University of Toulouse
Institut National des Sciences Appliquées de Toulouse
135 Avenue de Rangueil, 31400 Toulouse, France

DEPARTMENT OF
COMPUTER AND ELECTRICAL ENGINEERING

A REPORT

ON

"MAC Layers for Wireless Sensor Networks"

Protocols for Wireless Sensor Network

SUBMITTED BY

Nhat Luan TRUONG

FROM

5ISS B1

UNDER THE GUIDANCE OF

Prof. Daniela DRAGOMIRESCU

(Academic Year: 2020-2021)

January 8, 2021

Contents

1 Introduction

Wireless sensor networks (WSNs) have hundreds or potentially thousands of nodes, each of which are small computers capable of measuring physical characteristic(s) of the surrounding environment and transmitting the information using a radio link. WSNs can be used in monitoring applications such as weather, crops, surveillance, human health care, and structural health...

This paper will present different types of MAC layers and analyses some protocols develop for wireless sensor networks.

2 State of the art of Medium Access Control (MAC)

2.1 Medium Access Control Protocols

The MAC layer can be defined as a sublayer of the data link layer of the OSI model, which also includes the Logical Link Control (LLC) layer, in charge of the control of the frame synchronization, flow control and error checking. In short term, the Medium Access Control layer controls how a device on the network gains access to the data and how it can transmit them.

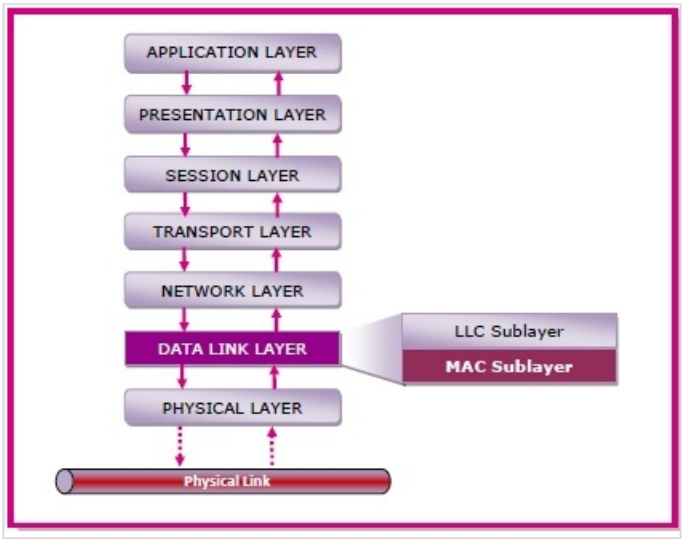

Figure 1: The OSI Model [1]

If we consider a network composed by wireless sensors, the medium to be considered is the air. So, every device of the network will send its messages by broadcasting them over the air. These messages will then be received be all the devices nearby them, depending of the range of the network used. Thus, the MAC layer need to handle different functionalities to allow data to transfer from one device to another by addressing the frames, by sending them on the medium on the right moment, by receiving and transferring them to upper layers.

The functions of MAC layer can be resumed in these points: [1]

- 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.

The MAC protocol used had to be scalable according to the network size and adjustable in case of adding or removing nodes. Moreover, as the MAC layer controls the radio transmission, which is one of the part of a device that consumes the most energy, it has to be evergy efficiency in order to allow a longer battery life.

2.2 The ALOHA protocol

The nature collision in wireless broadcast medium requires an efficient channel accessing method to control access to the shard medium. Therefore, this collision can be offer free communication among nodes. Specifically, accessing the channel is classified into two major categorizations; contention based networks and contention free networks. In contention based networks, devices are contending each other to gain access of the channel. Whereby, contention free networks uses time or frequency to schedule the channel. In this category, devices can only access their allocated channel slots, and these devices communicate with the central node in a collision free method. In the other hand, accessing channel scenarios have been already proposed to find the answer of who is allowed to access and how can access. However, the Additive Link On-Line Hawaii System (ALOHA) protocol is proposed in 1970s and also defined as pure ALOHA. [2].

The ALOHA protocol is a really basic protocol. It says that a device which uses it, sends a packet to a destination whenever it wants. But, if the message has not been delivered to the target, then the sending device sends again the message after a randomly-chose waiting time. The sending device knows that the message was received by the target only when it receives the acknowledgement message corresponding to the message sent. This protocols is not stable with a lot of devices communicating at the same time.

A later version of the protocol is the slotted-ALOHA. In this version, the nodes which want to send data have access to time slots. To send data, they can only start to send at the beginning of a time slot. Consequently, if a node want to send data to the target, then it has to wait for the begin- ning of the next time slot to be able to send it.This version of the ALOHA protocol reduces the frequency of data collision, but it is still not adapted to networks with a lot of communicating devices. However, the main concept behind the ALOHA protocol is the concept of random access to the medium. A lot of protocols are consequently based on it, and we are going to study some of them.

Both Pure Aloha and Slotted Aloha are Random Access Protocols. Following are the important differences between Pure Aloha and Slotted Aloha.

Sr. No.	Key	Pure Aloha	Slotted Aloha
1	Time Slot	In Pure Aloha, any station can transmit data at any time.	In Slotted Aloha, any station can transmit data only at beginning of any time slot.
2	Time	In Pure Aloha, time is continous and is not globally syncronized.	In Slotted Aloha, time is discrete and is globally syncronized.
3	Vulnerable time	Vulnerable time = 2 x Tt.	Vulnerable time = Tt.
4	Probability	Probability of successful transmission of data packet = G x e^{-2G}	Probability of successful transmission of data packet = G x e^{-G}
5	Maximum efficiency	Maximum efficiency = 18.4%.	Maximum efficiency = 36.8%.
6	Number of collisions	Does to reduces the number of collisions.	Slotted Aloha reduces the number of collisions to half thus doubles the efficiency.

Figure 2: Differences between Pure Aloha and Slotted Aloha.[3]

3 Classification of WSN MAC Protocols

As said in [2], several MAC protocols have been successfully proposed to meet the stringent design requirements of WSNs. Actually, these protocols depend on how protocol allows nodes to access the channel. WSN based MAC protocol has been classified as depicted in Figure 3 into four categories as; contention based, scheduling based, channel polling based, and hybrid protocols.

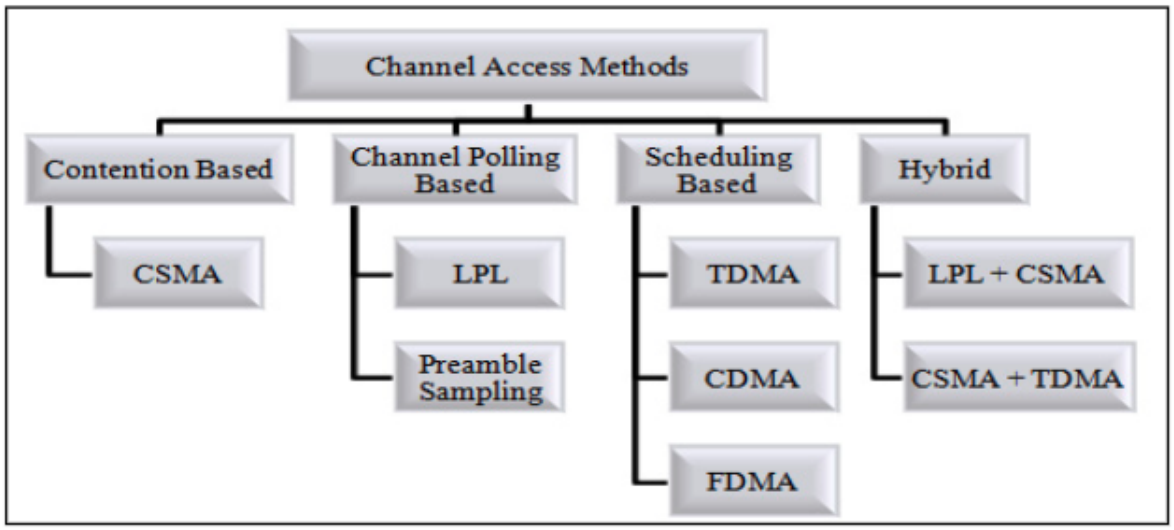

Figure 3: Channel Accessing Taxonomy in WSNs. [2]

3.1 Contention Based MAC Protocols

In this protocol, devices compete to the channel. The nodes listened to the medium before sending messages. When this one is free, they began the transmission. We can find in this family

the Carrier Sense Multiple Access with Collision Detect / Collision Avoidance (CSMA/CA) protocol. This protocol can be described like this:

When a device A want to send a message to another device B, it first listens to the network. If this one is busy, it delayed it transmission. Otherwise, if the medium is free, the device A send a Ready To Send (RTS) message to device B to tell him he wants to send him a message, and add some information like bit rate and message length. If device B is ready, he sends back a Clear To Send (CTS) message to A. Then, the transmission of data can begin. When all the data are transmitted, device B sends a ACK message to notify device A that the message has been successfully received.

In wire networks like Ethernet, another CSMA protocol exists: the CSMA/CD (Collision Detection). This one is impossible to apply in wireless network because is this protocol each device listens to the medium and is able to know if another device is "speaking" or not. In a wireless network, this is impossible because if we take for example two devices A B, talking to another device B, so A and B can be too far from each other to know that there are both talking to C at the same time.

3.2 Channel Polling Based MAC Protocols

Channel polling scheme is known as a preamble sampling and Low Power Listening (LPL). Moreover, sending prefixes data packets with extra bytes by node is called preamble. Specifically, node sends the preamble over the channel to ensure that the destination node detects the radio activity and wakes up before receiving the actual payload from the sender. On a wake-up, if a radio activity is detected by receiver, then the receiver will turn on its radio to receive data packets. Otherwise, the node (receiver) goes back to the sleep mode until the next polling interval. This checking should be performed as long as the check interval duration until the preamble is being sent. On other hand, since the common active/sleep schedules are not performed in channel polling based protocols, then the synchronization, scheduling, or clustering among nodes are not needed. [2]

3.3 Scheduling Based MAC Protocols

During the initialization phase, scheduling based schemes assign collision-free links between neighbouring nodes. Devices using this protocol are schedule on partitioned channels in time, frequency or code, in order to avoid collision. We have three different techniques:

- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)
- Frequency Division Multiple Access (FDMA)

3.3.1 Time Division Multiple Access (TDMA)

The TDMA allows several devices to communicate with a same target, using the same frequency, and at the same time. But how does it work? Actually, when a device tries to communicate with a target using a frequency, this target will allocate periodical time slots to this device. Then, the sender will only be able to send data during the time periods allocated by the target. This way, other devices can communicate with the same target, using the same frequency and at the same time, simply using time slots different from those already used.

Here is an example of a TDMA frame sent by a device, using time slots allocated by the target:

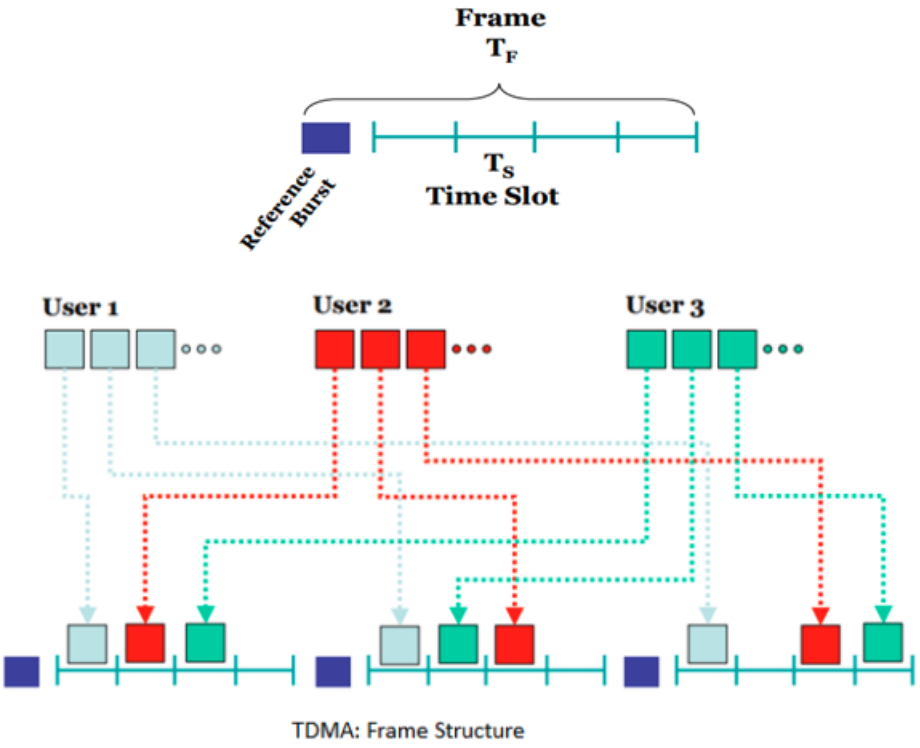

Figure 4: TDMA frame structure [4]

TDMA used a temporal multiplexing to control the access to the medium. Each node uses the communication channel at the same frequency but only during a definite time called slot. Thus, as each node is the only one to talk on the medium during its slot, it can use all the bandwidth allows by the network characteristics, to transmit its message. Regarding the power consumption, this method is very efficient because each device knows already when it will be able to send message so it avoids overhearing and idle-listening to know when the medium is free. The rest of the time, the device can be in sleep mode to save energy. However, one of the node has to periodically send synchronization frame to be sure that all nodes are well synchronize.

Finally, TDMA is not appropriate to networks with a lot of nodes because the more you add device, the smaller will be the slots.

3.3.2 Carrier Sense Multiple Access (CSMA)

Carrier Sense Multiple Access (CSMA) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. When a station has frames to transmit, it attempts to detect presence of the carrier signal from the other nodes connected to the shared channel. If a carrier signal is detected, it implies that a transmission is in progress. The station waits till the ongoing transmission executes to completion, and then initiates its own transmission. Generally, transmissions by the node are received by all other nodes connected to the channel.

Since, the nodes detect for a transmission before sending their own frames,collision of frames

is reduced. However, if two nodes detect an idle channel at the same time, they may simultaneously initiate transmission. This would cause the frames to garble resulting in a collision. [5]

There are multiple variations of CSMA:

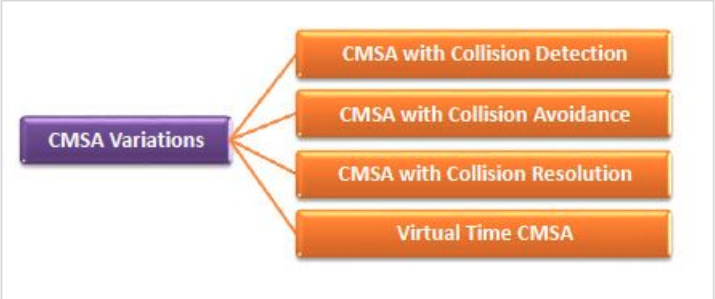

Figure 5: Variations of CSMA [5]

3.3.3 Frequency Division Multiple Access (FDMA)

This method separates channels by frequency, so if users want to have two channels they'll have two separate frequencies. If a conversation runs across a channel, it occupies the whole of the channel exclusively. There is only one conversation and one user at a time per radio channel. More radio channels require more frequencies. [6]

FDMA used a frequency multiplexing. This means that we allocate to each device of the network, a part of the total bandwidth of the network. Thus, all nodes can send data at the same time. Regarding the power consumption, this method avoids the synchronization of all devices, like in TDMA. The collisions are avoided because each device uses its own frequency band. However, because the bandwidth of each device is reduced, the transmission time will be bigger than in TDMA and CDMA, which increase the power consumption.

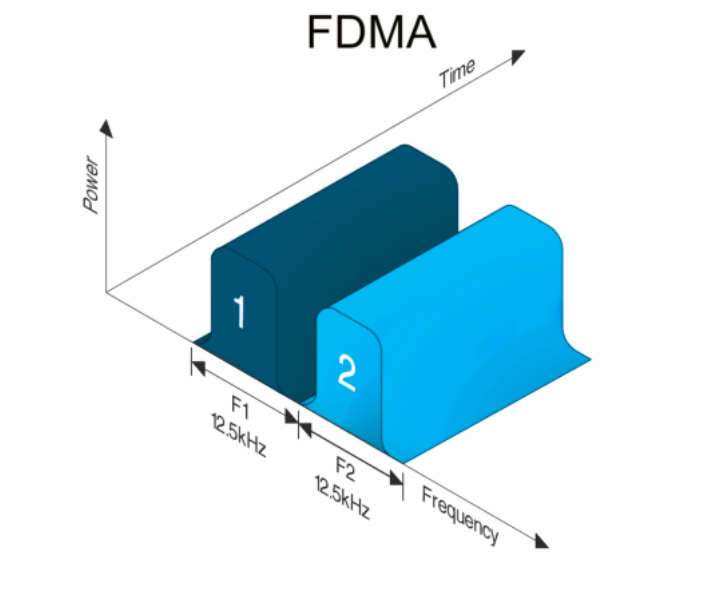

Figure 6: The FDMA technique

3.4 Hybrid MAC Protocols

These protocols are called "hybrid" because they combined two different protocols that we saw previously in order to compensate the weak points of each protocols take individually. For instance, we can take the example of CSMA/CA + TDMA which aims to access both contention period (CSMA/CA) and contention free period (TDMA). In order to check whether a channel is free for transmission CSMA/CA required a carrier sensing. For transmitting the packets during contention period the node competes with other nodes and sends the packets to other device using the CSMA/CA mechanism. But during the contention-free period, the node can transmit packets in a collision free manner using TDMA slots without any carrier sensing.

4 Protocols developed for wireless sensor networks

4.1 Zebra Media Access Control (Z-MAC)

The Zebra Media Access Control (Z-MAC) implements both CSMA and TDMA protocols. More exactly, the Z-MAC acts like CSMA if the communication medium is not used by a lot of devices, and like TDMA if it is. We are now going to study this protocol more precisely. On one side, the CSMA/CA protocol is really powerful for communications when there is low contention in the medium. However, when the contention is high, devices which are using CSMA face great latency due to high number of demands to access the channel.

On the other side, the TDMA protocol is powerful when a lot of devices are communicating at the same time, that is to say when there is high contention in the medium. But the TDMA uses a lot of resources, and is not really adapted for low data communications, or when a few devices are using the medium. The Z-MAC protocol takes advantages of both CSMA and TDMA by using CSMA only when there is low contention, and TDMA when the contention is higher. It allows also to not have the drawbacks of the two protocols, and is consequently a powerful MAC protocol.

4.2 Berkeley Media Access Control (B-MAC)

The Berkeley Media Access Control (B-MAC) protocol is used by devices which consume very low energy. A device which uses B-MAC is communicating using a channel. Periodically, even if it does not need to send data, the node checks the availability of the channel using Low-Power Listening (LPL). When a node want to send data, it first wait during a backoff time, and then it checks the avail- ability of the channel. If the channel is idle, then it starts sending data. But if the channel is busy, then it waits again during another random backoff (congestion backoff) before checking again the availability of the channel and so on. To check the availability of the channel, this MAC layer uses the CSMA/CA protocol. Bu then, during data exchange, the TDMA protocol is used. In the Figure.11 below, you can see 2 devices trying to send data (A and C) at the same time, and a third device (B) which does not have to send data:

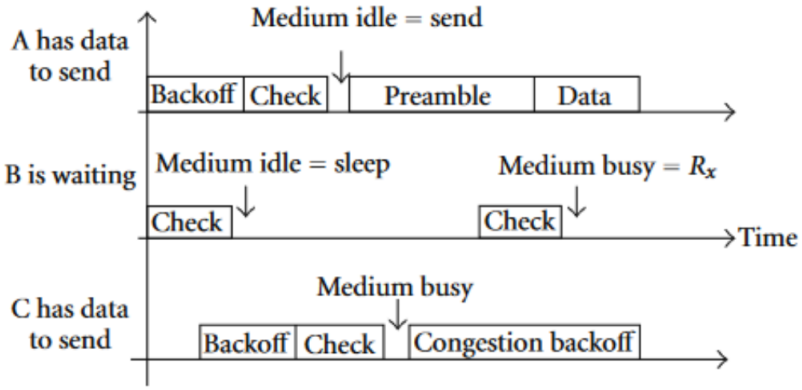

Figure 7: BMAC protocol Example [7]

- Advantage:
  - No synchronization.
  - Idle Listening is reduced to a minimum.
  - Simple to implement.
- Disadvantage:
  - Preambles create large overhead.

4.3 Sensor Medium Access Control (S-MAC)

S-MAC, for Sensor MAC, is based on CSMA/CA channel access method. So, it guarantees avoidance on collision and reduces power consumption. The S-MAC is based on the assumption that a sensor does no need to communicate very often. Consequently, a device which uses this MAC layer to communicate is either sleeping or listening. More precisely, if a node does not have nothing to send to an other node, then it sleeps and it sets a timer to wake up a certain time later. When it wakes up, it listen to the medium to this if someone wants to talk with it. If no, it sleeps again.

To communicate, S-MAC needs synchronisation between the two communicating devices. The CSMA/CA protocol is used to set this synchronisation at the beginning of the exchange. If a node wants to send data to an other one, then it waits for the target to be available, and then it starts sending the packets. The communication is not interrupted until the end.

The following Figure.8 shows a S-MAC exchange example. Nodes A, B, and C are within range of each other. D is within range of C and A transmits to B:

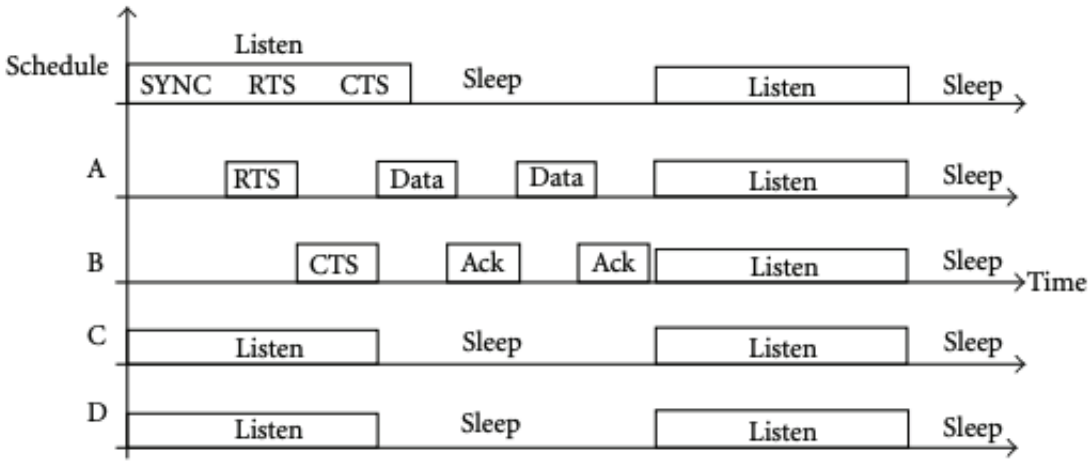

Figure 8: SMAC protocol Example [7]

- Advantage:
  - The battery utilisation is increased implementing sleep schedules.
  - This protocol is simple to implement, long messages can be efficiently transferred using message passing technique.
- Disadvantage:
  - Increase latency as the sender has to wait that the receiver wakes up before sending packets.
  - RTS/CTS are not used due to which broadcasting which may result in collision. Adaptive listening causes overhearing or idle listening resulting in inefficient battery usage.
  - Sleep and listen periods are predefined and constant, which decrease the efficiency of the algorithm under variable traffic load.

4.4 Timeout Medium Access Control (T-MAC)

The Timeout Medium Access Control (T-MAC) is based on S-MAC. It switches between active and sleeping states, exactly as for the S-MAC protocol. The difference between the two protocols is the length of the active time. This MAC layer is also using the CSMA/CA protocol for synchronisation, as for S-MAC. Actually, the T-MAC protocol defines a minimum active time for each active period, called "Tact". Each time a node wakes up, it stays active during this tact time, and listen to the medium. If no event happens, then it returns in sleep mode. But if it receives a RTS packet, then it adapts its active time to be able to communicate with the target until the end of the transmission.

Here is an example of the behaviour of a device using T-MAC which receives a communication request two times in a row:

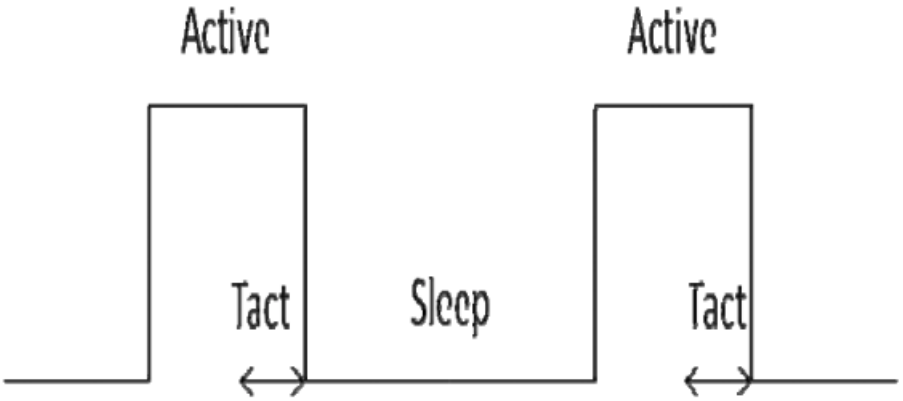

Figure 9: TMAC protocol [8]

- Advantage:
  - TMAC can easily handle variable load due to dynamic sleeping schedule.
  - Decrease even more the power consumption.
- Disadvantage:
  - TMAC's major disadvantage is early sleeping problem in which nodes may sleep as per their activation time and data may get lost especially for long messages. [8]
  - Increase even more the latency.

5 Comparison of existing MAC protocols

As we saw on the previous part, power consumption, at the MAC level, depends on the protocol used. Depending on the time passed in sleep-mode, listening-mode, transmission, if it's needed to send preamble or not, the consumption may vary a lot. As power consumption represents a big deal in sensor networks, some protocols try to reduce drastically the power consumption but it affects the performances such as latency. Now we are going to study what are the sources of energy waste in these MAC protocols.

- Overhearing: it happens when a device has to process messages that are not addressed to it. This occurs under heavy traffic situations and when messages are broadcasting.
- Idle listening: most of the time, the devices keep their radio in a ready to receive mode, because they don't know when they will receive a message. Because this mode keep the radio on, it consumes a lot.
- Collisions: when collision occurred between packets, this means that they have to be sent again. It results in a waste of energy to retransmit and receive other packets.
- Complexity: more the algorithm is complex, more the device will have to work to apply it and less it will remain in sleep-mode. But of course, a simple algorithm won't be able to provide complex functions. So, a compromise has to be found between performance and energy consumption.

- Over-emitting: it occurs when a device try to send a message to a receiver which is not ready to receive packets (if it is still in sleep mode for example).

The following chart is a comparison chart from [9]:

Protocols	Main objectives	Traffic adaptability	Topology adaptability	Packet priority	Fairness
Contention-based					
S-MAC [1]	↓ energy	Medium	Good	No	No
T-MAC [2]	↓ energy	Medium	Good	No	No
B-MAC [3]	↓ energy	Medium	Good	No	Medium
WiseMAC [14]	↓ energy	Medium	Good	No	No
TA-MAC [15]	↑ delivery, ↓ latency	Medium	Good	No	No
X-MAC [4]	↓ energy, ↓ latency	Medium	Good	No	Medium
MaxMAC [5]	↓ energy, ↑ delivery, ↓ latency	Good	Good	No	No
Schedule-based					
TRAMA [16]	↓ energy	Medium	Good	No	Yes
FLAMA [17]	↓ energy	Medium	Good	No	Yes
VTS [18]	bounded latency	Medium	Good	No	Yes
Hybrid					
Z-MAC [6]	↑ throughput	Good	Good	No	Yes
PMAC [19]	↓ energy, ↑ throughput	Good	Medium	No	Yes
Funneling-MAC [7]	↑ throughput	Good	Good	No	Medium
Crankshaft [20]	↓ energy	Medium	Good	No	Medium
RRMAC [21]	↑ delivery, ↓ latency	Medium	Good	No	Yes
EB-MAC [8]	↑ delivery, ↓ latency	Medium	Good	No	No
BurstMAC [22]	↓ overhead, ↑ throughput	Good	Good	No	Yes
i-MAC [23]	↓ latency	Medium	Good	No	Medium

Figure 10: Comparison of existing MAC protocols [9]

The following chart is a comparison under my point of view from all the previous sections:

Protocols	Latency	Data rate	Energy consumption	Energy conservation factors	Scheme used	Advantage	Disadvantage
SMAC	Low	Low	Low	Overhearing, idle listening	Fixed duty cycle, virtual cluster, CSMA	Low energy consumption when traffic is low	Sleep latency, broadcasting problem, can decrease the efficiency of algorithm under variable traffic load
TMAC	High	Low	Low	Idle listening, collision	Adaptive duty cycle, overhearing, FRTS	Can handle variable load, can decrease more power consumption	Early sleeping problem, increase latency
BMAC	High	Low	Low	Overhearing, sollision	LPL, channel assessment software interface	Low overhead when network is idle, simple to implement, consume less energy	Overhearing, bad performance at heave traffic, long transmission latency
ZMAC	High if high contention	Low	Low if low contention	N/A	N/A	Good traffic adaptability, good topology adaptability	Need to increase throughput

Figure 11: Another comparison chart of MAC protocols from section 4

6 Conclusion

We saw in this paper that there is a lot of MAC protocols develop to allow sensors to communicate in a wireless networks. Although there are various MAC layer protocols proposed for sensor networks, however, there is not one protocol which is accepted as a standard. One of the reasons behind this is the MAC protocol choice will be application-specific, which means that there will not be single standard MAC for sensor networks. Another reason is the lack of standardization at lower layers (physical layer) and the (physical) sensor hardware. Major area which needs attention is the extension of network life which is dependent on utilisation of battery with as much efficiency as possible. Major usage of battery is at the MAC Layer level where radio module is utilised.

As it has been shown by various researches that radio transmission needs more power as compared to processing of same amount of data. MAC Layer protocols needs to be developed efficiently.

References

[1] S. Samual, "Medium access control sublayer (mac sublayer)," Mar 2019. [Online]. Available: https://www.tutorialspoint.com/medium-access-control-sublayer-mac-sublayer

[2] A. S. Althobaiti and M. Abdullah, "Medium access control protocols for wireless sensor networks classifications and cross-layering," *Procedia Computer Science*, vol. 65, pp. 4 – 16, 2015, international Conference on Communications, management, and Information technology (ICCMIT'2015). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050915029002

[3] P. Mahesh, "Differences between pure aloha and slotted aloha," Nov 2019. [Online]. Available: https://www.tutorialspoint.com/differences-between-pure-aloha-and-slotted-aloha

[4] Yasbeer, "Explain tdma frame structure." 2018. [Online]. Available: https://www.ques10.com/p/41028/explain-tdma-frame-structure/

[5] Moumita, "What is carrier sense multiple access (csma)?" Sep 2020. [Online]. Available: https://www.tutorialspoint.com/what-is-carrier-sense-multiple-access-csma

[6] N. Dr.Jan, "The difference between fdma and tdma." [Online]. Available: https://www.taitradioacademy.com/topic/the-difference-between-fdma-and-tdma-1/

[7] J. Kabara and M. Calle, "Mac protocols used by wireless sensor networks and a general method of performance evaluation," *International Journal of Distributed Sensor Networks*, vol. 8, no. 1, p. 834784, 2012. [Online]. Available: https://doi.org/10.1155/2012/834784

[8] S. KHATARKAR and R. KAMBLE, "Wireless sensor network mac protocol smac and tmac," *Ind. J. Comput. Sci. Eng.*, vol. 4, pp. 304–310, 08 2013.

[9] L. Sitanayah, C. Sreenan, and K. Brown, "A hybrid mac protocol for emergency response wireless sensor networks," *Ad Hoc Networks*, vol. 20, 09 2014.