amendment with enhanced multiple medium access (*Time Slotted Channel Hopping,* TSCH), more robust to EM interferences and to collisions. Suited for industrial applications of IoT.

IEEE 802.15.4 Devices and Topologies

- Two types of devices: *Full Function device* (FFD) and *Reduced Function Device* (RFD).
  - RFD low complexity node that can communicate only with FFDs into its radio range
  - FFD high complexity node, can operate as *PAN Coordinator*, can interact with any other node into its radio range
- Two types of topologies: star / peer-to-peer.
  - **Star**: simpler contexts where an hub (*PAN Coordinator*) communicates with other nodes into its radio range. Setup a star topology is quite easy: the first activated FFD, establishes a new WPAN instance and becomes its coordinator; the other nodes attach the WPAN through signaling protocols with the *PAN Coordinator* (no need of routing protocols)
  - **Peer-to-peer**: more complex contexts with multi-hop communications (need of routing protocols at upper layers). Setup a peer-to-peer topology can involve more *PAN Coordinators,* to access other services, as syncronization, special terminals,…

Star topology



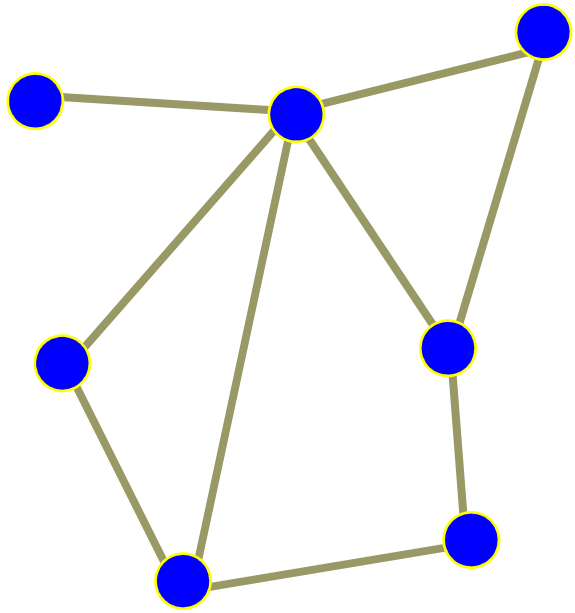
Master/slave

Full Function Device (FFD)

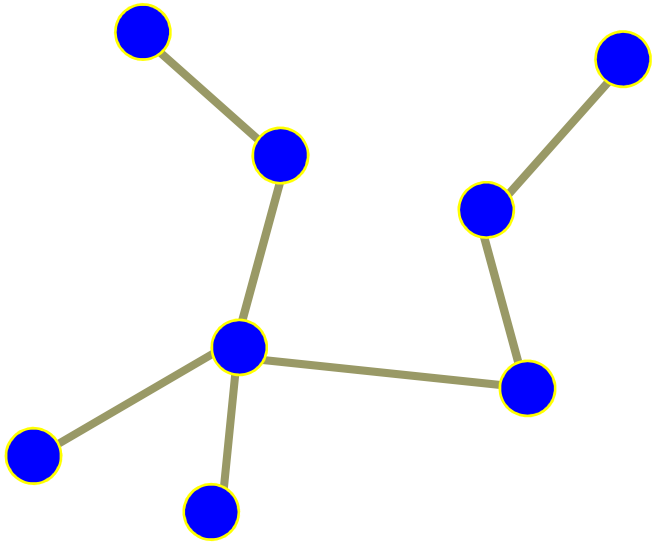
Reduced Function Device (RFD)

Communications Flow

Peer to peer topology



Point to point



Tree

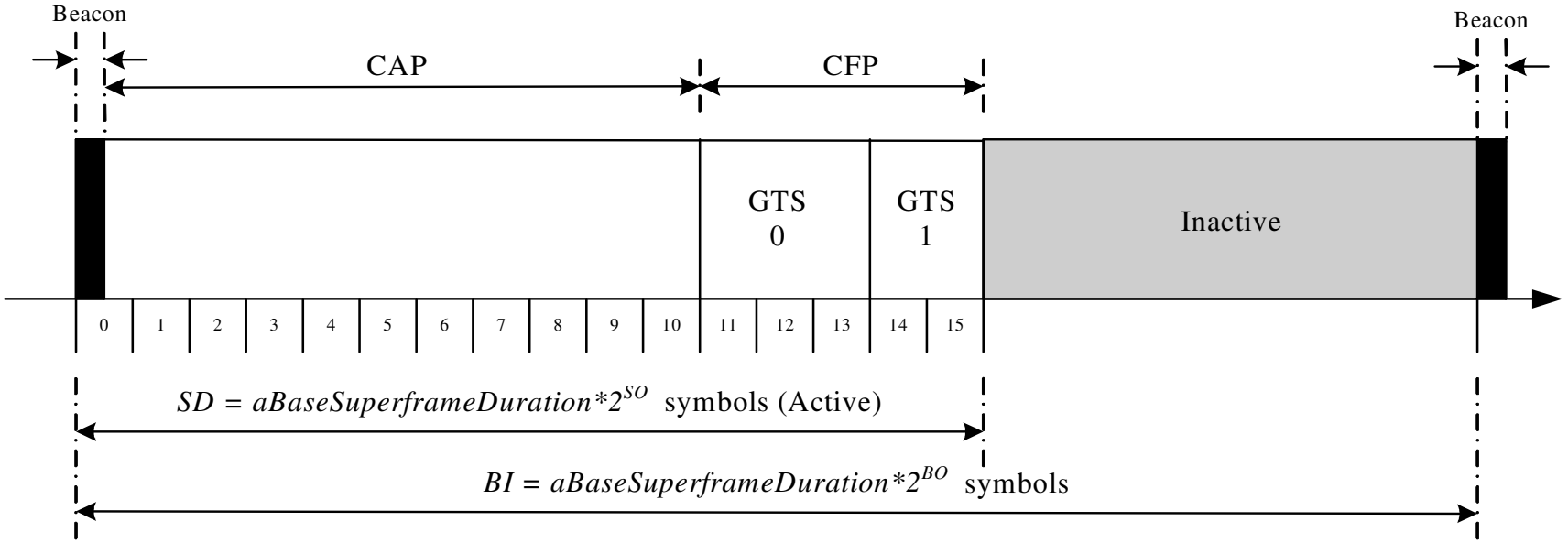
Full Function Device (FFD)

Communications Flow

IEEE 802.15.4 MAC

- **Beacon-enabled data transfer mode:**
  - Time is divided into a sequence of **super-frames**, each one delimitated by a special sync signal (**beacon**). Beacons are sents by the **PAN (Personal Area Network) Coordinator** and are in charge of the **synchronization** of all network devices.
  - The super-frame is subdivided in elementary time-slots which cointain a **Contention Access Period (CAP)** during which the mutiple channel access is managed by a low energy version of CSMA/CA algorithm (slotted CSMA/CA).
  - Optionally the super-frame can cointain a Contention Free Period (CFP) during which certain nodes can access without any collision through special guaranteed time-slot **(Guaranteed Time Slot, GTS)** and an Inactive Period, during which radio interfaces can be set in a sleep mode to save energy
- **No beacon-enabled data transfer mode:**
  - Nodes access the channel using the CSMA/CA algorithm (unslotted CSMA/CA) without any time partitioning.

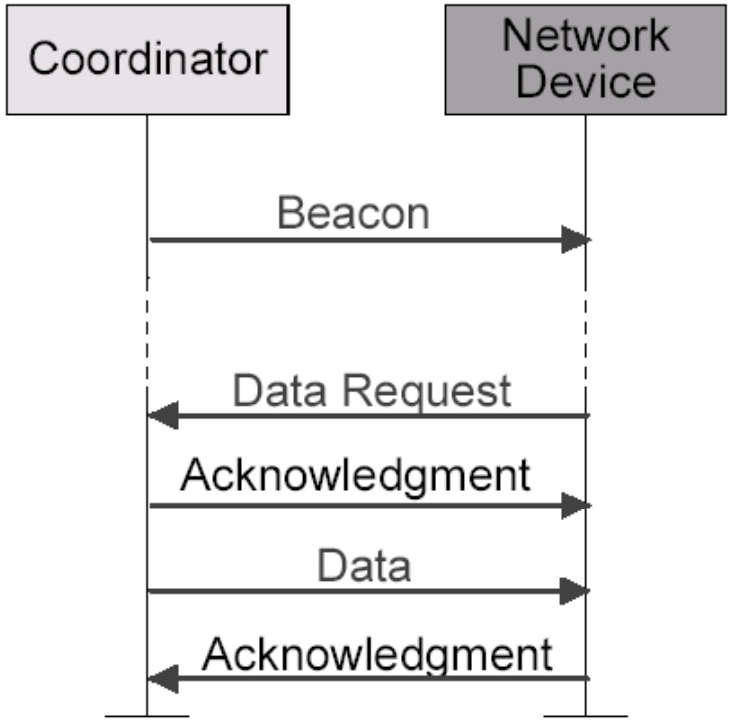
IEEE 802.15.4 MAC Super-frame



- A **super-frame** is divided into two parts
  - Inactive: all station sleep
  - Active:
    - Active period will be divided into 16 slots
    - 16 slots can further divided into two parts
      - Contention Access Period (CAP): contention-based channel access through CSMA/CA.
      - Contention Free Period (CFP): contention-free channel access controlled by the PAN coordinator through GTS

Beacon-Enabled Data Transfer Mode

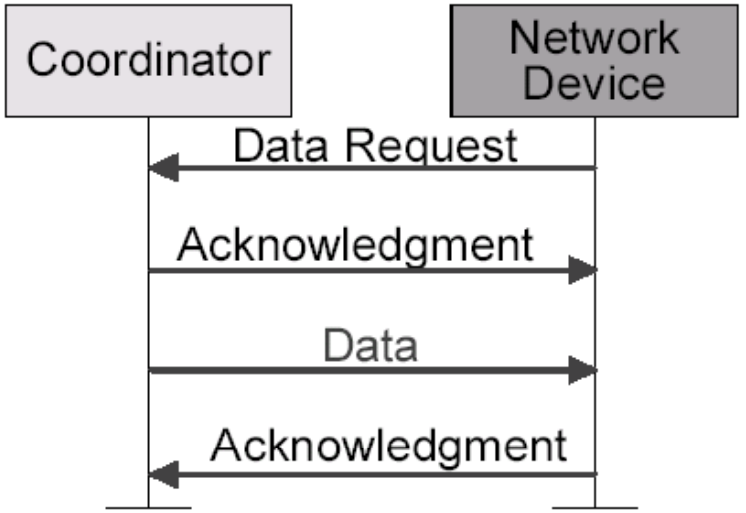
- Data transferred from coordinator to device in a beacon-enabled network:
  - The coordinator indicates in the beacon that some data is pending.
  - A device periodically listens to the beacon and transmits a Data Request command using slotted CSMA/CA.
  - Then ACK, Data, and ACK follow …



Communication from a coordinator
In a beacon-enabled network

No Beacon-Enabled Data Transfer Mode

- Data transferred from coordinator to device in a no-beacon-enable network:
  - The device transmits a Data Request using unslotted CSMA/CA.
  - If the coordinator has its pending data, an ACK is replied.
  - Then the coordinator transmits Data using unslotted CSMA/CA.
  - If there is no pending data, a data frame with zero length payload is transmitted.



Communication from a coordinator in a non beacon-enabled network