TIWSNE – Wireless Sensor Networks and Electronics – (2015-Q4)

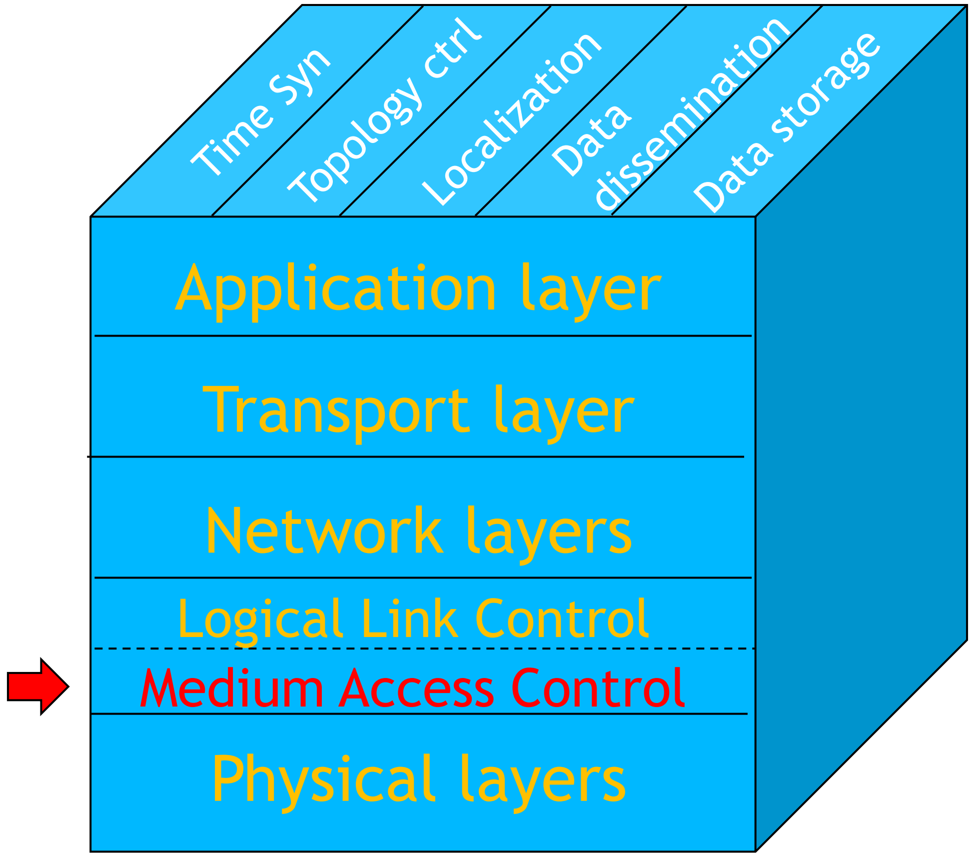
Lecture
Medium Access Control Protocols in WSN

Qi Zhang

(Email: qz@eng.au.dk; Edison 314)

AARHUS SCHOOL OF ENGINEERING

Relevant topics in WSN



Outline

- ***Principal options and challenges***
- Contention-based protocols
- Schedule-based protocols
- IEEE 802.15.4

AARHUS SCHOOL OF ENGINEERING

Objectives of WSN MAC Protocols

- Collision Avoidance
- Energy Efficiency
- Scalability
- Latency
- Fairness
- Throughput
- Bandwidth Utilization

Objectives of WSN MAC Protocols

- **Collision Avoidance**
- **Energy Efficiency**
- **Scalability**
- Latency
- Fairness
- Throughput
- Bandwidth Utilization

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

ASE | AARHUS SCHOOL OF ENGINEERING

Challenges for MAC in WSNs-1

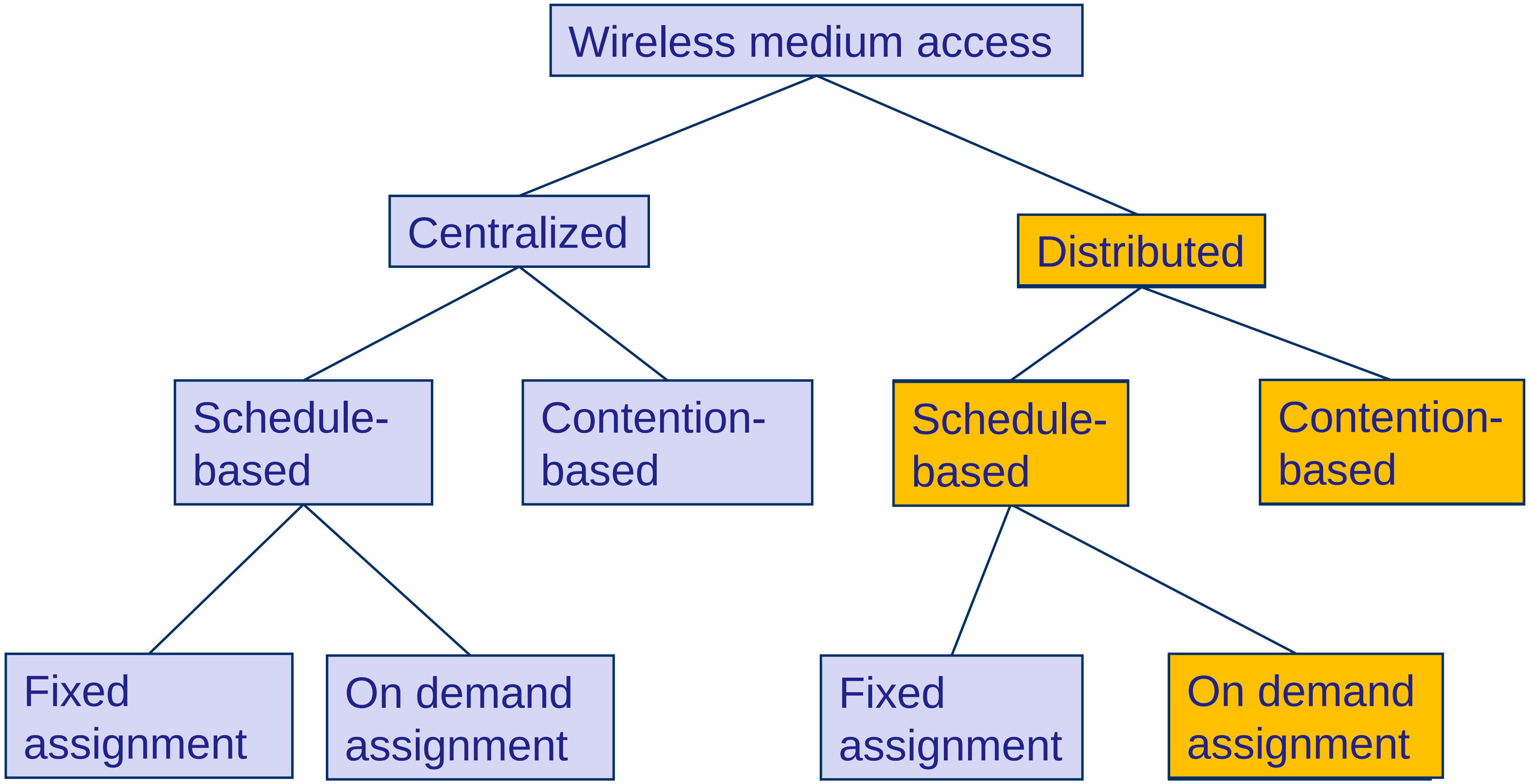
- WSN Architecture
  - High density of nodes
  - Increased collision probability
- Limited Energy Resources
  - Connectivity and the performance of the network is affected as nodes run of energy or malfunction
  - Frequent power up/down eats up energy
    - Prevent frequent radio state changes (active<->sleep)
  - Need very low power MAC protocols
  - Minimize signaling overhead
  - Avoid idle listening

Challenges for MAC in WSNs-2

- Limited Processing and Memory Capabilities
  - Complex algorithms cannot be implemented
  - Centralized or local management is limited
  - Simple scheduling algorithms required
  - Cross-layer optimization required
  - Self-configurable, distributed protocols required
- Limited Packet Size
  - MAC protocol overhead should be minimized
- Cheap Encoder/Decoders
  - Inaccurate Clock Crystals
  - Synchronization problems
  - TDMA-based schemes might not be practical

AARHUS SCHOOL OF ENGINEERING

Classes of MAC protocols



AARHUS SCHOOL OF ENGINEERING

Centralized medium access

- Idea: Having 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
- However, it can be quite useful when network is somehow divided into smaller groups
  - Clusters, in each cluster medium access can be controlled centrally – compare Bluetooth pico-nets, for example

In WSN, distributed medium access is usually considered

Schedule-based MAC

- A ***schedule*** exists, regulating which participant may use which resource at which time slot
- Typical resource: frequency band in a given physical space
- Schedule can be ***fixed*** or computed ***on demand***
- Usually, collisions, overhearing, idle listening no issues
- Needed: time synchronization!

Contention (Random)-Based MAC Protocols

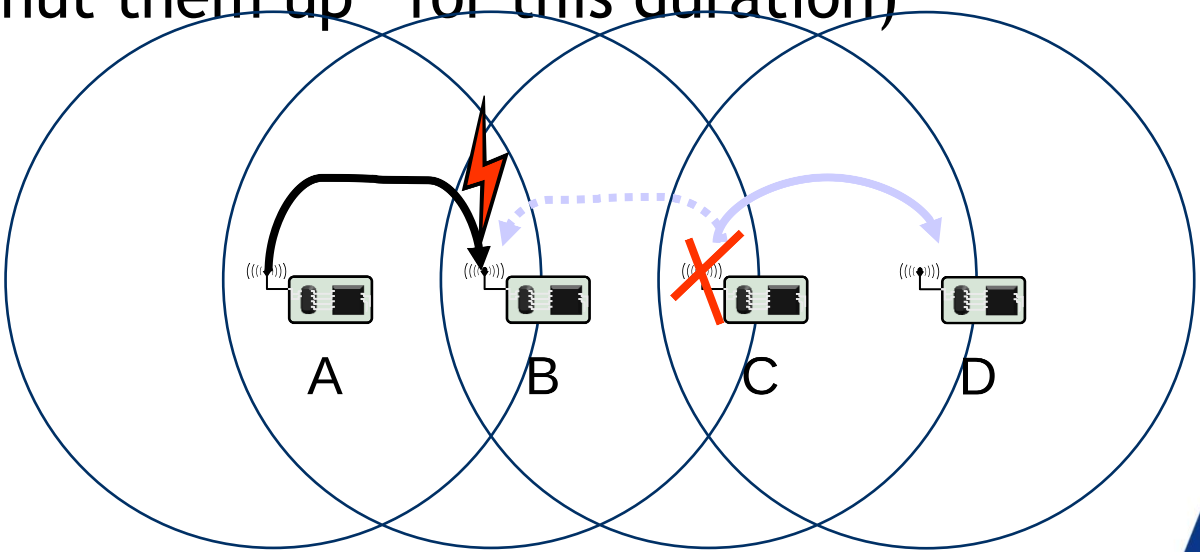
- Provide robustness and scalability to the network.
- Collision probability increases with increasing node density
- Mechanisms to handle/reduce probability/impact of collisions required
  - Channel access through carrier sense mechanism

Outline

- Principal options and challenges
- ***Contention-based protocols***
  - ***CSMA/CA***
  - S-MAC
  - B-MAC
- Schedule-based protocols
- IEEE 802.15.4

Carrier Sense Multiple Access-Collision Avoidance (CSMA/CA)

- Listen before talk
- However, it suffers from ***sender*** not aware what is going on at its ***neighbors***. It might destroy packets despite first listening for a while
- Hence, receiver additionally needs to inform possible senders in its vicinity about impending transmission (to "shut them up" for this duration)



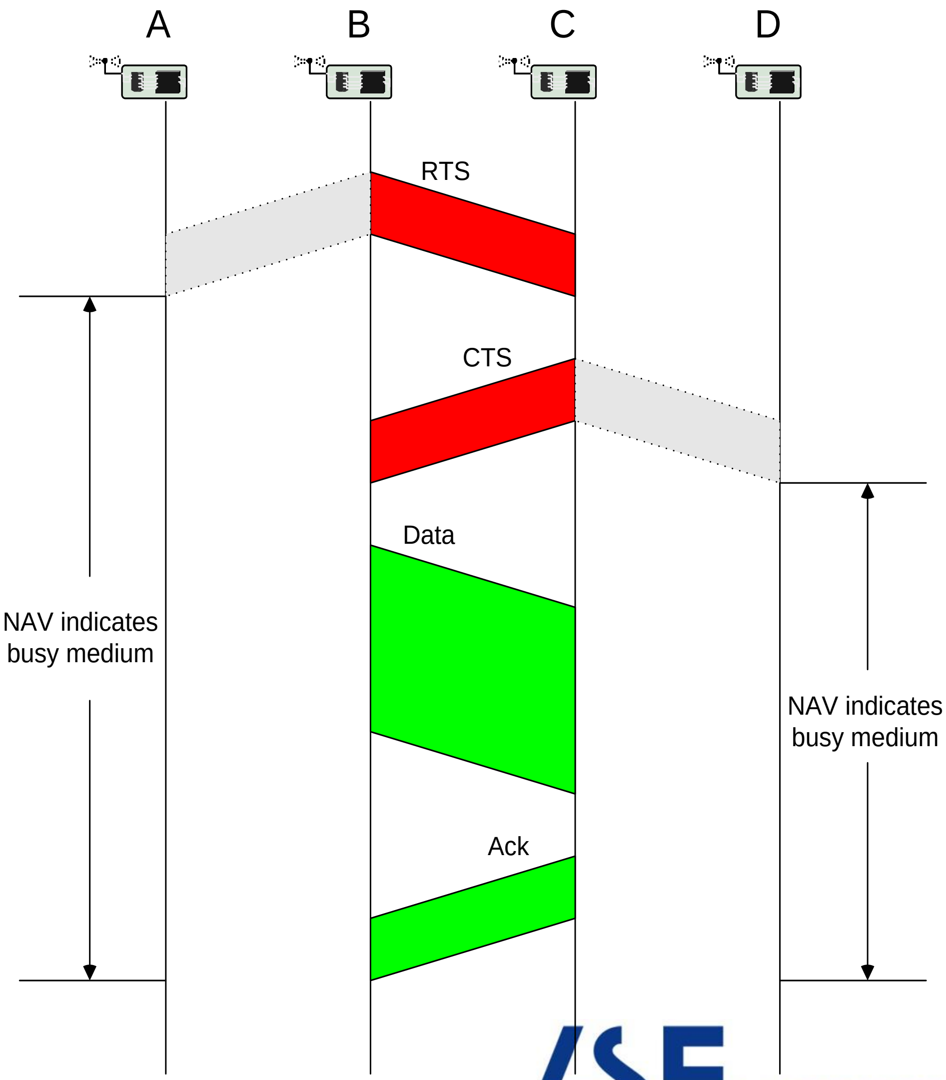
AARHUS SCHOOL OF ENGINEERING

RTS/CTS

- Use <u>short signaling packets</u> for Collision Avoidance
  - Smaller control packets lessen the cost of collision
  - RTS (Request To Send) Packet: A sender requests the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (Clear To Send) Packet: The receiver grants the right to send as soon as it is ready to receive
  - They contain
    - Sender Address
    - Receiver Address
    - Packet Size
  - RTS + CTS provide "virtual" carrier sense which protects against hidden terminal collisions

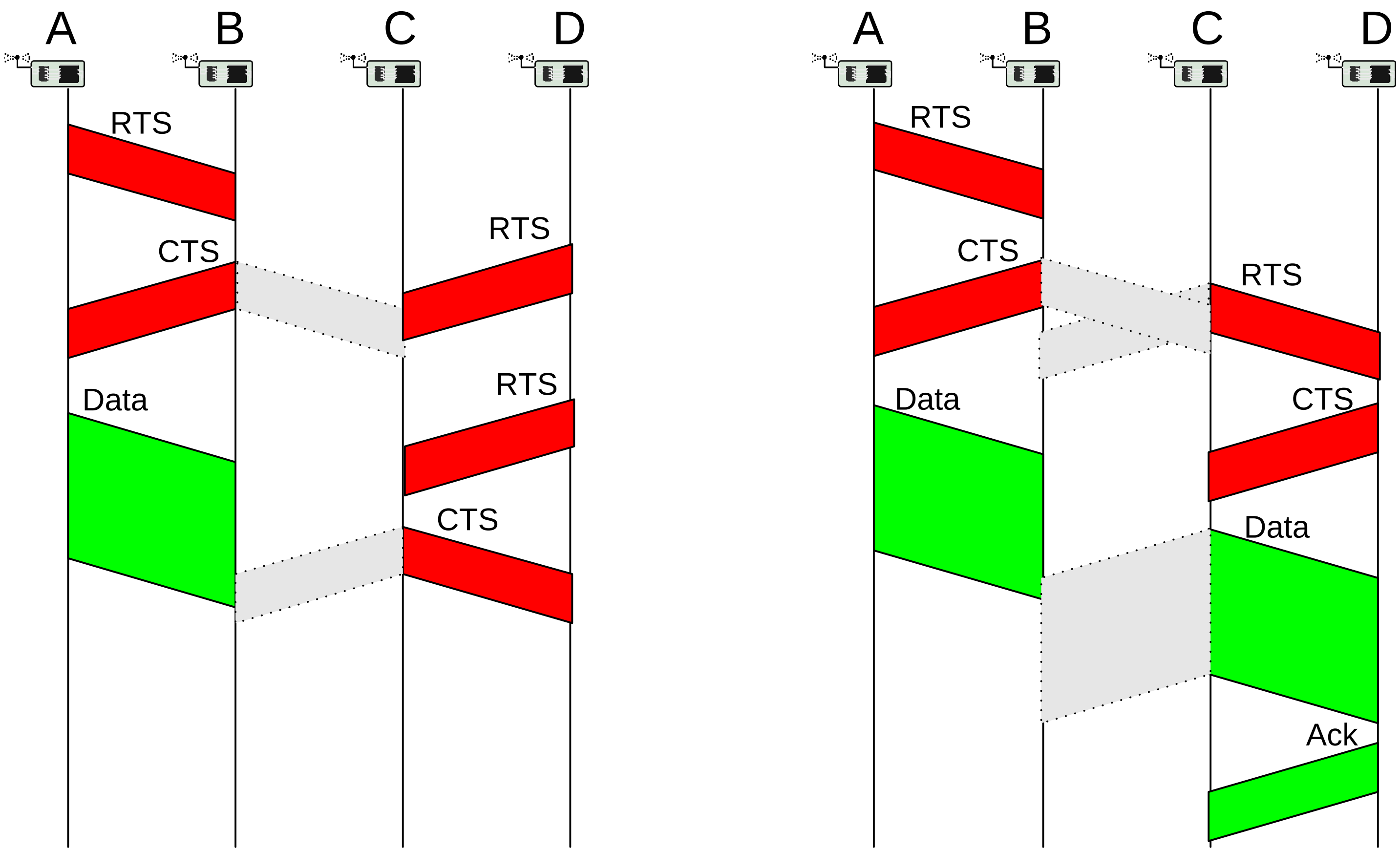
Transmission with RTS/CTS

- 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 (NAV)***
- B sends data, C ACKs



Hidden Terminal problem cases

- Hidden node problem cases:



Outline

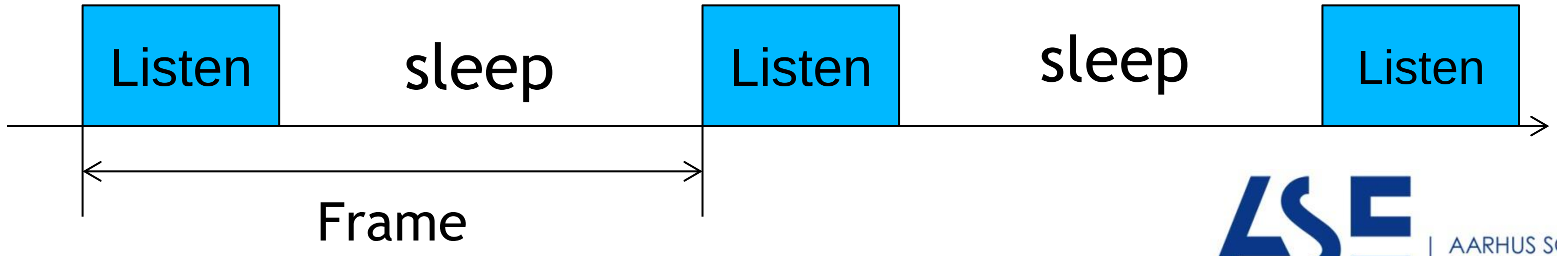
- Principal options and challenges
- ***Contention-based protocols***
  - CSMA/CA
  - ***S-MAC***
  - B-MAC
- Schedule-based protocols
- IEEE 802.15.4

S-MAC

Wei Ye et al. “Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks” IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 12, NO. 3, JUNE 2004

- Problem: “Idle Listening and overhear” consumes significant energy

- Solution: Periodic listen and sleep
  - Trades energy efficiency for lower throughput and higher latency
  - Nodes can go to sleep during other nodes transmissions
  - During sleeping, radio is turned off. Only in these ***active periods***, packet exchanges happen



S-MAC details

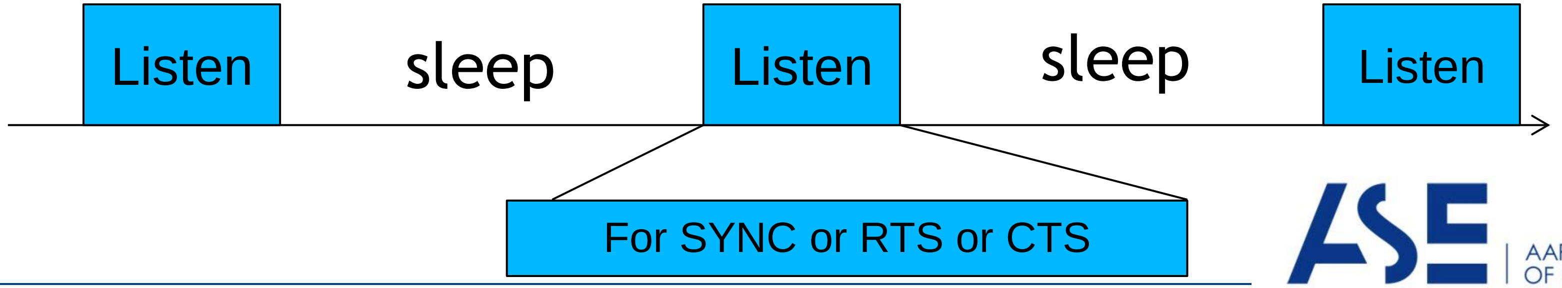
- Each node goes into periodic sleep mode during which it switches the radio off and sets a timer to awake later
- When the timer expires it wakes up and listens to see if any other node wants to talk to it
- The duration of the sleep and listen cycles are application dependent
  - They are set the same for all nodes
- A periodic synchronization among nodes is required as there are different types clock drift
  - By periodic exchange SYNC packets
  - Receivers will adjust their timer counters immediately after they receive the SYNC packet

SYNC packet format:

Sender Node ID	Next Sleep Time

S-MAC Periodic Sleep and Listen

- Listen interval
  - Normally fixed according to PHY and MAC parameters,
    - E.g. radio bandwidth, contention window size
  - Essentially used for exchange RTS/CTS between sender and receiver
  - Used to exchange wakeup schedule between neighbors by broadcasting SYNC packets
    - The period of a node sending a SYNC packet is called *synchronization period*.
    - Synchronization period often consists of many listen-sleep periods
- Sleep interval
  - It can be changed according to different application requirements



Collision Avoidance in S-MAC

- S-MAC is based on contention
  - i.e., if multiple nodes want to talk to a node at the same time, they will contend to send during the listening phase of the receiver.
  - Similar to CSMA/CA, i.e. use RTS/CTS mechanism to address the hidden terminal problem.
  - Perform carrier sense before initiating a transmission.
    - Both physical carrier sensing and virtual sensing (NAV) are needed
  - If a node fails to get the medium, it goes to sleep and wakes up when the receiver is free and listening again.
  - Broadcast packets are sent without using RTS/CTS.
  - Unicast data packets follow the sequence of RTS/CTS/DATA/ACK between the sender and receiver
  - Two nodes can use their normal sleep time for data transmission after successfully exchanging RTS/CTS, until data transmission finishes

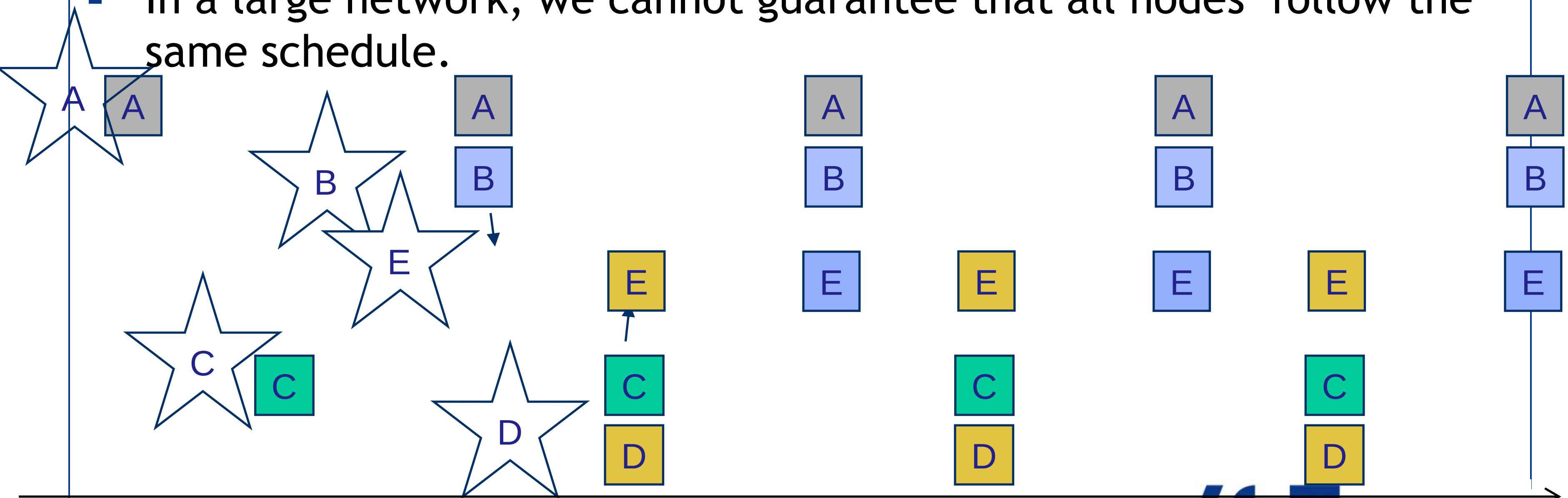
AARHUS SCHOOL OF ENGINEERING

S-MAC Synchronization Maintenance

- Each node maintains a schedule table that stores schedules of all its known neighbors
- Steps to choose schedule and establish schedule table
  - A node first listens to the medium for a certain amount of time (at least the synchronization period)
  - If it does not hear a schedule from another node, it randomly chooses its own schedule and broadcasts its schedule with a SYNC packet immediately. This node is called a Synchronizer
  - If a node receives a schedule from a neighbor before choosing its own schedule,
    - it just follows this neighbor's schedule, i.e. becomes a Follower
    - it broadcasts its schedule at its next scheduled listen time
  - If a node receives a different schedule after it chooses and announces its own
    - If it has no neighbors, it discard its current schedule
    - Otherwise, it adopts both schedules

S-MAC synchronized islands

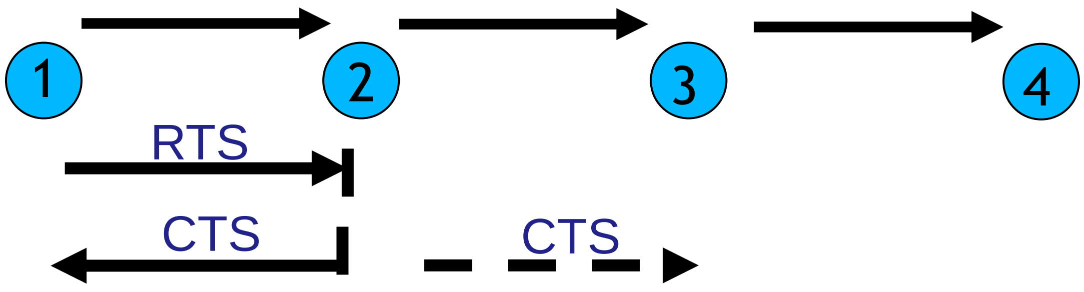
- If additional nodes join, some nodes at border might learn about two different schedules from different nodes
  - “Synchronized islands”
  - To bridge this gap, it has to follow both schedules.
  - Border nodes have less sleeping time and consumes more energy
- In a large network, we cannot guarantee that all nodes follow the same schedule.



AARHUS SCHOOL OF ENGINEERING

Adaptive Listening Feature

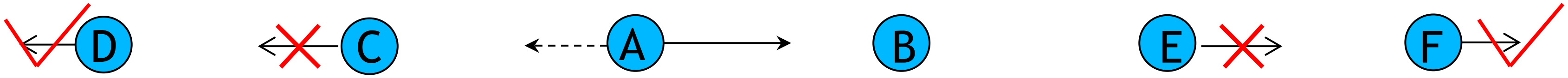
- Purpose: Reduce multi-hop latency due to periodic sleep
- BASIC IDEA: Let the node who overhears its neighbor's transmission stay awake instead of following the periodic sleep schedule.
  - From the duration field in the RTS and CTS, neighbors at both sides know the transmission time.
  - They adaptively wake up when the transmission is over.



  - e.g., CTS of node 2 is heard by node 3 also. Node 3 remains awake!! So node 3 can immediately forward packet to node 4, if node 4 is stilling listening.
  - It can reduce latency by at least half

Overhearing Avoidance

- S-MAC tries to avoid overhearing by letting interfering nodes go to sleep after they hear RTS/CTS
  - Each node maintains NAV from RTS/CTS
  - Each node should sleep if NAV is not zero
  - This prevent neighbors from overhearing DATA packets and ACKs



Message Passing

- A message is defined as the collection of meaningful, interleaved units of data
- A receiver usually needs to obtain all the data units before in-network processing such as aggregation
- However, a packet with long message has higher probability to get corrupted.
- Solution:
  - Fragment the long message into many small fragments, transmit them in a burst
  - Only one pair RTS/CTS is used to reserve the channel
  - The neighbors go to sleep when receiving RTS/CTS or ACK
  - Receiver sends an ACK for each fragment
  - If a node wakes up or a new node joins in the middle of a burst transmission, it can go to sleep by hearing ACK

Energy Consumption Performance

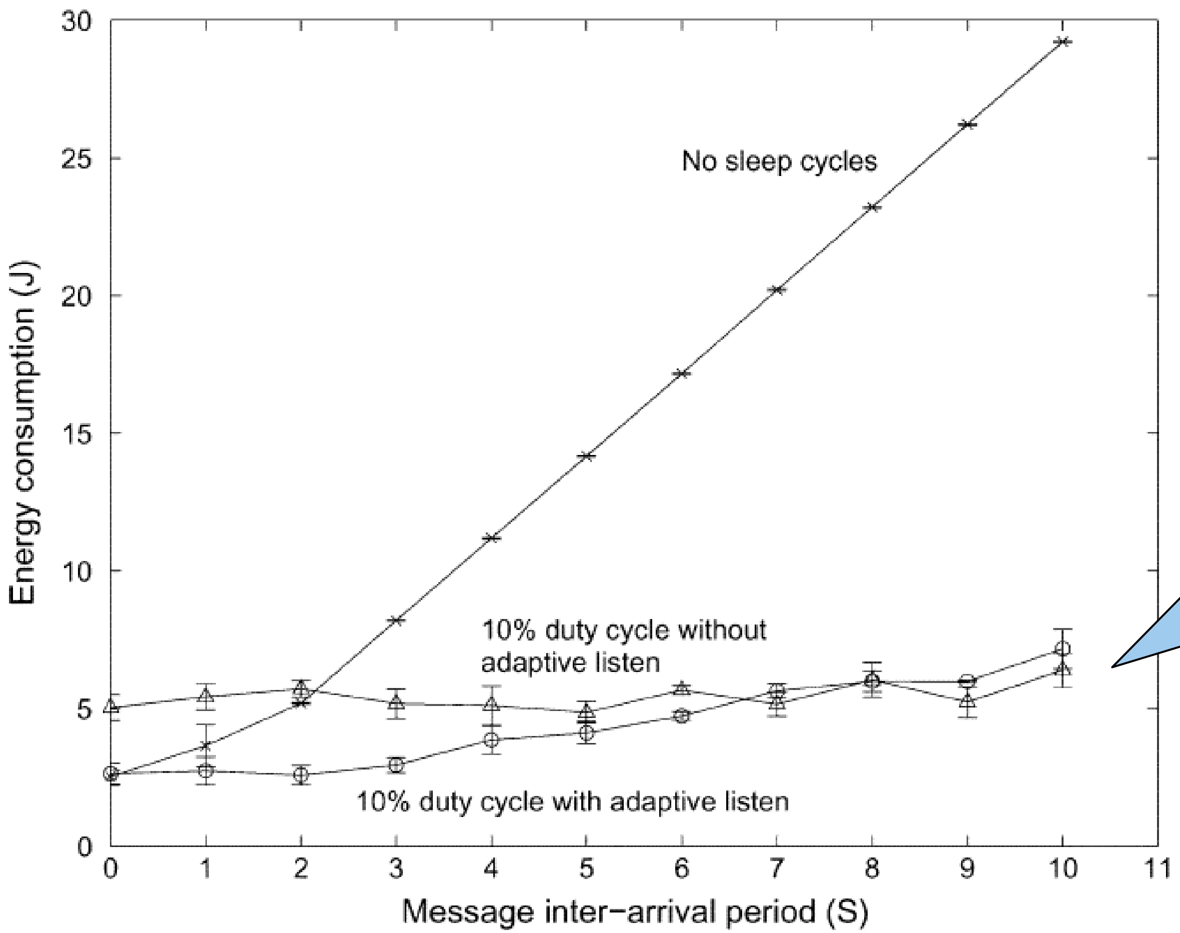
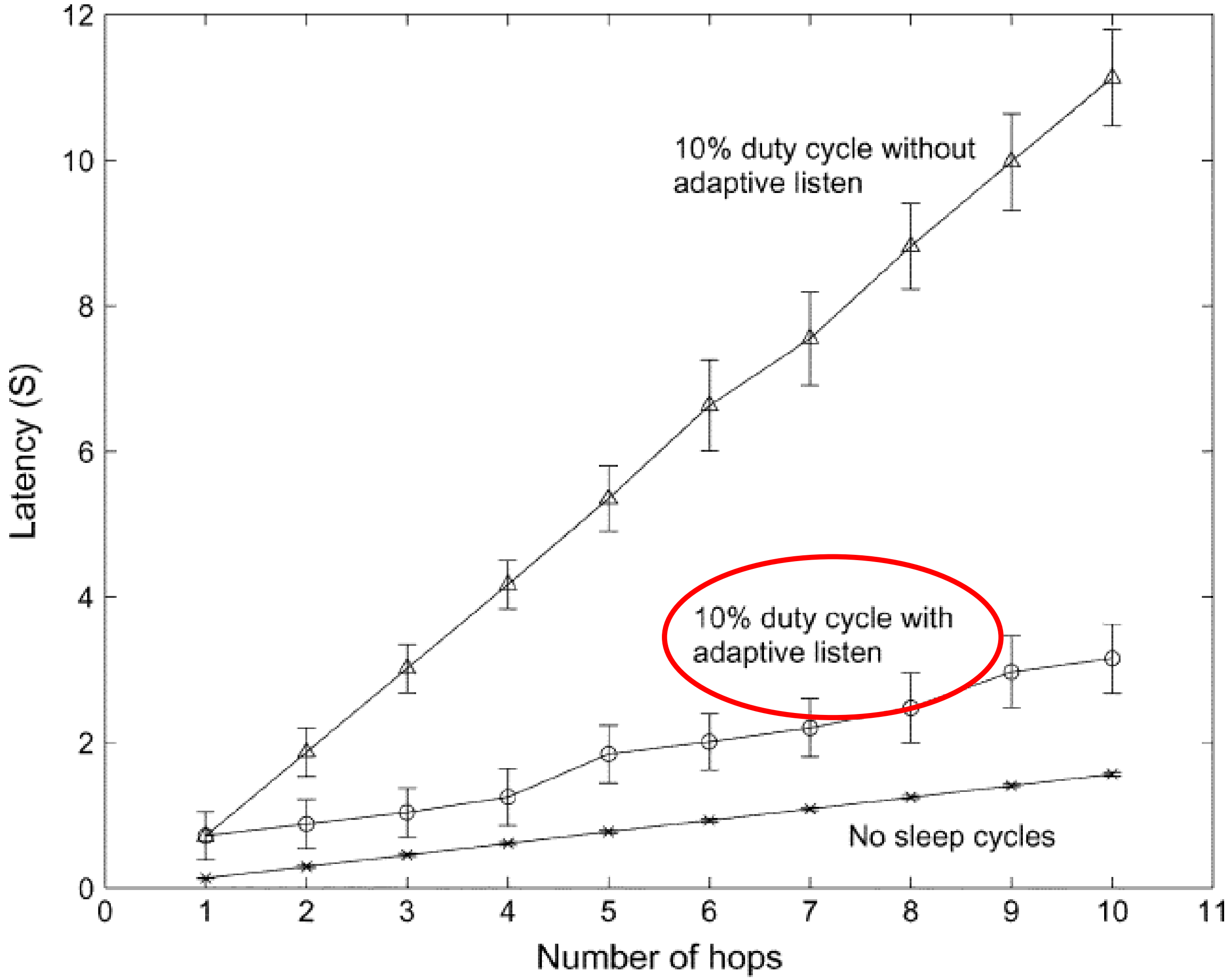


Fig. 10. Aggregate energy consumption on radios in the entire ten-hop network using three S-MAC modes.

The extra energy cost by Adaptive Listening is trivial.

Latency Performance



Outline

- Principal options and challenges
- ***Contention-based protocols***
  - CSMA/CA
  - S-MAC
  - ***B-MAC***
- Schedule-based protocols
- IEEE 802.15.4

B-MAC

J. Polastre, J. Hill, D. Culler, “Versatile Low Power Media Access for WSNs”, Proc. of ACM SenSys, Nov. 2004

- Design goals of B-MAC
  - Effective Collision Avoidance
  - Efficient Channel Utilization
  - Scalable to Large Numbers of Nodes
  - Reconfigurable by Network Protocols
  - Tolerant to Changing RF/Networking Conditions
  - Simple Implementation, Small Code and RAM Size

B-MAC Design Highlight

- Keep core MAC simple
- Provides basic CSMA access
- Optional link level ACK, no link level RTS/CTS
- CSMA backoffs configurable by higher layers
- Carrier sensing using Clear Channel Assessment (CCA)
- Sleep/Wake scheduling using Low Power Listening (LPL)

Clear Channel Assessment

- For effective collision avoidance, MAC must accurately determine if the channel is clear.
  - Need to tell what is noise and what is a signal
  - Ambient noise is prone to environmental changes
- Find out whether the channel is idle
  - If too pessimistic: waste bandwidth
  - If too optimistic: more collisions
- Key observation:
  - Packet reception has fairly constant channel energy
  - Ambient noise may change significantly depending on the environment
- B-MAC solution:
  - Software approach to estimate the noise floor (software automatic gain control)

Clear Channel Assessment

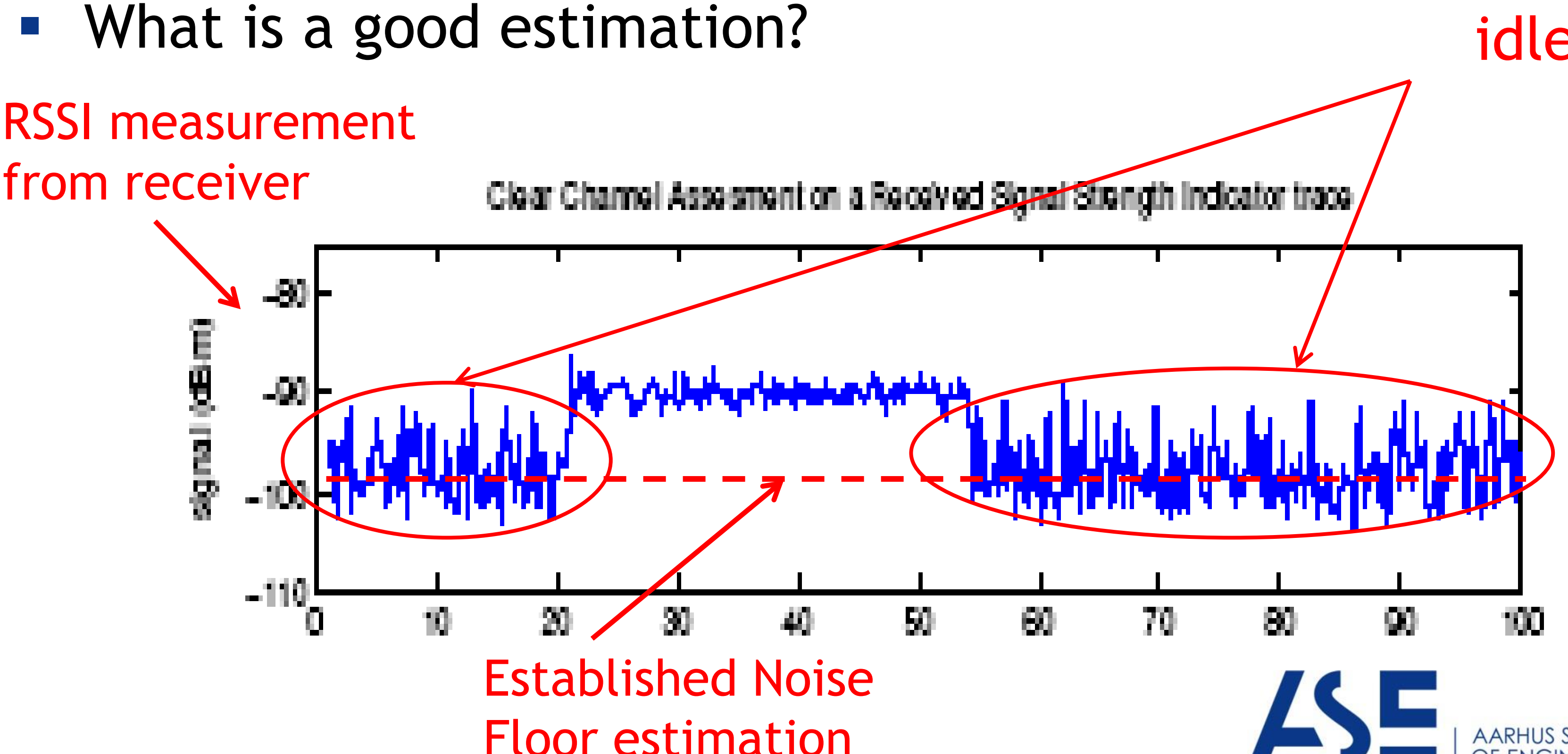
- Take a signal strength sample when the channel is assumed to be free/idle.
  - WHEN? Right after a packet is transmitted or when no valid data is received
  - Samples are entered into a FIFO queue.
  - Median of the queue is added to an exponentially weighted moving average (EWMA) with decay α.
  - Median signal strength is used as a simple low pass filter to add robustness to the noise floor estimate.
  - $S_m(t) = \alpha * S(t) + (1 - \alpha) * S_m(t-1)$
    - $S_m(t)$: EWMA at time t
    - $S(t)$: Signal strength of ambient noise at t
    - $S_m(t-1)$: EWMA at time t-1
    - where α value is assumed to be 0.06 and FIFO queue size of 10.

AARHUS SCHOOL OF ENGINEERING

CCA (Clear Channel Assessment)

- Once estimate of the noise floor is established,
  - TX requests to start monitoring the received signal from the radio (i.e, to assess if channel is clear)

- What is a good estimation?



CCA: Single-Sample Thresholding vs Outlier Detection

- Common approach: take single sample, compare it to the noise floor, i.e., single-sample thresholding
  - Large number of false negatives → lower effective channel utilization
- B-MAC uses outlier detection
  - search for outliers in received signal (RSSI)
  - If a sample has significantly lower energy than the noise floor during the sampling period, then the channel is clear
  - If 5 samples are taken and no outlier is found, the channel is busy.
  - Fully utilize the channel since a valid packet has no outlier significantly below the noise floor

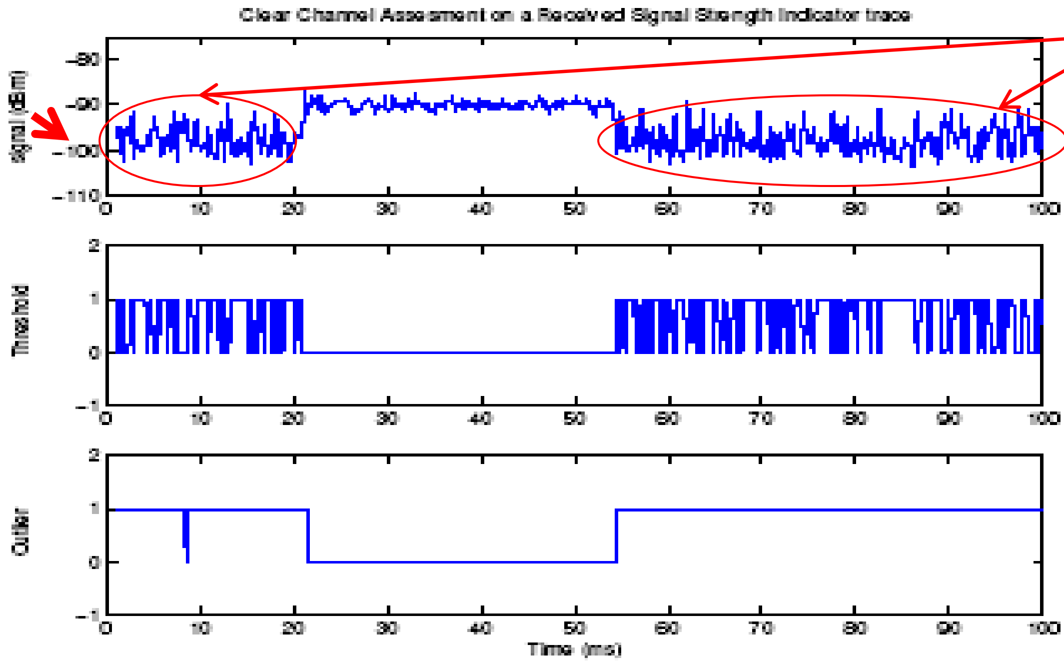
Single-Sample Thresholding vs Outlier Detection

RSSI measurement from receiver

Single-Sample Thresholding

Outlier Detection

Idle



- A packet arrives between 22 and 54ms.
- Y-axis: 1: channel clear, 0: channel busy
- The middle graph shows the output of single-sample thresholding algorithm
- Bottom shows the output of an outlier detection algorithm

Clear Channel Assessment

- CCA can be turned on/off
- If turned off, a schedule-based protocol can be implemented above B-MAC
- If turned on, B-MAC uses an initial channel backoff when sending a packet
  - After the initial backoff, the CCA outlier detection algorithm is run.
    - If the sample is below the current noise floor, channel clear, send immediately.
    - If five samples are taken, and no outlier found =>channel busy, take a random backoff (congestion backoff)
  - Noise floor updated when the channel is known to be clear, e.g., just after packet transmission

ASE | AARHUS SCHOOL OF ENGINEERING

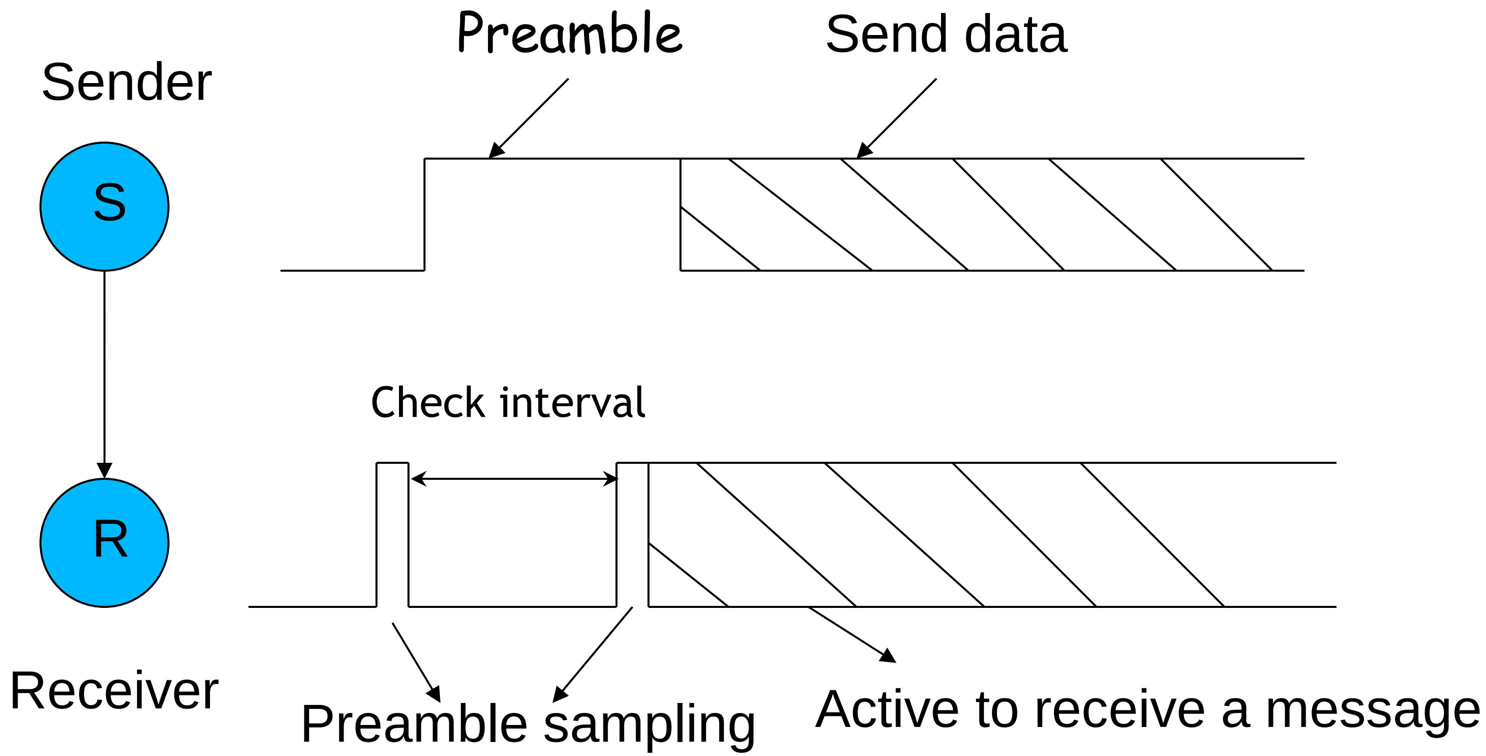
Low Power Listening

- Goal: minimize listening cost
- Principles
  - Node periodically wakes up, turns radio on and checks channel
  - If activity on the channel is detected, node powers up and stays awake for the time required to receive the incoming packet
  - Node goes back to sleep
    - If a packet is received
    - After a timeout, (if no packet received, i.e., a false positive)
  - Preamble length of a packet matches channel checking period
    - No explicit synchronization required
  - Noise floor estimation is also used to detect channel activity during LPL

AARHUS SCHOOL OF ENGINEERING

Lower Power Listening: Preamble Sampling

- Preamble is not a packet but a physical layer RF pulse
  - Minimize overhead



|Preamble| ≥ Sampling period (check interval)

Check Interval for Channel Activity

- To reliably receive data, the preamble length is matched to the interval that the channel is checked for activity.
- If the channel is checked for every 100 ms, the preamble must be at least 100 ms long for a node to wake up, detect activity on the channel, receive the preamble and then receive the message.
- Sampling rate (traffic pattern) defines optimal check interval
- Check interval
  - Too small: energy wasted on idle listening
  - Too large: energy wasted on transmissions (long preambles)

Comparison of S-MAC and B-MAC

	S-MAC	B-MAC
Collision avoidance	CSMA/CA	CSMA
ACK	Yes	Optional
Message passing	Yes	No
Overhearing avoidance	Yes	No
Listen period	Pre-defined + adaptive listen	Pre-defined
Listen interval	Long	Very short
Schedule synchronization	Required	Not required
Packet transmission	Short preamble	Long preamble
Code size	6.3KB	4.4KB (LPL & ACK)

Outline

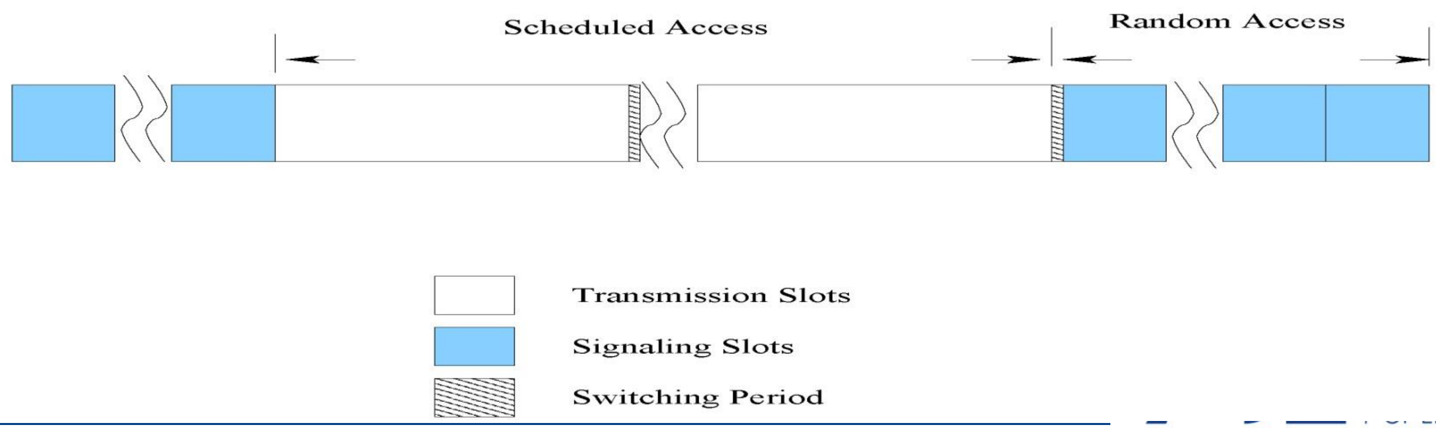
- Principal options and challenges
- Contention-based protocols
  - CSMA/CA
  - S-MAC
  - B-MAC
- ***Schedule-based protocols***
  - *TRAMA*
- IEEE 802.15.4

TRAMA: TRaffic-Adaptive Medium Access Protocol

Venkatesh Rajendran et al. "Energy Efficient, Collision Free Medium Access Control for Wireless Sensor Networks", *SenSys'03*, November 5–7, 2003, Los Angeles, California, USA

- Nodes are synchronized
- Time divided into cycles, divided into
  - Random access periods
    - Used for signaling: e.g., synchronization and updating two-hop neighbor information. Collision possible!!
  - Scheduled access periods
    - Used for contention-free data exchange between nodes.
    - Supports unicast, multicast and broadcast communication.

A time-slotted structure



TRAMA Components

- Neighbor Protocol (NP)
  - Gather 2-hop neighborhood information
- Schedule Exchange Protocol (SEP)
  - Gather 1-hop traffic information for SCHEDULING
- Adaptive Election Algorithm (AEA)
  - Elect transmitter, receiver and stand-by nodes for each transmission slot.
  - without any data to send are removed from the election process, thereby improving the channel utilization.

Neighbor Protocol (NP)

- Main Function:
  - Gather two-hop neighborhood information by periodic propagating one-hop neighbor information among neighboring nodes during the random access period.
  - Using Incremental neighbor updates to keep the size of the signaling packet small.
- Steps:
  - Sensors pick a random signaling slot and transmit a list of their one hop neighbors (to share topology information)
  - All sensors receive signaling messages from neighbors by listening during time slots in which they do not transmit.
  - As a result of NP, a sensor determines the network topology within a two hop neighborhood.
- Note: Collisions may occur for signaling messages, retransmissions take place.

Schedule Exchange Protocol (SEP)

- SEP establishes and maintains schedule based on the current traffic info at the node
- The node periodically broadcasts its schedule info to its 1-hop neighbors during scheduled access by Schedule PACKETS and schedule summaries
  - Schedule consists of list of intended receivers for future transmission slots.

- The interval of broadcasting schedule info is calculated by each node based on its own generated traffic, called *schedule_interval*
- The node can pre-calculate the time slots (winning slots) that it can use among [t, t+*schedule_interval*] slots
- The last winning slot is used to announce the node's schedule by Schedule PACKETS

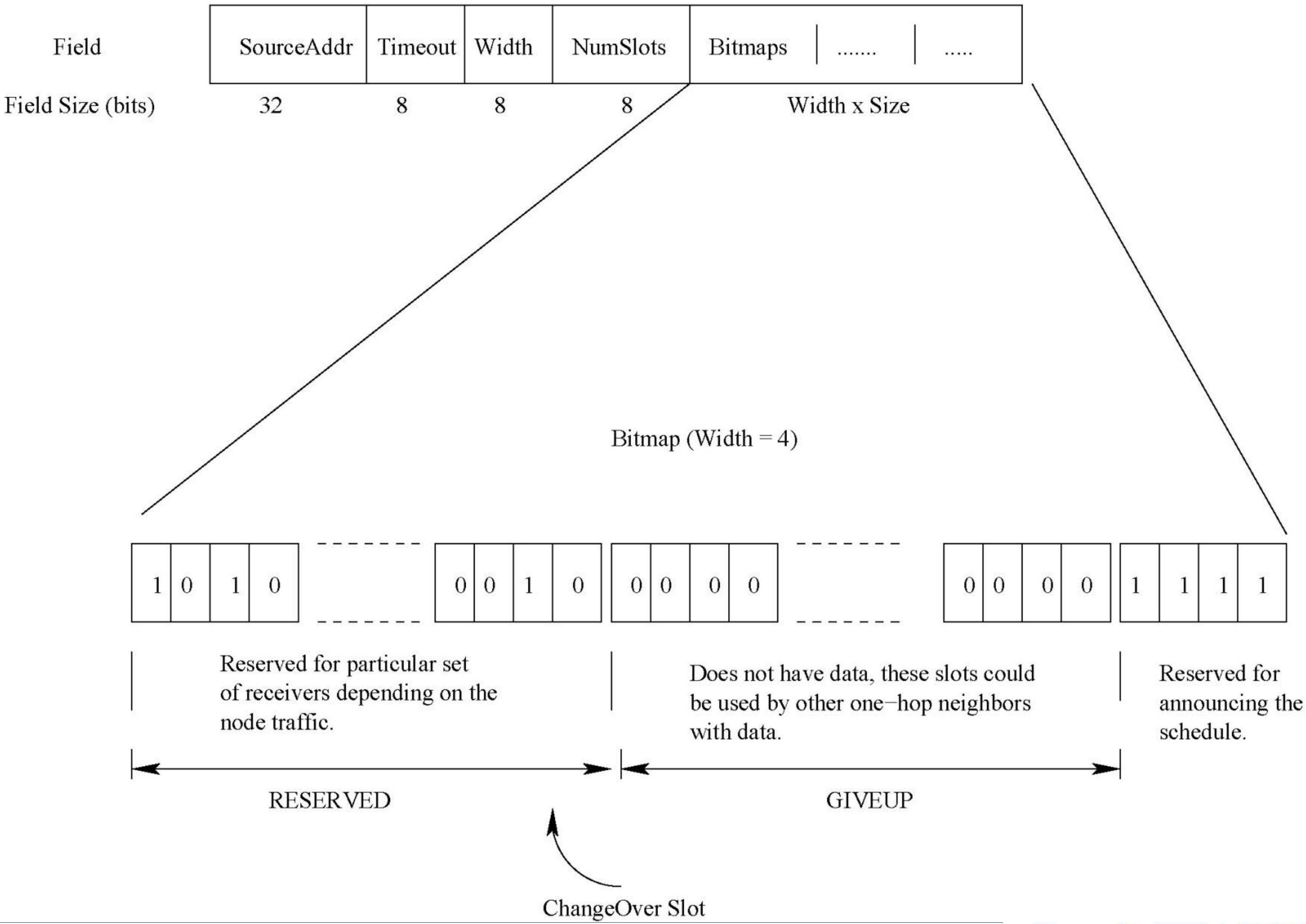
Schedule_interval

- EXAMPLE: Node_i's *schedule_interval* = 100 slots.
  - During time slot 1000, Node_i computes its winning slots between [1000,1100].
  - Assume: The winning slots are 1009, 1030, 1033, 1064, 1075, 1098.
  - Node_i uses slot 1098 to announce its next schedule by looking ahead from [1098,1198].

Schedule PACKETS

- Schedule PACKETS include
  - the number of slots the sensor owns in the next *schedule-interval* as determined by the Adaptive Election Algorithm (AEA)
  - A bitmap of the intended receivers
  - Data slots the sensor plans to use
- No need to send receiver addresses explicitly.
- Instead sensors convey the intended receiver information using a BITMAP!!
  - BITMAP: With the length equal to the number of one-hop neighbors.
  - Each bit corresponds to one particular receiver.
    - For example: One node with 4 neighbors 14,7,5 and 4, the BITMAP size = 4
    - For broadcast: all bitmap bits are set to 1.

Schedule Packet Format



SCHOOL
NEERING

Adaptive Election Algorithm

- Given: Each node knows its two-hop neighborhood and schedules of 1-hop neighbors
- How to decide which slot (in scheduled access period) a node can transmit?
  - Use node identifier x and globally known hash function h
  - For time slot t, compute priority $p = h(x \oplus t)$
  - Compute this priority for next k time slots for node itself and all two-hop neighbors (k= *schedule_interval*)
  - Node uses these time slots for which it has the highest priority

Priorities of node A and its two neighbors B & C

	t = 0	t = 1	t = 2	t=3	t = 4	t = 5
A	14	23	9	56	3	26
B	33	64	8	12	44	6
C	53	18	6	33	57	2

Comparison: TRAMA vs. S-MAC

- TRAMA Limitations:
  - Complex election algorithm and data structures.
  - Substantial memory/CPU requirements for schedule computation
  - Overhead due to explicit schedule propagation.
  - Higher queuing delay.
  - More energy consumption
- Comparison
  - Energy savings in TRAMA depend on the workload situation
  - Energy savings in S-MAC depend on duty cycle

Outline

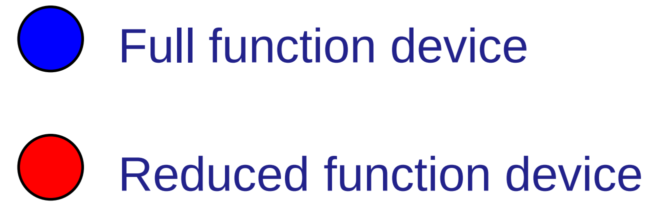
- Principal options and challenges
- Contention-based protocols
  - CSMA/CA
  - S-MAC
  - B-MAC
- Schedule-based protocols
  - TRAMA
- ***IEEE 802.15.4***

AARHUS SCHOOL OF ENGINEERING

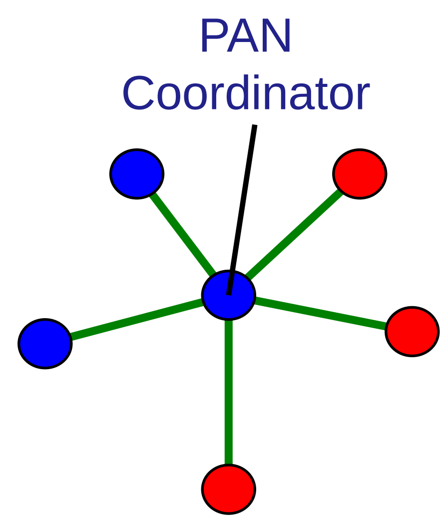
IEEE 802.15.4

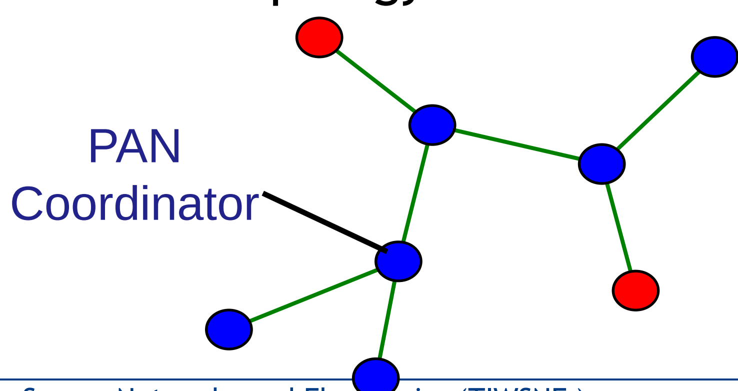
- IEEE standard for low-rate WPAN applications
- Goals:
  - low-to-medium bit rates,
  - moderate delays without too stringent guarantee requirements,
  - low energy consumption
- Physical layer
  - 20 kbps over 1 channel @ 868-868.6 MHz
  - 40 kbps over 10 channels @ 905 – 928 MHz
  - 250 kbps over 16 channels @ 2.4 GHz
- MAC protocol
  - Single channel at any one time
  - Combines contention-based and schedule-based schemes
  - Asymmetric: nodes can assume different roles

802.15.4 Type of nodes



- Full Function Device (FFD):
  - It can operate in three roles
    - PAN coordinator, a simple coordinator, device
  - Any topology, e.g., star topology, peer-to-peer topology
  - Talks to any other device
- Reduced Function Device (RFD):
  - only as normal device
  - It MUST be associated with a coordinator
  - Limited to star topology





Different Data Transmission Methods

- Data transfer can happen in three ways:
  - From a normal device to a coordinator, from a coordinator to a device; from one peer to another in a peer-to-peer multihop network
- There are three different types of data transfer:
  - **Direct data transmission**
    - This applies to all data transfers
    - Using unslotted CSMA/CA or slotted CSMA/CA
  - **Indirect data transmission**
    - This applies to data transfer from a coordinator to a normal device
    - Data frame is kept in a transaction list by coordinator, waiting for extraction by the corresponding device
    - A device knows it has pending data by checking beacon frames
  - **Guaranteed time slot (GTS) data transmission**
    - This applies to data transfer between a coordinator and a device

Beacon mode and non-Beacon mode

- 802.15.4 supports both beacon mode and non-beacon mode

- In beacon mode, a coordinator broadcasts beacons periodically to synchronize the attached devices
  - Superframe structure is used in beacon mode.

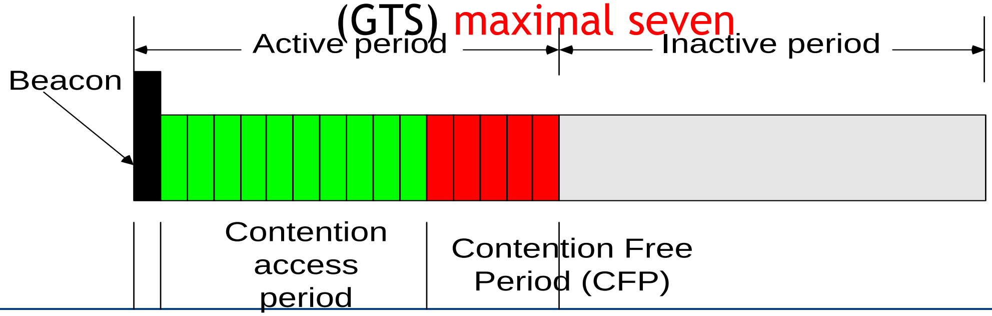
- In non-beacon mode, a coordinator does NOT broadcast beacon periodically, but may unicast a beacon to a device that is soliciting beacons

Coordinator

- Coordinator: Multiple coordinators form a personal area network (PAN)
  - Bookkeeping the associated devices
  - Allocate short address (16-bit) to devices
  - Generate frame beacon packets announcing PAN identifier
  - Process slots requests from devices
  - Exchange packets with devices and peer coordinator

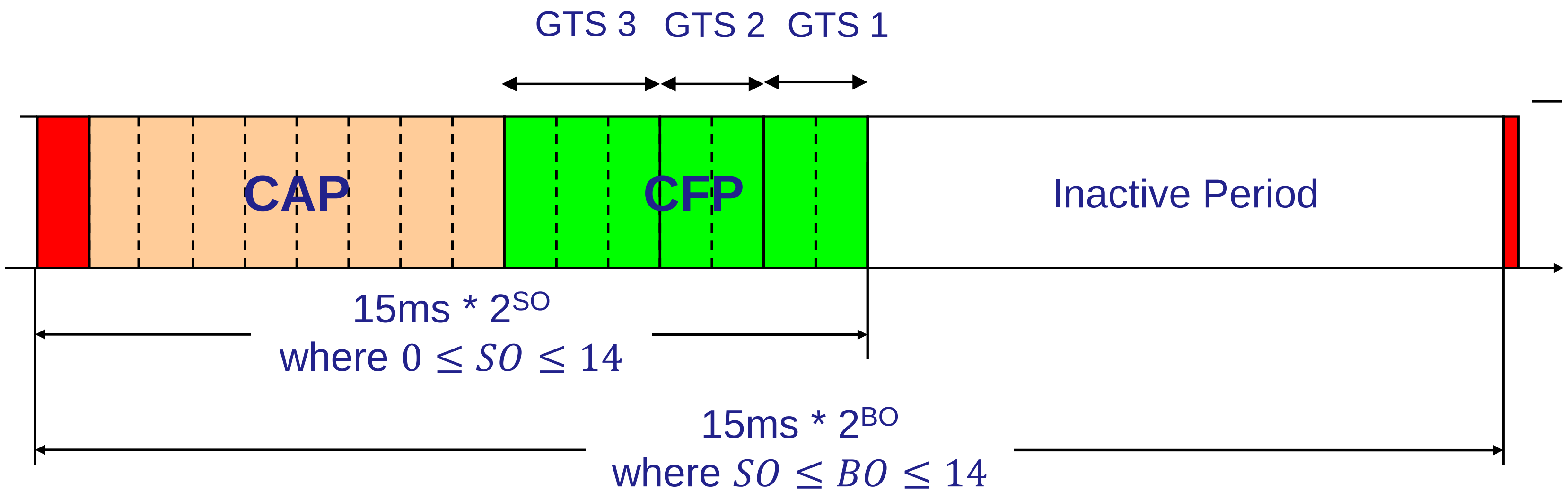
Superframe Structure

- Starts by a frame beacon packet
- Composed of active period and inactive period.
  - During inactive period, all nodes including coordinator switch off transceiver and go to sleep
  - Nodes wake up when inactive period ends and get ready to receive next beacon
  - Active period has 16 time slots.
    - First time slot used for beacon
    - The remaining time slots are partitioned into
      - Connection Access control (CAP)
      - Connection Free Period (CFP) consisting of Guaranteed Time Slots (GTS) maximal seven



AARHUS SCHOOL OF ENGINEERING

Superframe Structure



SO = Superframe order
BO = Beacon order

- Format defined by coordinator
- Bounded by network beacons

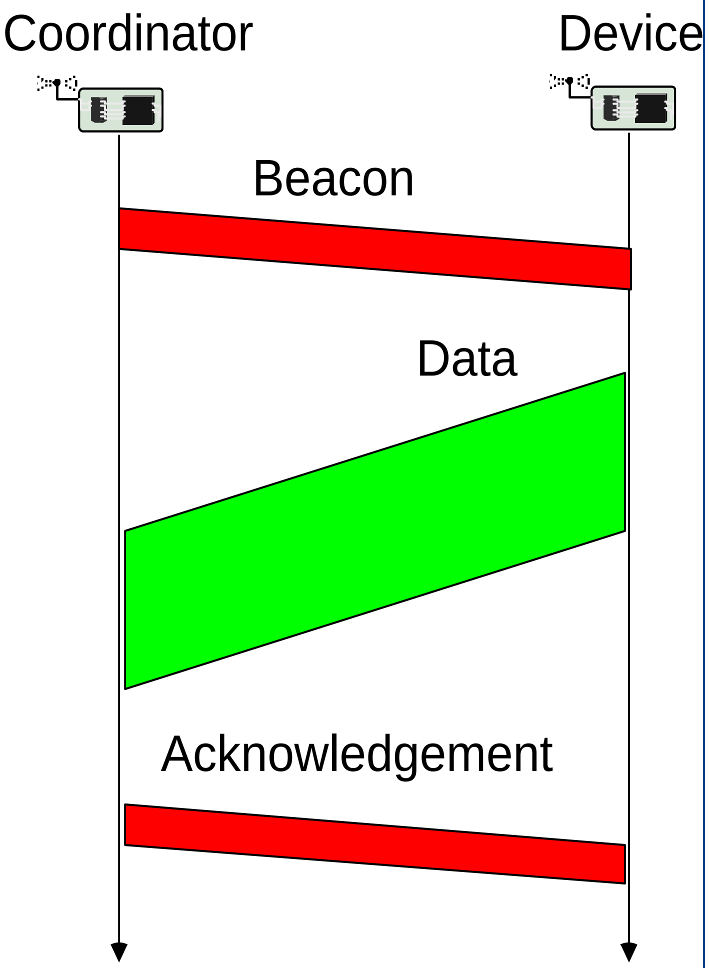
Data Transfer Procedure

- Beacon-Enabled Transmission
  - Transmitting device finds beacon before transmission
  - If not found, uses unslotted CSMA/CA to send
  - If found, transmits in appropriate portion of superframe
  - Transmissions in CAP use CSMA, in GTS no CSMA

- Beacon-Enabled Reception
  - Device determines that data for it is pending by examining beacon message contents
  - If data pending, sends request for that data to coordinator

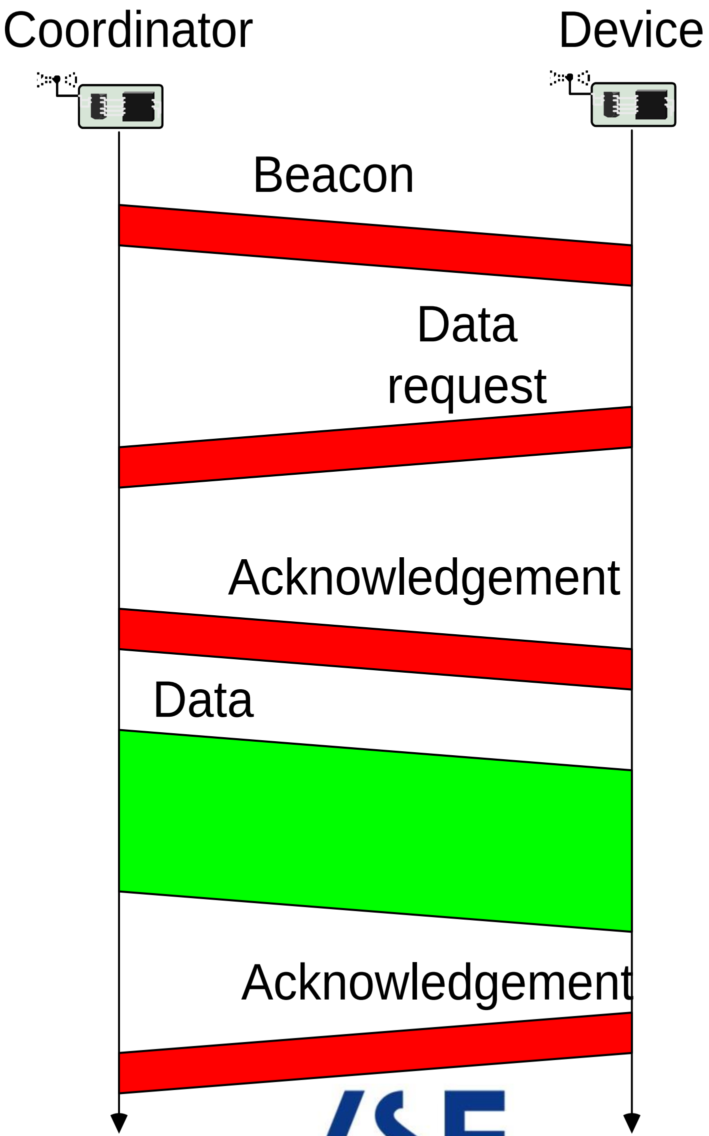
Data Transfer Procedure

- Device to Coordinator (Beacon-Enabled)
  - Device listens for network beacon
  - When found, synchronizes to superframe structure
  - At right time it transmits its data frame using slotted CSMA/CA to coordinator
  - Space for optional acknowledgements at end of slot

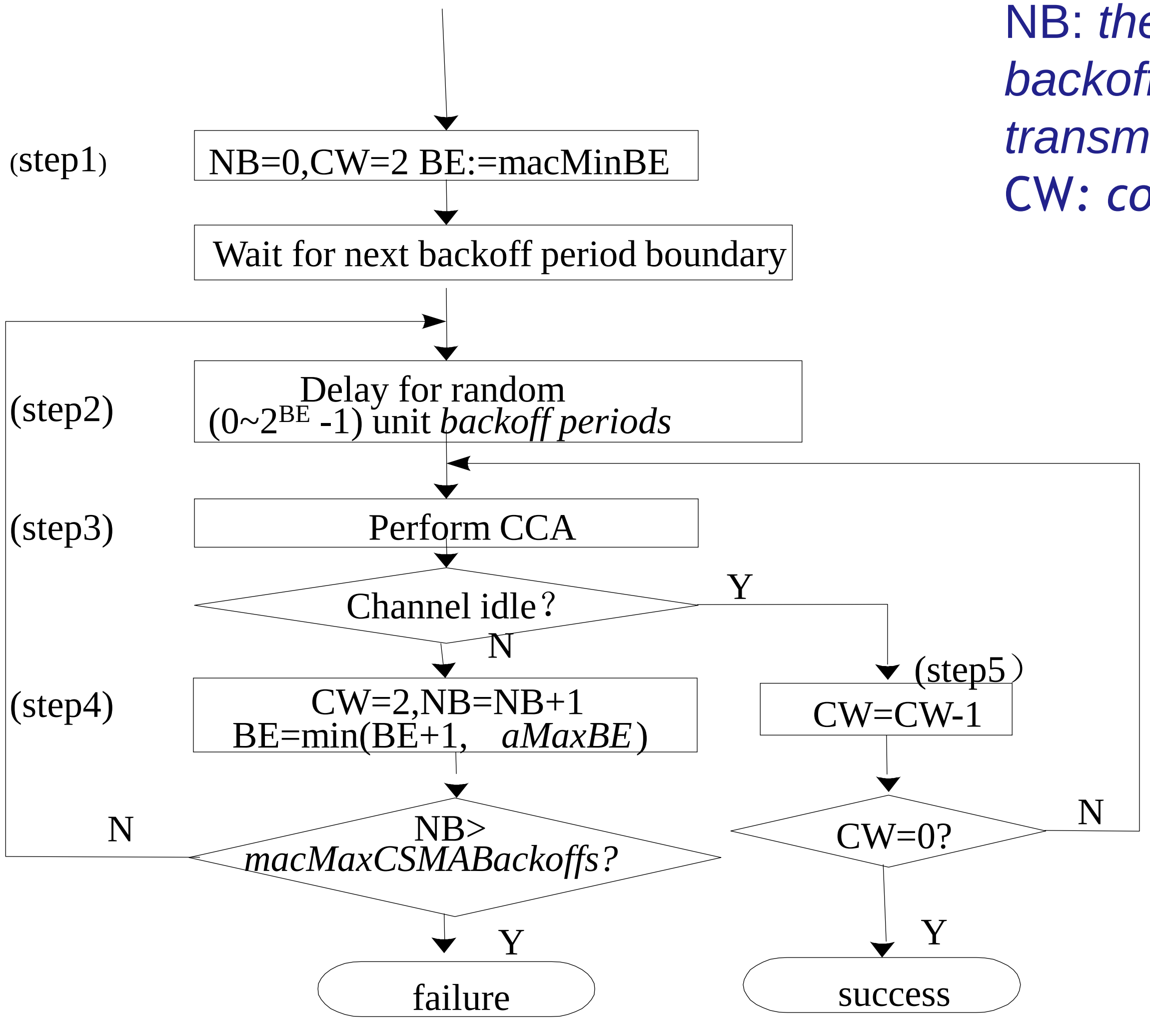


Data Transfer Procedure

- Coordinator to Device (Beacon-Enabled)
  - Coordinator indicates in beacon message that data pending
  - Device requests data using slotted CSMA/CA
  - Coordinator acknowledges request
  - Data sent from coordinator to device
  - Device acknowledges data sent



Slotted CSMA/CA



Note:

BE: *Backoff exponent*

NB: *the number of successive backoffs before the current transmission*

CW: *contention window*

Non-Beaconed mode

- This mode is much simpler:
  - no beacon packets, no superframe structure, no inactive periods
    - Coordinator must be switched on constantly
    - Devices can sleep as they like
  - only (unslotted) CSMA/CA mode available
  - Uplink traffic handled directly by CSMA/CA protocol
  - Downlink traffic: device sends explicit request packet to coordinator (using CSMA/CA), followed by immediate ACK, data packet, immediate ACK

Association/Disassociation with PAN

- Coordinator decides to release device from PAN
  - Sends dis-association notification command to device
  - Device sends ACK that it has dis-associated itself

- Device decides to release itself from PAN
  - Sends dis-association notification command to coordinator
  - Coordinator sends ACK that it has dis-associated device

- Both devices and coordinator remove all references of each other

Summary

- MAC protocols for sensor networks is one the most active research fields
  - Many different ideas exist for medium access control in WSN

- Comparing their performance and suitability is difficult

- Especially: clearly identifying interdependencies between MAC protocol and other layers/applications is difficult
  - Which is the best MAC for which application?

ASE | AARHUS SCHOOL OF ENGINEERING