MAC protocols for wireless sensor networks

Romain Moulin

Introduction

The Internet of Things (IoT) market exploded these past years, rising from 471,54 billion dollars in 2018 to more than 1177,21 billion in 2023. Everything from the house, to the cars become connected which explains why wireless protocols for sensor networks are crucial. These protocols share some particular characteristics like the need to be energy efficient and low power as sensors are often numerous and in places where physical maintenance is too costly. As sensor networks often include a lot of devices, it is important to define Medium Access Control which establishes rules on how to communicate between devices. In this report, we will study the characteristics for different MAC protocols for wireless sensor networks (WSN).

Contention Based Protocols

Contention based protocols are protocols where every node tries to send data when the medium seems available. This allows to reduce the general overhead of protocols but can lead to collisions which are costly in wireless networks. Examples of WSN contention based MAC protocol are T-MAC (Time-out MAC) and S-MAC (Sensor MAC). Wifi is also a contention based protocol but is not adapted for WSN as its power consumption is too high.

The access method for contention based protocols is often CSMA/CA (Carrier Sense Multiple Access Collision Avoidance). This access method is similar to the one used in ethernet (CSMA/CollisionDetection) with the difference that in wireless networks, we cannot detect a collision when we transmit as the transmitting power is highly superior to the receiving power. With CSMA/CA, devices transmit on the medium when it seems available

but wait for a backoff time chosen randomly before transmitting to be sure that the medium is available. With this method we reduce the risk of collision even if it can still occur.

In S-MAC there is a synchronization part as every node has to listen and transmit on the same active part before going to sleep to save power.

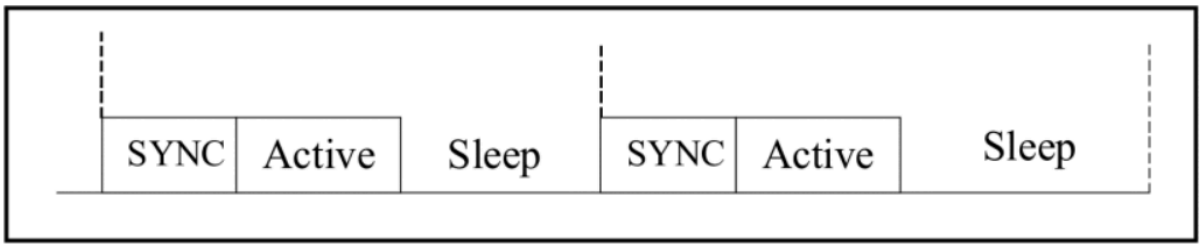

Figure 1: Cycle of S-MAC protocol

T-MAC is another protocol where a node that does not need to send or receive anything goes into sleep mode after not receiving anything in a time out period.

To make some guarantees on the bandwidth, nodes can make RTS/CTS (Request To Send / Clear To Send) in order to reserve the medium to transmit some data.

In both these protocols, it does not seem to implement built in security and relay the security aspect to other layers of the OSI model. As this protocols seems to be used for static sensor, there does not seems to be localization or roaming mechanism.

Scheduled Based Protocols

Another kind of MAC protocols for WSN are scheduled based protocols. With these protocols, each sender has a slot reserved to transmit or receive data. That way, all collisions are avoided and we can give some guaranties on the bandwidth if these reserved slots are periodical.

There are two kinds of scheduled based protocols, cluttered and distributed. With cluttered scheduled based protocols, the network is divided into clusters in which cluster heads are responsible for scheduling the nodes. Distributed scheduled protocols are harder to implement as we have to make sure to allocate non conflicting slots to every node.

A wireless protocol that is Scheduled Based is LEACH (Low Energy Adaptive Clustering Hierarchy). As its name states, it belongs to the clustered scheduled based protocols. In this protocol, nodes send data to a cluster head which aggregate it before sending it to the base station. The access method here is TDMA (Time Division Multiple Access) which means that a frame is divided into slots and nodes are allocated a certain slot to transmit data.

The cluster head sends advertisements to every node so that they know which slots are allocated to them, that way all the nodes in the cluster are synchronized with the cluster head.

It is possible to locate a node based on which cluster it belongs to. For the security part, this protocol does not have any native security. As every node has a dedicated slot, it is

possible to attack the network by transmitting at the same time as a node is supposed to transmit to create collision and that way blocking all communications from a particular node. Finally, this network is designed for WSN with sensors that are fixed so no mobility mechanism exists in this protocol.

Hybrids Protocols

Hybrid protocols implement both contention and scheduled access. One well known hybrid protocol for WSN is Zigbee. Zigbee is a full stack solution designed to connect multiple devices on a short range. Here we will focus on the 802.15.4 norm which is the IEEE norm Low Power Personal Area Networks (LP-PAN) physical and MAC layer which is implemented in Zigbee. For Zigbee there are two access types. One with contention simply using CSMA/CA and one without contention which introduces a coordinator that schedules transmissions on the network. Both access methods can be deployed even if the contention type is not well suited for a large scale network as the number of collisions grows with the number of devices on the network.

We will focus here on the scheduled access. Here a coordinator periodically send beacon message to every node so they can synchronize. A superframe is the active part of a transmission and is the time between two beacon transmissions. This superframe is divided into 16 slots with the first slot being reserved for the beacon. The rest of the frame is divided in two parts the CAP (Contention Access Period) in which devices can send using CSMA/CA and a CFP (Contention Free Period) in which each slot is dedicated to a node. These slots are reserved by the coordinator in order to give some guaranties of bandwidth to nodes. The division of slots between CAP and CFP is flexible and done by the coordinator.

In Zigbee there is no localisation. The node does not know where it is and where the other nodes are. For example the routing mechanism in Zigbees network is flooding the network by sending the packet to every node in radio range. That way you do not keep any information about the topology.

For security, Zigbee does not implement security concepts at the MAC layer. In addition to that, security is hard to implement in Zigbees network as the MTU (Maximum Transmission Unit) is small (about 127 bytes). Finally, no mobility is planned for Zigbees network.

Another hybrid protocol is ZMAC (Zebra MAC). It originally works as a scheduled based protocol, using TDMA and dedicated slots to access the medium but it also authorizes the nodes to compete to access the unused slots by allowing CSMA/CA communication for in unused slots.

Cross-Layer Protocols

Cross-layer are special and come in contradiction with the OSI model. In the model, each layer is supposed to implement a feature independently from the other layers. In the case of Cross-Layer protocols, it allows interaction between layers. Here we will take the example of the 802.16 norm, WiMax (Worldwide Interoperability for Microwave Access). The architecture of such a network is composed of a Base Station (BS) and Subscriber Station (SS). SS communicates with BS to send data. It is a cross-layer protocol because the MAC

layer can communicate to the physical layer to change the channel used depending on the interferences, noises … This is very important in wireless transmissions where interferences can make a network unable to communicate. The access type for this protocol is TDM (Time Division Multiplexing) in downlink (BS -> SS). For uplink (SS -> BS), TDMA is used. In the newest versions, OFDMA is used (Orthogonal Frequency Division Multiple Access).

Slots are allocated to end devices by the BS when a SS connects to the network. A frame is composed of an uplink part and a downlink part (in OFDMA, a frequency is allocated for uplink and one for downlink). In the standard, synchronization is done thanks to the GPS receiver system clock.

The network is divided into cells with one BS for each cell. A cell has a radius of at best 50km. We can locate a device based on which cell it is connected to.

The mobility is integrated into the protocol and a handover system is planned to switch from a cell to another for mobile devices without losing connectivity. It is the same principle as LTE networks. Security is not included in the 802.16 norm so no native security mechanism exists in WiMax protocol.

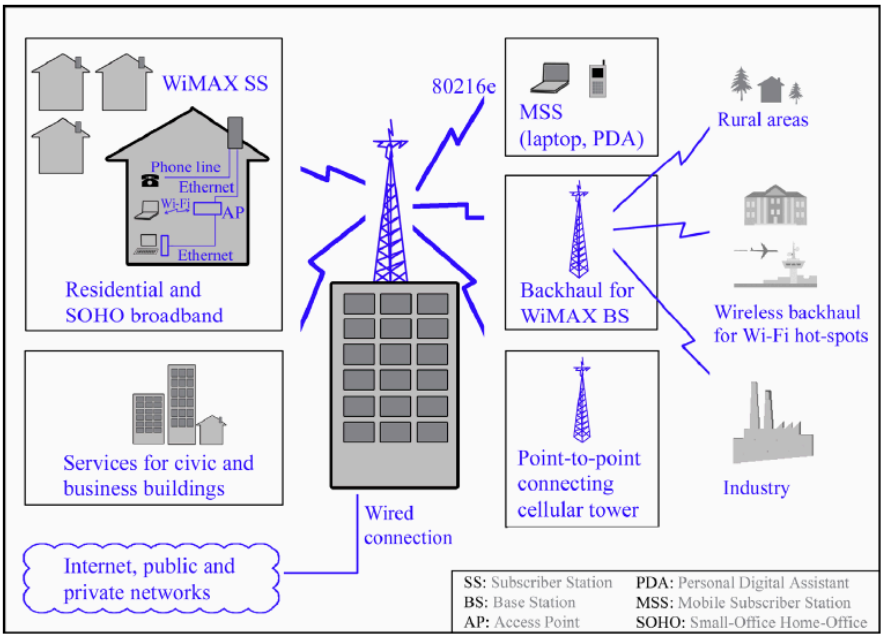

Figure 2: A WiMax network architecture

Conclusion

	Access Type	**Synchronization**	**Localisation**	**Security**	**Mobility**	**example**
Contention based	CSMA/CA	through beacons (not mandatory)	No localization	Not at this layer	No roaming	S-MAC, T-MAC

Scheduled Based	TDMA	advertisement / beacons	Locate in a cluster	No security	No roaming	LEACH
Hybrid	CSMA/CA - TDMA	Through beacons / no synch	/	No security	No mobility (PAN)	802.15.4 (Zigbee), Z-MAC
Cross Layer	TDMA / OFDMA	GPS receiver	in a cell	No security	Mobility like in LTE	WiMax

Sources

Contention and synchronization based network:
https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/5392834

Cross layer Network :
https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/7848335

Different types of WSN MAC protocols :
https://www.geeksforgeeks.org/mac-protocol-used-in-wireless-sensor-networks/

Zigbee network information :
https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/reseaux-locaux-42292210/technologie-zigbee-802-15-4-te7508/

Comparison between contention based and scheduled based protocols:https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/7370623

WiMax network synchronization :
https://www.microsemi.com/document-portal/doc_view/133242-timing-and-synchronization-in-wimax-networks