MAC PROTOCOLS

Marc KASSE - INSA 5ISS

Table des matières

I. Description

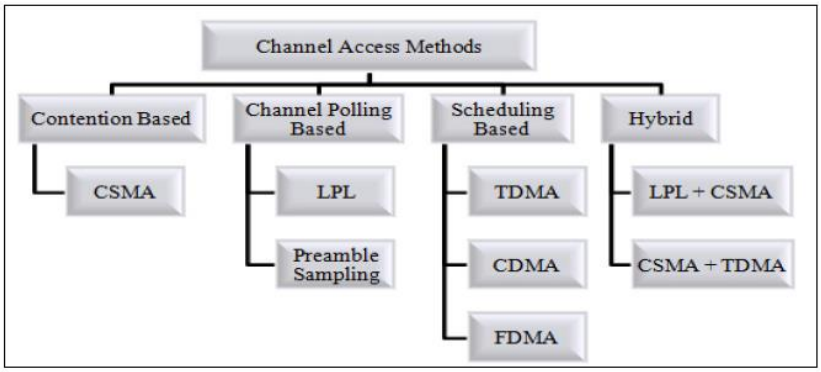
The OSI model is a communication protocol between computers that is based on 7 differents layers with defined roles. It means that in order to establish a communication between 2 machines, 7 elements are necessary.

The MAC sub-layer is a part of the data link layer which is in charge of the connection between devices on a local network. It provides the channel access mechanism to several medium sharing devices. A MAC protocol manages the communication traffic on a shared medium and creates a basic network infrastructure for sensor nodes to communicate with each other.

MAC protocols are concerced about optimisation of following criteria (source of energy dissipation) :

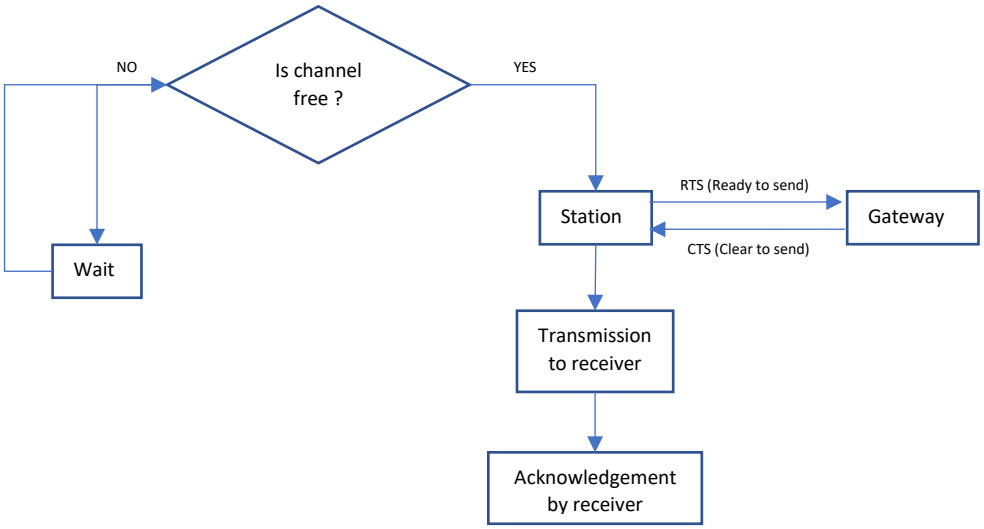
- Overhearing (time of listening of the channel)
- Passive listening (radio on but nothing to transmit)
- Collisions
- Protocol overcost (number of information transported in PDU)
- Utilisation rate of channel

II. Access Methods



1) CSMA (Carrier Sense Multiple Access)

CSMA/CA (CA stands for Collision Avoidance) is a method of media access. Each device (also called station) is free to communicate when the channe is free. It is useful when several device use a shared channel.

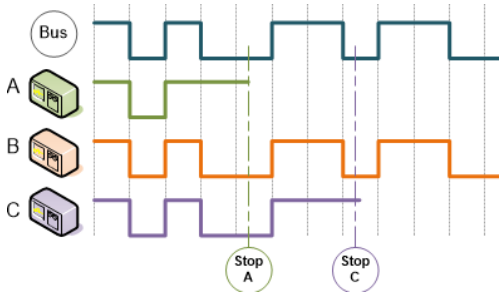


The MAC layers is informed about any collisions by the reception of the acknowledgement. If no acknowledgement received, it retransmits directly in a fast way.

To listen the channel, MAC layer and the PHY layer which uses an algorithm CCA (Clear Channel Detection) to evaluate the disponibility of the channel. The PHY layers measures the signal power RSSI and compare it to a threshold. Then, the PHY layer informs the MAC layer.

There 2 additionnal methods :

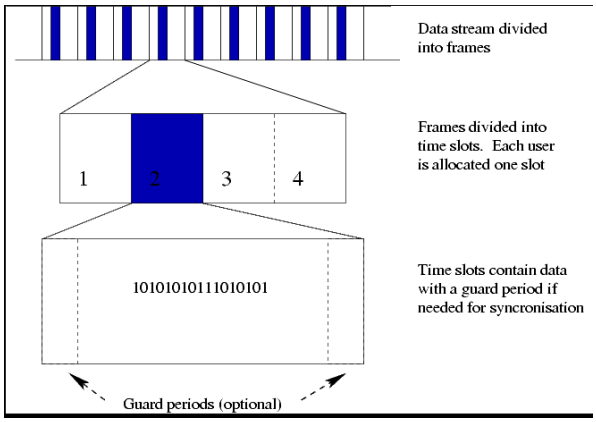
- CSMA/CD (Collision Detection) : the station is in self management and waits the media to free before transmitting. If a collision is detected, the operation is stopped and restarted after a defined time.
- CSMA/CR (Collision Resolution) : transmission is stopped once a collision is detected.



The problem with CSMA is that the number of collision increases with the node density. It is adapted to low traffic.

2) TDMA (Time-division multiple access)

Thanks to the attribution of different slots, each nodes can transmit at different times without causing collisions.



Problems that could be raised are the fact that it is more difficult to implement ; it uses more energy du to synchonization of nodes ; it is not flexible. Also when the traffic is slow, few slots are unless but still listening leading to high consumption .

3) LPL (Low power listening)

Each device has a passive period and active period. The duty cycle is the proportion of the active period over the passive period.

The main issue is to synchronize the awake period of the receiver nodes with the one of the transmiter node.

To help synchronization, each transmission of one packet is followed by the transmission of a long preamble.

LPL approach is based on the duration of transmission of the preamble, sent just after the packet. This preamble allows one receiver to transmit. The receiver is synchronised with the transmitter but meanwhile no other node can access the media during the transmission of the preamble.

4) LPP (Low power probing)

The receiver starts the communication by the diffusion of one beacon that informs his neighbors that it is ready to receive. The transmiter sends his packets as soon as it detects the beacon. Every node his memorize the sequence of active and passive periods of his neighbors.

Compared to the LPL, the transmission of the preamble is reduced and the channel can be free.

5) The point coordinated function (PCF)

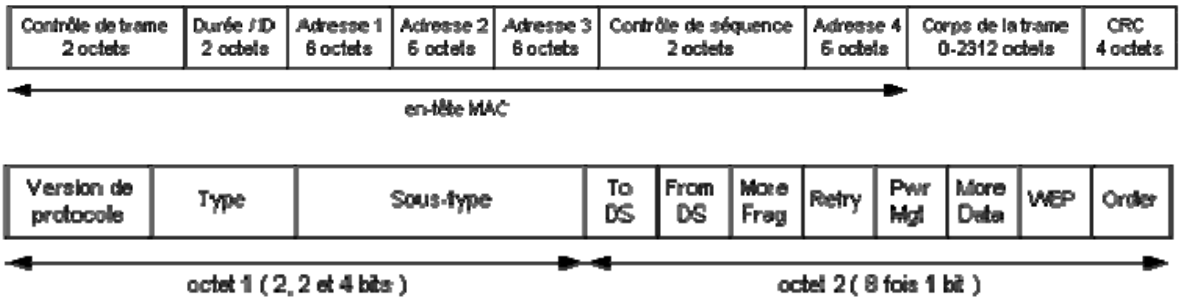
The point coordinated function (PCF) is localised on the point of access. PCF sends a frame to the different stations one by one and gives authorization to one station to transmit towards another station. Then, station waits for an acknowledgement from the PCF before transmitting.

III. Frame

The preambule includes a sequence used by the PHY layer to select the appropriate antenna and correct the frequency and synchronisation offset.

The header PLCP includes the logical informations needed to decode the frame.

The data MAC frame is composed as followed :



CRC is the cyclic redundancy check.

IV. Security

The goal of attackers is to affect network performances and degrad wireless channel quality. It can be classified in 2 categories : Faked clear-to-send or Faked request-to-send. Below is an example of security vulnerability in Cooperative MAC for IEEE 802.11g or 802.11n.

We can list few techniques that attackers use :

- Continuous Access Channel consists of keeping the channel busied and don't let any other devices have access to the channel
- Emission of a wrong acknowledgement to avoid one node to transmit data
- Unfairness : redirection of data to another node or violation of the time constraint related to transmission of data
- Generate random jammings
- Reactive jammings, only jamming when a node is emitting.
- Generate collisions and avoid messages RTS or CTS to arrive to his receiver
- Generate collisions by sending of periodic bits
- Interrogation is generated when an attacker consumes energy of a node by constantly sending RTS messages and receiving CTS messages.

Couche liaison de données	4. Création de collisions, brouillage « intelligent » 5. Épuisement de la batterie 6. Accaparement du canal de transmission 7. Falsification d'accusés de réception

V. Localisation

The whole process of localization is carried out by exchanging messages among the nodes at MAC level. It enables I-hop measurement among nodes, the global process and the position refinement process for each sensor node.

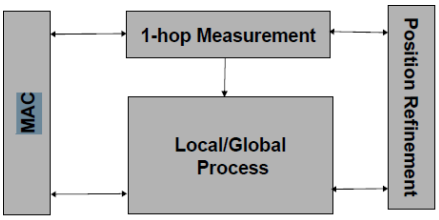


Figure 2.5: Localization Block Diagram

There are several way to **measure** and estimate the distance of communicating nodes :

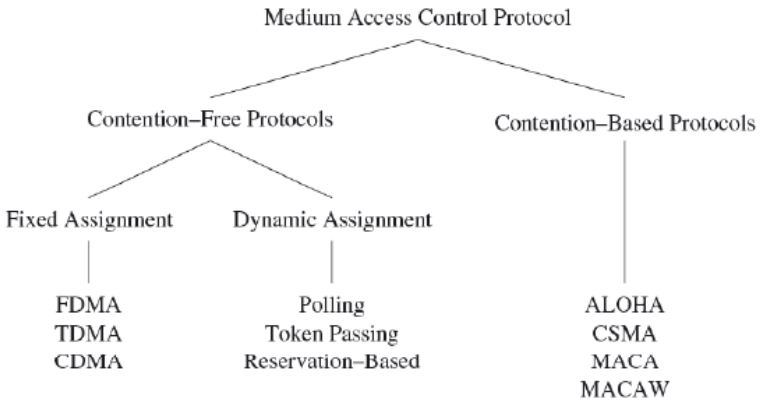
- By angle : very expansive
- RSSI (Received Signal Strength Indicator) : easy to use but no calibration possible and environement dependant
- Time Difference of Arrival (TDoA)
- Time Arrival (ToA) or Time of Flight (ToF) : use of ultrasound signal in combination (need ultrasonic transducer which takes place and is costly)
- Radio Frequency Time of Flight (RF TOF) based Ranging : interferences and clock drift can be improved thanks to Ultra Wide Band (UWB)

There are also different computation techniques to get node's coordinates from estimated distance.

In localization application, the interaction with the MAC layer helps saving the energy consumption.

VI. MAC Protocols

Over the years, several MAC protocols have been developped for WSN and are categorized as below. MAC protocols are categorised according to the way they access the channel.



1) SMAC

A node transmits the sequence of active and passive periods then the other node do the same. Finally, each node memorised the sequence of his neighbors. This protocol is problematic because it does not adapt to the traffic.

2) TMAC

TMAC is an evolution to SMAC. It allows to adapt the active period to the traffic. But there is overlistening because none-involved nodes have to stay active during the transmission period.

3) BMAC

BMAC uses Low Power Listening (LPL) and can adapt the size of the preamble resulting in the increase or decrease of the active period where nodes are listening. However, each node have to listen the preamble even if it not the receiver. Also it suffers from problems of CSMA/CA. XMAX is an improvement of BMAC.

4) ContikiMAC

It is widely used in industry. Compared to XMAC, data packet are transmited directly instead of transmiting preambles. Hence, the size of packets is reduced. It introduces the phase lock which the time when a node is waking up. An emitter memorizes the different phases lock of every receiver like this it can transmit only during the phase lock. It is inspired from WiseMAC protocol.

5) ZMAC

ZMAC is an hybrid protocol using CSMA and TDMA. When the traffic is low, it uses CSMA and when the traffic is high it uses TDMA. We talk about « slot stealing » because slots not used are stole and used by other nodes to transmit. But the access of slots is difficult because slots are synchronized. Then it is energy consumming because to know if one slot is free, we must wait a certain amount of time.

Conclusion

WSN are concerned by energy efficiency, scalability and latency (not exhaustive). The different MAC protocols have been developped to improve one or more criteria. It is important to identify the need when developping an Iot system. Methods to be used are chosen according to the described criteria.

The MAC layer is a key point for localisation application even if there is not many information availabe on the Web. The MAC layer is appropriated because it can deals with the processing and communication of data.