INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
TOULOUSE

Mac Layers for Wireless Sensors Networks

Protocols for Wireless Sensor Network

SUBMITTED BY

Yacine BENCHEHIDA 5ISS-A2

UNDER THE GUIDANCE OF

Prof. **Daniela DRAGOMIRESCU**

Academic Year: 2021-2022
November 19, 2021

Contents

Introduction

This report intends to discuss most of the MAC layers that could be used for the deployment of a wireless sensor network. With the emergence of wireless sensor network, new MAC protocols have been implemented. Indeed, Wireless sensor networks (WSN) are interconnected sensor nodes that communicate wirelessly to collect data about the surrounding environment.

The objective here is to present many available MAC Layer implemented in WSN and also their characteristics.

MAC Layer: *Media Access Layer*

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers:

- The logical link control (LLC) sublayer
- The medium access control (MAC) sublayer

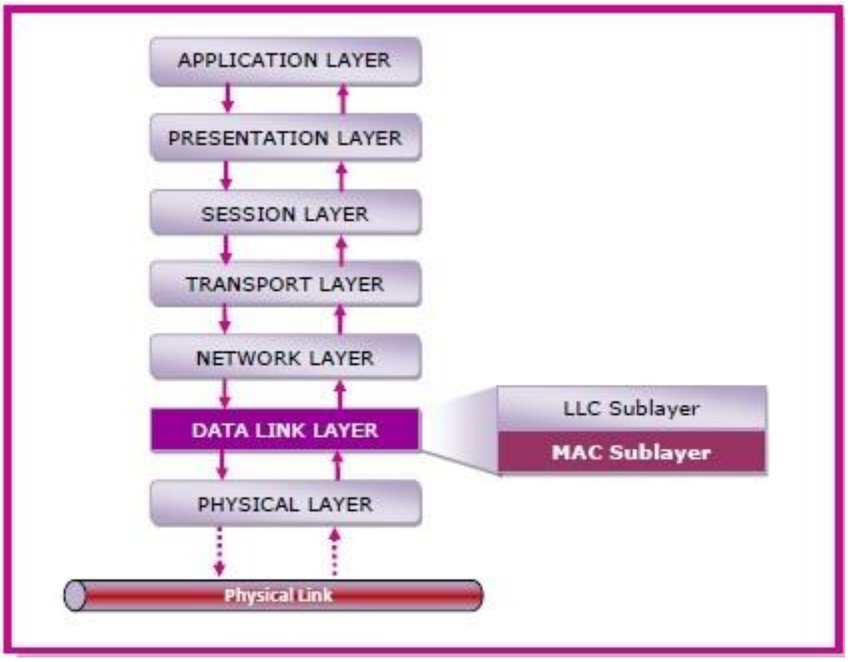
1. Generalities

The Medium Access Control layer (MAC) is the interface between the physical and the network layer. As it is evident from the name itself that for the Data link layer, the MAC layer serves the purpose of managing the media access to different devices. MAC Layer is one of the two sub-layers that are implemented as the **Data Link layer** of the OSI model.

It is part of the layer two in the seven-layer OSI reference model for network protocol design *(Figure1)*.

Figure 1:

OSI Model



OSI model is a conceptual model that characterises and standardises the communication functions of a telecommunication or computing system.

MAC layer function is to manage the access of the physical layer and thus, to allow multiple nodes to transmit on the same communication medium, that's why we're really interested by MAC layer in WSN.

2. Operating mode

MAC is the lower sublayer of the data link layer. The LLC sublayer communicates with the network layer while the **MAC sublayer allows various network access technologies**. MAC takes data from LLC, adds header and tail bytes and sends them to lower physical layer for transmission.

The main functions of the MAC layer are that:

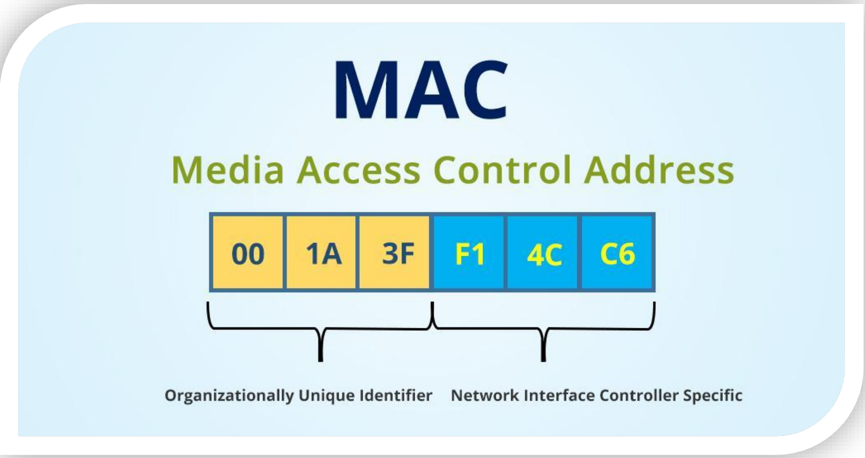
- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

Every device on a network has a unique number, generally called a MAC address, that is used by the data link layer protocol to ensure that data intended for a specific machine get to it properly. MAC layer works with MAC addresses. This address is assigned to a network adapter at the time of manufacturing.

As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator:

Figure 2:

Structure of MAC Address


MAC
Media Access Control Address
00
1A
3F
F1
4C
C6
Organizationally Unique Identifier
Network Interface Controller Specific

MAC Layer protocols for WSNs must **be energy efficient to maximize the lifetime**. Additionally, protocols must be scalable according to the network size and should adapt to changes in the network such as addition of new nodes, death of existing nodes, and transient noise on the wireless channel.

MAC Layers for Wireless Sensor Network

In WSN, efficient MAC protocols are present in the literature some of them are discussed in this report with their essential properties.

1. **Classification of MAC protocols**

Nowadays, several MAC protocols are implemented and used in different use case. We classified these MAC protocols into four categories:

- Contention based protocols without reservation (free).
- Contention based protocols with reservation.
- Contention based protocols with scheduling mechanisms
- Hybrid protocols which are other MAC Protocols.

The Figure 3 illustrates the first four MAC Layer categories:

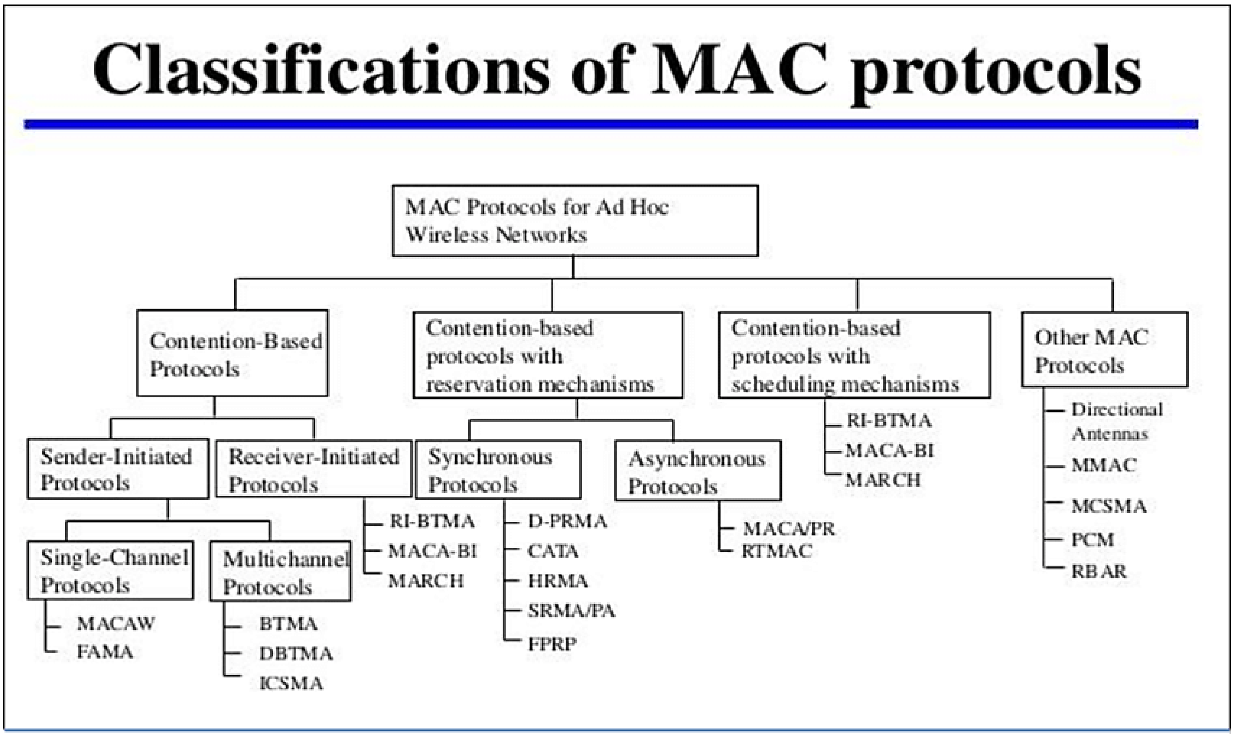

Classifications of MAC protocols
MAC Protocols for Ad Hoc Wireless Networks
Contention-Based Protocols
Contention-based protocols with reservation mechanisms
Contention-based protocols with scheduling mechanisms
Other MAC Protocols
Sender-Initiated Protocols
Receiver-Initiated Protocols
Synchronous Protocols
Asynchronous Protocols
RI-BTMA
MACA-BI
MARCH
Directional Antennas
MMAC
MCSMA
PCM
RBAR
Single-Channel Protocols
Multichannel Protocols
RI-BTMA
MACA-BI
MARCH
D-PRMA
CATA
HRMA
SRMA/PA
FPRP
MACA/PR
RTMAC
MACAW
FAMA
BTMA
DBTMA
ICSMA

Figure 3: Classification of MAC protocols

General definition of contention-free protocols

Here, the channel access policy is based on competition. Whenever a node needs to send a packet, it tries to get access to the channel. These protocols cannot provide QoS since access to the network cannot be guaranteed beforehand.

General definition of contention-based protocols

These protocols provide bandwidth reservation ahead (CSMA); therefore, they can provide QoS
support. These can be further subdivided into:

- **Synchronous Protocols:** there is time synchronization among all nodes in the network, the nodes in the neighbourhood are informed of the reservations.

- **Asynchronous Protocols**: no global synchronization is needed. Relative time is used for the reservations.

General definition of contention-based protocols with scheduling mechanisms

There can be packet scheduling at the nodes, or node scheduling for access to the channel (TDMA). Node scheduling should not treat the nodes unfairly. Some of these protocols consider battery power in their node scheduling.

General definition of hybrid protocols

These protocols combine contention based (CSMA) and contention based with scheduling mechanisms (TDMA) principles.

Moreover, we can also find MAC protocols especially designed to meet the requirements of WSN such as S-MAC, T-MAC, DS-MAC, A-MAC… We will detail these different MAC layers in the following sections.

1.1 FDMA – Frequency Division Multiple Access

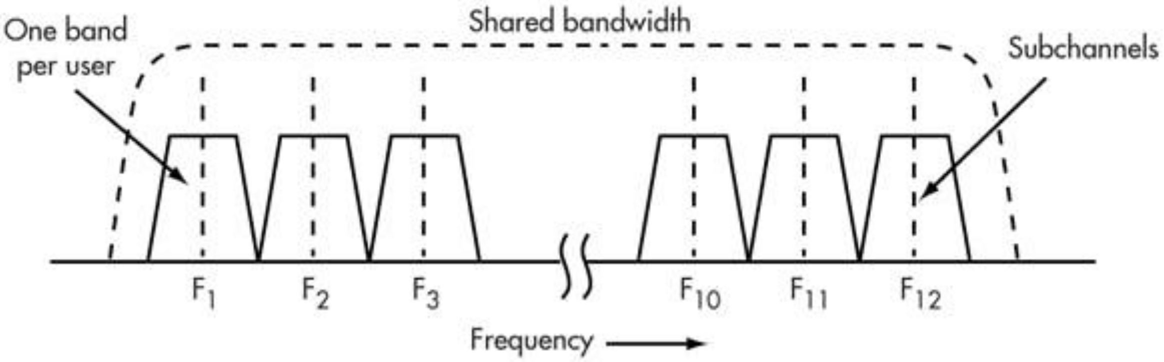


Figure 4: FDMA Principle

FDMA is the process of dividing one channel or bandwidth into multiple individual bands, each for use by a single user (Figure 1). Each node is assigned a unique frequency to transmit. Indeed, it's possible to add guard bands to separate each channel in order to limit the interference between them.

This MAC protocol is used in optic fiber communications systems, cable television, satellite transmission… However, it is not adapted for WSN because the implementation of protocols is very costly. The transceiver node must be able to receive on direct frequencies.

Thus, it is not the best solution as **the scalability is limited** due to the fact that each user is allowed a certain channel whereas WSN can be supported almost 1,000 nodes.

1.2 TDMA – Time Division Multiple Access

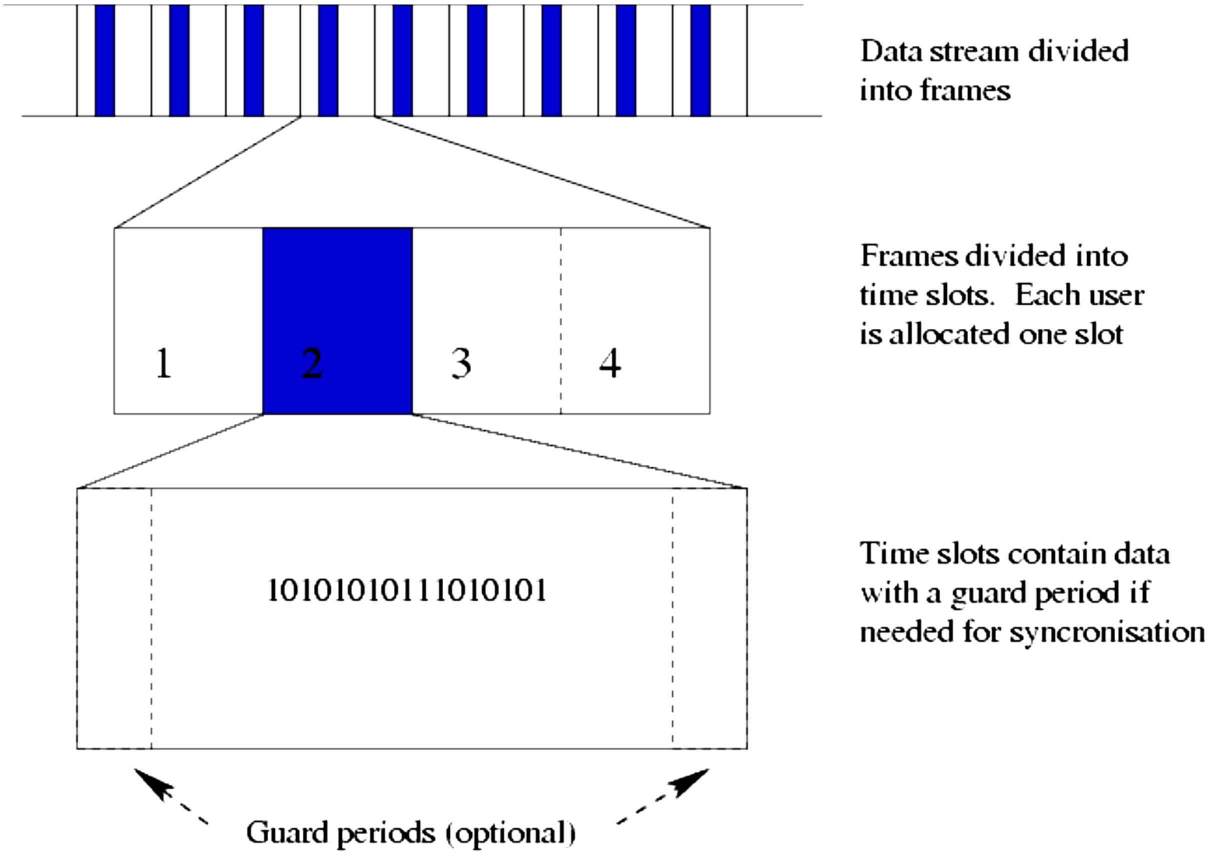

Data stream divided into frames
Frames divided into time slots. Each user is allocated one slot
1
2
3
4
Time slots contain data with a guard period if needed for syncronisation
10101010111010101
Guard periods (optional)

Figure 5: FDMA Principle

TDMA is a digital technique that divides a single channel or band into time slots. Each time slot is used to transmit one byte or another digital segment of each signal in sequential serial data format. Moreover, slots are allocated in the beginning and can sometimes be reallocated.

This MAC protocol is used in the cellular network like GSM (8 slots), GPRS, LTE… Nevertheless, it is not appropriate for WSN because nodes must be synchronized in time not to infer with each other's otherwise a collision could be possible. So, the cost of the synchronization in terms of data rate is very high and also indirectly in terms of power consumption.

1.3 CDMA - Code Division Multiple Access

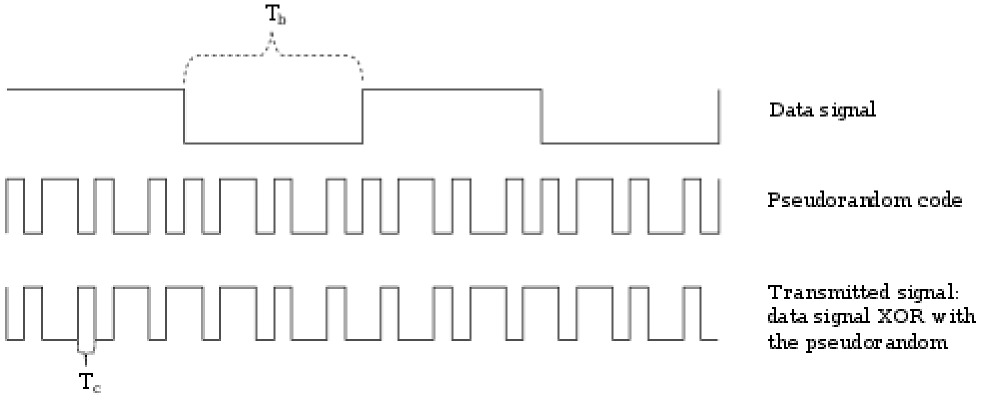


Figure 6: CDMA Principle

CDMA is another pure digital technique. It uses a code spreading technique (DS-SS), using a family of orthogonal or pseudo-orthogonal codes. Concretely, CDMA consists in "spreading the spectrum" by means of a code allocated to each communication. The receiver uses this same code to demodulate the signal it receives and extracts the useful information. There will therefore be several users in the same frequency band at the same time. The code itself carries no information.

This MAC protocol is used in the mobile network more specifically from the third generation (3G) cell-phone technology.

The operation requires significant computing power, and therefore more expensive components for consumer terminals. This can be a hindrance for WSNs because the devices available are limited in terms of computing power. Similarly, every transceiver requires complex electronics in order to generate the signal at emission and correlate with the specific code at the reception that’s why it’s difficult to implement it on WSNs.

1.4 CSMA - Carrier Sense Multiple Access

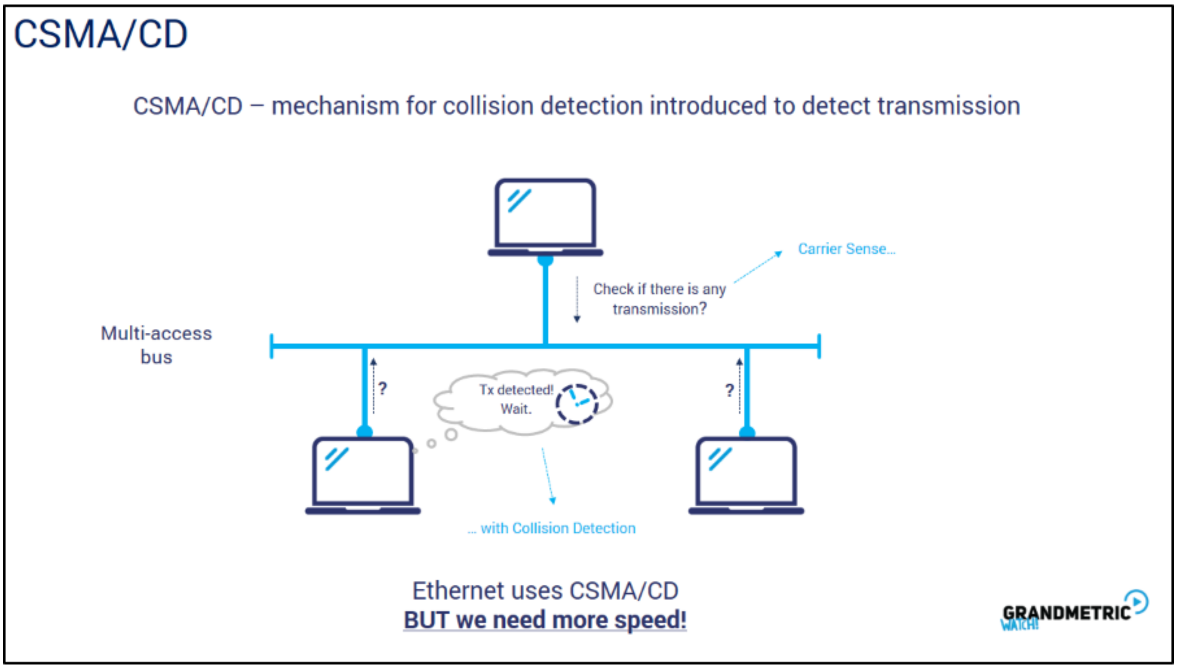
CSMA is a MAC protocol that senses the state of the shared channel to prevent or recover data packets from a collision. It is also used to control the flow of data packets over the network so that the packets are not getting lost, and data integrity is maintained.

In CSMA, when two or more data packets are sent at the same time on a shared channel, the chances of collision occurred. Due to the collision, the receiver does not get any information regarding the sender's data packets. And the lost information needs to be resented so that the receiver can get it.

Therefore, we need to sense the channel before transmitting data packets on a network. It is divided into three main parts, **CSMA/CA** (Collision Avoidance) and **CSMA/CD** (Collision Detection) and the last version **CSMA/CR**.

1.4.1 CSMA/CD

Collision Detection (CSMA/CD) avoids collisions by waiting for an idle signal before sending data. This was a protocol that was used in slower and less complex early networks. It’s a media access control method used most notably in local area networking.



CSMA/CD

CSMA/CD – mechanism for collision detection introduced to detect transmission

Carrier Sense...

Check if there is any transmission?

Multi-access bus

?

Tx detected! Wait.

?

... with Collision Detection

Ethernet uses CSMA/CD

BUT we need more speed!

Figure 6: CDMA/CD Principle

When two nodes send data packet at the same time, then a collision happens. When a collision happens, a jam signal is sent along the wire which tells all the nodes that there has been a collision in the wire. All the nodes stop sending data for a while, for a random time interval before resuming the sending process again.

1.4.2 CSMA/CA

CSMA/CA stands for Carrier Sense Multiple Access/Collision Avoidance. It means that it is a network protocol that uses to avoid a collision rather than allowing it to occur, and it does not deal with the recovery of packets after a collision. It is like the CSMA CD protocol that operates in the media access control layer.

In **CSMA CA**, whenever a station sends a data frame to a channel, it checks whether it is in use. If the shared channel is busy, the station waits until the channel enters idle mode. Hence, we can say that it reduces the chances of collisions and makes better use of the medium to send data packets more efficiently.

Here is the sequence diagram that shows how a device accesses the communication channel.

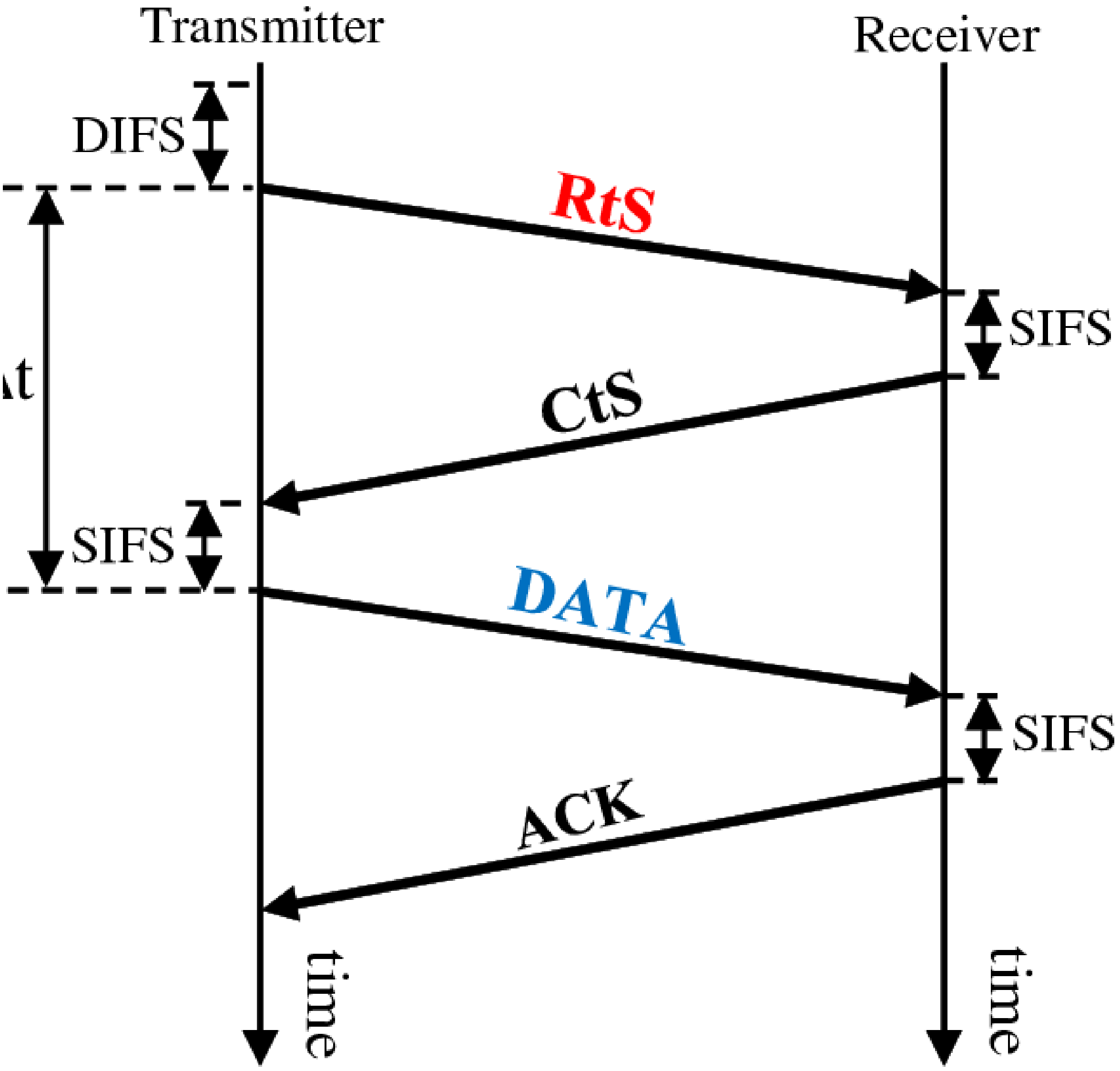


Figure 7: Simplified CSMA/CA diagram sequence with RTS/CTS

1.4.3 CSMA/CR

CSMA/CR stands for Carrier Sense Multiple Access with Collision Resolution. The process is the same before starting a transmission. It identifies a collision by additional sensing after data transmission starts.

If one station detects a collision, it transmits a jam signal to stop the other stations' transmissions and then retransmits the data without backoff, which resolves the next collision that may occur.

So, in this first part, we have seen that the classical MAC layers available were not too adapted to the WSN and to the requirements that this one must respect high scalability, low energy consumption ....

2. MAC Protocols designed for WSNs

We will now see the protocols adapted for WSN. The key requirements for these MAC protocols are the following:

- Collision avoidance
- Latency
- Scalability
- Energy efficiency
- Channel utilization
- Adaptability
- Range
- Data Rate

MAC Layer for WSN can be divided into two main parts: **Scheduled-based**, **Contention-based protocol** and **Hybrid protocols** must also be considered.

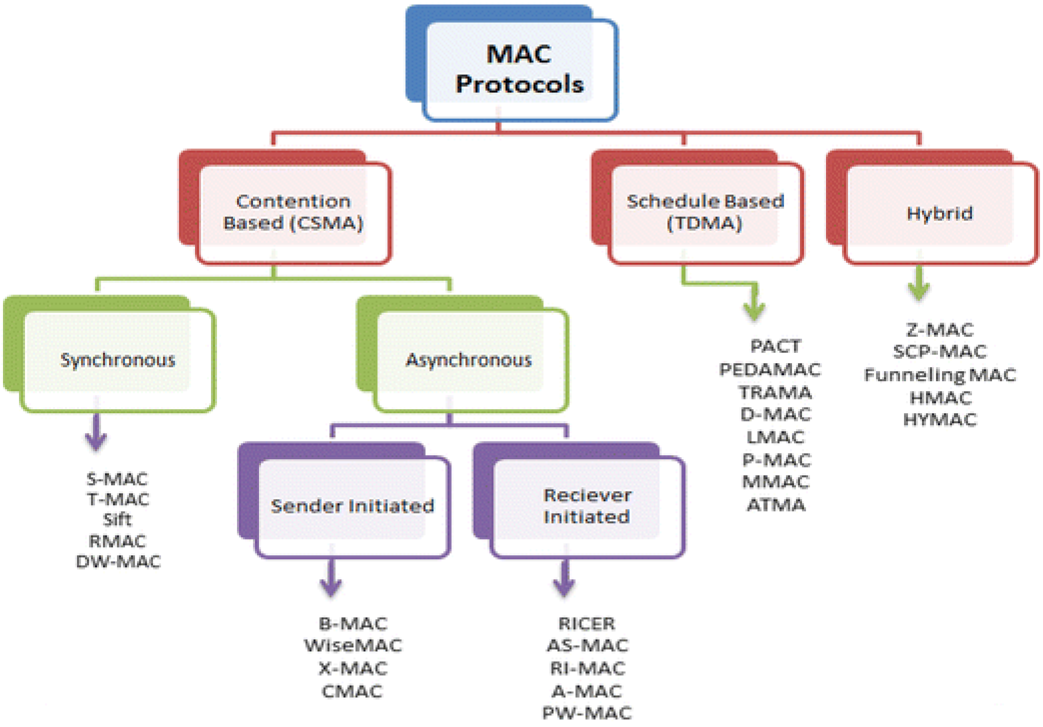


Figure 8: taxonomy of MAC Protocols

2.1 Contention-based MAC protocols

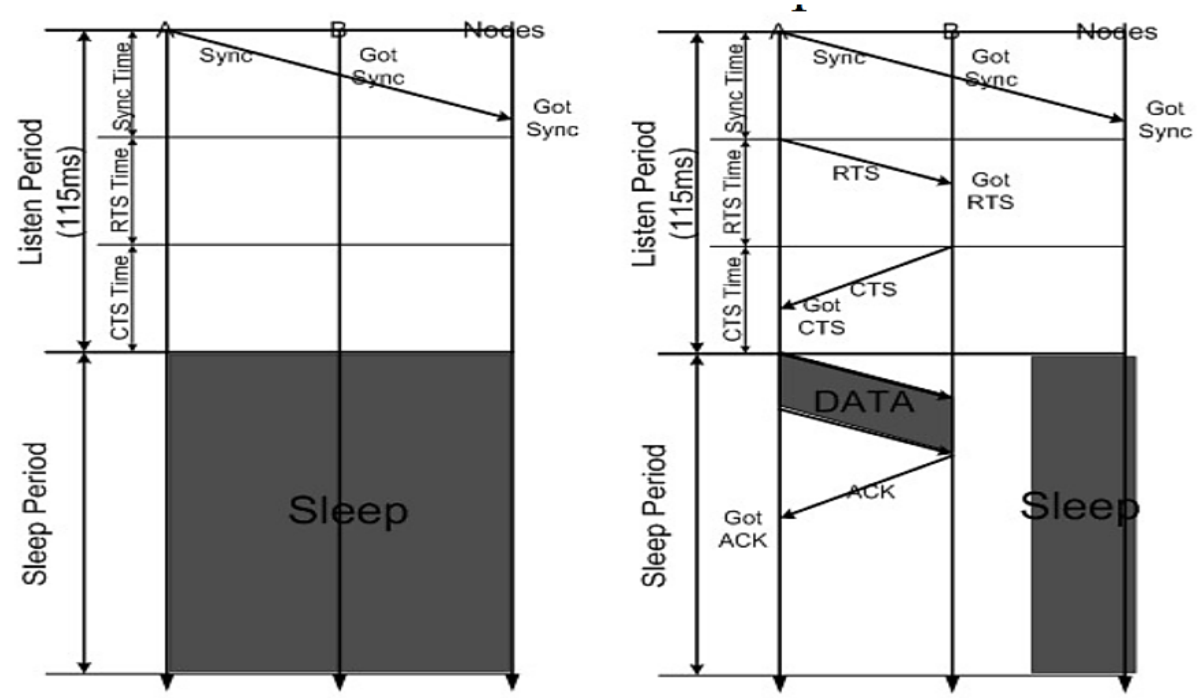
This protocol is a key component for the success of wireless data networks. Basic approach of contention-based MAC protocols are Carrier Sense Multiple Access (CSMA) and Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).

Advantage of these MAC protocol is to increase scalability and adaptability. Nevertheless, these protocols are less energy efficient because they spend a lot of time listening to the network and they waste energy in collisions.

Under this category these protocols T-MAC, S-MAC, D-MAC, A-MAC… are defined.

2.1.1 Sensor-MAC (S-MAC) - Synchronous Contention Based

S-MAC is a MAC protocol designed for WSN and is part of the subcategory: "Synchronous Contention Based". This protocol is a contention-based random-access protocol with a fixed listen/sleep cycle. S-MAC uses a coordinated sleeping mechanism. Nodes periodically sleep and trade energy efficiency for lower throughput and higher latency. A node sleep during other nodes transmissions.



(a) When no nodes have data traffic

(b) When node A has data for node B

<u>Figure 9:</u> Basic mechanism of S-MAC

A time frame in S-MAC is divided into two parts: one for a sleeping session and the other for a listening session (Figure 9). Just only for a listen period, sensor nodes can communicate with other nodes and send some control packets such as SYNC, RTS, and CTS like CSMA/CA.

For example:

- if a node A wants to talk to node B, it just waits until B is listening
- if multiple neighbours want to talk to a node, they need to contend for the medium
- after they start data transmission, they do not go to periodic sleep until they finish transmission

The aim of this protocols is to reduce energy consumption from all the sources that we have identified to cause energy waste (collision, overhearing, idle listening, and control overhead) while supporting good scalability and collision avoidance. To reduce energy consumption in listening to an idle channel, nodes periodically sleep.

Nonetheless, because of this reduce of energy, **the latency is very lower**. So, it is not adapted for time-critical applications.

2.1.2 Time-out MAC (T-MAC) - Synchronous Contention Based

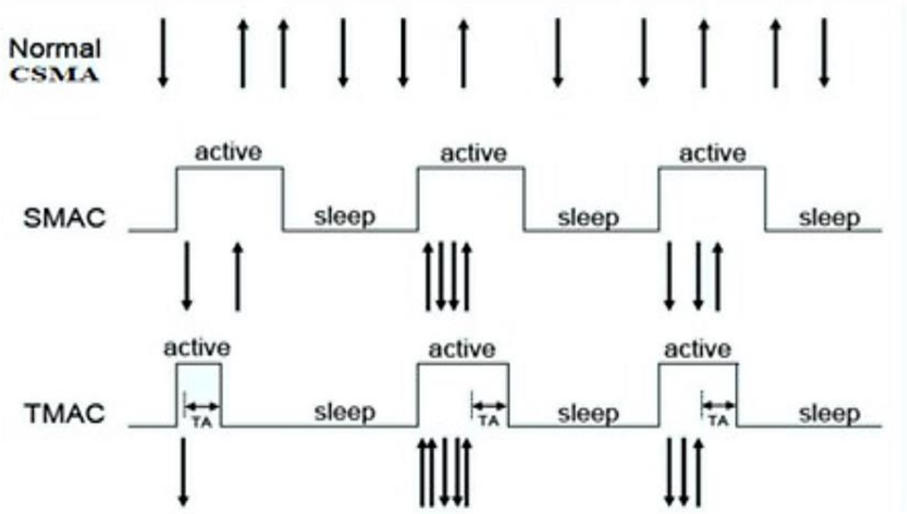
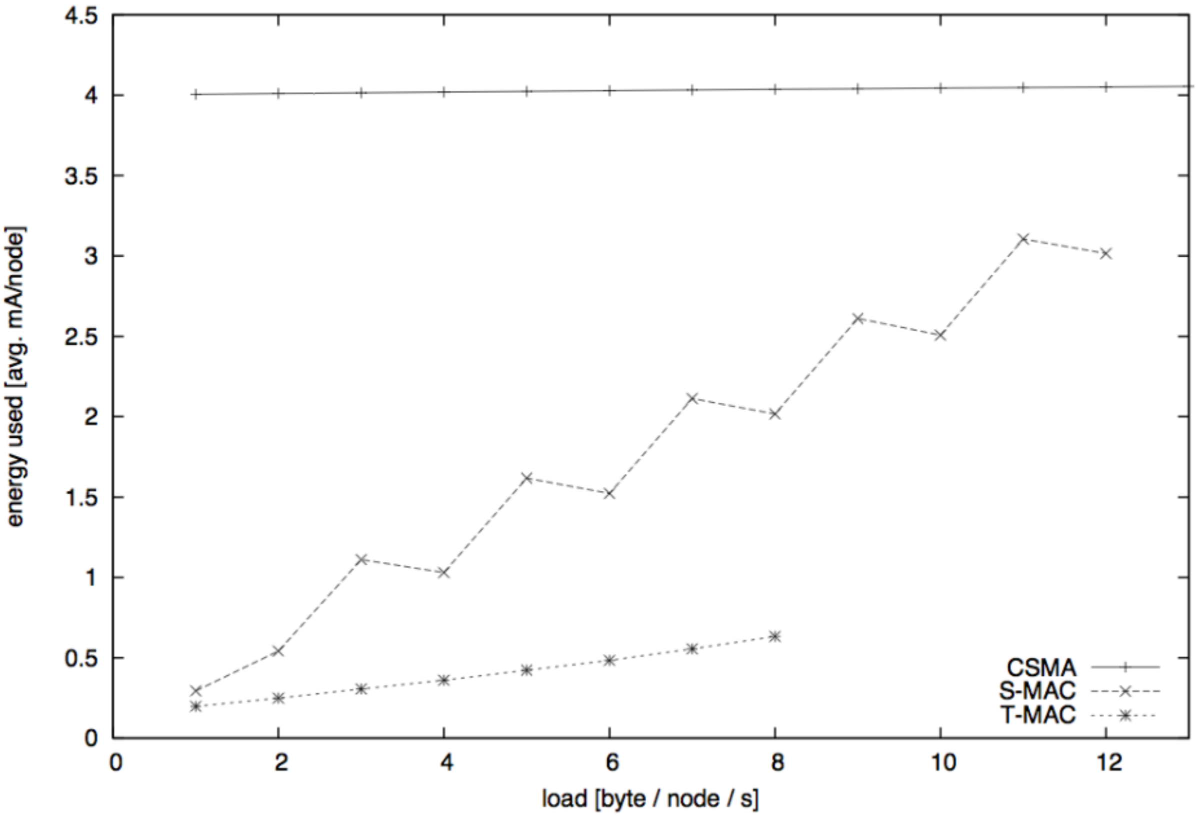


Figure 10: Sleep and wake-up cycles in S-MAC and T-MAC

T-MAC is a protocol derived from the S-MAC protocol. In S-MAC, the nodes must be deployed with an active time that can handle the highest expected load. And whenever the load is lower than that, the active time is not optimally used, and energy will be wasted on idle listening.

The purpose is to reduce idle listening by transmitting all messages in bursts of variable length and sleeping between bursts. To maintain an optimal active time under variable load, we dynamically determine its length. T-MAC end the active time in an intuitive way.

Figure 11: Comparative energy used between CSMA, S-MAC and T-MAC protocols



According to the Figure 11, T-MAC saves energy compared to S-MAC. The “early sleeping problem” limits the maximum throughput. Thanks to this mechanism, T-MAC has a lower power consumption at the expense of a worse latency.

Nevertheless, compared to the S-MAC, there is a greater chance to have more latency and data loss after a sudden burst of long messages.

2.1.3 Dynamic Sensor MAC Protocol (DS-MAC) – Synchronous Contention Based

This protocol is based on the S-MAC protocol and adds a dynamic duty-cycle feature. It uses the adaptive duty cycle.

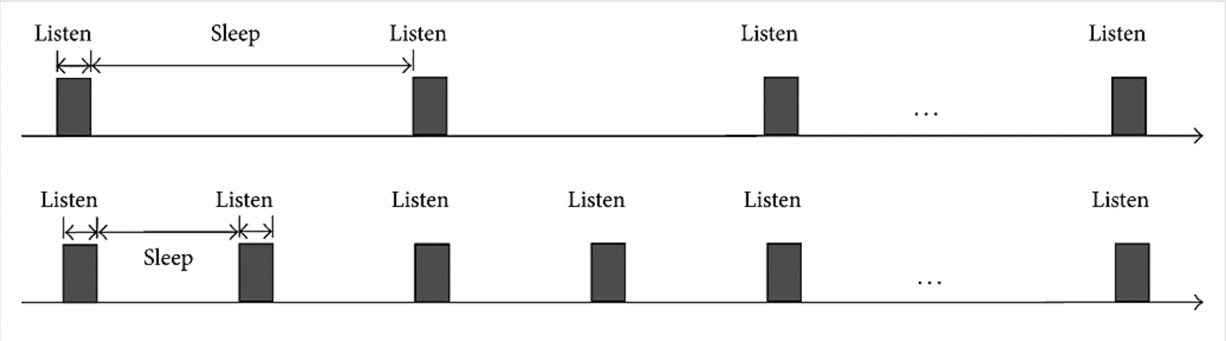


Figure 12: Dynamic duty cycling in D-MAC.

As all nodes share their one-hop latency values, every node calculates the average value. If this value is too high, a node will decide to shorten the sleep time and announce this in the SYNC period. The major aim in this extension is to decrease the latency for delay-sensitive applications.

2.1.4 Adaptative MAC (A-MAC) - Synchronous Contention Based

A-MAC is similar with S-MAC. This protocol introduces an adaptive duty cycle depending on ratio of the remaining energy to the initially supplied energy considering the pre-configured lifetime.

The more energy a node has, the more frequently the node will wake up and hence fasten relaying data. Moreover, the routing algorithm also considers the energy of the nodes that can increase latency.

2.1.5 Berkeley MAC (B-MAC) – Asynchronous Contention Based

B-MAC is a contention-based protocol for channel access that is uses also the CSMA/CA protocol. It provides a flexible interface to obtain ultra-low power operation, effective collision avoidance, and high channel utilization.

The aims of B-MAC are:

- Simple implementation
- Low power operation
- Reconfigurable by upper layers
- Tolerant to changes on the network
- Scalable to large number of nodes

- Effective collision avoidance

To achieve low power operation, B-MAC employs an adaptive preamble sampling scheme to reduce the duty cycle and minimize idle listening. B-MAC is designed for low traffic, low power communication, and is one of the most widely used protocols.

2.2 Scheduled-based protocols

These protocols allow each node to send frames at a specific time (TDMA).

2.2.1 Lightweight MAC (L-MAC) - TDMA

L-MAC is a MAC protocol designed for WSN and a typical TDMA protocol. It is an energy-efficient medium access protocol designed for wireless sensor networks. The mechanism is simple:

- Each node has a given time slot to send a header to indicate to other nodes that it wants to send a packet.
- When all nodes receive this header, they switch off their radio if they are receiving the data.
- Finally, the node can send his data over the medium.

The aim of L-MAC is to minimize the number of transceiver switches, to make the sleep interval for sensor nodes adaptive to the amount of data traffic and to limit the complexity of implementation.

2.2.2 Traffic Adaptive Medium Access Protocol (TRAMA) - TDMA

TRAMA is a MAC protocol based on TDMA mechanism. It allows for flexible and self-motivated scheduling of time slots. TRAMA reduces the energy consumption by avoiding the collisions of transmitted data packets and it allows the nodes to switch low power mode whenever they are not in transmitting and receiving mode.

TRAMA applies a traffic adaptive distribution election scheme that selects the receivers based on the schedules announced by transmitters. Nodes using TRAMA, exchange their two-hop information and the transmission schedules fixing which nodes are the intended receivers of their traffic in chronological order.

2.3 Hybrid protocols

These protocols combine contention based (CSMA) and contention based with scheduling mechanisms (TDMA) principles.

2.3.1 Energy-and-Rate based MAC (ER-MAC) – Hybrid

ER-MAC is a hybrid MAC protocol that follow the concept of energy-critical nodes. ER-MAC is designed as a hybrid of the TDMA and CSMA approaches, giving it the flexibility to adapt to traffic and topology changes.

It adopts a TDMA approach to schedule collision-free slots. Nodes wake up for their scheduled slots, but otherwise sleep to conserve energy. When an emergency occurs, nodes that participate in the emergency monitoring change their MAC behaviour by allowing contention in TDMA slots.

2.3.2 Zebra Media Access Control (Z-MAC) – Hybrid

Like ER-MAC, Z-MAC is based on a combination of CSMA and TDMA. It consists to allocate time slot to nodes as in TDMA using a distributed implementation of RAND. Unlike TDMA where a node can transmit only during its own assigned slots, a node can transmit in both its own time slots and slots assigned to other nodes.

Owners of the current time slot always have priority in accessing the channel over non-owners. Therefore, under low contention where not all owners have data to send, non-owners can "steal" time slots from owners. This has the effect of switching between CSMA and TDMA depending on contention.

Moreover, the main characteristic is that its performance is robust to synchronization errors, slot assignment failures and time-varying channel conditions. In the worst case, its performance always falls back to that of CSMA.

2.4 Comparative of existing MAC layers deployed for WSN

Protocols	Latency	Power management	Data rate	Adaptability to change	Fairness	Clock Synchronization
S-MAC	High	Efficient	Less	High	Good	Yes
T-MAC	High	Efficient	Less	High	Good	Yes
D-MAC	High	Really efficient	Less	High	Good	Yes
A-MAC	High	Really efficient	Less	High	Good	Yes
B-MAC	Low	Really efficient	Medium	High	Very Good	No
L-MAC	High		Good	Moderate	Good	No
TRAMA	High	Not so efficient	Bad	Moderate	Bad	Yes
ER-MAC		Really efficient	Moderate	Moderate	Best	No
Z-MAC		Really Efficient	Best during high contention	Moderate	Best	No

Conclusion

Wireless Sensor Networks are rapidly gaining prominence due to its nearly limitless potential in terms of applications for individuals and industries. However, these specific networks have many requirements like to be energy efficient, guarantee of QoS, Latency…. A lot of MAC protocols are implemented to meet these requirements. All these protocols are protocols based on historical one such as TDMA, CSMA or a combination of both.

Through this report, we saw that the choice of a MAC protocol depends on the use case. Indeed, each MAC protocols will be adapted for application monitoring (home monitoring …) and not at all for time-critical applications.

Furthermore, I didn't focus on the security of each protocols. Indeed, security is a crucial point if we want WSN to be largely developed in a near future. It implies encryption and thus extra processing, circuit complexity, power consumption, ...

For me, it would be the occasion to make a second report on it because it is a rather complex subject which deserves to be treated ([9]).

References

[1] “Power Efficient Dynamic MAC Protocol (D-MAC) for Wireless Sensor Networks” https://tarjomefa.com/wp-content/uploads/2018/05/TarjomeFa-F682-English.pdf

[2] “MAC Layer Protocols for Sensor Networks “, Leonardo Leiria Fernandes https://cpham.perso.univ-pau.fr/ENSEIGNEMENT/PAU-UPPA/INGRES-M1/07-wsn-mac.pdf

[3] “An adaptive energy-efficient MAC protocol for Wireless Sensor Networks” https://perso.ens-lyon.fr/eric.fleury/CPS/ART/Projet/pmac/01420161.pdf

[4] “ Analysis of S-MAC/T-MAC Protocols for Wireless Sensor Networks, Woochul Lee, Yutae Lee, 2006,Proceedings of the 10th WSEAS International Conference on COMMUNICATIONS” https://www.researchgate.net/publication/262169724_Analysis_of_S-MACT-MAC_protocols_for_wireless_sensor_networks

[5] “A lightweight Medium Access Protocol (LMAC) for Wireless Sensor” https://ris.utwente.nl/ws/portalfiles/portal/5427399/VanHoesel_INSS04_048.pdf

[6] “Analysis of S-MAC/T-MAC Protocols for Wireless Sensor Networks” http://www.wseas.us/e-library/conferences/2006cscc/papers/534-319.pdf

[7] “COMPARISON OF CSMA BASED MAC PROTOCOLS OF WIRELESS SENSOR NETWORKS” https://arxiv.org/ftp/arxiv/papers/1205/1205.1701.pdf

[8] “MAC Protocols for Wireless Sensor Networks” https://inet.omnetpp.org/docs/users-guide/ch-sensor-macs.html

[9] “Security of Wireless Sensor Networks: Current Status and Key Issues” https://www.intechopen.com/chapters/12457