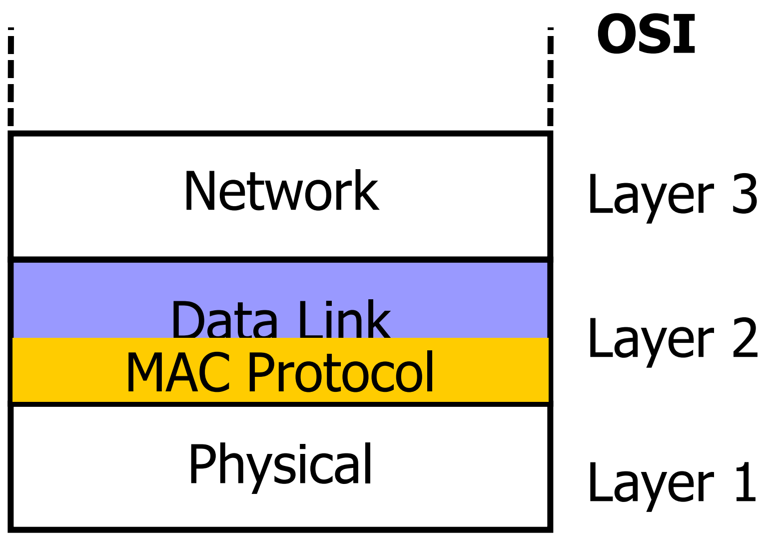
WSN Medium Access Control Protocols

Mohammad Hossein Yaghmaee
Associate Professor
Department of Computer Engineering
Ferdowsi University of Mashhad (FUM)

Part 1
MAC Layer Overview

Protocol Stack



Data link layer:

- mapping network packets ➔ radio frames
- transmission and reception of frames over the air
- error control
- security (encryption)

Challenges and Constraints

- Frequency allocation
  - All users operates on a common frequency band
  - Must be approved and licensed by the government
- Inference and reliability
  - Collision: begin transmission at the same time; hidden terminal; multipath fading
- Security
- Power consumption
- Human safety
- Mobility

Principal options and difficulties

- Medium access in wireless networks is difficult mainly because of
  - Impossible (or very difficult) to send and receive at the same time
  - Interference situation at receiver is what counts for transmission success, but can be very different from what sender can observe
  - High error rates (for signaling packets) compound the issues
- Requirement
  - As usual: high throughput, low overhead, low error rates, …
  - Additionally: energy-efficient, handle switched off devices!

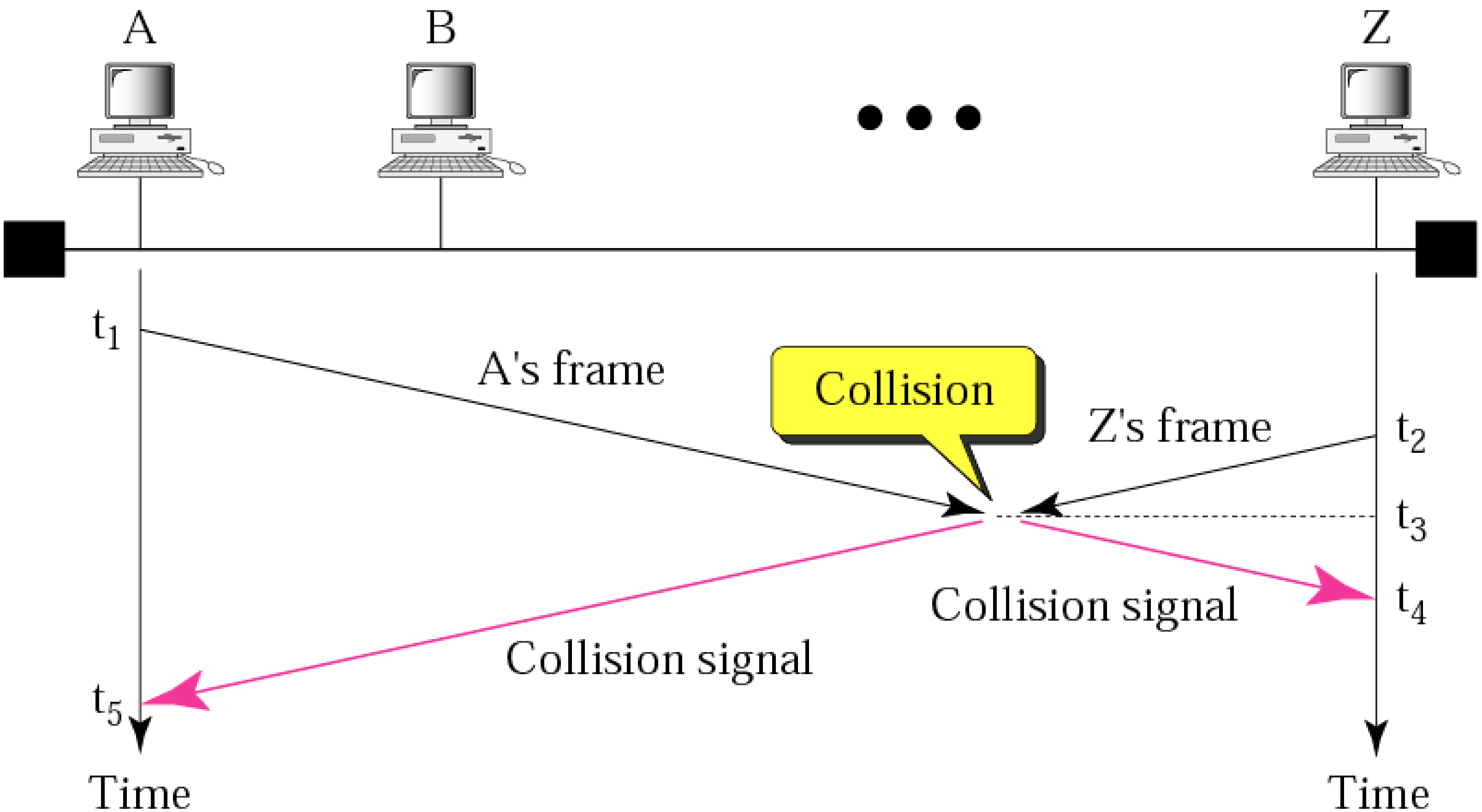
Requirements for energy-efficient MAC protocols

- Recall
  - Transmissions are costly
  - Receiving about as expensive as transmitting
  - Idling can be cheaper but is still expensive
- Energy problems
  - ***Collisions*** – wasted effort when two packets collide
  - ***Overhearing*** – waste effort in receiving a packet destined for another node
  - ***Idle listening*** – sitting idly and trying to receive when nobody is sending
  - ***Protocol overhead***
- Always nice: Low complexity solution

Wireless LAN: Motivation

- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - Send as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)

CSMA/CD

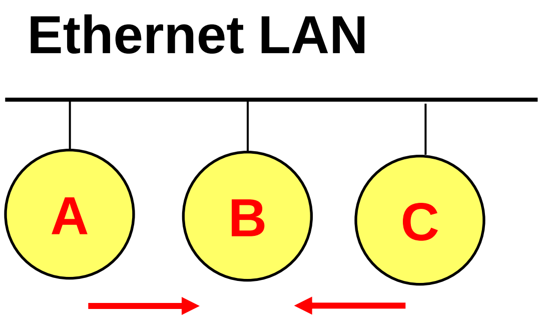


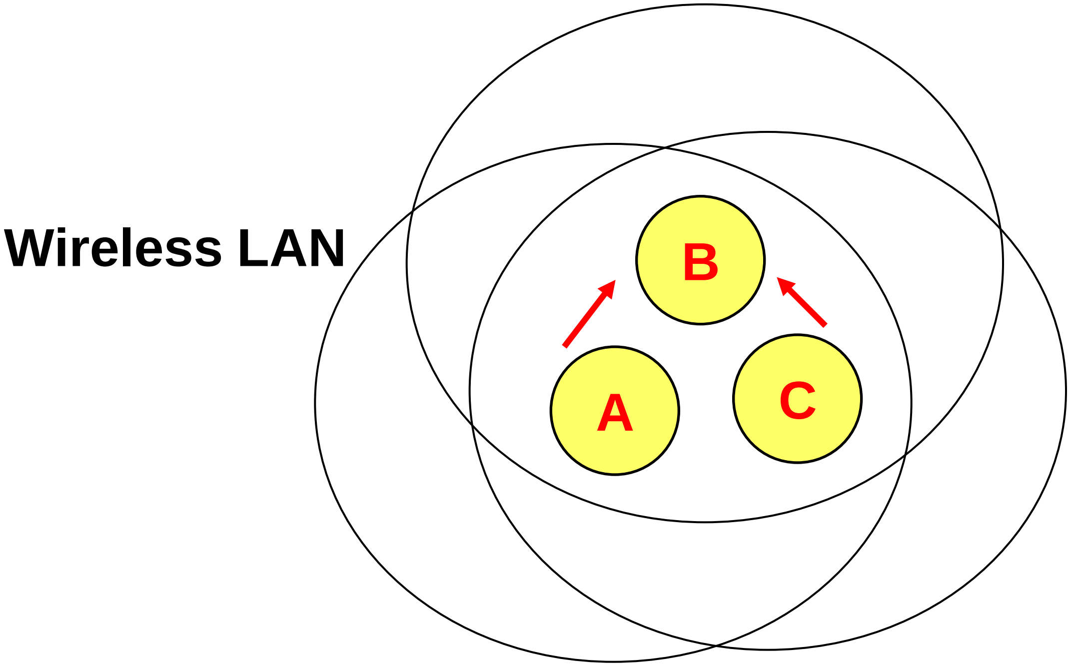
A
B
Z
t1
A's frame
Collision
Z's frame
t2
t3
t4
Collision signal
Collision signal
t5
Time
Time

Medium Access Problems in Wireless Networks

- Signal strength decreases proportional to the square of the distance
- Sender would apply CS and CD, but the collisions happen at the receiver
- Sender may not “hear” the collision, i.e., CD does not work
- CS might not work, e.g. if a terminal is “hidden”

Difference Between Wired and Wireless



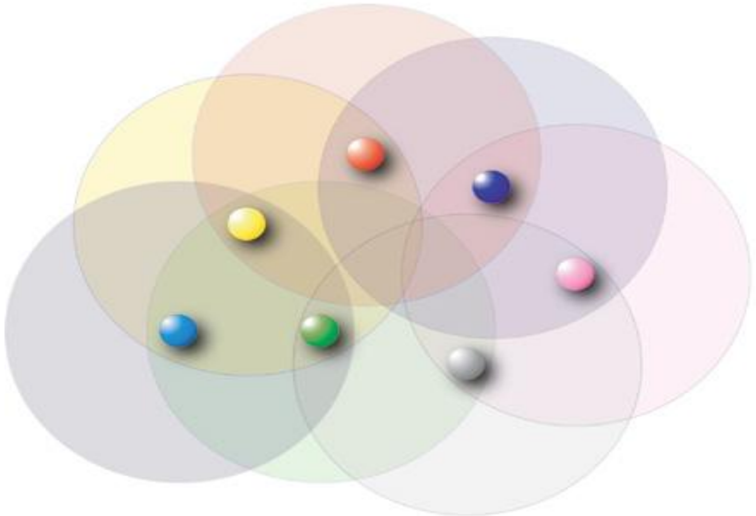


- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected at sender in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

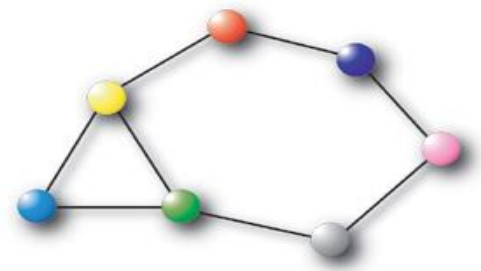
Wireless Sensor Networks Features

- A large number of limited power sensor nodes
- Distributed, multi-hop, ad-hoc operation; no infra-sctructure, no central control point
- Collect and process data from a target domain and transmit information back to specific sites
- Usage scenarios…
  - Disaster recovery
  - Military surveillance
  - Health administration
  - Environmental monitoring.

Wireless Sensor Networks



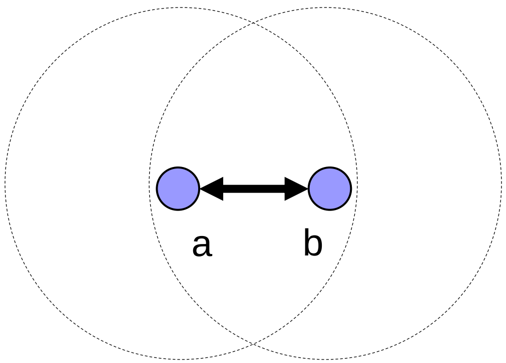
Each node has a **transmission range**, which determines its **neighbors**



Representation of the network as a graph

same transmission ranges ⇒ symmetric links ⇒ undirected graph

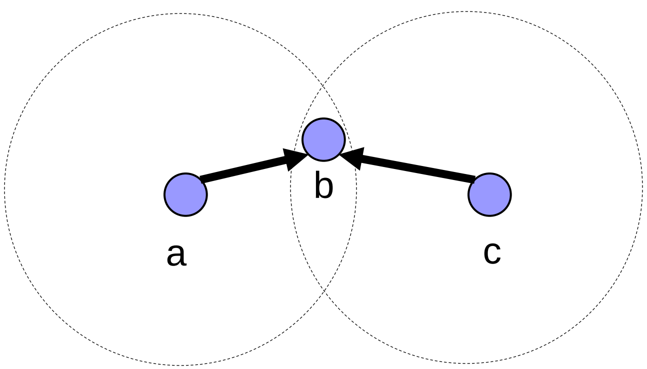
Interference / Collisions



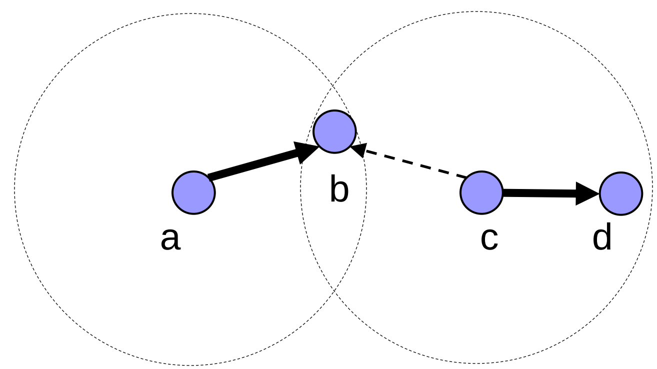
a and ***b*** interfere and hear noise only

Packets which suffered collisions should be re-sent.

Ideally, we would want all packets to be sent collision-free, only once…

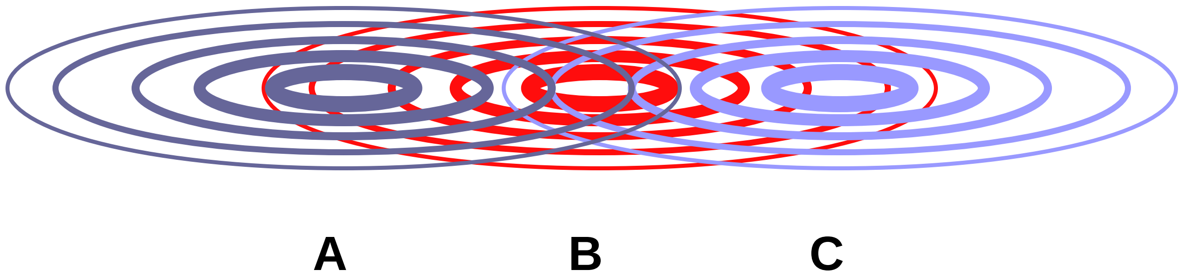


Interference on node ***b***
("Hidden terminal problem")



Interference on node ***b***

Hidden Terminal Problem

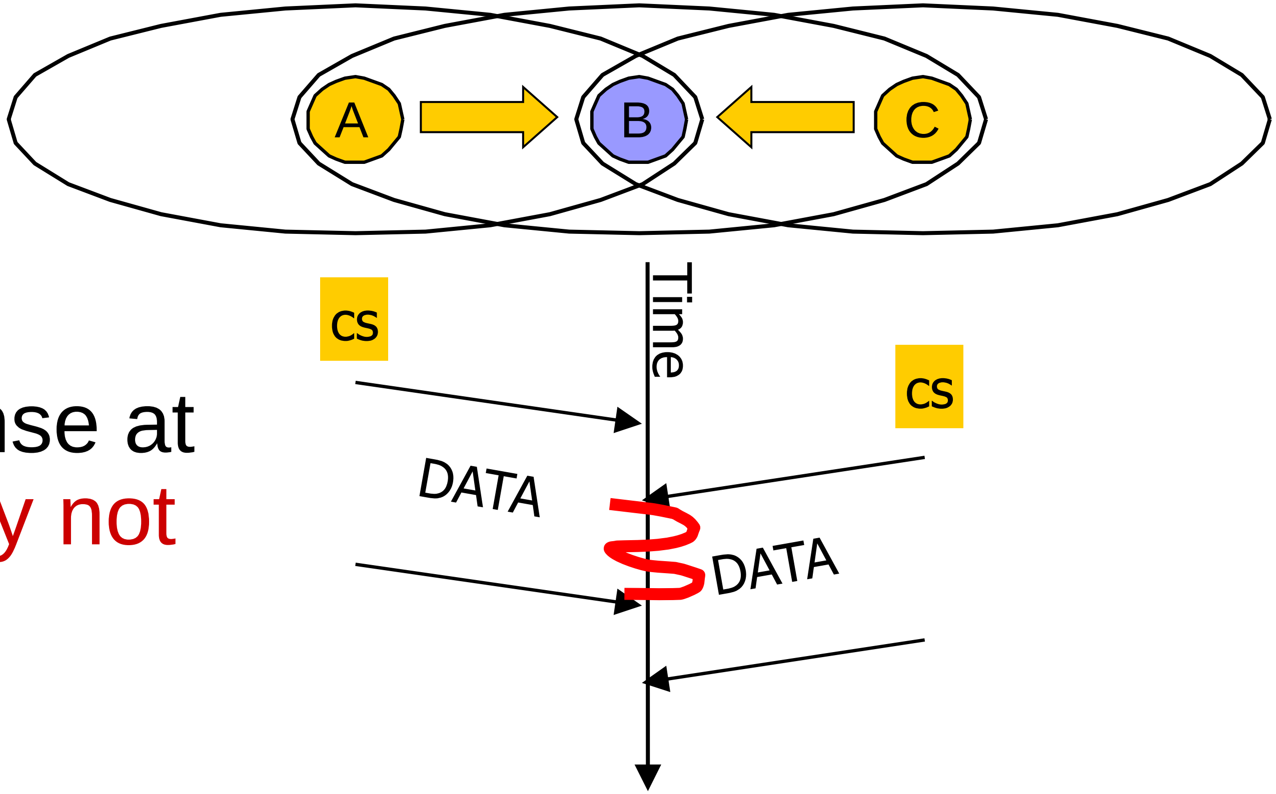


- Hidden terminals
  - A and C cannot hear each other.
  - A sends to B, C cannot receive A.
  - C wants to send to B, C senses a “free” medium (CS fails)
  - Collision occurs at B.
  - A cannot receive the collision (CD fails).
  - A is “hidden” for C.
- Solution?
  - Hidden terminal is peculiar to wireless (not found in wired)
  - Need to sense carrier at receiver, not sender!
  - “virtual carrier sensing”: Sender “asks” receiver whether it can hear something. If so, behave as if channel busy.

Wireless Problems

- Two main problems:
  - Hidden Terminal Problem
  - Exposed Terminal Problem

Hidden Terminal Problem



Carrier sense at sender may not prevent collision at receiver

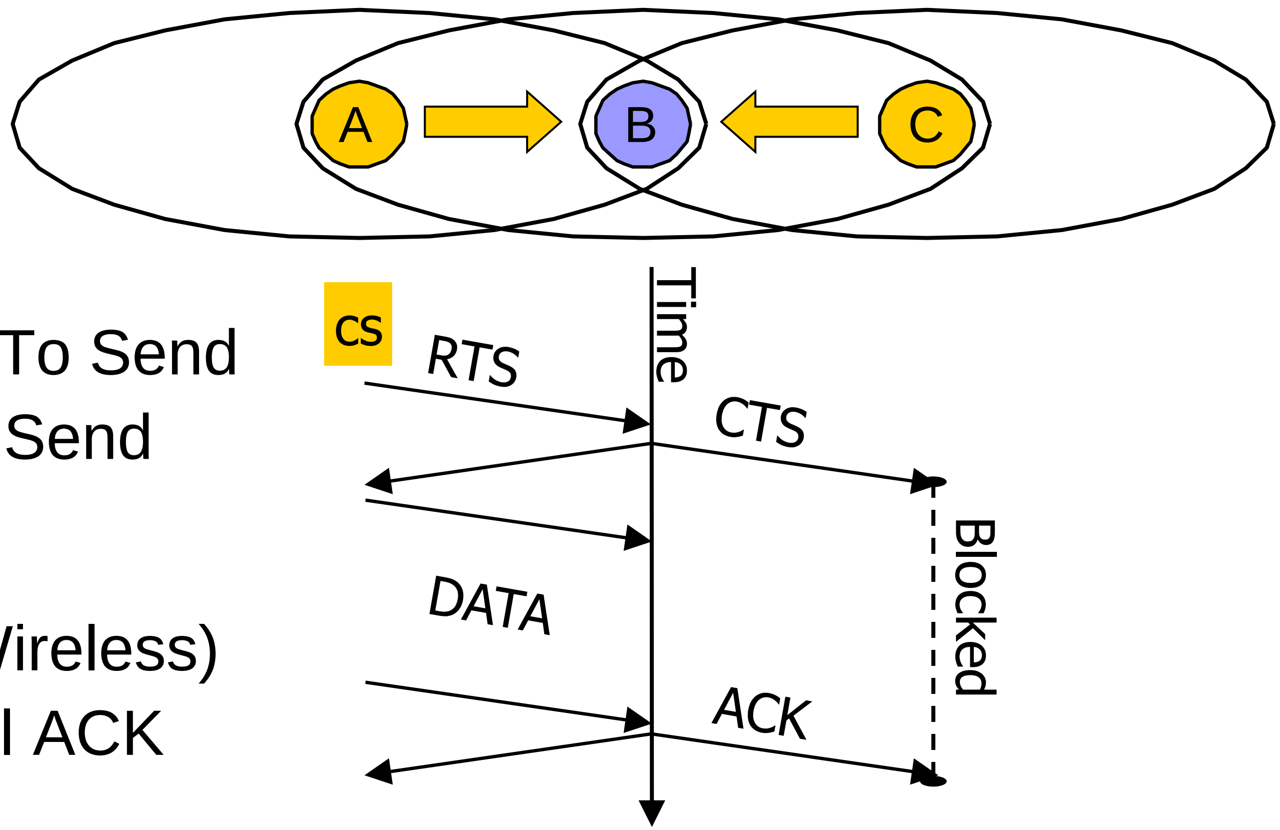
Solution: CSMA/CA: Collision Avoidance

MACA:

- Request To Send
- Clear To Send
- DATA

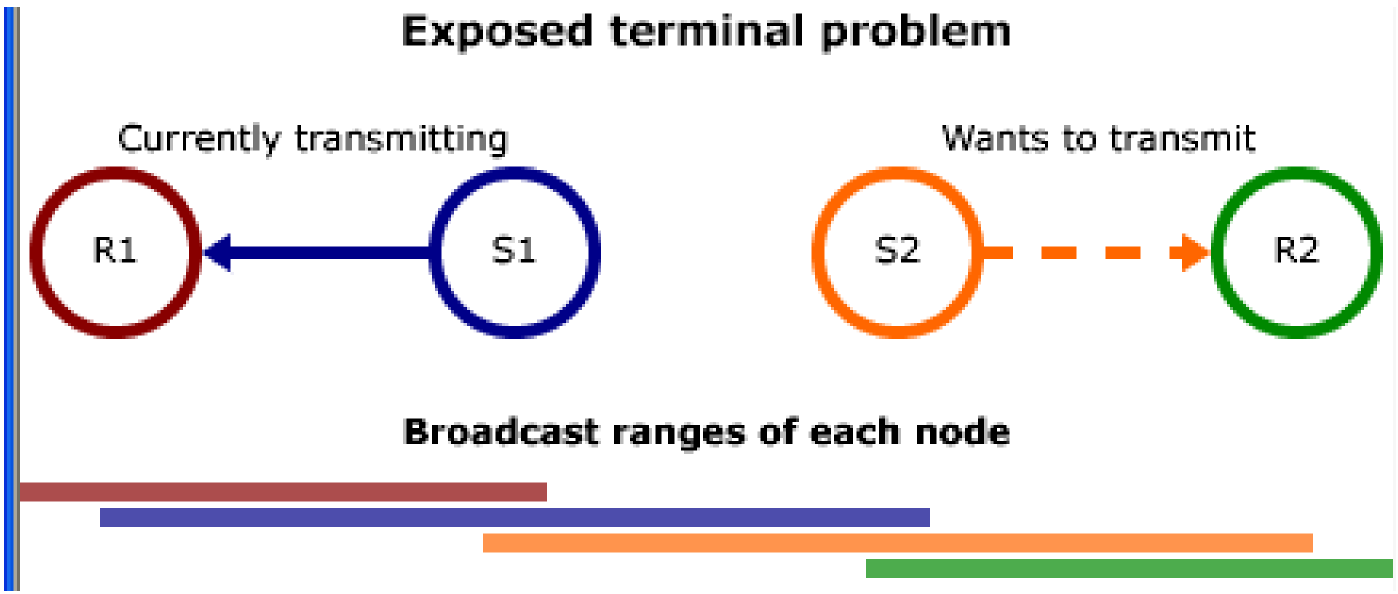
MACAW (Wireless)

- additional ACK

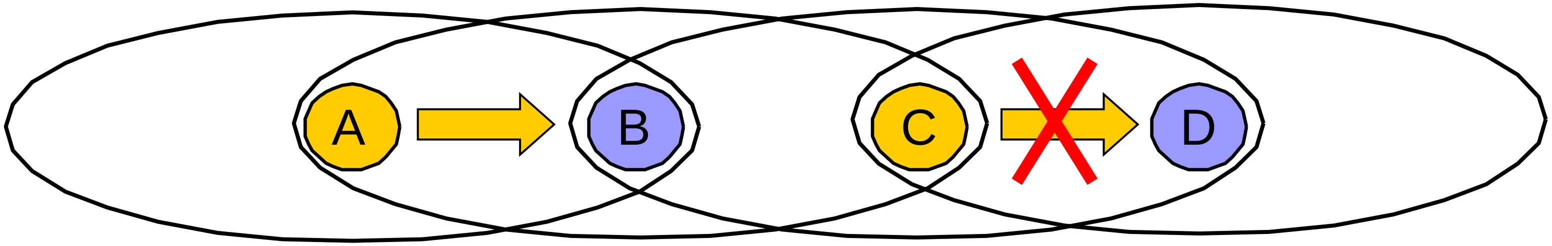


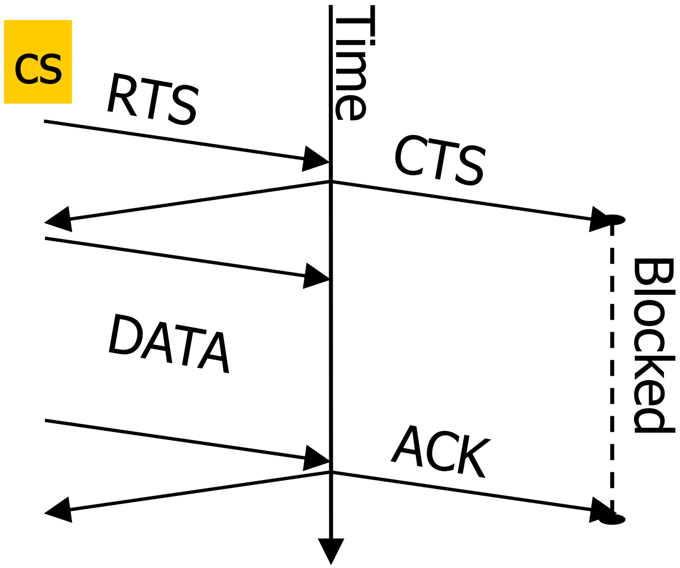
Exposed Terminal Problem

- A transmission between S1 and R1 is taking place.
- Node S2 is prevented from transmitting to R2.



Exposed Terminal Problem





Parallel CSMA transfers are synchronized by CSMA/CA

Collision avoidance can be too restrictive!

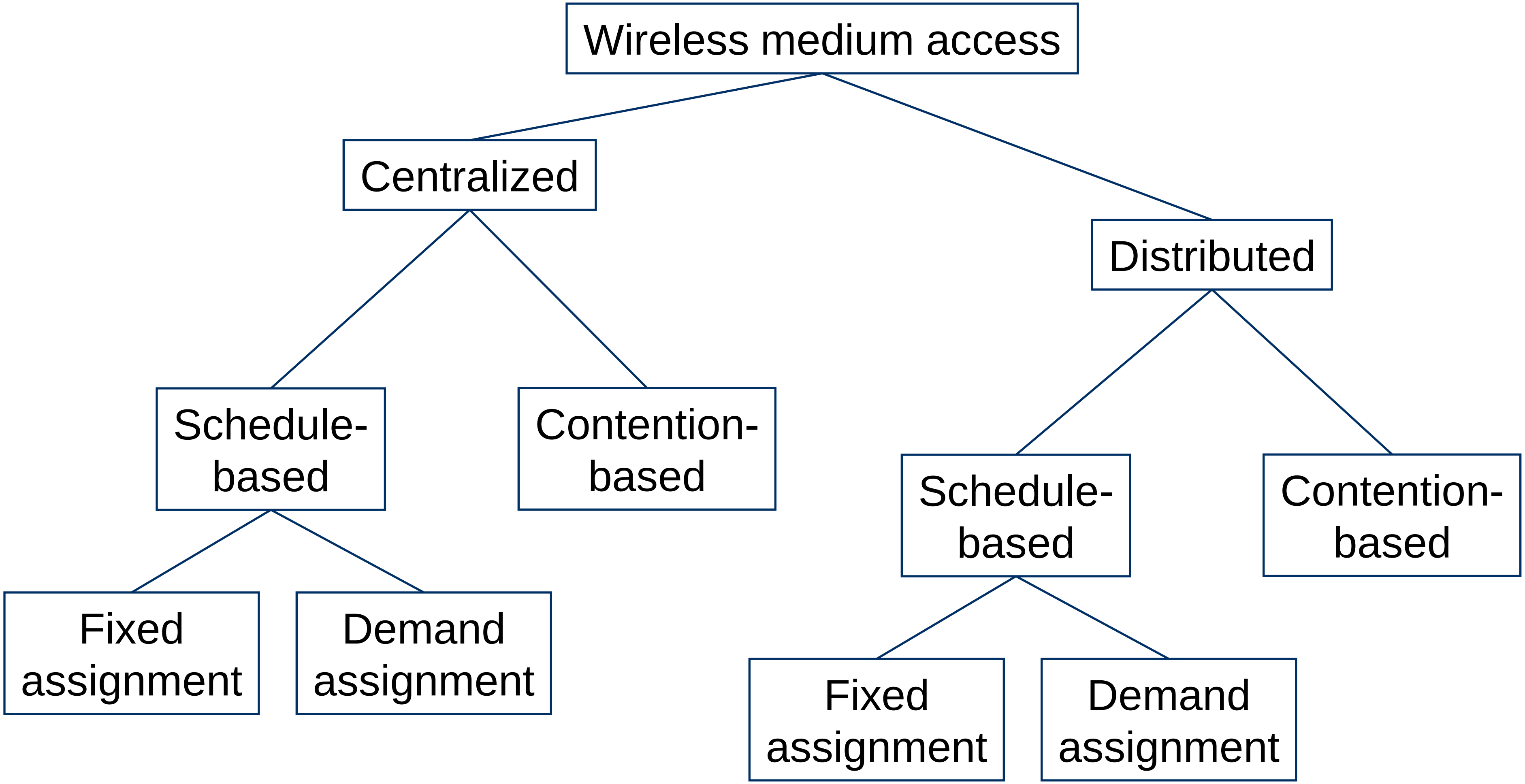
MAC (Medium Access Control) Protocols

- Specify how nodes in a network access the shared communication channel.

- Two basic types
  - contention-based
  - contention-free

- Desired Properties of a Sensor Net. MAC Protocol
  - distributed
  - contention-free (collision free)
  - self-stabilizing
  - not require common global time reference

Main options



Previous Works

- Contention-based (random access)
  - ALOHA
  - CSMA (Carrier Sense Multiple Access)
  - IEEE 802.11
- Contention-free
  - FDMA
  - TDMA
  - CDMA
- Multi-layered approach
  - ASCENT (nodes decide themselves to be on or off)
  - S-MAC (virtual clusters based on common sleep schedules)

Collision-based MAC Protocols

ALOHA :

- Packet radio networks
- Send when ready
- 18-35% channel utilization

CSMA (Carrier Sense Multiple Access):

- “listen before talk”
- 50-80% channel utilization

Centralized medium access

- Idea: Have a central station control when a node may access the medium
  - Example: Polling, centralized computation of TDMA schedules
  - Advantage: Simple, quite efficient (e.g., no collisions), burdens the central station

- Not directly feasible for non-trivial wireless network sizes
- But: Can be quite useful when network is somehow divided into smaller groups
  - Clusters, in each cluster medium access can be controlled centrally – compare Bluetooth piconets, for example

! Usually, distributed medium access is considered

Schedule- vs. contention-based MACs

- ***Schedule-based*** MAC
  - A ***schedule*** exists, regulating which participant may use which resource at which time (TDMA component)
  - Typical resource: frequency band in a given physical space (with a given code, CDMA)
  - Schedule can be ***fixed*** or computed ***on demand***
    - Usually: mixed – difference fixed/on demand is one of time scales
  - Usually, collisions, overhearing, idle listening no issues
  - Needed: time synchronization!
- ***Contention-based*** protocols
  - Risk of colliding packets is deliberately taken
  - Hope: coordination overhead can be saved, resulting in overall improved efficiency
  - Mechanisms to handle/reduce probability/impact of collisions required
  - Usually, ***randomization*** used somehow

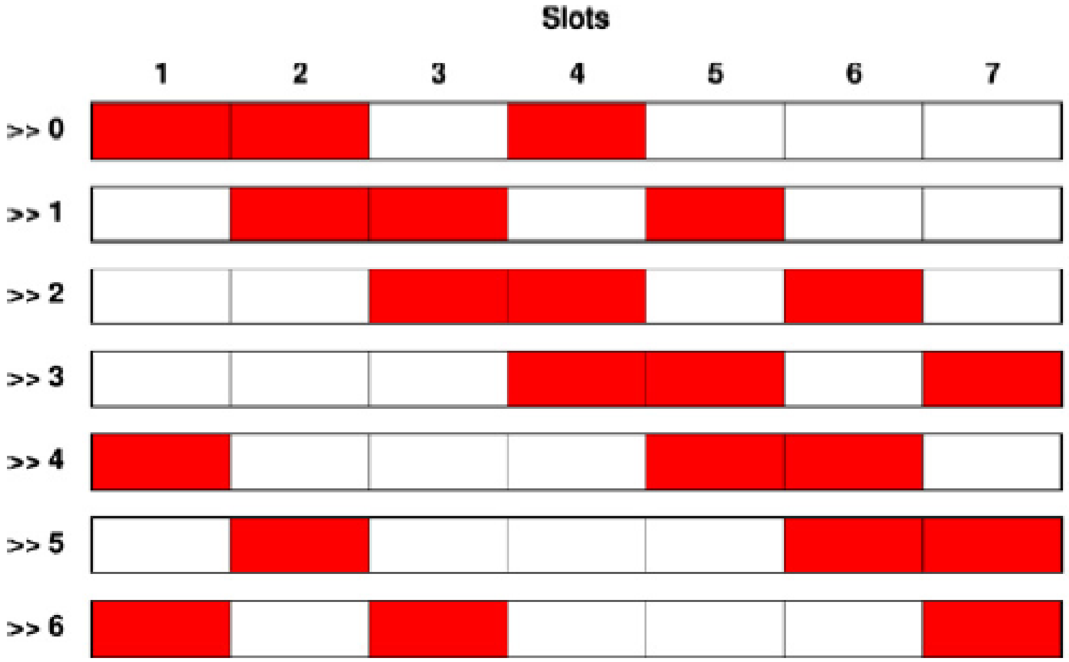
Slot-based Protocols

- Time is divided into periods each containing a certain number of fixed size lots.
- Nodes stay active in a certain predefined subset of the slots.
- In active period they send beacons announcing their schedule
- Activation schedules can be found such that any two neighbouring nodes eventually can hear each other's beacons.

Example

activation schedule: 1101000 (where 1s represent active slots and 0s represent inactive slots)

any two neighbours can hear each other (they have at least one overlapping active slot)



TDMA Protocols

- Schedule transmissions a priori so that any node exactly knows when it must turn on its radio and no collisions can ever result.
- All nodes can see each other and a master, starts a super frame providing synchronization timing for network operation.
- The super frame contains a sequence of slots that may be statically or dynamically allocated.

Overview

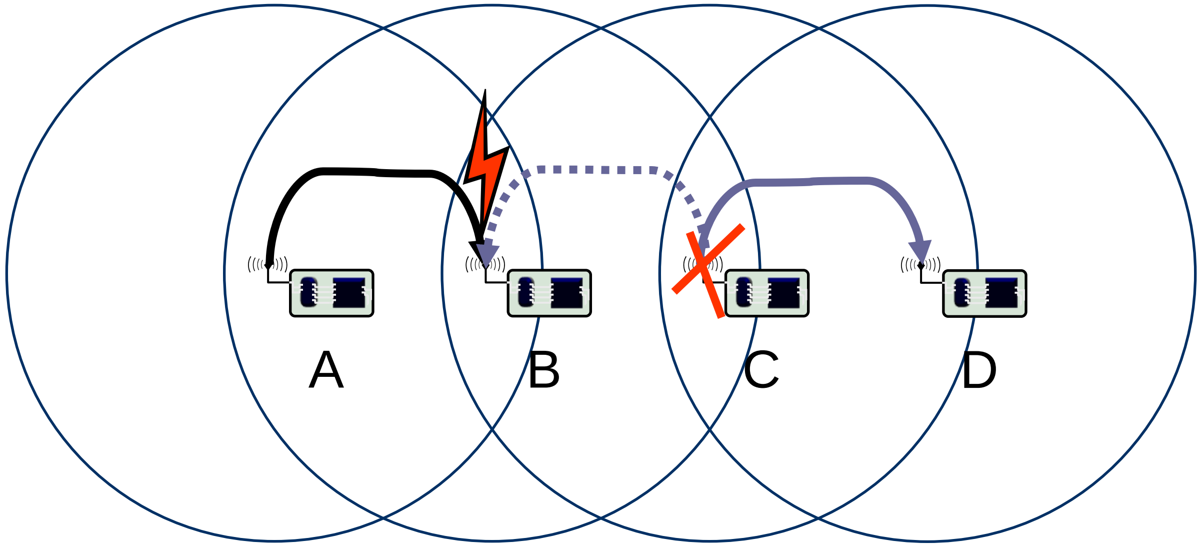
- Principal options and difficulties
- ***Contention-based protocols***
  - MACA
  - S-MAC, T-MAC
  - Preamble sampling, B-MAC
  - PAMAS
- Schedule-based protocols
- IEEE 802.15.4

Distributed, contention-based MAC

- Basic ideas for a distributed MAC
  - ALOHA – no good in most cases
  - Listen before talk ***(Carrier Sense Multiple Access, CSMA)* –** better, but suffers from ***sender*** not knowing what is going on at ***receiver***, might destroy packets despite first listening for a

! Receiver additionally needs some possibility to inform possible senders in its vicinity about impending transmission (to "shut them up" for this duration)

Hidden terminal scenario:



Also: recall exposed terminal scenario

Main options to shut up senders

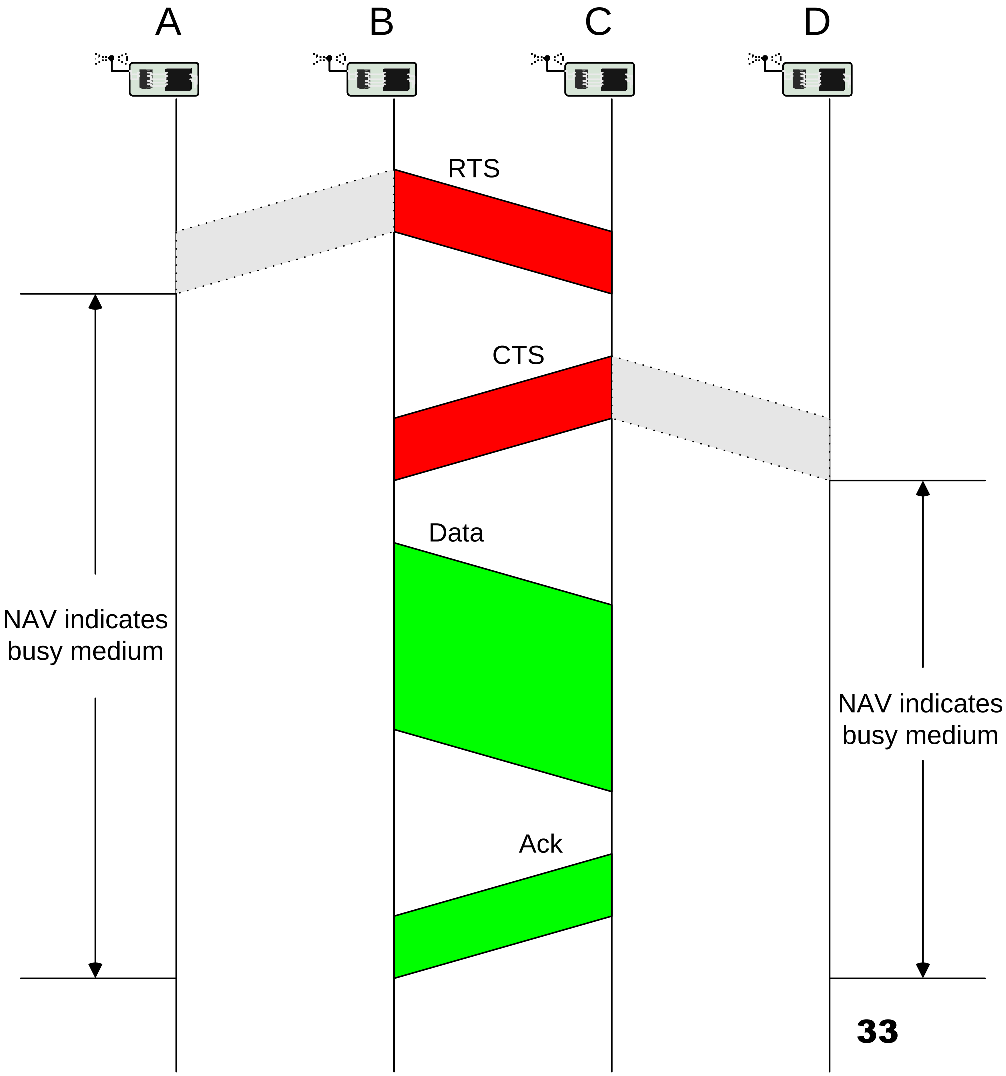
- Receiver informs potential interferers ***while*** a reception is on-going
  - By sending out a signal indicating just that
  - Problem: Cannot use same channel on which actual reception takes place

    ! Use separate channel for signaling
  - ***Busy tone*** protocol
- Receiver informs potential interferers ***before*** a reception is on-going
  - Can use same channel
  - Receiver itself needs to be informed, by sender, about impending transmission
  - Potential interferers need to be aware of such information, need to store it

Receiver informs interferers before transmission – MACA

- Sender B asks receiver C whether C is able to receive a transmission
  Request to Send (RTS)
- Receiver C agrees, sends out a ***Clear to Send*** (***CTS***)
- Potential interferers overhear either RTS or CTS and know about impending transmission and for how long it will last
  - Store this information in a ***Network Allocation Vector***
- B sends, C acks

! ***MACA protocol*** (used e.g. in ***IEEE 802.11***)



Part 2
Link layer protocols

Link layer tasks in general

- Framing – group bit sequence into packets/frames
  - Important: format, size
- Error control – make sure that the sent bits arrive and no other
  - Forward and backward error control
- Flow control – ensure that a fast sender does not overrun its slow(er) receiver
- Link management – discovery and manage links to neighbors
  - Do not use a neighbor at any cost, only if link is good enough

! Understand the issues involved in turning the radio communication between two neighboring nodes into a somewhat reliable ***link***

Overview

- ***Error control***
- Framing
- Link management

Error control

- Error control has to ensure that data transport is
  - Error-free – deliver exactly the sent bits/packets
  - In-sequence – deliver them in the original order
  - Duplicate-free – and at most once
  - Loss-free – and at least once
- Causes: fading, interference, loss of bit synchronization, …
  - Results in bit errors, bursty, sometimes heavy-tailed runs (see physical layer chapter)
  - In wireless, sometimes quite high average bit error rates – 10^{-2} … 10^{-4} possible!
- Approaches
  - Backward error control – ARQ
  - Forward error control – FEC

Backward error control – ARQ

- Basic procedure (a quick recap)
  - Put header information around the payload
  - Compute a checksum and add it to the packet
    - Typically: Cyclic redundancy check (CRC), quick, low overhead, low residual error rate
  - Provide feedback from receiver to sender
    - Send ***positive*** or ***negative acknowledgement***
  - Sender uses timer to detect that acknowledgements have not arrived
    - Assumes packet has not arrived
    - Optimal timer setting?
  - If sender infers that a packet has not been received correctly, sender can retransmit it
    - What is maximum number of retransmission attempts? If bounded, at best a semi-reliable protocols results

Standard ARQ protocols

- Alternating bit – at most one packet outstanding, single bit sequence number
- Go-back N – send up to N packets, if a packet has not been acknowledged when timer goes off, retransmit all unacknowledged packets
- Selective Repeat – when timer goes off, only send that particular packet

How to use acknowledgements

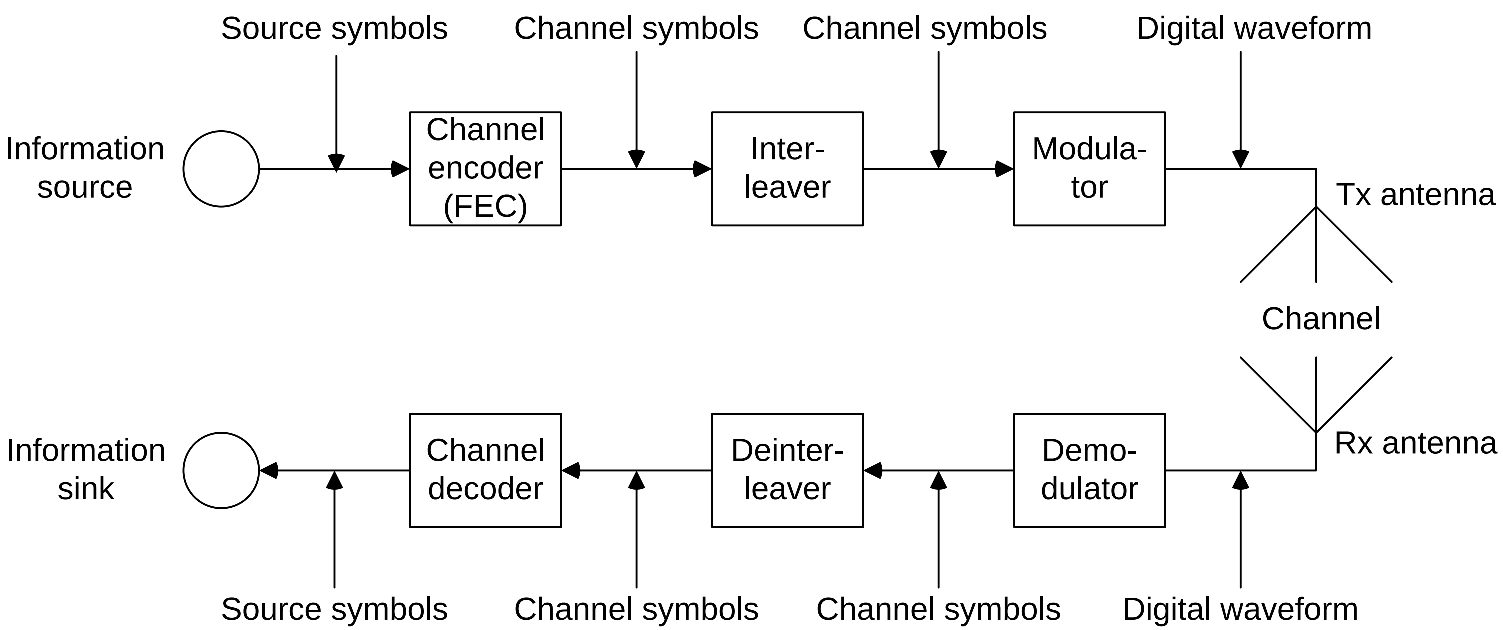
- Be careful about ACKs from different layers
  - A MAC ACK (e.g., S-MAC) does not necessarily imply buffer space in the link layer
  - On the other hand, having both MAC and link layer ACKs is a waste
- Do not (necessarily) acknowledge every packet – use cumulative ACKs
  - Tradeoff against buffer space
  - Tradeoff against number of negative ACKs to send

When to retransmit

- Assuming sender has decided to retransmit a packet – when to do so?
  - In a BSC channel, any time is as good as any
  - In fading channels, try to avoid bad channel states – postpone transmissions
  - Instead (e.g.): send a packet to another node if in queue (exploit multi-user diversity)
- How long to wait?
  - Example solution: Probing protocol
  - Idea: reflect channel state by two protocol modes, “normal” and “probing”
  - When error occurs, go from normal to probing mode
  - In probing mode, periodically send short packets (acknowledged by receiver) – when successful, go to normal mode

Forward error control

- **Idea: Endow symbols in a packet with additional redundancy to withstand a limited amount of random permutations**
  - Additionally: interleaving – change order of symbols to withstand burst errors



Block-coded FEC

- Level of redundancy: ***blocks of symbols***
  - Block: k p-ary source symbols (not necessarily just bits)
  - Encoded into n q-ary channel symbols
- Injective mapping (***code)*** of p^k source symbols ! q^n channel symbols
- ***Code rate***: (k ld p) / (n ld q)
  - When p=q=2: k/n is code rate
- For p=q=2: Hamming bound – code can correct up to t bit errors only if

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i}$$

  - Codes for (n,k,t) do not always exist

Popular block codes

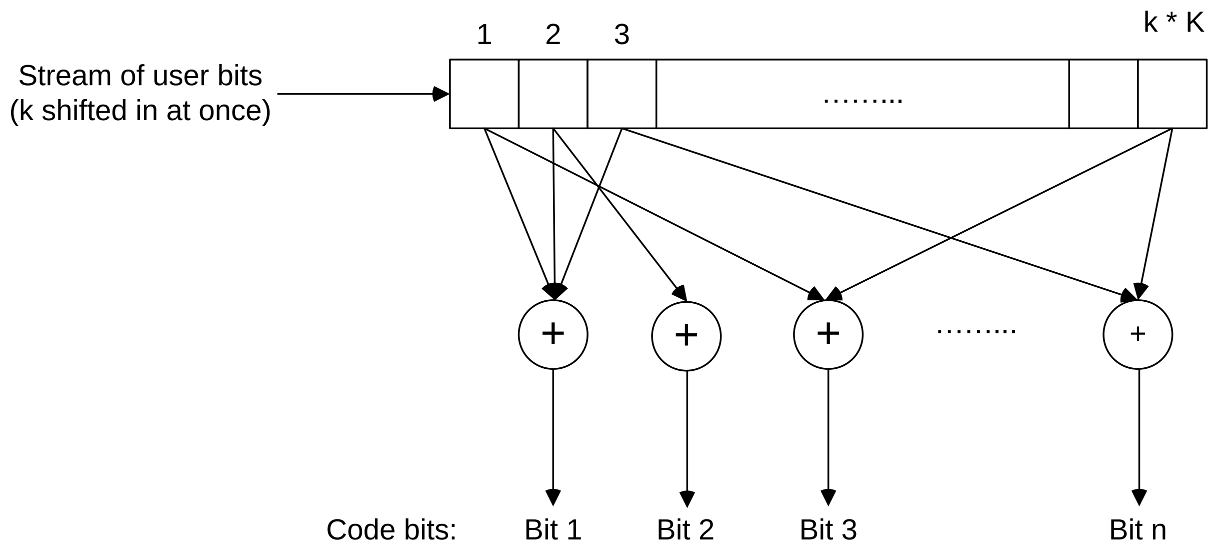
- Popular examples
  - Reed-Solomon codes (RS)
  - Bose-Chaudhuri-Hocquenghem codes (BCH)

- Energy consumption
  - E.g., BCH encoding: negligible overhead (linear-feedback shift register)
  - BCH decoding: depends on block length and Hamming distance (n, t as on last slide)

$$E_{\text{dec}} = (2nt + 2t^2) \cdot (E_{\text{add}} + E_{\text{mult}})$$

  - Similar for RS codes

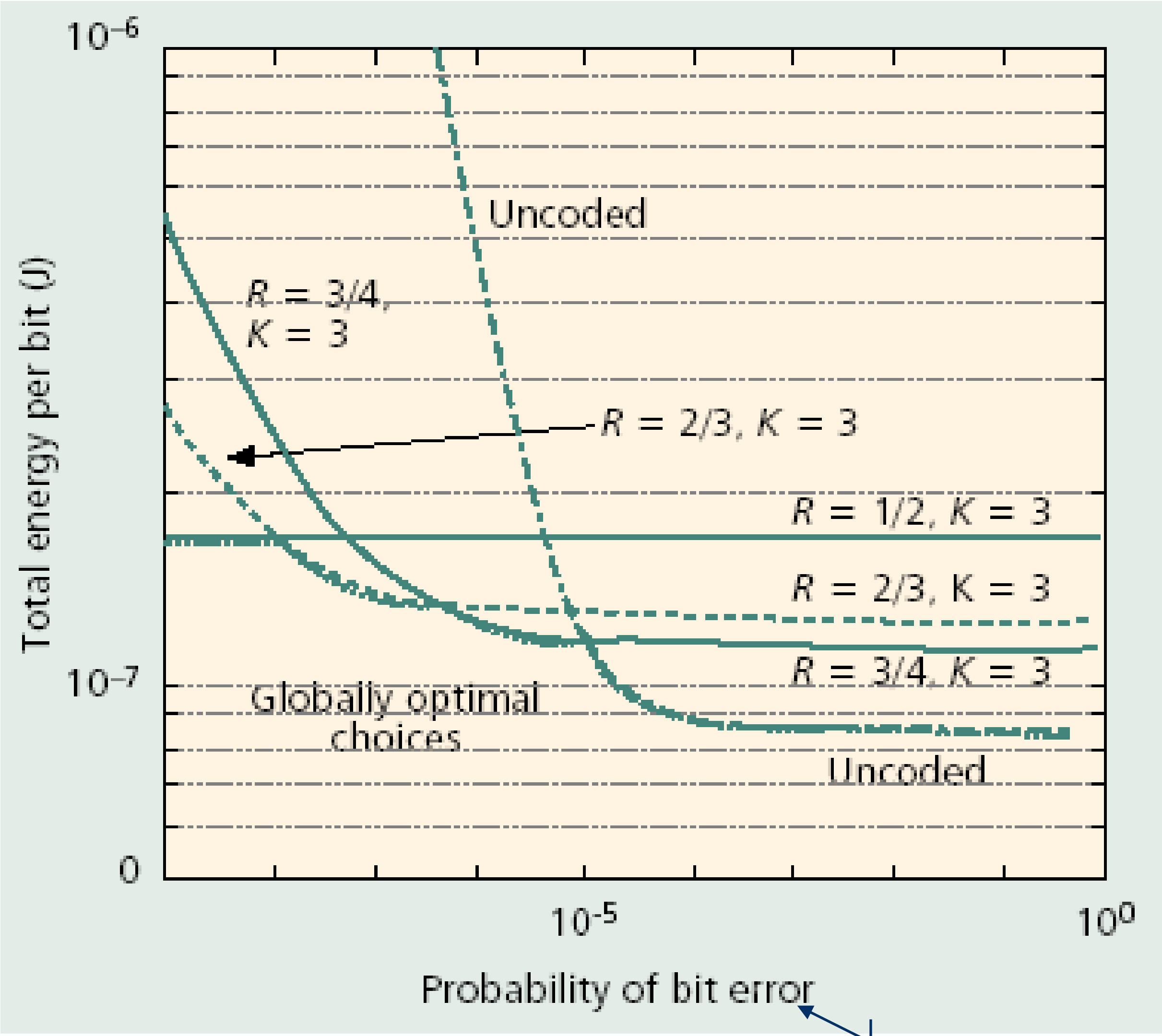
Convolutional codes



- Code rate: ratio of k user bits mapped onto n coded bits
- Constraint length K determines ***coding gain***
- Energy
  - Encoding: cheap
  - Decoding: Viterbi algorithm, energy & memory depends exponentially (!) on constraint length

Energy consumption of convolutional codes

- Tradeoff between coding energy and reduced transmission power (coding gain)
- Overall: block codes tend to be more energy-efficient

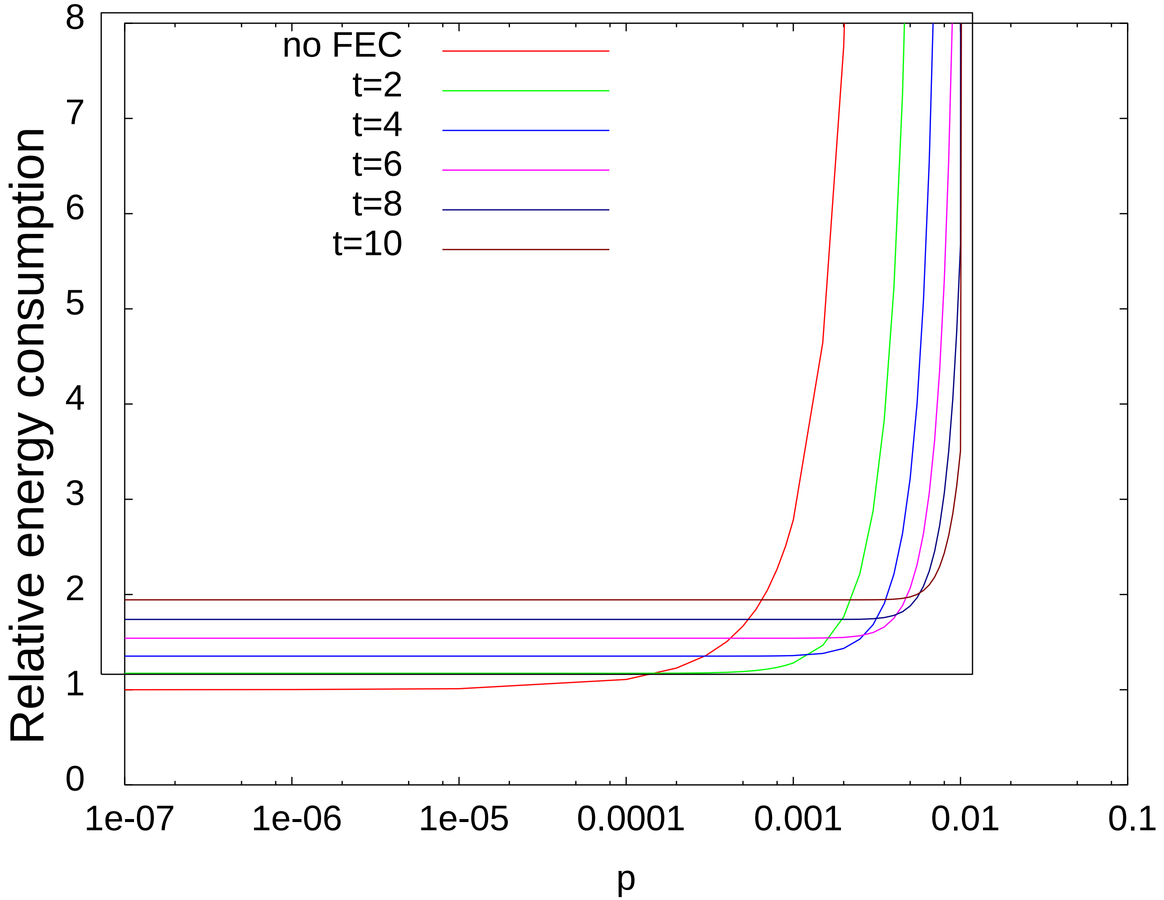


RESIDUAL bit error prob.!

Comparison: FEC vs. ARQ

- FEC
  - Constant overhead for each packet
  - Not (easily) possible to adapt to changing channel characteristics
- ARQ
  - Overhead only when errors occurred (expect for ACK, always needed)
- Both schemes have their uses ! ***hybrid schemes***

t: error correction capacity



BCH + unlimited number of retransmissions

Power control on a link level

- Further controllable parameter: transmission power
  - Higher power, lower error rates – less FEC/ARQ necessary
  - Lower power, higher error rates – higher FEC necessary
- Tradeoff!

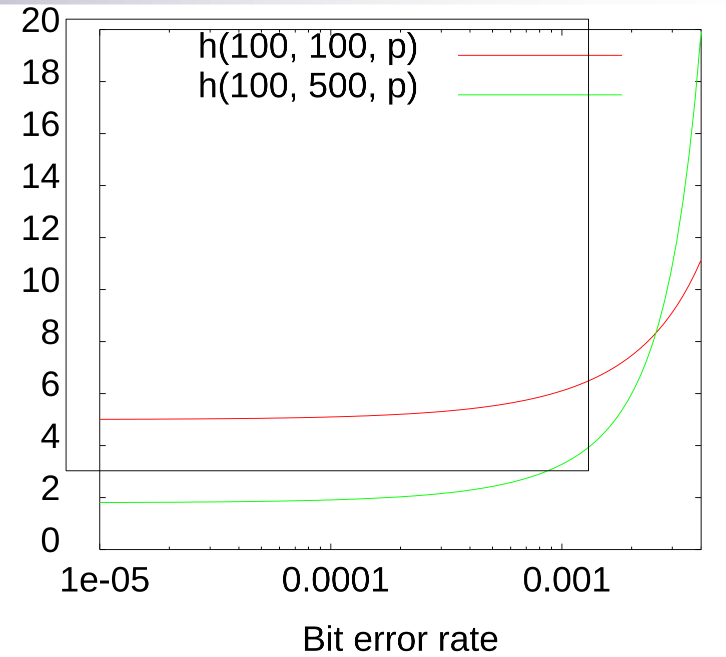
Overview

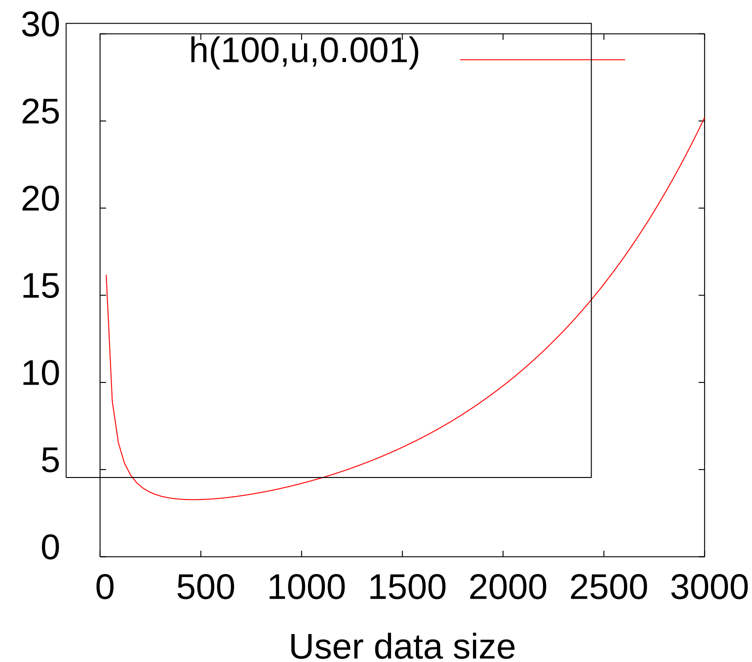
- Error control
- ***Framing***
- Link management

Frame, packet size

- Small packets: low packet error rate, high packetization overhead
- Large packets: high packet error rate, low overhead
- Depends on bit error rate, energy consumption per transmitted bit

- Notation: h(overhead, payload size, BER)



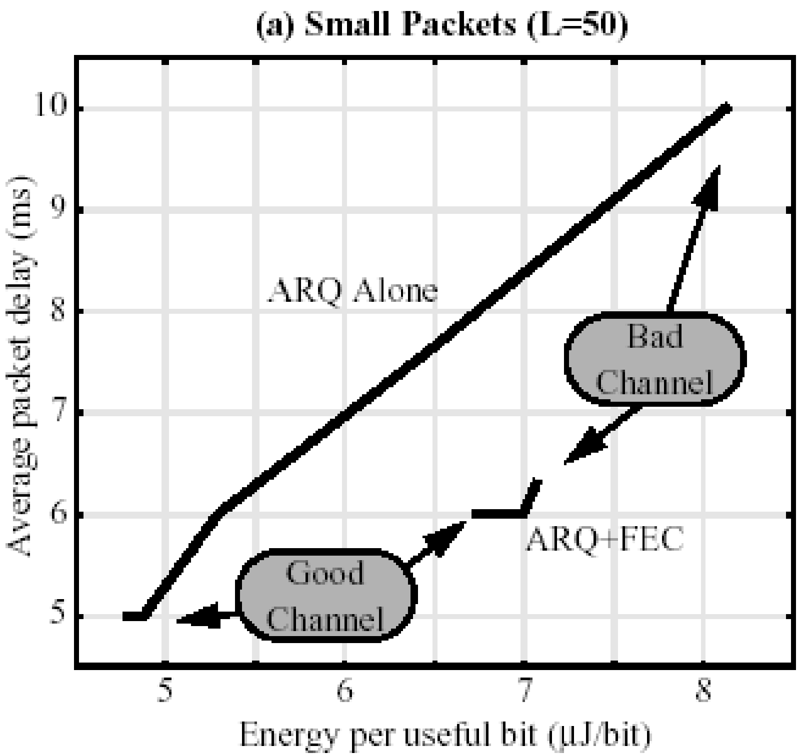


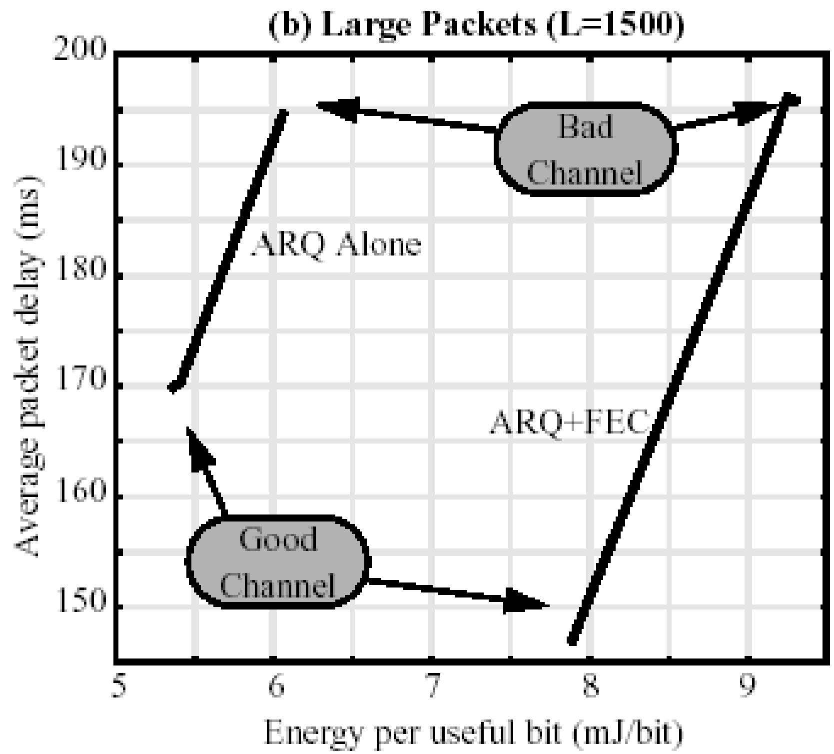
Dynamically adapt frame length

- For known bit error rate (BER), optimal frame length is easy to determine
- Problem: how to estimate BER?
  - Collect channel state information at the receiver (RSSI, FEC decoder information, …)
  - Example: Use number of attempts T required to transmit the last M packets as an estimator of the packet error rate (assuming a BSC)
    - Details: homework assignment
- Second problem: how long are observations valid/how should they be aged?
  - Only recent past is – if anything at all – somewhat credible

Putting it together: ARQ, FEC, frame length optimization

- Applying ARQ, FEC (both block and convolutional codes), frame length optimization to a Rayleigh fading channel
  - Channel modeled as Gilbert-Elliot





Overview

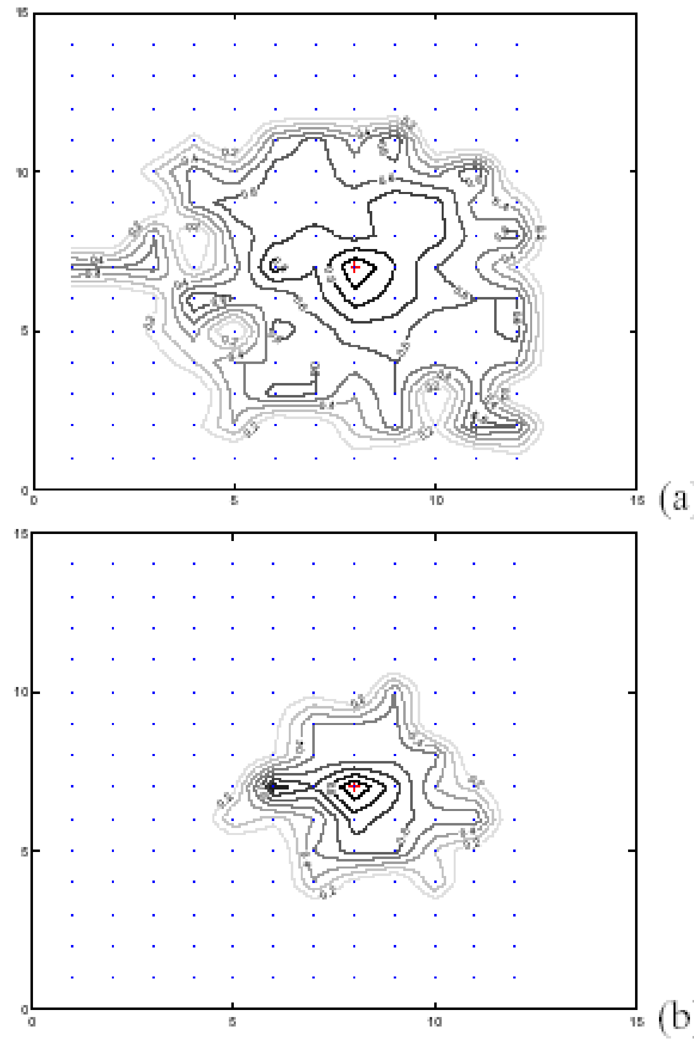
- Error control
- Framing
- ***Link management***

Link management

- Goal: decide to which neighbors that are *more or less* reachable a link should be established
  - Problem: communication quality fluctuates, far away neighbors can be costly to talk to, error-prone, quality can only be estimated
- Establish a ***neighborhood table*** for each node
  - Partially automatically constructed by MAC protocols

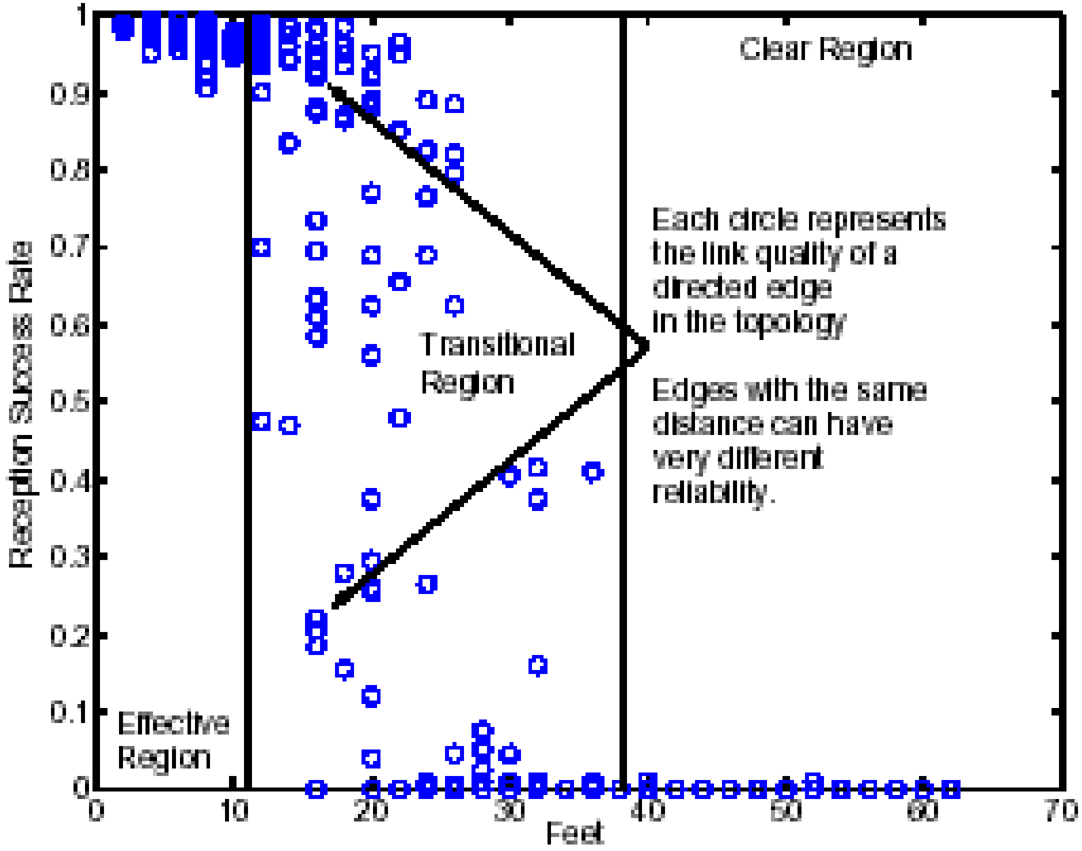
Link quality characteristics

- Expected: simple, circular shape of "region of communication" – not realistic
- Instead:
  - Correlation between distance and loss rate is weak; iso-loss-lines are not circular but irregular
  - Asymmetric links are relatively frequent (up to 15%)
  - Significant short-term PER variations even for stationary nodes



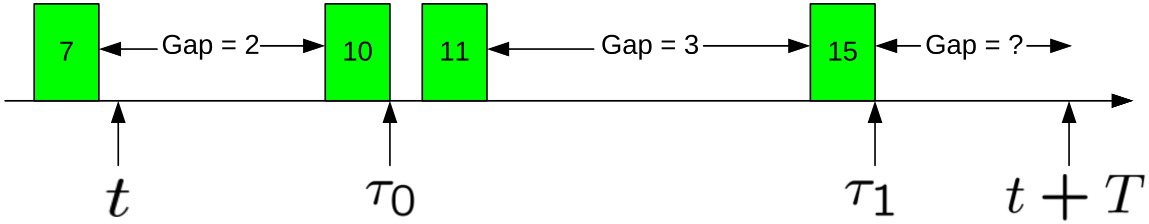
Three regions of communication

- ***Effective region***: PER consistently < 10%
- ***Transitional region:*** anything in between, with large variation for nodes at same distance
- ***Poor region***: PER well beyond 90%



Link quality estimation

- How to estimate, on-line, in the field, the actual link quality?
- Requirements
  - Precision – estimator should give the statistically correct result
  - Agility – estimator should react quickly to changes
  - Stability – estimator should not be influenced by short aberrations
  - Efficiency – Active or passive estimator



- Example: WMEWMA only estimates at fixed intervals

$$P_n = \alpha P_{n-1} + (1-\alpha)\frac{r_n}{r_n + f_n}$$

r_n: received packets in interval

f_n: packets identified as lost

Conclusion

- Link layer combines traditional mechanisms
  - Framing, packet synchronization, flow control

with relatively specific issues

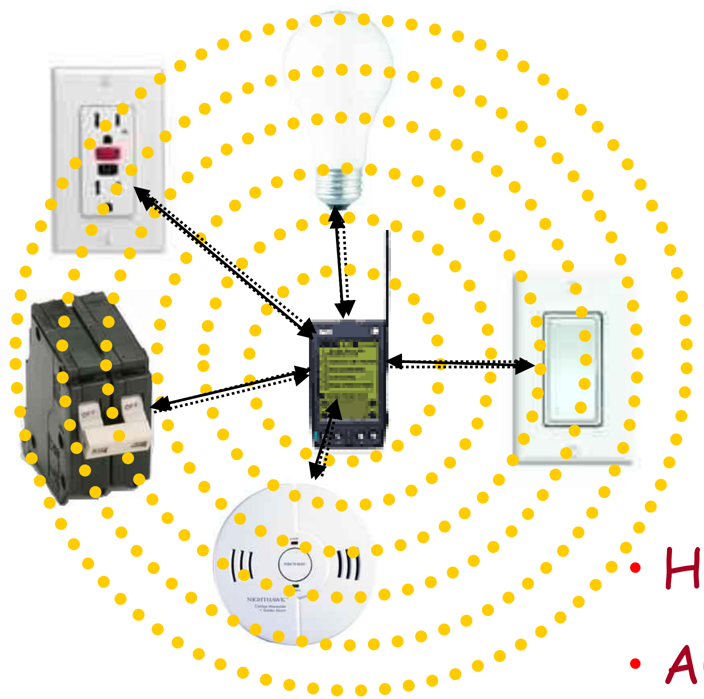
  - Careful choice of error control mechanisms – tradeoffs between FEC & ARQ & transmission power & packet size …
  - Link estimation and characterization

Part 3
IEEE 802.15.4
Standard

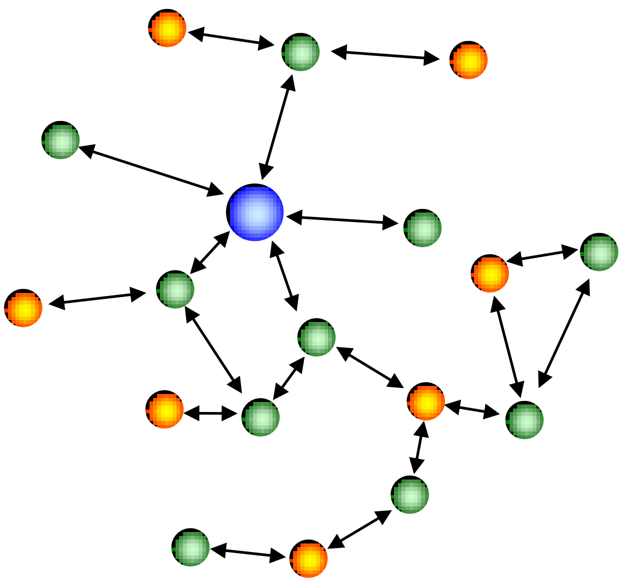
IEEE 802.15.4 Low-Rate Wireless Personal Area Networks (LR-WPAN)

- The main objectives:
  - ease of installation,
  - reliable data transfer,
  - short-range operation,
  - extremely low cost,
  - reasonable battery life,
  - maintaining a simple and flexible protocol.

802.15.4 Applications Space

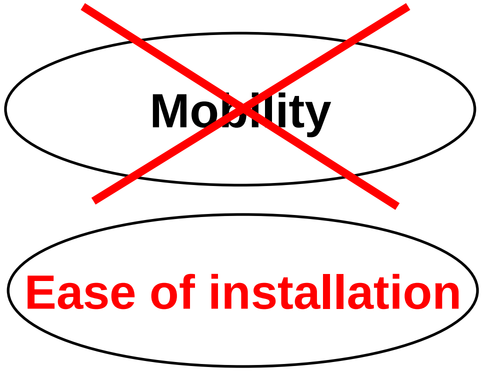


- Home Networking
- Automotive Networks
- Industrial Networks
- Interactive Toys
- Remote Metering



802.15.4 Applications Topology

- Cable replacement - Last meter connectivity
- Virtual Wire
- Wireless Hub
- Stick-On Sensor



Some Needs in The Sensor Networks

Thousands of sensors in a small space → **Wireless**

but wireless implies **Low Power**!

and low power implies **Limited Range.**

Of course all of these is viable if a **Low Cost** transceiver is required

Characteristics of an LR-WPAN

- Over-the-air data rates of 250 kb/s, 100kb/s, 40 kb/s, and 20 kb/s
- Star or peer-to-peer operation
- Allocated 16-bit short or 64-bit extended addresses
- Optional allocation of guaranteed time slots (GTSs)
- Carrier sense multiple access with collision avoidance (CSMA-CA) channel access
- Fully acknowledged protocol for transfer reliability
- Low power consumption
- Energy Detection (ED)
- Link Quality Indication (LQI)
- 16 channels in the 2450 MHz band, 30 channels in the 915 MHz band, and 3 channels in the 868 MHz band

Different Device Types of IEEE 802.15.4

- Two different device types:
  - a Full-Function Device (FFD)
  - Reduced-Function Device (RFD).
- The FFD can operate in three modes:
  - Personal Area Network (PAN) coordinator,
  - A coordinator,
  - A device.
- An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD.
- An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor;
  - No need to send large amounts of data and may only associate with a single FFD at a time.
  - The RFD can be implemented using minimal resources and memory capacity.

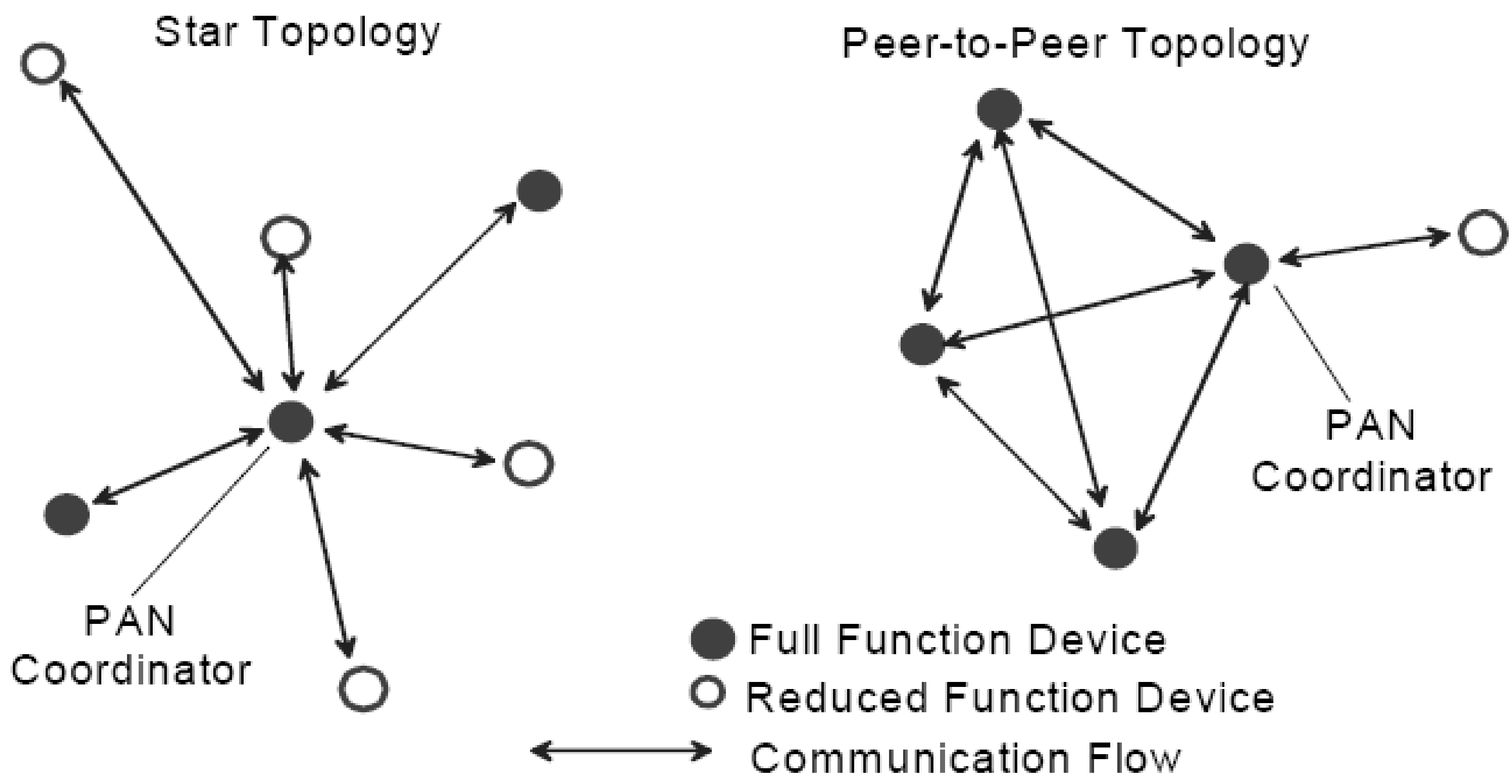
IEEE 802.15.4 Device Classes

- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

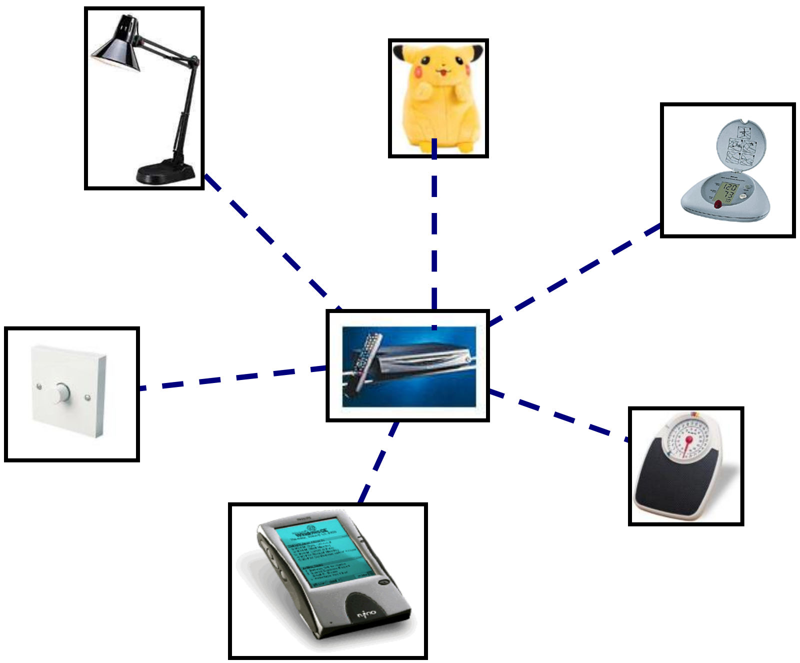
Network Topologies

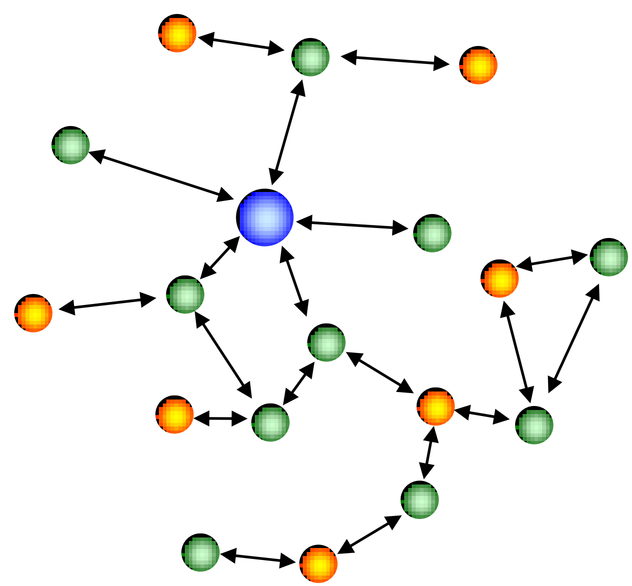
- Depending on the application requirements, an IEEE 802.15.4 LR-WPAN may operate in either of two topologies:
  - Star topology
  - Peer-to-peer topology.
- All devices operating on a network of either topology shall have unique 64- bit addresses.

Network Topologies



Typical Network Topologies





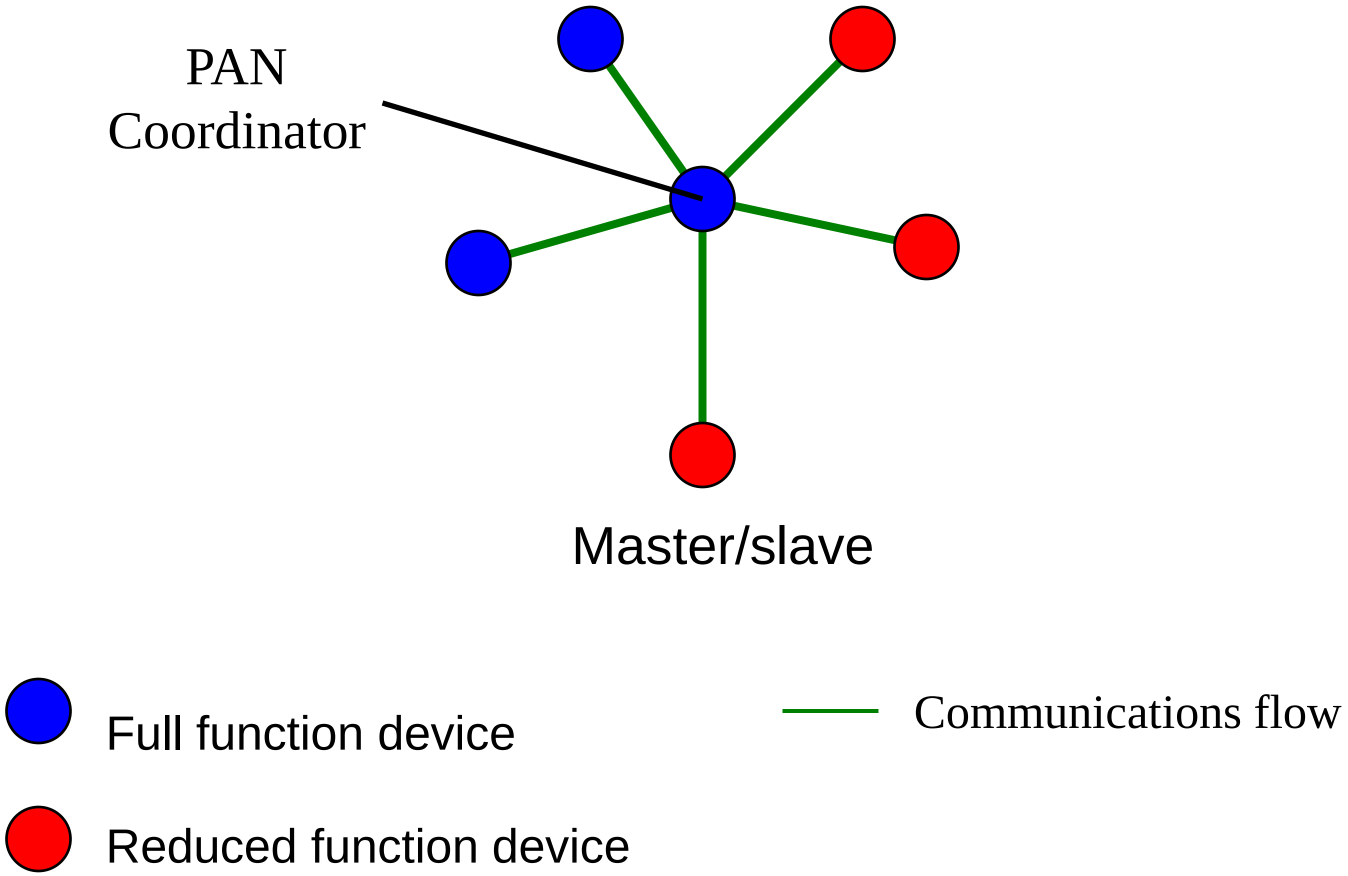
Star Topology

- Communication is established between devices and the PAN coordinator.
- A PAN coordinator can be used to initiate, terminate, or route communication around the network.
- The PAN coordinator might often be mains powered.
- Applications :
  - home automation,
  - personal computer (PC) peripherals,
  - toys and games,
  - personal health care.

Star Network Formation

- After an FFD is activated, it can establish its own network and become the PAN coordinator.
- All star networks operate independently from all other star networks currently in operation.
- The PAN coordinator allows other devices, potentially both FFDs and RFDs, to join its network

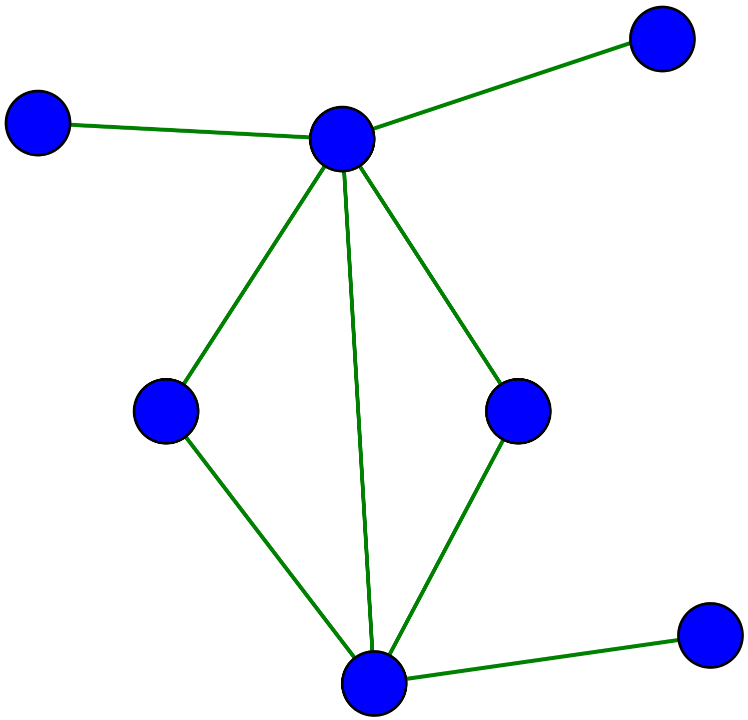
IEEE 802.15.4 MAC Overview Star Topology



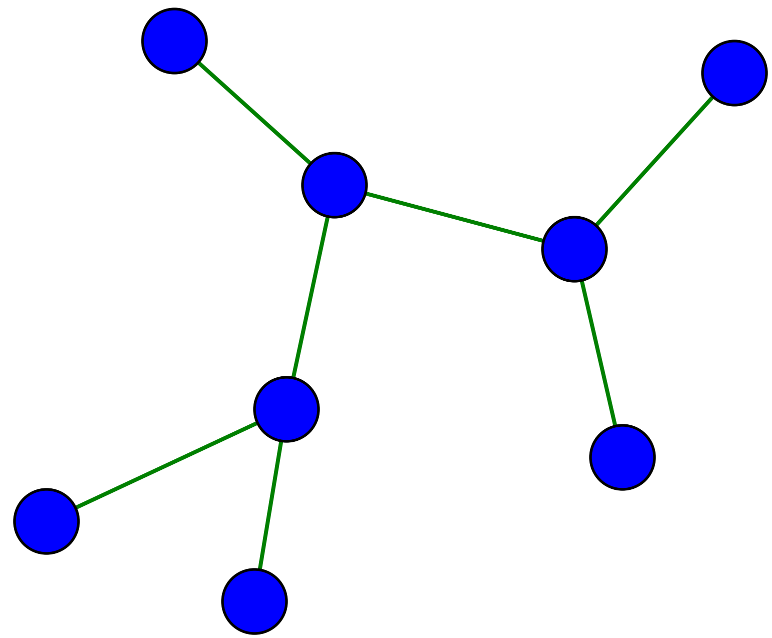
Peer-to-peer Topology

- Any device may communicate with any other device as long as they are in range of one another.
- One device is nominated as the PAN coordinator
- It allows more complex network formations
  - Mesh network
- It can be ad hoc, self-organizing, and self-healing.
- It may also allow multiple hops to route messages from any device to any other device on the network.
- Applications:
  - industrial control and monitoring,
  - wireless sensor networks,
  - asset and inventory tracking,
  - intelligent agriculture,

IEEE 802.15.4 MAC Overview
Peer-Peer Topology



Point to point



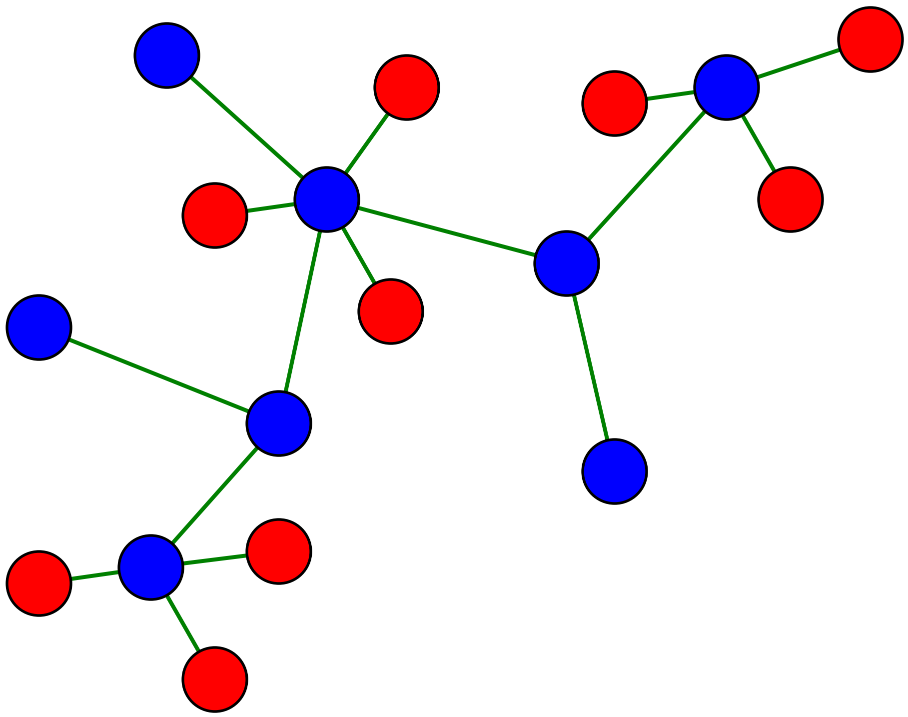
Cluster tree

Full function device

Communications flow

IEEE 802.15.4 MAC Overview

Combined Topology



Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

Full function device

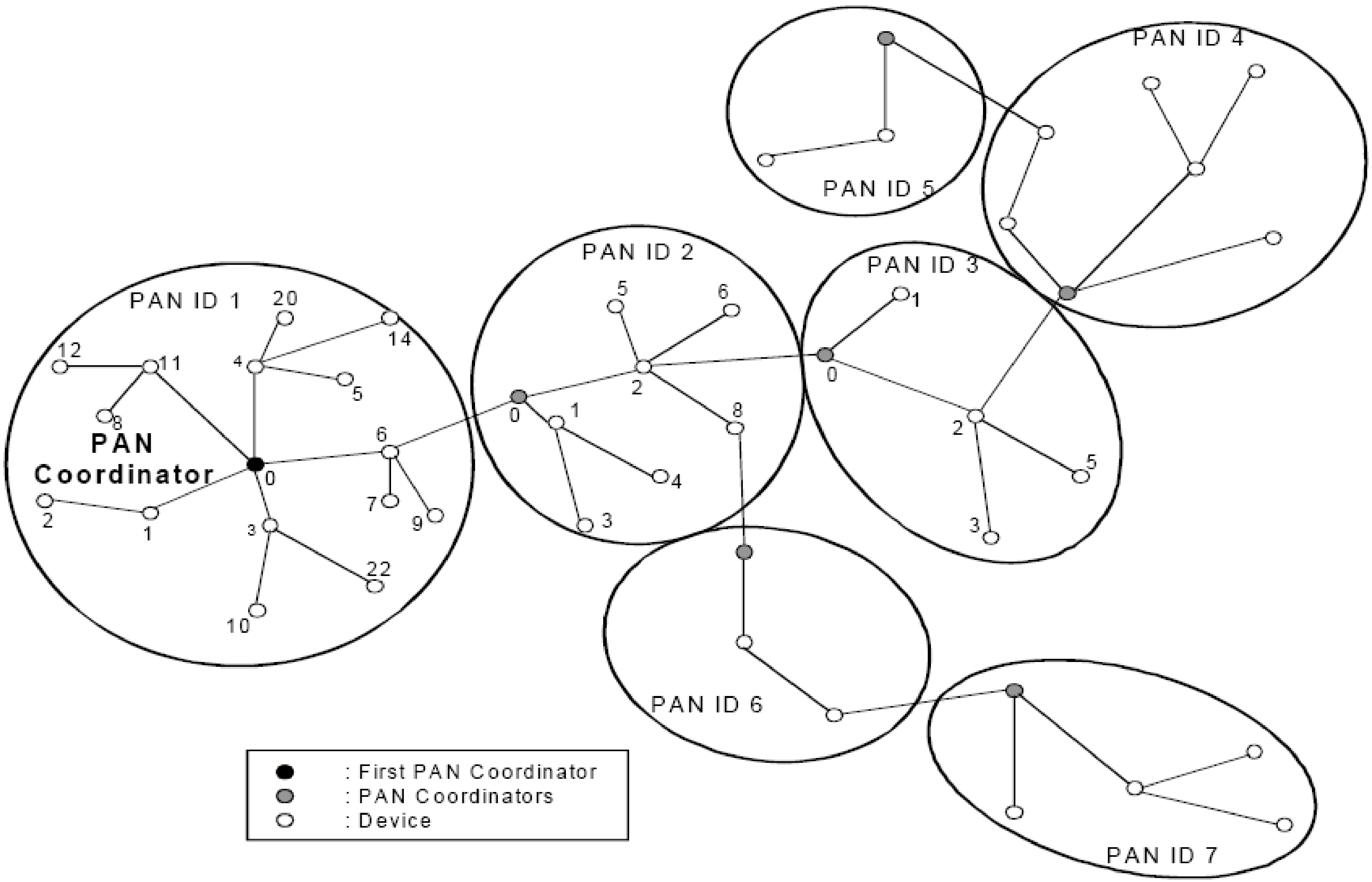
Reduced function device

Communications flow

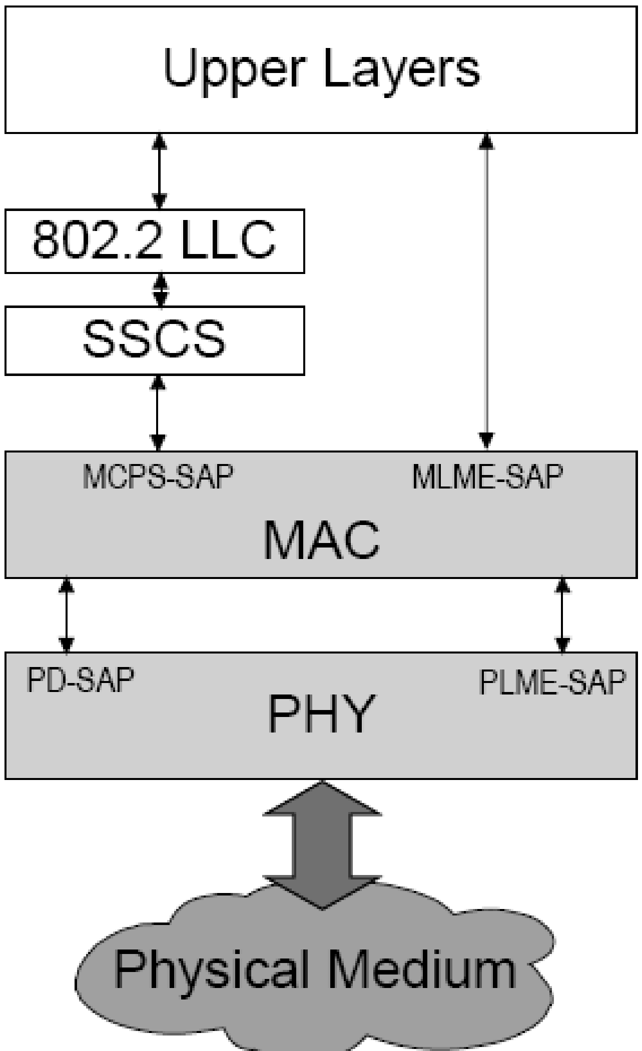
Cluster Tree Topology

- An example of peer-to-peer communications topology
- Most devices are FFDs.
- An RFD connects to a cluster tree network as a leaf device at the end of a branch.
- The PAN coordinator forms the first cluster by choosing an unused PAN identifier and broadcasting beacon frames to neighboring devices.
- A candidate device receiving a beacon frame may request to join the network at the PAN coordinator.
- If the PAN coordinator permits the device to join, it adds the new device as a child device in its neighbor list.

Cluster Tree Network



Layer Architecture



- The upper layers:
  - Network layer
    - Network configuration
    - Manipulation
    - Message routing
  - Application layer
    - Provides the intended function of the device.
- Logical Link Control (LLC) can access the MAC sub layer through the Service-Specific Convergence Sub layer (SSCS)

Physical Layer (PHY)

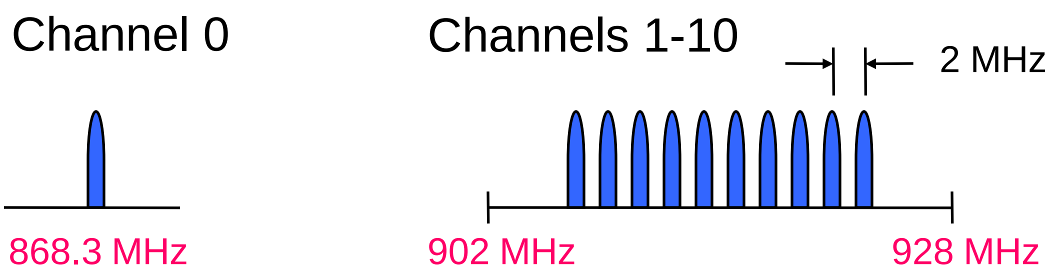
- Provides two services:
  - PHY data service
  - PHY management service
- The features of the PHY:
  - Activation and deactivation of the radio transceiver
  - Energy Detection (ED)
  - Link Quality Indication (LQI)
  - Channel selection
  - Clear Channel Assessment (CCA)
  - Transmitting and receiving packets across the physical medium

Unlicensed Frequency Bands

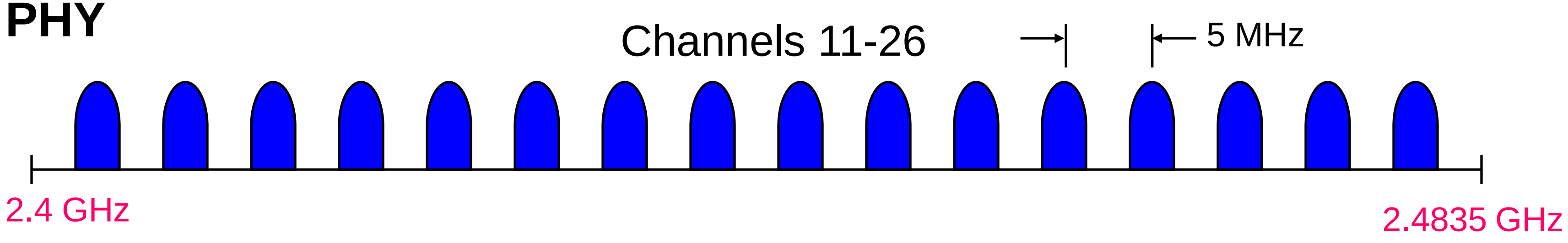
- 868–868.6 MHz (e.g., Europe)
- 902–928 MHz (e.g., North America)
- 2400–2483.5 MHz (Worldwide)

IEEE 802.15.4 PHY Overview Operating Frequency Bands

868MHz / 915MHz PHY



2.4 GHz PHY



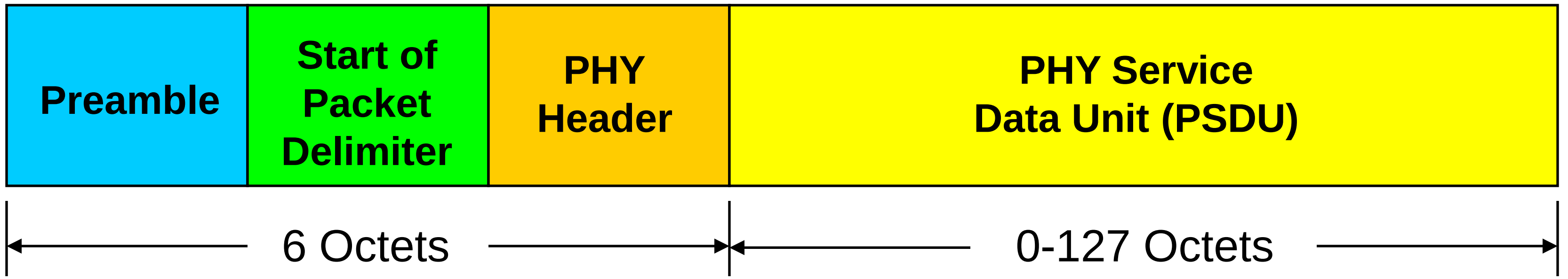
Frequency Bands and Data Rates

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

IEEE 802.15.4 PHY Overview Packet Structure

PHY Packet Fields

- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field



IEEE 802.15.4 PHY Overview Modulation/Spreading

2.4 GHz PHY

- 250 kb/s (4 bits/symbol, 62.5 kBaud)
- Data modulation is 16-ary orthogonal modulation
- 16 symbols are ~orthogonal set of 32-chip PN codes
- Chip modulation is MSK at 2.0 Mchips/s

868MHz/915MHz PHY

- Symbol Rate
  - 868 MHz Band: 20 kb/s (1 bit/symbol, 20 kBaud)
  - 915 MHz Band: 40 kb/s (1 bit/symbol, 40 kBaud)
- Data modulation is BPSK with differential encoding
- Spreading code is a 15-chip m-sequence
- Chip modulation is BPSK at
  - 868 MHz Band: 300 kchips/s
  - 915 MHz Band: 600 kchips/s

IEEE 802.15.4 PHY Overview Common Parameters

Transmit Power
- Capable of at least 1 mW

Transmit Center Frequency Tolerance
- ± 40 ppm

Receiver Sensitivity (Packet Error Rate <1%)
- -85 dBm @ 2.4 GHz band
- -92 dBm @ 868/915 MHz band

RSSI Measurements
- Packet strength indication
- Clear channel assessment
- Dynamic channel selection

IEEE 802.15.4 PHY Overview PHY Primitives

PHY Data Service

- PD-DATA – exchange data packets between MAC and PHY

PHY Management Service

- PLME-CCA – clear channel assessment
- PLME-ED - energy detection
- PLME-GET / -SET– retrieve/set PHY PIB parameters
- PLME-TRX-ENABLE – enable/disable transceiver

IEEE 802.15.4 MAC Overview Design Drivers

- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

Simple but flexible protocol

IEEE 802.15.4 MAC Overview Addressing

- All devices have IEEE addresses
- Short addresses can be allocated
- Addressing modes:
  - Network + device identifier (star)
  - Source/destination identifier (peer-peer)

MAC Sublayer

- Provides two services:
  - MAC data service
  - MAC management service
- The features of the MAC sublayer:
  - Beacon management,
  - Channel access,
  - Guaranteed Time Slot (GTS) management,
  - Frame validation,
  - Acknowledged frame delivery,
  - Association, and disassociation.

CSMA-CA Mechanism

- Two types of channel access mechanism, depending on the network configuration.
  - Nonbeacon-enabled PANs
    - Use an unslotted CSMA-CA channel access mechanism,
  - Beacon-enabled PANs
    - Use a slotted CSMA-CA channel access mechanism,

Unslotted **CSMA-CA Mechanism**

- Each time a device wishes to transmit data frames or MAC commands, it waits for a random period.
- If the channel is found to be idle the device transmits its data.
- If the channel is found to be busy, the device waits for another random period.
- Acknowledgment frames are sent without using a CSMA-CA mechanism.

Slotted **CSMA-CA Mechanism**

- Backoff slots are aligned with the start of the beacon transmission.
- Each time a device wishes to transmit data, it locates the boundary of the next backoff slot and then waits for a random number of backoff slots.
- If the channel is busy, the device waits for another random number of backoff slots
- If the channel is idle, the device begins transmitting on the next available backoff slot boundary.
- Acknowledgment and beacon frames are sent without using a CSMA-CA mechanism.

Frame Acknowledgment

- A successful reception and validation of a data or MAC command frame can be optionally confirmed with an acknowledgment.
- If the originator does not receive an acknowledgment after some period
  - It assumes that the transmission was unsuccessful and retries the frame transmission.
- If an acknowledgment is still not received after several retries:
  - The originator can choose either to terminate the transaction or to try again.
- When the acknowledgment is not required, the originator assumes the transmission was successful.

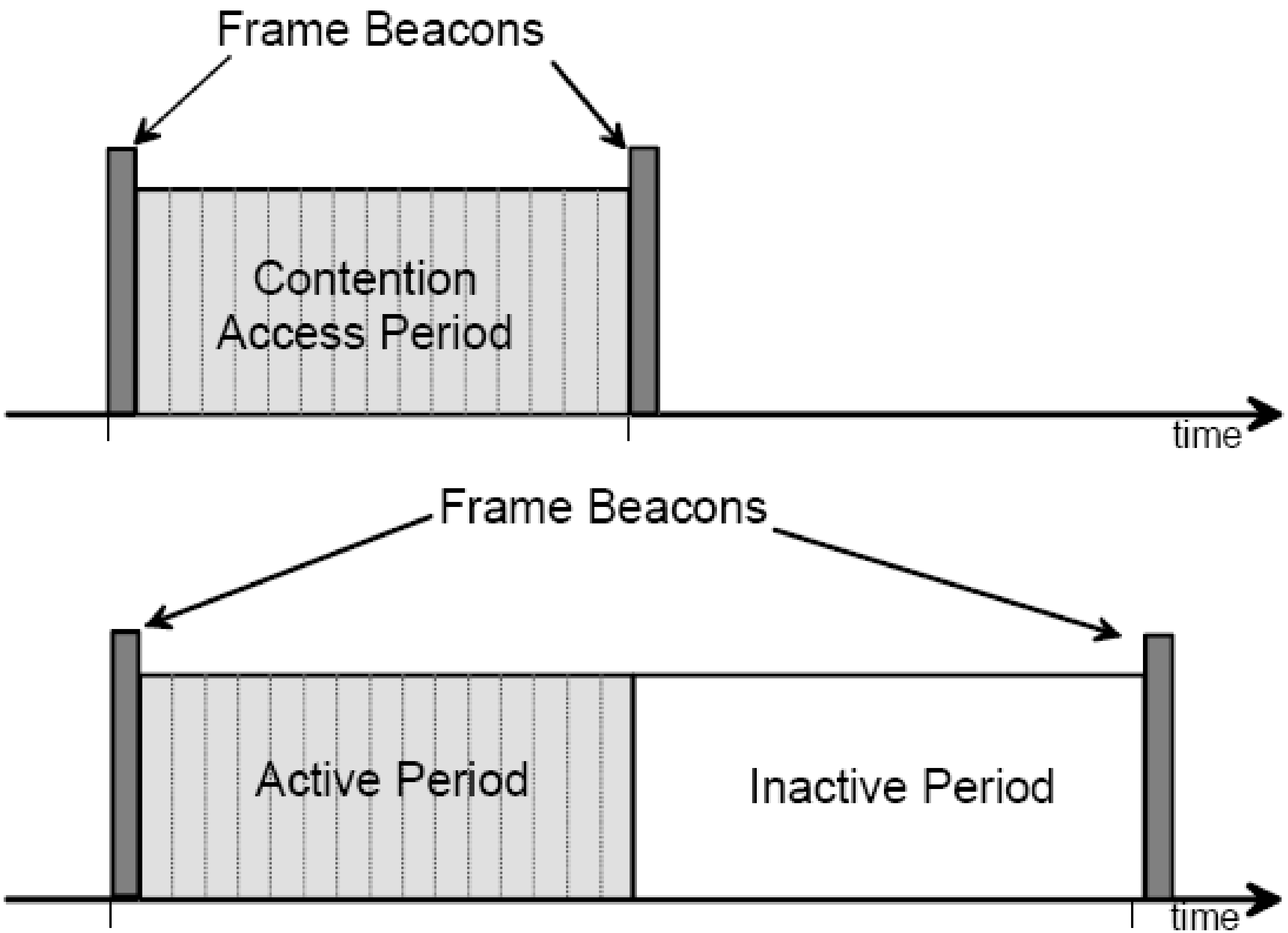
Super Frame Structure Without GTSs

- The format of the super frame is defined by the coordinator.
- The super frame is bounded by network beacons sent by the coordinator
- It is divided into 16 equally sized slots.
  - The beacon frame is transmitted in the first slot of each super frame
- Optionally, the super frame can have an active and an inactive portion
  - During the inactive portion, the coordinator may enter a low-power mode.
- If a coordinator does not wish to use a super frame structure, it will turn off the beacon transmissions.

Beacons

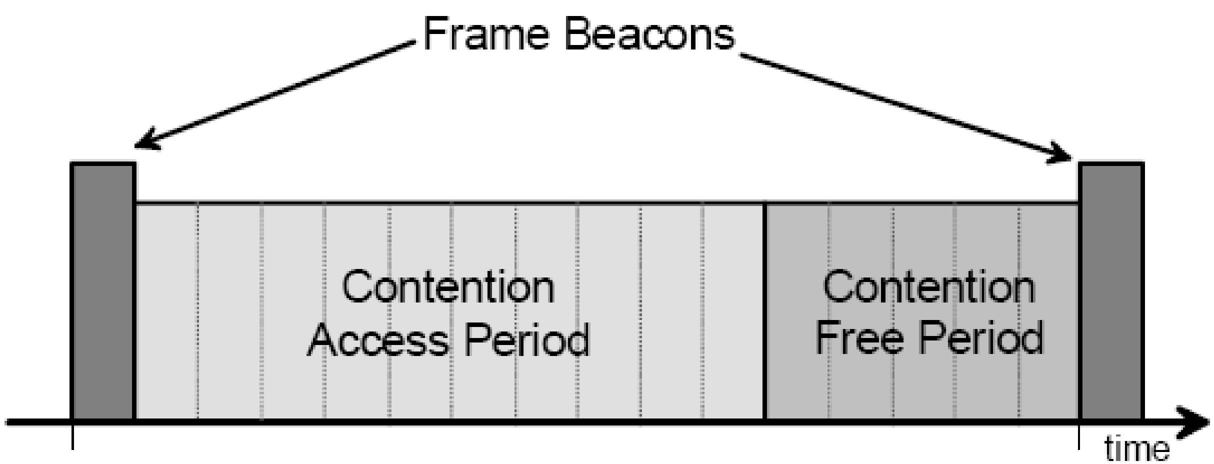
- The beacons are used:
  - To synchronize the attached devices
  - To identify the PAN
  - To describe the structure of the super frames
- Any device wishing to communicate during the Contention Access Period (CAP) between two beacons competes with other devices
- All transactions are completed by the time of the next network beacon.

Super Frame Structure Without GTSs

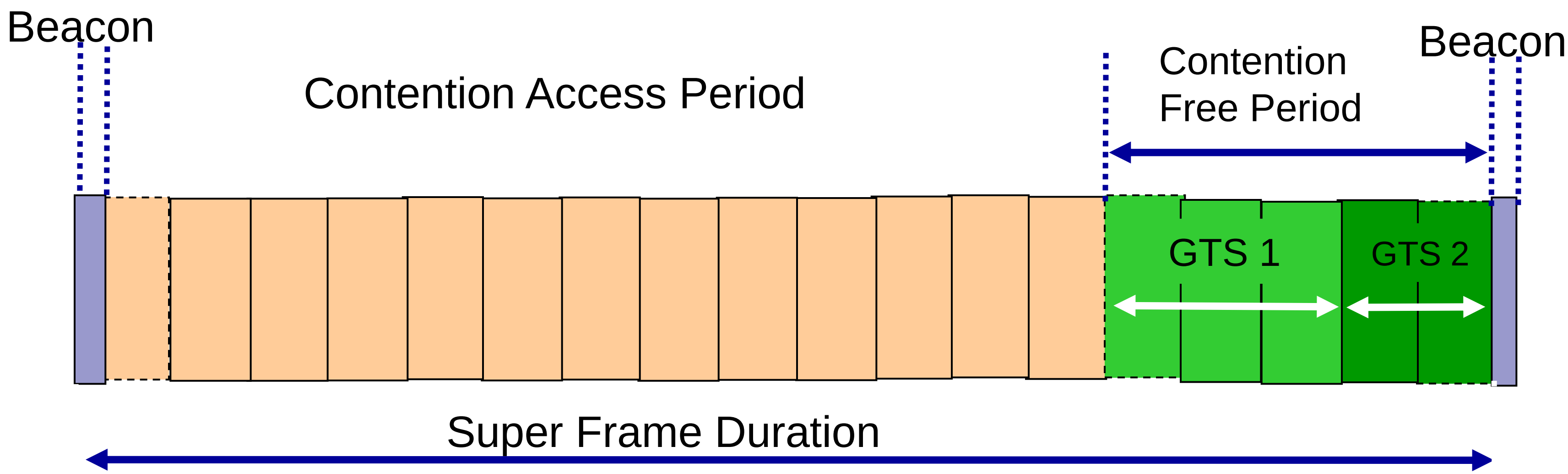


Super Frame Structure With GTSs

- Guaranteed Time Slots (GTSs).
  - For low-latency applications or applications requiring specific data bandwidth.
  - The GTSs form the Contention-Free Period (CFP).
  - Each device transmitting in a GTS ensures that its transaction is complete before the time of the next GTS or the end of the CFP



802.15.4 MAC Super Frame Structure



Network Beacon — Transmitted by nodes. Contains network information, super frame structure, and notification of pending messages

Contention Period — Access by any node using CSMA-CA

Allocated slot — Reserved for nodes requiring guaranteed bandwidth

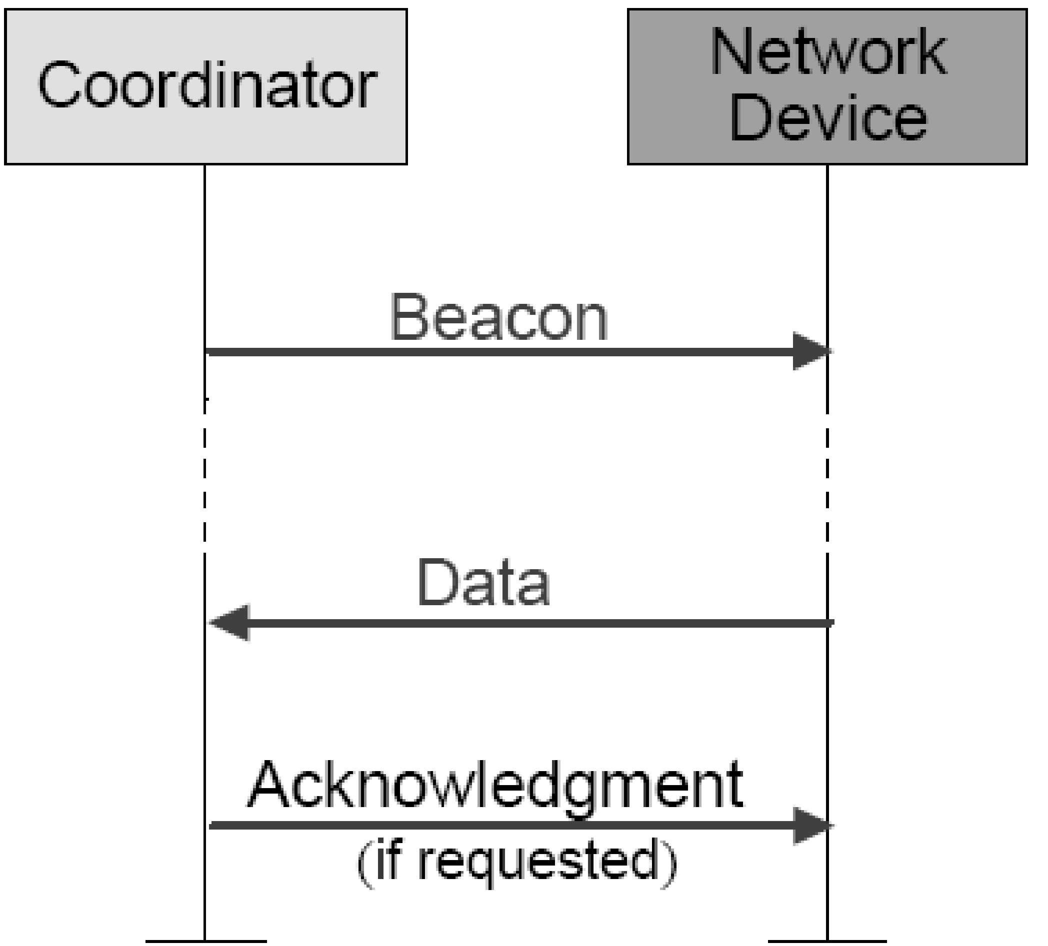
Data Transfer Model

- Three types of data transfer:
  - Data transfer to a coordinator
  - Data transfer from a coordinator
  - Data transfer between two peer devices.
- In star topology, only first two types are used
- In a peer-to-peer topology, data may be exchanged between any two devices on the network;

Data Transfer to a Coordinator

- Device first listens for the network beacon.
- When the beacon is found, the device synchronizes to the super frame structure.
- At the appropriate time, the device transmits its data frame, using slotted CSMA-CA, to the coordinator.
- The coordinator may acknowledge the successful reception of the data by transmitting an optional acknowledgment frame.

Data Transfer to a Coordinator in a Beacon-enabled PAN

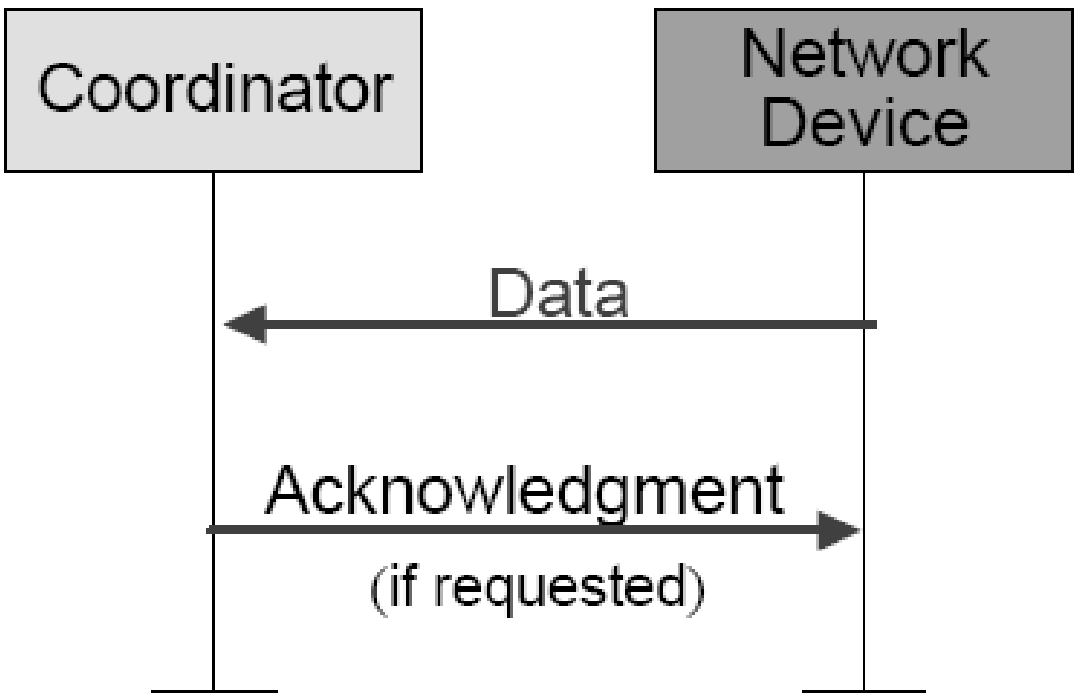


Data Transfer to a Coordinator in a Nonbeacon-enabled PAN

- The PAN coordinator never sends beacons.
- Communication happens on the basis of unslotted CSMACA.
- The coordinator is always on and ready to receive data
- Coordinator to coordinator communication poses no problems since both nodes are active all the time.

Data Transfer to a Coordinator in a Nonbeacon-enabled PAN

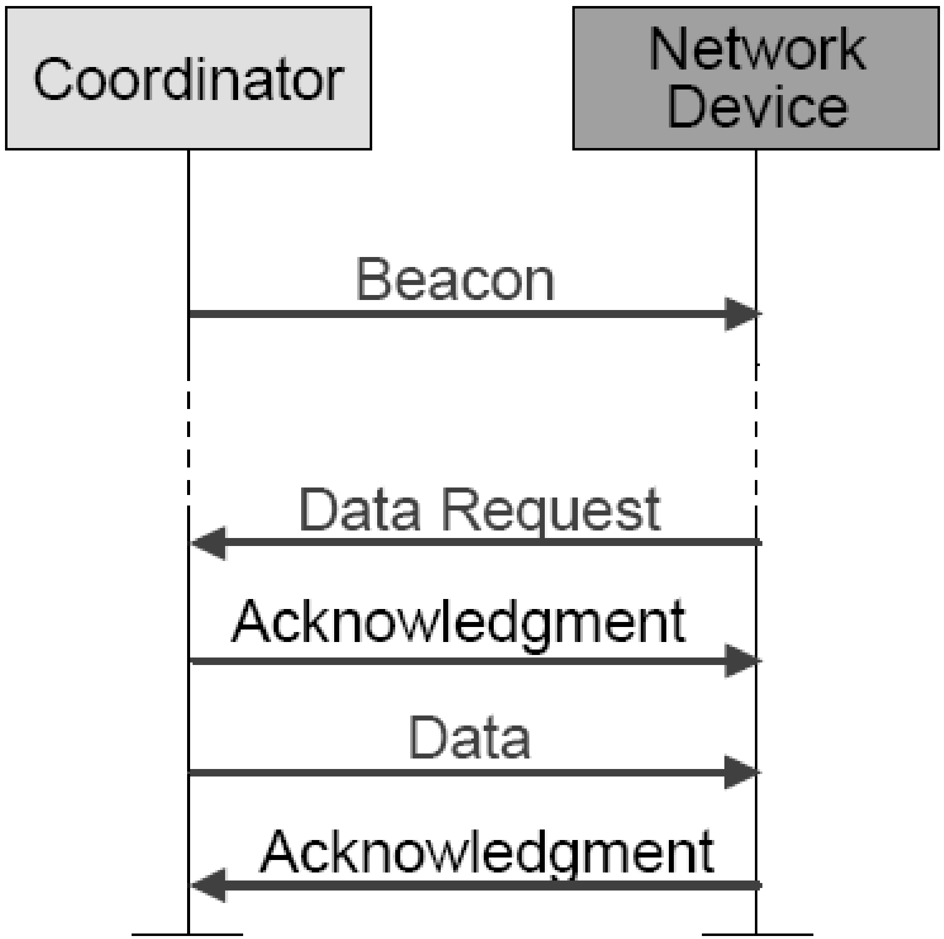
Device simply transmits its data frame, using unslotted CSMA-CA, to the coordinator.



Data Transfer From a Coordinator in a Beacon-enabled PAN

- Coordinator indicates in the network beacon that the data message is pending.
- The device periodically listens to the network beacon
- If a message is pending, device transmits a MAC command requesting the data.
- The coordinator acknowledges the successful reception of the data request
- The pending data frame is then sent
- The device may acknowledge the successful reception of the data
- Upon successful completion of the data transaction, the message is removed from the list of pending messages in the beacon.

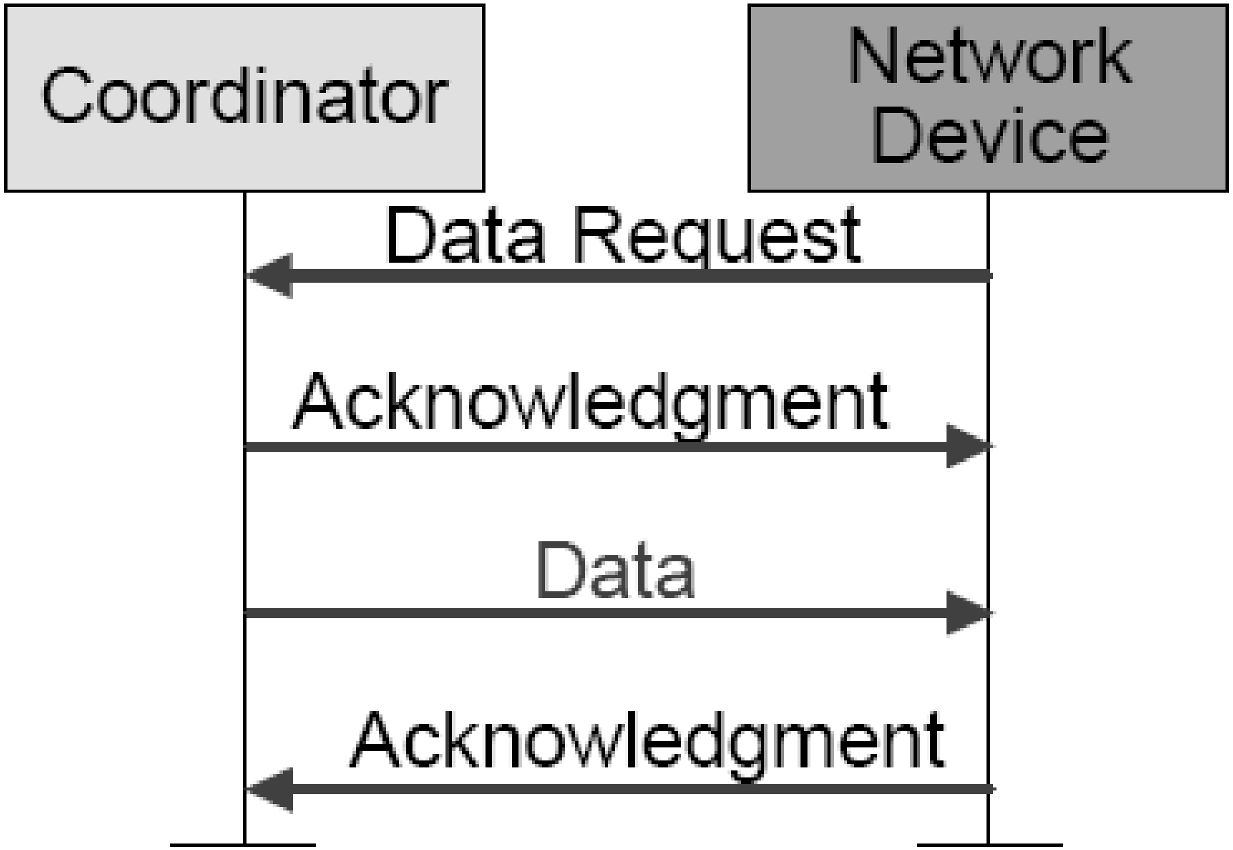
Data Transfer From a Coordinator in a Beacon-enabled PAN



Data Transfer From a Coordinator in a Nonbeacon-enabled PAN

- Coordinator stores the data for the appropriate device to make contact and request the data.
- A device may make contact by transmitting a MAC command requesting the data.
- The coordinator acknowledges the successful reception of the data request.
- If requested, the device acknowledges the successful reception of the data frame.

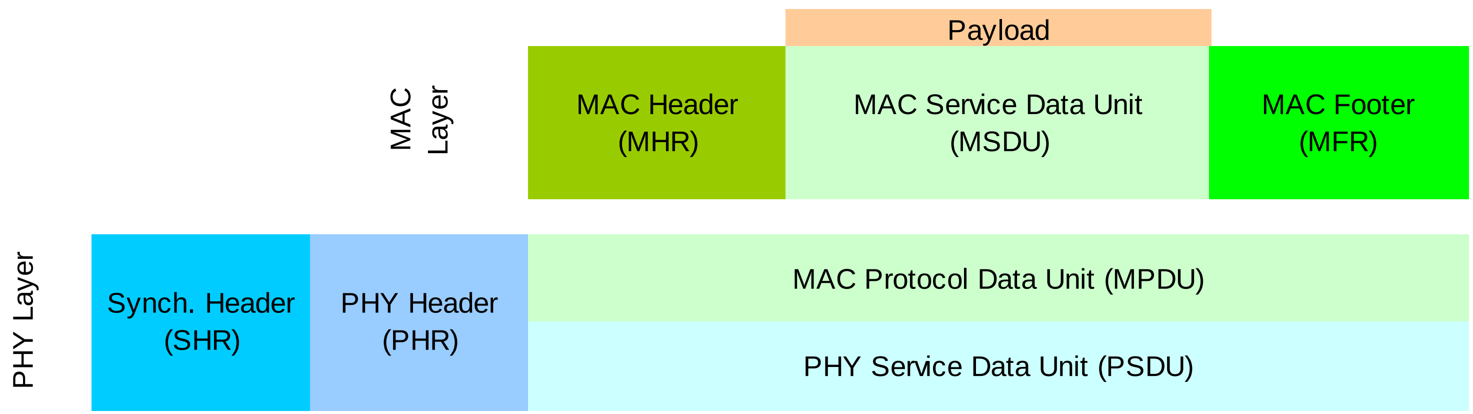
Data Transfer From a Coordinator in a Nonbeacon-enabled PAN



Peer-to-peer Data Transfers

- Every device may communicate with every other device in its radio sphere of influence.
- The devices wishing to communicate will need to either receive constantly or synchronize with each other.
- In the former case, the device can simply transmit its data using unslotted CSMA-CA.
- In the latter case, other measures need to be taken in order to achieve synchronization.

IEEE 802.15.4 MAC Overview General Frame Structure



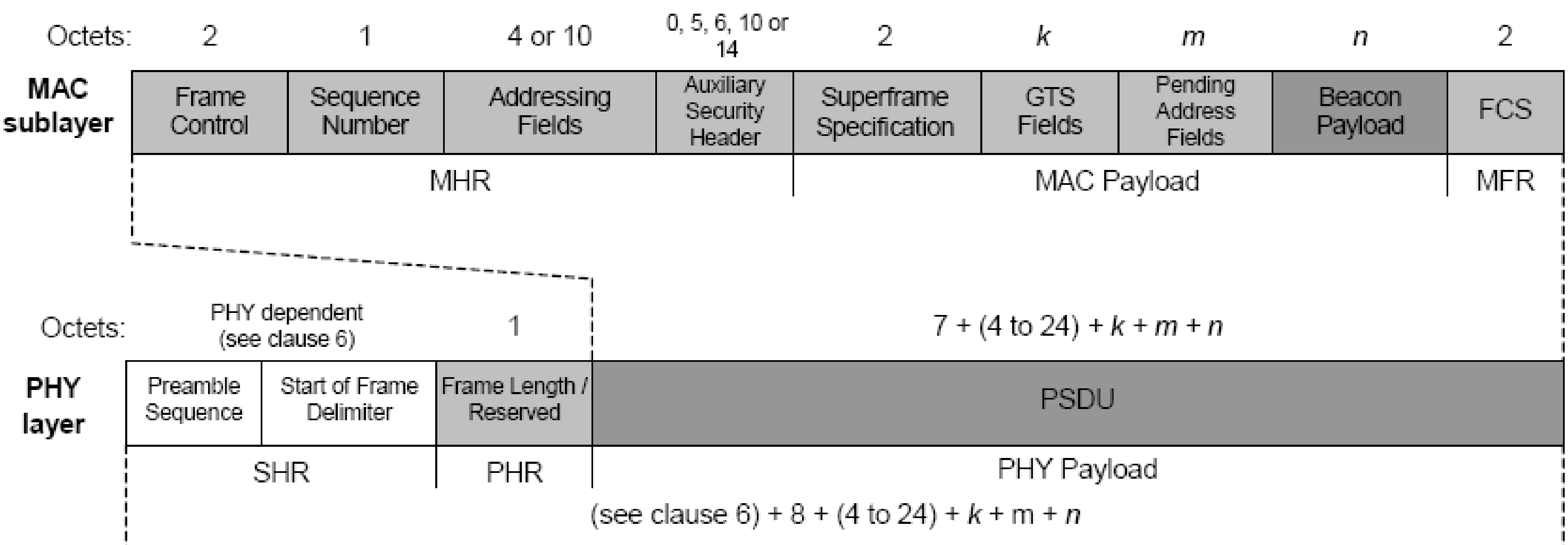
4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

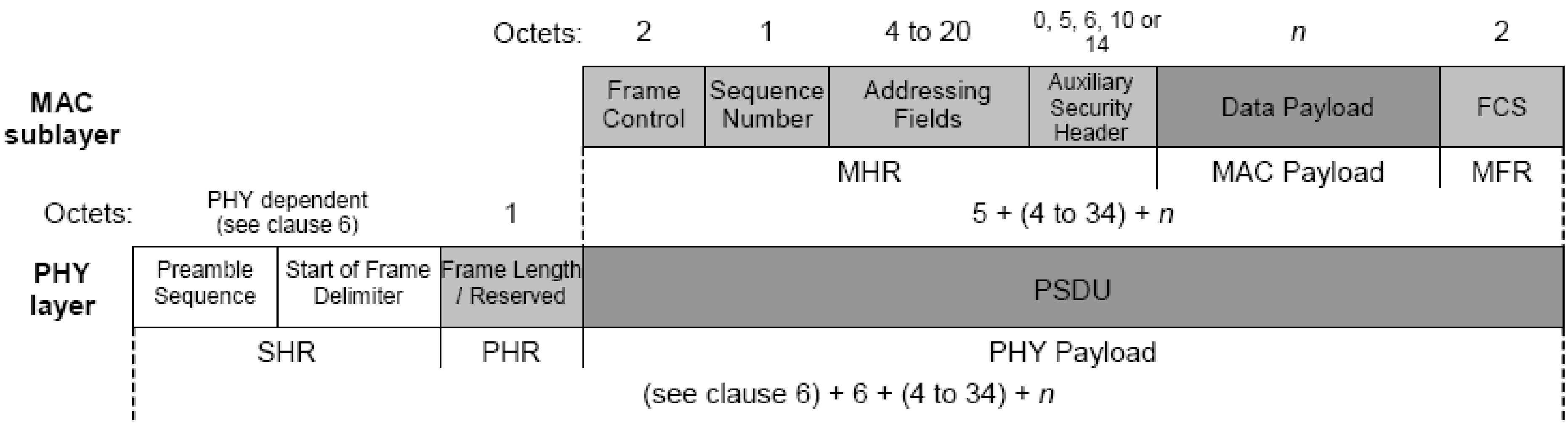
Frame Structure

- Four types of frame:
  - Beacon frame:
    - Used by a coordinator to transmit beacons
  - Data frame:
    - Used for all transfers of data
  - Acknowledgment frame:
    - Used for confirming successful frame reception
  - MAC command frame:
    - Used for handling all MAC peer entity control transfers

Beacon Frame

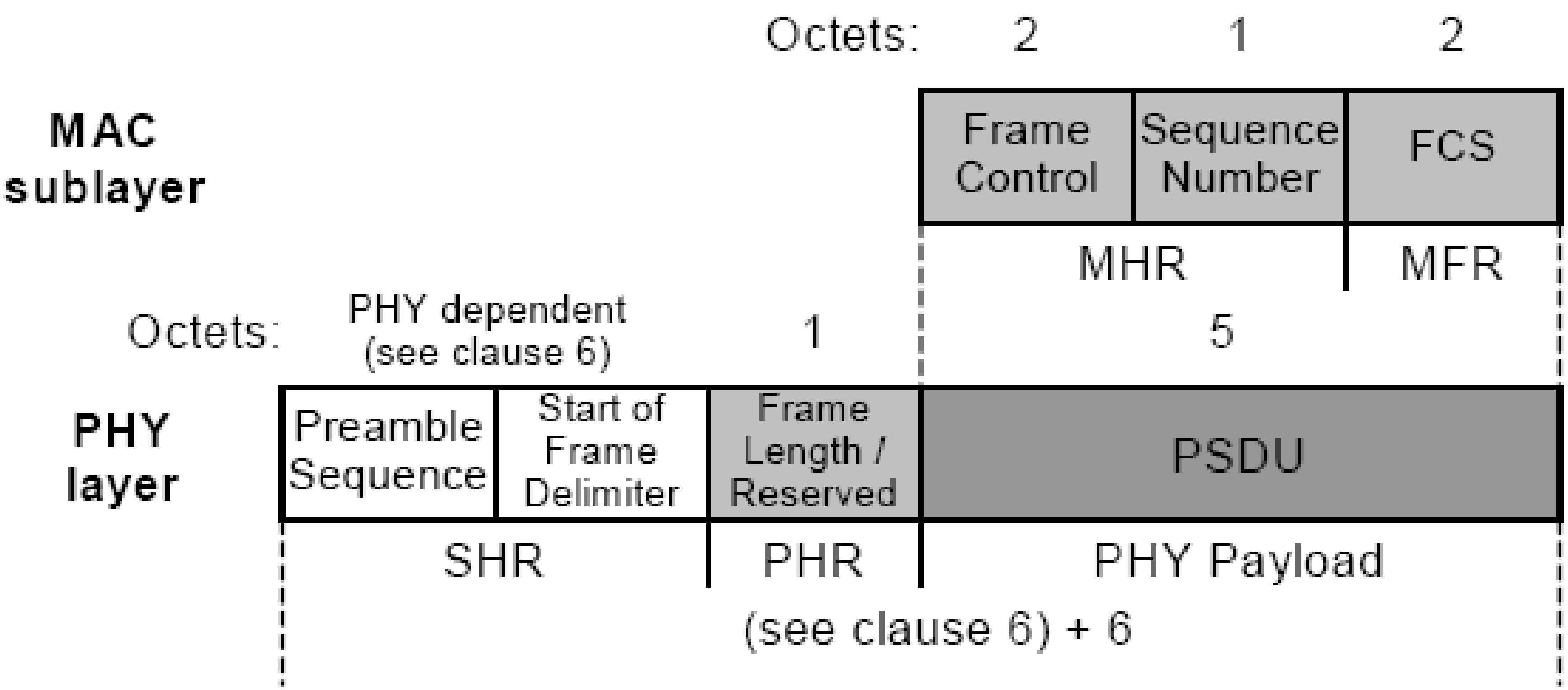


Data Frame

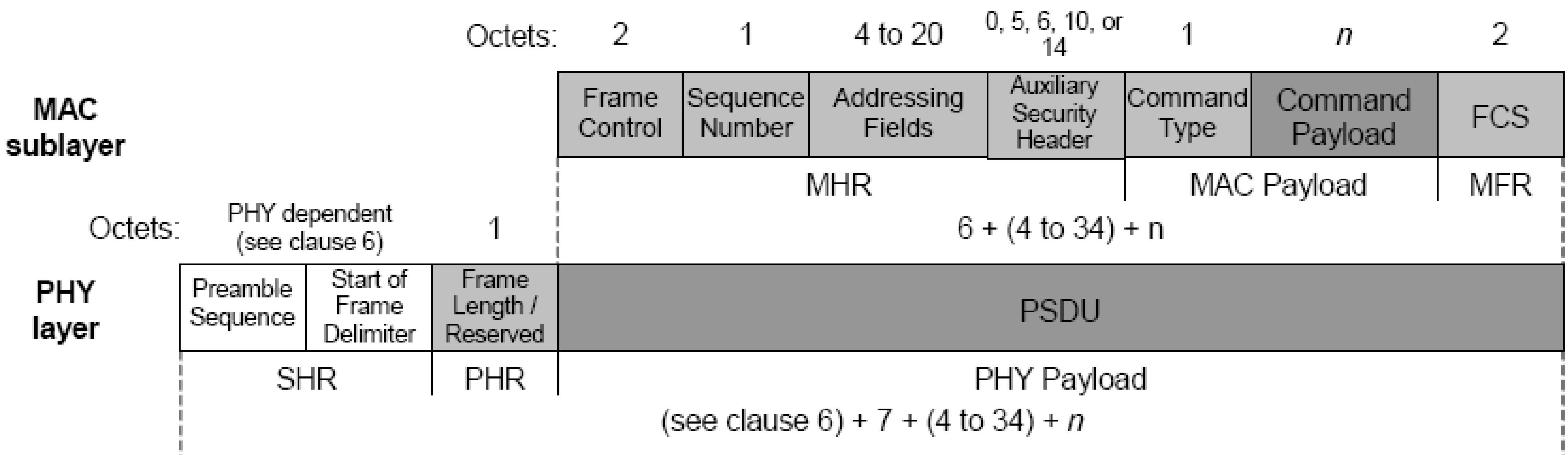


Octets: 2 1 4 to 20 0, 5, 6, 10 or 14 n 2
MAC sublayer
Frame Control
Sequence Number
Addressing Fields
Auxiliary Security Header
Data Payload
FCS
MHR
MAC Payload
MFR
Octets: PHY dependent (see clause 6) 1
5 + (4 to 34) + n
PHY layer
Preamble Sequence
Start of Frame Delimiter
Frame Length / Reserved
PSDU
SHR
PHR
PHY Payload
(see clause 6) + 6 + (4 to 34) + n

Acknowledgment Frame



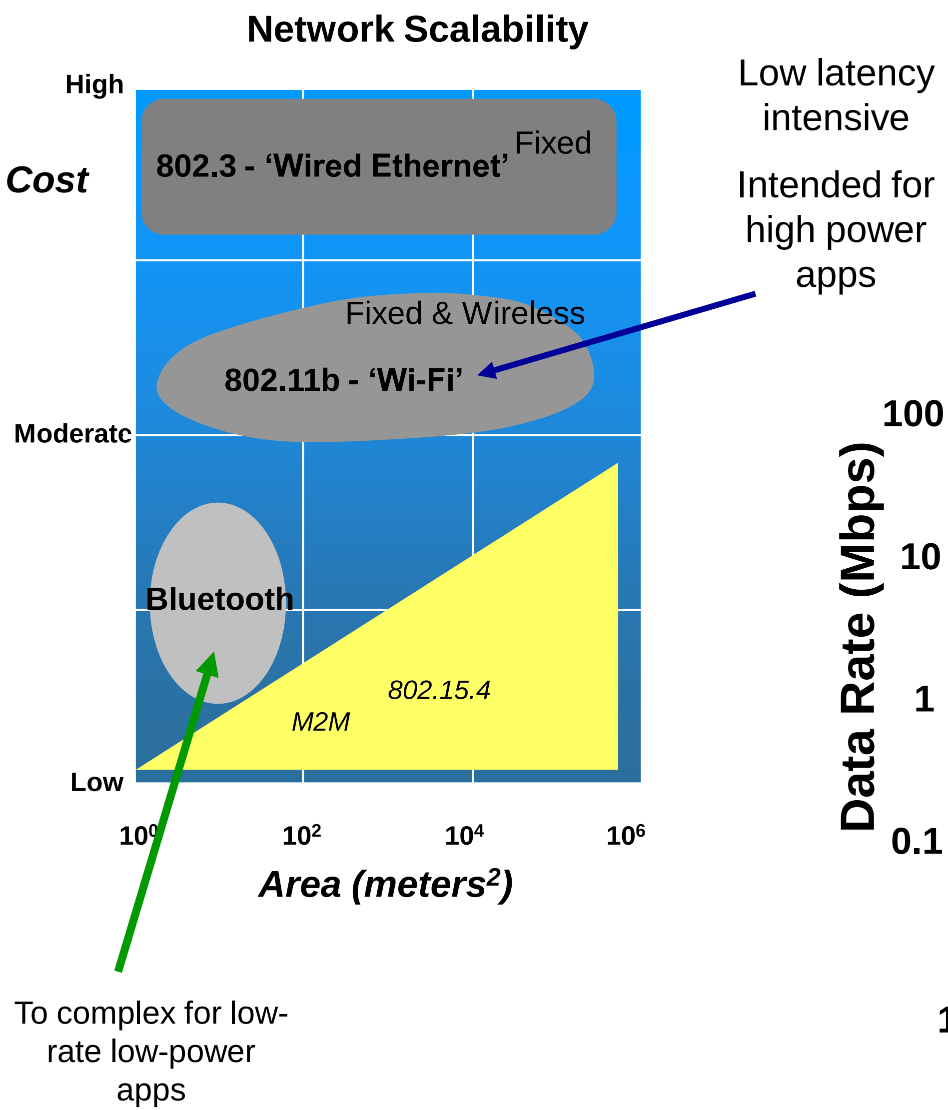
MAC Command Frame

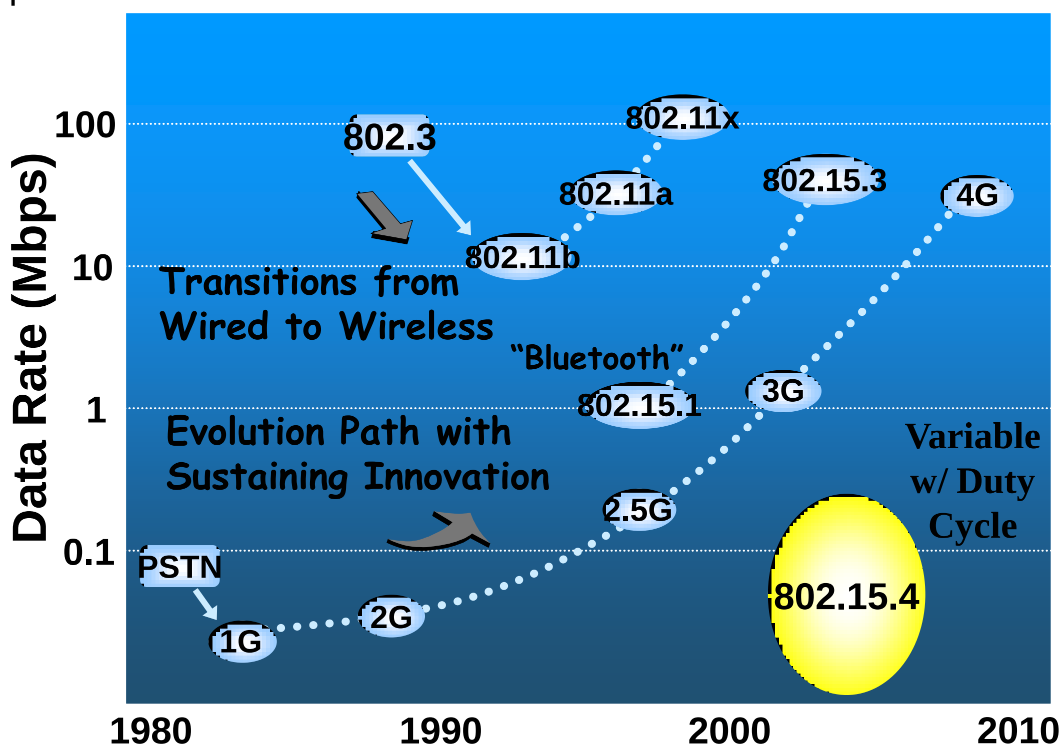


Security

- Devices are
  - Low-cost
  - Limited capabilities in terms of
    - Computing power,
    - Available storage,
    - Power drain;
- Most of security architectural elements can be implemented at higher layers.
- The cryptographic mechanism is based on symmetric-key cryptography and uses keys that are provided by higher layer processes.

Related Technologies





Part 4
ZigBee Standard

What is ZigBee?

- A low data rate, low power specification
- ZigBee Alliance is
  - *“an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard.“*

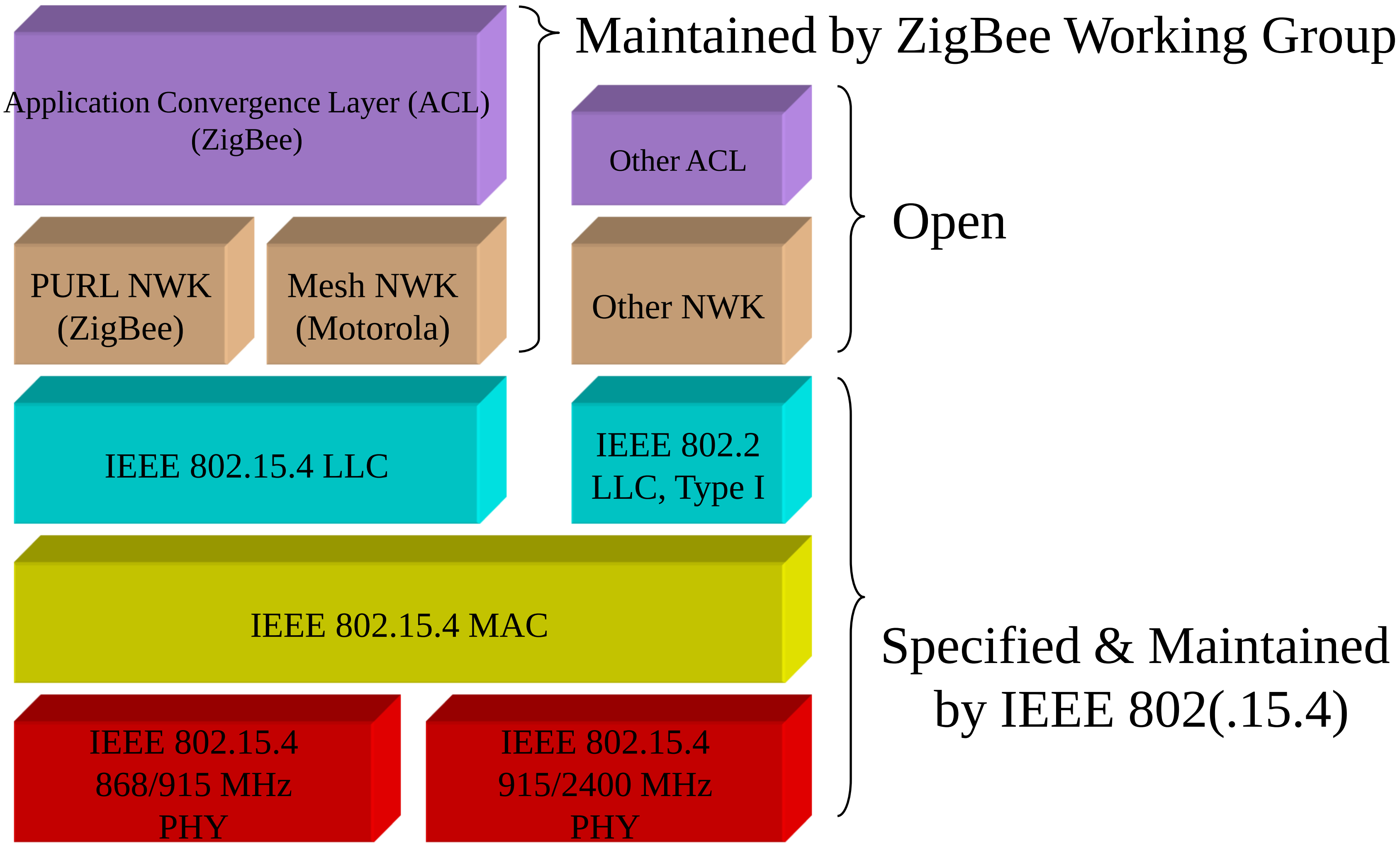
ZigBee/802.15.4

- 802.15.4 standardizes lower layers (Phy-MAC).
- ZigBee refers to additional set of higher-layer standards.
  - developed by industry group "the ZigBee Alliance"
- Alliance provides
  - upper layer stack and application profiles
  - compliance and certification testing
  - Branding
- Over 150 member companies
  - including Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Philips, and Samsung.

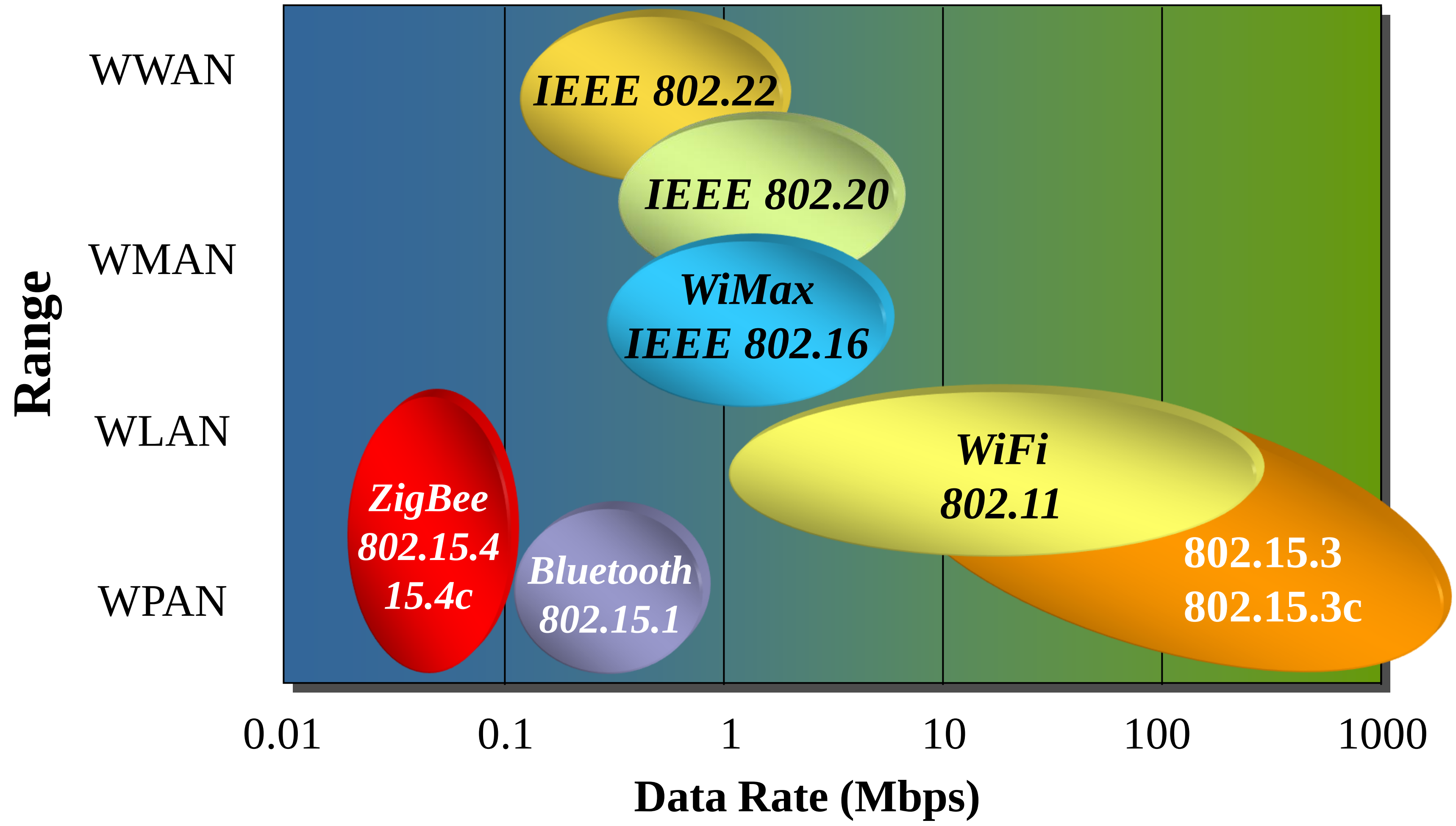
ZigBee

- The name "ZigBee" is derived from the erratic zigging patterns many bees make between flowers when collecting pollen.
- This is evocative of the invisible webs of connections existing in a fully wireless environment.

Low Rate Stack Architecture



ZigBee's Place



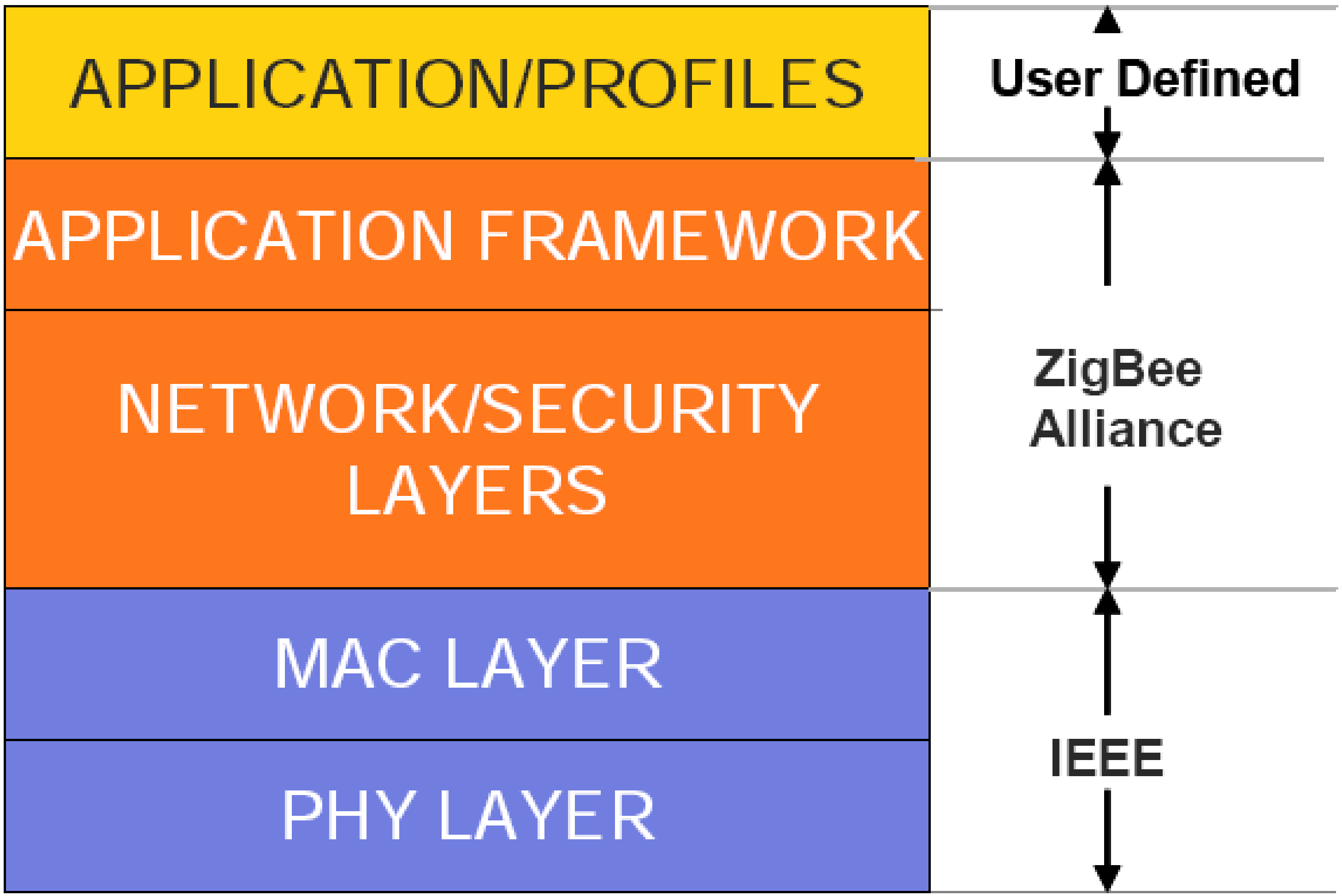
History of ZigBee

- No adequate solution for:
  - Smart badges
  - Home Automation
  - Interactive toys
- IEEE 802.15.4 task group set out to design a standard with:
  - Low data rate
  - Long battery life
  - Very low complexity
- In 2003, a standard was completed

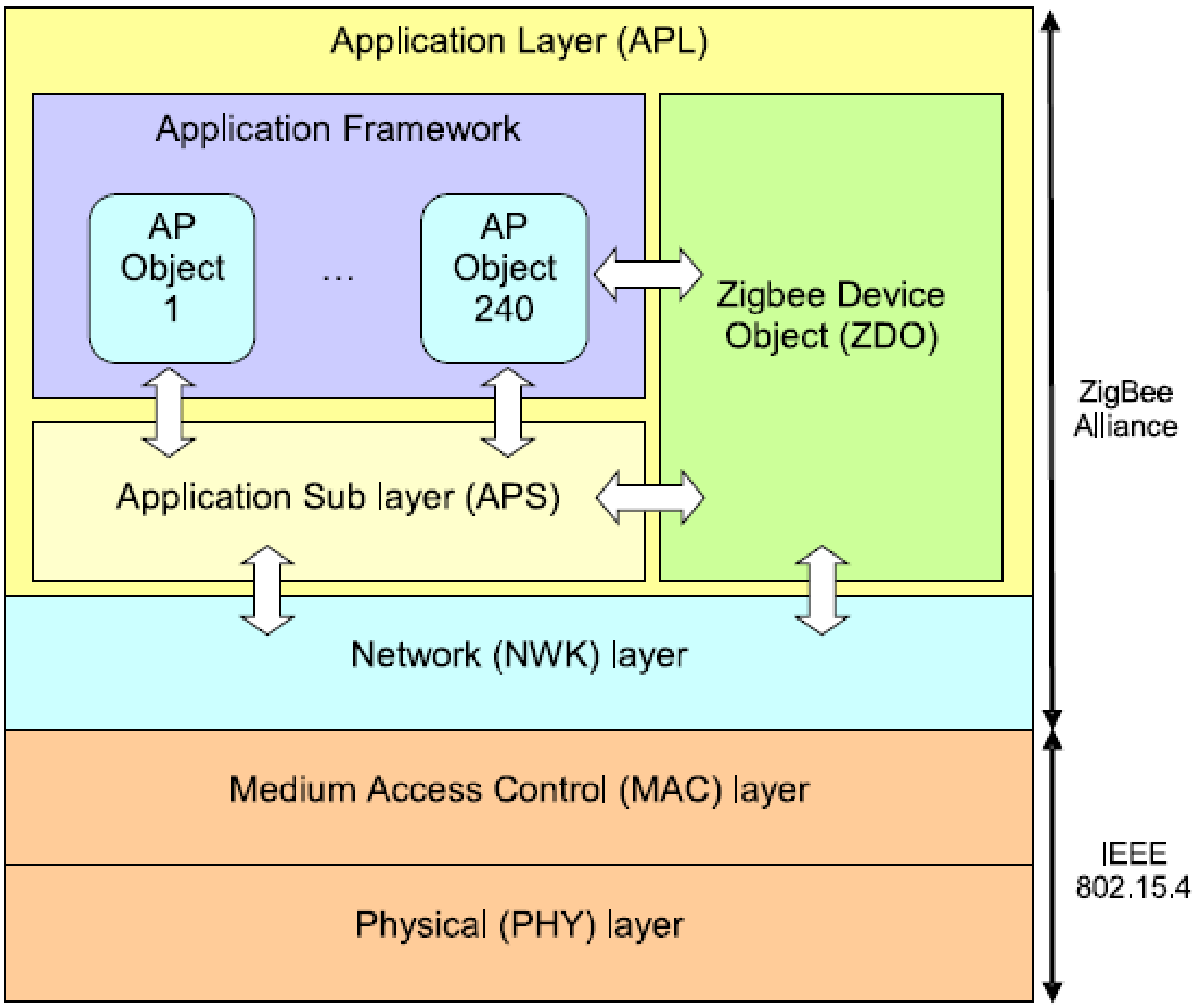
History of ZigBee

- October 2002
  - ZigBee Alliance is formed
- December 2004
  - ZigBee 1.0 is released
- Current releases
  - 802.15.4 is 2006
  - ZigBee specification is 2007

Protocol Stack and Responsibility



Protocol Stack



Zigbee Layers

- The network layer (NWK)
  - Organizing and providing routing over a multihop network
- Application Layer (APL)
  - Providing a framework for distributed application development and communication.
- The APL comprises:
  - Application Framework.
  - ZigBee Device Objects (ZDO).
  - Application Sub Layer (APS).
- The Application Framework can have up to 240 Application Objects, that is, user defined application modules which are part of a ZigBee application.
- The ZDO provides services that allow the APOs to discover each other and to organize into a distributed application.
- The APS offers an interface to data and security services to the APOs and ZDO.

IEEE 802.15.4 PHY

- Direct Sequence Spread Spectrum
- Link quality measurements
  - Used by higher layers

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

IEEE 802.15.4 MAC

- Two addressing modes
  - 16 bit (~65,000 devices)
  - 64 bit (lots of devices)
- CSMA/CA
- Allows for network beaconing
  - Wake up periodically, checking for a beacon
- Power savings
  - Nodes can sleep between beacons
  - Nodes that don’t have to route or randomly receive can sleep until needed

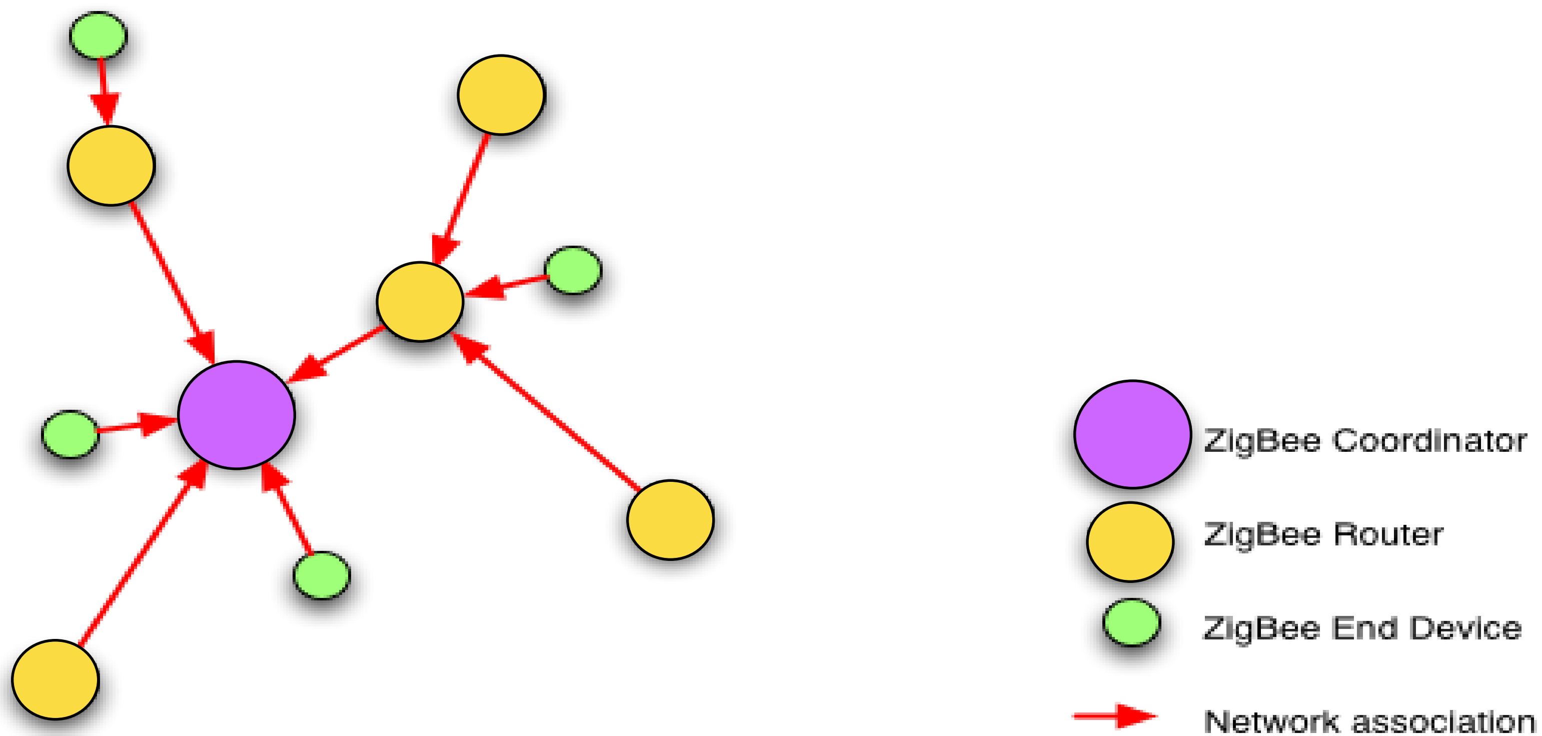
The Network Layer

- ZigBee identifies three device types:
  - ZigBee end-device corresponds to an IEEE RFD or FFD
  - ZigBee router is an FFD with routing capabilities
  - ZigBee coordinator (one in the network) is an FFD managing the whole network.
- ZigBee network layer also supports more complex topologies like the tree and the mesh
- Multihop routing
- Route discovery and maintenance
- Security and joining/leaving a network

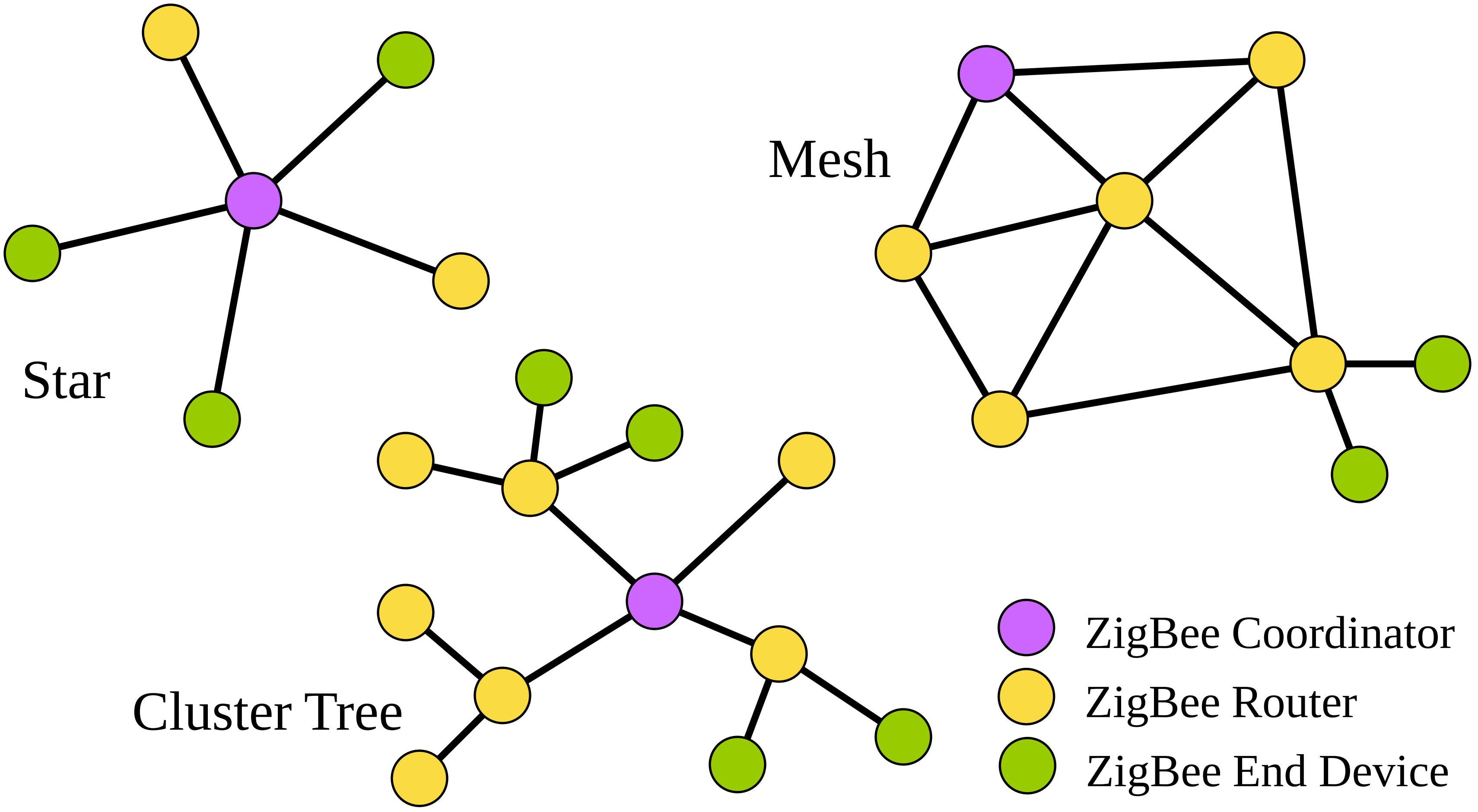
ZigBee Device Types

- 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) (some times called RFD)
  - Optional network component.
  - Shall not allow association.
  - Shall not participate in routing.

Device Associations



Network Topologies



Network Formation and Address Assignment

- A Multihop network is established by means of the join procedure.
- When a device c wishes to join an existing network, the network layer is requested to start a network discovery procedure.
- With support from the MAC layer scan procedure, it learns about neighbouring routers that announce their networks.
- After the upper layer has decided which network to join, the network layer selects a ‘‘parent’’ node p (in the desired network) from his neighbourhood, and asks the MAC layer to start an association procedure.
- Upon receiving an indication of the association request from the MAC layer, p’s network layer assigns c a 16-bit short address and lets the MAC layer successfully reply to the association request.
- Node c will use the short address for any further network communication.

ZigBee Tree

- Parent-child relationships established as a result of joins shape the whole network in the form of a tree
- The ZigBee coordinator is the root of tree
- The ZigBee routers are internal nodes
- The ZigBee end-devices are leaves
- The ZigBee coordinator fixes:
  - The maximum number of routers (Rm)
  - The maximum number of end-devices (Dm) that each router may have as children
  - The maximum depth of the tree (Lm)

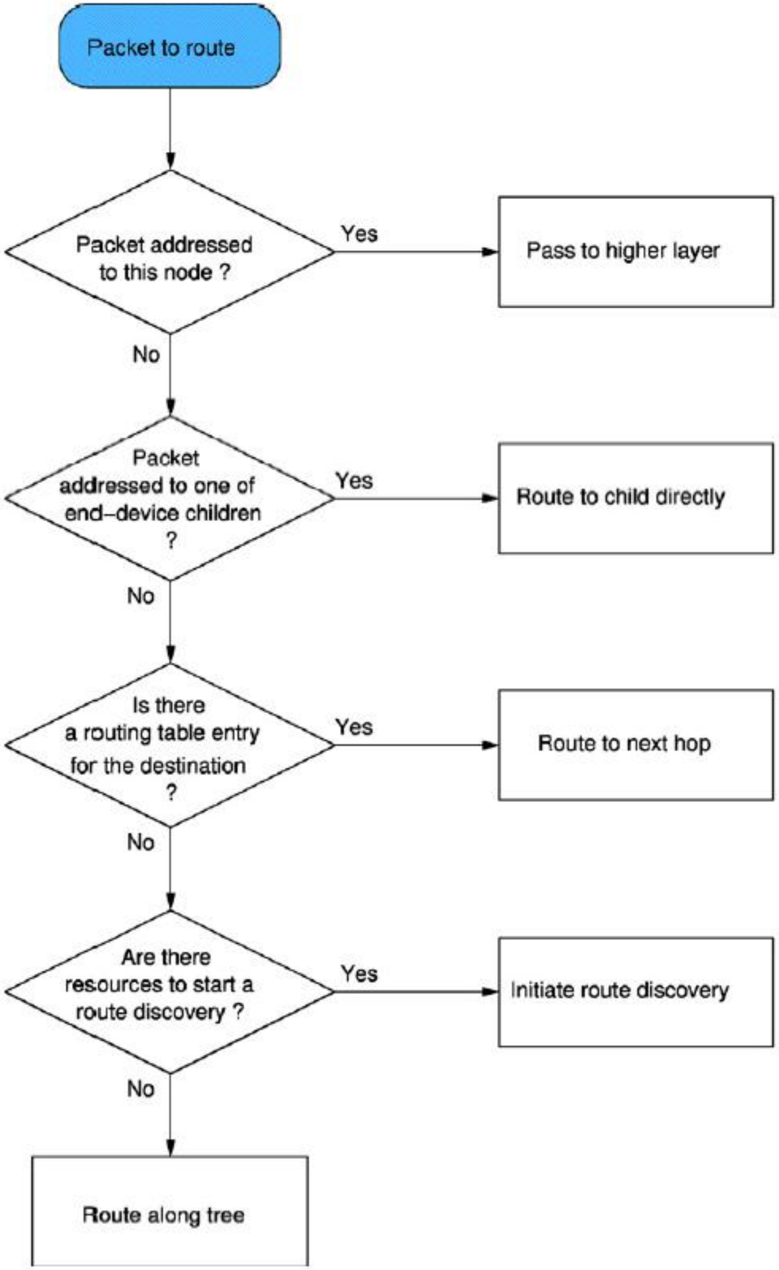
Routing

- The routing algorithm depends on the topology used in the sensor network.
- Ad hoc On Demand Distance Vector (AODV)
  - Used for mesh topologies
- Cluster-Tree Algorithm
  - Form clusters of nodes that make a tree

Tree-based Routing

- Routing can only happen along the parent-child links
- Routers maintain only their address and the address information associated with their children and parent.
- Given the way addresses are assigned, a router that needs to forward a message can easily determine whether the destination belongs to a tree rooted at one of its router children or is one of its end-device children.
- If so, it routes the packet to the appropriate child;
- Otherwise it routes the packet to its parent.

Routing Algorithm



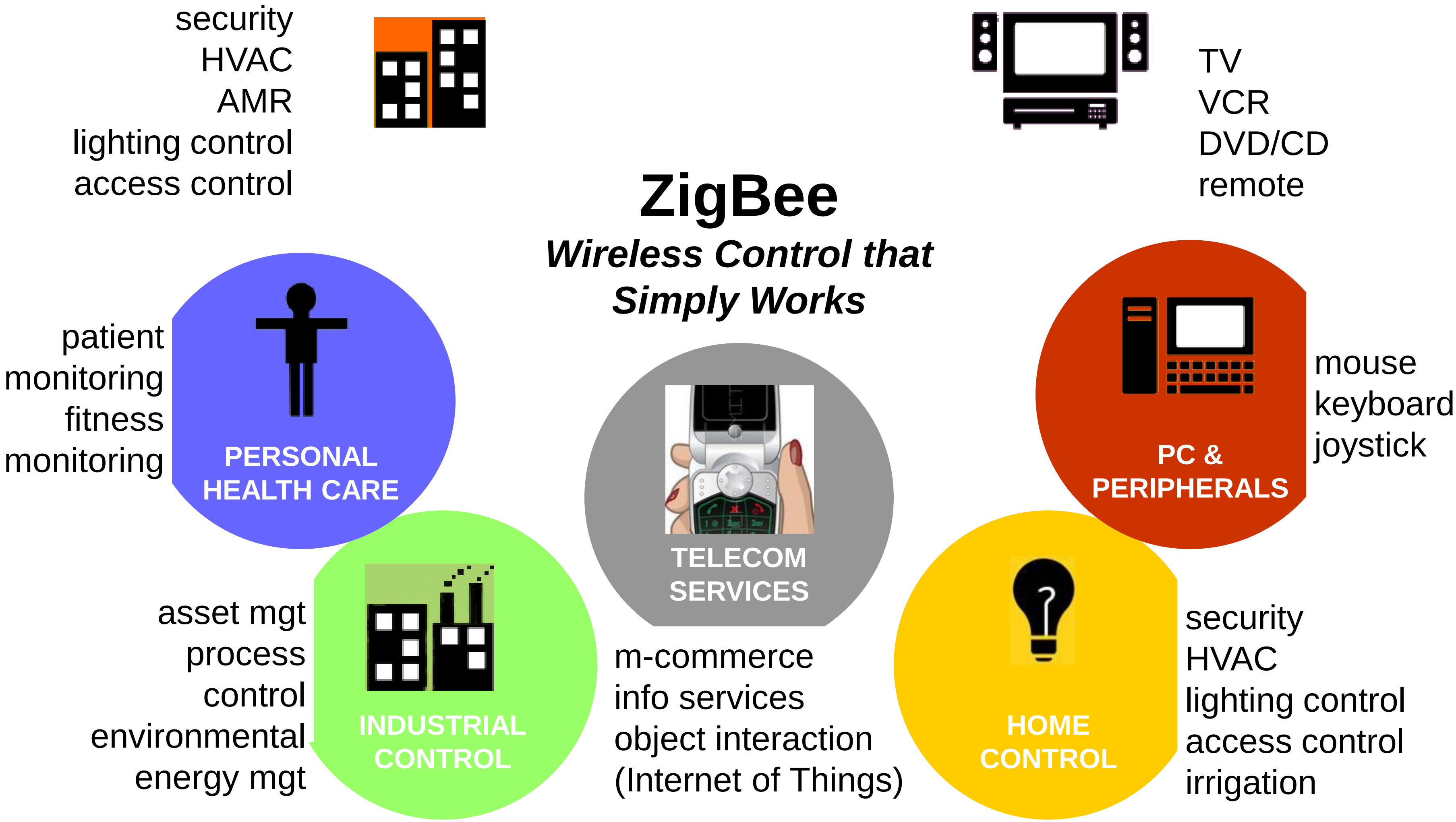
Route Discovery

- The process required to establish routing table entries in the nodes along the path between two nodes wishing to communicate.
- Route discovery in ZigBee is based on the well-known Adhoc On Demand Distance Vector routing algorithm (AODV)
- When a node needs a route to a certain destination, it broadcasts a route request (RREQ) message .
- RREQ message is propagated through the network until it reaches the destination.
- The RREP message is addressed to the route discovery originator and carries with it a residual cost value field that each node increments as it forwards the message.

The Application Layer

- A ZigBee application consists of a set of Application Objects (APOs) spread over several nodes in the network.
- An APO is a piece of software that controls a hardware unit (transducer, switch,lamp)
- Each APOis assigned a locally unique endpoint number that other APOs can use as an extension to the network device address to interact with it.
- The ZigBee Device Object (ZDO) is a special object which offers services to the APOs.
- It allows them to discover devices in the network and the service they implement.
- It also provides communication, network and security management services.
- The Application Sublayer (APS) provides data transfer services for the APOs and the ZDO.

ZigBee Applications



Application Profiles

- An application profile defines message formats and protocols for interactions between APOs
- Profiles regulate types of messages to and from end points
- Public Profiles
  - Interoperability
- Vendor Profiles
  - Undergoes certificate testing
  - Shouldn’t interfere with other ZigBee networks

Example Profiles

- Home Automation
  - Devices used:
    - Light switch
    - Lamp
    - Thermostat
- Industrial Plant Monitoring
  - Devices used:
    - Pressure sensors
    - Cameras
    - Thermostat

ZigBee Security

- Encryption using 128-bit key
  - Symmetric key (shared key)
- Multi-layer Security
  - Network layer uses Advanced Encryption Standard (AES)
  - Network layer has different levels of security

ZigBee Security

- ZigBee is touted as “highly secure”
- Relies on centralized infrastructure
  - Coordinator acts as trust center
- Types of keys:
  - Master key
    - Installed out-of-band
  - Network key
    - Shared by all devices
    - No protection against “insider” attacks
  - Link key
    - Derived from master key

ZigBee Vendors

- Freescale
- Cirronet
- GridConnect
- MaxStream
- AirBee
- Jennic
- Silicon Labs
- Meshnetics
- MicroChip

Typical ZigBee Device

Operating Frequency 2.4 GHz

250 Kbps O-QPSK in 5 MHz channels

Sensitivity ~-91 dBm

Output programmable from -27 to 4 dBm

Sleep Power = .5 uW

Transmit Power = 81 mW

Receive Power = 99 mW

ZigBee/802.15.4

ZigBee targets extremely low power/long-lifetime devices.

	802.11	Bluetooth	RFID	Zigbee
Power	Hours	Days	Passive:no power Active:months	Years
Configuration	Ad-hoc (DCF) and Access point (PCF) modes	Master- few slaves	Reader-tags	Master-many slaves
Nodes	30	7	100s	64000
Data rates	Few Mbps to 50 Mbps	1 Mbps	10 Kbps to 100 Kbps	250 Kbps
Range	100 meters	10 meters	Cm to a meter	70 – 100 meter

How does ZigBee compare to other wireless standards?

Market Name	ZigBee®	---	Wi-Fi™	Bluetooth™
Standard	802.15.4	GSM/GPRS CDMA/1xRTT	802.11b	802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Maximum Data Rate (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

ZigBee vs. Bluetooth

- Larger Range
  - 100m vs. 10m
- Lower Data Rate
  - 20 to 250 Kbps vs. 1 Mbps
- Lower Energy
  - Multi-year vs. multi-day battery life
- Device numbers
  - 7 slaves per network vs. 65,000 nodes

Conclusions

- ZigBee is beneficial for low data rate, low power applications
  - Control
  - Automation
  - Monitoring
- Centralized trust center helps to manage security

Part 5
Energy-Efficient MAC Layer

Energy Efficiency

- Energy efficiency is probably the most important issue in Wireless Sensor Networks (WSNs).
- It is extremely important to develop techniques that prolong battery lifetime as much as possible.
- Unnecessary energy consumption must be avoided by :
  - Attentive hardware/component design
  - Low level and high level software programming.

Requirements for Sensor Networks

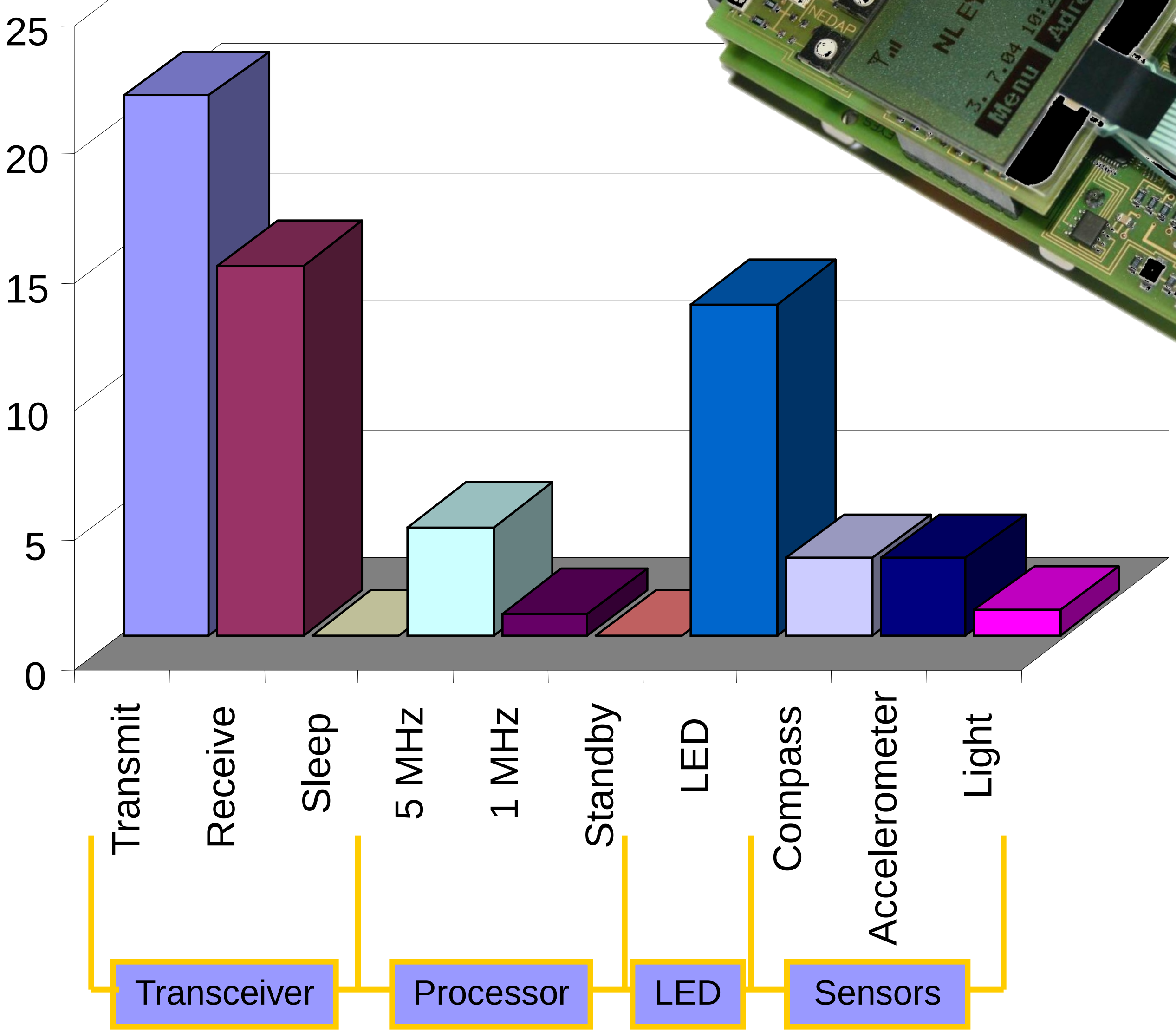
Handle scarce resources

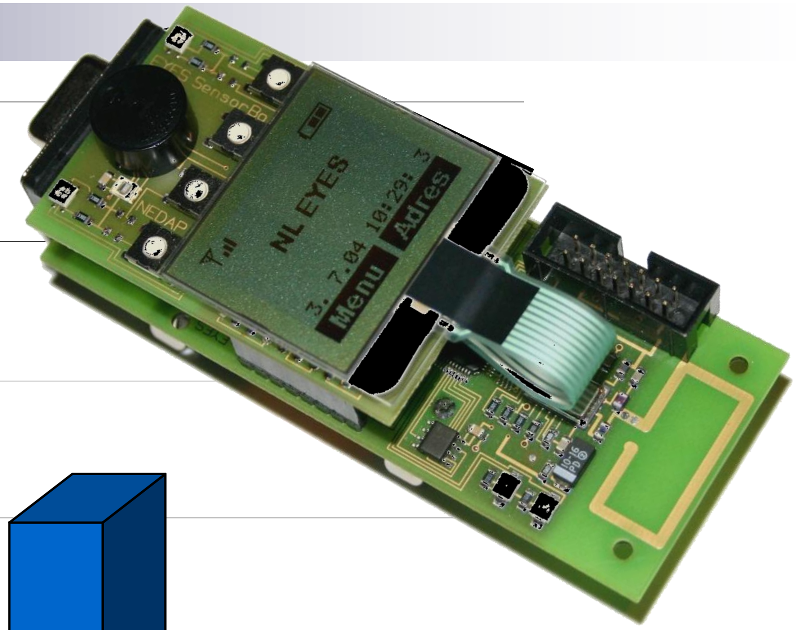
- CPU: 1 – 10 MHz
- memory: 2 – 4 KB RAM
- radio: ~100 Kbps
- energy: small batteries

Unattended operation

- plug & play, robustness
- long lifetime

Energy consumption (mW)





Reasons of Energy Waste

- The major reason for energy waste:
  - Idle listening
    - Node is listening to the radio channel waiting for something.
  - Packet collisions
  - Overhearing a packet destined to another node
  - Control packet overhead

Energy Saving Methods

- Connected dominating set approaches
- MAC layer approaches
- Cross layer approaches
- Topology control

Energy Saving Methodes

- Connected dominating set approaches
- MAC layer approaches
- Cross layer approaches
- Topology control

Connected Dominating Set (CDS)

- The idea of CDS approaches is to select some of the nodes to constitute a network backbone and be active all the time providing network connectivity and temporarily storing messages for neighbouring non-backbone nodes.
- Nonbackbone nodes sleep most of the time (saving energy) and periodically wake up to exchange messages with their backbone node neighbour.
- Since backbone nodes consume more energy than the other nodes, CDS protocols require nodes to alternate between backbone and non-backbone status.
- Examples: GAF and Span

Energy Saving Methodes

- Connected dominating set approaches
- MAC layer approaches
- Cross layer approaches
- Topology control

MAC Layer Approaches

- Attempt to achieve energy savings by exclusive use of medium access control facilities.
- Higher layers are unaffected and unaware of this.
- Methods:
  - Slot-based protocols
  - TDMA protocols
  - S-MAC, T-MAC and DS-MAC
  - Data and signaling channel
  - IEEE 802.15.4 energy efficiency

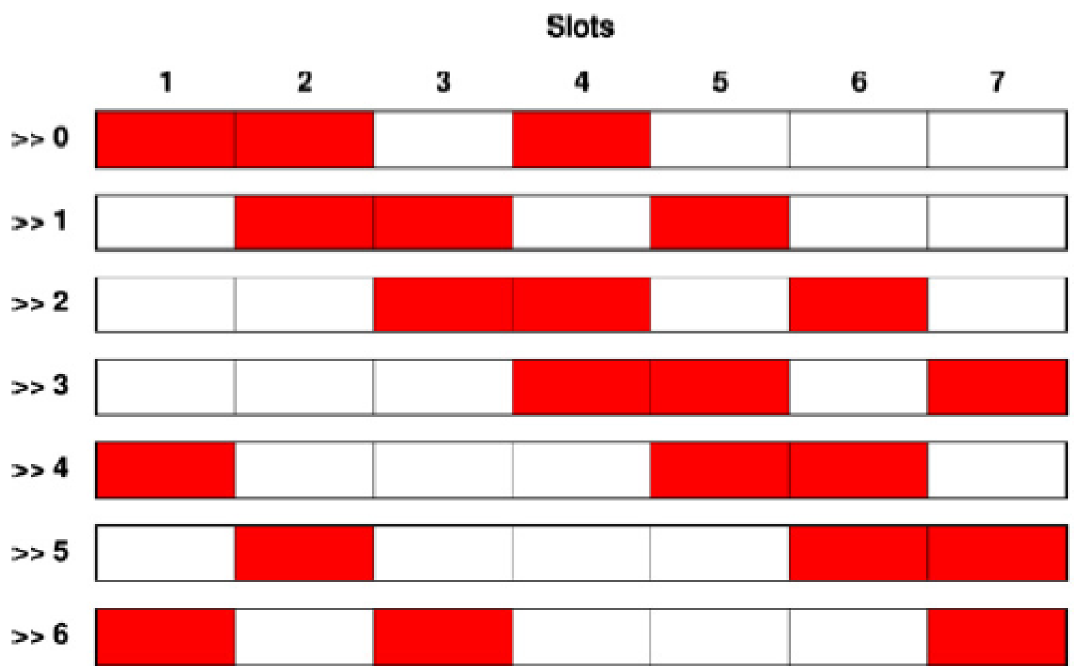
Slot-based Protocols

- Time is divided into periods each containing a certain number of fixed size lots.
- Nodes stay active in a certain predefined subset of the slots.
- In active period they send beacons announcing their schedule
- Activation schedules can be found such that any two neighbouring nodes eventually can hear each other's beacons.

Example

activation schedule: 1101000 (where 1s represent active slots and 0s represent inactive slots)

any two neighbours can hear each other (they have at least one overlapping active slot)



TDMA Protocols

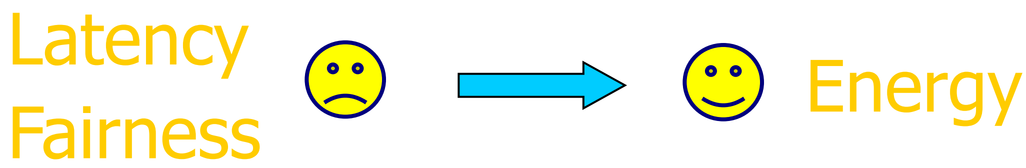
- Schedule transmissions a priori so that any node exactly knows when it must turn on its radio and no collisions can ever result.
- All nodes can see each other and a master, starts a super frame providing synchronization timing for network operation.
- The super frame contains a sequence of slots that may be statically or dynamically allocated.

S-MAC, T-MAC and DS-MAC

- To divide time into periods of fixed duration T consisting of a radio-on active window and a radio-off sleep window.
- Neighboring nodes must organize someway to exchange information about their relative active windows.

Case Study: S-MAC

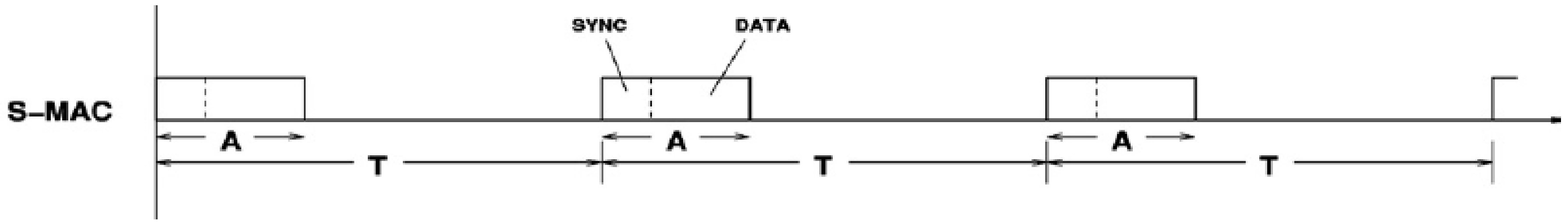
- S-MAC — by Ye, Heidemann and Estrin
- Tradeoffs



- Major components in S-MAC
  - Periodic listen and sleep
  - Collision avoidance
  - Overhearing avoidance
  - Massage passing

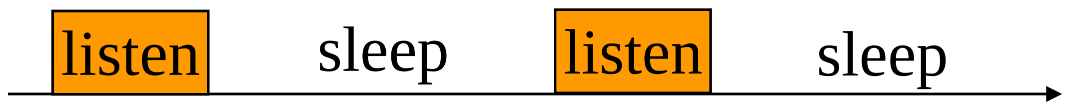
S-MAC

- Active and sleep windows have a fixed network-unique duration A and are divided into two parts.
- The first part is reserved for reception of SYNC messages from neighbours.
- A node informs neighbours of its schedule (the time to the next activation window) by means of periodic SYNC messages.



Coordinated Sleeping

- **Problem:** Idle listening consumes significant energy
- **Solution:** Periodic listen and sleep



  - Turn off radio when sleeping
  - Reduce duty cycle to ~ 10% (120ms on/1.2s off)

Latency ☹ → ☺ Energy

Scheduling

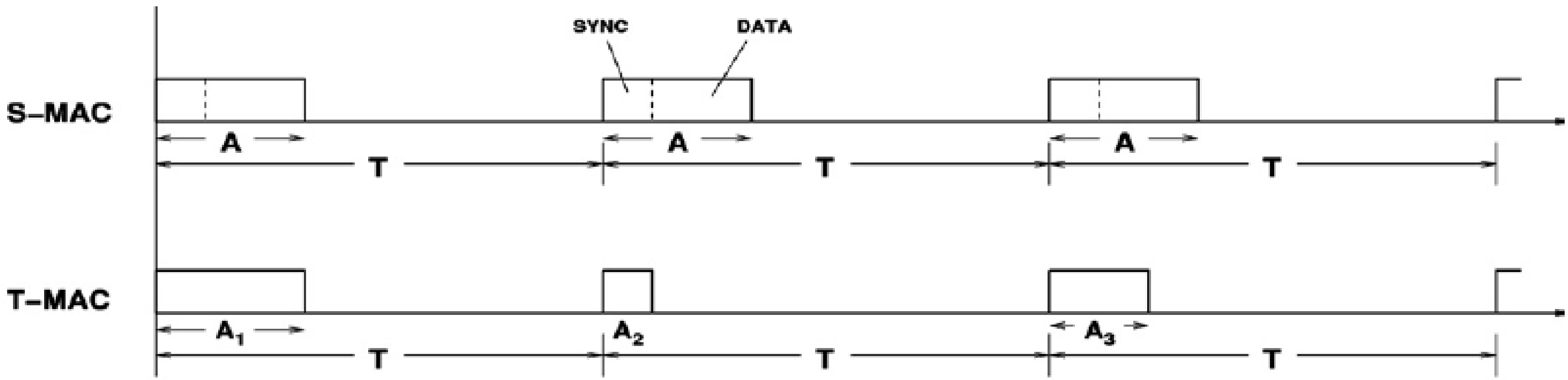
- At startup a node listens for some time to receive schedules from neighbouring nodes.
- It adopts the schedule from a neighbour if it receives one.
- Otherwise it chooses one on its own and starts to advertise it in SYNC messages.
- The above procedure attempts to coordinate nodes so that they use the same schedule.
- It is distributed in nature and some nodes may have to adopt multiple schedules.

Timeout MAC (T-MAC)

- The two main deficiencies of S-MAC are :
  - High latency
  - Insensitivity to varying traffic loads, given its fixed duty cycle.
- T-MAC builds on S-MAC and attempts to mitigate these problems.
- Nodes select their schedule as in S-MAC but active windows are not fixed in duration:
  - They may extend, adapting to different traffic rates.
- Every node turns its radio on at the beginning of its active window and turns if off if no activation event occurs for a certain period.
- Reception of messages is an activation event that prolongs the active window.

S-MAC and T-MAC

S-MAC has fixed active windows while T-MAC has variable active windows that extend as long as messages are received or other activation events occur.



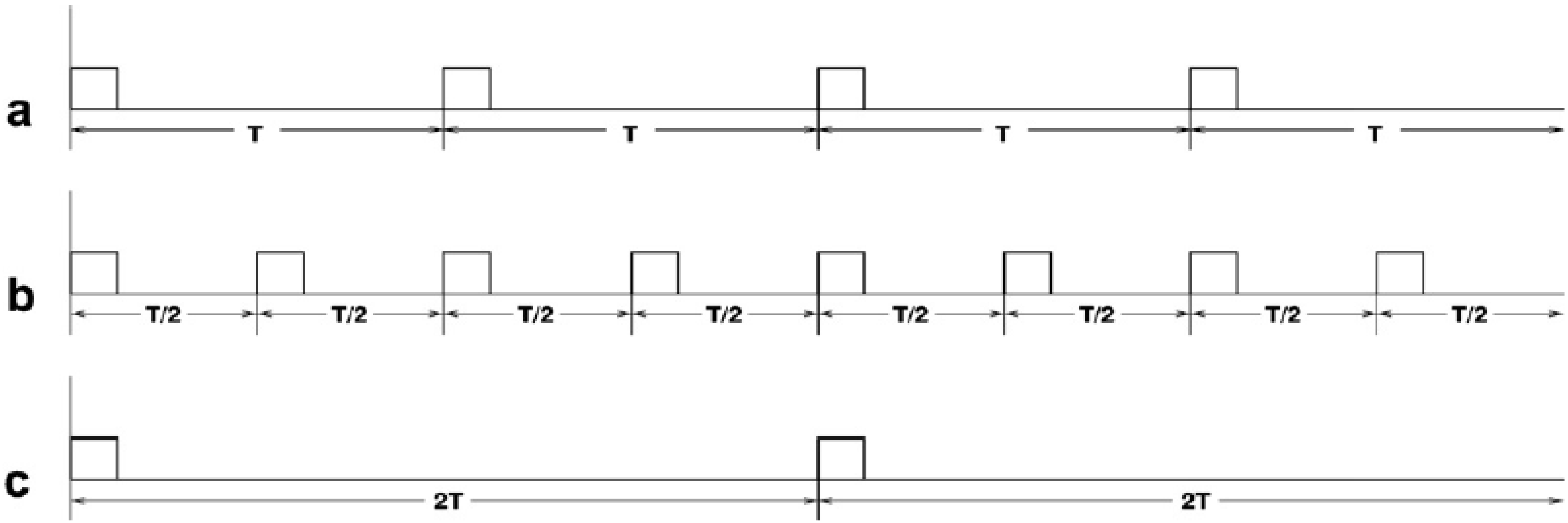
DS-MAC

- DS-MAC also based on S-MAC.
- Starts with a system defined period length but allows a node to double or halve it dynamically depending on traffic load conditions.
- If the average packet reception delay is too high a node will halve its current period duration.
- If packet reception delay is low the node will double the period duration.
- In either case the active window is kept constant.

DS-MAC

b) Average delay is high (node may halve its current period duration from T to T/2)

c) Average delay is low (it may double it from T to 2T)



Data and Signaling Channel

- Energy savings can be achieved augmenting the data channel with a separate signaling channel
- The data channel is used for data and some control messages
- It is only turned on when required
- The signaling channel providing wakeup notifications.
- The signaling radio is characterized by a fixed, low duty cycle but sleeps by different nodes are unsynchronized.

IEEE 802.15.4 Energy Efficiency

- Two modes of IEEE 802.15.4
  - Unslotted CSMA-CA mode (used in beacon-less mode)
  - Slotted CSMA-CA mode (used in beacon enabled mode)
- Unslotted CSMA-CA:
  - no power saving mechanisms
  - Does not provide any time delivery guarantee.
- Slotted CSMA-CA:
  - Adopts coordinated periodic sleeping
  - Achieves higher energy efficiency
  - Better copes with time delivery constrains.

Energy Saving Methods

- Connected dominating set approaches
- MAC layer approaches
- Cross layer approaches
- Topology control

Cross Layer Approaches

- Higher layers Information can be combined with MAC layer approaches to achieve higher energy savings.
- The Network and the Application layer in particular have much better information on:
  - Actual communication patterns,
  - Multihop data paths
  - Associated data rates
- This information can be used to obtain better radio activation schedules.

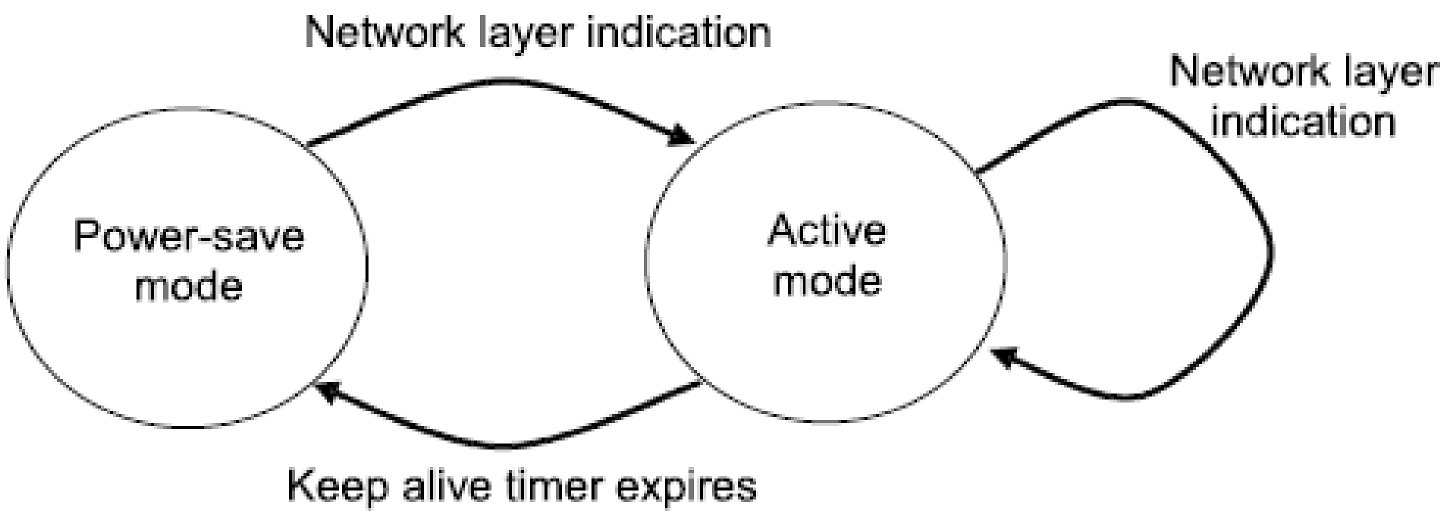
Cross Layer Approaches

- Methods:
  - Network support
  - Tree-based stream scheduling
  - Flexible stream scheduling

Cross Layer Approaches: Network Support

- Use network layer information to drive a MAC layer supporting active and power-save modes.
- Communication is possible only after the node is woken up and it transitions in the active mode.
- Arrival of Network layer messages fires a transition to active mode and starts a keep alive timer.
- As long as actual data messages arrive the timer is refreshed and the node remains in active mode.
- Timer expiration indicates that no more traffic is expected and the node may transition back to power-save mode.

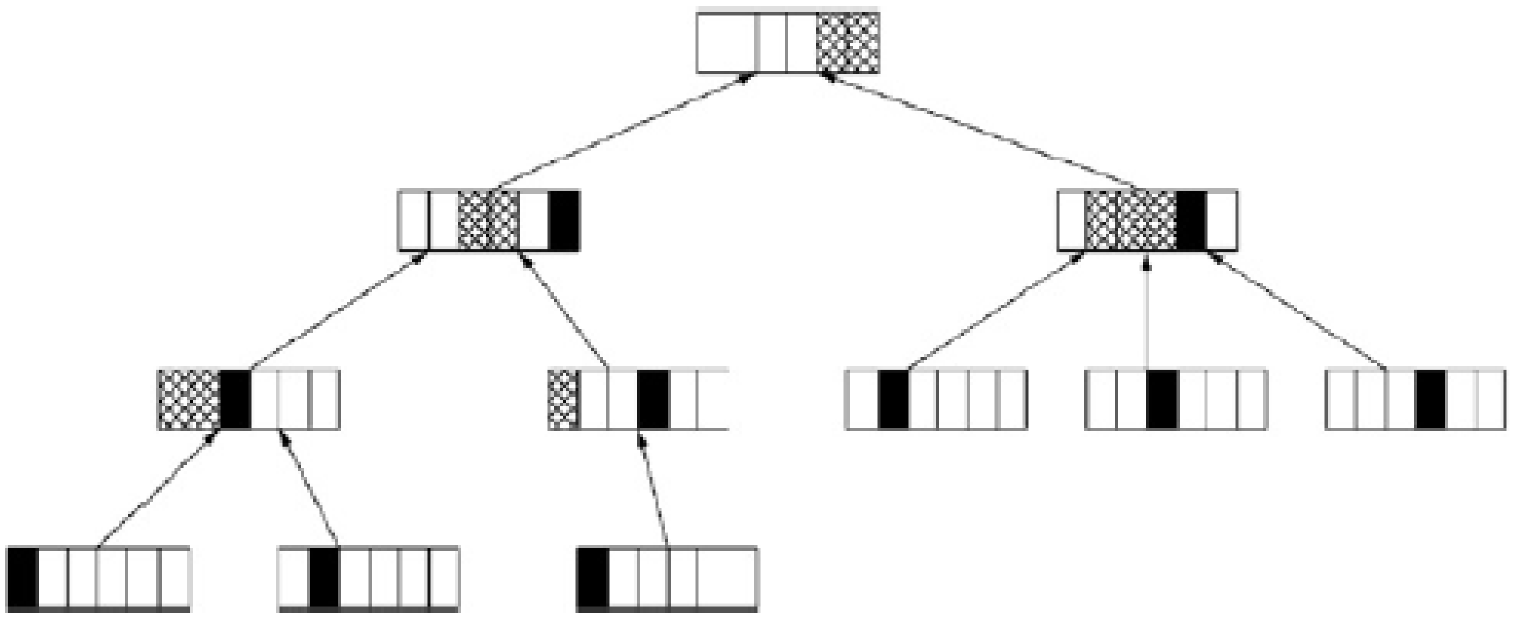
Cross Layer Approaches: Network Support



Cross Layer Approaches: Tree-based Stream Scheduling

- In trivial data gathering applications, nodes sample data from the environment and send them to the sink.
- In this leaf-to-root tree communication pattern, child to parent communication can be optimized by a sort of slot scheduling.
- Time is divided into periods each one consisting of fixed-size slots
- A node wishing to send or forward data to the sink must reserve a slot in the parent’s schedule
- Once reserved, a slot data transmission suffers no collisions.

Cross Layer Approaches: Tree-based Stream Scheduling



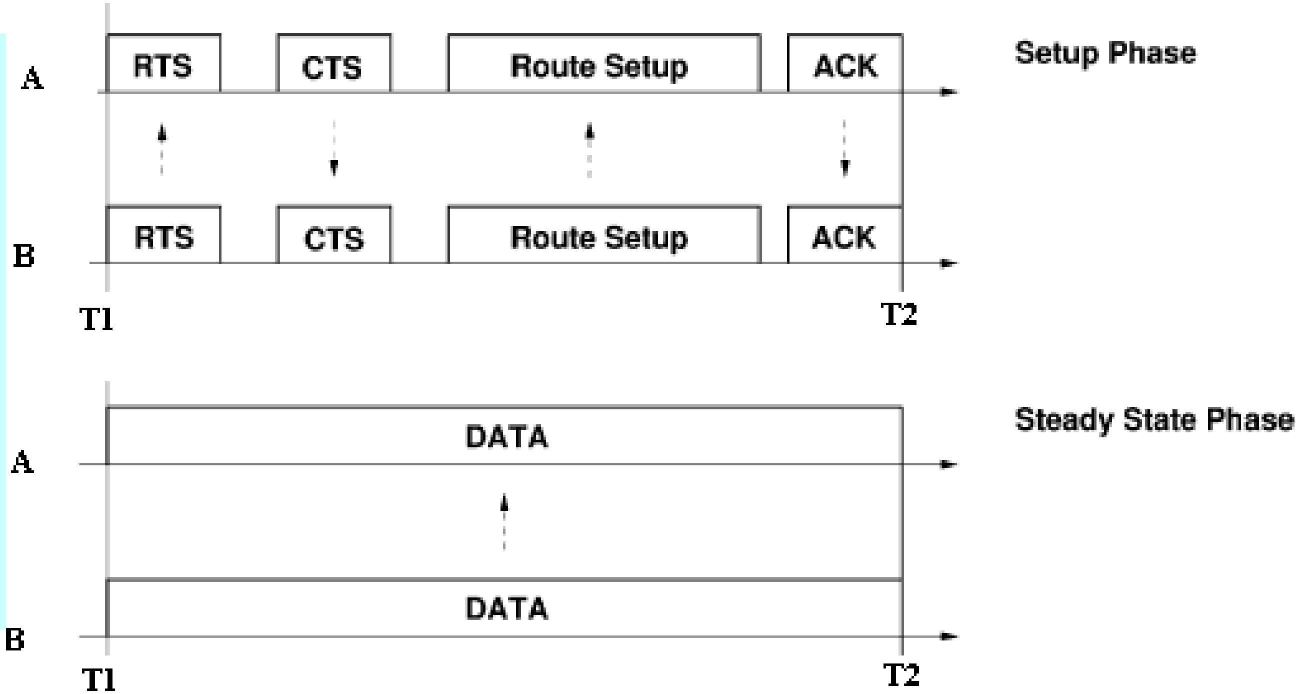
Cross Layer Approaches: Flexible Stream Scheduling

- Using a more flexible dynamic scheduling approach that easily extends to peer-to-peer communication.
- It is not limited to fixed size slots
- Protocol operation contemplates two phases for each data stream:
  - Setup/Reconfiguration phase:
    - Data path is established with the help of the Network layer and a RTS/CTS/RouteSetup/ACK
  - Steady State phase

Cross Layer Approaches: Flexible Stream Scheduling

•In the Setup Phase node A, reserves time interval [T1, T2] with a RTS/CTS/RouteSetup /ACK protocol

•In the Steady State Phase A, uses intervals [T1, T2] to send data packets to B.



Energy Saving Methodes

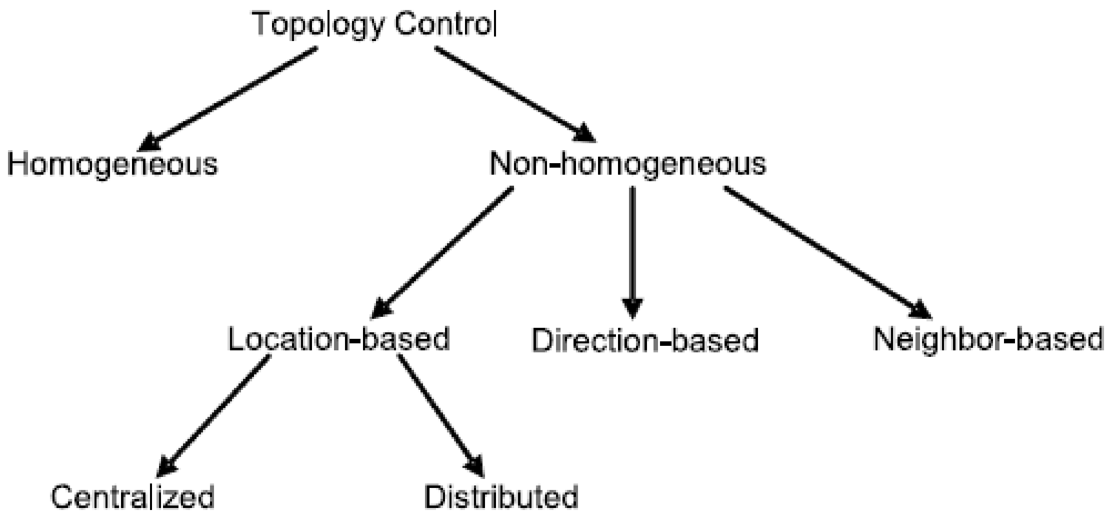
- Connected dominating set approaches
- MAC layer approaches
- Cross layer approaches
- Topology control

Topology Control

- In wireless sensor networks, the use of topology control mainly focuses on two aspects:
  - Extending network lifetime by reducing node energy consumption
    - The shortest path may not always be the most energy efficient
    - In this case topology control can be used to remove energy-inefficient links between nodes.
  - Increasing network capacity
    - Topology control can be used in this case to optimize signal strength in order to reduce the interferences and thus improve network capacity

Topology Control

- Two main approaches for topology control are:
  - Homogeneous power assignment.
  - Non-homogenous power assignment



Homogeneous Transmission Range Assignment

- Transmission range is the same for all nodes despite the fact that the radio transmission is also dependent on the propagation environment.
- The implementation of the topology control mechanism can be simplified to calculating the Critical Transmission Range (CTR) of the network.

Non Homogeneous Transmission Range Assignment

- Different nodes are assigned different transmission powers and consequently different transmission ranges.
- Nodes adjust their transmission power based on locally available information.
- Non-homogeneous transmission range assignment can be further subdivided into:
  - Location-based,
  - Direction-based,
  - Neighbour-based.

Location-based Topology Control

- Nodes are aware of their physical location.
- Two approaches:
  - Centralized approaches:
    - This information is collected by a single node which uses an optimization algorithm to select the transmission power of each node.
  - Distributed approaches:
    - This information is exchanged between nodes to compute an almost optimal power assignment.

Direction-based topology control

- It is assumed that the nodes do not know their position.
- Instead, their directions are made available using angle-of-arrival techniques.

Neighbour-based Topology Control

- Nodes will be connected to its k closest neighbours.
- A typical protocol in this type of topology control is the K-NEIGH protocol.
- The basic idea is to keep the number of neighbours per node around an optimal value k.
- The K-NEIGH protocol is distributed and generates a connected graph with high probability.
- Nodes announce their ID at high transmission power to discover potential neighbours.
- Neighbours will then be sorted by their separation distance.
- The k nearest neighbour that can mutually reach each other use the smallest transmission power that is sufficient to reach all of them.