INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

MAC layer protocols for Wireless Sensors Network

Study of the MAC protocols

MARTOCQ Caroline – 5ISS

Jeudi 15 décembre 2016

Table of contents

Introduction 1

1) MAC-related WSN properties 1

a) Power constraints 1

b) Security constraints 1

2) Several categories 2

a) Contention based 2

b) Scheduling based 2

c) Channel Polling based 2

d) Hybrid 2

3) Some MAC protocols for WSN 3

a) SMAC 3

b) WiseMAC 3

c) TRAMA 4

d) ZMAC 4

Conclusion 4

Bibliography 4

Introduction

This document is the result of my research about the MAC layer for Wireless Sensors Network (WSN) which has become a wide domain of research in the last years. This kind of network is needed for a large range of application such as Structural Health Monitoring, target detection and tracking and environmental monitoring. A WSN is built of multiple nodes (hundreds or thousands of them), communicating with each other[1]. A node is typically composed of a microcontroller communicating with sensors (analogue electronics), a RF module with an antenna and a source of energy. Within the first part, we will see the different constraints applied to the MAC protocols so that they can be used in WSN. Then, we will detail four categories of MAC protocols. Finally, we will propose some protocols used in WSN with their advantages and disadvantages. All along this document, we will discuss the quality of service and the security managed by the protocols.

1) MAC-related WSN properties

The MAC layer is specifying the communication method to transmit data from a node to another. When a node is transmitting, every other node within the transmission range is receiving. This can lead to collision and interferences problems. An efficient MAC protocol must be used to manage the communication between nodes in a shared medium.

a) Power constraints

In a wireless sensor network, the battery life is one of the most important parameter since nodes are considered dead when they are out of battery. A lot of elements can be a source of energy waste[2]:

Idle listening: A node needs to keep its radio in ready-to-receive mode because it never knows if it will receive a message or not. This consumes a lot of energy, almost the same as in receive-mode.

Collisions: When two frames collide with each other, the receiver is not able to recover the data and must discard the packet. It results in a retransmission of the packet by the sending node and consumes energy. A high-density network allows to multiply the number of communication but on the other hand it also increases the collision probability.

Overhearing: Every node is receiving packets that are destined to other nodes.

Control packet overhead: An increase in the number and size of control packets results in overhead and unnecessary energy waste for WSNs, especially when only a few bytes of real data are transmitted in each message. Such control signals also decrease the channel capacity. A balanced approach is required so that the required number of control packets can be kept at minimal.

Over-emitting: An over-emitting occurs due to the retransmission of a message when the destination node is not ready to receive it.

Other elements to consider are the scalability and the adaptability to changes in the network. This should be handled rapidly and effectively to have a successful adaptation.

b) Security constraints

For many application, security requirements is a very critical issue. Sometimes, data integrity and authentication is more important than confidentiality. Because of its short lifetime and its limited power resource compared to traditional networking, providing security in WSN is more

different than the other networks. Traditional techniques like Diffie-Helman key agreement protocol or RSA Encryption systems due to limited memory, low computational power and limited energy are not suitable for use in WSN. To conclude, the security requirements for MAC protocols are: data confidentiality, data integrity, data authentication, data freshness and accessibility.[3]

2) Several categories

In this part, we detail the different categories of protocols that can be applied to WSN.[2] The following figure sums up those categories with different types of protocols.

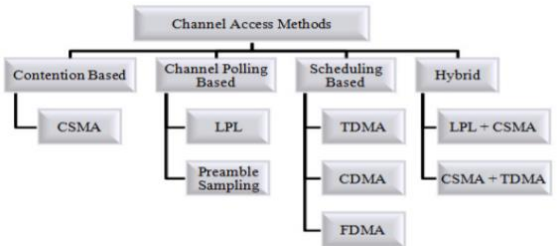

Figure 1 MAC protocols categories

a) Contention based

This type of protocol is working on the acquisition of the channel. Before transmitting, the node checks whether the network is available (no one is transmitting). If this is the case, the node starts transmitting otherwise it will defer the transmission for some time chosen randomly by an algorithm. This is what is used in the protocol CSMA (Carrier Sense Multiple Access). Furthermore, CSMA is using carrier sensing and collision avoidance or detection. Carrier sense is when the node is listening to the shared medium to determine whether another node is transmitting or not. The hidden node problem can lead to undetected transmissions. Collision avoidance allows to hear for the medium and wait for a period of time if another node is currently transmitting. To manage this, it using RTS/CTS (Ready to send/Clear to send) between two nodes. Collision detection allows to detect a collision while transmitting a frame.[4]

b) Scheduling based

A scheduling based protocol is assigning collision-free links between neighboring nodes. The element allocated can be of different type: frequency division multiplexing (FDM) bands, time division multiplexing (TDM) slots or code division multiple access (CDMA).

Let's look a bit further about the TDMA method. The node can transmit its frame in rapid succession using only its attributed time slot. We notice that all the nodes are using the same frequency. This allows to share a same frequency between multiple nodes. One of the disadvantages of this method is that there must be a synchronization between the nodes.

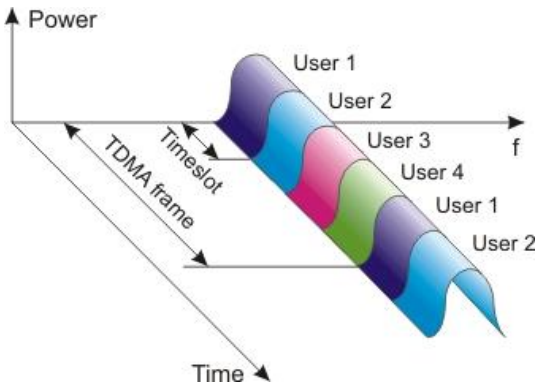

Figure 2 TDMA slot division[5]

c) Channel Polling based

This access method is also known as Low Power Listening. First, the node is transmitting a preamble over the channel to ensure that the destination node detects the radio activity and can wake up before receiving the data packet. If the receiver is detecting a radio activity, it wakes up and turn on its radio to receive the packets. Otherwise, the receiver is going back to sleep until the next polling interval.

d) Hybrid

Hybrid MAC protocols combine two different methods, usually a synchronized and a non-synchronized one. Thus, it is cumulating

the advantages of both the protocols used but can also be more complex. The Z-MAC protocol is an example of the most used hybrid MAC access that is combing TDMA and CSMA.

3) Some MAC protocols for WSN

A lot of MAC protocols are used in Wireless Sensors Network. This sections tries to detail some of them and see their advantages and disadvantages.

a) SMAC

SMAC stands for Sensor MAC. This protocols focuses on overhearing, idle listening and collision to reduce energy consumption. The node is either in sleep or active period. Those intervals are fixed by the algorithm. During the listening period, there are three phases:[6]

- Synchronization phase: The two nodes are synchronizing their listen periods. A broadcast SYNC packet is sent to immediate neighbors and contains the sender's address and the time of its next sleep.
- The node is then transmitting a RTS frame to start the transmission.
- The receiver sends back a CTS packet to tell the sender to start sending data.

A collision avoidance is also achieved by a carrier sense (CS in the next figure). Long messages are divided into frames set in a burst.

The energy waste caused by idle listening as seen previously is reduced thanks to sleep schedules. Furthermore, time synchronization overhead may be prevented by sleep schedule announcements. However, broadcast data packets do not use RTS/CTS method, which increases collision probability.

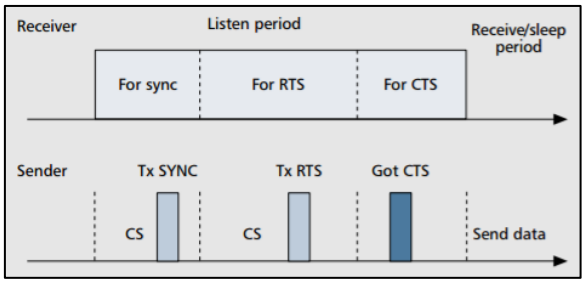

Figure 3 SMAC principle[7]

b) WiseMAC

WiseMAC has been developed by the Swiss Center for Electronics and Microtechnology and is is one of the most low-power consumption MAC layer for WSN. It is an unscheduled wireless protocol. When transmitting a frame, a preamble of variable length is sent to alert the receiving node in its wake-up interval not to go to sleep state but also to check if the medium is available. The sender sends its schedule offset to the receiver which replies with its own. Received schedule offsets of all neighbor nodes kept in a table periodically updated. Based on this table, a node can determine the wake-up patterns of all its neighbors, which in turn allows minimizing the preamble length for the upcoming transmissions. As the sender node is aware of the receiver's wake-up pattern, it only prepends a preamble that compensates for the maximum clock drift that the two involved nodes clocks may have developed during the time since the last schedule exchange.[8]

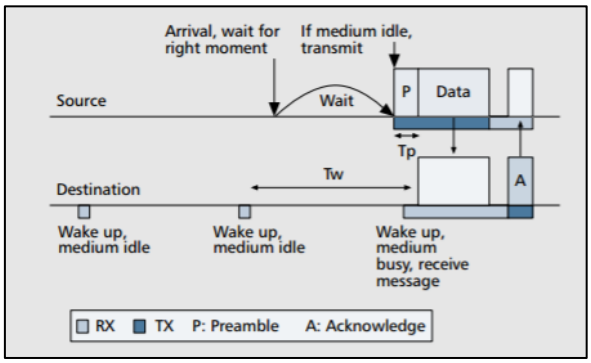

Figure 4 WiseMAC principle[6]

c) TRAMA

TRAMA, Traffic-adaptive medium access protocol is bases on a TDMA method. It has different phases: Neighbor Protocol (NP), Schedule Exchange Protocol (SEP) and Adaptive Election Algorithm (AEA). NP consists in the exchange of information between two-hop neighbors during their slot. SEP allows the nodes to exchange their schedule (slot re-use and sleep step switching) before starting transmission. Thanks to the AEA, a node can transmit only if it has the highest priority among its contending set (two-hop neighborhood).[9]

d) ZMAC

Z-MAC uses CSMA as the baseline MAC scheme, but uses a TDMA schedule as a "hint" to enhance contention resolution. Z-MAC has a setup phase in which it runs the following operations in sequence: neighbor discovery, slot assignment, local frame exchange, and global time synchronization.[10]

Neighbor discovery: this phase is the same as seen in the TRAMA protocol. When a node starts up, it first runs a simple neighbor discovery protocol where it periodically broadcasts a ping to its one-hop neighbors to gather its one-hop neighbor list.

Slot assignment: The two-hop neighbor list is used as input to a time-slot assignment algorithm. TRAND, an algorithm assigning time slots, ensures that two nodes within a two-hop neighborhood are not assigned at the same slot.

Local frame exchange: unlike TDMA, a node may transmit during any time slot. Indeed, when a slot is not in use by its owner, non-owner can steal it. Before transmission, the node performs carrier-sensing to check whether the medium is available.

Global time synchronization: the sender and the receiver are sending each other a packet containing its current clock value. When a node receives a synchronization message, it updates its clock value by taking a weighted moving average of its current value and the newly received value.

Conclusion

Wireless Sensors Network is used in many applications but has some constraints that the MAC layer needs to respect. One of the most element at stake is the power consumption. We have seen that MAC protocols answer to this problem by limiting the wake-up time of the nodes. Dozens of MAC protocols exist and can be applied to WSN but they have advantages and disadvantages regarding their efficiency. Finally, this research allowed me to understand the MAC layer and different protocols.

Bibliography

[1] "Wireless sensor network," *Wikipedia*. 07-Nov-2016 [Online]. Available: https://en.wikipedia.org/w/index.php?title=Wireless_sensor_network&oldid=748340861. [Accessed: 15-Dec-2016]

[2] A. S. Althobaiti and M. Abdullah, "Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross-Layering," *Procedia Comput. Sci.*, vol. 65, pp. 4–16, Jan. 2015.

[3] Ehsan Sharifi, Mohammadreza Khandan "MAC Protocols Security in Wireless Sensor Networks: A Survey" [Online]. Available: http://www.ijcit.com/archives/volume3/issue1/Paper030117.pdf. [Accessed: 15-Dec-2016]

[4] "Carrier Sense Multiple Access with Collision Avoidance," *Wikipédia*. 07-Jan-2016 [Online]. Available:

https://fr.wikipedia.org/w/index.php?title=Carrier_Sense_Multiple_Access_with_Collision_Avoidance&oldid=122070080. [Accessed: 15-Dec-2016]

[5] A. S. Althobaiti and M. Abdullah, "Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross-Layering," *Procedia Comput. Sci.*, vol. 65, pp. 4–16, Jan. 2015.

[4]Ilker Demirkol, Cem Ersoy, and Fatih Alagöz, Bogazici University "MAC Protocols for Wireless Sensor Networks: A Survey" [Online]. Available: http://vahabonline.com/wp-content/uploads/2015/01/Survey___as8edf4esg30.pdf. [Accessed: 15-Dec-2016]

[6] Philipp Hurni, Torsten Braun "Increasing Throughput for WiseMAC" [Online]. Available: http://home.inf.unibe.ch/~rvs/research/pub_files/HB08.pdf. [Accessed: 15-Dec-2016]

[7] Syed Haque "Wireless Sensor Networks" [Online]. Available: http://grid.cs.gsu.edu/yli/teaching/Fall10/sensor/Slides/syed.pdf. [Accessed: 15-Dec-2016]

[10] I. Rhee, A. Warrier, M. Aia, J. Min, and M. L. Sichitiu, "Z-MAC: A Hybrid MAC for Wireless Sensor Networks," *IEEEACM Trans. Netw.*, vol. 16, no. 3, pp. 511–524, Jun. 2008.