INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

PTP Innovative Smart Systems - Protocols for the Connected Objects

Mathieu Raynaud

Wireless Sensors Networks

MAC layers for wireless communications

December 10, 2018

Contents

Introduction

This document is produced as part of the Innovative Smart Systems (ISS) formation at INSA Toulouse. It is the result of a research work done for the course of "Protocols for the connected objects".

The word MAC stands for "Medium Access Control". In the OSI model, it corresponds to the second layer of communication in a connected device. Each connected device implements a MAC layer to be able to send or receive data to/from a target.

In this document, you may find information about the existing MAC layers used for wireless communications in the Internet of Things (IoT).

In a first part, we are going to see what are the main protocols in which are based the MAC layers used in connected networks.

In a second part, we will see what are the MAC layer used for wireless sensors networks.

1 Protocols

1.1 The ALOHA protocol

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 beginning 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.

Here is a comparison between the basic ALOHA and the slotted-ALOHA protocols:

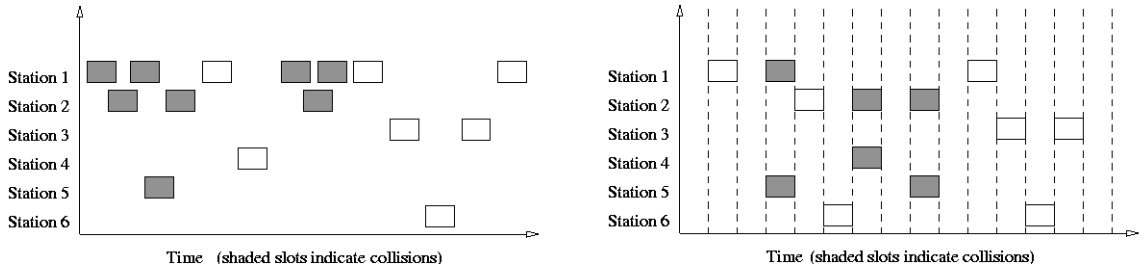

Figure 1: Comparison between basic ALOHA (left) and slotted-ALOHA (right)

1.2 Spatial Division Multiple Access (SDMA)

The Spatial Division Multiple Access (SDMA) protocol takes a great advantage of directional antennas.

In fact, it is based on the location of the communicating devices, and considers that two devices can use the same protocol, the same frequency, or whatever the same way to communicate, only if they are sufficiently separated to not be in the same communication beam.

In the picture below, you can see the efficiency of the SDMA protocol: in the first situation (top-left of the image), the computers C and D cannot communicate because they are perturbed by the communication between A and B. But in the second situation (bottom-right of the image), A and

B, C and E, and D and F can communicate by pairs at the same time, because directional antennas allow them to not perturb other communications, even if they are all in the same area.

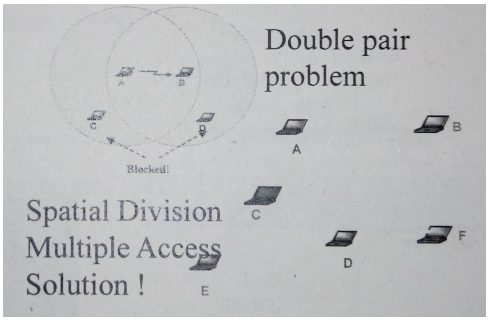

Figure 2: A situation in which SDMA is really powerful

1.3 Time Division Multiple Access (TDMA)

We are going to see what is the Time Division Multiple Access (TDMA) MAC layer.

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:

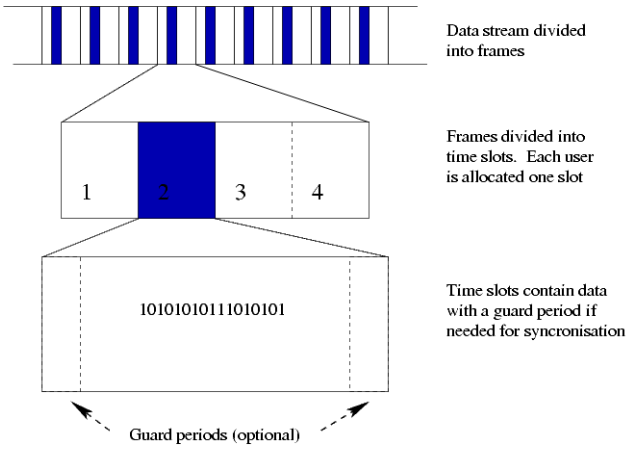

Figure 3: TDMA frames structure

1.4 Frequency Division Multiple Access (FDMA)

The Frequency Division Multiple Access (FDMA) is based on the same principle than the TDMA protocol. Each device which uses the FDMA protocol has an allocated frequency to communicate using a medium. Consequently, several nodes can communicate in the same medium at the same time, only if they use different frequencies.

Each node can have one or several frequency bands allocated to communicate using FDMA. This protocol is widely used in mobile telecommunications.

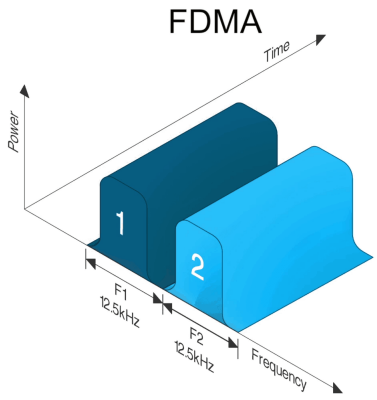

Figure 4: Two communications using FDMA with a bandwidth of 12.5kHz

1.5 Carrier Sense Multiple Access (CSMA)

Now we are going to study the Carrier Sensing Multiple Access protocols.

The main concept behind the name of CSMA is the concept of "carrier sensing". These two words mean that a node using this technology starts by "sensing" the medium. In other words, it checks if the medium is already used by another node, or if it is in an idle state.

Based on this principle, it exists three types of CSMA:

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

We are now going to see what is the difference between these three versions of the CSMA protocol.

1.5.1 CSMA with Collision Avoidance (CSMA/CA)

CSMA with Collision Avoidance works with a communication master node which allows or refuse the connection for a node to the medium. As a consequence, the availability of the medium is led by this master, and no collision can occurs because the access to the medium is allowed only if the

medium is available.

To check if the medium is available, the node first sends a Ready To Send (RTS) frame to the master. If the medium is idle, the master answers with a Clear To Send (CTS) frame. Otherwise, it does not respond and the node waits during a random backoff time, and sends again a RTS frame until it receives a CTS from the master.

The term of "backoff" is spreadly used in the area of communications to talk about a time used to wait, in which the concerned device does nothing.

Once the CTS frame is received by the node, it can start sending its frames to the target.

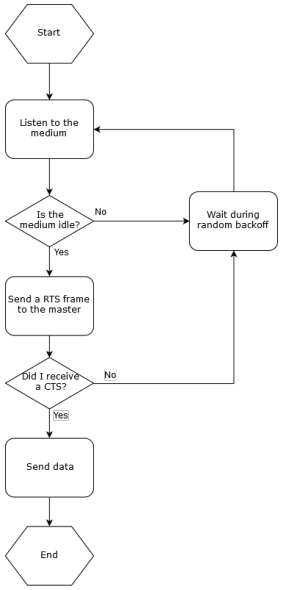

Figure 5: CSMA/CA working flow

1.5.2 CSMA with Collision Detection (CSMA/CD)

CSMA with Collision Detection works a little bit more differently from the CSMA/CA.

After having checked the availability of the medium, the node only sends data if the medium is idle. If not, it waits during a random backoff time before checking again the medium and send the data if possible, as for CSMA/CA.

The main difference is that the node which sends data, still checks if an other node does not use the medium at the same time (which creates collisions and data loss). If yes, both nodes stop using the medium, and wait during a random backoff time, before checking again the availability of the medium and so on.

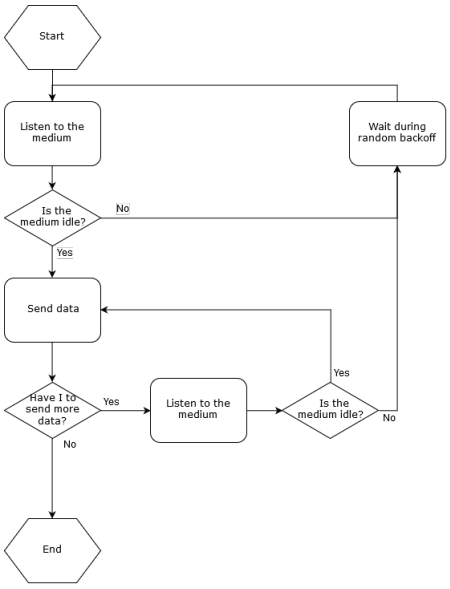

Figure 6: CSMA/CD working flow

1.5.3 CSMA with Collision Resolution (CSMA/CR)

This version of CSMA is based on the CSMA/CD protocol. The difference is that several devices can send on the medium at the same time. The emission of data by a device is interrupted only if the emission of data by an other device creates collisions and data loss.

To determine which device has to stop sending, the master node makes a logical AND between the several signals received. If this AND returns a "0", it means that at least one device sent a bit different from the other devices. In this case, the devices which sent a 1 will be interrupted.

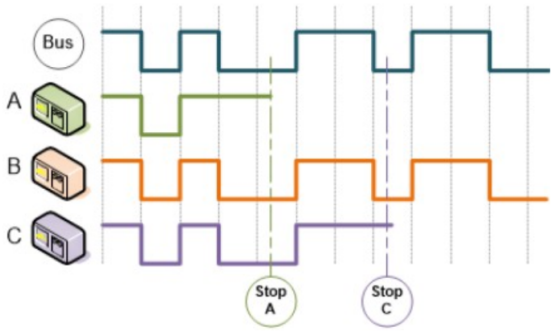

Figure 7: CSMA/CR communication example with three devices

2 MAC Layers

2.1 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.

2.2 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 availability 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 example above, 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:

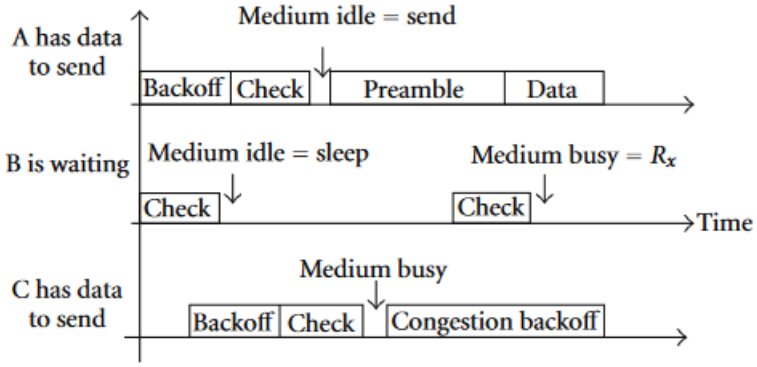

Figure 8: An example of B-MAC frames

2.3 Sensor Medium Access Control (S-MAC)

We are now going to explain how does the Sensor Medium Access Control (S-MAC) MAC layer works. This MAC layer is based on the CSMA/CA protocol.

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.

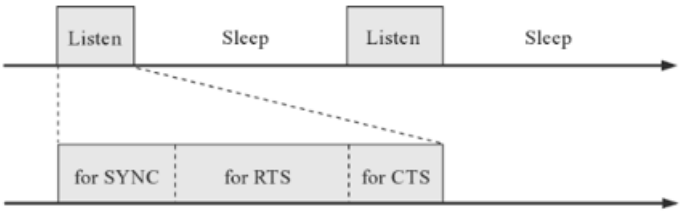

Figure 9: S-MAC Time Schedule

2.4 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:

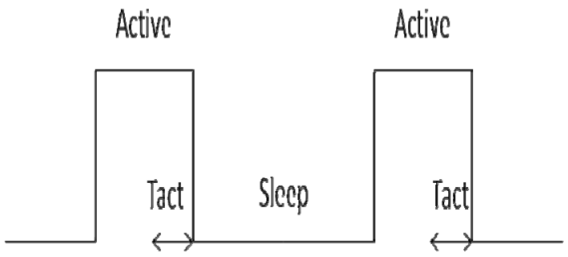

Figure 10: T-MAC time schedule

Thanks to this adaptive behaviour, T-MAC use less energy than S-MAC.

3 Conclusion

As a conclusion, we are going to summarise the studied MAC layers in a table which indexes the Qualities of Service (QoS) implemented by each MAC layer:

	Integrity	**Latency**	**Mobility**	**Data rate**	**Energy consumption**
B-MAC	Yes	Medium	Yes	Low	Low
S-MAC	Yes	High	No	Low	Low
T-MAC	Yes	High	No	Low	Low
Z-MAC	Yes	High if high contention	No	Low	Low if low contention

Talking about security, none of the MAC layer implements directly a security solution. But a data encryption can be added to it to ensure security. Moreover, TDMA-based protocols are more able to implement security than other ones. But it is also important to know that security solutions need energy and software computing, which impacts energy efficiency of MAC layers.

References

[1] "https://upload.wikimedia.org/wikipedia/commons/1/1d/Csma_ca.svg".

[2] "https://upload.wikimedia.org/wikipedia/commons/7/7a/Slotted_ALOHA.svg".

[3] "https://upload.wikimedia.org/wikipedia/commons/3/35/Pure_ALOHA1.svg".

[4] CS425: Computer Networks: Lecture 04. "https://www.cse.iitk.ac.in/users/dheeraj/cs425/lec04.html".

[5] CSMA-CR.png (Image PNG, 399 × 237 pixels). "https://upload.wikimedia.org/wikipedia/commons/1/1f/CSMA-CR.png".

[6] The difference between FDMA and TDMA. "https://www.taitradioacademy.com/the-difference-between-fdma-and-tdma-1/".

[7] Tdma-frame-structure.png (Image PNG, 657 × 456 pixels). "https://upload.wikimedia.org/wikipedia/commons/f/f9/Tdma-frame-structure.png".

[8] What is the key feature of SMAC explain it in detail justify its use in sensor network. "http://www.ques10.com/p/16977/what-is-the-key-feature-of-smac-explain-it-in-deta/".

[9] D-Link. Qu'est-ce que CSMA/CD? "https://eu.dlink.com/fr/fr/support/faq/switches/quest-ce-que-csma-cd".

[10] Daniela Dragomirescu. Toward Internet of Things. Technical report, 2018.

[11] Leonardo Leiria Fernandes. MAC Layer Protocols for Sensor Networks. page 32.

[12] Guillaume Ferré and Eric Simon. An introduction to Sigfox and LoRa PHY and MAC layers. page 7.

[13] Guillaume Ferré and Eric Simon. An introduction to Sigfox and LoRa PHY and MAC layers. Technical report, April 2018.

[14] 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, January 2012.

[15] Sarika Khatarkar and Rachana Kamble. Wireless Sensor Network MAC Protocol: SMAC & TMAC. 4:7, 2013.

[16] 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.

[17] Ajit Warrier, Jeongki Min, and Injong Rhee. Z-MAC: a Hybrid MAC for Wireless Sensor Networks. page 2.