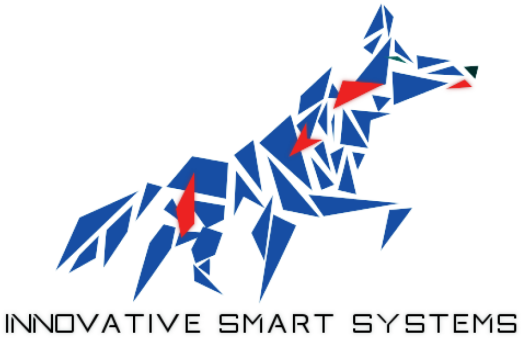
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

PTP Innovative Smart Systems - Semantic Data

Alex Noize

MAC Layers for Wireless Sensors Networks



January 20, 2019

Contents

1 Introduction

This document intends to present most of the MAC layers that could be used for the deployment of a wireless sensor network. Thus, We will see many available MAC layer and their characteristics. However, we will first begin, with a presentation of what is the MAC layer in the OSI model and see what are its functions.

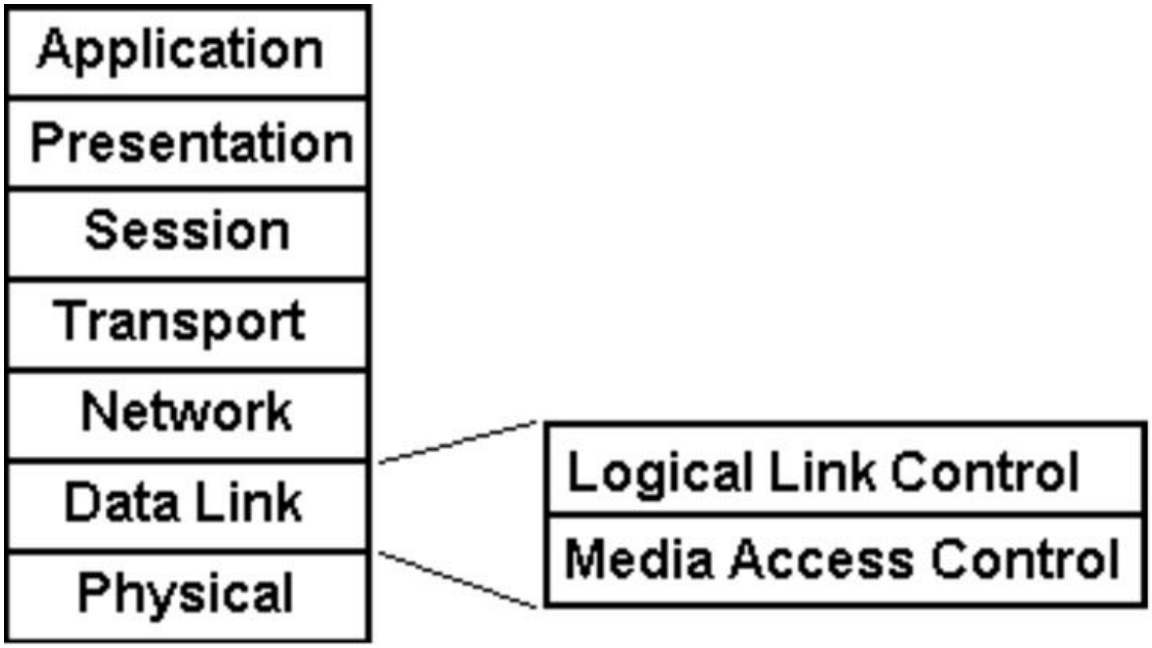


Figure 1: Data Link layer in OSI model

So, the Media Access Control (MAC) is one of the two sub-layers that are implemented as the Data Link layer of the OSI model. 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. For this, the MAC sublayer uses MAC protocols to ensure that signals sent from different stations across the same channel don't collide.

Therefore, we can sort the usuals MAC layers in three classes : controlled access, TDMA or contention.

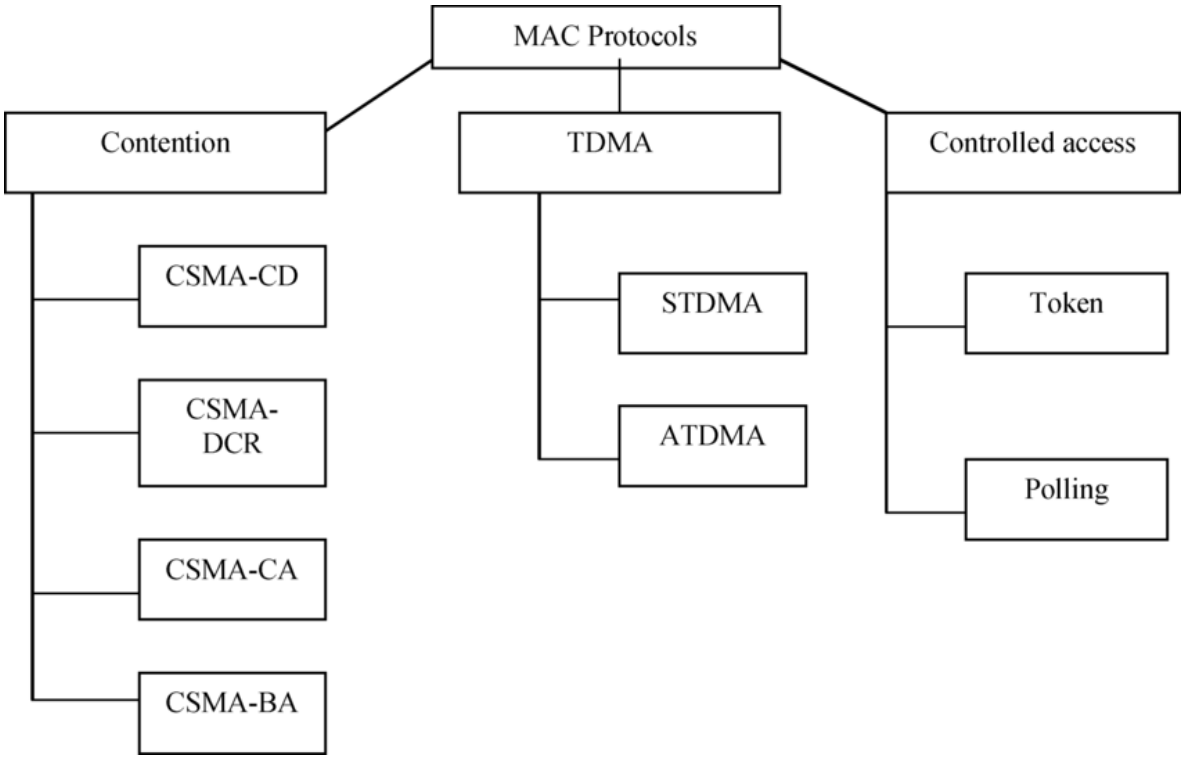


Figure 2: MAC protocol classification

But we can also find MAC protocols especially designed to meet the requirements of WSN such has S-MAC , T-MAC or Z-MAX. However, they are basically hybrids of existing solutions.

2 FDMA - Frequency Division Multiple Access

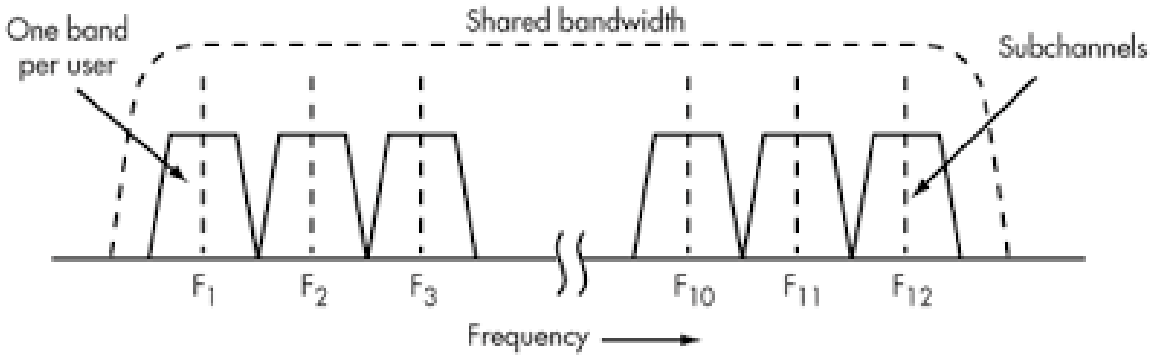


Figure 3: FDMA Principle

FDMA is one of the most common MAC technique. The principle is very simple, the system is given a certain bandwith and each users is allocated a certain channel in this bandwith. In this way, any avoidance should be avoided and it's possible to add guard bands to separate each channels in order to limit the interference between them. With this protocol, every user could be emitting for anytime

but all the bandwith will be used, it's a trade-off between time of emission and bandwith.

This MAC protocol is used for most of the satellite transmissions, cable television, fiber optic communication, ... But it is costly to implement as transceiver needs to be able to receive on different frequencies. Moreover, in the particular case of WSN, it's not the best solution as the scalability is limited due to the fact that each user is allowed a certain channel.

3 TDMA - Time Division Multiple Access

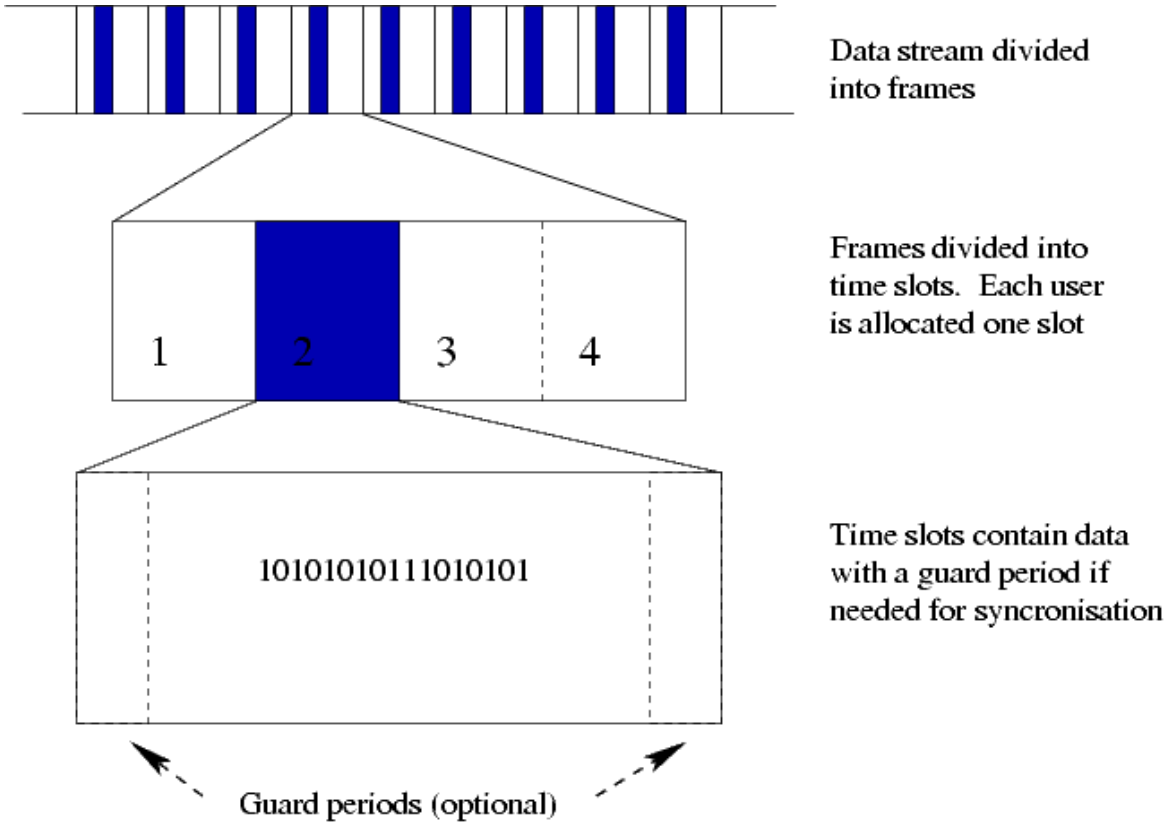


Figure 4: TDMA Principle

TDMA is another common MAC protocol. It's not so different from FDMA but it's a time-multiplexing rather than a frequency-multiplexing. In TDMA, each users is given a time slot during which it can transmits using all the available bandwith. The main problem of such a technique is that all the nodes has to be synchronized in time not to infer with each others. For this purpose, many techniques are used but the principal one is to periodically send packets to resynchronize every node and avoiding them to derive. This MAC protocol is principally used in Global System for Mobile communications (GSM) but it's not really appropriate for WSN because of the scalability and the cost of the synchronization in terms of data rate and power consumption.

4 CDMA - Code Division Multiple Access

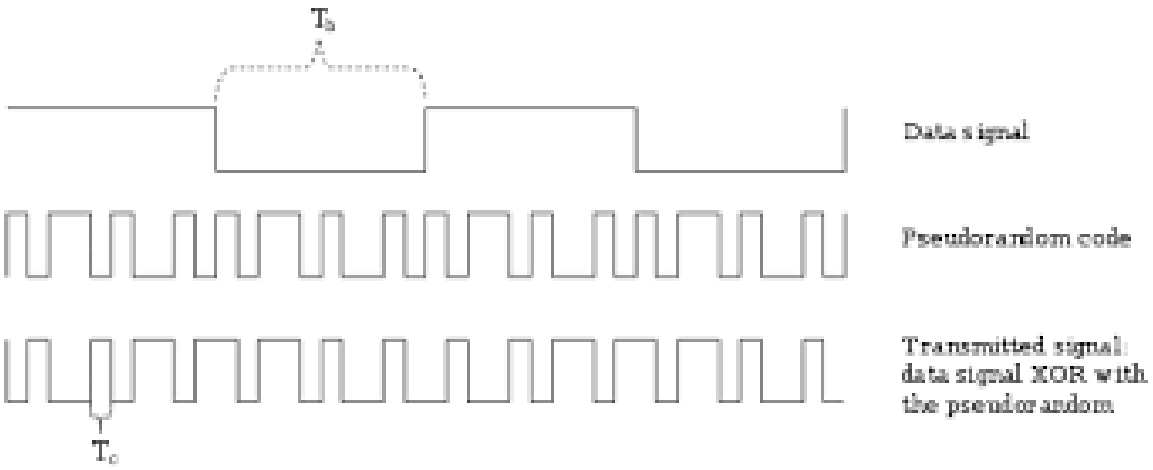


Figure 5: CDMA Principle

CDMA is a pure digital technique, it's also known as spread spectrum because it takes a digitized analog signal and spreads it over a a wider bandwith. With this technique many signals can occupy the same channel simultaneously because the resulting signal is at low- power level. Every transceiver requires complex electronics in order to generate the signal at emission and correlate with the specif code at the reception, it's the principal con of this technology and why it's hard to implement it on a WSN. The third generation (3G) cell-phone technology called wideband CDMA (WCDMA) uses a similar method with compressed voice and 3.84-Mbit/s chipping codes in a 5-MHz channel to allow multiple users to share the same band An intuitive analogy of FDMA, TDMA, and CDMA is talking at different pitches, talking at different times, and talking different languages respectively.

5 CSMA - Carrier Sense Multiple Access

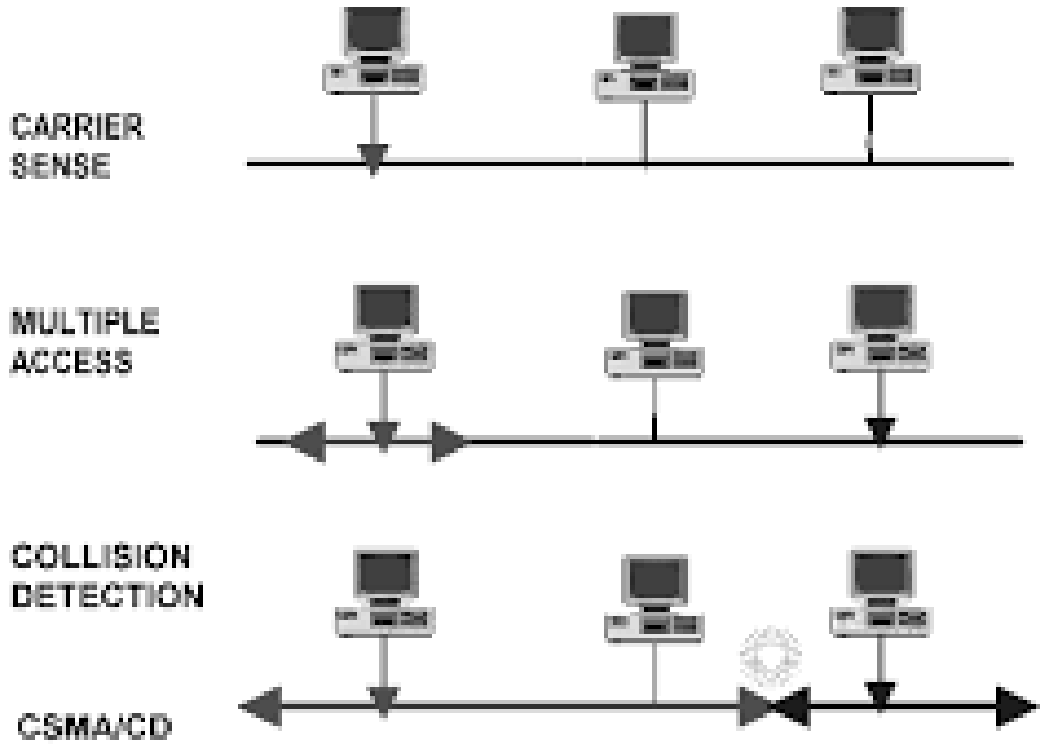


Figure 6: CSMA Principle

CSMA is a MAC protocol in which a node verifies that communication medium is not used before initiating a transmission on it. In this way, CSMA allows to detect collision and fro some protocols even avoid collision. It exists three main methods :

- **CSMA/CD** - Collision Detection
- **CSMA/CA** - Collision Avoidance
- **CSMA/CR** - Collision Resolution

In CSMA/CD, everyone can transmits if no one else is currently transmitting. If two users are transmitting at the same time, they both stop and wait for a random time before starting again.

In CSMA/CA, if the medium of transmission is free, the emitting node will send a Ready To Send (RTS) packet with the amount of data is wanting to send and the data rate. The receipting node will send back a Clear To Send (CTS) packet and the emiiting node wills start the transmission. Every other nodes will wait before emitting for a time based on the CTS packet. This way, any collision should be avoided.

CSMA/CR is working like this :

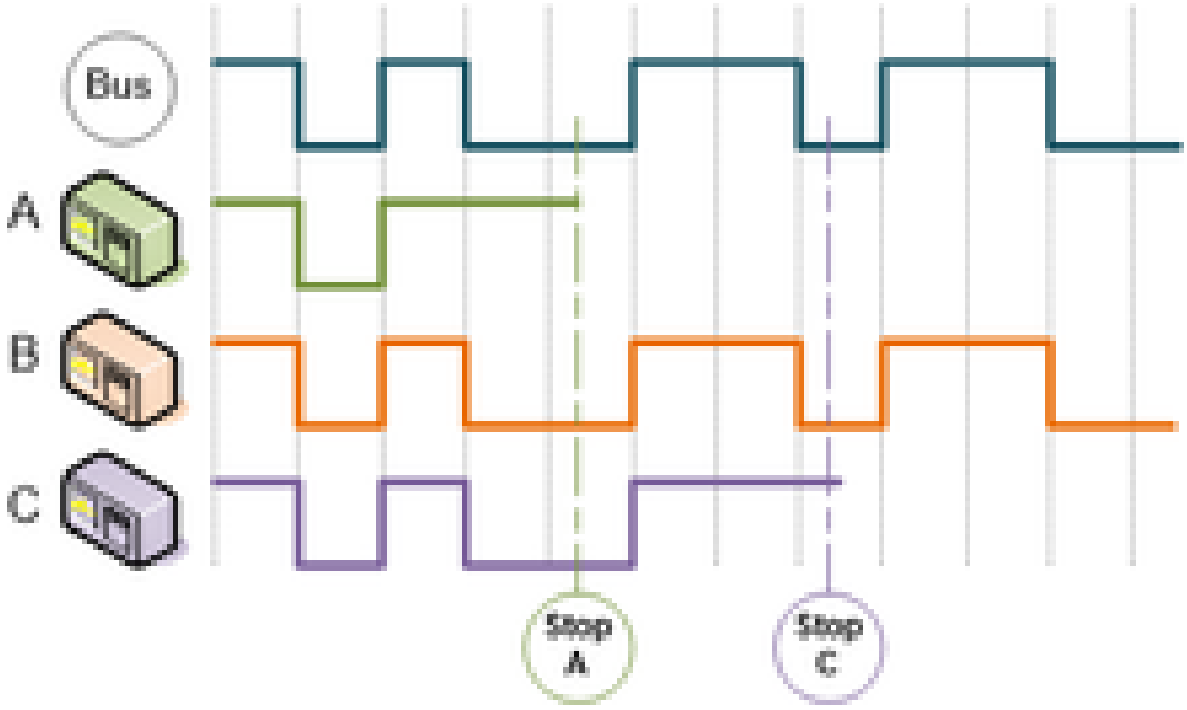


Figure 7: CSMA/CR Behavior

If multiple nodes are emitting at the same time, they apply a logical AND between the received and the emitted signals. If there is an inequality, nodes stop transmitting. This protocol is heavily based on CSMA/CD with more intelligence, if two nodes are sending the same things this protocol allows to finish this transmission.

6 Other MAC protocols

We will now see the protocols designed for WSN. The key requirements for these MAC protocols are the following : collision avoidance, energy efficiency, scalability, adaptability, channel utilization, latency, throughput. In order to do so those MAC protocols should minimize energy wastes which are cause by :

- Collisions/Interference
- Control packet overhead
- Overhearing unnecessary traffic
- Long idle time
- Synchronization overhead

6.1 S-MAC - Sensor Media Access Control

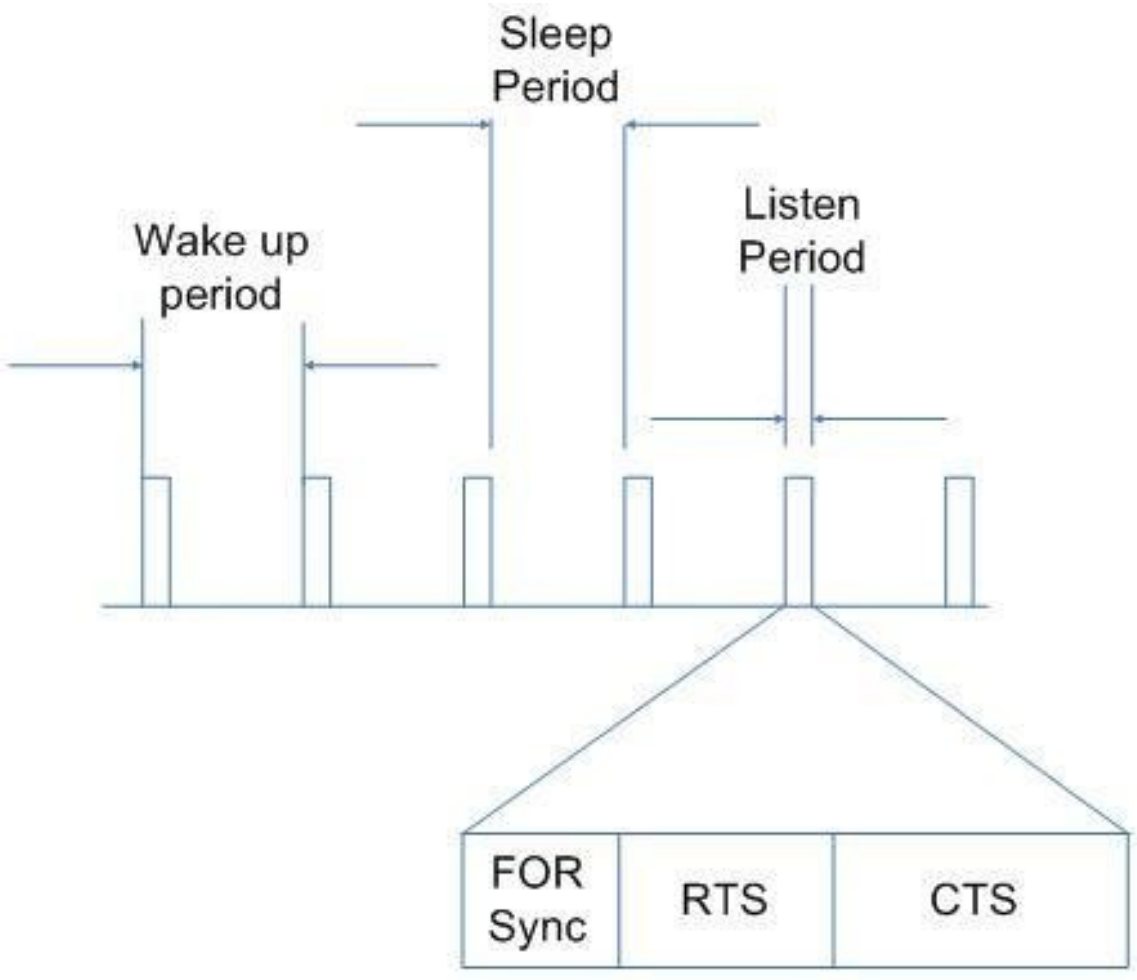


Figure 8: S-MAC Principle

S-MAC is a network protocol specifically designed to meets the requirement of sensor networks. As a matter of fact, S-MAC has a good scalability, a low power consumption and support self-configuration. This protocol allows nodes to sleep for a long period of time and emits whenever they detect an event. It's heavily based on CSMA/CA with the RTS/CTS packets. S-MAC is designed for WSN and so, the latency is not that great, thus, it's not optimal for time-critical applications.

6.2 T-MAC - Timeout Media Access Control

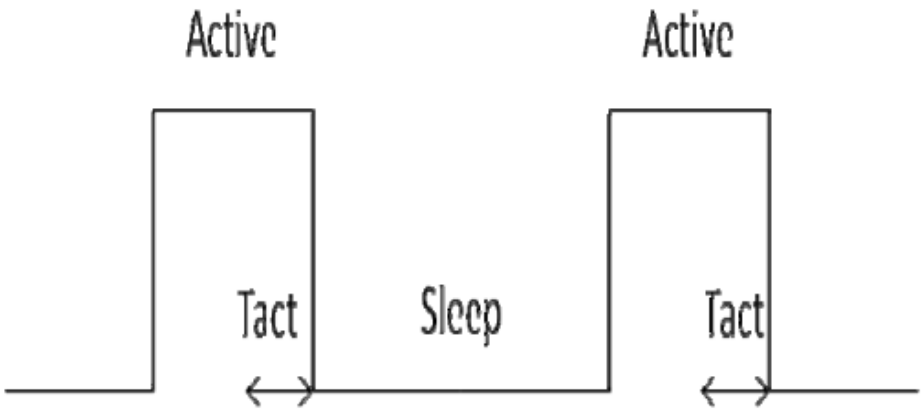


Figure 9: T-MAC Principle

T-MAC is a protocol derived from the S-MAC protocol. The aim is to adapt the sleep and active time, and so to have a lower power consumption at the expense of a worse latency. In TMAC the sensor node deviates to sleep period if no event has occurred for a time T_{act}.

6.3 Z-MAC - Zebra Media Access Control

Z-MAC is another MAC protocol designed for WSN. It is based on a combination of CSMA and TDMA, Z-MAC allocate time slot to nodes as in TDMA but the nodes can also emits when it is not their time slot if the owner of the time slot is not transmitting. A distinctive feature of Z-MAC 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.

6.4 B-MAC - Berkeley Media Access Control

The B-MAC is a contention based protocol for channel access and then TDMA for transmitting the datas. It uses an adaptive preamble in order to reduce idle listening and save energy. Each nodes uses Low-Power Listening (LPL) periodically to check is the channel is free. A back off time is used before checking and after it to see is the channel is free. The node goes back to sleep if it has no data to send or if the channel is busy. And this protocol is not using any kind of synchronization which will save some energy too. But the main disadvantage of B-MAC is that the preamble creates a large overhead.

7 Conclusion

As we saw before, wireless sensor networks have many constraints and, thus, need specific MAC protocols designed to meet their requirements. We saw many MAC protocols that could be used in WSN with all their pros and cons regarding the wanted Quality of Service (QoS), Energy Consumption, Latency, ... All these protocols are hybrid protocols based on historical one such as TDMA, CSMA, etc but adapted to WSN constraints. However, we didn't find a perfect MAC protocol and

each one efficiency depends of the context.
Moreover, in all this report, we didn't focus on the security of each protocols. As a matter of fact, security is a crucial point if we want WSN to be largely developed in a near future. Nonetheless, security implies encryption and thus extra processing, circuit complexity, power consumption, ... However, it's a complex subject and you can find further discussions in the following references [7, 6]

References

[1] Guillaume Ferré and Eric Simon. An introduction to sigfox and lora - phy and mac layers. 2018.

[2] L Frenzel. Fundamentals of communications access technologies: Fdma, tdma, cdma, ofdma, and sdma. *Electronic Design*, 2016.

[3] Joseph Kabara and Maria Calle. Mac protocols used by wireless sensor networks and a general method of performance evaluation. *International Journal of Distributed Sensor Networks*, 8(1):834784, 2012.

[4] Sarika Khatarkar and Rachana Kamble. Wireless sensor network mac protocol: Smac & tmac. *Indian Journal of Computer Science and Engineering (IJCSE)*, 4(4):304–310, 2013.

[5] Nasrin Hakim Mithila, Bushra Rahman, and Alif Bin Taher. *Study and Analysis of Protocols of Wireless Sensor Network*. PhD thesis, Department of Computer Science and Engineering, Military Institute of . . . , 2012.

[6] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, volume 2, pages 6–pp. IEEE, 2006.

[7] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57, 2004.

[8] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 95–107. ACM, 2004.

[9] Injong Rhee, Ajit Warrier, Mahesh Aia, Jeongki Min, and Mihail L Sichitiu. Z-mac: a hybrid mac for wireless sensor networks. *IEEE/ACM Transactions on Networking (TON)*, 16(3):511–524, 2008.

[10] Mastooreh Salajegheh, Hamed Soroush, and Antonis Kalis. Hymac: Hybrid tdma/fdma medium access control protocol for wireless sensor networks. In *PIMRC*, pages 1–5, 2007.

[11] J-P Thomesse. Fieldbus technology in industrial automation. *Proceedings of the IEEE*, 93(6):1073–1101, 2005.