IPP HURRAY!

www.hurray.isep.ipp.pt

Technical Report

Lower Protocol Layers for Wireless Sensor Networks: A Survey

Anis Koubâa

Mário Alves

Eduardo Tovar

TR-051101

Version: 1.0

Date: 24 November 2005

Lower Protocol Layers for Wireless Sensor Networks: A Survey

Anis KOUBAA, Mário ALVES, Eduardo TOVAR

IPP-HURRAY!

Polytechnic Institute of Porto (ISEP-IPP)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8340509

E-mail: {akoubaa, ffp}@dei.isep.ipp.pt

http://www.hurray.isep.ipp.pt

Abstract

Wireless Sensor Networks (WSNs) have been attracting increasing interests in the development of a new generation of embedded systems with great potential for many applications such as surveillance, environment monitoring, emergency medical response and home automation. However, the communication paradigms in Wireless Sensor Networks differ from the ones attributed to traditional wireless networks, triggering the need for new communication protocols and mechanisms. In this Technical Report, we present a survey on communication protocols for WSNs with a particular emphasis on the lower protocol layers. We give a particular focus to the MAC (Medium Access Control) sub-layer, since it has a prominent influence on some relevant requirements that must be satisfied by WSN protocols, such as energy consumption, time performance and scalability. We overview some relevant MAC protocol solutions and discuss how they tackle the trade-off between the referred requirements.

Lower Protocol Layers for Wireless Sensor Networks: A Survey

Anis KOUBAA, Mário ALVES, Eduardo TOVAR

IPP-HURRAY! Research Group, Polytechnic Institute of Porto

Rua Dr. Antonio Bernardino de Almeida, 431, 4200-072 Porto, PORTUGAL

{akoubaa, emt}@dei.isep.ipp.pt , mjf@isep.ipp.pt

Abstract

Wireless Sensor Networks (WSNs) have been attracting increasing interests in the development of a new generation of embedded systems with great potential for many applications such as surveillance, environment monitoring, emergency medical response and home automation. However, the communication paradigms in Wireless Sensor Networks differ from the ones attributed to traditional wireless networks, triggering the need for new communication protocols and mechanisms. In this Technical Report, we present a survey on communication protocols for WSNs with a particular emphasis on the lower protocol layers. We give a particular focus to the MAC (Medium Access Control) sub-layer, since it has a prominent influence on some relevant requirements that must be satisfied by WSN protocols, such as energy consumption, time performance and scalability. We overview some relevant MAC protocol solutions and discuss how they tackle the trade-off between the referred requirements.

Keywords: *Wireless Sensor Networks, wireless communication protocols.*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have revolutionized the design of emerging embedded systems and triggered a new set of potential applications. A WSN is typically composed of a large set of nodes scattered in a controlled environment and interacting with the physical world. This set aims the collection of specified data needed for the monitoring/control of a predefined area/region. The delivery of sensory data for process and analysis, usually to a control station (also referred as *sink*), is based on the collaborative routing work of the WSN nodes (Fig. 1).

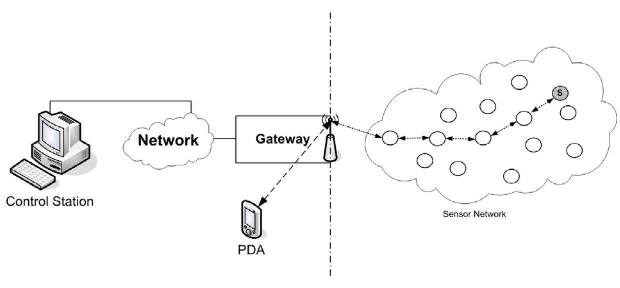


Fig.1. Typical topology of a Wireless Sensor Network

Hence, a WSN node should include some basic capabilities, namely sensing (eventually other I/O), processing (and memory) and wireless communications, acting namely as:

- *data source*, that produces sensory data by interacting with the physical environment and collecting a specified data needed for control, e.g. temperature, humidity, pressure, movement;
- *data router*, that transmits data from one neighbour sensor node to another, towards the control station, which processes and analyses the data collected from the different sensors/nodes in the network.

This particular form of distributed computing raises many challenges in terms of real-time communication and coordination due to the large number of constraints that must be simultaneously satisfied, including limited power, CPU speed, storage capacity and bandwidth. These constraints trigger the need for new paradigms in terms of sensor design and network communication/coordination mechanisms.

In this context, there are several open research initiatives aiming to provide reliable and real-time communications in WSNs. This Technical Report overviews the state of the art on communication protocols and architectures for WSNs, focusing on the lower communication layers. Section 2 addresses some generic characteristics of WSNs, namely about resource constraints and communication paradigms. Section 3 outlooks the layered architecture of WSNs. Then, Section 4 provides and overview of the most important aspects of the Physical Layer, presenting and comparing some of the existing technologies, namely those derived from the IEEE 802.15.x line of protocol standards. Section 5 focuses on aspects related to the Data Link Layer. This section starts (in 5.1) by summarizing and classifying existing MAC (Medium Access Control) protocols for traditional wireless networks. Then, it presents (in 5.2) some important issues on the design of MAC protocols for WSNs. Section 5.3 describes some limitations of the existing approaches outlined in 5.1 against the specific requirements of WSNs expressed in Section 5.2. In Section 5.4, some relevant MAC protocols for WSNs are briefly described. Finally, Section 6 overviews some general aspects on the Network Layer in WSNs.

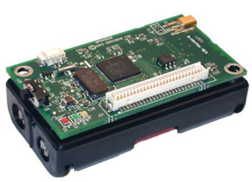
2. GENERAL CHARACTERISTICS OF WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) have very specific characteristics. When compared to commonly-used ad-hoc networks, WSNs typically differ in two aspects: resource constraints and communication paradigms. These issues are addressed next.

2.1. Resource Constraints

Traditional wireless communication networks such as Wireless Local Area Networks (WLANs) or Mobile Ad-hoc Networks (MANETs) do not have to cope with resource limitations. However, in WSNs, *power*, *memory*, *CPU* and *bandwidth* are scarce resources. This limitation in terms of resources results from two factors related to the design and deployment of WSN devices into a network. As for the design of WSN nodes, these devices must be low-cost, lightweight and of miniature size. They are intended to be deployed in large numbers in the environment being monitored/controlled. These severe constraints impose the design of creative solutions for supporting reliable and real-time communications in WSNs. New solutions are required not only to resolve specific problems but also to deal with trade-offs. For instance, Table 1 presents some relevant characteristics of the MICA2 (MPR400CB) mote, which is a solution from Crossbow Technology [xbow].

Table 1. Look and characteristics of the MICA2 mote



Program Flash Mem.	128 kbytes
Measur. Flash Mem.	512 kbytes
Config. EPROM	4 kbytes
Data Rate	38.4 kbits/s
Radio Channel	916 MHz
Battery	2 x AA
Battery Voltage	2.7 – 3.3 V
Size (mm)	58 x 32 x 7
Weight (grams)	18 (without batteries)

Resource limitations are reflected by short-sized programme (128 kbytes) and storage (512 kbytes) memory capacity and low data rate (38,4 kbits/s) when compared to typical MANET technologies. Even the 250 kbit/s bit rate supported by [IEEE 802.15.4] is considered as "low rate".

As a consequence, these constraints turn out to be of utmost importance in the design of a communication framework for WSNs. For instance, the operating system of a WSN node should take into consideration the limitation in power resources. TinyOs [Hill00] is one of the first operating systems designed for WSNs, featuring a reduced code size while supporting communication, multitasking, data acquisition and hardware driver capabilities.

2.2. Communication Paradigms

Wireless sensor networks are driven by different communication paradigms from the ones of traditional wireless networks. These new paradigms result from the severe constraints previously mentioned and also from the large number of nodes envisaged for most WSN applications. In most WSN applications, it is envisaged to monitor a area/region in a certain environment. Therefore, it is not mandatory to know the logical identification of a sensor node producing sensory data, but more prominence is given to the geographic location where the data is originated from. As a result, we enumerate three communication paradigms that can be associated to WSNs:

- *Data-centric*

  While classical WLANs/MANETs are based on a logical address to identify each mobile station (address-centric), WSNs typically operate in a different manner. WSN nodes may not have a global identification such as a MAC or IP address typically used in traditional networking schemes. In data-centric networks, importance is given to data rather than to the devices where that data are produced. Data from multiple sources related to the same physical phenomenon need to be aggregated and sent to the control station.

- *Large-Scale*

  In WSNs, nodes are deployed in large numbers. Consequently, communication protocols should be adequate for networks with a large number of nodes and introduce a small communication overhead.

- *Location-based routing*

  The identification of a node within a WSN should be based on its geographic position in the controlled area and not on a logical address. This kind of identification fits better the data-centric and large-scale properties of WSNs. In a location-based routing, a WSN node is only required to know the position of its immediate neighbours, without having to maintain a large routing table based on logical addresses.

The resource limitation issues and this shift in the communication paradigms have prompted the development of new WSN-specific communication protocols oriented to location-based geographic routing (e.g., GPSR [Karp00], SPEED [He03], direct diffusion [Intanagonw00]), which minimize energy consumption and storage requirements, efficient data dissemination protocols (e.g. SAFE [Kim03]) and data link protocols optimized for time critical applications and energy saving (e.g. [IEEE 802.15.4]).

3. PROTOCOL ARCHITECTURE

A general scheme for the architecture of a WSN communication protocol was proposed in [Akyildiz02] and consists in a conjunction of a five-layer protocol stack and three management plans (Fig. 2). The authors present the purpose of each layer in the protocol stack and the challenges that must be considered in its design.

Concerning the Application Layer, different types of applications can be devised, depending on what is expected from the system. The Transport Layer aims to maintain the flow of data, if it is required by the system. The Network Layer routes sensory data regarding the new communication paradigms described in Section 2.2. The Data Link Layer must provide timely and reliable peer-to-peer communications, namely a MAC (Medium Access Control) mechanism for managing distributed access to a shared transmission medium with minimum power consumption and communication overhead. The Physical Layer addresses the need of simple yet robust modulation, transmission and receiving techniques.

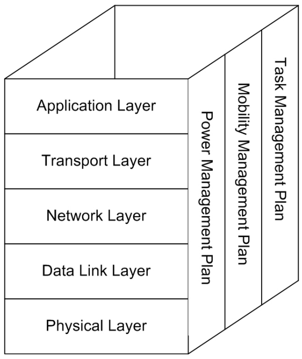


Fig.2. Architecture of a WSN communication protocol

The management planes represent the additional issues needed to deal with optimal power consumption, mobility of sensor nodes and resources sharing.

In the following, we discuss the most relevant features of each communication layer and present the related solutions, with a particular emphasis on the Data Link Layer.

4. PHYSICAL LAYER (PHL)

This section reviews the physical layer features in wireless networks and its adequateness to WSNs.

4.1. General aspects on Wireless PhLs

In wireless communications, the physical layer must provide the appropriate signal modulation with respect to the frequency range allowed for the target applications. On the receiving side, this layer must also perform signal detection and deal with propagation effects (e.g. path loss, delay spread).

In WSNs, the physical layer has to dedicate a special care to the inherent constraints, including low-power consumption and hardware design. An important requirement for wireless sensor networks is the efficient power management which is typically related to the modulation scheme, data rate, transmit power (depending on the transmission distance) and operational duty cycle.

4.2. Modulation schemes

Since WSNs may be used in hostile environments (e.g. battlefields) or in severe weather conditions (environmental monitoring), the modulation schemes have to be designed to be resistant to noise, interference, jamming, and unauthorized detection. The Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are modulation schemes typically used in wireless networks (e.g. IEEE 802.11), including WSNs. Both modulation techniques are robust but DSSS in more efficient than FHSS in the case of narrowband interference, i.e. the interfering signal remains inside the spreading band. However, the opposite is true when the interfering signal is larger than the spreading band [McCune00].

4.3. Wireless Media

Another important feature of WSNs is that they feature *short-range* wireless links. This is due to the fact that transmit power increases with the distance to the receiver.

Essentially, two types of wireless media may be used in WSNs: radio and optical (e.g. infrared), where the former is the most common due to the inherent limitations of optical communications (e.g. line-of-sight requirement).

Current commercial WSN technologies use the license-free ISM (Industrial, Scientific, and Medical) radio bands, defined by the International Telecommunication Union. In this context, [Porret00] recommends ultrahigh frequency ranges, in order to achieve power savings. Common carrier frequencies of the ISM bands deployed in today's WSNs include the 433 MHz and 868 MHz frequencies (proposed for Europe and Japan), the 915 MHz frequency (proposed for North America) and the 2.4 GHz frequency.

4.4. Comparing IEEE802.15.1/2/4 protocols

Although the IEEE 802.15.1 and IEEE 802.15.2 (supporting Bluetooth) have been considered as potential solutions for some WSN applications, these protocols have some important limitations in this context. In fact, IEEE 802.15.1/2 protocols have not been designed to fit the inherent requirements of WSNs in terms of power consumption, data rate, timing constraints and cost.

The increasing need of a typical solution for WSNs has lead to the release of the IEEE 802.15.4 standard [IEEE 802.15.4]. This protocol, which constitutes the lower part of the ZigBee protocol [ZigBee], uses the same frequency bands as IEEE 802.15.1/2 but implements different modulation schemes, in order to enhance power management. Table 2 presents the physical layer differences between the IEEE 802.15.1/2 and IEEE 802.15.4 protocols.

Table 2. Differences between IEEE 802.15.1/2/4 physical layers

	IEEE 802.15. 1/2	IEEE 802.15.4
Modulation	FHSS	DSSS
Maximum data rate	~ 1 Mbit/sec	~ 250 Kbit/sec
Range	Up to 100 meters	Up to 70 meters

As an example, the MICAz mote [xbow] manufactured by Crossbow Technology is IEEE 802.15.4 compliant (only at the Physical Layer) and provides a significant enhancement on the overall functionality of the Crossbow's MICA mote family. Compared to the MICA2 mote radio module, which provides 38.4 Kbit/s with RF power varying from -20 dBm to +5 dBm for an outdoor range of 150 meters, the MICAz mote offers better data rate of 250 Kbit/s with lower RF power from -24 dBm to 0 dBm for an outdoor range of 75 m to 100 m.

The design of the physical layer for WSNs has a significant impact on the efficiency of energy consumption, but a negligible effect on real-time issues. The latter requirement is particularly considered at the Data Link and Network Layers.

5. DATA LINK LAYER (DLL)

The Data Link Layer (DLL) is mainly divided into 2 sub-layers: Logical Link Control (LLC) and Medium Access Control (MAC). In the following, we will only address the MAC sub-layer, since it has more significant effects in terms of energy-consumption and real-time issues. This section firstly presents some typical MAC approaches for wireless networks. Then, it presents the design issues of MAC protocols for WSNs and later a discussion on the advantages and limitations of the above MAC protocols. Finally, we present a set of MAC protocols for WSNs that have recently been proposed.

5.1. MAC protocols for Wireless Networks

A common challenge of the DLL is to schedule the available data for transmission (in the overall network) and provide a mechanism for each node to decide when and how to access the shared medium to transmit its data. These functionalities are basically performed by Medium Access Control (MAC) protocols. In the literature, a wide variety of MAC protocols has been proposed for traditional wireless networks such as IEEE 802.11 and Bluetooth.

Existing MAC protocols in traditional wireless networks fit into three basic categories (Fig. 3): s*cheduling-based*, c*ollision-free* and *contention-based*.

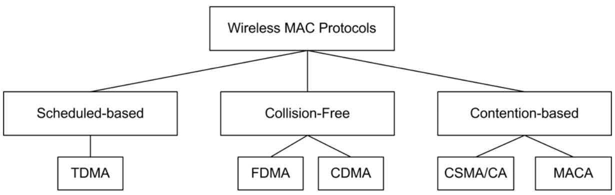


Fig.3. Wireless MAC Protocols Families

These MAC protocol classes differ in the mechanism for collision avoidance. A collision occurs when two nodes send their data at the same time on the same shared medium. Thus, the purpose of MAC protocols is to mitigate potential collisions as much as possible. The most important aspects of these MAC categories are presented next.

Scheduling-based protocols

Scheduling-based protocols avoid collisions by means of a centralized scheduling algorithm that determines the time at which a node can start its transmission. TDMA (Time Division Multiple Access) [Baker82], [Baker84], [Stevens90] is a scheduling-based protocol that gained much interest in wireless networks. Basically, it consists on dividing the shared channel into N time slots, allowing only one node transmit in each time slot. This centralized approach requires a central (base) station that *schedules* the medium access to other mobile nodes (Fig. 4), and thus, mobile nodes must be inside the covering range of the base station to get connected to the overall network.

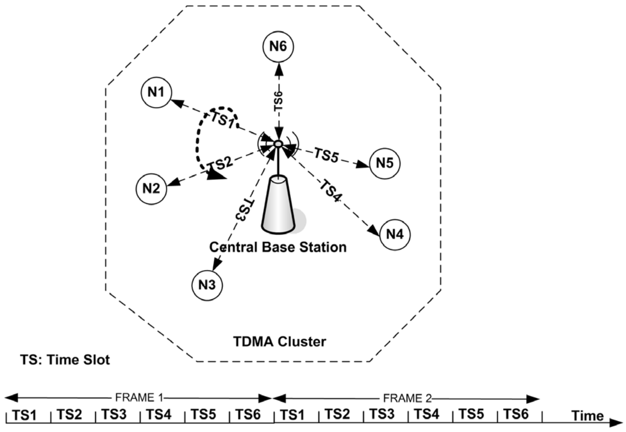


Fig. 4. Scheduling-Based MAC Protocol (TDMA)

A set of base station with mobile nodes within its range is commonly called a *cluster*. Hence, TDMA-like protocols offer an excellent way for collision avoidance in wireless networks, but at the cost of:

- Strong limitation in terms of mobility pattern of mobile nodes, since the scattered nodes must communicate with the base station to send data to any other node within a single cluster,
- Time synchronization requirement between the base station and mobile nodes.

The advantages and limitations of TDMA-like protocols regarding WSN requirements are discussed later in this Technical Report.

Collision-free protocols

Collision-Free protocols avoid collisions by using different radio channels (frequencies or codes) to each communication action between two mobile nodes, enabling simultaneous data transmission without interference or collision. There are two basic collision-free approaches used in wireless communications:

- FDMA (Frequency Division Multiple Access) consists on dividing the whole spectrum into separated frequency bands, so that each pair of communicating nodes is allocated a part of the spectrum (all the time). Hence, simultaneous transmissions on the different radio channels are possible, with no collision problems.
- CDMA (Code Division Multiple Access): While TDMA protocols allocate the whole spectrum to a node for a part of time and FDMA protocols allocate a part of the spectrum to a node for all the time, CDMA protocols allocate the whole spectrum to a node for all the time (Fig. 6). In Fact, CDMA uses unique codes to spread the base band data before transmission. Each code enables

the identification of a unique communication among all simultaneous transmissions on the shared spectrum.

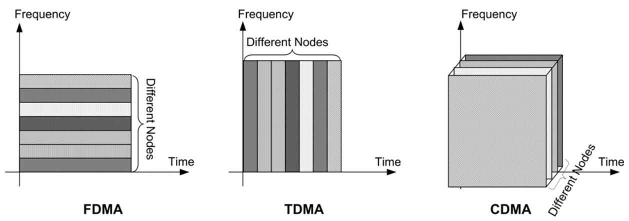


Fig. 6. Multiple Access Schemes

FDMA and CDMA protocols have been basically used for communication between different clusters of the same wireless network. Each cluster is assigned a different frequency/code to avoid interference with any adjacent cluster.

Contention-based protocols

The *Contention-based* protocol paradigm consists on dealing with collisions while trying to minimize their occurrence rather than avoiding them completely (such as in Scheduling-based or Collision-Free protocols). Instead, a single radio channel is shared by all nodes and it is allocated on-demand. Consequently, if two or more nodes try to allocate the shared medium at the same time, collisions occur. In this case, distributed algorithms are used to re-allocate the channel between competing nodes in a way to reduce the probability or even avoid collisions.

Basically, most distributed MAC protocols are contention-based and employ carrier sensing and/or collision avoidance mechanisms (except pure ALOHA). Therefore, they are commonly known as CSMA (Carrier Sense Multiple Access) protocols [Kleinrock75], which consists on listening before transmitting. The purpose of listening is to ensure that the channel is idle before starting the transmission. In this case, the node starts transmitting immediately (in non-persistent CSMA and 1-persistant CSMA variants) or with a certain probability (*p*-persistent CSMA variant) [Kleinrock75][Ye03]. If the medium is busy, the node waits a random amount of time before it starts sensing the medium again (in non-persistent CSMA variant), or it continues to listen until the medium becomes idle, and then transmits immediately (in 1-persistant CSMA).

In multi-hop wireless networks, using CSMA-based protocols leads to the hidden and exposed node problems, illustrated in Fig. 7. In the hidden node problem (Fig. 7a), nodes *S1* and *S2* cannot directly communicate due to insufficient radio coverage. Hence, if *S1* start transmitting data to its immediate neighbour R, *S2* will not be aware of that transmission and may also start sending its available data, since it assumes that the medium is idle. As a consequence, a collision will occur on the receiving node *R*. In the exposed terminal problem (Fig. 7b), while S1 is transmitting to R1, S2 overhears the transmission and does not transmit to R2 believing that a collision would occur (since the medium is busy). However, R2 and R1 are not within range and therefore simultaneous successful transmissions would be possible.

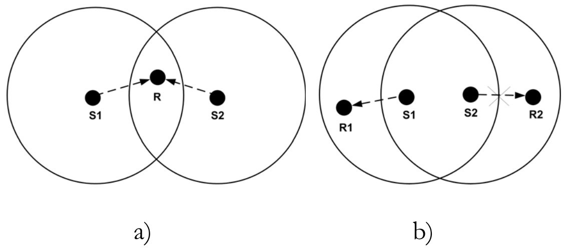


Fig. 7. a) *Hidden Node Problem* b) *Exposed Node Problem*

Hence, additional signalling control messages have been proposed to cope with the hidden and exposed terminal problems, which can be grouped in these two classes:

- *out-of-band signalling*, which consists on sending a busy tone, out of the communication frequency band, when a node hears an ongoing transmission, so that other nodes do not initiate their transmissions. This mechanism is called the Busy-Tone Multiple Access (BTMA) [Tobagi75], which eliminates the hidden terminal problem, but increases the exposed terminal problem;
- *in-band handshaking*, which consists in exchanging in-band control packets as startup messages before the effective data transmission. This mechanism initiates the transmission between two nodes and all other nodes in this communication range are aware of that transmission.

The most renowned protocol using in-band handshaking is CSMA/CA (Collision Avoidance), supported by the IEEE 802.11 standard. Before the effective transmission, the sender transmits a short *Request-To-Send* (*RTS*) packet to the receiver. The latter replies by sending back a *Clear-To-Send* (*CTS*) packet, allowing the sender to start sending its data upon reception of the CTS packet. All other neighbour nodes hearing RTS/CTS packets should go to a back-off state and defer their transmission. The hidden terminal problem is not completely eliminated with CSMA/CA since collisions may occur on RTS packets, but it is mitigated to a large extent.

Many other extensions of CSMA/CA have been proposed to enhance the RTS/CTS mechanism. For instance, Multiple Access with Collision Avoidance (MACA) was proposed in [Karn90] on the basis of CSMA/CA, in which a duration field is added in both RTS and CTS packets indicating the amount of data to be transmitted. This additional information enables other nodes (hearing RTS/CTS packets) to know the length of data to be sent and thus to estimate their back-off delay. Other variations of MACA, such as MACAW [Bharghavan94] that includes the use of an acknowledgement after a successful transmission, MACA/PR [Lin99], which provides guaranteed bandwidth support (via reservation) to real-time traffic, and MACA-BI, which eliminates the RTS part from the RTS/CTS handshake, have been proposed. The CSMA/CA, MACA and MACAW protocols have been integrated in the IEEE 802.11 standard in its Distributed Coordinator Function (DCF), designed for ad hoc networking.

For more details about wireless MAC protocols, interested readers can refer to [Ye03], [Stankovich03] and [Fullmer97].

Section 5.2 outlines some important design issues of MAC protocols for WSNs. Then, Section 5.3 presents some limitations of the above MAC protocols regarding the requirements of WSNs. Finally, Section 5.4 describes some recent MAC schemes for WSNs.

5.2. MAC protocols for WSNs: design issues

The design of the data link layer in WSNs has been subject of many controversial research studies. In fact, considering all protocol layers, the data link layer is the one that plays the most important role in terms of real-time guarantees, energy efficiency, scalability, and QoS issues (throughput, latency, reliability). The design challenge is not only to provide novel solutions that target a specific attribute, but also to deal with trade-offs between all attributes. In other words, a MAC protocol designed to perfectly mitigate power consumption in a sensor node, and thus increasing its lifetime, might be inadequate if it does not address the scalability issue or take into account the timing constraints of the applications. Thus, an effective MAC protocol for WSNs must consider these attributes. However, the weight of each attribute may vary from one application to another due to the wide variety of WSN applications and their diverse requirements. For instance, an application might be more sensitive to real-time guarantees (e.g. emergency control, fire alarm, motion monitoring etc.) while others may be more demanding in terms of network lifetime and thus energy consumption (environment monitoring, home automation, etc.). For that reason, there is no predominant standard solution for WSNs, but rather a large set of MAC protocol proposals, while each approach is more suitable for a certain application pattern.

In the following, we examine some important MAC attributes in WSNs, namely energy, timeliness and scalability.

Energy

A primary goal in the design of a MAC protocol for WSNs is to minimize the power consumption and thus enabling longer network lifetime. To design an energy efficient MAC protocol, we have to identify energy-consuming factors, namely the ones described next:

- *Collisions*

  When a collision occurs, the collided packet must be discarded and then re-transmitted, which results in wasted (transmission) energy. Thus, avoiding collisions is an important issue to save energy and increase the network lifetime.

- *Overhearing*

  Overhearing occurs when a node receives a packet destined to other nodes. Consequently, for a heavy traffic load, overhearing unwanted packets leads to increasing power consumption uselessly, particularly in high-density networks.

- *Idle listening*

  Idle listening occurs during channel sensing to receive possible data in contention-based MAC protocols. Even if a node is neither receiving nor transmitting, the consumed power is important [Kasten],[Schurgers02]. The cost of energy consumption in idle state depends on radio hardware and operation modes. While the transmit power is dominant for long-range radio tranceivers, this is not generally the case for short-range radio tranceivers typically deployed in WSNs. Some authors (e.g. [Kasten], [Schurgers02]) state that the order of magnitude of listening, receiving and transmitting in terms of power consumption is almost the same. In [Kasten] the measurements made on the Digitan Wireless LAN module (IEEE 802.11 at 2 Mbit/s) show that the power consumption ratios of *idle*:*receive*:*transmit* are 1:2:2,5. [Schurgers02] shows that power ratios are 1:1,01:1.2 for the TR1000 radio from RF Monolithics [ASH02], with the transmit range set to approximately 20 meters. Recent advances in the design of radio transceivers result in an important mitigation of energy consumption in idle listening. For instance, on the IEEE 802.15.4 compliant MICAz mote [xbow], the ratios of current draw are 1:985:870 at 2,4 GHz with a RF power of 1 mW. This enhancement is very beneficial in terms of power saving in WSNs.

- *Control-packet overhead*

  Control-packet overhead also results in wasted energy, since the transmission, reception and listening of those packets are energy consuming. Hence, it is important that the number of control packet should be reduced to save energy.

- *Over emitting*

  Over emitting is also a possible source of wasted energy, occurring when a sender transmits a packet to a node which is not available anymore.

Thus, energy-aware MAC protocols must take into account all previous energy dissipation factors by tightly controlling the radio transceiver to avoid collisions, continuous unnecessary listening and long-range communications. Also, it is always beneficial to turn off the radio when it is not needed so that to save energy (e.g. sleep mode).

Timeliness

Another important feature of MAC protocols for WSNs is to provide real-time guarantees for time-critical applications. Although real-time communications was not considered as a primary goal for primitive applications in WSNs, there is an increasing demand of time-sensitive applications that require bounded communication delays. For instance, among the wide variety of applications being deployed in WSNs, many applications such as surveillance and emergency medical care have stringent timing constraints. One of the motivating examples of real-time applications in sensor networks is tracking and monitoring doctors and patients inside a hospital [Malan04]. In such an application, each patient may have small WSN nodes attached, where each sensor has its specific sensory data (e.g. heart rate, oxygen saturation or blood pressure). Medical staff may supervise all sensor data using mobile devices (PDA, Laptop, PCs) through a WSN. It is evident that for the sake of efficiency, critical data have to be displayed in limited time (particularly in emergency situations) to perform the adequate actions on corresponding patients.

Therefore, the MAC layer of WSNs must provide real-time guarantees (or at least some level of QoS) to fulfil the requirements of time-critical applications.

Scalability and adaptability

The scalability and adaptability features are typically related to the large-scale, node density, node unreliability and dynamically-changing topology characteristics of WSNs. A MAC protocol must be highly scalable to deal with a large number of nodes with different node density patterns in the controlled environment. Also, it must also be adaptable to dynamic topology changes due to node failure or mobility. Hence, one important issue in WSNs is the system to be *self-organizing*. Moreover, to deal with the intrinsic unreliability of any single node and the large-scale features of WSNs, MAC protocols must implement *decentralized* algorithms.

The above attributes are the most significant for the design of MAC protocols in WSNs. Nevertheless, there are several other less important features that may also have to be considered, such as throughput, fairness, and channel utilization [Ye03].

After specifying the predominant attributes of MAC protocols for WSNs, we can evaluate and compare existing approaches, according to how they fulfil each individual requirement and also assess in what extent these MAC protocols accomplish a balance among these attributes.

5.3. Limitation of existing Wireless MAC protocols for WSNs

This section discusses the limitations of existing MAC protocols (Section 5.1) to fulfil the specific requirements of WSNs (Section 5.2). A MAC protocol should provide a good trade-off among energy-efficiency, real-time and scalability attributes, rather than providing excellent performance on one and neglecting the others.

Scheduling-based protocols

Scheduling-based protocols such as TDMA and its variants are inherently energy-efficient since they avoid collisions while scheduling medium access among all nodes and also enable fair sharing of the shared channel, if provided with an adequate scheduling algorithm. Also, scheduling-based protocols can ensure bounded delays to real-time applications since each node has the guarantee to access the medium within its pre-allocated time slots. Also, overhearing can be avoided by turning off the radio during the slots of other nodes. However, the main limitation of those protocols that hinder their deployment in large-scale sensor networks is their hierarchical organization and synchronization requirement, reducing their capacities to cope with dynamic topology changes and highly dense networks. Such centralized behaviour is impractical in general WSNs, which require ultra high adaptability and scalability.

Collision-free protocols

Collision-free protocols also fulfil energy efficiency requirements due to the inexistence of collisions. They have also the capacity to provide real-time guarantees with potential throughput increase and lower delay bound [Stankovic03]. The only problem is related to the additional complexity of these schemes when implemented on WSN nodes, which potentially leads to increased hardware cost. In [Stankovic03], further studies to investigate whether the performance gain would overcome the increased hardware cost are recommended.

Contention-based protocols

Contention-based protocols are likely to be the less adequate for WSNs since they may be quite power consuming due to potential collisions that may occur, especially in highly-dense large-scale WSNs. Other factors of energy waste in contention based protocols are idle listening, overhearing and control packet overhead. Moreover, due to the distributed contention-based MAC mechanism, a packet may not be transmitted or may experience an unbounded medium access delay. One positive feature of contention-based protocols, with regards to sensor networks requirements is their ability to scale and self-organize easily when facing frequent topological changes. This interesting feature has fostered the research in this area to enhance power management by largely reducing the chances of collisions, and controlling the radio transceiver by going to sleeping state when it is not needed. For instance, the MICAz mote only consumes 1 μA in sleep mode while it consumes 20 μA in idle listening mode. This figures show the important gain in terms of energy saving when the radio transceiver is turned-off. This can be suitable for some applications that are more demanding in terms of energy efficiency rather than in terms of timeliness. However, those protocols should at least provide soft-real time guarantees so that the delay remains statistically limited to a well-defined bound.

5.4. MAC protocols for WSNs: some representative proposals

A large number of MAC protocols were proposed (some of them derived from traditional MAC protocols) for achieving trade-offs between the data link layer attributes previously described, namely energy, real-time and scalability. This section presents a number of recently proposed MAC protocols for WSNs.

LEACH [Heinzelman00]

The LEACH (*Low Energy Adaptive Clustering Hierarchy*) protocol [Heinzelman00] is a scheduling-based MAC protocol, basically extending the cellular TDMA model to WSNs. In fact, the LEACH protocol consists on dividing the WSN in several adjacent clusters and applying TDMA within each cluster (Fig. 9). Inter-cluster communication is based on CDMA protocols to avoid interference between adjacent clusters.

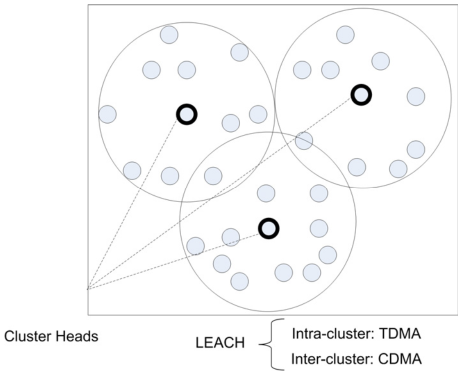


Fig. 9. LEACH Communication Structure

The main purpose of the LEACH protocol is to evenly distribute energy load among the WSN nodes. In fact, LEACH does not rely on "static" clustering, since such a scheme would quickly drain the battery of the selected cluster-head nodes. Instead, LEACH performs dynamic clustering by randomly assigning the cluster-head functionality between all nodes to extend the overall WSN lifetime. A new round is started cyclically, and the set of cluster-head nodes is dynamically redistributed after a certain period of time of the previous selection round.

In each round, the LEACH protocol consists on three phases: advertisement phase, set-up phase and steady phase. These are briefly described next.

In the *advertisement phase*, a random selection of a cluster-head node is performed, where each node decides whether to become a cluster-head or not. The decision is positive when a randomly chosen value between 0 and 1 is lower than a threshold $T(n)$ defined as:

$$T(n) = \begin{cases} \dfrac{P}{1-P\left[r \bmod (1/P)\right]} & \text{if } n \in G, \\ 0 & \text{Otherwise,} \end{cases} \qquad (1)$$

Where P is the desired percentage of cluster heads, r is the current round, and G is the set of nodes that have not been cluster-heads in the last 1/P rounds.

Once a node has self-elected as a cluster-head, it broadcasts an advertisement message to all other nodes using a CSMA MAC protocol. All other cluster-head nodes must transmit their advertisement message with the same transmit power level.

The *set-up phase* starts when non cluster-head nodes receive the advertisement messages of elected cluster-head nodes. Based on the strength of the received signal, a node decides to which cluster (cluster-head) it will be associated with. Then, each cluster-head creates its TDMA schedule based on the number of nodes in its cluster. This schedule is then delivered to all nodes in the cluster.

From this moment, the *steady phase* starts, enabling data transmission until the beginning of the next round. Using the TDMA paradigm, all nodes within a cluster can only communicate with cluster-head and during their pre-allocated slots. The cluster-head then performs data aggregation and sends the composite data directly to the base station via a long-range transmission medium (since the base station is generally far from the cluster-heads). However, note that this action is particularly energy consuming.

Discussion: LEACH shows a good performance in terms of energy efficiency since it implements dynamic clustering, enabling a balanced distribution of power consumption between all nodes in the network, thus extending the overall WSN lifetime. However, the maximum number of nodes within a cluster should be limited, since the TDMA mechanism imposes scalability restrictions. Also, the duration of a clustering round directly affects the energy/latency trade-off. In fact, for longer round durations, the energy of the cluster-head will be quickly consumed. Nevertheless, it is able to support real-time communications thanks to the TDMA protocol. For short re-clustering cycles, the frequent reconfiguration of the network will be very time consuming, especially for large-scale WSNs, since effective data communications (steady phase) will be pending until the complete set-up of the network (advertisement and set-up phases).

S-MAC [Ye02] [Ye04]

The primary purpose of the S-MAC (*Sensor MAC*) protocol ([Ye02], [Ye04]) is to adapt the contention-based CSMA/CA protocol used in the IEEE 802.11 standard to WSNs, by improving the energy efficiency issue. This adaptation consists on reducing the excessive energy consumption of the CSMA protocol in multi-hop WSNs typically due to idle-listening, collisions, overhearing and control overhead (see section 5.2). The energy saving with S-MAC is achieved by:

- Low *operational duty cycle*, varying from 1 to 10%. This means that a WSN node using S-MAC will cyclically alternate between *Listen* and *Sleep* states, where the listen state never exceeds 10% of the cycle duration.
- Going into the sleep state as often as possible, by turning off the radio transceiver during the transmission periods of other nodes to avoid overhearing unwanted packets.

In the S-MAC protocol, all nodes are free to choose their own listen/sleep schedule at the initial phase. A complete Listen/Sleep cycle is called *Frame*. All communication activities (sending and receiving) are limited to the Listen period. In the Sleep period, the node is completely unavailable. The schedule of each node is shared with its neighbours so that they know at which time this node is able to receive data. A basic example of a communication scenario with two nodes – *a* and *b* – is shown in Fig. 10.

This communication paradigm imposes a periodic synchronization between neighbour nodes to prevent jamming. In fact, S-MAC compliant nodes periodically broadcast their Listen/Sleep schedules in a SYNC packet, which provides clock synchronization.

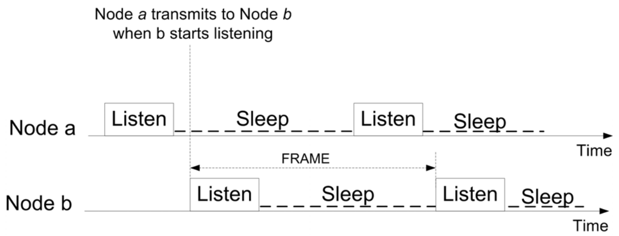


Fig. 10. S-MAC listen/sleep schedule

An interesting way to reduce control overhead in S-MAC is by adopting an identical schedule in all neighbor nodes. Hence, a node joining the network must wait for a synchronization period and adopt the first schedule it receives.

As for the data transmission process, S-MAC is similar to the IEEE 802.11 DCF operation mode. In fact, the transmission of a packet respects the RTS-CTS-DATA-ACK sequence and medium access control is made according to the CSMA/CA protocol. S-MAC puts a duration field in each packet which indicates the time needed for the current transmission. This information helps the neighboring nodes to know the transmission duration so that they keep silent during this period, reducing energy consumption by avoiding overhearing.

Discussion: the advantage of S-MAC is to efficiently mitigate the energy consumption in WSNs and thus extending network lifetime. However, this approach is not suitable for time-sensitive applications. In fact, a node that has data to send must wait until the beginning of its listening period, which increases latency especially for low duty cycles (where the sleeping period is not negligible). Timing performance will drastically degrade particularly in multi-hop large-scale WSNs, where the latency cost will accumulate at each hop in the path. To fix this problem, the authors propose an extension of S-MAC in [Ye04] using *adaptive listening*. With adaptive listening, each node wakes up immediately after the end of a transmission (following RTS-CTS-DATA-ACK) rather than waiting until the beginning of the next frame. This dynamic scheme allows the nodes which have data to send to immediately contend for the channel and other nodes to be ready to receive data. In [Ye04], the authors show that using adaptive listening reduces the latency by at least a half.

Even with this improvement, S-MAC remains limited in providing real-time guarantees, though very efficient in energy conservation. S-MAC fits better the need of applications where energy consumption is the most valuable resource, i.e. that need to extend the network lifetime rather than providing reduced communication delays. Environment monitoring, which involves collecting readings of some physical parameters over time, is one of potential suitable applications for the S-MAC protocol, since in such kind of applications the variation of the physical quantities (e.g. temperature and pressure) is typically slow.

Some other MAC protocols that are similar to S-MAC were also defined, namely B-MAC [Polastre04] and WiSe-MAC [El-Hoiydi04].

DMAC [Luo4]

The DMAC protocol [Lu04] tackles the problem of real-time guarantees in WSNs that utilizes active/sleep duty cycles, such as in the S-MAC protocol. The main problem mentioned by the authors is the data forwarding interruption problem, since some nodes on a multihop path to sink are not notified of data delivery in progress, resulting in significant sleep delay.

As shown in Fig. 11, DMAC is based on a data gathering tree, which must be constructed in an initial phase. Then, DMAC performs synchronized assignments of time slots on different nodes.

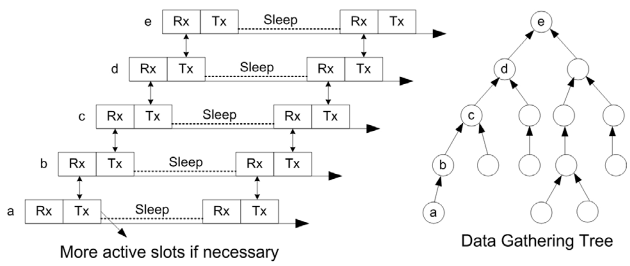


Fig. 11. Data Gathering Tree and DMAC Implementation

Three states are defined: *receive*, *transmit* and *sleep*. When a node is in the *receive* state, all its child nodes are in the *transmit* state and have to contend for the medium. After each data reception, a node can forward data during its *transmit* period to a parent node (which should be ready to receive), while child nodes continue in the *sleep* state. Low latency is achieved by synchronizing *transmit* and *receive* periods of a parent node with its child nodes.

Discussion: DMAC achieves a very good performance in terms of delay reduction compared to other protocols using sleep/active duty cycles. It also removes the control overhead packets like RTS/CTS, thus reducing energy consumption. However, the strong limitation of DMAC is its static data gathering tree which presumes a fixed path from the sources to the sink, which may not be the case in WSNs. Actually, this kind of assumption is not practical in large-scale self-organizing WSNs. Also, DMAC does not implement any collision avoidance scheme, and this would lead to inevitable collisions when a number of child nodes with the same transmission schedule send their data.

DB-MAC [Bacco04]

The DB-MAC (*Delay-Bounded MAC*) protocol [Bacco04] is a distributed MAC protocol designed to reduce the communication latency in time-critical applications, using a dynamic *priority assignment* scheme. It also aims to reduce energy consumption by means of a *path aggregation* mechanism that improves path sharing.

DB-MAC is an extension of the CSMA/CA contention scheme used in the IEEE 802.11 protocol, adapted to the requirements of WSNs in terms of bounded delays and low energy consumption. This extension is based on two concepts:

- *Priority assignment*

  In DB-MAC, a transmission close to the source has higher priority than a transmission close to the sink. This distributed MAC protocol ensures that a node with higher priority gains medium access before a neighbour node with lower priority. At the beginning, each source has the highest priority P_{max}, which is decreased by one from hop to hop towards the destination.

  In the IEEE 802.11, if a node detects an idle channel, it picks a random number called Contention Window (CW) between CW_{min} and CW_{max} and waits for a Backoff Interval (BI) proportional to CW into the range of [0..1023]**tic*. *tic* is defined as the time unit of the MAC protocol and is equal to one time slot defined in IEEE 802.11 (20μs).

  In DB-MAC, the *CW* is divided into P_{max} equal subintervals named *CWp* depend on the priority level *p*. The contention window of priority *x* is defined:

  $$CWp = \left[CW_{\min}(\Pr = p),\ CW_{\max}(\Pr = p)\right]$$

  Hence, a node with a transmission priority *x* picks a random value *RCWp* in the interval *CWp* and calculates its backoff interval BI as:

  $$BI\left(\Pr = p\right) = RCWp * tic$$

  This protocol ensures that

  $$BI\left(\Pr = p\right) > BI\left(\Pr = q\right) \quad \forall p \geq q$$

  This property is very interesting to reduce the latency for winning the medium access for higher priority flows.

- *Path aggregation*

  In DB-MAC, flows are dynamically aggregated in the path toward the sink using a modified version of the RTS/CTS mechanism (Fig. 11).

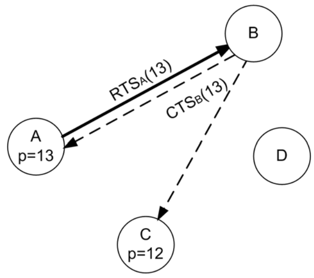


Fig. 11. Path Aggregation in DB-MAC

  In fact, a node (*c*, in Fig. 11) that has data to send and that overhears a CTS packet from an intermediate node (*b*, in Fig. 11) that has just completely received a packet (from *a*), must forward its data to this latter. The intermediate node performs data aggregation either with or without size reduction and forwards the aggregate data towards the sink.

Discussion: the priority-based backoff algorithm of DB-MAC presents an interesting approach to reduce the medium access latency of high priority flows. A drawback of this protocol with regard to WSN requirements is the lack of reduced duty cycles, which turns energy consumption not negligible by overhearing unwanted traffic. This is because the IEEE 802.11 does not take into consideration the balance between Active and Sleep periods. This lack has been fixed in the IEEE 802.15.4 protocol [IEEE 802.15.4] that has been recently proposed for Wireless Private Area Networks and which fits better the requirements of WSNs.

IEEE 802.15.4 [IEEE 802.15.4]

The IEEE 802.15.4 protocol specifies the Medium Access Control (MAC) sub-layer and physical layer for Low-Rate Wireless Private Area Networks (LR-WPAN). Even thought this standard was not specifically developed for WSNs, it is potentially suitable for them, since WSNs can be built up from LR-WPANs. In fact, the IEEE 802.15.4 protocol targets low-data rate, low power consumption, low-cost wireless networking, with typically fits the requirements of WSNs.

The remainder of this section outlines the most relevant characteristics of the IEEE 802.15.4 MAC sublayer. For a more detailed description, refer to [Koubâa05].

The MAC sub-layer of the IEEE 802.15.4 protocol has many common features with the MAC sub-layer of the IEEE 802.11 protocol, such as the use of CSMA/CA (*Carrier Sense Multiple Access / Contention Avoidance*) as a channel access protocol and the support of contention-free and contention-based periods. However, the specification of the IEEE 802.15.4 MAC sub-layer is adapted to the requirements of LR-WPANs as, for instance, eliminating the RTS/CTS mechanism (used in IEEE 802.11) to reduce the probability of collisions, since collisions are more likely to occur in low rate networks and result in wasted energy.

One specific node, the PAN (Personal Area Network) coordinator, plays a special role in the PAN, as described next.

The MAC protocol supports two operational modes that may be selected by the PAN coordinator:

- *Beacon-enabled* mode
  Beacons are periodically generated by the coordinator to synchronize attached devices and to identify the PAN. A beacon frame is (the first) part of a superframe, which also embeds all data frames exchanged between the nodes and the PAN coordinator. Data transmissions between nodes are also allowed during the superframe duration.
- *Non Beacon-enabled* mode
  In non beacon-enabled mode, the devices can simply send their data by using unslotted CSMA/CA. There is no use of a superframe structure in this mode.

Fig. 12 presents a structure of the IEEE 802.15.4 operational modes.

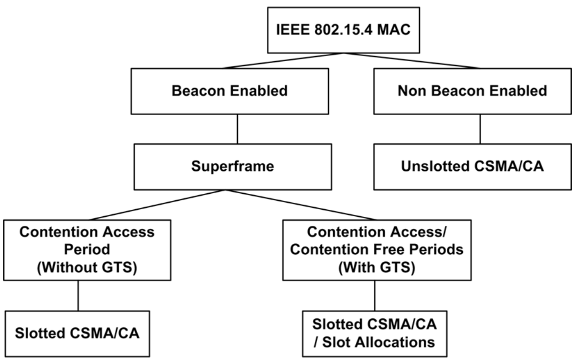


Fig. 12. IEEE 802.15.4 Operational Modes

In the beacon-enabled mode, the *Beacon Interval* (BI) defines the time between two consecutive beacons, and includes an active period and, optionally, an inactive period. The active period, called *superframe*, is divided into 16 equally-sized time-slots, during which transmissions are allowed. During the inactive period (if it exists), nodes may enter in a sleep mode, thus saving energy. Fig. 13 illustrates the beacon interval and superframe structures.

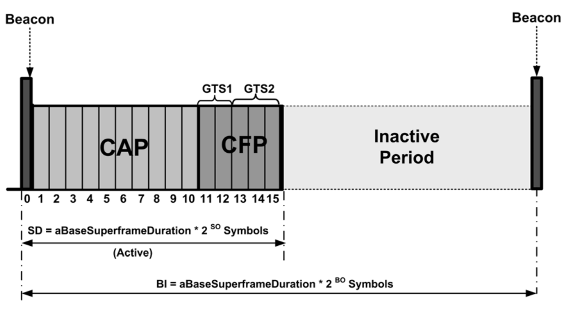


Fig. 13. Beacon Interval and Superframe Concepts

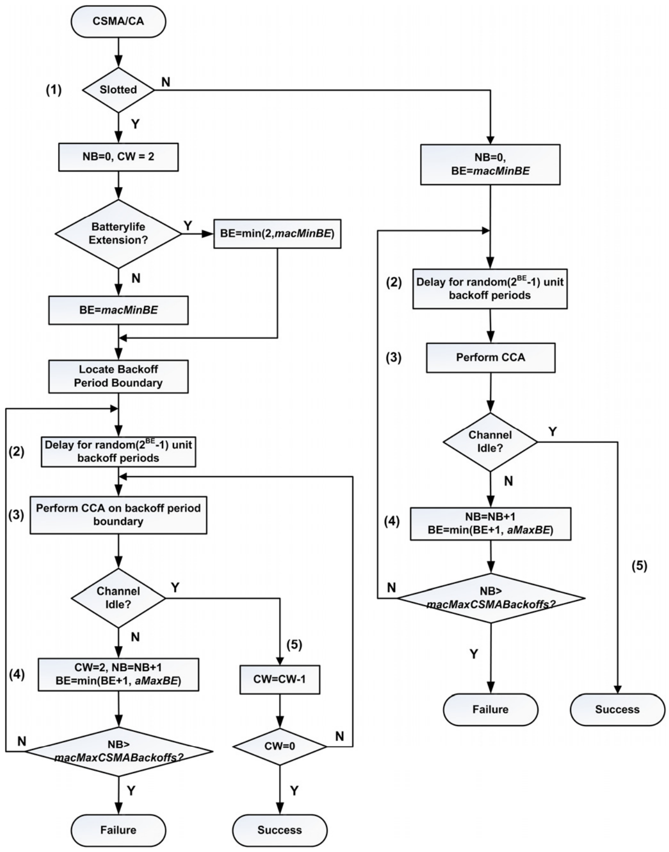


Fig. 14. The CSMA/CA Mechanism

The lengths of the Beacon Interval and the *Superframe Duration* (SD) are determined by two parameters, the *Beacon Order* (BO) and the *Superframe Order* (SO), respectively. The Beacon Interval is defined as follows:

$$BI = aBaseSuperframeDuration * 2^{BO}$$
$$for\ \ 0 \le BO \le 14,$$

The Superframe Duration, which determines the length of the active period, is defined as follows:

$$SD = aBaseSuperframeDuration * 2^{SO}$$
$$for\ \ 0 \le SO \le BO \le 14,$$

During *SD*, the nodes are allowed to send their frames at the beginning of each time-slot. By default, the nodes compete to access to the medium using slotted CSMA/CA during the Contention Access Period (CAP) (see Fig. 14). In case the channel is busy, a node computes its backoff period based on a random number of time-slots. The IEEE 802.15.4 protocol also offers the possibility of having a Contention-Free Period (CFP) within the superframe. The CFP, being optional, is activated upon a request sent by a node to the PAN coordinator for allocating time-slots depending on the node's requirements. Hence, upon receiving the request, the PAN coordinator checks whether there are sufficient resources and, if possible, allocates the requested time-slots. These time-slots are called *Guaranteed Time-Slots* (GTSs) and constitute the CFP. If the available resources are not sufficient the GTS request fails. The corresponding node then continues to send its data frames during the CAP.

A detailed description of GTS management and of the slotted CSMA/CA mechanism is presented in [Koubâa05].

When the PAN coordinator selects the non-beacon enabled mode, there are neither beacons nor superframes. Medium access control is provided by an unslotted CSMA/CA mechanism (see Fig14).

6. General Aspects on the Network Layer

One of the most important roles of the Network Layer is taking routing decisions to relay sensory data, hop-by-hop, from their sources to the control station. However, routing is a very challenging problem in WSNs due to their inherent features that make them different from classical wireless networks like MANET or cellular networks. For instance, using a large number of sensor nodes scattered in the monitored region, it is not possible to use a logical address-based routing because it is very heavy to maintain the logical ID of individual nodes in a large scale topology. Therefore, traditional IP-based protocols cannot be applied to WSNs.

Position awareness is another important issue for the network layer in WSNs, since applications are typically interested in a certain phenomenon that occurs in a given area of the monitored environment. Hence, it is mandatory to have a locating system such as Global Positioning System (GPS). However, for practical considerations including hardware size, form factor, cost and power constraints it is not feasible to have a GPS system in all nodes for a large-scale network [Bulusu00]. This triggers the need of new localization approaches dedicated for WSNs that respect their inherent constraints.

On the other hand, WSN nodes are tightly constrained in terms of energy, CPU speed and storage capacity, thus the network layer must not introduce excessive processing overheads.

Another characteristic of WSNs is *data redundancy*, since sensory data is typically related to common phenomena. Thus, there is a high probability that the same data value is captured from different sources and routed through the network. Data redundancy should be exploited by the routing protocol to reduce energy consumption and increase bandwidth utilization. This may be accomplished using data aggregation by intermediate hops. For example, if two or more sensor report the same temperature measurement for near locations, then an intermediate node that receive these measures could send an aggregated data packet instead of forwarding individual data separately, resulting in energy and bandwidth resources savings.

Finally, WSNs are data-centric, which means that data is requested based on a certain attribute, not specifically from a certain node. This paradigm is opposite to the address-centric paradigm used in classical address-based networks. For example, in environmental monitoring applications, if the control station sends a query such that [*Temperature* ≥ 40ºC], then only the nodes detecting this event need to report their readings.

7. Final Remarks

In this technical report, we have presented a survey on communication protocols for wireless sensor networks (WSNs) with a particular emphasis on the lower layers. We have also briefly described some proposed MAC protocols for WSNs and discussed their advantages and limitations.

From this survey, it is noticed that there is no universal protocol solution for WSNs. In fact, the sensor network applications might have different requirements. For instance, an environment monitoring application (pressure, temperature,…) is more sensitive to energy consumption and aims to extend network lifetime. No real-time guarantees are imposed in such an application. On the other hand, in emergency medical response applications there is an interest on assuring reliable and real-time communications in emergency situations, which imposes different communication paradigms.

However, the IEEE 802.15.4 protocol seems to be adequate to a large variety of sensor network applications with different requirements. IEEE 802.15.4 presents a flexible solution by adequately adjusting its parameters to fit the requirements of a given application. For instance, the beacon order and the superframe order can be dynamically adjusted differently either to reduce energy consumption (lower duty cycles) or to reduce communication latencies (higher duty cycles) depending on the need of the application. A key challenge is to determine the best setting of IEEE 802.15.4 parameters for a given application.

References

[Akyildiz02] I.F. Akyildiz et al., "Wireless Sensor Networks: A Survey", *Journal of Computer Networks*, 38 (2002), 393-422.

[ASH02] "ASH Transceiver Designer's Guide" http://www.rfm.com , May 2002.

[Bacco04] G. D. Bacco et al., " A MAC Protocol for Delay-Bounded Applications in Wireless Sensor Networks", in Proc. *Third Annual Mediterranean Ad Hoc Networking Workshop, June 27-30, 2004*

[Baker82] D. J. Baker and J. Wieselthier, "A distributed algorithm for scheduling the activation of links in a self-organizing, mobile, radio network," in *Proc. Int. Conf. Commun.*, 1982, pp. 2F.6.1–2F.6.5.

[Baker84] [10] D. J. Baker,A. Ephremides, and J. Flynn, "The design and simulation of a mobile radio network with distributed control," *IEEE Trans. Select. Areas Commun.*, vol. SAC-2, pp. 226–237, Jan. 1984.

[Bandyopadh03] S. Bandyopadhyay and E.J. Coyle. "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks", *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. Volume: 3* , 30 March - 3 April 2003

[Bharghavan94] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless LANs," in *Proc. ACM SIGCOMM Conf.*, vol. 24, Aug. 1994, pp. 212–225.

[Bulusu00] N. Bulusu, J. Heidemann, D. Estrin,\GPS-less low cost outdoor localization for very small devices", IEEE Personal Communications, vol. 7, no. 5, October 2000 pp. 28-34.

[Dasgupta03] K. Dasgupta, K. Kalpakis, and P. Namjoshi. An Efficient Clustering-based Heuristic for Data Gathering and Aggregation in Sensor Networks. *Wireless Communications and Networking (WCNC 2003). IEEE , Volume: 3* , 16-20 March 2003.

[El-Hoiydi04] A. El-Hoiydi and J.-D. Decotignie, "WiseMAC: An Ultra Low Power MAC Protocol for Multi-hop Wireless Sensor Networks," in *Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS) 2004*, July 2004.

[Elson01] J. Elson and D. Estrin. Time Synchronization for Wireless Sensor Networks., *Proceedings 15th International Symposium Parallel and Distributed Processing*, 23-27 April 2001.

[Fullmer97] C. L. Fullmer and J. J. Garcia-Luna-Aveces, "Solutions to hidden terminal problems in wireless networks," in *Proc. ACM SIGCOMM Conf.*, 1997, pp. 39–49.

[Ganeriwal03] S. Ganeriwal, R. Kumar, and M.B. Srivastava. Timing-Sync Protocol for Sensor Networks. *SenSys'03*, Los Angeles, California, USA. November 5-7, 2003.

[He03] T. He et al., "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks", International Conference on Distributed Computing Systems ICDCS 2003, pp. 46-55.

[Heinzelman00] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," in Proc. of the Hawaii International Conference on Systems Sciences, Jan. 2000.

[Heizelman99] W. Heizelman, J. Hill, and H. Balakrishnan. "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks". In Proc. of the Fifth Annal ACM/IEEE International Conference on Mobile Computing and Networking (*MobiCom '99)*, Seattle, WA, USA, August 1999.

[Hill00] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for network sensors," in Proc. Int. Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), Cambridge, MA, Nov. 2000.

[IEEE 802.15.4] IEEE 802.15.4 Standard-2003, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE-SA Standards Board, 2003. website: http://grouper.ieee.org/groups/802/15/pub/TG4b.html

[Intanagonw00] C. Intanagonwiwat, R. Govindan, and D. Estrin. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. In Proc. of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networks (MobiCom 2000), Boston, Massachusetts, August 2000.

[Karn90] P. Karn, "MACA—A new channel access method for packet radio," presented at the ARRL/CRRL Amateur Radio 9th Computer Networking Conf., 1990.

[Karp00] B. Karp and H. T. Kung. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. In IEEE MobiCom, August 2000.

[Kasten] Oliver Kasten, Energy Consumption, http://www.inf.ethz.ch/~kasten/research/bathtub/energy_consumption.html ,Eldgenossische Technische Hochschule Zurich.

[Kim03] S. Kim, et al. "SAFE: A Data Dissemination Protocol for Periodic Updates in Sensor Networks", 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03)

[Kleinrock75] L. Kleinrock and Fouad Tobagi, "Packet switching in radio channels: Part I - carrier sense multiple access modes and their throughput delay characteristics," IEEE Transactions on Comm., Vol. 23, N. 12, pp. 1400–1416, Dec. 1975.

[Koubâa05] A. Koubâa , M. Alves, E. Tovar, "IEEE 802.15.4 for Wireless Sensor Networks: A Technical Overview" IPP-HURRAY Technical Report, HURRAY-TR-050702, July 2005.

[Lin99] C. R. Lin and M. Gerla, "Real-time support in multihop wireless networks," *ACM/Baltzer Wireless Networks*, vol. 5, no. 2, pp. 125–135, 1999.

[Lu04] G. Lu, B. Krishnamachari, C.S. Raghavendra, "An adaptive energy efficient and low-latency MAC for data gathering in wireless sensor networks", *Proceedings of 18th International Parallel and Distributed Processing Symposium*, Pages: 224, 26-30 April 2004.

[Malan04] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care", International Workshop on Wearable and Implantable Body Sensor Networks, April 2004

[McCune00] E. McCune, "DSSS vs. FHSS narrowband interference performance issues", RF Signal Processing Magazine, Sept. 2000.

[Perkins99] C. E. Perkins, E. M. Royer, "Ad-hoc On Demand Distance Vector Routing", In WMCSA'99, February 1999.

[Polastre04] J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," in *ACM SenSys 2004*, November 2004.

[Porret00] A. Porret, T. Melly, C.C. Enz, E.A. Vittoz, "A low-power low-voltage transceiver architecture suitable for wireless distributed sensors network," IEEE International Symposium on Circuits and Systems'00, Geneva, Vol. 1, 2000, pp. 56–59.

[Savvides01] A. Savvides, C.C. Han, and M.B. Srivastava. Dynamic Fine Grained Localization in Ad-Hoc Sensor Networks. *Proceedings of the Fifth International Conference on Mobile Computing and Networking, Mobicom 2001, pp. 166-179*, Rome, Italy, July 2001

[Schurgers02] C. Schurgers et al., "Optimizing Sensor Networks in the

Energy-Latency-Density Design Space", IEEE Transactions on Mobile Computing, Vol. 1, No. 1, January-March 2002.

[Stankovic03] J. A. Stankovic et al., "Real-Time Communication and Coordination in Embedded Sensor Networks", Proceedings of IEEE

[Stevens90] D. S. Stevens and M. H. Ammar, "Evaluation of slot allocation strategies for TDMA protocols in packet radio networks," in *Proc. IEEE MILCOM Conf.*, 1990, pp. 835–839.

[Stojmenovic99] I. Stojmenovic and X. Lin. GEDIR: Loop-Free Location Based Routing in Wireless Networks, IASTED Int. Conf. on Parallel and Distributed Computing and Systems, November 3-6, 1999

[Tobagi75] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part II—The hidden terminal problem in carrier sense multiple access and the busy tone solution," IEEE Trans. Commun., Vol. COS-23, pp. 1417–1433, Dec. 1975.

[xbow] http://www.xbow.com/

[Ye02] Wei Ye, John Heidemann, and Deborah Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor networks," in *Proceedings of the IEEE Infocom*, New York, NY, June 2002, pp. 1567–1576.

[Ye03] W. Ye, J. Heidemann, "Medium Access Control in Wireless Sensor Networks", USC/ISI Technical Report ISI-TR-580, October 2003.

[Ye04] Wei Ye, John Heidemann, and Deborah Estrin, "Medium access control with coordinated, adaptive sleeping for wireless sensor networks," IEEE/ACM Transactions on Networking, April, 2004.

[ZigBee] ZigBee Alliance, "ZigBee Specification", Document 053474r05, Version 1.0, 14th of December 2004. Available (since June 2005) at: http://www.zigbee.org/