Yanis Imekraz

Wireless Sensor Network - MAC Protocols

Channel access type :

Carrier Sense Multiple Access (CSMA) :

CSMA is a media access protocol. Before sending a trame, it'll check the disponibility of the transmission medium. There is 3 main methodes which are :

CSMA/CD (Collision Detection)

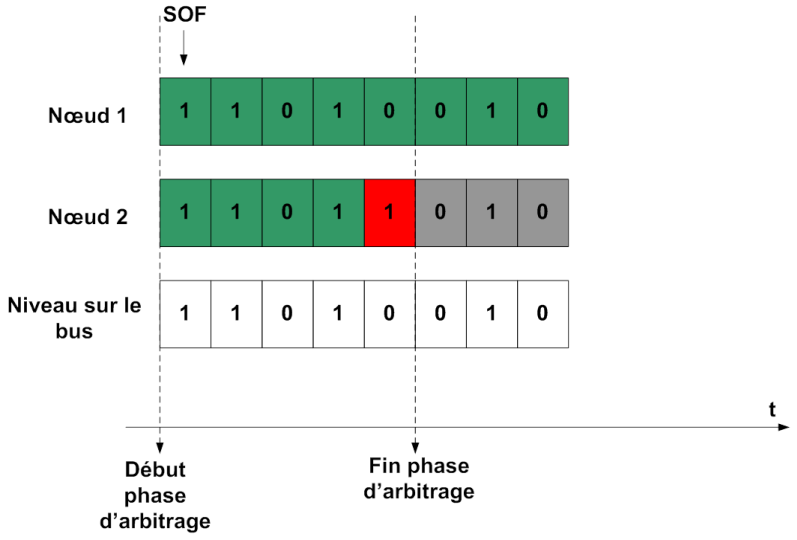
CSMA/CA (Collision Avoidance)

CSMA/CR (Collision Resolution)

CSMA/CD is mainly used on wire network and work as follow : Before sending any data, each nodes listen to the medium to ensure that no one is currently transmitting data. If the medium is free, then any device can start it's transmitting. Throughout the transmission process, the transmitter must listen to the medium to ensure that it is the only one to have taken hold of the medium. If there is none, the data are considered as transmited. On the other hand, if another entity started transmitting at the same time, both stop transmitting and wait a random time before starting the transmission process again (back off).

CSMA/CA is mainly used on wireless network and work as follow : The process is the same as before but instead of transmitting data, it first transmit it's intention to send because two nodes can be out of reach from each others. The intend to communicate result in a send request (RTS - Request to Send) to the master station. The master station respond by a CTS (Clear to send) trame. If the node does not receive a reponse, then it considers this as a negative reply and waits a random time before resending its request.

CSMA/CR work as follow : The process is the same before starting a transmission. When a station transmits a message, it listens to the network and applies a logical AND between what it transmits and what it receives. If there is a discrepancy at a given time, it means that several stations are transmitting and the one which detects the collision stops transmitting.



Time Division Multiple Access(TDMA):

TDMA is a media access protocol with time distribution. Each node has is own period of time to transmit its message.

S-MAC :

This protocol use a CSMA/CA type medium access method with RTS/CTS (Request to send, Clear to send). What the S-MAC protocol bring compared to a classic CSMA/CA is a succession of sleeping and listening phase in order to reduce the power consumption of the nodes. But this succession of awakening and sleeping phase bring one trouble which is the synchronization of the nodes so that the communication is always possible. In the case that a transmission is in progress, the awake-sleep cycle is suspended until the transmission is complete.

The synchronization process work such as :

When a node wakes up, it first listens in order to not interrupt any transmission that are already started. If he did not hear anything for some time, it chooses a frame schedule and transmits it as a SYNC packet that contains the time until it falls asleep. This SYNC packet is broadcasted to all is direct neighbour. All the nodes are free to choose their own listen and sleep schedules but they try to coordinate their sleep schedules rather than randomly sleep on their own.

If a node has already adopted a sleep schedule but receives another schedule from a SYNC packet, it'll then adopt the two schedule and wake up at both active phase. It'll also send it's own schedule to the other nodes so that it know that there is another sleep schedule occurrence.

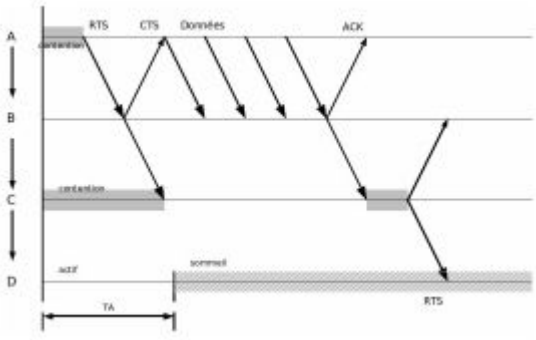
Each node has a NAV (Network Allocation vector) where it record the activity of the network. When a node receives a packet of which it is not the recipient, il'll update its NAV. It'll periodically decrease, if it's above zero. If the vector is not null it means that a transmission is in progress and the node will return in its sleeping state. Its the overhearing avoidance mechanism.

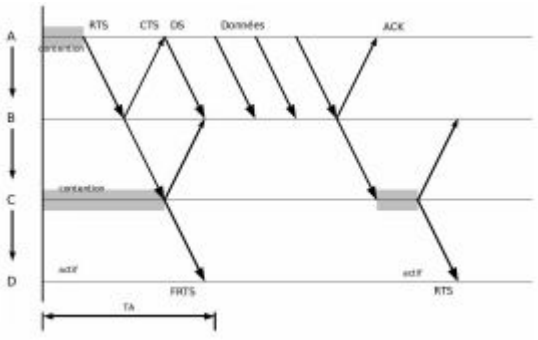
T-MAC :

This protocol also use a CSMA/CA type medium access with RTS/CTS. T-MAC or Timeout MAC used the same principle of S-MAC with two phases (Sleeping-Listening). What's different from S-MAC is that a node can return to a sleeping state before the end of the listening phase. When no activation envent occurs in a time TA which must be longer than the allocated time for a SYNC and a potential RTS, the node return to its sleeping state.

In some case, data flux can be troublesome for some node that are distant :

In this case, A and D are reachable with 2 hops from each others. If A want to send to D, it'll first send a RTS to B and B will reply with CTS that A and C will take notice off but D which is not a direct neighbour of B, will return to sleep due to TA that wind up.



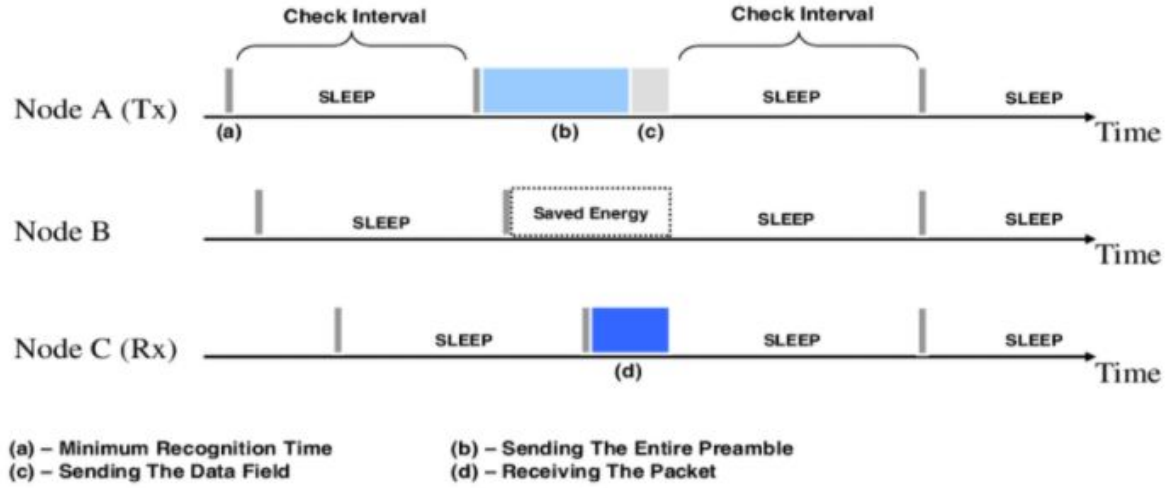


The mechanism of FRTS (Future request-to-send) is used in case like that. The C node'll send a FRTS to D so that D do not return to its sleeping state early.

B-MAC :

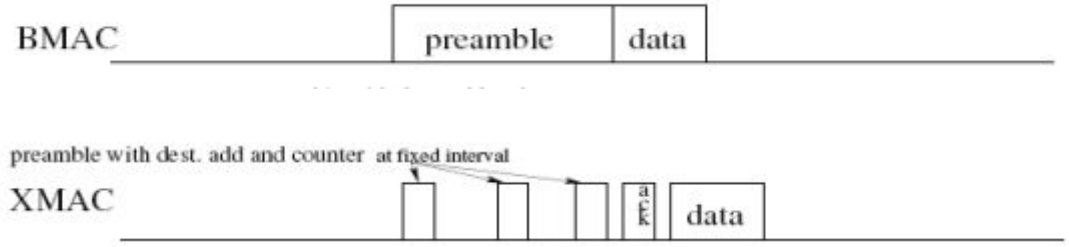
BMAC or Berkeley MAC is a mac protocol. It was developed by the University of Berkley. It uses the same principle of CSMA / CA. It differs from other protocols in the way it listens to the medium. It determines if the medium is free by listening to "noise" and signal strength. In the absence of noise, the medium is free and can therefore emit. In the other case, it is busy. Before starting data transmission, it must first send a preamble.

Most of their time the nodes are in a state of sleep and they listen to the noise when they wake up before going back to sleep if there is no noise or if they have nothing to make. If there is any, it is because a preamble is sent and therefore a node wants to send data. The preamble must be long enough so that the node have time to wake up. Following this, the node which made the request to send emits and all the nodes which are not the addressee return to their sleeping state. The B-MAC protocol is an asynchronous protocol, the nodes don't have to synchronize.



X-MAC:

The BMAC protocol uses a long preamble before sending the data to wake up the receiver. Despite the fact that this protocol is asynchronous and does not require SYNC between the nodes, these extended preambles are the real problem since the sender loses energy and creates latency due to its preamble. The XMAC protocol remedies this by sending more frequently a small preamble containing the recipient's address and the number of remaining preambles. When the receiver receives the preamble when it wakes up, it sends an Ack and the sending node can directly start the data transfer. The sending of preambles is designed so that the receiver has time to respond between each preamble.
When another node wants to transmit data but hears the preamble and the ACK of another node, it goes back to sleep for a random period of time but sufficient for the exchange already initiated.



Z-MAC:

Zebra Media Access Control (Z-MAC) is a network protocol for wireless sensor networks.
Z-MAC combines the two approaches Carrier Sense Multiple Access (CSMA) and Time Division Multiple Access (TDMA).
ZMAC ou Zebra MAC is a network protocol for wireless sensor network. Unlike the others, it use two channel access type depending on the traffic which are Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and Time Division Multiple Access (TDMA). The principle of hybrid protocols is to use one or the other depending on the traffic condition. In low data traffic, CSMA is preferred to TDMA while in the case of high traffic it is the reverse.

Localization & Nodes mobility:

The location of nodes is an information that can be acquired in two ways.
The first is to record the position of the nodes when they are put into service, the second is the use of a GPS. The first method is inconceivable. Manually registering all the sensors is unthinkable and moreover the nodes could not move. The other solution, with the GPS module is very costly and is very energy intensive.
Several localization systems have been developed to assign geographic coordinates to nodes. They use the strength of the received signal to calculate their distance to the transmitter. This is the RSSI (Received Signal Strength Indication). Its precision is a few meters which will limit its uses. Based on RSSI and lateration, several algorithms and methods have been developed such as Static Beacon, Mobile Beacon, Bounding Box and so on.

Security:

Sensor networks are susceptible to several attacks such as Identity Theft, Node Replication or DDoS.

In the identity theft attack, the malicious node takes a large number of identities that can be stolen or imagined.

The replication attack is when the attacker recovers a node. It extracts the secrets and it transfers them to generic nodes in order to deploy them to be able to subsequently inject the data in it.

Denial of service attacks are well known and the malicious node floods the radio frequencies used by the network with noise in order to prevent transmissions.

Some security mechanism are deploy depending the scenarios of applied architectures and concerns of security requirements in WSNs. Node authentication, Key establishment, AES encryption,Key revocation and Comparison of wavelengths.

Power consumption:

In SMAC and TMAC, energy savings at high traffic is due to Overhearing avoidance. More neighbour nodes sleep for more time on hearing RTS and CTS when traffic is high, at low traffic they do not hear RTS/CTS thus wasting energy in idle listening during fixed duty cycle. Such observation is not seen in BMAC and XMAC. TMAC has better performance than SMAC due to waiting for timeout and falling asleep earlier.

Regarding BMAC and XMAC, XMAC optimizing the preamble alongside TMAC, reduces its energy consumption.

Thus, the order of energy consumption is:

XMAC<BMAC<TMAC<SMAC.

https://inet.omnetpp.org/docs/users-guide/ch-sensor-macs.html

http://www.julienvaudour.fr/fichiers/memo.pdf

https://arxiv.org/ftp/arxiv/papers/1205/1205.1701.pdf

http://cpham.perso.univ-pau.fr/ENSEIGNEMENT/PAU-UPPA/PROTOCOLES/Capteurs.pdf

https://arxiv.org/ftp/arxiv/papers/1301/1301.5065.pdf

https://hal.archives-ouvertes.fr/hal-01373430/document

https://www.researchgate.net/publication/265845857_Localization_in_wireless_sensor_networks_Classification_and_evaluation_of_techniques

https://arxiv.org/ftp/arxiv/papers/1205/1205.1701.pdf