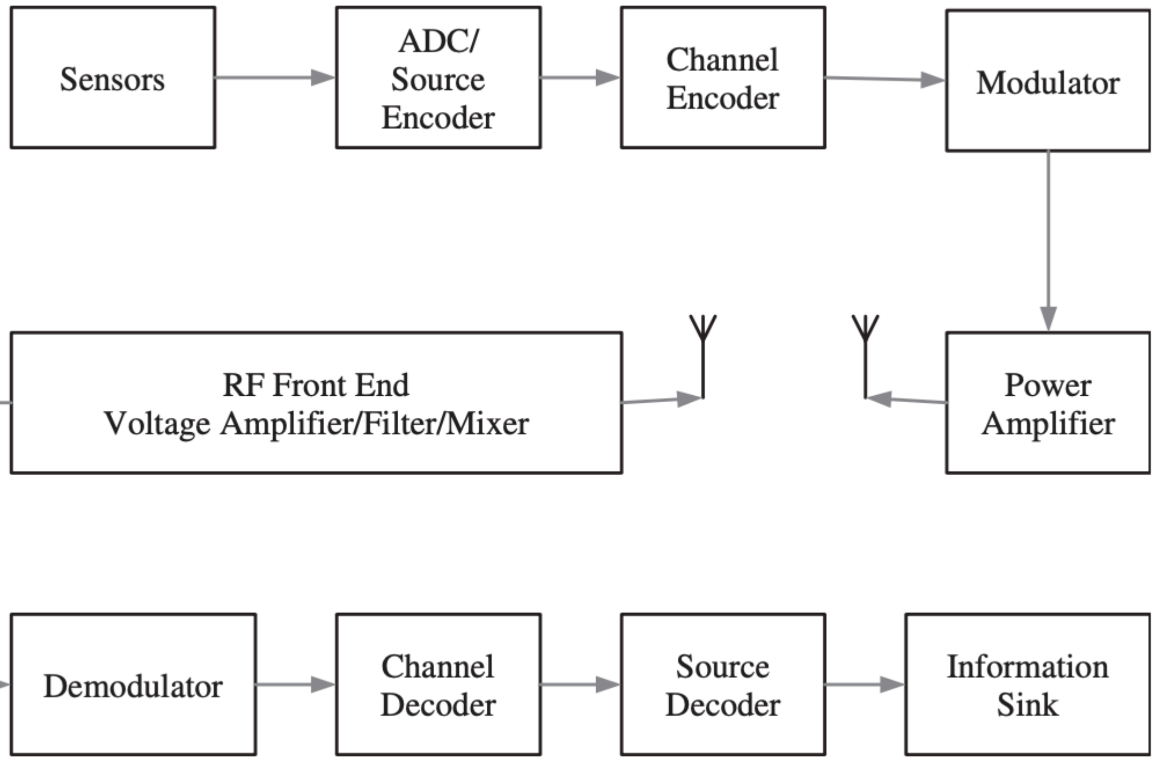
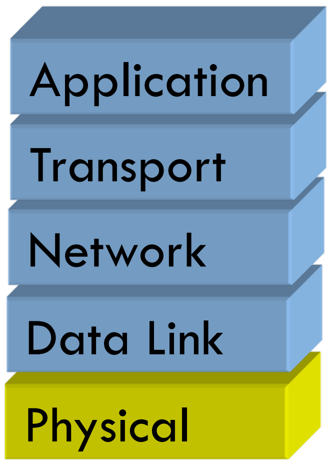
PHYSICAL LAYER

COMPONENTS OF A DIGITAL COMMUNICATION SYSTEM.





Source Encoding

A source encoder transforms an analog signal into a digital sequence. The process consists of sampling, quantizing, and encoding.

Channel Encoding

The main purpose of a channel encoder is to produce a sequence of data that is robust to noise and to provide error detection and forward error correction mechanisms. In simple and cheap transceivers, forward error correction is costly and, therefore, the task of channel encoding is limited to the detection of errors in packet transmission.

Modulation

Modulation is a process by which the characteristics (amplitude, frequency, and phase) of a carrier signal are modified according to the message (a baseband) signal. Modulation has several advantages:

• the message signal will become resilient to noise;
• the channel's spectrum can be used efficiently;
and • signal detection will be simple.

SIGNAL PROPAGATION

Signal Propagation

Wireless sensor networks operate in the license-free ISM spectrum and therefore, they must share the spectrum with and accept interference from devices that operate in the same spectrum – such as cordless phones, WLAN, Bluetooth, Microwave ovens, etc.

A simple channel model ignores the effect of interference and considers the surrounding noise as the predominant factor that affects the transmitted signal. Furthermore, the noise can be modeled as an Additive White Gaussian Noise (AWGN) that has a constant spectral density over the entire operating spectrum and a normal amplitude distribution. In this model, the noise distorts the amplitude of the transmitted signal.

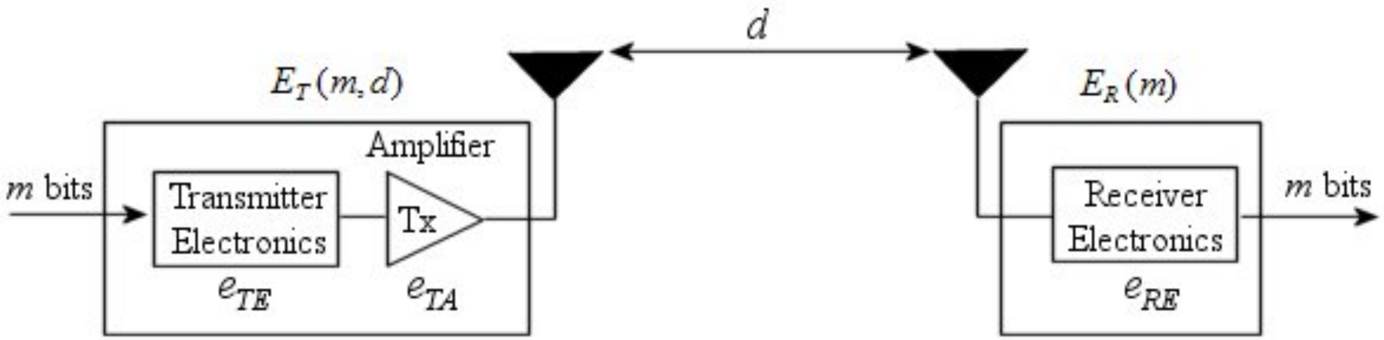
There are two approaches to deal with noise. First, one can increase the received power so that the signal-to-noise ratio is significantly high and the channel becomes agnostic to noise.

THE INDUSTRY, SCIENTIFIC AND MEDICAL (ISM) SPECTRUM AS DEFINED BY THE ITU-R

Spectrum	Center frequency	Availability
6.765–6.795 MHz	6.780 MHz	Subject to local regulations
13.553–13.567 MHz	13.560 MHz	
26.957–27.283 MHz	27.120 MHz	
40.66–40.70 MHz	40.68 MHz	
433.05–434.79 MHz	433.92 MHz	Europe, Africa, the Middle East west of the Persian Gulf including Iraq, the former Soviet Union and Mongolia
902–928 MHz	915 MHz	The Americas, Greenland and some of the eastern Pacific Islands
2.400–2.500 GHz	2.450 GHz	
5.725–5.875 GHz	5.800 GHz	
24–24.25 GHz	24.125 GHz	
61–61.5 GHz	61.25 GHz	Subject to local regulations
122–123 GHz	122.5 GHz	Subject to local regulations
244–246 GHz	245 GHz	Subject to local regulations

PHYSICAL LAYER

Energy consumption minimization is of paramount importance when designing the physical layer for WSN in addition to the usual effects such as scattering, shadowing, reflection, diffraction, multipath, and fading.



Radio Model – Energy Consumption

$$E_L(m,d) = E_T(m,d) + E_R(m) \qquad E_T(m,d) = E_{TC}(m) + E_{TA}(m,d)$$

$E_{TC} =$ energy used by the transmitter circuitry

$E_{TA} =$ energy required by the transmitter amplifier to achieve an acceptable signal to noise ratio or at the receiver

PHYSICAL LAYER

Assuming a linear relationship for the energy spent per bit by the transmitter and receiver circuitry

$$E_T(m,d) = m\left(e_{TC} + e_{TA} d^{\alpha}\right) \qquad E_R(m) = m e_{RC}$$

An explicit expression for e_{TA} can be derived as,

$$e_{TA} = \frac{\left(\frac{S}{N}\right)_r (NF_{Rx})(N_0)(BW)\left(\frac{4\pi}{\lambda}\right)^{\alpha}}{(G_{ant})(\eta_{amp})(R_{bit})}$$

$(S/N)_r$ = minimum required signal to noise ratio at the receiver's demodulator for an acceptable *Eb/N0*

NF_{rx} = receiver noise figure

N_0 = thermal noise floor in a 1 Hertz bandwidth (Watts/Hz)

BW = channel noise bandwidth

λ = wavelength in meters

α = path loss exponent whose value varies from 2 (for free space) to 4 (for multipath channel models)

G_{ant} = antenna gain

η_{amp} = transmitter power efficiency

R_{bit} = raw bit rate in bits per second

PHYSICAL LAYER

$$\varsigma = \frac{(NF_{Rx})(N_0)(BW)\left(\frac{4\pi}{\lambda}\right)^{\alpha}}{(G_{ant})(\eta_{amp})(R_{bit})} \Rightarrow e_{TA} = \varsigma\left(\frac{S}{N}\right)_r$$

$(S/N)_r$ = minimum required signal to noise ratio at the receiver's demodulator

NF_{rx} = receiver noise figure

N_0 = thermal noise floor in a 1 Hertz bandwidth (Watts/Hz)

BW = channel noise bandwidth

λ = wavelength in meters

α = path loss exponent whose value varies from 2 (for free space) to 4 (for multipath channel models)

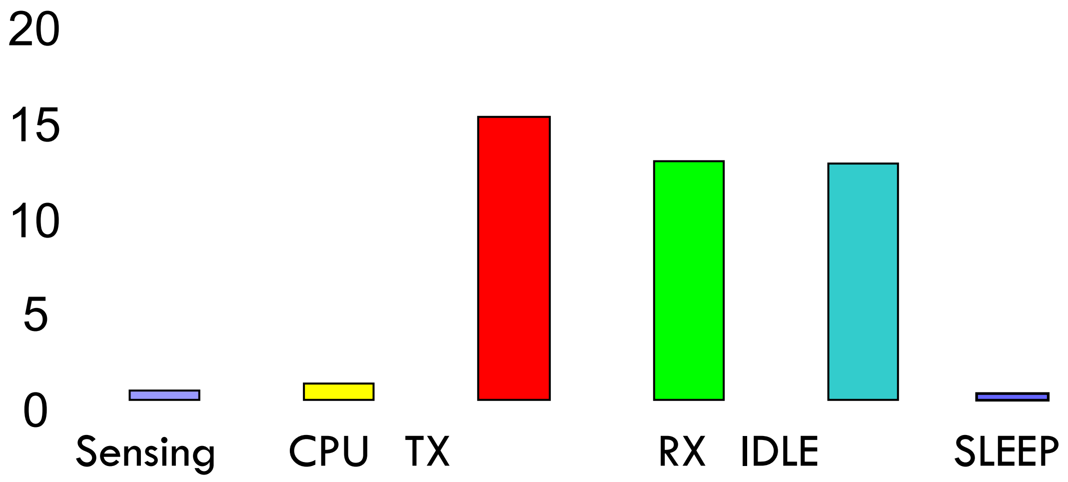
G_{ant} = antenna gain

η_{amp} = transmitter power efficiency

R_{bit} = raw bit rate in bits per second

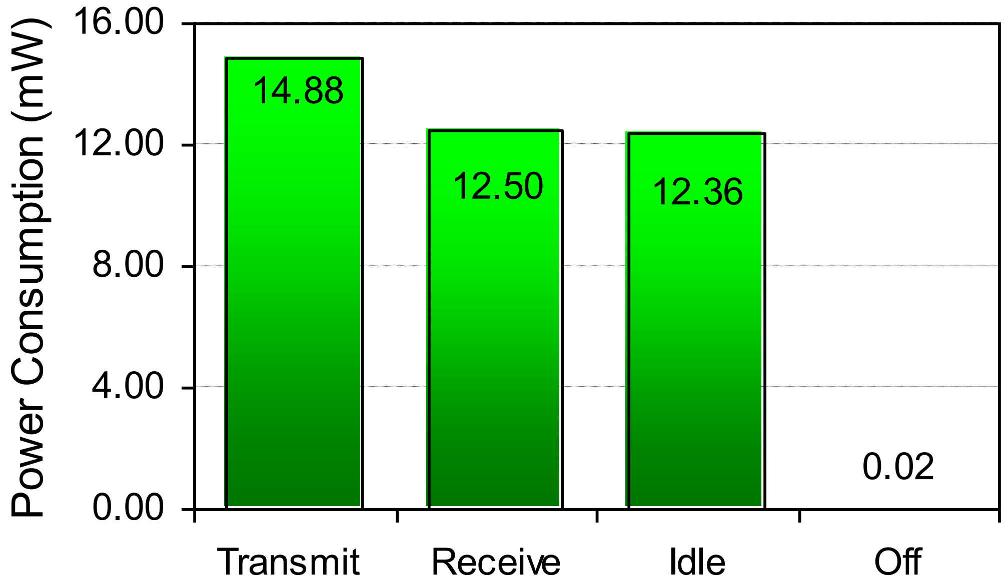
ENERGY LIMITATIONS

- Each sensor node has limited energy supply
- Nodes may not be rechargeable
- Energy consumption in
  - Sensing
  - Data processing
  - Communication (most energy intensive)



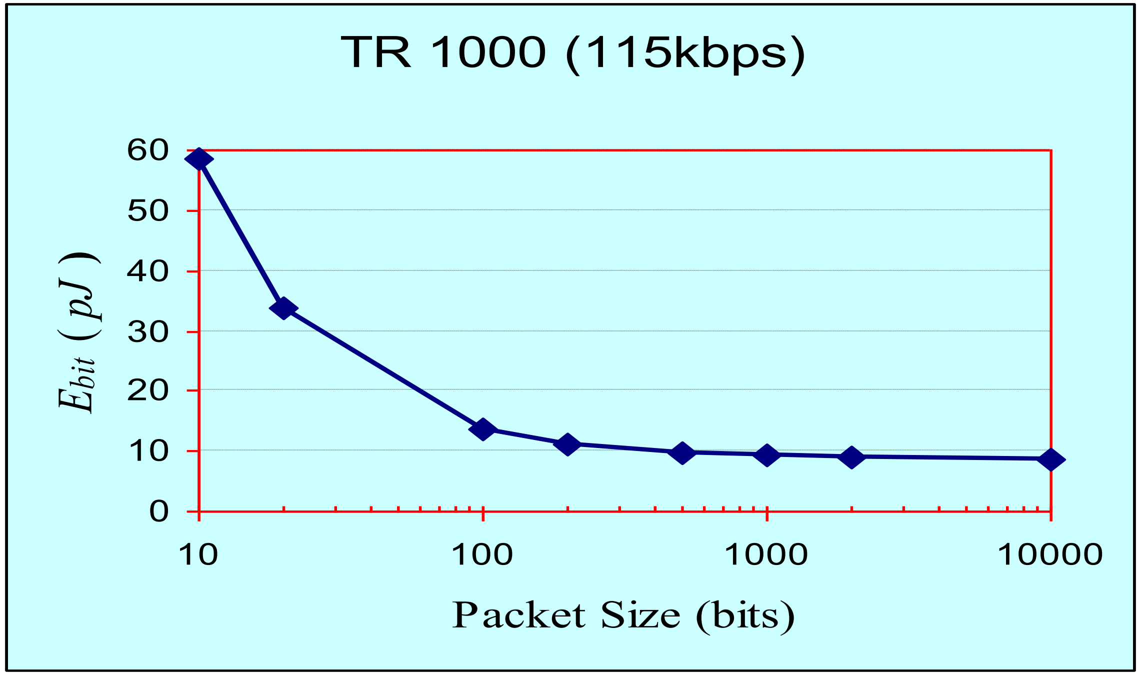
PARAMETERS

Parameter	Value
Transition time from sleep to receive mode	500 μs
Transition time from sleep to transmit mode	16 μs
Transition time from transmit to receive mode	500 μs
Transition time from receive to transmit mode	12 μs
Bit rate	115.2 kbps



POWER SAVING MECHANISMS

- The amount of time and power needed to wake-up (start-up) a radio is not negligible and thus just turning off the radio whenever is not being used is not necessarily efficient
- The energy characteristics of the start-up time should also be taken into account when designing the size of the data link packets. The values shown in the figure below clearly indicate that when the start-up energy consumption is taken into account the energy per bit requirements can be significantly higher for the transmission of short packets than for longer ones

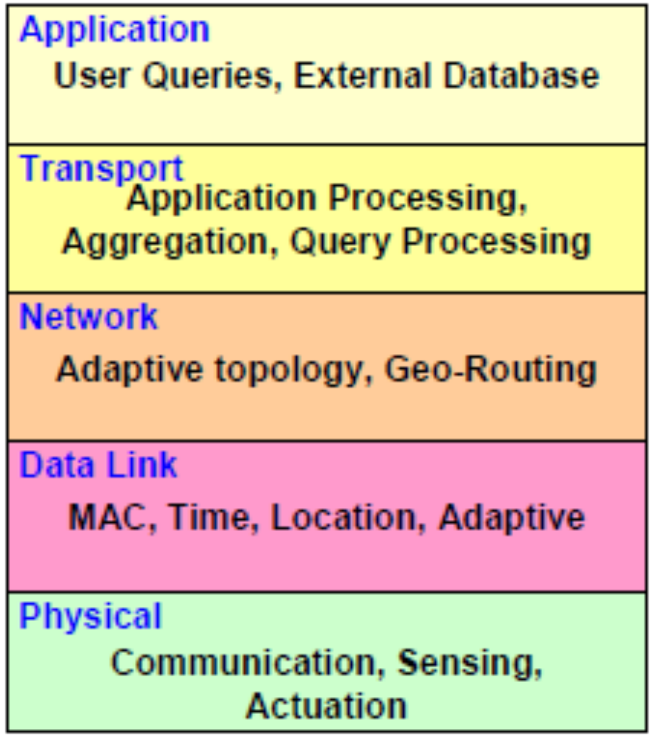


DATA LINK LAYER

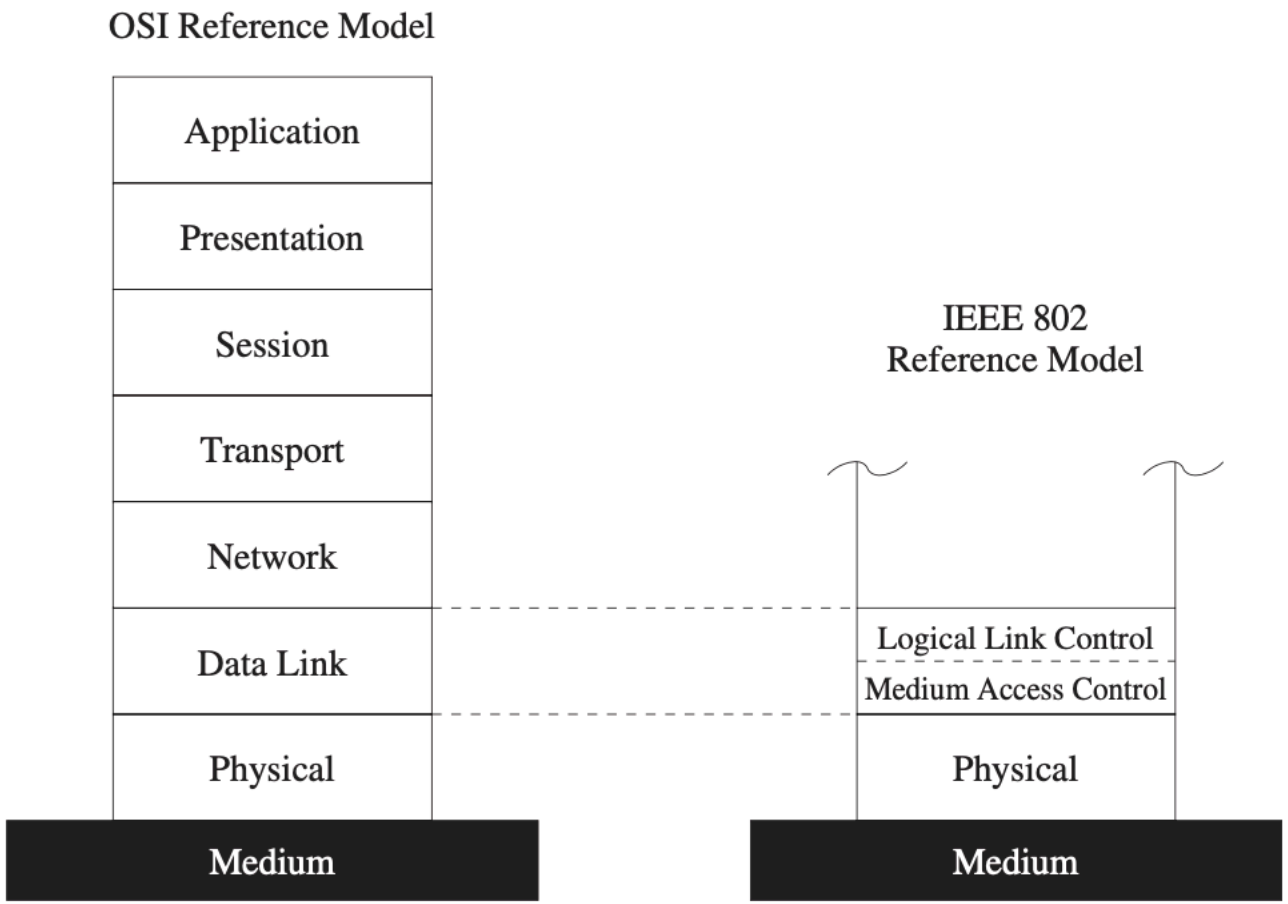
The wireless medium must be shared by multiple network devices, therefore a mechanism is required to control access to the medium. This responsibility is carried out by the second layer of the OSI reference model (Figure 6.1), called the *data link* layer.

According to the IEEE 802 reference model. This layer is further divided into
- the *logical link control* layer and
- the *medium access control* layer.

The MAC layer operates directly on top of the physical layer, thereby assuming full control over the medium.
- The main function of the MAC layer is to decide when a node accesses a shared medium and to resolve any potential conflicts between competing nodes.
- It is also responsible for correcting communication errors occurring at the physical layer and performing other activities such as framing, addressing, and flow control.



MAC LAYER IN THE IEEE 802 REFERENCE MODEL

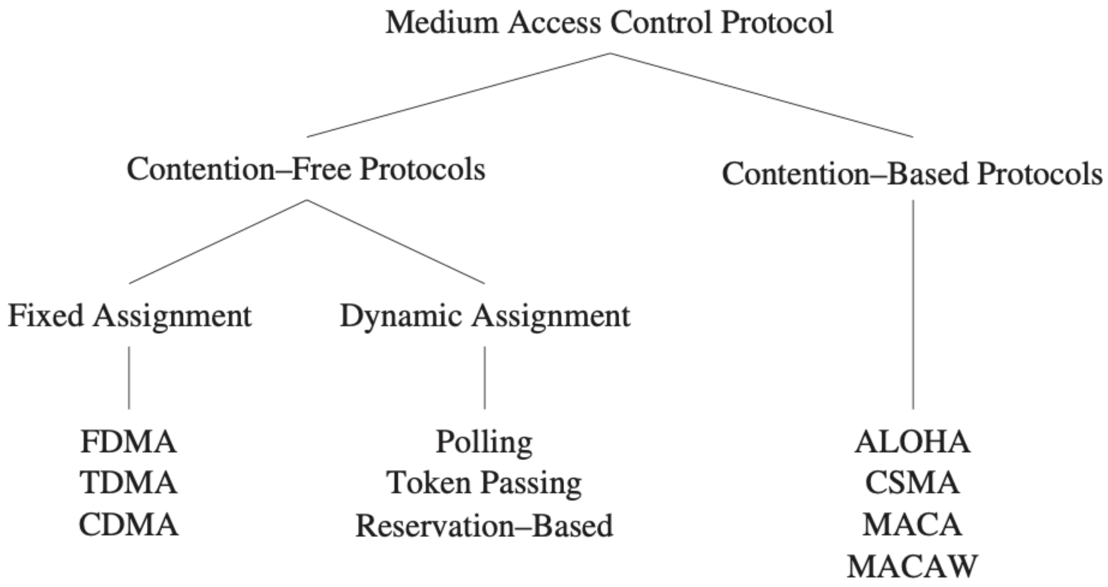


CATEGORIES AND EXAMPLES OF MEDIUM ACCESS PROTOCOLS.

- Existing MAC protocols can be categorized by the way they control access to the medium.
- Most MAC protocols fall either into the categories of *contention-free* or *contention-based* protocols.

- In the first category, MAC protocols provide a medium sharing approach that ensures that only one device accesses the wireless medium at any given time. This category can further be divided into *fixed* and *dynamic* assignment classes, indicating whether th slot reservations are fixed or on- demand.
- In contrast to contention-free techniques, contention-based protocols allow nodes to access the medium simultaneously, but provide mechanisms to reduce the number of collisions and to recover from such collisions.

Finally, some MAC protocols do not easily fit into this classification since they share characteristics of both contention-free and contention-based techniques. These *hybrid* approaches often aim to inherit the advantages of these main categories, while minimizing their weaknesses.



LIGHTWEIGHT MEDIUM ACCESS CONTROL

- The Lightweight Medium Access Control (LMAC) protocol (Van Hoesel and Havinga 2004) is based on TDMA, that is, time is again divided into frames and slots, where each slot is owned by exactly one node.
- However, instead of relying on a central manager to assign slots to nodes, nodes execute a distributed algorithm to allocate slots.
- Each node uses its slot to transmit a message consisting of two parts:
  - a control message
  - and a data unit.
- The fixed-size control message carries information such as the identity of the time slot controller, the distance (in hops) of the node to the gateway (base station), the address of the intended receiver, and the length of the data unit.
- Upon receiving a control message, a node determines if it is the intended receiver and decides whether to stay awake or to turn off the radio until the next slot.
- The *Occupied Slots* field of the control message is a bitmask of slots, where an unoccupied slot is represented by 0 and an occupied slot is represented by 1.

- By combining control messages from all neighbors, a node is able to deter- mine unoccupied slots.
- The process of claiming slots starts at the gateway device, which determines its own slots.
- After one frame, all direct neighbors of the gateway know the gateway’s slots and choose their own slots.
- This process continues throughout the network and during each frame, a new set of nodes with a higher hop distance from the gateway determine their slots.
- Each node must select slots that are not in use within a two-hop neighborhood.
- Slots are selected randomly, therefore, it is possible for multiple nodes to select the same slot.
- This will result in a collision of control messages during a slot, which can be observed by the competing nodes, which, in turn, results in a restart of the selection process.

SENSOR MAC

- The goal of the sensor MAC (S-MAC) protocol (Ye *et al.* 2002) is to reduce unnecessary energy consumption, while providing good scalability and collision avoidance.
- S-MAC adopts a duty-cycle approach, that is, nodes periodically transition between a *listen state* and a *sleep state*.
- Each node chooses its own schedule, though it is preferred when nodes synchronize their schedules such that they listen or sleep at the same time.
- In this case, nodes using the same schedule are considered to belong to the same *virtual cluster* , but no real clustering takes place and all nodes are free to communicate with nodes outside their clusters.
- Nodes periodically exchange their schedules with their neighbors using SYNC messages, that is, every node knows when any of its neighbors will be awake.
- If node A wants to communicate with a neighbor B that uses a different schedule, A waits until B is listening and then initiates the data transfer. Contention for the medium is resolved using the RTS/CTS scheme.

SENSOR MAC

- In order to choose a schedule, a node initially listens to the medium for a certain amount of time.
- If this node receives a schedule from a neighbor, it chooses this schedule as its own and this node becomes a *follower*.
- The node broadcasts its new schedule after a random delay td (to minimize the possibility for collisions from multiple new followers).
- Nodes can adopt multiple schedules, that is, if a node receives a different schedule after it has broadcast its own schedule, it adopts both schedules.
- Further, if a node does not hear a schedule from another node, it determines its own schedule and broadcasts it to any potential neighbors.
- This node becomes a *synchronizer* in that other nodes will begin to synchronize themselves with it.

SENSOR NODE

S-MAC divides a node’s listen interval further into a part for receiving SYNC packets and a part for receiving RTS messages.
Each part is further divided into small slots to facilitate carrier sensing.
A node trying to send a SYNC or RTS message randomly selects a time slot (within the SYNC or RTS part of the interval, respectively) and senses the carrier for activity from when the receiver begins listening to the selected slot.
If no activity has been detected, it wins the medium and begins transmission.

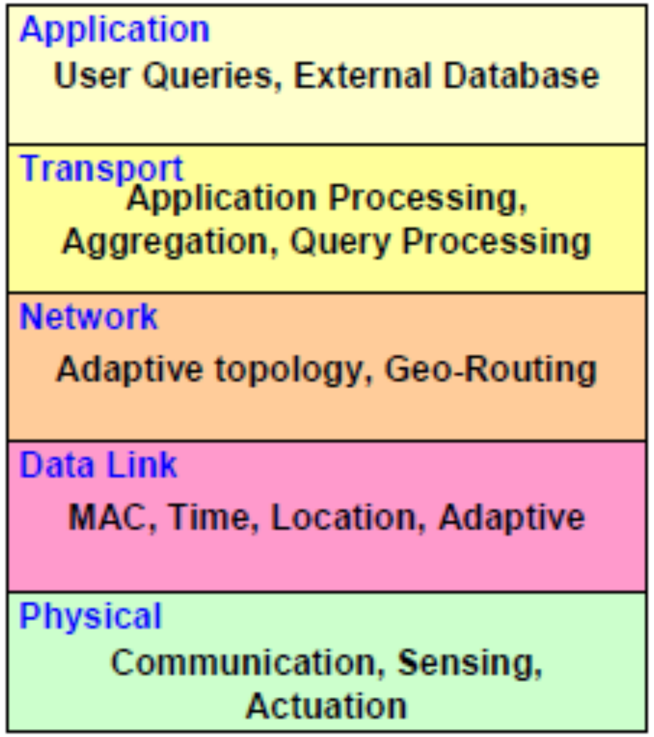
S-MAC adopts a contention-based approach, where contention for the medium is addressed using collision avoidance based on RTS/CTS handshakes.
When a node hears an RTS or CTS and concludes that it cannot transmit or receive at the same time, it can go to sleep to avoid energy waste through overhearing (a node may only overhear brief control messages, but not the typically longer data messages).
In summary, S-MAC is a contention-based protocol that utilizes the sleep mode of wire- less radios to trade energy for throughput and latency. Collision avoidance is based on RTS/CTS, which is not used by broadcast packets, thereby increasing the collision prob- ability. Finally, duty cycle parameters (sleep and listen periods) are decided beforehand and may be inefficient for the actual traffic characteristics in the network.

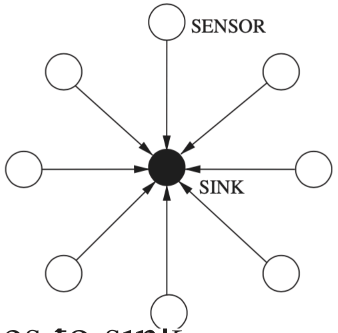
THE NETWORK LAYER

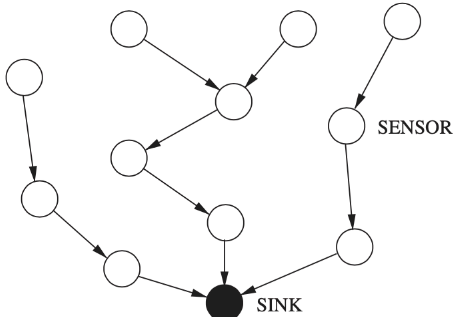
NETWORK LAYER

- Data collected by sensor nodes in a WSN is typically propagated toward a base station (gateway) that links the WSN with other networks where the data can be visualized, analyzed, and acted upon.

- In small sensor networks where sensor nodes and a gateway are in close proximity, direct (single-hop) communication between all sensor nodes and the gate- way may be feasible.
- However, most WSN applications require large numbers of sensor nodes that cover large areas, necessitating an indirect (multi-hop) communication approach.
- That is, sensor nodes must not only generate and disseminate their own information, but also serve as relays or forwarding nodes for other sensor nodes.
- The process of establishing paths from a source to a sink (e.g., a gateway device) across one or more relays is called *routing* and is a key responsibility of the network layer of the communication protocol stack.
- However, since the nodes are deployed in a randomized fashion (i.e., they are scattered into an environment randomly), the resulting topologies are nonuniform and unpredictable. In this case, it is essential for these nodes to self-organize, that is, they must cooperate to determine their positions, identify their neighbors, and discover paths to the gateway device.

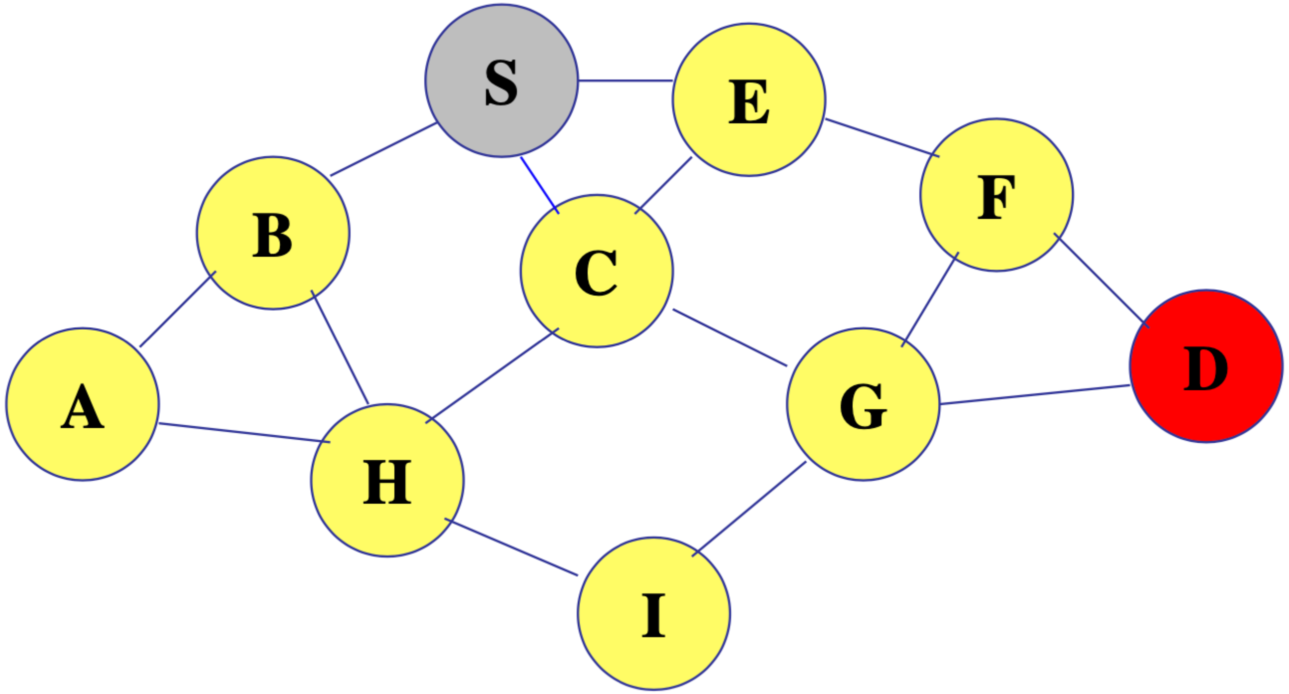






- The key responsibility of the network layer is to find paths from data sources to sink devices (e.g., gateways).
- In the single-hop routing model, all sensor nodes are able to communicate directly with the sink device. This direct communication model is the simplest approach, where all data travels a single hop to reach the destination.
- However, in practical settings, this single-hop approach is unrealistic and a multi-hop communication model must be used.
- In this case, the critical task of the network layer of all sensor nodes is to identify a path from the sensor to the sink across mul- tiple other sensor nodes acting as relays.
- This design of a routing protocol is challenging due to the unique characteristics of WSNs, including resource scarcity or the unreliabil- ity of the wireless medium.
- For example, the limited processing, storage, bandwidth, and energy capacities require routing solutions that are lightweight, while the frequent dynamic changes in a WSN (e.g., topology changes due to node failures) require routing solutions

ROUTING



Routing problem – find path between S and D

ROUTING PROTOCOLS IN SENSOR NETWORKS

Routing queries to nodes that have observed a particular event

- Retrieve data on the event

- Obtain route information between pairs of nodes wishing to communicate.
- Proactive protocols: maintain routing tables at each node that is updated as changes in the network topology are detected.
  - Heavy overhead with high network dynamics (caused by link/node failures or node movement).
  - Not practical for ad hoc networks.

PROTOCOLS

- Reactive protocols: routes are constructed on demand. No global routing table is maintained.
- Due to the high rate of topology changes, reactive protocols are more appropriate for ad hoc networks.
  - Ad hoc on demand distance vector routing (AODV)
  - Dynamic source routing (DSR)
- However, both depend on flooding for route discovery.

- Hybrid –

- First Compute all Routes;
- Then Improve While Routing

ROUTING PROTOCOLS

- Direct – Node and Sink Communicate Directly (Fast Drainage; Small Scale)
- Flat (Equal) –Random Indirect Route (Fast Drainage Around Sink; Medium Scale)
- Clustering (Hierarchical) – Route Thru Distinguished Nodes

- Location Aware –Nodes know where they are
- Location-Less –Nodes location is unimportant
- Mobility Aware – Nodes may move – Sources; Sinks; All

- Unicast –One-to-One Message Passing
  - Multicast (actually Local Broadcast) – Node-to-Neighbors Message Passing
  - Broadcast – Full-Mesh – Source to Everyone

DATA CENTRIC/GR ROUTING

- “Data-centric” routing: routing is frequently based on a nodes’ attributes and sensed data, rather than on pre-assigned network address.
- Geographical routing uses a node’s location to discover path to that route.

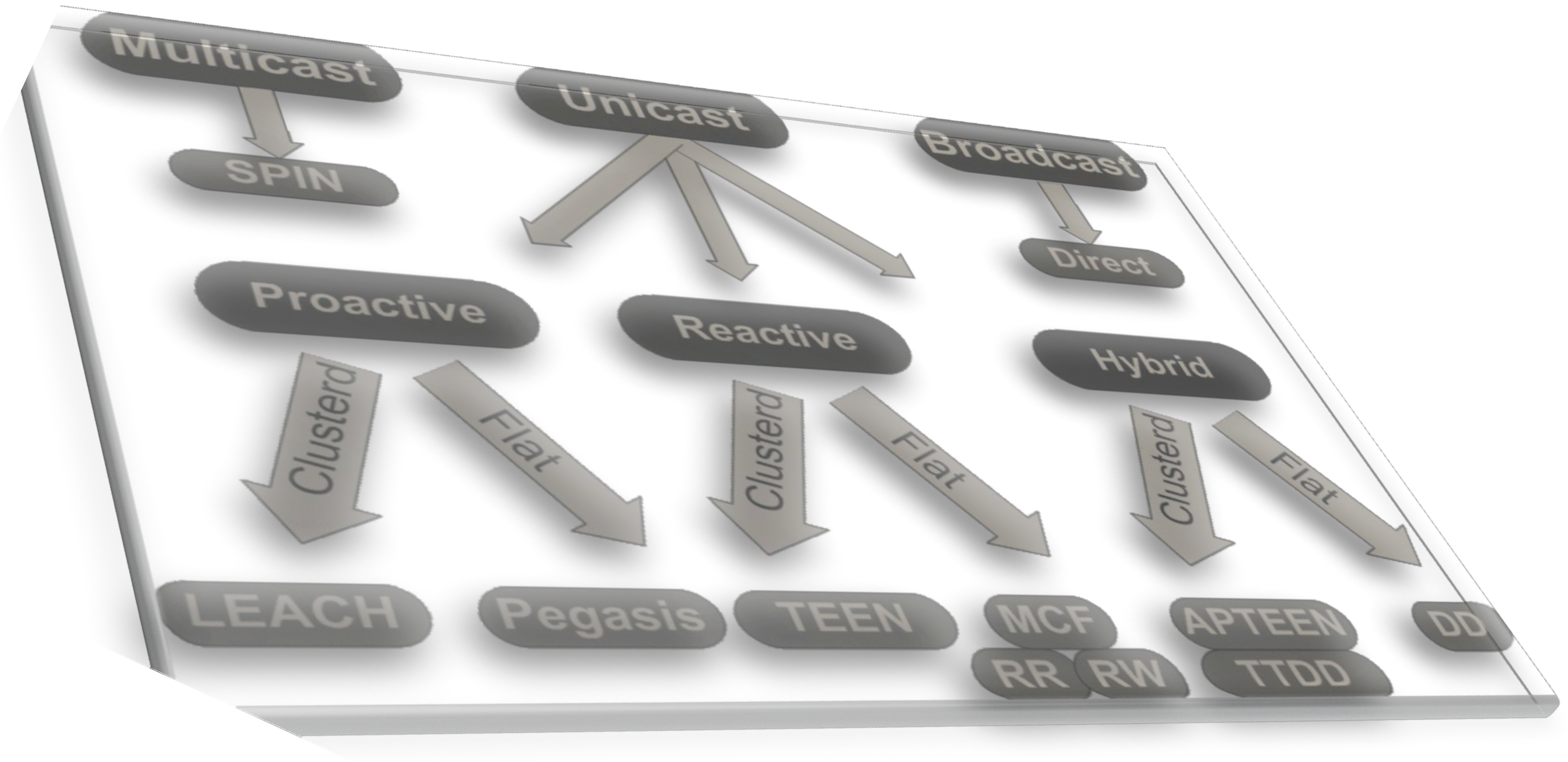
GR BASED ROUTING

- The source node knows
  - The location of the destination node;
  - The location of itself and its 1-hop neighbors.
- Geographical forwarding: send the packet to the 1-hop neighbor that makes most progress towards the destination.
  - No flooding is involved.
- Many ways to measure "progress".
  - The one closest to the destination in Euclidean distance.
  - The one with smallest angle towards the destination: "compass routing".

ROUTING MODELS

- Routing Models
  Historical Queries: Analysis of historical data
  “What was the watermark 2h ago in the southeast?”
- One-time Queries: Snapshot view
  “What is the watermark in the southeast?”
- Persistent Queries: Monitoring over time
  “Report the watermark in the southeast for the next 4h”

PROTOCOL CLASSIFICATION



ROUTING PROTOCOLS CLASSIFICATION

Routing protocols

Network Structure

Flat routing
- SPIN
- Directed Diffusion (DD)

Hierarchical routing
- LEACH
- PEGASIS
- TTDD

Location based routing
- GEAR
- GPSR

Protocol Operation

Negotiation based routing
- SPIN

Multi-path network routing
- DD

Query based routing
- DD, Data centric routing

QoS based routing
- TBP, SPEED

Coherent based routing
- DD

Aggregation
- Data Mules, CTCCAP