MAC Protocols for WSN
Introduction

• Wireless sensor Networks are typically composed of large number of low-cost, low power, multifunctional wireless devices deployed over a geographical area in ad hoc fashion and without careful planning.

• The establishment of multihop wireless network infrastructure for data transfer requires the establishment of communication links between neighboring sensor nodes.
• Communication among wireless sensor nodes is usually achieved by means of a unique channel.
• It is the characteristic of this channel that only single node can transmit message at any time, therefore shared access of the channel requires establishment of MAC protocol among the sensor nodes.
• The objective of the MAC protocol is to regulate access to the shared wireless medium such that the performance requirement of underlying application are satisfied.
OSI reference model and the logical architecture of the DLL for shared medium access in wireless networks.

- From the perspective of the Open System Interconnection (OSI) reference model (OSIRM), the MAC protocol functionality are provided by the lower sub layer of the data link layer (DLL).
- The higher sub layer of the DLL is referred as the logical link control (LLC) layer.
Physical Layer

- The physical layer (PHY) typically includes a specification of the *transmission medium* and the *topology* of the network.
- It defines the procedures and functions that must be performed by the physical device and the communications interface to achieve bit transmission and reception.
- It also coordinates the various functions necessary to transmit a stream of bits over the wireless communication medium.
- The major services provided by the physical layer typically include the
  1. encoding and decoding of signals,
  2. Preamble generation and removal to achieve synchronization, and
  3. The transmission and reception of bits.
• The subdivision of the data link layer into two sub layers is necessary to accommodate the logic required to manage access to a shared access communications medium.

• Furthermore, the presence of the LLC sub layer allows support for several MAC options, depending on the structure and topology of the network, the characteristics of the communication channel, and the quality of service requirements of the supported application.
MAC Sublayer

• The MAC sub layer resides directly above the physical layer. It supports the following basic functions:

1. The assembly of data into a frame for transmission by appending a header field containing addressing information and a trailer field for error detection.

2. The disassembly of a received frame to extract addressing and error control information to perform address recognition and error detection and recovery.

3. The regulation of access to the shared transmission medium in a way commensurate with the performance requirements of the supported application.
LLC Sublayer

• The LLC sublayer of the DDL provides a direct interface to the upper layer protocols.

• Its main purpose is to shield the upper layer protocols from the characteristics of the underlying physical network, thereby providing interoperability across different types of networks.

• The use of the LLC sublayer, however, has been very limited, as interoperability is typically achieved by other network layer protocols.
Fundamentals of MAC Protocols

• The main difficulty in designing effective MAC protocols for shared access media is to decide which node can access the communication channel at any given time, the nodes must exchange some amount of coordinating information.

• The exchange of this information, however, typically requires use of the communication channel itself. This recursive aspect of the multi-access medium problem increases the complexity of the access control protocol and consequently, the overhead required to regulate access among the competing nodes.
• Spatial distribution does not allow a given node on the network to know the instantaneous status of other nodes on the network.

• Any information explicitly or implicitly gathered by any node is at least as old as the time required for its propagation through the communication channel.

• There is a trade-off between two factors, the *intelligence* of the MAC protocol and *Overhead* involved in the Protocol.

• These two factors are unavoidably intertwined. An attempt to improve the quality of decisions does not necessarily reduce the overhead incurred. On the other hand, reducing the overhead is likely to lower the quality of the decision.
MAC Protocol Performance requirements
Delay

- Delay refers to the amount of time spent by a data packet in the MAC layer before it is transmitted successfully.
- Delay depends not only on the network traffic load, but also on the design choices of the MAC protocol.
- Guaranteed delay bounds are required to obtain proper QoS.
- Guaranteed delay bounds are usually provided through careful message scheduling both locally within a communicating node and globally among all nodes in the network.
There are two types of delay guarantees:

1. Probabilistic and
2. Deterministic.

Probabilistic delay guarantees are typically characterized by an expected value, a variance and a confidence interval.

Deterministic delay guarantees ensure a predictable number of state transitions between message arrival and message transmission. Therefore, Deterministic MAC schemes guarantee an upper bound for the access time.
Throughput

• Throughput is typically defined as the rate at which messages are serviced by a communication system. It is usually measured either in messages per second or bits per second.

• Throughput increases as the load on the communication system increases initially. After the load reaches a certain threshold, the throughput ceases to increase, and in some cases, it may start to decrease.

• An important objective of a MAC protocol is to maximize the channel throughput while minimizing message delay.
Robustness

- Robustness, defined as a combination of reliability, availability, and dependability requirements,
- It reflects the degree of the protocol insensitivity to errors and misinformation.
- Robustness is a multidimensional activity that must simultaneously address issues such as
  1. error confinement,
  2. error detection and masking,
  3. reconfiguration, and
  4. restart.
Scalability

• Scalability refers to the ability of a communications system to meet its performance characteristics regardless of the size of the network or the number of competing nodes.

• A common approach to achieve scalability is to avoid relying on globally consistent network states.

• Another approach is to localize interactions among the communicating nodes, through the development of hierarchical structures and information aggregation strategies.
Stability

• Stability refers to the ability of a communications system to handle fluctuations of the traffic load over sustained periods of time.

• A stable MAC protocol, for example, must be able to handle instantaneous loads which exceed the maximum sustained load as long as the long-term load offered does not exceed the maximum capacity of the channel.
Fairness

• A MAC protocol is considered to be fair if it allocates channel capacity evenly among the competing communicating nodes without unduly reducing the network throughput.

• Achieving fairness among competing nodes is desirable to achieve equitable QoS and avoid situations where some nodes fare better than other nodes.
Energy Efficiency

- One possible approach to reducing energy consumption at a sensor node is to use low-power electronics.
- The integration of low-power chips in the design of sensor nodes is a necessary step toward achieving high levels of power efficiency.
Several sources contribute to energy inefficiency in WSN

• The first source of energy waste is *collision*, which occurs when two or more sensor nodes attempt to transmit simultaneously. The need to retransmit a packet that has been corrupted by a collision increases energy consumption.

• The second source of energy waste is *idle listening*. A sensor node enters this mode when it is listening for a traffic that is not sent. This energy expended monitoring a silent channel can be high in several sensor network applications.

• The third source of energy waste is *overhearing* which occurs when a sensor node receives packets that are destined to other nodes. Due to their low transmitter output, receivers in sensor nodes may dissipate a large amount of power.
• The fourth major source of energy waste is caused by *control packet overhead*. Control packets are required to regulate access to the transmission channel. A high number of control packets transmitted, relative to the number of data packets delivered indicates low energy efficiency.

• Finally, *frequent switching* between different operation modes may result in significant energy consumption. Limiting the number of transitions between sleep and active modes.