INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
TOULOUSE

Wireless Sensor Network MAC Protocols

Author : Louis Chauvet-Smart

5ISS – 07/01/2021

1. Introduction

A Wireless Sensor Network (WSN) is a large network comprised of many nodes. These sensor nodes are cheap and many, giving the WSN novel capabilities in measuring a physical environment in detail. There are many applications to this technology, such as security, automation, smart cities and much more. These networks, characterized by their large amount of nodes and wireless communication, come with different requirements, especially regarding energy consumption and sensor features. One of the determining factor in these fields is the Medium Access Control (MAC) protocol, which controls the nodes' radio functionalities.

In this document, we are going to review the main MAC protocols used in WSNs, more specifically looking at the synchronization, localization, security and mobility aspects. We will then classify and compare these protocols to see in which cases they are best applied.

2. MAC Protocols

There are many MAC protocols to study, so we will be seperating them by how they allow nodes to access the channel.

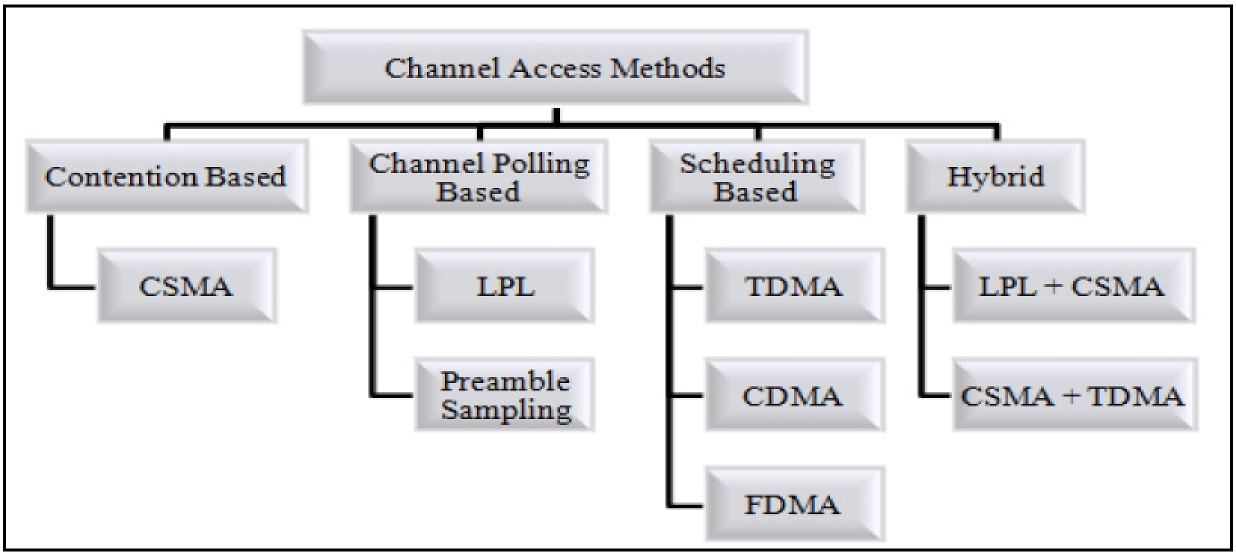

Figure 4: Channel Accessing Taxonomy in WSNs.

Source :*Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross-Layering*, Ahlam Saud Althobaiti and Manal Abdullah

1. Contention Based

In contention based protocols, nodes have to compete with neighbouring nodes to acquire the channel. To do so, the node checks the carrier's status before starting its own data transmission. If it sees the carrier is idle, the node starts its transmission. If the carrier is busy, the nodes tries the same process again after some time. Contention based protocols are usually light on processing resources consumption, but are still pretty flexible to network scaling.

The most common contention based protocol is S-MAC, which works by putting a node in a listening state. If it doesn't hear anything, it sends a SYNC packet detailing a schedule of listen and sleep periods ; every node hearing this packet will then adopt this schedule (each note can adopt multiple schedules). Nodes therefore keep tables with the schedules of their neighbours. A node with a packet to send will send a request to send (RTS), and the receiving node will send back a clear to send (CTS). Every other node not involved in the communication will enter a sleep state for the time of the communication.

This protocol includes clock syncronization, but does not require tight synchronization from a central entity. This also introduces the disadvantage that if the nodes' respective clocks drift, they can become unsynchronized. The sleep periods improve energy consumption, and there are two improvements on this protocol : Timeout T-MAC, by reducing the energy consumption of idle listening by calculating the optimal idle listening and sleeping time based on the nztwork load. The second improvement is DSMAC, and it adds a dynamic duty cycle feature : every node shares their one-hop latency values (the sleep time between each listen), and every node calculates the average value. If it's too high, a node will shorten its sleep time and share it with the network through a SYNC packet. This improvement doesn't reduce consumption, and is instead aimed at reducing latency for delay-sensitive applications.

2. Channel Polling Based

Channel Polling based protocols, also known as Low Power Listening (LPL) or preamble sampling protocols, sends small packets over the channel to make sure the receiving node detects the radio activity and wakes up to receive the transmission. They can fit inside the contention based category, but the differences are enough that they can be considered a category of their own. Every time a node wakes up, if it detects radio activity, it will turn on its radio to receive data packets. Otherwhise, it will go back to sleep until the next polling interval. Therefore, ontrary to the S-MAC based protocols, these protocols are asynchronous and do not require scheduling.

The most commonly used channel polling based protocol is Berkeley MAC, or B-MAC. Each node sleeps, but checks the channel periodically using low powered listenning to check if there is data to transmit, as explained in the previous paragraph. The preamble size (the length of time during which the emiting node sends an emiting notice) is adapted to be as long as the sleep time, to avoid having preambles go unnoticed because of sleep time. The main disadvantage of B-MAC is then that the preambles create a large overheard, needing usually much more data than the actual payload.

3. Schedule Based

Scheduling based MAC protocols assign collision-free links between neighbouring nodes during the initialization phase. There are however many ways to assign links : time division multiplexing (TDM) slots, fequency division multiplexing (FDM) bands, or code division multiple access (CDMA). However, since FDMA and CDMA schemes are pretty complex, WSNs usually prefer TDMA schemes to reduce complexity.

In TDMA schemes, time is divided into slots that are assigned to all the neighbouring nodes, and the schedule is regulated by a central activity. This negates the need to contention between nodes, avoids collisions and overhearing, but requires a knowledge of the network topology, and therefore makes it less flexible for network expansion, and less suited to large networks where synchronizing all nodes is complex. There is also no peer-to-peer communication between nodes, as they can only communicate with the central authority.

Among the most common TDMA based protocols are TRAMA and DMAC. TRAMA is optimised for low power consumption by putting nodes to a low power idle state when they are not transmitting or receiving. To that end, TRAMA gather information about neighbouring nodes, and plans which time slots to allocate to which nodes based on the schedule and the neighbouring nodes information. It's energy efficient, but has higher latency so isn't suited for delay-sensitive applications.

DMAC works under the assumption that often, most of the trafic consists in data collection from several nodes, so it forwards it to a sink through a unidirectional tree, as shown in the following diagram

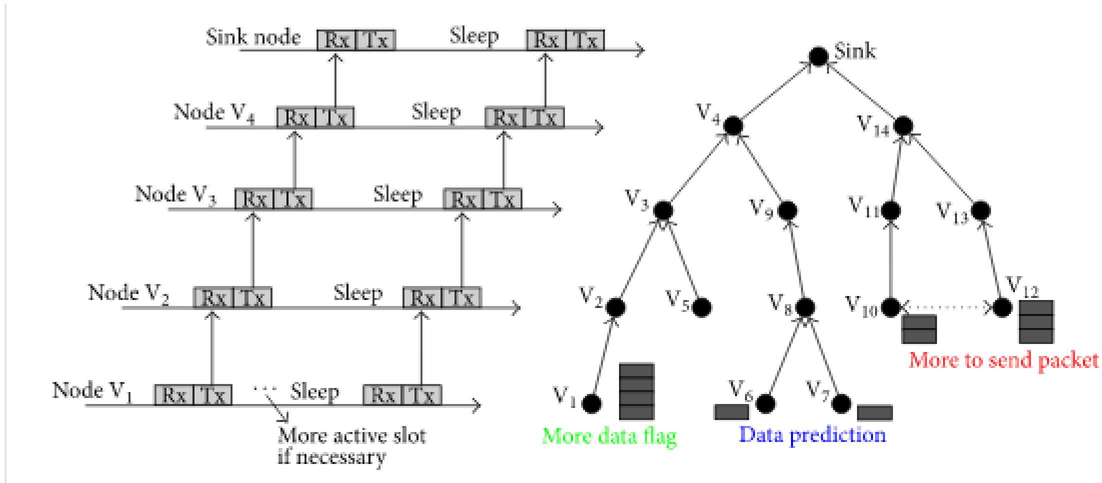

Fig. DMAC in a data gathering tree

4. Hybrid

The idea behind hybrid MAC protocols is to combine the strengths of two or more different MAC schemes. This comination is usually going to be between a synchronous protocol and an asychronous one. The most important hybric MAC protocols are Zebra MAC (Z-MAC) and Funneling-MAC.

In Z-MAC, time slots are allocated to a node, but that node can transmit at any time slot. The allocated time slot is a time during which the node has a priority ; before sending a packet, the node performs carrier sensing and transmits when he gets a clear to transmit. In that way, it adopts two different behaviours depending on contention levels : if the network is overloaded, it behaves like a TDMA protocol. Under low network load, it behaves like a CSMA protocol. It is much more flexible than any of the two modes, but in a very stable environement it will be less efficient pure TDMA or pure CSMA.

Funneling-MAC is closer to DMAC in its structure, with the goal of getting information to a sink node. However, its transmission method is more flexible : in high contention zones, it uses a contention-based schema. In low contention zones, it's schedule based. This way, it can reduce collisions and congestion,

3. Classification
4.

Protocol Type	Contention Based	Channel Polling based	Schedule Based	Hybrid
Examples	CSMA, S-MAC, T-MAC, DSMAC	B-MAC, ALOHA	TRAMA, D-MAC, P-MAC, WISE-MAC	Z-MAC, Funneling-MAC,SCP-MAC,H-MAC

5. Conclusion

With the huge expansion of IoT, a myriad of MAC protocols have appeared to solve all the problems the technology is facing. They each have they advantages and drawbacks, and are suited for particular applications. Scheduled schemes are going to be efficient and low consumption, but lack flexibility and don't allow inter-node communication. Contention-based schemes offer more flexibility, but lose out on energy consumption and payload size. Hybrid protocols offer the best of both worlds, but will show less efficient than a pure scheme in specialized applications.

There's a lack of standardisation among these technologies, and we can find nearly 28 different MAC protocols for various uses. Because of all these niches, it can be hard to find detailed information : we originaly set out to categorize localization, security and mobility capabilities, but were not able to find convincing data for all the different protocols we studied.

Sources :

- Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross-Layering, Ahlam Saud Althobaitia Manal Abdullahb
https://www.sciencedirect.com/science/article/pii/S1877050915029002

-Implementation of a Modified Wireless Sensor Network MAC Protocol for Critical Environments, Viktor Richert , Biju Issac and Nauman Israr
https://www.hindawi.com/journals/wcmc/2017/2801204/#abstract

-MAC Protocols Used by Wireless Sensor Networks and a General Method of Performance Evaluation, Joseph Kabara and Maria Calle
https://journals.sagepub.com/doi/full/10.1155/2012/834784