Mac Layer for Wireless Sensor Network

Abderrazzak Mahraye

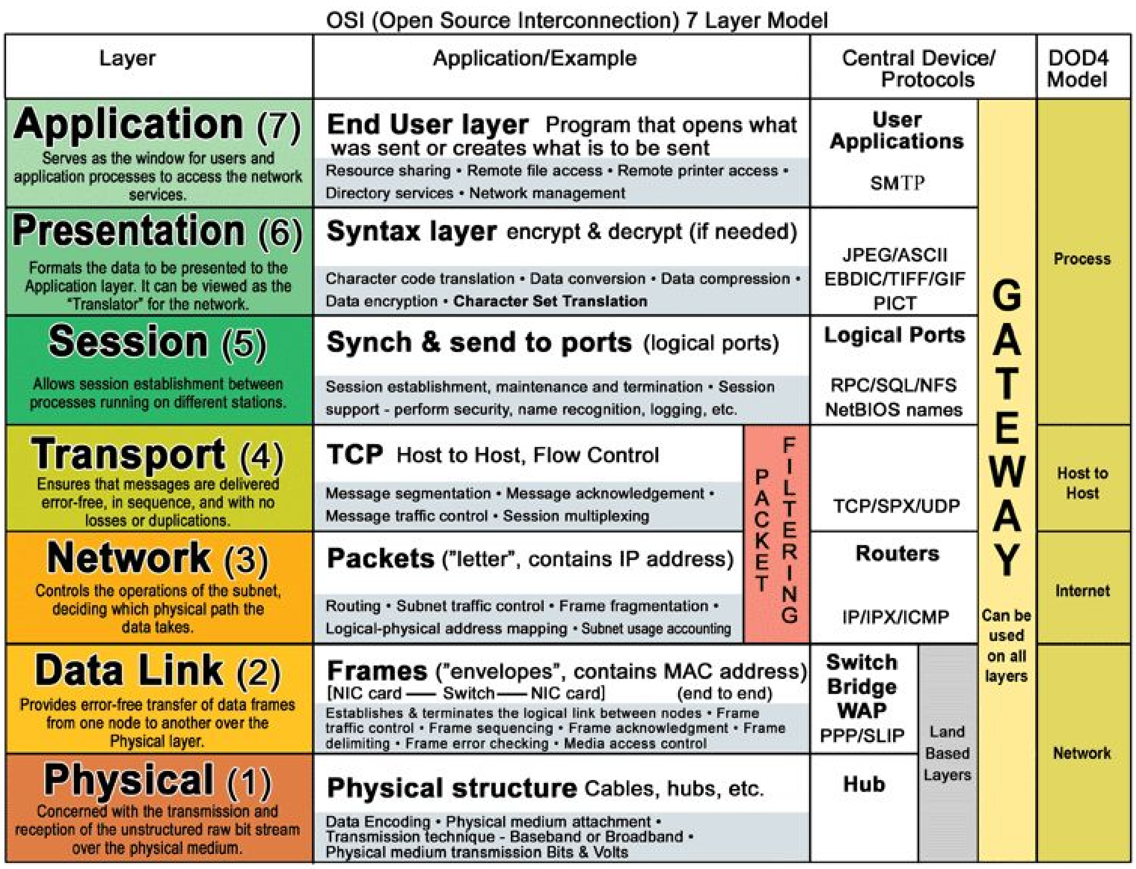
INSA TOULOUSE ISS B1

I Introduction

As part of the courses of Protocols for connected objects this document aims to make the state of the art and a comparison of the different MAC layers for WSN (Wireless Sensor Network). With the emergence of wireless sensor networks, new protocols have been implemented. It is important to know them and to understand how a MAC layer has a primordial role to play in systems' communication.

II The MAC layer

MAC Layer is the second layer in the seven-layer OSI model for network protocols. The OSI (Open Systems Interconnection) is a conceptual model which characterizes and standardizes the functions of communication systems. The next figure shows the different layers of OSI:



Thus, we will focus on the second layer called Data Link, and especially on the sub-layer responsible for controlling how devices in a network gain access to a medium and permission to transmit data: the MAC layer.

MAC layer aims to encapsulate frames in order they can be suitable for transmission via the physical medium. In fact, a MAC layer works with MAC addresses, and each device/component has its own address in the network (As example, a PC has a MAC address that allows its identification). MAC address is assigned to a network adapter at the time of manufacturing and they have the following structure: six groups of two hexadecimal digits (for example : *9C:35:5B:5G:4C:D7)*. Its six first digits correspond to the manufacturer and consequently are common for the devices from the same manufacturer. And, the six last correspond to the network interface card.

III MAC LAYERS FOR WSN COMPARISON

III.1 MAC protocols categories

There are several MAC protocols that use different technologies. The next figure shows these different categories. The next sections will be about some of them.

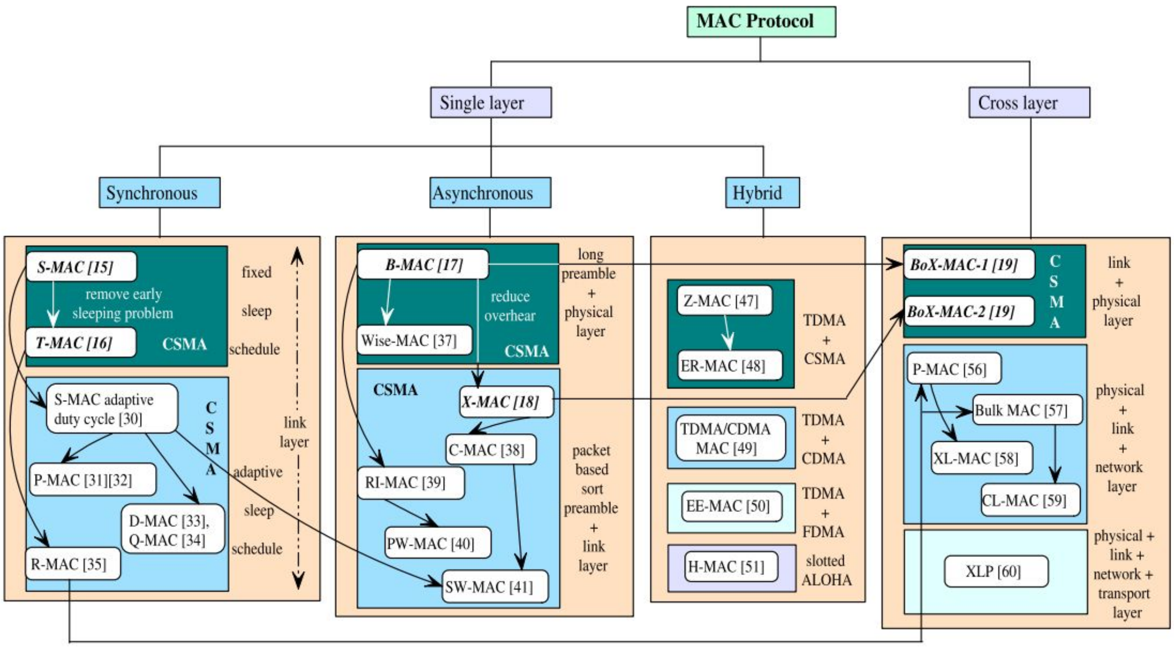


Fig. 6. Taxonomy of MAC protocols.

III.1.1 TDMA

Time Division Multiple Access is a protocol that uses temporal division of the bandwidth. Each device can send when his turn arrives.

III.1.2 CDMA

Code Division Multiple Access is a protocol that uses orthogonal code for each communication. Consequently, it is possible to recover every different trame even if they are sent at the same time.

III.1.3 CSMA

Carrier Sense Multiple Access is a protocol where the sender listens to the medium in order to know when it is possible to make an emission. Before sending a trame, it'll check the disponibility of the transmission medium. There is 3 main methods which are :

CSMA/CD (Collision Detection)
CSMA/CA (Collision Avoidance)
CSMA/CR (Collision Resolution)

The first version was **CSMA/CD**: It is mainly used on wired networks. In this version, the sender listens to the medium all the time and checks that no message is being transmitted when it wants to transmit one. Moreover, if two entities send a trame at the same time, both must stop the transmission and wait a time before resending their trame (this is called back off).

The second version was **CSMA/CA**: It is mainly used in wireless network. In this version, every entity has to request an authorization (*RTS - Request to Send*) to the master entity before sending the trame. If the entity does not receive a response then it considers this as a negative reply (authorization denied). It must wait a random time and resend a RTS.

The last version was **CSMA/CR:** The process is the same before starting a transmission. But, the receiver 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.

III.1.4 FDMA

Frequency Division Multiple Access is a protocol that uses frequency division of the bandwidth. Each device has its own frequency.

III.2 MAC layers for WSN

There are two categories of MAC layers for WSN : **schedule-based** and **contention-based** protocol. **Schedule-based** protocols include TDMA, FDMA and CDMA and **contention-based** protocols include IEEE 802.11, S-MAC, T-MAC. These protocols will be explained in the next parts.

III.2.1 Schedule-Based Protocols

The purpose of these protocols is that they allow each node to make a transmission at a specific time.

LMAC

The Lightweight Medium Access Protocol is one from the TDMA protocol. It works as follows: each entity has a time slot where it can send a header to other entities in order to prevent that it wants to send a packet. Once the others get this header, they can not transmit and wait for the first entity to send its packet over the medium.

ZMAC

The Zebra Medium Access Protocol is a hybrid protocol. In fact, it combines the two approaches Carrier Sense Multiple Access (CSMA) and Time Division Multiple Access (TDMA).

It works as follows: an entity can use wasted time slots to send their packets. Consequently, an entity can use the time slot of other entities: the collision-free is not guaranteed.

TRAMA

The Traffic Adaptive Medium Access Control Protocol is a complex protocol that works as follows: Each entity transmits a broadcast in order to discover all its two-hops neighbours. Then, only the node in a two-hop neighborhood will transmit in a given slot.

III.2.2 Contention-Based Protocols

The purpose of these protocols is that they handle the issues of collision. Their main benefits is that they can manage the fluctuation of the traffic over the network. However, they are not efficient regarding the energy consumption insofar as they spend a lot in listening over the network.

S-MAC

The Sensor Medium Access Control Protocol is a WSN specialisation. It uses the CSMA/CA protocol and works in duty cycle as follows: A cycle is composed of a synchronisation phase, an active phase and a sleep phase. But this succession of awakening and sleeping phases bring one trouble which is the synchronization of the nodes. Consequently, if a transmission is in progress the active and sleep phase cycle is suspended in order to allow the transmission to finish.

The synchronisation cycle works such as: once a device wakes up, it listens to the medium in order to discover if any transmission is in progress. If it does not hear anything, it transmits a synchronisation packet that contains the time needed before it falls asleep. 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 is already asleep and receives a SYNC packet it can adopt the two schedules and wake up at both active phases and send its schedule.

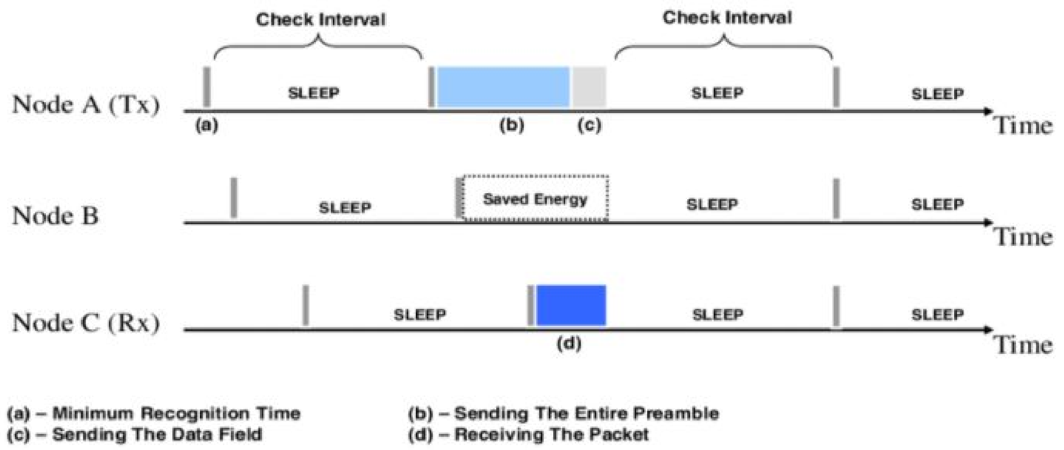
T-MAC

The Timeout Medium Access Control Protocol uses also the CSMA/CA protocol and works in duty cycle but an adaptive one as follows: It uses only the active phase and a sleep phase, there is not a synchronisation phase. A node goes to sleep if it doesn’t detect any activity. Then it goes again in active mode after a sleep period. The total amount of energy used is less than for S-MAC and it gives better results but it can be harmful to the network performance.

III.2.3 Others MAC Protocols

B-MAC

The Berkeley Medium Access Control Protocol uses also the CSMA/CA protocol and works as follows: It differs from the other CSMA/CA protocol in the way that it discovers if the medium is free. In fact, a device listens to the “noise” and the signal strength to determine if the medium is free. If there is noise, the medium is not free, if not, the medium is free. Once the medium is free, the device must send a preambule packet to prevent the other device that the medium is not free (they listen to the noise in the medium, and the preambule product noise in the medium). Then, the device can send the request to send a packet, and the devices that are not receiver fall asleep to allow the transmission from the sender device to the receiver device. The next figure explains this mechanism:



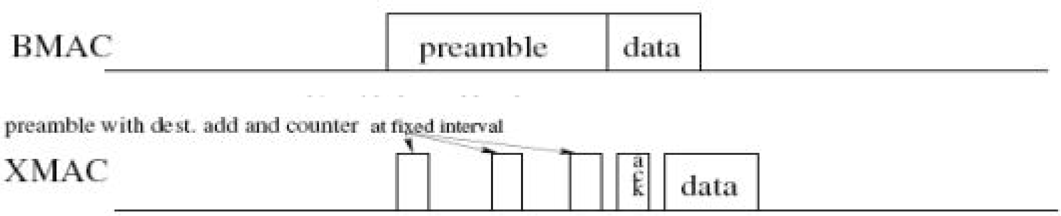
X-MAC

The X Medium Access Control Protocol also uses the CSMA/CA protocol. The BMAC protocol uses a long preamble which is not efficient in terms of energy consumption insofar as the sender loses energy and creates latency due to its long preamble. The XMAC protocol corrects this issue by using short preambles which contain their numbers and the receiver adresse.

Consequently, once the receiver receives the preamble, it sends an Ack packet in order to prevent the sender, and allow the sender to send its data.

Like BMAC if another node wants to transmit data but it listens to a preamble, it falls asleep for a random period of time in order to enable the sender and receiver to make the transmission.

The next figures explain and compare the BMAC and XMAC mechanisms:



IV CONCLUSION

There are a lot of MAC protocols existing for WSN. I presented only the commonly used MAC protocols, the list is a non-exhausting one. There are a lot of other MAC sophisticated protocols. What I have learned is that there is a MAC protocol for each use case and requirements of a system. Consequently, I will take seriously into account the MAC protocol when I will have to develop a system depending on its specification.

IV SOURCES

https://www.researchgate.net/figure/Protocole-TRAMA-Traffic-Adaptative-Medium-Access-Control-Cette-methode-se-base-sur-le_fig13_308802089

https://www.researchgate.net/publication/235930503_Code_Contribution_Implementation_of_the_B-MAC_Protocol_for_WSN_in_MiXiM

https://publications.waset.org/10002124/performance-evaluation-of-xmac-and-bmac-routing-protocol-under-static-and-mobility-scenarios-in-wireless-sensor-network

https://link.springer.com/chapter/10.1007/978-3-642-37949-9_4

https://www.researchgate.net/publication/329514255_A_Taxonomy_for_MAC_Protocols_in_Wireless_Sensor_Networks_Based_on_Traffic_Prioritization

https://www.researchgate.net/publication/272623927_Comprative_Analysis_of_WSN_MAC_Protocols

https://www.researchgate.net/publication/283297218_OSI_layers