Universidade do Minho
Escola de Engenharia

Óscar Sílvio Marques de Almeida Gama

A MAC Protocol for Quality of Service Provisioning in Adaptive Biomedical Wireless Sensor Networks

September 2011

A MAC Protocol for Quality of Service Provisioning in Adaptive Biomedical Wireless Sensor Networks

Óscar Sílvio Marques de Almeida Gama

UMinho | 2011

Universidade do Minho
Escola de Engenharia

Óscar Sílvio Marques de Almeida Gama

A MAC Protocol for Quality of Service Provisioning in Adaptive Biomedical Wireless Sensor Networks

Doctorate Program on Electronics and Computer Engineering

PhD Thesis developed under the scientific supervision of:
Professor Paulo Mateus Mendes
and
Professor Paulo Manuel Martins de Carvalho

September 2011

Acknowledgement

I would like to thank my supervisors, Professor Paulo Mendes and Professor Paulo Carvalho, for the help and guidance given throughout the work, essential for the accomplishment of this thesis.

My gratefulness also goes to “FCT - Fundação para a Ciência e a Tecnologia” for funding this research work along four years.

Abstract

New healthcare solutions are being explored to improve the quality of care and the quality of life of patients, as well as the sustainability and efficiency of the healthcare services. In this context, wireless sensor networks (WSNs) constitute a key technology for closing the loop between patients and healthcare providers, as WSNs provide sensing ability, as well as mobility and portability, essential characteristics for wide acceptance of wireless healthcare technology.

Despite the recent advances in the field, the wide adoption of healthcare WSNs is still conditioned by quality of service (QoS) issues, namely at the medium access control (MAC) level. MAC protocols currently available for WSNs are not able to provide the required QoS to healthcare applications in scenarios of medical emergency or intensive medical care. To cover this shortage, the present work introduces a MAC protocol with novel concepts to assure the required QoS regarding the data transmission robustness, packet delivery deadline, bandwidth efficiency, and energy preservation. The proposed MAC protocol provides a new and efficient dynamic reconfiguration mechanism, so that relevant operational parameters may be redefined dynamically in accordance with the patients' clinical state. The protocol also provides a channel switching mechanism and the capacity of forwarding frames in two-tier network structures.

To test the performance of the proposed MAC protocol and compare it with other MAC protocols, a simulation platform was implemented. In order to validate the simulation results, a physical testbed was implemented to replicate the tests and verify the results. Sensor nodes were specifically designed and assembled to implement this physical testbed.

Preliminary tests using the simulation and physical platforms showed that simulation results diverge significantly from reality, if the performance of the WSN software components is not considered. Therefore, a parametric model was developed to reflect the impact of this aspect on a physical WSN. Simulation tests using the parametric model revealed that the results match satisfactorily those obtained in reality.

After validating the simulation platform, comparative tests against IEEE 802.15.4, a prominent standard used in many wireless healthcare systems, showed that the proposed MAC protocol leads to a performance increase regarding diverse QoS metrics, such as packet loss and bandwidth efficiency, as well as scalability, adaptability, and power consumption. In this way, AR-MAC is a valuable contribution to the deployment of wireless e-health technology and related applications.

Keywords: wireless sensor network, e-health, medium access control, quality of service, network reconfiguration, modeling, validation.

Resumo

Novas soluções de cuidados de saúde estão a ser exploradas para melhorar a qualidade de tratamento e a qualidade de vida dos pacientes, assim como a sustentabilidade e eficiência dos serviços de cuidado de saúde. Neste contexto, as redes de sensores sem fios (*wireless sensor networks* - WSN) são uma tecnologia chave para fecharem o ciclo entre os pacientes e os prestadores de cuidados de saúde, uma vez que as WSNs proporcionam não só capacidade sensorial mas também mobilidade e portabilidade, caracteristicas essenciais para a aceitação à larga escala da tecnologia dos cuidados de saúde sem fios.

Apesar dos avanços recentes na área, a aceitação genérica das WSNs de cuidados de saúde ainda está condicionada por aspectos relacionados com a qualidade de serviço (*quality of service* - QoS), nomeadamente ao nível do controlo de acesso ao meio (*medium access control* - MAC). Os protocolos MAC actualmente disponíveis para WSNs são incapazes de fornecer a QoS desejada pelas aplicações médicas em cenários de emergência ou cuidados médicos intensivos. Para suprimir esta carência, o presente trabalho apresenta um protocolo MAC com novos conceitos a fim de assegurar a QoS respeitante à robustez de transmissão de dados, ao limite temporal da entrega de pacotes, à utilização da largura de banda e à preservação da energia eléctrica. O protocolo MAC proposto dispõe de um novo e eficiente mecanismo de reconfiguração para que os parâmetros operacionais relevantes possam ser redefinidos dinamicamente de acordo com o estado de saúde do paciente. O protocolo também oferece um mecanismo autónomo de comutação de canal, bem como a capacidade de encaminhar pacotes em redes de duas camadas.

Para testar o desempenho do protocolo MAC proposto e compará-lo com outros protocolos MAC foi implementada uma plataforma de simulação. A fim de validar os resultados da simulação foi também implementada uma plataforma física para permitir replicar os testes e verificar os resultados. Esta plataforma física inclui nós sensoriais concebidos e construídos de raiz para o efeito.

Testes preliminares usando as plataformas de simulação e física mostraram que os resultados de simulação divergem significativamente da realidade, caso o desempenho dos componentes do *software* presentes nos componentes da WSN não seja considerado. Por conseguinte, desenvolveu-se um modelo paramétrico para reflectir o impacto deste aspecto numa WSN real. Testes de simulação efectuados com o modelo paramétrico apresentaram resultados muito satisfatórios quando comparados com os obtidos na realidade.

Uma vez validada a plataforma de simulação, efectuaram-se testes comparativos com a norma IEEE 802.15.4, proeminentemente usada em projectos académicos de cuidados de saúde sem fios. Os resultados mostraram que o protocolo MAC conduz a um desempenho superior no tocante a diversas métricas QoS, tais como perdas de pacotes e utilização de largura de banda, bem como no respeitante à escalabilidade, adaptabilidade e consumo de energia eléctrica. Assim sendo, o protocolo MAC proposto representa um valioso contributo para a concretização efectiva dos cuidados de saúde sem fios e suas aplicações.

Palavras-chave: rede de sensores sem fios, cuidados de saude electrónicos, controlo de acesso ao meio, qualidade de serviço, reconfiguração da rede, modelação, validação.

Contents

List of Figures

List of Tables

Acronyms and Abbreviations

ABN	Array Beacon Number
ACK	Acknowledgement
AES	Advanced Encryption Standard
AR1c	AR-MAC in one-color mode
AR2c	AR-MAC in two-color mode
AR-MAC	Adaptive and Robust MAC
ARQ	Automatic Repeat Request
ART	Arterial Rate
b	bit
B	Byte
BAN	Body Area Network
BC	Beacon Color
BER	Bit Error Ratio
BI	Beacon Interval
BN	Beacon Number
BO	Beacon Order
BP	Beacon Period
BPSK	Binary Phase-shift Keying
BR	Beacon Received
BS	Base Station
BSN	Body Sensor Network
CAP	Contention Access Period / Phase (IEEE 802.15.6)
CCA	Clear Channel Assessment
CDMA	Code Division Multiple Access
CFP	Contention Free Period
CICADA	Cascading Information retrieval by Controlling Access with Distributed slot Assignment
CO_2	Carbon Dioxide
COOJA	Contiki Operating System Java
CPU	Central Processing Unit
CR	Configuration Received
CR-SLF	Channel Reuse - Smallest Latest Transmission Start Time First
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear-To-Send
DER	Delivery Error Ratio
DPR	Duplicate Packet Ratio
DSSS	Direct Sequence Spread Spectrum
EAP	Exclusive access Phase
ECG	Electrocardiography, Electrocardiogram
EEG	Electroencephalography, Electroencephalogram
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMG	Electromyography, Electromyogram
ERP	Extra Retransmission Period
FCS	Frame Check Sequence
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction

FH	Frequency Hopping
FTP	File Transfer Protocol
GinMAC	Ginseng MAC
GTS	Guaranteed Time-Slot
HR	Heart Rate
ICU	Intensive Care Unit
I-EDF	Implicit prioritized-Earliest Deadline First
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	Inter-Frame Space
INF	Infinite
ISM	Industrial, Scientific, and Medical
ITU	International Telecommunications Union
ITU-T	ITU - Telecommunication Standardization Sector
J-Sim	Java Simulator
LMAC	Lightweight MAC
LPRT	Low Power Real Time
LPU	Local Processing Unit
MAC	Medium Access Protocol
MAP	Managed Access Phase
MCU	Micro-Controller Unit
MiXiM	Mixed Simulator
MPPS	Maximum Physical Packet Size
NAP	Non-Active Period
NRP	Normal Retransmission Period
NRPU	NRP Usage
NS	Network Simulator
NTP	Normal Transmission Period
OMNeT	Objective Modular Network Testbed
OPNET	Optimized Network Engineering Tools
O-QPSK	Offset Quadrature Phase-shift Keying
OXI	Oximetry, Oximeter
PAN	Personal Area Network
PC	Personal Computer
PCB	Printed Circuit Board
PDA	Personal Digital Assistant
PEDAMACS	Power Efficient and Delay Aware MAC for Sensor Networks
PR-MAC	Priority Reservation MAC
PRR	Packet Reception Ratio
PSIFT	Prioritized Sift
QoMOR	QoS-aware MAC protocol using Optimal Retransmission
QoS	Quality of Service
RAM	Random Access Memory
RAP	Random Access Phase
RF	Radio-Frequency
RiP	Reconfiguration in Progress
RL-MAC	Reinforcement Learning based MAC
RP	Retransmission Period
RR	Respiratory Rate
RRMAC	Real time and Reliable MAC
RTS	Request-to-Send
SASW-CR	Slotted Aloha with Sliding Window & Cooperative Retransmissions
SC	Superframe Color
SD	Superframe Duration
SDMA	Spatial Division Multiple Access

SensorSim	Sensor Simulator
S-MAC	Sensor MAC
SNR	Signal-to-Noise Ratio
SPI	Serial Peripheral Interface
SpO_2	Saturation of Peripheral Oxygen
SRAM	Static Random Access Memory
SWAN	Simulator for Wireless Ad-Hoc Networks
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TEMP	Body Temperature
T-MAC	Timeout MAC
TOSSIM	TinyOS Simulator
TSMP	Time Synchronized Mesh Protocol
TtC	Time to Change
TTL	Transistor - Transistor Logic
USB	Universal Serial Bus
UWB	Ultra Wideband
VTS	Virtual TDMA for Sensors
WBSN	Wireless Body Sensor Network
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network
Z-MAC	Zebra-MAC

Latin terms

c. (*circa*)	means “around”
cf. (*confer*)	means “compare” or “consult”.
e.g. (*exempli gratia*)	means “for example”.
etc. (*et cetera*)	means “and the rest”.
i.e. (*id est*)	means “that is”.

Chapter 1

Introduction

1.1 Context

The wireless sensor network (WSN) concept appeared in the nineties of the last century as a utopia. According to this vision, a dense, homogeneous, and autonomous wireless network composed of low cost and very tiny devices cooperate mutually for a common goal. These devices with very constrained hardware and computing resources are provided with sensing capabilities and are energetically independent through energy scavenging. The unstructured network starts up autonomously without human participation. It is scalable, tolerant to nodes' failures and able to self-reorganize in case of faults. These networks, usually referred as conventional WSNs, were conceived for monitoring or tracking applications, such as environmental surveillance in forests.

Although still distant of that envisioned WSN scenario, recent advances in wireless communications, electronics and networking technologies, as well as in embedded computing systems have contributed for deploying WSNs in diverse monitoring application fields, such as industrial control, buildings, civil structures, and medical care [Yick08]. These WSNs are composed of small sensor nodes equipped with one or more physical sensors, data acquisition circuits, processor, memory, radio transceiver, and a low-capacity battery. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors is available to measure the parameters required by the application. Sensor nodes may be placed at specific locations, forming structured WSNs.

One important characteristic of WSNs is that they are dependent on the type of application. Normally, a WSN developed for a specific application can hardly be deployed directly in a different type of application, because the monitored physical signals, the network properties and the traffic characteristics are usually distinct, as described in [Arampatzis05]. So, a WSN protocol presenting a good performance in a certain application field may be inadequate in another application context. For this reason, the application field must be specified when developing protocols and mechanisms for a WSN. From a wide range of potential WSN application scenarios, the healthcare application field will be considered along this work due to its overwhelming importance to society and patients in particular. More specifically, the work will focus on the key aspect of collecting continuously physiological signals of patients and forward wirelessly the data to a remote monitoring system for subsequent analysis. Special emphasis will be paid to intensive medical care services, because they require

real-time monitoring capability to allow fast medical response in case of clinical emergency [Astaras08].

E-health is a term often employed vaguely to characterize not only the healthcare delivered over the Internet, but also practically everything related to computers and medicine. In order to determine the contexts in which the term has been used, definitions of e-health were systematically searched in dictionaries and scientific literature from electronic databases [Oh05]. Upon collection, the authors identified fifty one (!) unique definitions. For example, e-health is defined as "the use of information and communication technology to enhance health care" or "an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology" [Eysenbach01]. Although the latter is the most commonly cited e-health definition on the Internet [Oh05], this work assumes the former, because it is a concise and clear definition that expresses well the role of WSNs in healthcare services.

E-emergency is other term related with healthcare and is defined as "emergency healthcare systems and services" [Pattichis06]. In the ambit of this work, e-emergency is defined as "emergency or intensive medical healthcare systems and services", because both clinical situations present similarities from the perspective of networking requisites, such as real-timeliness, data delivery robustness, and fault-tolerance.

Wireless e-health is an emerging technology used in healthcare support and it may be the natural evolution of traditional e-health systems used in hospitals consisting mostly of legacy wired equipments, which prevents patients to move around freely. This evolution expectedly will have a deep impact on some of the existing healthcare services and will reshape the workflow and practices in the delivery of these services. Novel healthcare paradigms will come up to provide personalized care in diverse fields, such as stroke rehabilitation, cognitive diseases, emergency, and intensive care. The new envisaged solutions will contribute to improve the quality of care of patients by permitting pervasive and continuous monitoring, This idea is supported by real

healthcare studies on the field, such as the one described in [Kyriacou03] and those referred in [Ko10]. Since WSNs provide sensing and mobility facilities, they constitute a key technology for closing the loop between patients and healthcare providers. The abilities provided by e-health WSNs goes into direction of the properties expected in future medical applications - integration with existing medical practice and technology, real-time and long-term monitoring, wearable sensors, and assistance to chronic patients, elders or handicapped people [Virone06].

E-health WSNs are composed of one or more body sensor networks (BSNs). A BSN consists of a group of small biomedical sensor nodes placed on the body of a patient to monitor diverse physiological signals and actions, such as health status and mobility. BSNs enable unobtrusive and comfortable monitoring of patients, and so they are essential to build e-health systems to assist clinicians in monitoring or delivering care remotely without sacrificing the patient's quality of life.

E-health WSNs exhibit particular characteristics and constraints, especially when operating in emergency or intensive care scenarios.

In e-health WSNs, sensor nodes may deliver continuously regular traffic without significant temporal variability to a sink. As physiological signals are sampled at different frequencies, traffic is transmitted at diverse rates, originating heterogeneous traffic flows within the WSN.

Depending on the monitoring signals, timeliness can be an important property to satisfy. Indeed, while some physiological signals (e.g., body temperature) can be monitored with a relatively long time period and loose timeliness constraints, other data such as electrocardiography (ECG), electroencephalography (EEG), and electromyography (EMG) must be monitored continuously and timely. For example, according to IEEE 1073, ECG traffic should have a maximum latency of five hundred milliseconds.

Energy[1] conservation is consensually relevant to allow WSNs to operate autonomously for long time periods, resulting in low battery maintenance. Direct data transmission from sensor nodes to a base station (BS) may not be feasible nor energy efficient in e-health WSNs [Latré07], because of high path loss around the human body and transmission energy cost. So, it is desirable that an e-health WSN can operate in a

[1] The terms energy and power used along this thesis refer to the electrical energy and electrical power.

two-tier network structure. IEEE 802.15.6 confirms this idea, since it will provide an optional two-hop star network extension [Batra11]. Network scalability also benefits from two-tier structure, because data can be delivered to the BS as an aggregate, resulting in bandwidth saving.

Mobility and portability are important features in e-health WSNs to improve patients' quality of life. Mobility requires multi-hop WSNs with location tracking. However, mobility may lose relevance if the patients being monitored lay in static beds, for instance, in intensive care units. Portability demands compact biosensors, as well as unobtrusive and comfortable wearable devices. Additionally, e-health systems should be user-friendly to be used easily by both patients and caregivers.

Security is also an important requirement since physiological signals of patients are confidential and must be accessed only by authorized personnel.

In addition to the described e-health WSN requisites, e-emergency WSNs should be able to adapt dynamically to satisfy specific performance requirements. For instance, increasing monitoring activity and data delivery guarantee might be required when the clinical condition of a patient changes from normal to emergency state. In the inverse situation, the monitoring activity and data delivery guarantee might be decreased to save energy and free network resources. Thus, e-emergency WSNs should comprise autonomous reconfiguration mechanisms to allow a fast adaptive response to new monitoring scenarios. In this context, an e-emergency WSN may benefit from being centralized, as a central coordinator with a global awareness of the network status eases the reconfiguration process.

E-emergency WSNs should assure controlled delays to provide real-time healthcare services. Guaranteed bandwidth and high reliability should also be assured. Bandwidth should be used efficiently to increase scalability and to assure the delivery of all physiological samples. Reliable data delivery is needed because lost packets can cause data misinterpretation or missing alert events. Robustness against interferences and fairness among BSNs of patients with identical clinical conditions are also relevant properties to pursue. Since multiple patients may be present in an emergency or intensive care unit, an e-emergency WSN should also have coexistence capacity, i.e., it should support the coexistence of close-neighbor wireless BSNs operating in the same channel.

In summary, timeliness and robustness of data delivery, energy and bandwidth preservation, adaptability, fairness, scalability, coexistence capacity, and two-tier operability are relevant properties in e-emergency WSNs. To assure these properties, quality of service (QoS) techniques must be deployed in such networks. QoS refers to the ability of a healthcare system to guarantee a certain level of performance in accordance with the patient´s clinical condition, through the deployment of resource reservation mechanisms in the medical care network.

1.2 Motivation and Objectives

Although collective effort of all communication protocol stack entities is essential for QoS provisioning, medium access control (MAC) layer possesses a particular importance among them since it rules the sharing of the medium and all other upper layer protocols are bound to that. QoS support in the network or transport layers cannot be fully provided without the assumption of a MAC protocol which solves the problems of medium sharing and supports reliable link communications. Moreover, communications between entities within a BSN are commonly single-hop, thus not requiring the network layer implementation. Therefore, the present work is focused on QoS provisioning at MAC layer within e-health WSN context.

Many MAC protocols available for WSNs use contention or reservation-based techniques. Contention–based protocols work well under low traffic loads, but they degrade drastically under higher loads because of collisions and retransmissions, as analytical studies [Liang07] and simulation tests [Chevrollier05] in e-health scenarios have shown. Reservation-based MAC protocols are preferable for networks requiring significant traffic loads and low latency, because QoS is more easily assured in a collision-free environment. For this reason, most MAC protocols with real-time requirements use reservation rather than contention techniques, as can be confirmed through the survey of real-time MAC protocols presented in [Teng10]. IEEE 802.15.6 also adopts a reservation technique for priority traffic communications [Batra11]. In reservation-based MAC protocols, time is divided into time-frames, also known as superframes. These are divided into time-slots, which are used by sensor nodes to transmit data without the need to contend for the medium.

Diverse reservation-based MAC protocols have been proposed for WSNs with deterministic and/or real-time requisites, namely VTS [Egea-López08], LMAC [Hoesel04], PEDAMACS [Ergen06], I-EDF [Caccamo02], Dual-mode MAC [Watteyne06], CR-SLF [Li05], RRMAC [Kim08], LPRT [Afonso06], CICADA [Latré07], GinMAC [Suriyachai10], TSMP [Pister08], Bluetooth, IEEE 802.15.4 with guaranteed time-slots (GTSs) [IEEE4]. However, as it will be discussed in Chapter 3, none of these protocols has the ability of providing integrally the characteristics for e-emergency applications identified in the last section, namely adaptability, robustness, bandwidth efficiency, energy preservation, coexistence capacity, and two-tier operability. For example, let us consider TSMP and GinMAC. TSMP was adopted for the WirelessHART standard [WHART07] in industrial automation. However, it lacks dynamic reconfiguration capacity and has poor bandwidth efficiency, because time-slots are fixed and long enough (typically 10 ms) to allow a sender transmit the maximum length packet and receive the respective acknowledgement. GinMAC is the MAC protocol used in the Ginseng project [Ginseng08] and it was developed for applications requiring controlled packet delivery delay and high reliability. However, it is conceived for WSNs with very small size packets and maximum sampling frequencies of one Hertz. So, both protocols are not fully appropriate for e-emergency WSNs. Identical analysis on the remaining MAC protocols drives to the same conclusion. In fact, a novel MAC protocol is required to assure all the mentioned relevant properties for e-emergency applications[2]. This issue is the principal motivation of the present work.

To pursue the identified research goal, an experimental e-emergency scenario was implemented in a simulation platform and sensor nodes were designed and assembled to build a physical testbed.

1.3 Contributions

The main research contribution of the present work is the conception, implementation and testing of a novel MAC protocol that assures the QoS regarding the data

[2] IEEE 802.15.6 standard is being developed specifically for BSNs and it may expectedly assure most of the identified e-emergency requisites. The author became aware of its definitive features in the final period of his work.

transmission robustness and the packet delivery deadline, with energy efficiency, bandwidth efficiency, and presenting the capacity of reconfiguring dynamically the network in accordance with the patients' health state, along with the capacity of forwarding frames in two-tier network structures. Since the proposed MAC protocol has the ability of switching automatically the communication channel in case of intolerable level of interfering traffic, it is prepared to operate in unlicensed bands, such as 2.4 GHz industrial, scientific, and medical (ISM) band. The proposed MAC protocol is intended for non-dense WSNs presenting regular and heterogeneous traffic, such as e-emergency WSNs, which makes it a valuable contribution to the deployment of wireless e-health technology and related applications. To the best of author's knowledge, no MAC protocol with these characteristics has been advocated in the scientific literature. In order to accomplish the required goals, the proposed MAC protocol uses diverse solutions, as it will be discussed in Chapter 4. Next, it is presented briefly the innovative solutions used by the proposed MAC protocol to achieve the e-emergency WSN requisites.

Adaptability is achieved through a novel dynamic reconfiguration scheme, capable of reconfiguring the WSN when a context change occurs.

To provide communication robustness, an array of short-size beacons is sent at the start of each superframe to reduce the beacon loss probability. An innovative strategy based on colors attributed to superframes and sensor nodes contributes to enhance robustness, by reducing the number of transmissions and releasing bandwidth for eventual retransmissions. To improve data delivery robustness, failed (re)transmissions are (re)send in a specific retransmission periods. An original channel switching mechanism is also proposed to improve the data delivery robustness against external wireless interferences.

Power efficiency is achieved using strategies based on colors and short-size beacons. To shorten the beacon size, the time-slot assignment is carried out using a new distributed slot allocation algorithm.

The proposed MAC protocol also has the capacity of forwarding frames in two-tier network structures, using an original forwarding scheme.

Preliminary comparative tests carried out on a validated simulated e-health scenario revealed a notorious data delivery robustness presented by the proposed MAC protocol. While IEEE 802.15.4, in beacon and non-beacon mode, showed packet delivery performances too unacceptable for e-emergency services, the proposed MAC protocol

presented a null packet delivery ratio in the same test conditions. This excellent performance was achieved without aggravating the power consumption significantly.

The research contributions of the present work are discussed in detail along the thesis and a full list of publications is included in Appendix A. Notwithstanding, a summary of the published research contributions is presented next.

The lack of a study in the literature stressing the need for QoS in wireless e-health and e-emergency services resulted in the publication [Gama08].

A new reconfiguration scheme was published in [Gama09], so that a WSN may react optimally in accordance with the patients' clinical state.

A simulation study showing the efficiency of diverse strategies adopted by the proposed MAC protocol to improve the packet delivery robustness, as well as the respective impact on the energy consumption and network scalability, was published in [Gama09a] [e-Book11].

The utilization of the physical testbed in a specific ambient assistance living scenario was published in [Gama10].

Taking advantage of the stable topology and traffic pattern characteristics found in e-emergency WSNs, a collaborative time-slot allocation algorithm with QoS requirements for single-hop networks was published in [Gama10a].

The results of experiments carried out in the physical and simulation platforms to test the performance of the proposed MAC protocol and IEEE 802.15.4 were published in [Gama11].

In order to improve the reliability of the simulation results, a generic parametric model reflecting the impact on the network performance of the software components within real sensor nodes was published in [Gama11a].

1.4 Thesis Outline

The remainder of this thesis is organized as follows. Chapter 2 provides an overview of wireless e-health, including BSNs and respective communication architectures and technologies. It is also discussed the suitability for e-emergency services of current wireless e-health projects.

Chapter 3 presents design issues and techniques typically used in the MAC layer to access the transmission channel, as well as generic mechanisms available in the MAC layer to provide QoS. It is also discussed the suitability for e-emergency WSNs of current MAC protocols available in the research literature.

Chapter 4 introduces AR-MAC, a MAC protocol presenting original concepts conceived for WSNs requiring efficient bandwidth allocation, low energy consumption, bounded latency, data transmission robustness, coexistence, and adaptability. It is introduced the novel network reconfiguration scheme used by AR-MAC, so that an e-health WSN may react optimally in accordance with the patients' clinical state. It is also presented the distributed and collaborative time-slot scheduling algorithm used by AR-MAC, as well as the frame formats of this protocol.

Chapter 5 presents the simulation and physical platforms used in this work to test the AR-MAC performance and compare it with other MAC protocols.

Chapter 6 proposes a set of equations to model the performance of software components within WSN devices. Validation tests using contention and reservation-based MAC protocols are presented to show that the inclusion of the parametric model in a generic network simulator improves the reliability of the simulation results significantly.

Chapter 7 evaluates the performance efficiency of AR-MAC protocol regarding multiple network metrics and compares it with IEEE 802.15.4 MAC protocol, under a realistic e-health simulation scenario.

Finally, Chapter 8 presents the conclusions and points out perspectives and directions for future work.

Chapter 2

Wireless E-health Overview

2.1 Introduction

Wired e-health technologies have been used in hospitals during the last decades using equipment with cables, thus hampering patients to move around freely. However, recent advances in distinct technological areas, such as electronics, wireless communications, biomedical sensors, micro-electromechanical systems, and electronic textiles, are changing this scenario by allowing permanent monitoring of patients during their normal daily activities [Kyriacou07], or in emergency and intensive medical healthcare services [Paksuniemi05].

Wireless e-health systems can improve effectively both the quality of life and the quality of care of patients, when compared with wired systems. Indeed, portability and unobtrusiveness facilities provided by wireless e-health systems allow patients to move around freely in their living spaces without compromising their activities, thus improving the patients' quality of life. In addition, measurements can be recorded over a long time interval, improving the quality of the health information [Park03]. Such electronic medical record offers a clearer view to the doctors than that obtained during short stays at the hospital using wired equipment, thus improving the patients' quality of care. For example, a wireless mobile telemetry system detected serious cardiac arrhythmias in fifty three percent of patients who had been previously monitored with wired equipment, where no arrhythmia was detected [Kumar08]. Wireless e-health also allows immediate response by the caregivers or the patient, because this is monitored continuously. However, the benefits of wireless technologies should be always evaluated against potential side effects, including interference and network management [Cypher06].

Following a top-down approach, the next section provides an encompassing view of the architecture of a typical wireless e-health system. Then, the discussion will focus on the core networks of wireless e-health systems – the body sensor networks, which are the key element in these systems. Finally, it will be discussed the suitability of current wireless e-heath systems to implement e-emergency services.

2.2 Wireless E-health Architecture

The architecture of a wireless e-health system is typically multi-tiered. The first tier is composed of one or more body sensor networks (BSNs). A BSN consists of a group of biomedical sensor nodes carried by a patient to monitor diverse physiological activities and actions. The diverse types of BSN architectures will be discussed in the next section. Multiple BSNs, sharing or not the same physical space, may be present in an e-health system. The collected data in a BSN is sent wirelessly to a nearby BS, eventually through a personal server (e.g., PDA).

Heterogeneous sensor nodes placed inside the patient's living space may also be present to monitor diverse environment properties, such as luminosity, temperature, humidity, and movement. This emplaced infrastructure form the personnel area network (PAN) and it helps providing contextual information about the people to be monitored (cf., ALARM-NET [Wood06]). Sensor nodes of a PAN may vary in their capabilities, but normally have little processing and storage capabilities, and may use either battery or wired power. Typically, the radio coverage of BSNs and PANs ranges up to two meters and ten meters, respectively [Liolios10]. The data of a PAN is normally transmitted wirelessly to a BS. The data of a BSN may also be transferred to a BS through the PAN [Virone06].

A BS bridges the sensor networks (PAN, BSNs) to a data communication infrastructure. Depending on the location of the patient (e.g., at hospital, at home, in ambulance, outdoors), this infrastructure may be (*i*) a private backbone network, (*ii*) a public data network (e.g., Internet, cellular network), or (*iii*) an ad-hoc network. These situations are discussed next.

(*i*) Let us consider the patient is being monitored at a clinical unit. The backbone network implemented in the building connects end devices (e.g., PDAs, PCs) and databases to the patient's BSN and PAN, through the BSs. Patient's data may also be forwarded through a public communication network to a diagnosis centre or a database for long-term archiving and data mining.

(*ii*) Let us consider the patient is being monitored at home or in an ambulance. In both cases, the personal server communicates, eventually through the BS, with remote

healthcare servers or clinicians using the Internet [Zhou07], a cellular data service (UbiMon [Ng04], MobiHealth [Halteren04]), or satellite links [Cova09]. After assessing the patient´s information, the clinicians provide the proper assistance or treatment.

(*iii*) Let us consider that a mass casualty event occurs outdoors. In this case, an ad-hoc network may be formed among patients' devices with short-range transmission capacity. Packets of a patient's sensor node may be transmitted to another nearby patient's sensor node and so on, until reaching the caregiver's device (e.g., CodeBlue [Shnayder05]). Several repeater nodes may also be strategically placed throughout the incident area forming a mesh network (e.g., AID-N [Gao07]).

At the last tier, patients and clinicians interface with the healthcare network using computing devices, such as PCs or PDAs. Patients use these devices to receive memory aids and clinical alerts from the e-health system. Caregivers use the computing devices to specify medical sensing tasks and to view important data.

As mentioned, a wireless e-health system has at least one BSN. This key technology for wireless health monitoring applications is discussed in the next sections.

2.3 Body Sensor Networks

A wireless BSN is a networking technology that interconnects small heterogeneous nodes with sensor or actuator capabilities in, on, or around a human body [Liolios10] and capable of establishing a wireless communication link. BSNs are intended to be open, extensible platforms which can be customized not only to a class of patients (e.g., diabetic, cardiac) but also to the particular set of health problems (e.g., chronic, acute) of the individual patient [Jones01]. Sensor nodes are small enough so that a person can use them comfortably on the body for a long time period. Interaction with the user or other persons is usually handled by a personal server, which acts as a sink for data from the sensor nodes.

2.3.1 BSN Characteristics

A BSN is a type of WSN, and consequently several challenges faced by BSNs are similar to conventional WSNs (e.g., limited computing and energy resources). However, there are intrinsic differences between both networks. BSNs present unique characteristics and application requirements that are distinct of the conventional WSNs. As a result, many of the significant advances in conventional WSNs regarding communication models, localization, time synchronization, and energy management, should be reevaluated given the new network requirements [Shnayder05]. Protocols and algorithms designed for conventional WSN, such as those surveyed in [Perillo05], are not always well suited to support a BSN [Latré11] [Chen11]. In the following, the characteristics of BSNs are discussed comparatively to conventional WSNs.

Interdependency. Unlike conventional WSNs, which normally operate as autonomous systems, BSNs seldom work alone. A BSN is the first tier of a multi-tiered, closed-loop wireless system, as seen in the last section.

Heterogeneity. The sensor nodes in a BSN are often heterogeneous and may require different resources of the network in terms of data rate, power consumption and reliability. Instead, sensor nodes and traffic characteristics are typically homogeneous in conventional WSNs.

Sensor placement. In conventional WSNs, sensor nodes are scattered (sometimes randomly) through the monitoring region and generally are insensitive to placement errors (unstructured network). Sensor nodes of a BSN are placed strategically at the human body (structured network). Ineffective placement or unintended displacement can significantly degrade the quality of the captured data.

Transmission power. In BSNs, a low transmission power per sensor node is needed to minimize interference and to cope with health concerns [RFsafety99]. Moreover, the propagation of the radio waves takes place in a medium of great losses, the human body. As a result, radio waves may reach the receiver considerably attenuated.

Latency. Depending on the application requirements, latency may be traded for improved reliability and energy saving. In a conventional WSN, battery lifetime may be maximized at the expense of higher latency. However in latency-critical BSN applications, such as alert generation and emergency response, this trade-off is hard to fulfill.

Data rate. BSNs are employed for registering human's physiological activities and actions regularly, resulting in the data streams with relatively stable rates. However, conventional WSNs are employed to monitor events occurring at long, irregular intervals.

Energy. Although energy conservation is definitely beneficial, replacement of batteries is easier in the non-implanted sensor nodes of a BSN than in conventional WSNs, whose sensor nodes may be physically unreachable after deployment and, therefore, should operate for months or years.

Density. Conventional WSNs use many sensor nodes and employ redundant sensor nodes to cope with failures. In contrast, BSNs use few sensor nodes and seldom employ redundant sensor nodes. Consequently, BSNs are not node-dense. The network density *D* can be expressed in terms of the number of sensor nodes per nominal coverage area through the expression:

$$D = \pi.N.R^2/A \qquad (2.1),$$

where *R* is the transmission range of the sensor nodes' radio and *N* is the number of sensor nodes placed in the area *A* [Bulusu01].

Mobility. As BSN users may move around, sensor nodes share the same mobility pattern, unlike the usually stationary sensor nodes in conventional WSNs. The relative inter-positioning of the sensor nodes in a BSN may also change, for example if placed in different limbs of the body. Therefore, BSNs should be robust against frequent changes in the physical topology.

Reliability. If BSNs are to control or help assess life-critical physiological events, they must be reliable. Unlike conventional WSNs, the failure of one sensor in the BSN could threaten life. Such e-health applications require fail-safe, fault-tolerant design principles.

The discussed characteristics show that BSNs have unique requisites, which are distinct of conventional WSNs. The devices typically found in BSNs are presented next.

2.3.2 BSN Devices

A BSN may be composed of sensor nodes, actuator nodes, and personal servers.

A (wireless) sensor node is a device that collects data on physical phenomena, processes the data if required and reports this information (wirelessly) [Latré11]. It consists of several components: one or more physical sensors, a data acquisition circuitry to collect data from sensors, a battery, a processor, memory, and a radio transceiver. Sensor nodes have very limited computing and energy resources.

Sensor nodes are used to measure certain parameters of the human body, either externally or internally. Examples include measuring the blood oxygen saturation or motion patterns. Every BSN has at least one sensor node.

A (wireless) actuator node is a device that acts according to data received (wirelessly) from the sensors or through interaction with the user [Latré11]. The components of this device consist of the actuator hardware, a battery, a processor, memory and a radio receiver or transceiver. A BSN may have not any actuator node. Computing and energy resources of actuator nodes are also very limited.

Actuator nodes take some specific actions according to the data they receive from the sensor nodes or through interaction with the user. For example, an actuator node, equipped with a built-in reservoir and a micro pump, administer to a diabetic the correct dose of insulin based on glucose level measurements. Another example of an actuator is a spinal cord stimulator implanted in the body for long-term pain relief [Krames02].

A personal server (or body-gateway) is a set that gathers all the information acquired by the sensor and actuator nodes and informs actuator nodes, the patient or a clinician (in this case via an external gateway) [Latré11]. Personal servers may perform a multitude of functions, including sensing, aggregating data from sensor nodes, serving as a user interface, and bridging BSNs to higher-level infrastructures [Hanson09]. The basic components of a personal server are a power unit, a processor, memory and a radio transceiver. Computing and energy resources are considerably higher than sensor and actuator nodes.

Some implementations use a custom designed microcontroller-based device, a PDA, or a cellular phone as personal server. However, some BSNs operate without the personal server, such as in CodeBlue.

Since sensor and actuator nodes have very limited energy resources, the energy available in the battery should be consumed carefully in order to prolong the BSN lifespan. Energy scavenging techniques may also be used for this goal.

2.3.2.1 Energy Scavenging

The available energy is very restricted in wireless sensor and actuator nodes. Consequently, these nodes should scavenge energy during its operation, in order to enhance the lifetime. However, energy scavenging only delivers small amounts of energy [Paradiso05].

Energy scavenging from on-body sources, such as body heat and body vibration, seems very convenient for BSNs [Bonfiglio11]. Regarding body heat-based solutions, it is used, for example, a thermoelectric generator to transform the thermal gradient between the environment and the human body into electrical energy [Gyselinckx06]. A wireless pulse-oximeter fully powered by the patient's body heat is presented in [Torfs06]. Regarding body vibration-based solutions, it is used, for example, the human gait as primary energy source [Buren06].

2.3.3 Biophysical Sensors

Biosensors are the key components of a BSN, as they bridge the physical world and electronic systems. Next, it is presented briefly the non-invasive biosensors used in the experimental e-health scenario considered in this work. The electrical characteristics of the physiological signals monitored by these biosensors will be presented in the next section. A deeper insight on diverse wearable sensors is provided in [Bonfiglio11].

Electrocardiogram (ECG) sensors measure the electrical activity of the heart. Several electrodes are attached at specific sites on the skin and the potential differences between these electrodes are measured to produce a waveform trace showing the contraction and relaxation phases of the cardiac cycles.

Blood pressure sensors measure the systolic (maximum) and diastolic (minimum) blood pressure exerted by circulating blood on the walls of vessels, through non-invasive oscillometric techniques, such as the arm cuff-based set.

Oxigen Saturation (SpO_2) is monitored with a pulse-oximetry sensor. This measures the blood oxygen saturation as a ratio of oxygenated hemoglobin to the total amount of hemoglobin. A small clip with a sensor is attached to the person's finger. The sensor uses two infrared lights to detect the infrared absorption of oxygenated hemoglobin.

CO2 gas sensors monitor the carbon dioxide concentration during respiration using, for example, a non-dispersive infrared light.

Respiratory rate sensors utilize piezoelectric or piezoresistive components to measure the number of movements indicative of inspiration and expiration per unit time[3].

Heart rate can be measured with a pulse-oximetry set or during ECG or blood pressure measurements.

2.3.4 Physiological Signals

A BSN may monitor several physiological signals simultaneously. According to the information specified in [ACSS08], emergency medical services should measure the ECG, the non-invasive blood pressure, the blood oxygen saturation, and the heart rate signals; intensive medical care services add the invasive blood pressure, the body temperature, and the respiratory rate/CO_2 gas signals[4].

Table 2.1 presents the electrical characteristics of the physiological signals usually used in the healthcare [Arnon03] [Paksuniemi05]. If some signal exceeds the threshold, the local supervisor node should send an alert to inform a caregiver or the patient. Table 2.2 presents typical thresholds for blood oxygen saturation (SpO_2), heart rate (HR), and blood pressure signals for alert detection [Gao05].

At non-emergency medical situations, signals such as ECG and SpO_2 may be transmitted in bursts at regular time periods, while signals such as body temperature and blood glucose are usually transmitted in single packets to the BS (cf. AMON [Anliker04]). In this case, physiological data transfer occurs only in intermittent occasions. However, in emergency cases this should not be the rule, since patient´s life

[3] Respiratory rate, oxygen saturation, and heart rate and can also be measured using photoplethysmogram (PPG) sensors [Lee08]. A PPG sensor monitors optically the pulse wave by detecting the change in the volume of blood flowing through the vessels of a finger. The combination of PPG and ECG allows for continuous cuff-less blood pressure monitoring based on pulse arrival time measurements [Espina06].

[4] While normal intensive care uses CO_2 gas, neonatology intensive care uses the respiratory rate.

is priceless and above to any other kind of considerations. Continuous and bulky data transfer in real-time might be prevalent here. To reduce the traffic load and the power consumption of a BSN, e-health systems may also enhance intelligence, available memory, and processing power of personal servers and sensor nodes (e.g., HUMAN++ [Gyselinckx06]).

bio-signal	**freq. range** (Hz)	**sampling rate** (Hz)	**resolution** (bit)	**data rate** (kb/s)
EMG	0...10000	20000	16	320
EEG (per lead)	0.5...70	350	12	4.2
ECG (per lead)	0.01…60~125	120-250	16	4
Blood pressure	0 … 60	120	12	1.44
SpO_2	0 … 30	60	12	0.72
Respiration rate	0.1 … 10	20	12	0.24
Heart rate (HR)	0.4 … 5	10	12	0.12
Temperature	0…1	2	12	0.024
Blood Glucose	0...1	2	8	0.016

Table 2.1 – Physiological signal electrical characteristics.

Alert type	**Detection parameter**
low SpO_2	SpO_2< 90%
bradycardia	HR < 40bpm
tachycardia	HR > 150bpm
heart rate change	|ΔHR / 5 min| > 19%
heart rate stability	max. HR variability from past 4 reads > 10%
blood pressure	systolic or diastolic change > ±11%

Table 2.2 – Alert detection parameters.

After presenting the characteristics of a BSN and its typical components, it is discussed next how data are transferred between the entities of a BSN.

2.4 BSN Communication Architectures

Depending on the way how sensor nodes transmit data to a BS or a personal server, BSNs can be classified as wireless, wired, or hybrid [Chen11], as shown in Figure 2.1.

In wired BSNs, physical sensors collect data and send them through cables to a personal server, which in turn communicates wirelessly with a BS. This case is schematically illustrated in Figure 2.1*a*. Wired BSNs avoids the challenges of wirelessly interconnecting sensors, but compromises the patients' quality of life as they are obliged to use special suits or to live with wires attached to the body. For example, MITHril [Pentland04], SMART [Curtis08], LifeGuard [Mundt05], and Bi-Fi [Farshchi07] utilize cables to connect multiple physical sensors directly to a personal server.

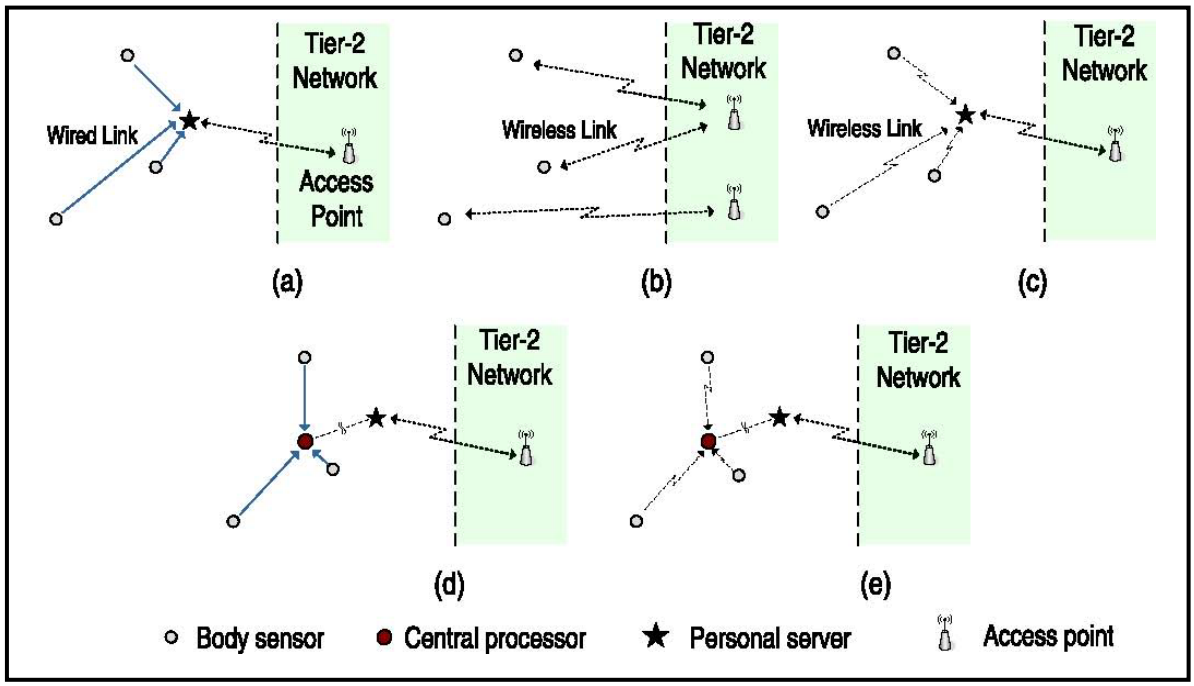

Figure 2.1 – Architecture of BSN communication: (*a*) wired; (*b*) direct wireless; (*c*) indirect wireless; (*d*) wired hybrid; (*e*) wireless hybrid [Chen11].

In wireless BSNs, data is directly transmitted wirelessly to a BS, as shown in Figure 2.1*b*, or indirectly through a personal server, as shown in Figure 2.1*c*. In this case, the personal server may process, aggregate, and compress the physiological data

before forwarding it to the BS. ALARM-NET [Wood06] and CareNet [Jiang08] are examples of the situation illustrated in Figure 2.1*b*. WiMoCa [Farella08] and SENSATION [Astaras08] exemplify the case in Figure 2.1*c*. Low-power wireless technologies are required in these communications to cope with health concerns [RFsafety99], to maximize the continuous monitoring lifespan, and to minimize interference among nearby BSNs.

Figures 2.1*d* and 2.1*e* present alternative strategies to a two-level BSN. Multiple wired or wireless sensors are connected to one central processor in order to reduce the amount of raw data and to save energy. After data fusion, the size of data that needs to be transmitted from the central processor to a personal server is reduced. However, these solutions involve more challenges, such as advanced sensor data processing.

The present work considered only the full wireless solutions shown in Figure 2.1*b* and 2.1*c*, because wired e-health systems, irrespectively of the level of wired connections, imposes necessarily some degree of obtrusiveness, and consequently increases the possibility of patients rejecting the sensor technology.

A communication protocol that is suitable for the case shown in Figure 2.1*b* may be also convenient for the situation of Figure 2.1*c*, because the protocol operates in a smaller size network. Moreover, the case of Figure 2.1*c* does not solve the mutual interference problem that may occur in nearby BSNs operating in the same channel. This coexistence problem may be avoided in the case of Figure 2.1*b* with a BS performing centralized management. For these reasons, the wireless architecture of Figure 2.1*b* was chosen for this work.

After presenting the diverse communication architectures, it is discussed next physical communication issues of BSNs, namely the human body influence in radio-frequency (RF) communications, and the communication technologies typically used.

2.5 BSN Physical Layer

The physical layer imposes a design tradeoff between communication distance, transmission symbol rate, and power consumption. The distance of BSN

communications is normally limited to a range of two meters [Latré11], in order to reduce the transmission power level of radio transceivers, as well as to reduce patient exposure to RF energy and to decrease interference among adjacent BSNs. The BSN power consumption also decreases because the power consumption of a sensor node decreases with the power transmission level (see Table 5.1). In addition, the power consumption of a sensor node depends on the application data rate, the radio-frequency modulation scheme, the wireless channel quality, and the human actions. The effect of application data rate and RF modulation techniques on the power consumption of a sensor node has been considered in several studies, such as in [Kohvakka06] and [Wang01] [Cui05a], respectively. More challenging is the influence of the human action and body on the RF channel of a BSN, which naturally affects the power consumption.

2.5.1 Body Influence on RF Communications

Next, it is discussed the influence of the human body on wireless communications executed on-body.

The path loss in a wireless channel is commonly represented through the following empirical log-normal shadowing path loss model:

$$P_{dB}(d) = P_{0dB} + 10.\eta.\log(d/d_0) + X_\sigma \qquad (2.2),$$

where d is the distance from the antenna, d_0 is the reference distance, P_{0dB} is the path loss at the reference distance, X_σ is a zero-mean Gaussian random variable with standard deviation σ, and η is the path loss exponent (or propagation coefficient)[5] [Rappaport96]. So, in wireless networks the transmitted power generally decays with d^η. In free air space, η is equal to two.

Most of the sensing devices used in BSNs are attached on the body. The propagation along the human body can be divided into line-of-sight and non-line-of-sight situations. In the former, all sensor nodes are located at one side of the body. In the latter, the transmitting and receiving antennas are placed at different sides of the body.

[5] The signal-to-noise ratio at a receiver distanced d from the sender is $SNR = P_{t\,dB} - P_{dB}(d) - P_{n\,dB}$, where $P_{t\,dB}$ is the transmission power, $P_{dB}(d)$ is the power loss in the channel at distance d, and $P_{n\,dB}$ is the thermal noise of the radio plus the power of interfering signals that may reach the receiver.

The channel model for line-of-sight propagation along the human body was studied in diverse works, including [Zasowski03] [Roelens06] [Fort06]. It was found that η is between three and four, depending on the position of the device (e.g., η is lower on the arm than on the trunk). It is shown in [Roelens06] that there is a significant impact of the antenna height on the path loss exponent - the closer the antenna is to the body, the higher is the path loss.

In non-line-of-sight situations, the electromagnetic wave is more likely to diffract around the human body rather than pass directly through it. A η ranging from five to six was found [Zasowski05] [Fort06]. The results above show that it is not always possible to assume single-hop communication along the body. Furthermore, it is shown that in terms of energy efficiency, the use of multi-hop communication in a BSN could lead to a more optimal network topology [Zasowski03] [Braem07].

The body movement also has an important role in the strength of the received signal. Loss rates above fifty percent were found when the body was in motion [Ylisaukko04].

Studies have shown that three main factors contribute to the wireless channel characteristics of a BSN: (*i*) *environment*: where the BSN user is located (i.e., indoors, outdoors) and the interference degree from other nearby users or external RF sources; (*ii*) *link type*: where the sensor nodes are located (i.e., in-body, on-body, off-body), whether the linked sensor nodes are located in distinct parts of the body, and whether the linked sensor nodes are in line-of-sight or not; (*iii*) *activity*: the user's current activity (e.g., walking, running, jumping) and the duration of the activity.

2.5.2 Radio Technologies

This section presents standardized radio technologies used in BSNs, namely Bluetooth, IEEE 802.15.4, and IEEE 802.15.6. The MAC layer aspects of these standards will be discussed in Chapter 3. The ultra wideband (UWB) is also discussed. Proprietary radio technologies are not referred, but they can be overviewed in [Chen11].

2.5.2.1 UWB

UWB radio signals are transmitted in very fast impulses, originating a large broadband signal spectrum with extreme low power spectral density. Signals behave as noise to other radio systems, which results in low probability of interception and detection (security), and less interference. UWB assures robust and energy efficient communications [Falck06] and is suitable for wireless short-range applications, as well as in environments sensitive to RF emissions, such as hospitals.

One great advantage of UWB technique is providing a data rate up to around 27 Mb/s (cf. IEEE 802.15.4a) or even higher, such as 110 Mb/s at ten meters and 480 Mb/s at two meters (cf. IEEE 802.15.3a). Nevertheless, it is argued in [Hao08] that UWB is inappropriate for BSNs due to its high complexity and the unsuitable wide bandwidth modulation. Also, UWB chips have exhibited higher power consumptions than that of the conventional narrowband short-range chips [Gharpurey08].

BASUMA [Falck06] is an example of a project exploiting UWB as BSN communication technique to enable continuous monitoring of chronically ill patients at their homes.

2.5.2.2 Bluetooth

Bluetooth[6] [IEEE1] is an industry standard for connectivity between devices and operates in star topology in the 2.4 GHz ISM band. It uses frequency-hopping technique over seventy nine 1 MHz channels at a nominal rate of 1600 hops/s to allow the coexistence of multiple networks in the same region and to reduce external interferences. It has a complex protocol stack, from the physical layer up to the application layer, and specifies three classes of devices with different transmission powers and corresponding coverage, although ten meters is the most common mode. The low power version provides a maximum data rate of 1 Mb/s and devices' synchronization can be done in a few milliseconds.

[6] Bluetooth was named after Harald Blåtand (*c*.935-*c*.985), viking king of Denmark from *c*. 958 and king of Norway for a few years, probably *c*. 970.

2.5.2.3 IEEE 802.15.4

IEEE 802.15.4-2003 [IEEE4], widely named ZigBee[7], operates in sixteen channels in the 2.4 GHz ISM band at 250 kb/s with offset quadrature phase-shift keying (O-QPSK) modulation, and in one channel in the 868 MHz European band at 20 kb/s with binary phase-shift keying (BPSK) modulation[8]. It uses direct sequence spread spectrum (DSSS) coding. The coverage area is 10~75 m and supported network topologies include star, tree cluster, and mesh topologies. The IEEE 802.15.4a amendment specifies two additional physical layers using UWB and chirp spread spectrum in the 2.4 GHz ISM band.

According to [Barth08], BSNs using the IEEE 802.15.4 present unsatisfactory performance because BSNs operating at 2.4 GHz suffer from significant and highly variable path loss near the human body. An additional concern with IEEE 802.15.4 is that the maximum supported data rate is only 250 kb/s, which is not the best rate to support real-time and large-scale BSNs. IEEE 802.15.4 may also suffer from interference with wireless local area networks (WLANs) transmissions. For example, IEEE 802.11 uses the same 2.4 GHz band and transmits bigger signal power [Shin07].

Diverse studies have concluded that IEEE 802.15.4 is not the best solution for supporting communication in BSNs [Timmons04] [Golmie05] [Cavalcanti07]. Indeed, IEEE 802.15.4 was not designed to support BSNs[9]. Even so, it is currently the most widely used radio standard in BSNs [Chen11] [Latré11].

2.5.2.4 IEEE 802.15.6

Still in development, IEEE 802.15.6 will be a communication standard specifically optimized for BSNs. It is a short-distance protocol (2~5 m) that guarantees very low latency and very low power consumption, and it supports coexistence with other BSN networks and other wireless technologies. It defines three physical layers: narrowband, UWB, and human body communications layers. In narrowband, it may operate in

[7] ZigBee [ZigBee07] specifies the network, security and application layers on top of IEEE 802.15.4.

[8] IEEE 802.15.4-2006 also permits 100 kb/s with O-QPSK modulation in the 868 MHz band.

[9] Nevertheless, ZigBee Alliance states that ZigBee applications include, among others, medical sensors.

diverse bands, including the 2.4 GHz ISM band at 971.4 kb/s. In UWB, data rates range approximately from 0.4 Mb/s up to 12.6 Mb/s. Human body communications uses capacitive coupling and data rates may scale up to 2 Mb/s [Batra11].

2.5.3 Human Body communications

Researchers have been investigating the possibility of using the human body as transmission medium for small amounts of data, namely through capacitive coupling techniques. A transmitter generates a weak electric field that is capacitively coupled to the body. The radiated energy only extends outwardly a couple of centimeters from the skin, making eavesdropping difficult and enabling interference-free personalized communication. Moreover, power requirements are low and channels are highly stable and potentially interference-free [Zimmerman96]. Path loss also appears to be smaller than what would be measured in a wireless channel [Batra11]. These systems work at low frequencies, ranging from some kHz to a few tens of MHz.

Capacitive coupling is appealing for BSNs because it allows: (*i*) a body-worn sensor node to identify the person it belongs to; (*ii*) a sensor node to discover all other sensor nodes attached to the same person, but not more; (*iii*) exchange network parameters between necessary sensor nodes; and (*iv*) wake up radio transceivers from sleeping mode [Falck07].

2.6 Wireless E-Health Systems

Research and development of wireless healthcare systems has grown during the last decade, in academic and private institutions for monitoring patients in distinct scenarios, such as mass casualty events, disaster recovery, triage, and assisted living [Kyriacou07]. Regarding the assisted living, applications have been developed for monitoring (*i*) daily living activities; (*ii*) fall and movement detection; (*iii*) location tracking; (*iv*) medication intake; and (*v*) medical status. However, the kind of application more widely studied in healthcare systems focus on capturing and sending the medical status data of patients to a remote site for further evaluation [Alemdar10]. Surveys on wireless e-health systems

are presented in [Kyriacou07] [Pantelopoulos09].

Upon reviewing twenty one wireless e-health projects, most of them referred along this chapter, the author concluded that:

(*i*) 74% of the fifteen projects with wireless BSN architecture use IEEE 802.15.4 and Bluetooth in the BSN communications, and 26% use UWB or solutions based on time division multiple access (TDMA) schemes.

(*ii*) 81% of all projects were developed for remote health status monitoring of individual patients at their homes (33%) or ambulatory (48%). In generic terms, the monitored bio-signals data are delivered to a portable hardware module which in turn uses public data networks to transmit the data to health centers.

(*iii*) 19% of all projects were developed for detecting or monitoring several patients in emergency medical situations at the same physical area. All these projects use standard protocols in the BSN communications. As this class of projects is closer to the e-emergency scenario considered in this work (emergency and intensive care monitoring of several patients in a hospital room), one representative project is described next for a better insight. CodeBlue was chosen because it is commonly cited in e-health literature and a few performance studies are available. UbiMon is also described, since it is a typical example of the class of projects referred in (*ii*).

CodeBlue uses a message delivery system for emergency medical care and mass casualty incidents. Pulse oximetry and two-lead ECG data from patients are transmitted by ZigBee compliant sensor nodes to a recording system. As shown in Figure 2.2, data packets can be routed through the network to multiple receivers carried by caregivers. CodeBlue is based on a publish/subscribe message delivery framework, allowing multiple sensor nodes to relay data to all receivers interested in that data. Sensor nodes filter the data locally to save bandwidth. Multi-hop routing is used when publishers and subscribers are not within the radio range. A discovery protocol is used for sensor nodes to discover one another and determine the respective capabilities. Moreover, the system uses an RF-based localization system to track the location of patients and caregivers. A query interface allows a caregiver´s receiver to request data from specific sensor nodes in accordance with some filter rules.

Evaluation studies revealed that further work on reliable communication, bandwidth limitation issues and security is needed. Tests carried out in a network composed of fifteen sensor nodes at maximum, with sensor nodes generating packets of 115 B at a

rate of 3 Hz, showed that CodeBlue presents an average packet reception ratio lower than 90% [Ko08], which is unsuitable for e-emergency WSNs.

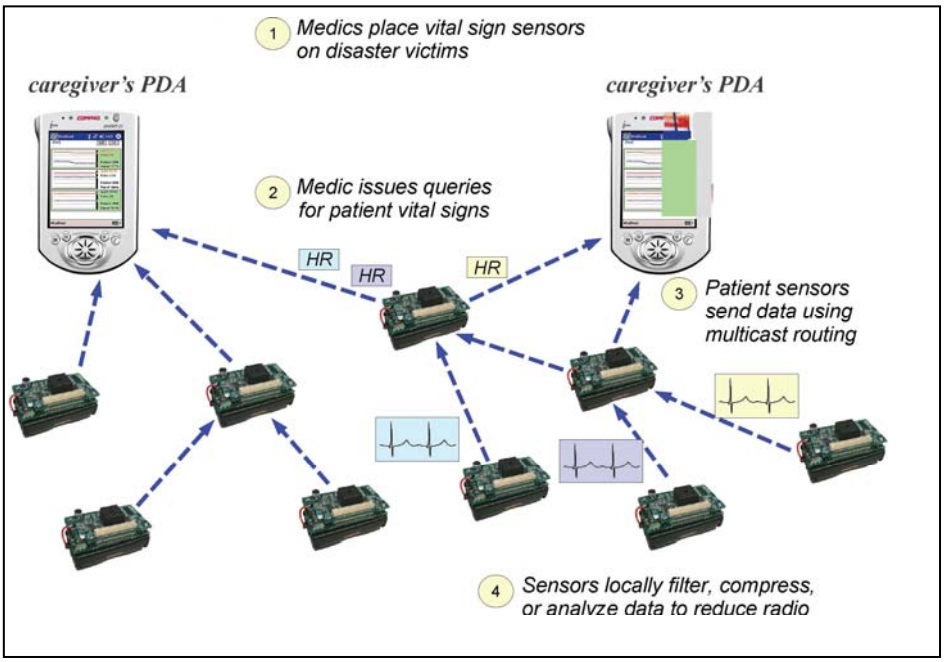

Figure 2.2 – Ad-hoc network infrastructure of CodeBlue [Welsh05].

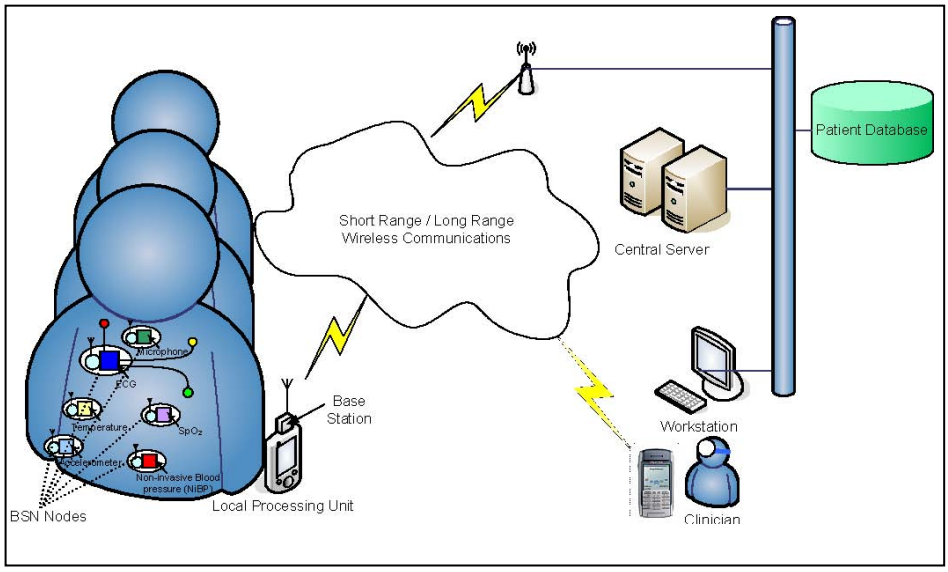

Figure 2.3 – UbiMon architecture [Ng04].

UbiMon consists of five major components, namely the BSN nodes, the local processing unit (LPU), the central server, the patient database, and the workstation, as shown in Figure 2.3. All the sensor data collected by the BSN nodes are transmitted wirelessly using a special TDMA-based protocol to deal with the high data rate requirement of the ECG signal and gathered by the LPU (e.g., PDA, mobile phone). The LPU also detects abnormalities and provide immediate warnings to the patients. In addition, it acts as a wireless router between the BSN nodes and the central server. Upon receiving real-time multisensory monitoring information from the LPU, the central server will store the data to the patient database, and also perform long-term trend analysis. Through deriving the pattern and trend from the physiological data, the central server predicts the patient's health condition to prevent any potential life-threatening abnormalities. Portable workstations also allow clinicians to analyze the patient data.

IEEE 802.15.4 is prominently used in the projects referred along this chapter. Such option is possible because the BSNs of those projects operate in e-health scenarios (*i*) with a single patient or (*ii*) with multiple patients in the same area but generating relative low traffic volumes. However, both cases hardly are met in emergency or intensive care units of a hospital. Moreover, many of those projects are not truly real-time systems. Therefore, it is expected that those systems are inappropriate to implement e-emergency WSNs.

2.7 Summary

With the recent technological advances in miniature bio-sensing devices, microelectronics, micromechanics, wireless communications, and electronic textiles, it is expectable that BSNs provide a wide range of benefits to patients and caregivers through pervasive and continuous monitoring and early detection of possible health state abnormalities. However, if BSNs are to control or help assess life-critical physiological events, they must be very reliable. The responsibility of the MAC layer towards this goal is fundamental, as discussed in the next chapter.

Chapter 3

MAC: Fundaments and Protocols

3.1 Introduction

QoS is required in e-emergency WSNs, since timeliness and robustness of data delivery, energy and bandwidth preservation, adaptability, fairness, and scalability are relevant properties in these networks, as discussed in Chapter 1. To assure these properties, QoS techniques must be deployed in such networks.

Within the protocol stack, the multi-layer cooperation regarding the QoS support is fundamental. The MAC layer plays a special role in this support, as the medium access and the reliability of the communication channel directly impact on the performance of upper layer protocols. Besides contributing directly to the channel access delay and the bandwidth utilization, the importance of the MAC layer is also emphasized as transmission is typically the most expensive operation that a sensor node performs in terms of energy dissipation [Bachir10].

Diverse actions can be carried out in the MAC layer to contribute to meet QoS objectives [Yigitel11]: (*i*) a MAC protocol should minimize the medium access delay of sensor nodes to assure that its contribution to end-to-end packet delay is reduced; (*ii*) a MAC protocol should minimize packet collisions to improve delivery delay, throughput, and energy efficiency. It should also maximize the reliability of packet delivery through retransmission and recovery techniques; (*iii*) energy consumption should be minimized through duty cycling and transmission power control techniques; (*iv*) the overhead of the MAC protocol should be minimum to improve the efficiency of both energy and bandwidth utilization; (*v*) interferences should be minimized and parallel transmissions maximized by tuning the related parameters, such as time scheduling, transmission power, operating channel; (*vi*) fairness should be guaranteed, i.e., the MAC protocol must not exhibit preference for any particular node when multiple nodes contend for the channel access to send packets of the same traffic class. It should be noted that it is not mandatory or practical to provide all these characteristics in a single MAC protocol, unless the WSN application requires it. The QoS performance expected from a MAC layer depends naturally on how its inner mechanisms are developed, tuned and deployed.

After presenting the techniques typically used in the MAC layer to access the transmission channel, and the generic mechanisms available in the MAC layer to provide QoS, this chapter discusses the suitability for e-emergency WSNs of current

MAC protocols providing deterministic packet delivery service.

3.2 Medium Access Strategies

The primary function expected from a MAC layer is to rule the medium access of a node in order to avoid or minimize packet collisions. The algorithms used in this task are normally based on random, scheduled, hybrid, or round-robin access. Each approach presents advantages and drawbacks, as discussed next.

3.2.1 Random Access

In these medium access schemes, nodes contend for the wireless channel access to send packets, originating eventually packet collisions in the network. A central entity responsible for synchronizing and managing the WSN is not required. Due to the distributed and random backoff nature of this class of algorithms, it is difficult to provide a deterministic channel access guarantee. Hence, this class of MAC protocols is not suitable for hard real-time networks. It is also not the best option for networks requiring high throughput and low latency, or networks presenting highly correlated and dominantly regular traffic. Instead, they are more adequate for conventional large multi-hop WSNs with low-traffic loads and nodes remaining largely inactive for long time, becoming active when an event is detected, such as in surveillance or environmental monitoring applications. In these cases, the MAC protocol must consider primarily the energy efficiency to prolong the network lifetime, the scalability and the adaptability to changes in the network size and topology. Attributes such as latency, throughput, bandwidth utilization, and fairness may be considered secondary.

Aloha [Abramson70] was the first MAC protocol proposed for wireless data communications. In this straightforward random access protocol, a node sends a packet as soon as it needs to do it and waits for the respective acknowledgment frame from the receiver. If the confirmation is not received, the sender waits a random time and retransmits the packet again. However, Aloha presents a low efficiency regarding the channel utilization (18.6%, or 36.8% with the slotted variant).

The Carrier Sense Multiple Access (CSMA) algorithm [Togabi75] is the most representative example used in random access protocols. Diverse variants of CSMA have been developed. CSMA with Collision Detection (CSMA/CD) was developed for wired bus networks, such as 10Base2 Ethernet. Basically, when a node needs to transmit, it listens firstly to the wired medium. If this is busy, the node waits a random time until the medium is sensed free. Otherwise, it sends the packet to the medium. If two or more nodes begin transmitting at the same time, the nodes sense the collision between the packets, stop transmitting, and repeat the whole process again.

However, CSMA/CD cannot be used in wireless networks, such as IEEE 802.11 WLANs or WSNs, because the transmitting power signal is normally much stronger than the receiving power signal, masquerading it, and so it is not possible to detect collisions of ongoing transmissions. In this case, the CSMA uses the Collision Avoidance (CA) variant to minimize collisions. Nodes sense the wireless medium before transmitting and if the channel is busy, defer transmission. This simple strategy may cause a well-known phenomenon known as hidden node problem. This situation, reported in the mid seventies of the last century, occurs when the source node cannot truly evaluate the channel activity at the receiver node, because sensing the channel activity at the source does not reflect the real state of the channel at the receiver. To minimize this problem, it is used the request-to-send (RTS) / clear-to-send (CTS) dialogue. The source node sends an RTS packet to the channel and waits for a CTS packet from the receiver node allowing the transmission. As this solution adds overhead to the MAC protocol, it is normally only used with large packets [Gast02].

The exposed node problem is another phenomenon that may occur in networks using CSMA/CA. It occurs when a node refrains from transmitting to node *d* because a neighbor node *n* transmits, but node *d* is not in the coverage area of node *n* and, consequently, should not experience a collision. Since this problem affects only the number of parallel transmissions, and not the correct reception of transmissions, it is not considered as critical as the hidden node problem, because this may cause collisions. For time-sensitive traffic, dealing with hidden nodes is even more crucial, since a collision may cause a deadline miss.

One disadvantage of random access approach is that a lot of energy is often wasted due to idle listening. To tackle this problem, protocols using preamble sampling techniques have been developed, such as B-MAC [Polastre04] and WiseMAC [El-Hoiydi04]. Basically, each packet is sent with a preamble signal to alert potential

receivers about an upcoming message transfer. Nodes wake up periodically for sensing the channel. When activity is detected, nodes stay awake for the time required to receive the packet. After reception, the node returns to sleeping state. By making the preamble signal longer than the sleep time interval, a sender is able to wake up the intended receivers. The preamble signal may be implemented tuning the physical layer preamble length.

3.2.2 Scheduled Access

In these medium access schemes, each node uses a dedicated channel allocation to transmit or receive packets without collisions. As nodes only need to turn on the radio during their assigned time-slots, low overhearing, low idle-listening, and low active-sleep duty-cycle operations can be achieved, resulting in good energy efficiency comparatively to random access strategies, as shown in [Ergen06]. Scheduling-based techniques are appropriate to implement real time networks, because a bounded and predictable medium access delay can be guaranteed. The data throughput is controlled and limited to the utilization of all available slots. Fairness is assured among nodes as slots are assigned to them in each frame. These protocols are generally variants of the time division multiple access (TDMA) scheme, eventually combined with the frequency division multiple access (FDMA) technique. In the TDMA scheme, time is split into equal intervals known as time-frames or superframes. Each time-frame is further divided into slots of fixed duration known as time-slots. Nodes use dedicated time-slots to transmit data without the need to contend for the medium. Beaconing is the traditional approach to facilitate the network time synchronization, but beaconless solutions may be used too. For example, GinMAC [Suriyachai10] uses the existing exchange of data and control messages for time synchronization. FDMA divides medium access by frequency, where transmission channels are allocated individually to nodes. FDMA combined with TDMA is used, for example, in [Shih01] and TSMP [Pister08].

It should be also mentioned the Code Division Multiple Access (CDMA) and Spatial Division Multiple Access (SDMA) schemes. CDMA is a form of spread-spectrum technique where a code (or chip sequence) assigned to each transmitter allows multiple users to transmit in parallel over the same channel, causing only minor distortion to one another. CDMA is used, for example, in [Chung07] and [Yu06]. However, the form how

codes are assigned to nodes (code management) may not be a trivial task. In SDMA, a network area is divided in independent communication sectors to take advantage of spatial reuse. Multi-beam directional antennas are used in [Hussain10] to create an SDMA environment in a BSN.

3.2.2.1 Scheduling Methods

The central concern in TDMA-based MAC protocols is how to set up and maintain a specific schedule. To this goal, three scheduling methods are used [Bachir10].

(*i*) In the *link-based* scheduling method, a time-slot dedicated to a specific sender and specific receiver is set up, thereby minimizing idle listening and eliminating collisions and overhearing. This is the method traditionally used in reservation-based MAC protocols (e.g., TSMP), since it is commonly the most efficient in terms of energy saving. However, varying traffic conditions and network dynamics require over-provisioning or new schedules to be set up which incurs large overheads.

(*ii*) In the *sender-based* scheduling method, the time-slots used by the senders to transmit data are specified, which requires all receiving sensor nodes to listen. Any changes at the receiving side remain transparent to the established schedule. Overhearing remains a problem in this approach, but it may be minimized by putting the sensor node in sleeping mode as soon as it detects the packet is not addressed to it. PicoRadio [Guo01] uses this approach to avoid collisions.

(*iii*) In the *receiver-based* scheduling, the receiving time-slots are specified. Each sensor node has its own time-slot during which it wakes up to receive potential data. Network dynamics at the transmitting side are transparent to the schedule. However, collisions between various transmissions can potentially occur if more than one transmitter wishes to reach a specific receiver. Crankshaft MAC protocol [Halkes07] uses this method to avoid overhearing.

The link-based and sender-based methods are suited to periodic, delay sensitive and appreciable traffic load. The receiver-based method is appropriate to periodic and low-load traffic.

The schedule definition can be centralized or distributed. In the former, a central coordinator establishes a scheduling scheme after collecting the traffic characteristics of

the nodes and the network topology. This schedule allows each node to access collision-free the channel. The central coordinator also keeps the network tightly synchronized in time. In the latter, scheduling is defined without the participation of any central entity, using instead a localized collision-free scheduling or a distributed scheduling method. A reservation-based MAC protocol may also consider other aspects in addition to the medium access scheduling, such as, rotating the cluster-head role throughout the nodes to balance the energy drainage, handling the nodes' mobility, adapting the scheduling to traffic changes, and using different communication frequencies. In some cross-layers implementations, the MAC protocol can also route the traffic through a multi-hop WSN.

Reservation-based MAC protocols have some shortcomings resulting from their dependency on network topology and frequent time synchronization. These commitments lead to over-provisioning, protocol overhead, and complexity, and networks of reduced flexibility and scalability. Thus, these MAC protocols are not attractive in large-scale networks. Instead, they are most suitable for small or medium scale, non-node-dense networks presenting periodic and appreciable traffic loads. E-emergency WSNs typically present these characteristics.

As mentioned previously, the link-based scheduling method presents the best efficiency in terms of energy saving. Accordingly, scheduling algorithms proposed for WSNs normally adopt this approach.

3.2.2.2 Link Scheduling Algorithms

Several TDMA scheduling algorithms have been developed taking into account the latency or the energy consumption in one-hop or multi-hop scenarios. In one-hop WSNs the BS is the receiver of all sensor data transmissions, and so only one node can transmit in a time-slot. However, such direct communication between the sensor nodes and the BS is not energy efficient and even not always possible [Latré07]. This is particularly true in BSNs, as the propagation loss around the human body is high (see Section 2.5.1). In multi-hop WSNs, more than one node can transmit at the same time-slot (spatial reuse), if their receivers are not in interfering regions of the network.

Regarding link scheduling in multi-hop networks, a simple algorithm for an arbitrary loop-free topology with one sink node is proposed in [Cui05] to find the minimum-delay

schedule given the time-slot lengths for all the links. The tradeoff between the total energy consumption and delay is also studied. According to [Gandham05], the time-slot assignment problem is closely related to the edge coloring problem for a graph, i.e., no two edges incident on the same node are assigned the same color. Using this assumption, the authors proposed a distributed algorithm using a minimal number of time-slots to reduce the communication latency. However, the topology of the network must stay unchanged during the time-slot assignment. This condition is hard to find in WSNs, as topology may change due to displacement or failure of nodes.

It is proposed in [Ergen05] two centralized coloring algorithms based on a conflict graph to determine the smallest length conflict-free assignment of time-slots during which the packets generated at each node reach their destination. The conflict graph, constructed from the original graph, includes all nodes that cannot transmit at the same time. These algorithms are inappropriate for large networks, because a lot of communication among the nodes is required. In [Sridharan04] is proposed a distributed solution to improve the medium access fairness of flows in a WSN, which outperformed random MAC in terms of fairness and delay.

It is presented in [Mao07] a centralized time-slot assignment algorithm based on genetic algorithms and particle swarm optimization, with an *n*-hop neighborhood criterion to avoid interferences in the time-slots (only nodes above *n* hops of distance can reuse time-slots). Scheduling algorithms using the *n*-hop criterion can only be used in regular network topologies. To overcome this limitation, it is presented in [Nunes07] a distributed time-slot allocation algorithm based on the interference physically experienced by the WSN nodes through the received signal strength. Capable of coping with irregular node deployments, the algorithm assures that the access to each time-slot is free of interferences. It assigns each time-slot to only one node within the interference vicinity, and allows spatial time-slot reuse outside of that vicinity.

3.2.3 Hybrid Access

Hybrid schemes have also been developed to overcome the drawbacks of both scheduled and contention methods. Hybrid schemes can classify the packets (e.g., data, control, low priority, high priority) and choose the proper way to access the medium regarding the class that particular packet belongs to.

Z-MAC [Rhee05] and Crankshaft are examples of hybrid MAC protocols. For instance, Z-MAC builds a TDMA overlay on top of CSMA and dynamically switches between both modes, depending on the number of lost packets detected by the sensor nodes.

3.2.4 Round-robin Access

This class of medium access protocols uses polling and token passing techniques.

3.2.4.1 Polling

In this kind of MAC protocols, a station named master plays the role of central coordinator, ruling the medium access of the networked nodes called slaves. A slave node can only transmit after being polled by the master. The master may send data to a slave in the polling packet. After receiving the data from a slave, the master continues the polling process with the next slave. Typically the master station polls the slave nodes following a round-robin scheme, irrespectively of the traffic patterns. Bluetooth [IEEE1] is an example of MAC protocol using polling. Due to the polling overhead, the protocol efficiency in terms of bandwidth utilization and energy is low if the slave nodes do not have frequently any data to send during the master queries.

3.2.4.2 Token Passing

In this class of protocols, a token is passed from node to node sequentially. The station with the token has permission to transmit on the communication medium. In wireless networks, the probability of losing a token is not negligible and the token recovery process may not be simple. Token-based protocols present the same efficiency problems as polling protocols, and also introduce significant increase in hop-to-hop delivery latency.

A token-based MAC protocol for WSNs is proposed in [Ray11] to reduce flooding, collision, traffic congestion and, consequently, the energy consumption in the network.

3.3 QoS Mechanisms at the MAC Layer

The techniques used to improve the performance of the MAC layer may contribute directly or indirectly to QoS provisioning. Error control, data suppression and aggregation, power control, clustering, adaptation, and service differentiation are examples of techniques that may be implemented at the MAC layer [Yigitel11]. As explained next, these techniques may contribute to QoS provisioning.

Error control mechanisms improve the data delivery reliability by using automatic repeat request (ARQ), forward error correction (FEC) and hybrid ARQ techniques. ARQ scheme uses persistent retransmissions until the data is successfully delivered. The sender uses the frame bytes to calculate a frame check sequence (FCS) code, which is normally included in the frame trailer. The receiver uses this code to detect packets corrupted during the transmissions. The receiver may request a retransmission explicitly or implicitly. In the former, the receiver sends a negative acknowledgment frame. In the latter, the sender does not receive a positive acknowledgment frame within a stipulated time interval after having transmitted a packet. ARQ scheme can be used to provide hard QoS in terms of packet delivery by persistent retransmissions. However, ARQ is only effective if the channel is in good condition and not overloaded; otherwise, latency and energy consumption can grow to unacceptable levels. ARQ is not recommended to transmit real-time traffic when the propagation time is high or when the transmission rate is low, because the cumulative delay of successive retransmissions may lead to an unacceptable total delivery delay.

FEC mechanisms prevent retransmissions of data packets received with partial errors. An error-correcting code is included in the data packet, so that the receiver is able to recover the corrupted bits. However, to achieve acceptable levels of error correction, the length of the code must be about the same as the length of the data. So, this technique leads to significant bandwidth waste if the channel conditions are good, or it may be inefficient if the channel conditions are too bad. A FEC algorithm, if deployed in sensor nodes, must be lightweight and simple since their computing resources are very limited. Bluetooth is an example of a MAC protocol that uses the FEC technique for transmitting voice and audio traffic.

Hybrid ARQ takes advantage of both ARQ and FEC mechanisms. Initially, data

packets are weakly coded or not coded at all by the sender. If the received packet is corrupted and cannot be recovered, the receiver sends a negative acknowledgement and the sender retransmits the packet with a more powerful FEC code. This cycle continues until the packet is successfully delivered.

Data suppression and aggregation mechanisms try to reduce the traffic load of the network by eliminating data redundancy or by combining the data coming from different sources. These strategies improve the bandwidth utilization and reduce the network congestion, the probability of collision, and the energy consumption [Krishnamachari02]. However, the application of these techniques is very application dependent. Also, the latency increases because the intermediate nodes need to wait for other packets to complete the aggregation. It should be noted that data suppression and aggregation mechanisms, and error control can be implemented in any layer of the protocol stack.

Energy saving can be counted as a primary contribution of power control to QoS provisioning. The power control adjusts the radio transmission power of the sensor nodes to the minimum power required for successful transmission [Pantazis08]. Thus, the energy efficiency is improved, as well as the channel utilization through spatial reuse. Diverse factors affect the required minimal power, such as the band frequency, the wireless channel conditions (e.g., noise, path loss, multipath fading, shadowing[10]) and the distance to the receiver. Although power control is directly related with physical layer, it has a significant impact on both MAC and network layers, because it affects the network connectivity. However, the dynamic nature of the wireless links makes the implementation of power control mechanism a challenging task.

Clustering mechanisms simplify the synchronization and coordination by grouping sets of neighboring sensor nodes. Clustering provides significant energy saving by improving sensor nodes' connectivity and reducing the transmission power, as well as facilitating data aggregation and improving the network scalability.

Adaptation mechanisms at the MAC layer provide QoS by adapting operation parameters (e.g., duty cycle, contention window size, backoff exponent) of the sensor nodes to the WSN dynamic behavior, such as number of active nodes, traffic pattern, network topology, collision probability or channel condition. For this goal, the MAC

[10] Shadowing phenomena may occur, for example, when the caregivers move around the room obstructing the direct signal path between the transmitter and the receiver.

layer needs lightweight learning algorithms to carry out the required adaptations proactively.

Differentiation based on data priority is inherent to WSNs, since it is normal to have sensors monitoring simultaneously physical parameters of distinct importance [Bhatnagar01]. So, service differentiation mechanisms are required to prioritize and differentiate the traffic flows based on pre-defined criteria.

3.3.1 Service Differentiation

In order to provide service differentiation, each traffic flow is mapped to a given traffic class. Then, the MAC and network layers treat each traffic class differently by managing the resource sharing in accordance with the traffic class requisites. Thereby, service differentiation consists of two phases: (*i*) priority assignment; and (*ii*) differentiation between priority levels.

Priority assignment can be static or dynamic. In static mode, depending on the traffic class or source type, the priority is assigned to a packet when it is generated and never changes until its destination. In dynamic mode, packet priority may vary during the delivery. Diverse criteria have been proposed for dynamic prioritization, such as remaining hop count, traversed hop count, packet deadline, remaining energy of the relaying node, or traffic load.

Traffic classes can be treated differentially at the MAC layer using distinct techniques: (*i*) in contention-based medium access schemes, it can be carried out attributing shorter contention window size to nodes with high priority traffic. In this way, their medium access chance is improved relatively to the nodes with low priority traffic. For example, SASW-CR [Tan08] is a slotted Aloha-based MAC protocol that assumes all nodes in the network are classified as high or low priority, depending on the traffic they generate, and service differentiation between them is achieved by using disjoint contention windows; (*ii*) employing distinct inter-frame space (IFS) duration values for sensor nodes generating flows of different traffic classes provides service differentiation amongst them, e.g., traffic flows using shorter IFS have higher precedence. For example, PSIFT [Nguyen06] and PR-MAC [Firoze07] provide traffic differentiation by varying the IFS and contention window size for each traffic class;

(*iii*) using non-uniform probability distribution for contention slot selection also makes significant difference [Liu05]; (*iv*) the backoff mechanism reduces the probability of collision by expanding the contention duration. Thus, assigning distinct backoff exponents to different traffic classes also allows implementing service differentiation [Kim07]; (*v*) MAC protocols using error control mechanisms can provide service differentiation by changing either persistency of retransmissions or strength of the error control codes in accordance with the priority of each traffic class. For example, QoMOR [Yoon07] MAC protocol finds the minimum number of retransmissions required to achieve a certain level of frame delivery probability bounded by a maximum delay threshold; (*vi*) employing a distinct degree of aggregation for each traffic class can be a technique for service differentiation in terms of delivery latency, because latency tends to increase with the degree of aggregation [Jeong10]; (*vii*) changing the duty-cycle schedule of the sensor nodes according to their priority level. For example, RL-MAC [Liu06] changes adaptively the duty cycle of the sensor nodes based on local observations, as well as on the observations of neighbor nodes; (*viii*) changing the adaptation speed of the different traffic classes to the current network conditions according to their priority levels can also provide service differentiation. For example, the MAC protocol proposed in [Saxena08] achieves service differentiation between traffic classes by using different coefficients for each traffic class to control increase and decrease speed of the congestion window sizes. In this way, congestion window size for higher priority traffic decreases faster than the lower priority traffic.

3.4 Deterministic MAC Protocols for WSNs

Many MAC protocols developed for WSNs use contention or reservation-based techniques. As discussed before, contention-based protocols are convenient for WSNs with low traffic loads, whose nodes remain idle for a long time until an event is detected. Moreover, these protocols cannot assure reliable data delivery and deterministic delay bounds. Therefore, these protocols are inadequate for networks requiring significant traffic loads and low latency. Here, TDMA-based MAC protocols are preferable, because QoS is more easily assured in a collision-free environment. For performance

reasons, TDMA is recommended for non-dense, controlled networks, such as e-emergency WSNs.

It is presented next an overview of TDMA-based MAC protocols conceived for WSNs. The suitability of these MAC protocols for e-emergency WSNs is discussed too. MAC protocols designed for large, low data rate, event triggered WSNs are naturally unmentioned here. However, a survey covering contention-based MAC protocols for WSNs can be found in [Demirkol06].

3.4.1 TDMA-based MAC protocols

This section presents diverse TDMA-based MAC protocols developed for WSNs with deterministic requisites in terms of latency, as required in e-emergency. Since IEEE 802.15.4 [IEEE4] is used in this work as comparative MAC protocol and IEEE 802.15.6 [IEEE6] is expected to be a prominent standard for BSNs, both will be described with more detail in the following sections.

LMAC [Hoesel04] allows a WSN to self-organize in terms of time-slot assignment and synchronization without the need of a central coordinator. At the network setup, LMAC uses a random time-slot assignment algorithm that ensures that nodes at two-hop distance do not use the same time-slot. Nodes will maintain their time-slots until their battery runs out or collisions occur in their time-slot. During its time-slot, a node will always transmit a message composed of two parts: the control message and a fixed-length data unit. All nodes endeavor to receive the control messages broadcasted by their neighboring nodes to stay synchronized and to know the destination node address. If a node is not the message receiver, it will switch off the transceiver after the control message and only wakes up at the next time-slot to avoid listen to the data unit. During each time-frame, the message is forwarded one hop towards the gateway. Since a time-slot can be controlled uniquely by one node, a node can transmit only one message per time-frame. This rigidity makes LMAC inadequate to networks operating in multi-state conditions, as required in e-emergency. Also, nodes must always listen to the control messages of all slots in a time-frame even if time-slots are unused, and it is not easy to guarantee that nodes at three-hop distance do not interfere mutually at all.

PEDAMACS [Ergen06] aims to achieve both energy efficiency and delay guarantee. It considers that the BS can reach all nodes in one hop. This allows the BS to synchronize the nodes and to schedule their transmissions and receptions. Also, it assumes that nodes generate packets periodically. Since most sensor nodes cannot reach the BS directly to inform it about their communication demands, PEDAMACS includes a special initialization procedure. First the BS sets up a spanning tree and then nodes report back about their local topology (parent, children, and others) and anticipated data rate (periodic reporting) using CSMA. Once all this information has reached the BS, it knows the full topology and can compute a collision-free global schedule, which it broadcasts out to the complete network. Then the data collection phase starts and nodes receive and send messages according to that schedule. Time-slots are long enough to carry one data packet. As every transmission is scheduled beforehand, PEDAMACS has no data packet retransmission mechanism in the data collection phase. However, transmission errors due to interferences, distortion, or noise may occur in a wireless network, as well as transmission collisions due to time synchronicity failures. Thus PEDAMACS is unsuitable for networks demanding QoS in terms of packet loss.

VTS [Egea-López08] was developed inspired on the canonical S-MAC protocol [Ye02]. VTS provides a TDMA access scheme, in which the number of slots is equal to the number of nodes in the cluster. Nodes transmit data packets in different time-slots using CSMA/CA. In a cluster with *m* nodes, a node can only send a packet every *m* slots. The superframe length is adjusted dynamically as nodes join and leave the cluster. A sink node adjusts the duty cycle to control the latency. VTS gives timeliness guarantees, but presents energy inefficiency because all sensors at the beginning of each time-slot wake up and listen to control packets. Robustness against interferences and reconfiguration mechanisms are not considered too.

I-EDF [Caccamo02] protocol organizes the static nodes in hexagonal cells with a router node in their centers equipped with two transceivers. Each cell operates at a frequency different from all of its neighbors. All nodes of a cell are time-frame synchronized and follow the earliest-deadline-first algorithm. Packets with the closest deadline are transmitted first to guarantee bounded delay. Inter-cell communication is supported by a synchronized TDMA scheme and the messages are ordered by their earliest deadlines too. The FDMA-TDMA scheme offers a collision-free solution. However, it assumes that only a single constant size packet can be sent during each time-frame, the inter-cell/intra-cell time-frame pattern are initially pre-defined and unmodified

at run-time. This rigidity makes it unsuitable for e-emergency WSNs. Robustness against interferences and energy efficiency are not considered too, and channel assignment needs to be carefully handled to avoid interference between neighboring cells.

Dual-mode MAC [Watteyne06] protocol uses more relaxed assumptions than I-EDF. The goal is to guarantee deterministic transmission time compatible to application deadline. A linear network is considered with identical nodes deployed roughly along a line. Two modes are provided: protected and unprotected modes. First, the unprotected mode is started. It does not employ cellular structure and collisions are possible. As soon as a collision occurs, the protected mode which adopts the cellular network structure with globally synchronized TDMA is used to offer collision-free transmission. Switching between two modes, the protocol is able to provide worst case delay bound and also good performance if traffic load is low. However, this last condition is not true in e-emergency WSNs. Moreover, this protocol does not fit in e-health WSNs, because their topologies are not linear.

CR-SLF [Li05] schedules messages by carefully exploiting spatial channel reuse for each per-hop transmission to avoid collisions. The set of message transmissions is partitioned into disjoint sets such that transmissions within each set do not interfere with one another and can be executed in parallel. A central coordinator cognizes the message deadlines at each hop and schedules the messages so that deadline misses are minimized. As the deadline is not assured, CR-SLF is not suitable for e-emergency WSNs.

Bluetooth [IEEE1] organizes nodes into piconets with one master and up to seven data service slaves. Communications use frequency-hopping and time division duplex medium access techniques. In active mode, a slave listens to the channel for master transmissions at all times. On receiving a packet from the master, every active slave reads the destination slave address and packet length from the packet header. If the packet is not addressed to a slave, it stops scanning the channel for the duration of the packet length announced in the packet header. The addressed slave will reply in the following reverse slot. If the master has no data to send during a slot when it polls a slave, it sends a null packet; the slave replies to the packet received from the master since the reply contains an acknowledgement for the received packet. In addition to the active mode, there are three low power modes. The fact that Bluetooth needs a master continuously polling its slaves in active mode, and the low number of supported active slave nodes limits its application in e-health.

RRMAC [Kim08] is based on the IEEE 802.15.4 superframe structure. Cluster-heads aggregate data collected from their nodes and forward the data to the ascendant cluster-head. Only upper level cluster-heads have dedicated time-slots in the TDMA superframe. Low latency is achieved by assigning subsequent slots to the nodes that are successive in the data transmission path so that data can quickly flow from the leaves to the sink through the convergecast tree structure. It assumes that the small transmission range of sensor nodes enables sensors in one cluster to transmit packets to their parent node, while other sensors in a different cluster are transmitting packets to their parent nodes. However, this assumption is not easy to guarantee when the BSN clusters of several patients share the same clinical room.

LPRT [Afonso06] is a MAC protocol for star topology, single-hop networks. It uses a highly-grained superframe and the allocation of time-slots is announced explicitly in the beacon sent by the BS. Data frames transmitted by the first time are acknowledged by the beacon of the next superframe. LPRT uses relatively large size beacons, a single retransmission procedure, and data is only transmitted in the superframe if the corresponding beacon is received. These three characteristics may lead to a significant packet loss, if communications occur in a wireless channel with an appreciable bit error ratio. Also, no mechanism is available to reconfigure the WSN dynamically.

CICADA [Latré07] is a slotted protocol for BSNs that uses a cross-layer approach where MAC and routing traffic are handled in the same spanning tree to increase throughput, and reduce delay and energy dissipation. The spanning tree is set up autonomously across the sensor nodes placed in the patient's body and is used to route the data toward the sink. Traffic from the sink to the nodes is not supported, and so the sink cannot reconfigure the BSN. Moreover, CICADA is not a protocol planned for e-health WSNs with multiple patients coexisting in the same area.

GinMAC [Suriyachai10] provides QoS support by assuring deterministic delay bounds and reliability. Time is divided into epochs (i.e., time-frames). In each epoch, a sensor node has k exclusive slots for single data-ACK message exchange. All k slots are used for retransmission until a successful packet delivery occurs, upon receiving an ACK frame. Packet delay is bounded by the duration of an epoch. If a sensor node does not have any data to send in an epoch, it sends a control message at the first reserved time-slot indicating the fact. To obtain maximum temporal distance in order to mitigate channel burst errors, k retransmission time-slots are distributed through the epoch. Energy consumption is reduced due to the use of different duty cycles for each sensor

node depending on the number of child nodes in the predetermined data gathering tree. However, since each node synchronizes its clock with its parent node, synchronization errors can be propagated. Also, each node must be aware of its position in the data gathering tree for slot assignment and duty cycling. GinMAC is conceived for WSNs requiring small size packets (4 B), maximum sampling frequencies of 1 Hz, and transport delays up to 1 s. Consequently, it is not appropriate for e-emergency WSNs.

TSMP [Pister08] is a multi-hop medium access and networking protocol presenting low power consumption, network-wide time synchronization, channel hopping, dedicated slotted unicast communication bandwidth, link-layer acknowledgements, mesh graph-based routing, and multi-layer security on every packet. It uses time synchronization to schedule collision-free frequency-hopping communication. A central network manager calculates optimal routes and assures that each channel can be used without concern for collisions or wasteful overhearing of packets. TSMP guarantees an upper delay bound and ensures routing reliability with a mesh topology. It also employs FDMA and channel hopping techniques. Different links use distinct frequencies (FDMA) and the same link hops pseudo-randomly over a set of channels. This yields high robustness against interference and other channel impairments. Tests in industrial environments have shown packet delivery ratio above 99.9% for an average traffic rate of *circa* 1.5 packets/s (delay bound is not mentioned). Although TSMP supports different time-varying traffic patterns, time-slots are fixed and long enough (*circa* 10 ms) to allow a sender to transmit the maximum length packet and receive the respective acknowledgement, which results in poor bandwidth efficiency.

3.4.2 IEEE 802.15.4

IEEE 802.15.4-2003 [IEEE4] specifies the physical layer and the MAC layer for low data rate WSNs. The MAC sub-layer can operate either in CSMA-CA or in superframe structure. In this operation mode, the format of the superframe is defined by the coordinator. The superframe is bounded by network beacons sent by the coordinator and is divided into sixteen equally sized slots. The beacon frame is transmitted in the first slot of each superframe. The beacons are used to synchronize the attached devices, to identify the WSN and to describe the structure of the superframes. This is composed of the contention access period (CAP) and contention free period (CFP). The CFP always

appears at the end of the active superframe starting at a slot boundary immediately following the CAP.

Any device wishing to communicate during the CAP competes with other devices using a slotted CSMA-CA mechanism. A sufficient portion of the CAP remains in every superframe for contention-based access of other networked devices or new devices wishing to join the network. All contention-based transactions must be completed before the CFP begins.

For low-latency applications or applications requiring specific data bandwidth, the network coordinator may dedicate portions in the CFP. These portions are called guaranteed time-slots (GTSs)[11]. Only a network coordinator can assign GTSs to its sensor nodes. A sensor node transmits to the network coordinator a MAC command requesting some GTSs and, if available, the BS responds granting the number of superframe time-slots requested by the sensor node. GTSs expire if unused during a few consecutive superframes. The network coordinator may allocate up to seven of these GTSs, and a GTS may occupy more than one slot period. No transmissions within the CFP shall use a CSMA-CA mechanism to access the channel. If a single transmission attempt in the GTS has failed, the device shall repeat the process of transmitting the packet and waiting for the acknowledgment, up to a maximum number of retries. A device transmitting in the CFP shall ensure that its transmissions and requested acknowledgments are completed before the end of the GTS.

IEEE 802.15.4 offers the advanced encryption standard (AES) algorithm with 128-bit keys to guarantee message integrity and privacy and to perform authentication.

The low granularity of the GTSs (seven) leads to poor bandwidth efficiency. Such low number of time-slots hardly suits in an e-emergency WSN with multiple patients.

3.4.3 IEEE 802.15.6

The IEEE 802.15.6 standard will operate in star topology using beacon and non-beacon mode. In beacon mode, beacon frames are transmitted by the central coordinator in each beacon period of the superframe. Beacons contain no information about the sensor nodes' allocation, but provide information about timing and the superframe

[11] IEEE 802.15.4-2006 makes optional the GTS support.

structure, and information for unconnected sensor nodes to join the network. The superframe is divided into two exclusive access phases (EAP1, EAP2), two random access phases (RAP1, RAP2), one managed access phase (MAP), and one contention access phase (CAP), as shown in Figure 3.1. In EAP, RAP and CAP periods, sensor nodes contend for resource allocation. The EAP1 and EAP2 are used for highest priority traffic. The RAP1, RAP2, and CAP are used for regular traffic. The MAP is used for allocating time-slots. In non-beacon mode, there is only the MAP. Depending on the application requirements, the coordinator can eliminate any of those periods. The duration and the starting location of the phases are completely programmable.

The access mechanisms used in each period of the superframe are divided into three categories: (*i*) random access mechanism (beacon mode only), which uses either CSMA/CA (the length of the contention window depends on the user priorities) or a slotted Aloha procedure for resource allocation; (*ii*) improvised and unscheduled access (connectionless contention-free access in beacon and non-beacon mode), which uses unscheduled polling/posting for resource allocation; (*iii*) scheduled access (connection-oriented contention-free access in beacon and non-beacon mode), which schedules the allocation of time-slots in one or multiple upcoming superframes [Kwak10]. For scheduled access, all the necessary information is communicated during the connection setup. A sensor node specifies its bandwidth and power management requirements and the coordinator returns the respective usage parameters. Therefore, sensor nodes can only use the resources allocated during the connection phase, and so it does not allow a transparent dynamic reconfiguration of the network.

The MAC layer also provides an optional two-hop star network extension and a security mechanism.

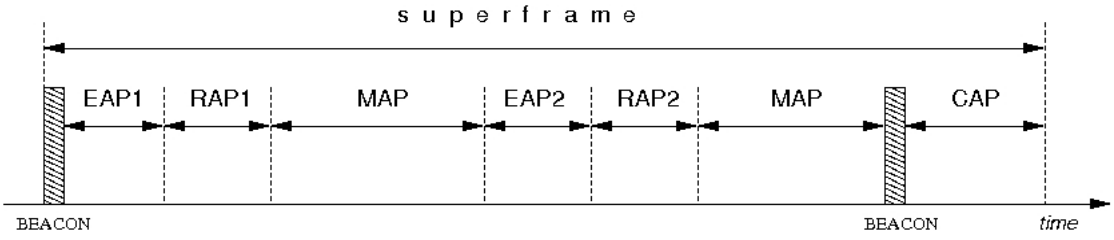

Figure 3.1 – Superframe structure in IEEE 802.15.6.

3.5 Need for a new MAC protocol

A MAC protocol for e-emergency WSNs should present preferably the following properties (see Chapter 1):

- *adaptability*: capacity to reconfigure promptly the network operating parameters;
- *coexistence capacity*: capacity of coexisting close-neighbor BSNs in the same channel;
- *robustness*: capacity to improve the data transmission reliability against communication failures;
- *bandwidth efficiency*: capacity of allocating just the required bandwidth to a sensor node;
- *power efficiency*: capacity to control the energy consumption;
- *two-tier operability*: capacity of the WSN to operate in two-tier network structures;
- *timeliness*: capacity of guaranteeing controlled packet delivery delay;
- *scalability*: capacity of the network performance do not deteriorate significantly with the admission of new patients;
- *fairness*: capacity of treating with equity traffic flows of identical priority and requiring the same network resources.

Attending to the multiple MAC protocols available and to allow a comparative qualitative analysis, Figure 3.2 illustrates the relative positions of the surveyed protocols in the previous section regarding the presented e-emergency properties. The left diagram relates adaptability, coexistence capacity (assuming that BSNs monitor at least five independent physiological signals, cf. Section 2.3.4), and robustness. The right diagram relates bandwidth efficiency, power efficiency, and two-tier operability[12]. The label TRUE means that the protocol provides the specific attribute, and the label FALSE otherwise.

[12] Timeliness and fairness are not considered. In TDMA-based MAC protocols, delay can be predicted and fairness is assured, because time-slots are assigned to nodes in each superframe.

Preferably, MAC protocols for e-emergency WSN should be positioned in the green cube of both figures in order to fulfill e-emergency requisites. As observed, none of the surveyed protocols is able to accomplish such goal[13]. This gap motivated the design of the new Adaptive and Robust MAC (AR-MAC) protocol.

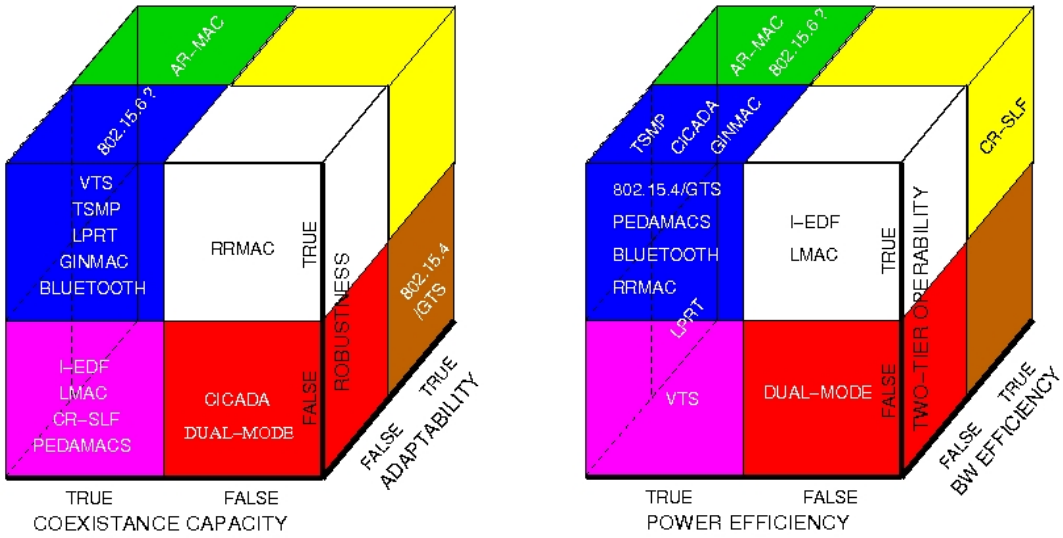

Figure 3.2 – Comparison of deterministic MAC protocols.

3.6 Summary

This chapter has discussed several aspects related to medium access control design in wireless media. It was argued that MAC protocols based on reservation techniques are preferable to random access schemes for networks requiring high-traffic loads and low latency, such as e-emergency WSNs. Also, TDMA-based networks are more power efficient, since nodes may enter in inactive state until their scheduled time slots. For these reasons, diverse MAC protocols currently available for WSNs with timing deterministic properties were overviewed, namely LMAC, PEDAMACS, VTS, I-EDF,

[13] The final publication of the IEEE 802.15.6 standard is expected to occur in January 2012. Since the definitive specifications are not yet available, the position of this protocol in Figure 3.2 should be regarded with precaution. For this reason, IEEE 802.15.6 presents a question mark.

Dual-mode, CR-SLF, Bluetooth, IEEE 802.15.4, IEEE 802.15.6, RRMAC, LPRT, CICADA, GinMAC, and TSMP. As explained, these protocols for diverse reasons fall short meeting the properties required by e-emergency WSNs regarding adaptability, coexistence capacity, robustness, bandwidth efficiency, power efficiency, and two-tier network hierarchy support. This lacuna has motivated the design of the new MAC protocol proposed in the next chapter.

Chapter 4

AR-MAC Protocol

4.1 Introduction

Within WSN context, e-emergency networks are characterized by requiring QoS guarantees to provide a reliable and timely data delivery for a useful clinical diagnostic. Reconfiguration is another desirable feature of e-emergency WSNs in order to allow handling distinct clinical situations of patients. Moreover, e-emergency WSNs must be energetically efficient to operate autonomously for a long time period and should be scalable to admit new patients. Other desirable requisites include coexistence capacity, bandwidth efficiency, and operability in two tier network structures. All these aspects must be considered when choosing a MAC protocol for an e-emergency WSN. As discussed in the previous chapter, the real-time MAC protocols available for WSNs are not capable of fulfilling integrally those requirements. In order to cover this shortage, the next section introduces the Adaptive and Robust MAC (AR-MAC) protocol. This protocol presents original concepts and is conceived for e-health WSNs requiring efficient bandwidth allocation, coexistence, low energy consumption, bounded latency, data transmission robustness, and adaptability.

AR-MAC includes a new network reconfiguration scheme, so that a WSN may react optimally in accordance with the patients' clinical state. The reconfiguration algorithm is described in Section 4.3. In a network using a reservation-based MAC protocol, a sensor node needs to know which time-slots in the superframe may use to transmit collision-free data. Knowing that patients of an e-emergency WSN are normally monitored by the same number and type of sensor nodes, originating a regular traffic pattern, a distributed and collaborative time-slot allocation algorithm is also introduced in Section 4.4. The AR-MAC frame formats are presented in Section 4.5.

4.2 AR-MAC Protocol Description

AR-MAC is an adaptive and robust protocol that inherits some concepts from the IEEE 802.15.4 and LPRT, namely the contention access period (CAP), the contention free period (CFP), the normal transmission period (NTP), the retransmission period (RP), the non-active period (NAP), and the NTP acknowledgment (ACK) bitmap. However, AR-MAC introduces novel concepts and features to meet required e-

emergency requisites, as discussed in the next section. According to the classification scheme proposed in Figure 3.2 (see Section 3.5), AR-MAC is expected to occupy both green cubes in the diagram.

AR-MAC is based on the TDMA scheme to assure that the channel can be used without concern for collisions or wasteful overhearing of packets. AR-MAC is centrally coordinated in order to provide controlled packet delivery delays and low-power connectivity. Also, the BS can have a global view of the network, which is essential for WSN reconfiguration purposes and to ensure fairness. Centralized network management may be criticized for presenting problems regarding scalability, robustness, and network-wide synchronization. However, it is shown in [Pister08] with real deployment tests that these criteria can be met in a managed network with a centralized controller that coordinates the communication schedule for the multi-hop network.

4.2.1 AR-MAC Design Goals

A MAC protocol for e-emergency WSN should exhibit diverse properties, so that applications can benefit from improved service quality. Adaptability, robustness, coexistence capacity, bandwidth efficiency, timeliness, power efficiency, scalability, fairness, and two-tier operability are desirable properties for MAC protocols operating in emergency or intensive care units with several patients (see Chapter 1). In order to reach these design goals, AR-MAC protocol uses diverse innovative solutions, as explained in the following.

Adaptability is achieved through a dynamic reconfiguration scheme and an automatic channel switching mechanism. The former reconfigures the WSN when a change of context occurs. The latter switches the channel frequency when it detects unacceptable transmission conditions in the operating channel.

To improve communication robustness, an array of short-size beacons is sent at the start of each superframe to reduce the beacon loss probability. A strategy based on colors attributed to superframes and sensor nodes contributes to enhance robustness, by reducing the number of transmissions and releasing bandwidth for eventual retransmissions. Data packets may be retransmitted in specific periods in accordance with the acknowledgement bitmaps transmitted in the beacon. The channel switching mechanism also contributes to improve robustness, because it looks for low interference

channels. High-grained superframes may also improve robustness, because bandwidth saving increases the retransmission capacity.

To afford bandwidth efficiency, high-grained, colored superframes are used. Specific bitmaps, regarding the activity and criticality status of sensor nodes, are also used to optimize the bandwidth utilization.

Timeliness is provided by the use of colored superframes and retransmissions performed in specific time periods.

Power efficiency is achieved putting sensor nodes in sleeping mode when they are not communicating and using strategies based on colors and short-size beacons. The channel switching mechanism also improves power efficiency by avoiding interferences, thus reducing the number of retransmissions. To shorten the beacon size, the time-slot assignment is carried out using a distributed slot allocation algorithm.

Network scalability is pursued with the use of high-grained superframes, colored superframes, activity bitmap, and cluster-mode operation.

solutions, strategies	**design goals**							
	adaptabi-lity	robustness	coexistence capacity	bandwidth efficiency	power efficiency	timeli-ness	two-tier operability	scalability
centralized network	●	●						
high-grained superframe		●	●	●		●		●
NRP				●		●		
NTP ACK bitmap		●		●				
ERP		●		●		●		
NRP ACK bitmap		●		●				
criticality bitmap				●				
activity bitmap				●				●
coloring scheme		●		●		●		●
short-size beacons		●			●			
distributed slot allocation		●	●		●			
reconfiguration scheme	●							
channel switching	●	●			●			
cluster mode operation			●		●		●	●
beacon array		●						

Table 4.1 – Solutions and strategies included in AR-MAC to pursue the design goals. Innovative features are shown in bold italic.

Coexistence capacity is provided through a collaborative and distributed algorithm that schedules dedicated time-slots to sensor nodes in the high-grained superframes.

The operation in cluster mode offers the ability of forwarding frames in two-tier network structures, which improves the power efficiency and the scalability of the WSN.

The AR-MAC design goals and the innovative solutions used to achieve them are summarized in Table 4.1. All these aspects are discussed in detail in the next sections.

4.2.2 AR-MAC in One-hop WSNs

AR-MAC uses high-grained superframes to maximize the bandwidth efficiency. It requires one BS to provide timely data delivery, low-power connectivity, and a global network view for reconfiguration purposes and fairness assurance.

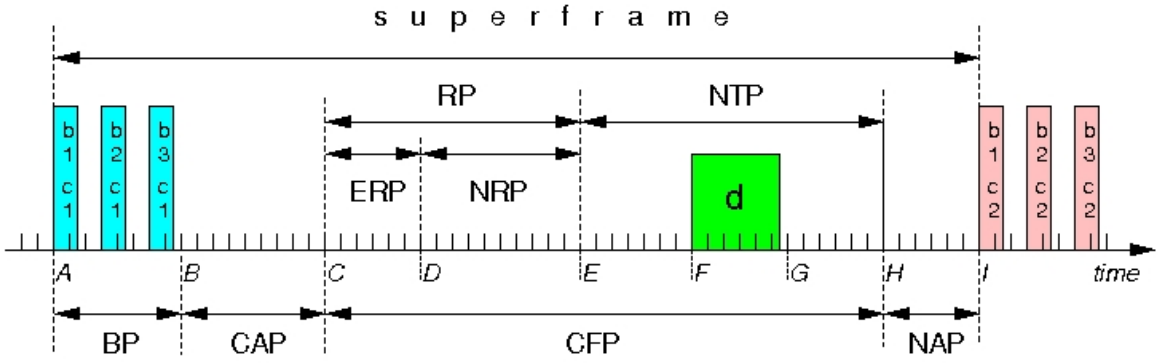

Figure 4.1 – Superframe structure in the AR-MAC protocol.

Beacon Period. As shown in Figure 4.1, the superframe starts with the Beacon Period (BP). The BS broadcasts a new beacon frame in every BP. Beacon frames are used for sending data to sensor nodes, synchronizing and announcing the WSN. To improve the probability of a sensor node receiving the beacon, the BS transmits a sequence of redundant beacon frames $b_1 \ldots b_n$ equally spaced in time with consecutive beacon numbers. Since a superframe always starts with the transmission of the first beacon, the beacon number of the received beacon allows a sensor node to

resynchronize easily with the WSN. After receiving a beacon, the sensor node turns off the transceiver to avoid receiving the next redundant beacons, thus saving energy. If a sensor node does not receive a beacon during *maxLostBeacons* (sixteen) consecutive superframes, it must leave the WSN.

CAP. This period follows the BP. The slotted-CSMA algorithm [IEEE4] is used in the CAP. The CAP may be used for sending MAC commands and responses, which are used, for example, to allow sensor nodes to associate with or disassociate from a WSN. It may also be used to convey low transmission duty-cycle traffic, such as temperature data. The last time-slot of the CAP is announced in all beacon frames.

CFP. This period uses TDMA and is composed of the Normal Transmission Period (NTP) and the Retransmission Period (RP). The NTP is used for sensor nodes to transmit new data. Lost data are retransmitted in the RP, which is composed of the Normal RP (NRP) and the Extra RP (ERP). Data packets transmitted to the BS during NTP are acknowledged through the NTP ACK bitmap present in the beacon of the next superframe. The BS sends the NTP ACK bitmap only if one or more packets failed to be transmitted in the NTP of the last superframe. Unacknowledged packets in the NTP ACK bitmap are retransmitted in the NRP of the current superframe. Data packets sent in the NRP are acknowledged through the NRP ACK bitmap broadcasted in the next superframe, as described in the following topic. Data packets not acknowledged by the NRP ACK bitmap are retransmitted once in the ERP. NRP and/or ERP are present in a superframe only if retransmissions are required in the respective periods. As the RP size varies along the superframes in accordance with the number of required retransmissions, the CAP size varies from a predefined minimum size (*minCAPLength*) to a maximum value imposed by the NTP size. If a sensor node does not receive any beacon during the BP, it may continue to send its new data in the NTP, since a sensor node's clock drift in the order of microseconds allows the WSN to continue synchronized during a few consecutive beacon intervals. However, a sensor node cannot retransmit data in the RP because the ACK bitmaps are not available, and so it does not know how the RP time-slots are being allocated to the others sensor nodes. As the timers of the sensor nodes are imprecise, a small number of safeguard slots are required to avoid the superposition of adjacent transmissions.

NRP ACK bitmap. To show the use of the NRP ACK bitmap, let us consider a superframe without retransmission requests from the BS and that some critical data packets were lost during NTP. The lost packets are identified through the NTP ACK bitmap sent in the beacon of the next superframe. According to this bitmap, sensor nodes retransmit the lost data packets once in the NRP, independently of being critical or not. Then, critical data packets are retransmitted as many times as possible in the remaining available slots in the NRP. These available slots must be fairly distributed through the sensor nodes with critical data packets to retransmit. A sensor node stops the retransmission trials after receiving the ACK frame. Only critical data packets are acknowledged, except in the last retransmission. If critical data packets fail to be retransmitted in the NRP of the superframe, then the BS includes the NRP ACK bitmap in the beacon of the following superframe. So, critical data packets may be retransmitted once again in the ERP, improving the probability of being delivered. The BS sends the NRP ACK bitmap only if one or more critical packets failed to be retransmitted in the NRP of the last superframe.

The set of time-slots needed for a sensor node to send a data packet and, if required, to receive the ACK frame, is called super time-slot. For example, in Figure 4.1 the set of time-slots from *F* to *G* is the super time-slot used to send the packet *d*. The NRP ACK bitmap concept was introduced for the sake of bandwidth saving and time-slot allocation fairness in the NRP. Indeed, if two super time-slots were reserved in advance for critical data packets, the second super time-slot would be wasted if the retransmission in the first super time-slot was successful. In this case, bandwidth within NRP is inefficiently used, possibly preventing other sensor nodes from retransmitting due to unavailability of slots. The use of the NRP ACK bitmap mechanism may contribute to increase the delay, although keeping it controlled and bounded to a maximum value. In fact, the maximum packet delay is always below twice the superframe duration.

Out-of-sequence packets may also arrive to the BS, i.e., AR-MAC does not guarantee in-order delivery. If a critical data packet P_1 from sensor node *M* fails to be retransmitted in the NRP of superframe *S*, it has to wait for the next superframe for a new retransmission trial in the ERP. Meanwhile, a critical data packet P_2 from sensor node *M* may be successfully transmitted in the NTP of superframe *S*. So, P_1 may arrive after P_2 to the BS. In such cases, the upper protocol layers must assure reordering of data packets.

NAP. The non-active period follows the NTP. No communication takes place in the NAP between the BSN coordinator and the sensor nodes. The NAP is absent in the superframes of one-hop WSNs, but it may be present in the superframes of clustered WSNs, as it will be discussed in Section 4.2.3.

Reconfiguration. A BS needs to send reconfiguration instructions in the beacon frames whenever it decides to reconfigure the WSN. This occurs if a BSN (dis)associates to the WSN or a new clinical situation is detected in some BSN. To perform this action, all sensor nodes must follow a reconfiguration scheme, as described in Section 4.3

Criticality and activity bitmaps. During the reconfiguration of a WSN, the BS announces in the beacon frames the superframe specifications and the ACK bitmaps, as well as the criticality bitmap, the activity bitmap, and the new operational parameters of some sensor nodes along with other relevant information. The criticality bitmap informs the WSN about the signals considered critical by the BS, in order to improve or protect the QoS of such signals, as the packet delivery ratio. The activity bitmap allows for the BS informing on the activity state of all sensor nodes in the WSN, so that sensor nodes are capable of optimizing the time-slots utilization without bandwidth waste. The BS considers a sensor node inactive if it does not receive data from that sensor node after a number of consecutive superframes. The BS also uses the activity bitmap to inform specific sensor nodes for not transmitting data. A sensor node can only transmit data when the respective activity flag is set.

Time-slots assignment. The BS only sends the superframe specifications and the ACK bitmaps during the steady state of the network. As the BS does not assign directly the time-slots to the sensor nodes, these must run a distributed algorithm to compute which time-slots should be used to (re)transmit data without interfering with each other, in accordance with a predefined order schema. This topic will be thoroughly discussed in Section 4.4.

Critical traffic protection. To protect and improve data delivery of critical traffic, AR-MAC adopts the following rules: (*i*) the BSNs in emergency state may retransmit *P* times in the NRP and once in the ERP; (*ii*) if there is no BSN in emergency state, then BSNs in steady state may retransmit *P* times in the NRP and once in ERP; and (*iii*) if

there is at least one BSN in emergency state, then BSNs in steady state may retransmit N times in the NRP and none in ERP, with $N < P$. This retransmission policy tends to improve the QoS of the critical traffic at the cost of QoS degradation of the non-critical traffic.

Channel switching. To improve data transmission robustness against external wireless interferences, AR-MAC may operate in channel-switching mode. A channel is used by the WSN while the interference degree is acceptable; otherwise a new free channel must be allocated. For this purpose, the BS requires an expeditious method to evaluate the interfering degree in the operating channel. A light-computing method is to take this information from the NRP usage and ERP usage parameters.

The NRP usage of a superframe expresses the percentage of sensor nodes, regarding the total number of active sensor nodes in the WSN, which failed to deliver a data packet during the NTP of that superframe. As the NRP usage parameter can be directly inferred from the NTP ACK bitmap broadcasted in the next superframe, no additional significant computational load is required to the BS. Identically, the ERP usage parameter of a superframe expresses the percentage of sensor nodes, regarding the total number of active sensor nodes in the WSN, which failed to deliver a data packet during the ERP of that superframe, in accordance with the NRP ACK bitmap broadcasted in that superframe. No significant computational load is imposed additionally to the BS in order to calculate this parameter. The NRP usage parameter allows evaluating the interference level on the wireless channel. The ERP usage parameter takes additionally into consideration the AR-MAC robustness capacity against interferences, as it will be seen in Section 7.3.3.8. The information collected from both parameters improves the ability of the BS to decide correctly about the channel switching need.

Channel switching algorithm. In order to switch dynamically the communication channel, the Time to Change (TtC) flag present in the MAC header of AR-MAC is used, as explained in the following.

Let us assume that the BS decides to change the channel. The BS initializes TtC to *maxLostBeacons* and broadcasts the new channel. After sending the beacon, the BS decreases TtC by one. When receiving a beacon with TtC not null, sensor nodes save the TtC value. If a sensor node does not receive a beacon, it needs to decrease by one the saved non-zero TtC to keep synchronism with the BS. If TtC is one, then the sensor

nodes and the BS must change to the new channel at the beginning of the next superframe. Then, the BS sends beacons with TtC equal to zero until the next channel change. The time required to change channel is always the product of *maxLostBeacons* and beacon interval.

Coloring scheme. Sensor nodes with low sampling rates and flexible time delays should not transmit in every superframe in order to save energy and free time-slots for retransmissions, thus contributing to improve data delivery robustness. To implement this strategy, a coloring scheme of C colors is applied to sensor nodes and superframes. In this scheme, each color assumes a value 2^k (with $0 \leq k < C$), that represents a reference threshold for transmission purposes. The color of each sensor node is constant during the steady state operation and can only be changed through a reconfiguration procedure. If $C > 1$, the color of a superframe changes successively along the time in a round-robin fashion. For instance, if a superframe is of color 2^k, the next superframe will be of color 2^{k+1}, and when k equals to C, k becomes zero. When the BS sends a beacon of color 2^k, all sensor nodes with color not above 2^k may transmit in the current superframe. So, sensor nodes can only transmit in superframes with the same or a superior color. Regarding retransmissions, a sensor node of color 2^k may resend a lost packet in the NRP of the superframe of color 2^{k+1} or in the ERP of the superframe of color 2^{k+2}, respecting the round-robin color scheme. The color c of a superframe is identified in the beacon header, as shown in Figure 4.1, where beacons of two colors are represented.

Short-size beacons. Taking advantage of the fact that the patients of an e-health WSN are normally monitored resorting to the same number and type of sensor nodes, beacons only carry essential data for the proper operation of the WSN during its steady state (namely the superframe specifications and the ACK bitmaps). These essential data must enable all sensor nodes in the WSN to find implicit and unambiguously their time-slot allocation in the CFP. As sensor nodes receive short-size beacon frames, the power saving in each BSN is improved. Also, the beacon delivery probability increases because the beacon frame is less exposed to interferences, and consequently the performance of the WSN improves too. Simulation tests confirmed the validity of this hypothesis, as described next.

4.2.2.1 WSN performance with Short-Size Beacons

In order to study the impact of the beacon size in a WSN, evaluation tests were carried out using AR-MAC configured with one beacon per BP, two retransmissions at most in the NRP and none in the ERP. The channel was simulated with the bit error ratio (BER) model. This is the channel model used, for example, in TOSSIM [Levis03]. It was assumed an equal BER in both communication directions. The results are presented in Figure 4.2. It shows the packet loss ratio considering the probability of a fully-loaded IEEE.802.15.4 packet being delivered, for beacon frame payloads of 4B, 36B, 68B, and 100B. The probability P of a fully-loaded IEEE.802.15.4 packet being delivered is related with the channel BER through the expression:

$$BER = 1 - P^{1/(8.MPPS)} \quad (4.1),$$

where MPPS is the maximum physical packet size. Knowing that MPPS is 133 B, the BER changes between 0 and around 6.5×10^{-4} as P decreases from 1 to 0.5 along the simulation runs. It is observed in Figure 4.2 that as the beacon payload becomes larger, the beacon loss probability increases, and so the packet loss ratio.

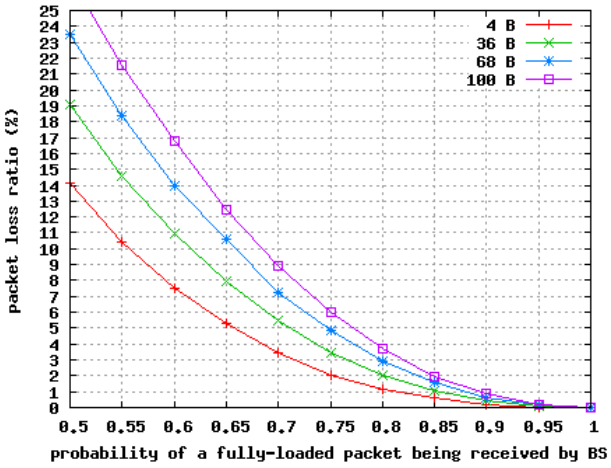

Figure 4.2 – Packet loss ratio for several beacon payload sizes.

4.2.2.2 AR-MAC State Transition Diagram

To provide a clear view of the AR-MAC operation in a one-hop WSN, Figure 4.3 illustrates the main protocol state transitions occurred in both a BS and a sensor node, considering a WSN operating in single color mode.

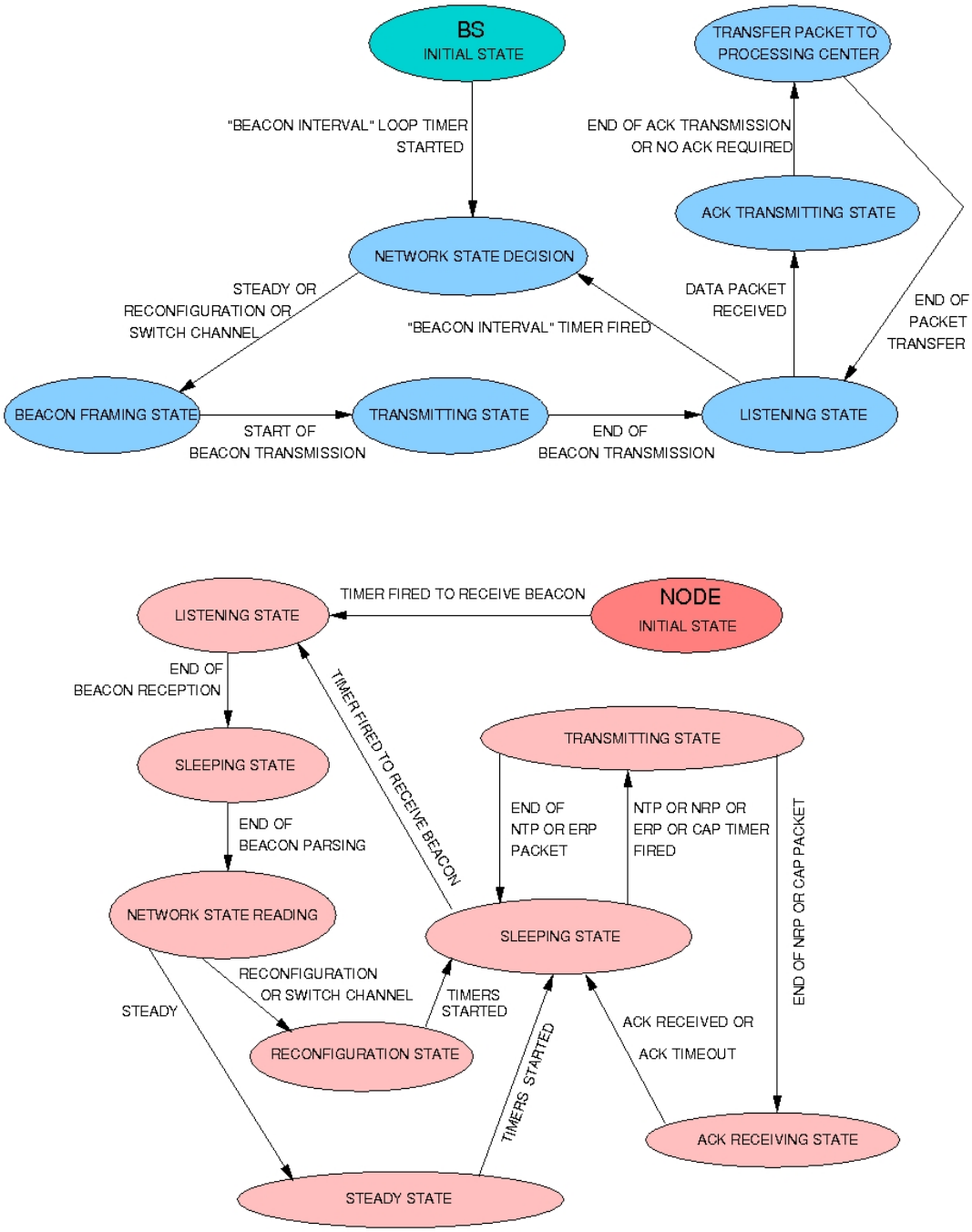

Figure 4.3 – Simplified state transition diagram of BS (up) and sensor node (down).

4.2.3 AR-MAC in Clustered WSNs

In one-hop WSNs the BS is the receiver of all sensor data transmissions. However, as mentioned in the previous chapter, such direct transmission may not be feasible nor energy efficient. Accordingly, AR-MAC is also designed to operate in clustered WSNs. An e-health WSN is typically a clustered network, since each BSN may form a cluster. In such cases, sensor nodes of each BSN send data to the respective cluster-head node, which can be a sensor node of the BSN or a portable device (e.g., PDA). Then, the cluster-head forwards the received data, eventually aggregated, to the BS. This strategy is adopted, for example, in the project SENSATION, as exemplified in Figure 4.4.

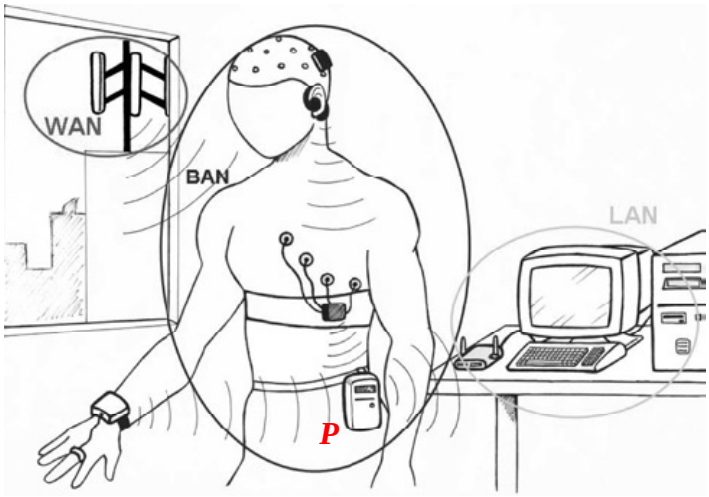

Figure 4.4 – A BSN with a portable device *P* operating as cluster-head [Montón08].

Since neighbor clusters should operate in distinct wireless channels to avoid inter-cluster interferences, AR-MAC in clustered WSNs uses a combination of TDMA and FDMA techniques. Clusters that do not interfere mutually may operate in the same channel (spatial reuse). Sensor nodes communicate with the cluster-head and cluster-heads communicate with the BS using AR-MAC for one-hop networks. Clusters should use superframes with CAP to allow the (dis)association of sensor nodes. The active period of the cluster superframe must occur during the CAP of the ascendant cluster superframe. As both superframes occur in distinct channel frequencies, the transmissions in these time periods do not interfere mutually. Clusters must only have a few sensor

nodes to guarantee that the cluster-head can receive data from all sensor nodes in the limited active period. Also, the superframe active period of a cluster becomes shorter as its level in the tree decreases. Next, it is described how AR-MAC works in a two-hop network. The discussion could easily be extended to a larger multi-hop network. However, delay bounds and synchronization aspects inherent to real WSNs impose limitation in the number of hops.

Let us consider a network with the clusters grouped hierarchically in a two-level tree. The second level of the tree holds the leaf sensor nodes monitoring the physical signals. The first level is composed of the sink sensor nodes of the leaf sensor nodes. A sink sensor node may also monitor a physical signal. After receiving a beacon from the BS during the BP, the cluster-head switches the radio to the channel frequency of its cluster, as shown in Figure 4.5. For simplicity, only one beacon frame is represented in the BP of the first and second-level superframes. Cyan-colored packets are transmitted in channel k_1, and green-colored packets are send in channel k_2. Transmitted and received packets are depicted above and below the time axis, respectively. During the CAP of the first-level superframe, the cluster-head sends a beacon at the start of the second-level superframe. During the NTP of the second-level superframe, the cluster-head collects the data packets from the leaf sensor nodes. In Figure 4.5, the cluster-head received new data from sensor nodes *a*, *b*, and *c*. Once finished the CAP of the first-level superframe, the cluster-head switches the radio frequency and delivers the aggregated data to the BS. If the aggregated data cannot be hold in a single packet, the cluster-head sends two or more data packets to the BS in the NTP of the first-level, as shown in Figure 4.5.

Each aggregated data packet sent by the cluster-head must be individually acknowledged by the NTP (and NRP) ACK bitmap. New data is transmitted to the BS in the NTP of the first-level superframe. If the cluster-head failed to deliver successfully an aggregate data packet to the BS in the NTP of the last first-level superframe, retransmission trials should occur in the NRP of the current first-level superframe. If a leaf sensor node fails to deliver a data packet to the cluster-head, the cluster-head should recover the lost data during the NRP of the next second-level superframe, as shown in Figure 4.5 with packet c_1. Then, the cluster-head retransmits the recovered data in the NRP of the current first-level superframe. If a flag in the NTP ACK bitmap does not acknowledge an aggregate data packet p it is because (*i*) the BS did not received packet p; or (*ii*) the packet p was received but the aggregate data was incomplete due to the missing data of one or more leaf sensor nodes. By analyzing the NTP ACK bitmap of

the current second-level superframe, the cluster-head can differentiate both situations and actuate accordingly.

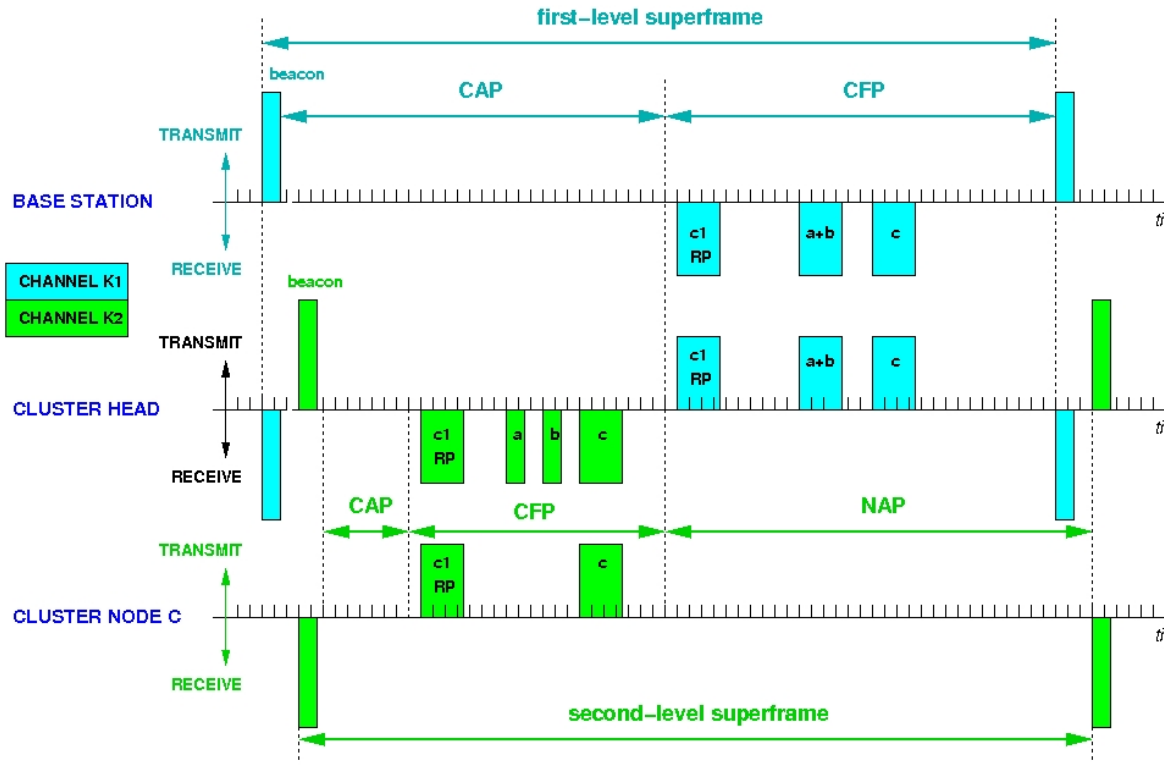

Figure 4.5 – Example of AR-MAC operating in a two-hop WSN.

AR-MAC uses a forwarding scheme presenting some similarities with RRMAC [Kim08]. However, there are important differences. In RRMAC, a sensor node communicates with its parent sensor node during the CFP of the ascendant level superframe. In AR-MAC protocol, this communication occurs during the CAP of the ascendant level superframe, not wasting the limited CFP bandwidth. In RRMAC, packets flow continuously in the tree structure from the leaf level to the base station to reduce the packet delay. This situation is difficult to implement in an e-health WSN due to the distinct traffic characteristics of the sensor nodes in a BSN. RRMAC uses a single channel and so clusters must be distanced away to not interfere with each other. This condition is not assumed in AR-MAC.

4.3 Reconfiguration Scheme

In an e-health WSN, parameters of interest may be redefined dynamically along the time in accordance with the patients' clinical state. For example, when the clinical situation of a patient changes, the application layer at the BS may need to redefine the sampling rate and the sampling resolution of diverse physiological signals, as well as the criticality degree of the patient. So, after receiving a message from the upper layer notifying the new network requisites, the MAC layer may redefine, for example, the colors to be assigned to sensor nodes or the maximum number of retransmissions trials in case of transmission failure. Also, if a BSN is associated or disassociated to the WSN, the BS may reschedule the allocation of time-slots to sensor nodes. In such cases, the WSN should leave the steady state and enter in the reconfiguration state to adapt the network to the new situation. To perform this action in a short-size beacon WSN, all sensor nodes must follow a reconfiguration scheme, because a short-size beacon only sends the superframe specifications and the ACK bitmaps. Next, it is described a new scheme conceived to reconfigure short-size beacon WSNs.

In order to control the reconfiguration process of a short-size beacon WSN, the proposed scheme uses the Reconfiguration in Progress (RiP), the Beacon Received (BR), and the Configuration Received (CR) flags. These flags are in the frame control field of the AR-MAC header (see Section 4.5). The BS uses the flag RiP to indicate if the WSN is in steady state (RiP = 0) or in reconfiguration state (RiP = 1). Sensor nodes use the flag BR to acknowledge the received beacons. According to Table 4.2, a sensor node sets BR to 1, whenever it receives a beacon; otherwise it sets BR to 0. The sensor nodes use the flag CR to inform the BS about the awareness of new configuration instructions. A sensor node sets CR to 1, whenever a beacon has been received during the reconfiguration state; otherwise, it sets CR to 0.

Let us suppose that the WSN is in the steady state. The BS sends short-size beacons carrying the superframe specifications and the ACK bitmaps, with the flag RiP set to 0. Then the BS needs to reconfigure the WSN, for example, for a new NTP time-slot scheduling. The BS sets RiP to 1 and broadcasts the new configuration instructions along with the superframe specifications and the ACK bitmaps. By receiving a beacon with RiP set to 1, sensor nodes know that new configuration instructions are present in the

beacon payload and save these instructions. However, sensor nodes continue transmitting using the old allocation of slots in the CFP. While a sensor node does not receive a beacon with RiP set to 0, it must always transmit its packets with CR set to 1 to inform the BS that the new configuration instructions have been read.

If a sensor node does not receive a beacon and the previous received beacon contained the new configuration instructions (RiP = 1), then it may only transmit data in the CAP. As the lost beacon could have renewed configuration instructions, CAP transmissions should be sent with CR set to 0. The identification of the sensor nodes that transmitted successfully frames with CR set to 1 is registered by the BS in the CR table.

If during the reconfiguration process a new configuration is required, then the BS cleans up the CR table and broadcasts the recent new configuration instructions with RiP set to 1. To avoid registering a CR value relative to the old reconfiguration, sensor nodes that do not receive the beacon frame may only transmit packets in the CAP with CR set to 0. Packets received in the NRP and ERP imply that the respective originators received the beacon frame with the new reconfiguration, and so those packets should be received with CR set to 1. Sensor nodes must always save the instructions contained in a beacon with RiP set to 1 to be informed of the last new configuration instructions.

BR	CR	received beacon?	sensor knows the new instructions?	states where it may occur
0	0	no	no	reconfiguration, steady
0	1	no	yes	reconfiguration, steady[14]
1	0	yes	no	Steady
1	1	yes	yes	Reconfiguration

Table 4.2 – Semantic of flags BR and CR steady.

When the BS has received from each sensor node a packet with CR set to 1, it knows every sensor node is aware of the new configuration instructions. Hence, the BS considers the reconfiguration process complete. In the next beacon, the BS only sends the superframe specifications and the ACK bitmaps, with RiP set to 0. Whenever a sensor node receives a new beacon with RiP set to 0, it resets CR and starts transmitting according to the new instructions.

[14] It may occur in the steady state while a beacon announcing the end of the reconfiguration state (RiP=0) is not received by the node.

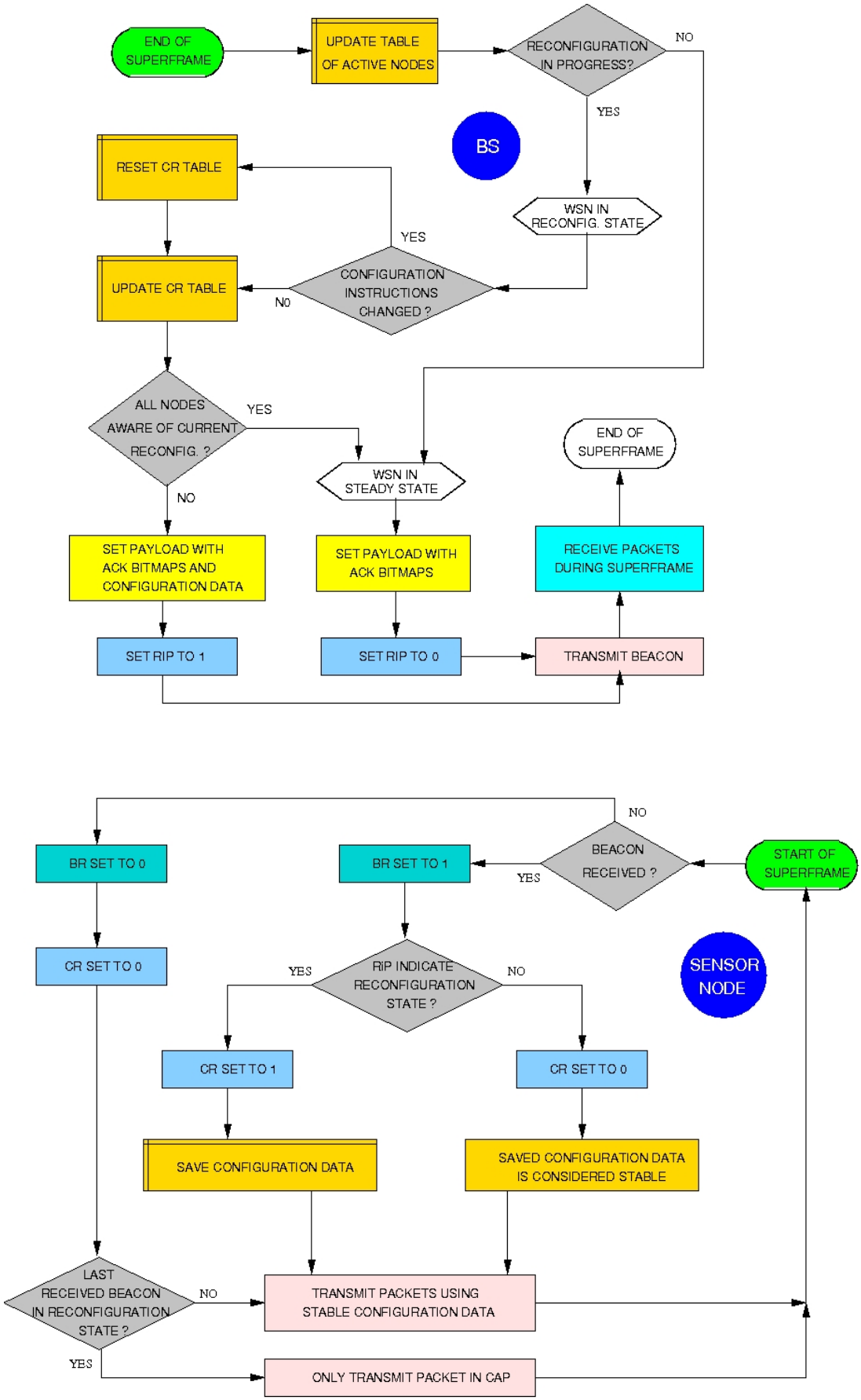

Figure 4.6 – Reconfiguration scheme relative to BS (up) and to sensor node (down).

If during the reconfiguration process the BS never receives a packet with CR set to 1 (or BR set to 1) from a given sensor node, the process hangs. To prevent this, if the BS only received packets with BR set to 0 from one sensor node after transmitting a number of consecutive beacons (*maxLostBeacons* = 16), the BS ignores the corresponding sensor node. In the same way, if a data frame transmitted by a sensor node in the NTP is not acknowledged in the ACK bitmap during a number of successive superframes (*maxUnackedFrames* ≤ *maxLostBeacons*), the sensor node leaves the WSN at once. Both procedures are valid for the reconfiguration and steady states.

Figure 4.6 presents the flowchart of the described algorithm. During the reconfiguration state the packet loss ratio may increase, because beacon frames with RiP set to 1 have a larger size, and also because sensor nodes do not send any data in the CFP if a beacon is not received and the last received beacon frame had RiP set to 1. Hence, to reduce the packet loss, sensor nodes may transmit in the CAP. However, the reconfiguration state tends to occur sporadically when compared with the steady state.

A reconfiguration process may occur in simultaneous with a channel switching process, as the respective schemes operate without correlation.

4.4 Time-slot Allocation Algorithm

Protocols using short-size beacons, such as AR-MAC, are valuable for the sake of energy saving and packet delivery improvement. As time-slots allocation is not announced in the short-size beacons explicitly, sensor nodes should use a distributed scheduling algorithm to find the time-slots to transmit collision-free data.

In this section, a distributed and collaborative time-slot scheduling algorithm for a TDMA-based MAC protocol using short-size beacons and operating in one-hop e-health WSNs characterized by regular traffic pattern, homogeneity regarding the number and types of sensor nodes in the BSNs, and stable network topology is formulated mathematically. With the proposed algorithm, each sensor node is able to compute the time-slot that may use in the superframe to start transmitting collision-free data, as well as the number of contiguous time-slots required to complete the data transfer. The algorithm takes as input the total number of BSNs in the e-health WSN, the BSN identification and the type of sensor node that is running the algorithm, the ACK

bitmaps, as well as the activity and criticality states of all sensor nodes. This information is known by all active sensor nodes in the WSN. To help with the interpretation of the notation used in the proposed formulation, Table 4.3 of Section 4.4.2 presents the meaning of the diverse symbols.

Let us consider that a TDMA-based MAC protocol using superframes is operating in an e-health WSN containing *n* sensor nodes. To guarantee a maximum delay for packet delivery, the superframe duration[15] t_{SD} must be less than half the maximum packet delivery delay $t_{D\ max}$ to assure that retransmitted packets are delivered timely. Also, the superframe duration must be below the time required to fill up the frame payload with sampling data. These conditions can be expressed as:

$$t_{SD} \leq \min\left(\left\lfloor t_{D\,max} / 2 \right\rfloor , \left\lfloor MAC_{d\,max}.8 / \{r.H\}_{n,max} \right\rfloor \right) \quad (4.1),$$

where $MAC_{d\ max}$ is the maximum MAC payload length in bytes, and $\{r.H\}_{n,max} = max(r_1.H_1, r_2.H_2, \ldots, r_n.H_n)$ is the maximum product between the sampling resolution *r* bits and the sampling rate *H* samples/s found in the *n* sensor nodes of the WSN[16]. This maximum product is normally found in ECG sensor nodes.

The total number of time-slots *S* in the superframe should be large enough to tune accurately the time division allocated to each sensor node and so minimizing the bandwidth waste, without leading to time-slot duration beyond the sensor nodes timer resolution.

The number of time-slots S_s that a sensor node occupies in the superframe to transmit a data packet is:

$$S_s = \left\lceil S.t_{TX} / t_{SF} \right\rceil \quad (4.2),$$

[15] A superframe is bounded by the transmission of a beacon frame and can have an active portion and an inactive portion. For simplicity, the present discussion assumes that the inactive superframe duration is null. So, the active superframe duration is equal to the beacon interval.

[16] min(*x*,…,*y*) and max(*x*,…,*y*) returns the smallest and the largest of the arguments, respectively. The floor function $\lfloor x \rfloor$ returns the largest integer not greater than *x* (i.e., the integer part of *x*). The ceiling function $\lceil x \rceil$ returns the smallest integer not less than *x* (i.e., $\lceil x \rceil = \lfloor x \rfloor + 1$).

where S is the total number of time-slots in the superframe, and t_{TX} is the transmission duration.

For a packet with a physical header size PHY_h, a MAC header plus trailer size MAC_h, a MAC payload length MAC_d bytes, and a nominal transmission rate R bps:

$$t_{TX} = (PHY_h + MAC_h + MAC_d).8/R \quad (4.3).$$

Considering a null overhead for the layers above the MAC layer, MAC_d is equal to:

$$MAC_d = t_{SD}.H.r/8 \quad (4.4).$$

S_g additional time-slots are included for safeguarding purposes. Furthermore, if a data packet must be acknowledged, then S_a time-slots have to be included to receive the ACK packet. Therefore, a sensor node may occupy a total number of S_t time-slots:

$$S_t = S_s + S_g + S_a \quad (4.5).$$

Consecutive super time-slots may be used for multiple transmission trials. For example, with a maximum of two transmission trials, the second super time-slot is used for retransmission if the packet is not correctly received by the BS during the first transmission. Accordingly, the first transmission must be acknowledged. If a packet is sent with success during the first transmission, then the time-slots reserved for the second retransmission are unused, resulting in bandwidth waste. The last retransmission is not acknowledged. So, the total number of time-slots required by sensor node M_i can be represented generically as:

$$S_t(M_i) = [(S_s(M_i) + S_g(M_i) + S_a(M_i)).T(M_i) - S_a(M_i)].A(M_i) \quad (4.6),$$

where the Boolean activity flag $A(M_i)$ indicates whether sensor node M_i is going to transmit data in the current superframe or not, and $T(M_i)$ represents the maximum number of trials for sensor node M_i to transmit one data packet.

4.4.1 Transmission in the NTP

Let us consider that a WSN running AR-MAC protocol contains *p* patients (i.e., BSNs), and each patient has *m* sensor nodes to monitor distinct physiological signals. To simplify the algorithmic definition, and without losing generality, it is assumed that the time-slots in the superframe are occupied by the sequence defined in Figure 4.7. Here, *b* represents the beacon and B_j the BSN of patient *j* ($1 \leq j \leq p$). Every sensor node may transmit only one data packet in the NTP, so the maximum number of trials for sensor node M_i to transmit one data packet $T(M_i) = 1$ ($1 \leq i \leq m$). If $m = 5$ and $p = 3$ are taken for instance, then $M_1(B_1, B_2, B_3) = (M_1(B_1), M_1(B_2), (M_1(B_3))$ represents the following sequence in the NTP: after sensor node M_1 of BSN B_1 transmits a data packet, then sensor node M_1 of BSN B_2, and sensor node M_1 of BSN B_3 transmit successively their data packets. The same criterion is applied to the remaining types of sensor nodes. M_1 and M_2 may represent, for instance, ECG and arterial pressure sensor nodes respectively.

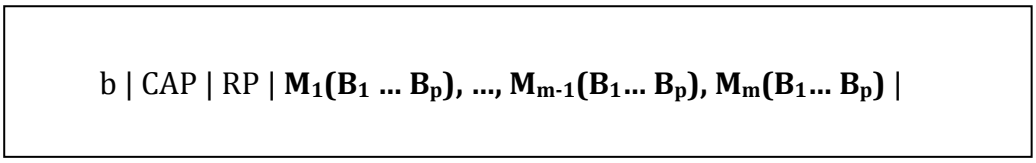

Figure 4.7 – Time-slot occupation sequence in the NTP.

As during the reconfiguration state every sensor node becomes aware of the operating parameters used by the remaining sensor nodes in the WSN, each sensor node is able to compute the initial transmission time-slot in the NTP using the following expression:

$$S_{NTP}(M_i(B_j)) = S_{NTP} + \sum_{k=1}^{i-1} \left(\sum_{n=1}^{p} S_t(M_k(B_n))\right) + \sum_{n=1}^{j-1} S_t(M_i(B_n)) \qquad (4.7),$$

where $S_{NTP}(M_i(B_j))$ represents the NTP time-slot which sensor node M_i of BSN B_j must use to start transmitting its data. For example, in Figure 4.1, a sensor node uses Equation (4.7) to find the initial transmission time-slot *F* to send packet *d*. S_{NTP} represents the time-slot where NTP starts and is given by:

$$S_{NTP} = (S - S_r) - \sum_{i=1}^{m} \sum_{i=1}^{p} S_t(M_i(B_i)) \quad (4.8),$$

considering the last S_r time-slots of the superframe reserved to allow the sensor nodes to enter in listening mode in order to receive the next beacon. In Figure 4.1, S_{NTP} is the time-slot *E*.

These calculations need to be performed only once after the conclusion of every reconfiguration process.

4.4.2 Retransmission in the NRP

The retransmission time-slot scheduling in the NRP depends on the NTP ACK bitmap and criticality bitmap received from the BS. The activity bitmap is not required, since it is implicit in the NTP ACK bitmap. Indeed, if the BS asks for a sensor node to retransmit, it is because the BS considers that sensor node active. An inactive sensor node should have the respective flag in the NTP ACK bitmap set to 1.

Using an increasing time-slot sequence and a predefined order scheme, firstly the data packets of all sensor nodes having the bit true in the criticality bitmap and the bit false in the NTP ACK bitmap are retransmitted successively. This strategy increases the probability of allocating retransmission time-slots to packets containing critical data. When the number of available time-slots is insufficient for all required retransmissions, the less important physiological signals should not be retransmitted. As body temperature changes slowly along the time, temperature is a good candidate to be discarded in such situation.

As consecutive super time-slots may be used for multiple retransmission trials, $T(M_i) \geq 1$ ($1 \leq i \leq m$). In AR-MAC, if there is at least one BSN in emergency state, then BSNs in steady state may retransmit *N* times in the NRP and BSNs in emergency state may retransmit *P* times in the NRP, with $N < P$ (see Section 4.2.2). This condition can be expressed as,

$$\begin{cases} T(M_i) = N, \ if \ \ C(M_i) = 0 \\ T(M_i) = P, \ if \ \ C(M_i) = 1 \end{cases} \quad (4.9),$$

where the criticality flag $C(M_i)$ indicates whether data from sensor node M_i is critical ($C(M_i) = 1$) or not.

Let us assume that a WSN contains p BSNs, and each BSN is composed of m sensor nodes to monitor distinct physiological signals. It is assumed that the NRP time-slots are occupied in accordance with Figure 4.8, considering the same low criticality status for every type of sensor node in every BSN, i.e., $C(M_i(B_j)) = 0$, $1 \leq i \leq m$, $1 \leq j \leq p$. $nack_p(M_i) = (nack_{i,1}, \ldots, nack_{i,p})$ represents the complement of the ACK bitmap for all sensor nodes M_i present in the p BSNs. The meaning of $nack_p(M_1).M_1(B_1 \ldots B_p)$ is equivalent to $M_1(nack_{1,1}.B_1, \ldots, nack_{1,p}.B_p)$. M_m must be the type of sensor node to be discarded firstly in case of truncation. For instance, if $m = 5$, $p = 6$, and if the complement of the ACK bitmap for sensor nodes M_1 and M_2 of all BSNs is $nack_6(M_1) = nack_6(M_2) = (1,0,1,1,0,0)$ and $nack_6(M_i) = (0,0,0,0,0,0)$, $2 < i \leq 5$, then $nack_6(M_1).M_1(B_1,B_2,B_3,B_4,B_5,B_6) = M_1(B_1,B_3,B_4)$ represents the following transmission sequence in NRP: after sensor node M_1 of BSN B_1 retransmitting a data packet, then sensor node M_1 of BSN B_3 and sensor node M_1 of BSN B_4 retransmit successively their data, followed by the sensor nodes M_2 of BSN B_1, BSN B_3, and BSN B_4. Every retransmission occurs only once per superframe. But, considering the same ACK bitmap, if the criticality flag is true for sensor nodes M_1 of BSN B_1 and BSN B_2, i.e., $C(M_1(B_1)) = C(M_1(B_2)) = 1$, and false for the remaining sensor nodes, then sensor nodes M_1 of BSN B_1 and BSN B_2 may retransmit their packets in this order twice, if required. Next, sensor nodes M_1 of BSN B_3 and BSN B_4 retransmit successively their data once, followed by the sensor nodes M_2 of BSN B_3 and BSN B_4.

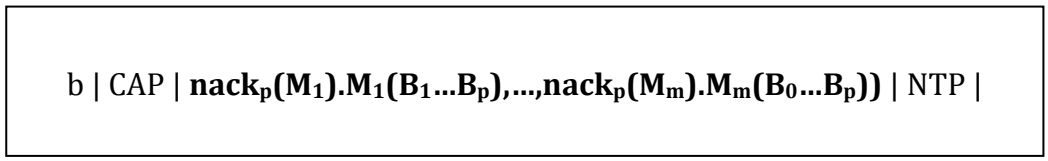

Figure 4.8 – Time-slot occupation sequence in the NRP.

As during the reconfiguration state every sensor node becomes aware of the parameters used by the remaining sensor nodes of the WSN, each sensor node is able to compute the initial transmission time-slot in the NRP using the following expression:

$$S_{NRP}(M_i(B_j) = S_{NRP} + \sum_{k=1}^{i-1} \left(\sum_{n=1}^{p} nack_p(M_k).S_t(M_k(B_n))\right) + \sum_{n=1}^{j-1} nack_p(M_i).S_t(M_i(B_n)) \quad (4.10),$$

where $S_{NRP}(M_i(B_j))$ represents the NRP time-slot which sensor node M_i of BSN B_j must use to start transmitting its data. S_{NRP} represents the time-slot number where NRP starts. In Figure 4.1, S_{NRP} is the time-slot *D*. For simplicity of representation, Equation (4.10) does not consider the premise of sensor nodes having the bit true in the criticality bitmap to be retransmitted firstly.

Symbol	Description
$A(M_i)$	boolean activity state of sensor node M_i
B_i	body area network B_i
$C(M_i)$	boolean criticality state of sensor node M_i
H	sampling rate of the sensor, in samples/s.
M	number of sensor nodes per BSN.
MAC_h	MAC header plus trailer size.
MAC_d	MAC payload length, in bytes.
$MAC_{d\,max}$	MAC payload maximum length, in bytes.
M_i	sensor node M_i
M_i (B_j)	sensor node M_i of BSN B_j
$nack_p(M_i)$= ($nack_{i,1}$…,$nack_{i,p}$)	complement of the ACK bitmap for all sensor nodes M_i present in the *p* BSNs.
N	total number of sensor nodes in the e-health WSN.
p	number of patients, i.e. BSNs.
PHY_h	physical header size.
R	sampling resolution of the sensor, in bits.
$\{r.H\}_{n,\,max}$	maximum product of sampling resolution and sampling rate found in the *n* sensor nodes of WSN.
R	nominal transmission rate, in bits/s.
S	total number of time-slots in the superframe.
$S_a(M_i)$	time-slots used by sensor node M_i to receive the ACK frame.
$S_g(M_i)$	safeguard time-slots used by sensor node M_i
S_r	nr. of reserved final time-slots in the superframe.
$S_s(M_i)$	nr. of time-slots used by sensor node M_i to transmit a packet.
$S_t(M_i)$	total nr. of time-slots allocated to sensor node M_i
S_{NTP}	time-slot where NTP starts.
$S_{NTP}(M_i(B_j))$	NTP time-slot for sensor node M_i of BSN B_j to start data transmission.
S_{NRP}	time-slot where NRP starts.
$S_{NRP}(M_i(B_j))$	NRP time-slot for sensor node M_i of BSN B_j to start data retransmission.
t_D	packet delivery delay, in seconds.
$t_{D\,max}$	maximum packet delivery delay, in seconds.
t_{TX}	transmission duration, in seconds.
t_{SD}	superframe duration, in seconds.
$T(M_i)$	maximum number of trials for node M_i to retransmit one data packet.

Table 4.3 – Meaning of the symbols.

These calculations need to be performed by a sensor node every time a beacon is received and the respective flag in the ACK bitmap requests for a retransmission in the NRP. The critically bitmap is known during the reconfiguration state, and remains unchanged until the next reconfiguration procedure.

4.4.3 Retransmission in the ERP

The algorithm presented for retransmissions in the NRP also holds for transmission in the ERP, with the difference that the retransmission time-slot scheduling in the ERP depends on the NRP ACK bitmap rather than the NTP ACK bitmap. ERP starts immediately after the last time-slot of the CAP announced by the BS.

4.4.4 Example of Time-slot Allocation

In order to illustrate the operation and simplicity of the proposed scheduling algorithm, an example of its use is given next. Let us consider a hospital room containing a few beds with one patient per bed. Each patient is monitored by a body sensor network, and a BS collects and analyses the physiological signals of all patients. The signals being monitored by dedicated sensor nodes are ECG, arterial pressure (ART), oximetry (OXI), respiration rate (RR), and temperature (TEMP). The NTP time-slots in the superframe are occupied in the order shown in Figure 4.9.

Figure 4.9 – Example of time-slot occupation order in the NTP.

$ECG_{1\text{-}6}$ represents the following transmission sequence in NTP: after ECG sensor node of BSN_1 (ECG_1) transmitting the data packet, then ECG_2, ECG_3, ECG_4, ECG_5, and ECG_6 transmit successively their data. The same criterion is applied to the remaining types of sensor nodes. During the association phase, every sensor node must indicate its type to the BS. For example, ECG, ART, OXI, RR, and TEMP sensor nodes would correspond to sensor nodes M_1, M_2, M_3, M_4, and M_5, respectively, in Figure 4.7. Also, each sensor node must indicate the BSN it belongs to. Whenever a new BSN identification is received, the BS updates the total number of BSNs in the e-health network and attributes this number to the new BSN. Every time a sensor node enters or leaves the WSN, the network enters in reconfiguration state to inform the active sensor nodes about the fact.

Figure 4.10 presents a possible pseudo-code for the procedure that sensor node M_i at BSN B_j should invoke to find the initial transmission time-slot in the NTP to transmit a new data packet (slotNTP), considering the activity bitmap A, and the number of time-slots S_s required by each sensor to transmit data. For instance, sensor node OXI_2 should call slotNTP with $M_i = 3$ and $B_j = 2$ to find its initial transmitting time-slot in the NTP.

Figure 4.10 also shows the procedure for a sensor node to find its initial transmission time-slot in the NRP (slotNRP). In this case, the input arguments of the procedure are the sensor node M_i, the BSN B_j, the array S_s, the NTP ACK bitmap *ack*, and the criticality bitmap C. Two possible retransmission trials are allowed for critical data. slotNRP returns zero if no more time-slots are available in the NRP of the superframe.

```
constants (cf. Table 4.3): m, p, S, Sg, Sr, Sa, T;

S_NTP ← SNTP(A[m][p], Ss[m][p])  // first index of arrays is 1

slotNTP( Mi, Bj, A[m][p], Ss[m][p] )
{
   Sntp[m][p]
   auxiliary variables: b, s, a[m]

   for s=1 to Mi–1   {
       if ( s=1 ) then a[s] ← S_NTP else a[s] ← a[s–1]
       for b=1 to p  {
            a[s] ← a[s] + ( Ss[s][b] + Sg )*A[s][b] }
   }
   if (Mi=1) then Sntp[Mi][Bj] ← S_NTP  else Sntp[Mi][Bj] ← a[s–1]
   for b=1 to Bj–1 {
        Sntp[Mi][Bj] ← Sntp[Mi][Bj] + (Ss[Mi][b]+Sg)*A[Mi][b] }
   return Sntp[Mi][Bj]
}

slotNRP( Mi, Bj, Ss[m][p], ack[m][p], C[m][p] )
{
   S_NRP, Snrp[m][p]
   auxiliary variables: a[m], b, k, q, s, v, z

   S_NRP ← 1 + last time-slot of the CAP
   for k=1 to 2    {
    for z=1 to m   {
      for v=1 to p    {
       if( k=2  or  C[Mi][Bj] ) then  z ←Mi, v ←Bj
       for s=1 to z–1   {
          if( s=1 ) a[s] ← S_NRP else a[s] ← a[s–1]
          for b=1 to p  {
           if( k=1 ) then q ← C[s][b]*T else q ← 1–C[s][b]
            a[s] ← a[s] + (Ss[s][b]+Sg+Sa)*(1–ack[s][b])*q  }
          }
      if( z=1 ) then Snrp[z][v] ← S_NRP else Snrp[z][v] ← a[s–1]
      for b=1 to v–1 {
         if( k=1 ) then q ← C[z][b]*T  else q ← 1–C[z][b]
         Snrp[z][v] ← Snrp[z][v]+(Ss[z][b]+Sg+Sa)*(1–ack[z][b])*q  }
    if( k=2  or  C[Mi][Bj] ) {
       if( Snrp[z][v] ≥ S_NTP ) then Snrp[z][v] ← 0
       return Snrp[z][v]  }
    }}
  S_NRP ← Snrp[m][p]
}}

SNTP( A[m][p], Ss[m][p] )   // procedure to find S_NTP
{
   auxiliary variables: a[m], b, s
    for s=1 to  m  {
    if ( s=1 ) then a[s] ← S–Sr else a[s] ← a[s–1]
       for b=1 to  p  {
            a[s] ← a[s] – (Ss[s][b] + Sg)*A[s][b] }
   }
   return  a[s–1]
}
```

Figure 4.10 – Procedures for a sensor node to find the initial transmission time-slot in NTP and NRP, as well as the time-slot where NTP starts.

4.5 AR-MAC Frame Formats

The frames in the MAC layer are described as a sequence of fields in a specific order. Next, it is presented both the general frame formats and the format of individual frame types used in AR-MAC protocol.

4.5.1 General AR-MAC Frame Format

The general AR-MAC frame format is composed of a header, a payload, and a trailer, as illustrated in Figure 4.11.

In order to minimize the AR-MAC overhead on the data communications, the header has a length of 7 B only and the trailer 2 B. The header contains the fields: frame control (1 B), sequence number (1 B), destination address (1 B), source address (1 B), WSN identification (1 B), and frame check sequence (FCS) (2 B).

The *frame control field* contains the subfields: frame type (3 bits), acknowledgment request (1 bit), BR/TtC (1 bit), RiP/CR (1 bit), and security enabled (1 bit).

The *frame type* subfield identifies whether it is a beacon, an acknowledgment, a MAC command, or a data frame, according to Table 4.4. In the case of a data frame, this subfield indicates if the data frame was transmitted in the NTP, NRP, ERP, or CAP.

The *ACK request* subfield specifies whether an acknowledgment is required from the recipient node on receipt of a data or MAC command frame. If this subfield is set to 1, the recipient node shall send an acknowledgment frame after determining that the frame is valid; otherwise, the recipient node shall not send an acknowledgment frame.

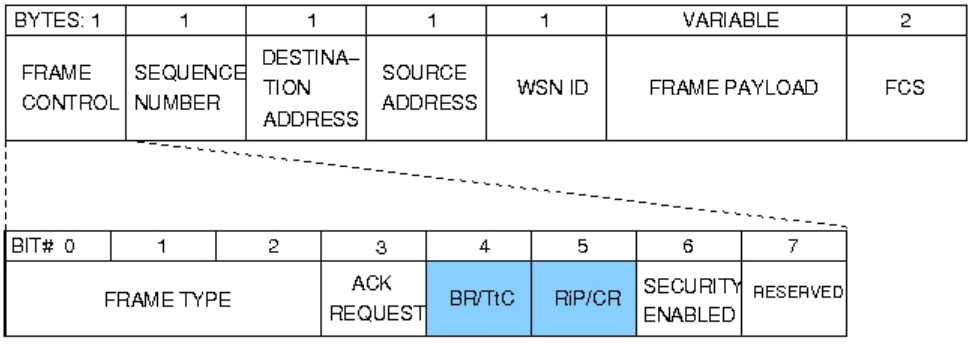

Figure 4.11 – General MAC frame format (up) and frame control field format (down).

b2 b1 b0	Description
0 0 0	beacon
0 0 1	acknowlegment
0 1 0	MAC command
0 1 1	reserved
1 * *	data
1 0 0	NTP data
1 0 1	NRP data
1 1 0	ERP data
1 1 1	CAP data

Table 4.4 – Values of the frame type subfield.

The *BR/TtC* subfield must be interpreted as "beacon received" in a data frame and "time to change" in a beacon frame. In a data frame, if the originator of the frame received the beacon of the current superframe, the originator sets this subfield to 1; otherwise it sets to 0. In a beacon frame, if the recipient of the frame must change the radio to the specified channel, the BS sets this subfield to 1; otherwise, the BS sets it to 0.

The *RiP/CR* subfield must be interpreted as "reconfiguration in progress" in a beacon frame and "configuration received" in a data frame. In a beacon frame, the RiP subfield specifies whether a reconfiguration process is in course. If the WSN is in reconfiguration state, the BS sets this subfield to 1; otherwise the BS sets it to 0. In a data frame, the CR subfield specifies whether a recipient node is aware of the new configuration data. The recipient node sets this subfield to 1 whenever a beacon frame is received during the reconfiguration state; otherwise, it sets it to 0.

The *security enabled* subfield is set to 1, if the frame is cryptographically protected by the MAC layer; otherwise it is set to 0.

The *sequence number field* specifies a unique sequence identifier for the data frame or beacon frame. It is incremented by one each time a beacon or data frame is generated. For a data, acknowledgment, or MAC command frame, the sequence number field specifies a data sequence number that is used to match an acknowledgment frame to the data or MAC command frame.

The *destination address field* specifies the address of the intended recipient of the frame. The value of 255 in this field represents the broadcast address.

The *source address field* specifies the address of the originator of the frame.

The *WSN identifier field* specifies the unique WSN identifier of the originator of the frame. The WSN identifier of a device is initially determined during association on a WSN.

The *frame payload field* has a variable length and contains information specific to individual frame types. If the security enabled subfield is set to 1 in the frame control field, the frame payload is protected by a security suite. Beacon frames carry in the payload the beacon order, the beacon color, the NTP ACK bitmap, the NRP ACK bitmap, and the last time-slot of the CAP. In addition, reconfiguration data are also present if subfield RiP is set to 1. Data frames carry in the payload the application data.

The *FCS field* contains the FCS of a 16 bit ITU-T cyclic redundancy check. The FCS is calculated over the MAC header and MAC payload parts of the frame.

4.5.2 Format of individual frame types

Four frame types are defined: beacon, data, acknowledgment, and MAC command. Beacon frames are used by a coordinator to transmit beacons. Data frames are used for all transfers of data. Acknowledgment frames are used for confirming successful frame reception. MAC command frames are used for handling all MAC peer entity control transfers, such as association request, association response, disassociation notification, data request, WSN identifier conflict notification, orphan notification (used by sensor nodes that have lost synchronization with the BS), and beacon request.

MAC command frames are not discussed, because it would require a long section to describe all commands. Beacon, data, and acknowledgment frames are discussed in the next sections.

4.5.2.1 Beacon frame format

A beacon frame uses the MAC payload field to add the superframe specification field (3 B), the NTP ACK bitmap field, the NRP ACK bitmap field, and the optional reconfiguration data field, as shown in Figure 4.12.

The *superframe specification field* contains the subfields: beacon order (3 bits), superframe order (3 bits), final cap slot (11 bits), array beacon number (2 bits), beacon color (4 bits), and association permit (1 bit).

The *beacon order* subfield specifies the transmission interval of the beacon. If *BO* is the value of the beacon order, the beacon interval (*BI*) is computed as follows: $BI = baseSuperframeDuration \times 2^{BO}$ seconds, where $0 \leq BO \leq 7$. *baseSuperframeDuration* is the duration of a superframe when the superframe order is equal to 0 (*baseSuperframeDuration* = 125 ms). The number of slots contained in a superframe is: *numSuperframeSlots* = *baseSuperframeDuration* / *baseSlotDuration*, where *baseSlotDuration* is the duration of a time-slot (*baseSlotDuration* = 0.5 ms).

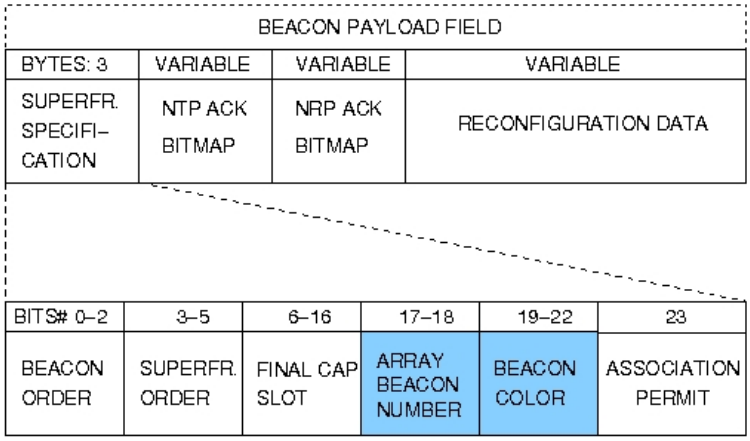

Figure 4.12 – Formats of beacon payload field (up) and superframe specification field (down).

The *superframe order* subfield specifies the length of time during which the superframe is active, including the beacon frame transmission time. The coordinator interacts with its WSN only during the active portion of the superframe. If *SO* is the value of the superframe order, the superframe duration (*SD*) is computed as follows. For $0 \leq SO \leq BO \leq 7$, $SD = baseSuperframeDuration \times 2^{SO}$ seconds.

The *final CAP slot* subfield specifies the final superframe time-slot utilized by the CAP. The duration of the CAP, as implied by this subfield, shall be greater than or equal to the value specified by *minCAPLength*, to ensure that MAC commands can be sent to devices.

The *array beacon number* subfield specifies the beacon number sent in the BP. If *ABN* is the value of the array beacon number, the beacon number (*BN*) is computed as follows: $BN = 1 + ABN$.

The beacon color subfield specifies the color of the superframe. If *BC* is the value of the beacon color, the superframe color (*SC*) is computed as follows: $SC = 2^{BC}$.

The association permit subfield is set to 1, if the coordinator is accepting association requests on its WSN; otherwise it is set to 0.

The *NTP ACK bitmap field* carries the NTP ACK bitmap. The *NRP ACK bitmap field* carries the NRP ACK bitmap. The size of these fields is equal and depends on the number of sensor nodes in the e-health WSN.

The *reconfiguration data field* contains the data required to reconfigure the WSN. This field only exists while the network is in reconfiguration state.

4.5.2.2 Data frame format

Data frame format is identical to the generic MAC frame format presented in Figure 4.11. The payload of a data frame contains the sequence of bytes that the next higher layer has requested the MAC layer to transmit.

If a physical platform is used to deliver traffic with real-time requirements, the data payload format shown in Figure 4.13 is proposed.

The data payload field is composed of the header with a length of 3 B and the samples data field with a variable length. The first byte in the header is the identification field, which contains two subfields: the sensor signal identification (3 bits) and the BSN identification (5 bits). Therefore, up to eight distinct signals captured in a maximum of thirty two patients are identified unequivocally. The next two bytes contain two reserved bits and the sequence number field. Two bits are reserved for internal operation of the application. The sequence number field (14 bits) contains the sequence number of the latest sample contained in the payload, i.e., the last sample in the packet payload to be transmitted to the BS. This sample-oriented approach was chosen to identify all undelivered samples. As the packet payload may be variable, a packet-oriented sequence number is not convenient for this aim. Null padding bits are included for the payload size

to become a multiple of byte length. In every field, the most significant bit is the first bit to be transmitted into the wireless channel.

BITS: 0–2	3–7	8–9	10–23	24–33	34–43			
SENSOR ID	BSN ID	RESER-VED	SEQ. NR. OF SAMPLE N	SAMPLE 1	SAMPLE 2	...	SAMPLE N	PADDING

Figure 4.13 – Data payload format proposed for transmission of data samples.

4.5.2.3 Acknowledgment frame format

The acknowledgment frame is four bytes in length and contains a header, a trailer, and no payload field.

The MAC header contains only the frame control field and the sequence number field. In the *frame control* field, the frame type subfield contains the value that indicates an acknowledgment frame, as shown in Table 4.4. All other subfields are set to 0 and ignored on reception. The *sequence number* field contains the value of the sequence number received in the frame for which the acknowledgment is to be sent. The MAC trailer contains only the FCS field.

4.6 Summary

New healthcare paradigms will not become widely available and deployed until novel WSN solutions meet the specific needs of healthcare services. To contribute to this goal, the new AR-MAC protocol has been designed to target relevant characteristics of e-emergency WSNs. The AR-MAC protocol aims at providing (*i*) QoS support to guarantee a reliable and timely data delivery for a useful clinical diagnostic; (*ii*) power efficiency; (*iii*) cluster mode support; (*iv*) reconfiguration mechanisms to accommodate autonomously the diverse clinical situations of patients; (*v*) capacity of switching the operating channel when the interference level is unacceptable (*vi*) coexistence capacity;

and (*vii*) bandwidth efficiency. These goals cannot be simultaneously accomplished using the deterministic MAC protocols currently available for WSNs.

As discussed in this chapter, protocols using short-size beacons, such as AR-MAC, can be valuable regarding energy saving and packet delivery ratio improvement. Taking advantage of the traffic and sensor node characteristics found in e-health WSN, a lightweight, distributed, and collaborative time-slot scheduling algorithm has been proposed to avoid explicit time-slot allocation, thus reducing the beacon size.

In order to test the AR-MAC performance and compare it with other MAC protocols, a physical testbed and a simulation platform were implemented. Both test platforms are introduced in the next chapter.

Chapter 5

WSN Test Platforms

5.1 Introduction

In order to carry out performance analysis in WSNs, analytical modeling, real deployment, physical testbed, emulation, and simulation techniques can be used.

Analytical methods are not commonly used due to the inherent complexity of WSNs, (e.g., node density, node mobility, channel varying characteristics, application-specific nature), which the usually simplified mathematical models cannot take into account. Notwithstanding, analytical studies have been developed, for example, to quantify the impact of cooperative diversity on the energy consumption of WSNs [Shastry05].

Using a real deployment to study the actual behavior of protocols and network performance supposes a huge effort, sometimes installed in very harsh environmental conditions, such as high alpine environments [Keller09] and volcanoes [Werner06]. Also, long time periods are usually required to collect meaningful datasets. For example, a habitat was monitored during four months to produce unique datasets [Szewczyk04].

With a physical testbed, it may be hard and time-consuming to collect metrics and test different scenarios. Performance tests are limited to the number of nodes available in the testbed. Moreover, results are often irreproducible and difficult to explain, as shown in [Pham07], which makes very hard to compare experimental results from different research groups. Several public test platforms are presented in [Imran10].

Emulation is a hybrid approach that combines simulated and real systems, making possible real time debugging and analysis of information. However, the user is tied to a single platform either hardware (e.g., Mica motes) or software (e.g., TinyOS/NesC[17])

Consequently, simulation techniques have been extensively adopted in the networking research community to carry out performance studies of algorithms and protocols. A review based on one hundred and fifty one wireless network articles from a five-year-period reported that seventy six percent from those works used simulations [Kurkowski05]. The preference for simulation tools is justified by the difficulty of deploying real networks, as (re)programming a lot of sensor nodes, gathering the performance metrics of the sensor nodes, and managing the power sources is tedious

[17] TinyOS [TinyOS] is an open source, event-driven operating system for motes. TinyOS is coded in nesC, an extension to C programming language designed to embody the structuring concepts and execution model of TinyOS. Both TinyOS and nesC were developed at the University of Berkeley, U.S.A., for their Mica motes.

and time-consuming. Because WSNs use distributed programming and debuggers are hard to use in the sensor nodes, software errors are harder to detect and correct in a testbed than in a simulator. On the other hand, simulators allow building and modifying easily network scenarios, as well as the topology and the size of a network, the models are easily monitored from the global view of the simulator, and the experiments are reproducible. For all these reasons, the experiments carried out in this work to test and compare the performance of AR-MAC protocol in e-health scenarios were mostly carried out on a simulation platform.

Furthermore, some physical test platforms, including the one implemented in this work, use a BS that is identical to a sensor node in terms of software performance. This is an important limitation of the physical testbed, because in a typical WSN the BS has more computing and hardware resources than sensor nodes. This limitation of the BS does not occur in a simulation platform, which stresses the preference in carrying out the performance tests with a network simulator. However, simulators must be used carefully because simulation results may diverge significantly from the reality, if the device, link or channel models are optimistic or wrongly parameterized. Such divergence may be particularly relevant in WSNs, as nodes present very limited computing and hardware resources.

Aware of the difficulty that a simulator may have in presenting accurate results, a physical testbed was used to validate the simulation results and, if necessary, to allow developing a new simulation model to improve the accuracy of the results when compared with those obtained in real conditions.

The simulation platform used in this work is presented in the next section. The physical testbed is presented in Section 5.3.

5.2 Simulation Platform

Diverse simulation tools are available for WSNs (see [Singh08], [Korkalainen09], [Imran10]), each one with different characteristics, models and architectures. In order to choose an appropriate simulator for this work, some available simulation tools were analyzed beforehand. NS-2 [Downard04], SensorSim [Park00], J-Sim [Sobeih05], OPNET [Prokkola06], TOSSIM [Levis03], COOJA [Österlind06], OMNeT++

[Varga00], MiXiM [Köpke08], and Castalia [Boulis09] were the considered simulators, since they are popular tools in the research community. After evaluating the advantages and disadvantages of these simulation tools, Castalia was selected for the reasons presented in Section 5.2.2. The reasons that declined the other simulators are argued next.

5.2.1 Network Simulators

NS-2 is a well-known general purpose discrete event simulator for communication networks, including WSNs. NS-2 was mainly built for traditional networks whose nodes send and receive traffic through a data communication infrastructure. Despite of supporting a few WSN protocols (e.g., IEEE 802.15.4, S-MAC [Ye02]), the simulator does not support channel sensing, physical processes and management of resources at the sensor nodes, Also, NS-2 lacks the ability to introduce easily distributed algorithms into the network, as usually it is required in WSNs. Energy modeling is simplified to the basic receiving, transmitting, and listening states of sensor nodes. Moreover, the MAC, physical, and channel components are all involved in the transmission of a message. This non-modular architecture does not facilitate the development of new MAC protocols. For all these reasons, NS-2 was not selected[18].

SensorSim is a WSN simulator built on NS-2. It provides additional features for modeling sensor networks including channel sensing, sensor and battery models, lightweight protocol stacks for WSNs, scenario generation. However, it remains unfinished and without any support or maintenance. Consequently, it was excluded.

J-Sim is a component-based simulation environment developed entirely in Java. Therefore, J-Sim is platform independent and its models are easily reusable and interchangeable offering the maximum flexibility. It provides real-time process-based simulations and offers a considerable list of supported protocols, including a WSN simulation framework with a very detailed model of WSNs. However, it is not easy to use [Singh08] and presents relative slow execution times. Therefore it was not selected.

[18] Despite of the recent NS-3 simulator having improved diverse shortcomings of NS-2, namely the scalability in terms of memory usage and the simulation run-time, most of the mentioned drawbacks remain valid.

OPNET is a discrete event, general purpose network simulator. It was originally built for the simulation of wired networks and contains extensive libraries of accurate models from commercial wired network hardware and protocols. However, OPNET offers only a few ready models for recent wireless systems. The strength of OPNET in wireless network simulations is the accurate modeling of the radio transmission. Different characteristics of physical-link transceivers, antennas, and antenna patterns are modeled in detail. OPNET can also model three-dimension outdoor scenarios and take into account different kinds of obstacles like terrain shape and buildings. Since OPNET is a commercial tool, it was not considered.

TOSSIM is an emulator for WSNs specifically designed for TinyOS applications to be run on Mica motes. It simulates the hardware of these sensor nodes at bit level, i.e., an event is generated for each transmitted or received bit, instead of one event per packet. Simulated application code can be transferred directly to the testbed, and vice-versa. TOSSIM assumes a probabilistic bit error model for the wireless medium, which makes it unrealistic in evaluating low-level protocols. Moreover, every node must run the same code, which limits the convenience of this emulator. TOSSIM does not have an energy consumption model, which is important in WSNs. All these reasons, along with the fact that Mica motes are not used in this work, were sufficient to decline it.

COOJA is a Java-based simulator conceived for WSNs running the Contiki operating system [Dunkels04]. It is able to simulate the application, operating system, and hardware levels. In the application level, nodes run the application logic coded in Java. In the operating system level, nodes use the same Contiki code as real nodes. In the hardware level, nodes run the same object code as used in the real nodes. COOJA was not chosen, because it is oriented for a specific WSN operating system.

OMNeT++ is a framework which provides the basic tools to write discrete-event simulators. OMNeT++ scales well for large network sizes, but it does not provide by itself any specific components for computer network simulations. However, its user community has provided support mainly for standard wired and wireless IP networks, although some extensions for WSN exist. Yet, suitable protocols and proper energy modeling for sensor networks are lacking. Therefore, OMNeT++ was not considered as primary development platform.

MiXiM is an open-source merger of several OMNeT++ frameworks written in C++ to support mobile and wireless simulations. It provides detailed models of wireless channel, connectivity, mobility, obstacles, and diverse MAC protocols (e.g., IEEE 802.11, IEEE 802.15.4). MiXiM provides modules for easy implementation of new MAC protocols. Despite of its attractive features, MiXiM was not chosen because it was in development by the time this work needed a simulator. Instead, Castalia was chosen for the motives presented next.

5.2.2 Castalia Simulator

Castalia is a discrete event-driven simulator, programmable in C++, which uses OMNeT++ as base platform. From the range of network simulators initially considered, Castalia[19] (version 2.3b) was selected to implement the simulation platform, because it is an open-source simulator conceived specifically for WSNs, with support and maintenance from its developers. Indeed, Castalia has gained wide acceptance in the WSN research community, with a number of citations in the literature [Pediaditakis10], since it presents diverse advantages. Castalia is designed for adaptation and expansion, which is fundamental to implement new algorithms and protocols, such as AR-MAC. Moreover, Castalia presents a modular architecture, which is an important aspect when considering the implementation of new MAC protocols. Castalia is suitable to implement e-health scenarios, since it includes BSN models for temporal variations and average path losses. These models were based on real on-body measurements. Its authors claim that Castalia is the most realistic simulator for WSNs and BSNs concerning the wireless channel, even among the commercial simulators [Boulis09].

Castalia uses the communication model proposed in [Zuniga04], which explained empirically measured data (more specifically packet reception rate as a function of distance) from WSN platforms by combining known wireless channel and radio models. Castalia offers three interference models: (*i*) no interference - interferences are never considered; (*ii*) simple collision - two transmissions partially overlapped are both

[19] In the Greek mythology, Castalia was a nymph who was transformed into a fountain at Delphi, at the base of Mount Parnassus. Castalia was regarded as a source of poetic inspiration.

discarded; and (*iii*) additive interference - the signal interference ratio is calculated considering all possible interferences from other sensor nodes. Thus, the model proposed in [Zuniga04] is augmented in the sense that Castalia may not use static packet reception probabilities for the links between the nodes[20], but these probabilities may be calculated dynamically based on the transmission power of all transmitting nodes. Castalia allows multiple transmission powers and uses a complex model for temporal variation of path loss. It provides parameters to model accurately the physical layer in accordance with the transceiver characteristics, and packet buffers to all communication layers. The behavior of the radio is also carefully modeled with respect to carrier sensing, transitions between various states, and energy consumption. Diverse MAC protocols are implemented in Castalia, namely IEEE 802.15.4, S-MAC, and T-MAC [Dam03] protocols. Castalia also features clock drift, sensor and CPU energy consumption, and monitors resources such as energy in the battery, memory usage and CPU time. Fully mobility of the nodes is supported too.

The sensed physical phenomena are very often not modeled in WSN simulators. The usual practice is to attribute static or random numbers to nodes or run the nodes with traces of sensed data. Castalia offers a generic physical process model with correspondence to real processes (e.g., spatial correlation of data, variability over time). Castalia also presents a set of parameters to model the physical process distortion due to inaccuracies of the sensing devices (e.g., noise, bias, saturation, sensibility). This issue is rarely taken into account in WSN simulations.

Despite of being specifically oriented to WSNs, Castalia and most of the generic network simulators, including those presented in the last section, do not model the very limited computing resources of sensor nodes. Consequently, these simulators cannot produce very reliable results on real-time WSN scenarios, because operating system and layer code execution delays are not taken into account. These simulators need to be extended or modified for more accurate WSN simulations [Korkalainen09]. As discussed in the next chapter, Castalia was extended with a parametric model in order to improve appreciably its accuracy.

[20] Castalia allows a user to define a specific connectivity map among pairs of nodes, for instance, measured from a real testbed. The user can specify the received signal power among nodes or just define packet reception probabilities among different nodes. For example, the user can specify that packets transmitted from node *n* to node *m* with a power level *w* have a reception probability equal to *p*.

5.2.2.1 Castalia Structure

Castalia uses a model based on modules and messages. A simple module is the basic unit of execution. Modules communicate through passing of messages. A module accepts a message from other modules or itself and according to the message it executes the respective code. The code can keep state, which is altered when messages are received, and can send or schedule new messages. There are also composite modules. A composite module is just a construction of simple modules and/or other composite modules. A sensor node is an example of a composite module, as shown in Figure 5.1.

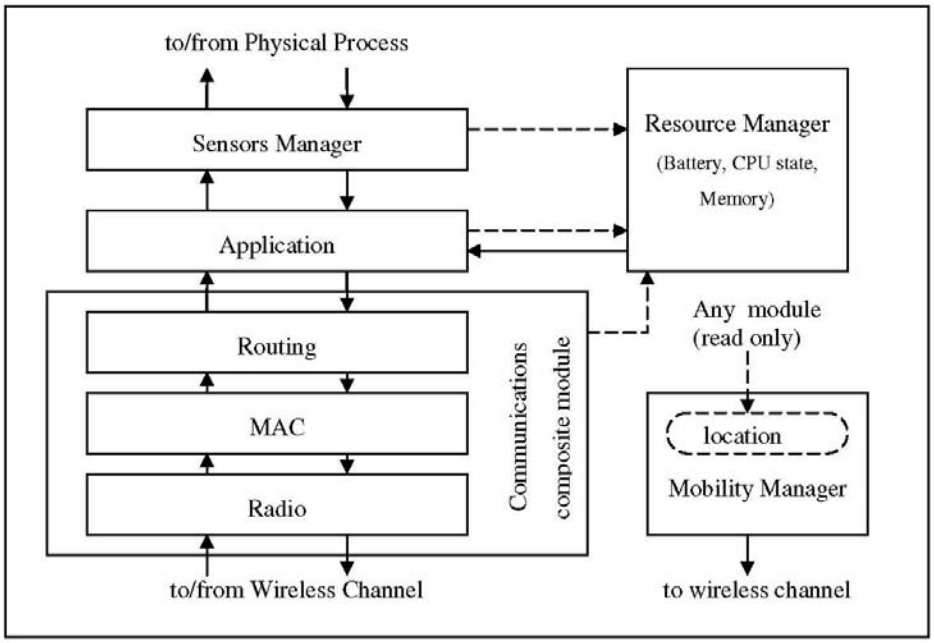

Figure 5.1 – The node composite module.

Nodes do not connect to each other directly but through the wireless channel module. When a node has a packet to send this goes to the wireless channel, which then decides which nodes should receive the packet. The nodes are also linked through the physical processes that they monitor. There is a one-to-one correspondence between a sensing device type and a physical process module. So, for one physical process there is one module which the nodes sample in space and time to get their sensor readings. There can be multiple physical processes, representing the multiple sensing device types that a node might have, as well as multiple wireless channels to represent the multiple radio

transceivers that a node might have operating orthogonally (e.g., different frequencies or different codes), as illustrated in Figure 5.2.

Castalia treats all entities as objects. During a simulation run-time, each sensor node is instantiated by a distinct and unique object in the memory of the computer. For example, if a simulation runs ten sensor nodes, then ten node objects are created. Also, every simple or compound module used during the simulation is instantiated by an object. So, there are also ten application modules, ten sensing device manager modules, ten MAC modules, and so on, each module instantiated by an object. However, if all radio transceivers operate non-orthogonally in the same channel, then there is only one Wireless Channel Module.

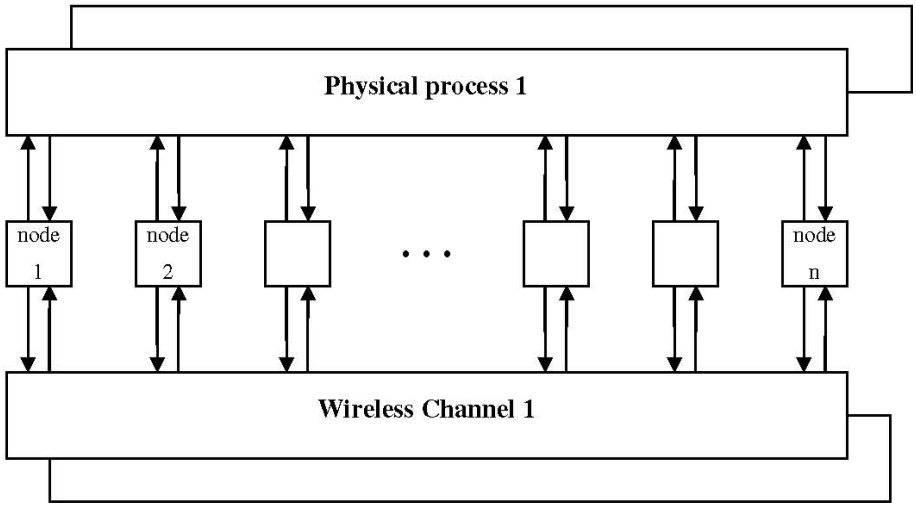

Figure 5.2 – The modules and their connections.

5.2.3 Castalia as Simulation Platform

There was a long way to go since the moment Castalia was installed in the computer until a fully operational e-health simulation platform was ready to use. It was required to implement AR-MAC protocol in Castalia, the whole application functionality, as well as all auxiliary functions required to obtain network communication statistics, as Castalia provides no facility to achieve this goal. To accomplish these issues, it was necessary to write about 360 kB of C++ source code.

The only way of Castalia-2.3b outputting results is writing them to a text file along

the simulation run-time. Once all simulation runs are over, the output file contains for each run results relative to each node and each BSN. Afterwards, a developed auxiliary tool parses the output file of Castalia, calculates the several statistics and creates multiple files properly formatted. A plotting program is then invoked to show graphically the experimental results.

In order to have a user-friendly simulation environment, a framework was developed to integrate all these procedures. The user configures a text file containing diverse operational parameters and then the framework automatically runs Castalia, presents the test graphics to the user, and save them in the directory specified by the user.

The configuration file allows changing easily multiple aspects of the simulation platform, including, but not limited to, the number of BSNs, the number of sensor nodes per BSN, the sampling rate of each type of sensor node, the superframe specifications, the MAC protocol scheme (i.e., based on TDMA or CSMA), the used TDMA MAC protocol (AR-MAC, LPRT, IEEE 802.15.4/GTS), and the interfering traffic parameters.

The simulation framework can provide performance evaluation tests regarding the (maximum, average, minimum) packet delivery ratio, goodput, (maximum, average, minimum, deviation mean root, variance) delay and jitter, scalability, and power consumption. These are the usual metrics for testing the QoS performance of a MAC protocol in a WSN. Reconfiguration metrics, as well as usage NRP and usage ERP metrics are also available to test unique characteristics of AR-MAC.

Simulations always require certain assumptions about the real world, which may lead to results and conclusions which do not reflect the behavior of real WSNs. For example, simulations commonly do not model the limited computing resources of sensor nodes. The omission of this important characteristic may affect negatively the accuracy of the simulation results. In order to have confidence on the simulation results, these should be corroborated, at an initial phase, by tests carried out in a physical testbed. This important aspect motivated the implementation of a physical testbed too.

5.3 Physical testbed

This section presents the physical testbed implemented in this work. This testbed was built mainly to validate the results of the simulation platform. Also, it was used in an ambient assistance living project [Gama10].

First, it is described the ZigBit-A2 chip and the transceiver used in the sensor nodes. Then, the devices and equipment developed for the testbed, including the sensor nodes. Finally, it is introduced the physical testbed.

5.3.1 ZigBit-A2 Module

The ZigBit-A2 is an IEEE 802.15.4/ZigBee-compliant module operating in the 2.4 GHz band. Each module contains one AT86RF230 transceiver coupled to a dual chip antenna and one ATmega1281V microcontroller comprising 128 kB flash memory, 4 kB EEPROM, and 8 kB SRAM. The ZigBit-A2 architecture is shown in Figure 5.3.

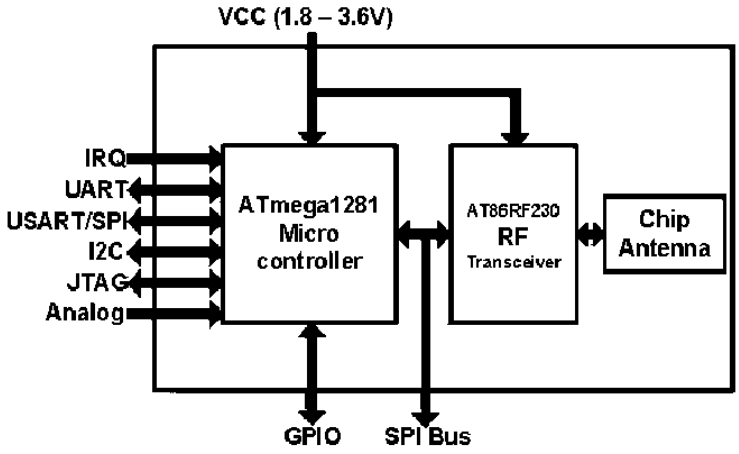

Figure 5.3 – Architecture of ZigBit-A2 modules.

ZigBit-A2 modules run the TinyOS operating system. The physical layer and some MAC layer functions of the IEEE 802.15.4 standard are implemented in the transceiver's firmware of ZigBit-A2. This firmware code is not open source. The remaining part of the MAC layer functionality is implemented openly in nesC and runs

in the ZigBit-A2 microcontroller. User applications are developed in C code, following an event-oriented approach.

ZigBit-A2 modules may operate in diverse modes: *sleeping*, *idle-listening*, *receiving*, and *transmitting*. The sleeping mode may be full or partial. In full-sleeping mode, both the microcontroller unit (MCU) and the transceiver are off. In partial-sleeping mode, only the transceiver is off. In idle-listening mode, the receiver listens to the channel persistently for packet reception. In this mode, as well as in receiving and transmitting modes, the MCU and the transceiver are on.

As measured power consumption may diverge from what is expected from manufacturer datasheets [Figueiredo10], the ZigBit-A2 current consumption in the diverse operating modes was measured directly in a board, where ZigBit-A2 was the only load in the circuit. Table 5.1 presents the measured values. The current consumptions obtained from the ZigBit-A2 datasheet are indicated too. In order to evince clearly the contribution of the diverse subsystems to the power consumption of a sensor node, Figure 5.4 shows the power consumption of both a ZigBit-A2 module operating in diverse modes and an ECG signal acquisition module, which is described in [Gama10].

operating mode	**transceiver ON**	**MCU ON**	**measured value (mA)**	**from ZigBit datasheet (mA)**
transmission	yes	yes	18.6@ 3.0dBm, 17.8@ -0.2dBm 16.8@ -3.2dBm, 13.5@ -17.2dBm	18@ 0dBm
receive	yes	yes	18.4 (55.2 mW)	19
idle listen	yes	yes	18.2 (54.6 mW)	n/a
partial sleep	no	yes	5.2 (15.6 mW) [21], 7.2 [22]	14 [23]
full sleep	no	no	0.0051 (0.0153 mW)	0.006

Table 5.1 – ZigBit-A2 current consumption (Vcc = 3V).

[21] MCU with no load.
[22] MCU increments continuously an integer variable.
[23] MCU alternates between 50% load mode and sleep mode each 10 s. The 50% MCU load is simulated by alternating between 100% MCU load in dummy loop and staying idle during the same period.

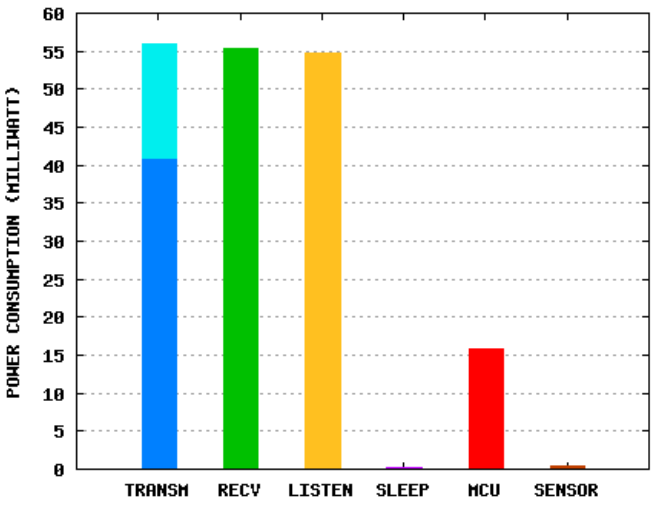

Figure 5.4 – Power consumptions in the ZigBit-A2 and ECG sensor modules.

Energy preservation is an important topic in WSNs, because sensor nodes are operated by low-capacity batteries. As the available energy *e* in a battery with *n* cells, having each cell *v* Volt and a capacity of *c* milli-Ampere.hour is:

$$e = 3.6 \times n \times v \times c \text{ Joule} \quad (5.1),$$

a sensor node with a power consumption *w* Watt may live *e* / *w* seconds at maximum. The average power *w* used by a node consists of the average power consumed by receiving (w_r), transmitting (w_t), listening (w_l), sleeping (w_s), and data sampling (w_d) operations [Polastre04]:

$$w = w_r + w_t + w_l + w_s + w_d \quad (5.2).$$

5.3.2 Radio Transceiver

As mentioned, each ZigBit-A2 module includes one AT86RF230 radio transceiver. Table 5.2 presents the transceiver consumption in sleeping, listening, and receiving mode obtained from the AT86RF230 technical specifications. The sleeping state may be partial or full. In partial-sleeping state, the serial peripheral interface (SPI) and the crystal oscillator are enabled. The microcontroller can access all digital functions, including the frame buffer. In full-sleeping state, the entire radio transceiver is disabled.

No circuitry is operating, and the power consumption is due to leakage current only. Table 5.3 shows the state transition delays of the AT86RF230 transceiver.

transceiver state	power consumption (mW)
transmission	49.5@3dBm, 43.5@1dBm, 37.5@-3dBm, 28.5@-17dBm
receive	46.5
idle listen	46.0
partial sleep	4.5
full sleep	0.00006

Table 5.2 – AT86RF230 power consumption specifications (Vcc = 3V).

transceiver state transition	delay (ms)
full sleep to listen	1.060
partial sleep to listen	0.180
listen to full sleep	0.036
listen to partial sleep	0.001
transmission to full sleep	0.036
transmission to partial sleep	0.001
full sleep to transmission	1.060
partial sleep to transmission	0.180
listen to transmission	0.181
transmission to listen	0.181

Table 5.3 – AT86RF230 specifications for state transition delays.

The values presented in Tables 5.1, 5.2 and 5.3 are important since they affect directly the power consumption of the sensor node. The simulation platform was parameterized with these values in order to perform realistic energy efficiency studies.

5.3.3 Devices and Equipment

The developed sensor nodes, as well as the BS, the channel analyzer, the packet sniffer and the communication cables used in the testbed are presented next.

Sensor Nodes. In order to build a physical testbed, wireless sensor nodes were projected and mounted in printed circuit boards (PCBs). The PCB layout was designed with a computer-aided design program. Figure 5.5 shows an assembled sensor node. Although the PCB could be made smaller, the final dimensions (29.5 x 33.0 mm) were dictated by the available ECG signal acquisition and conditioning module. One module can be connected to the board to collect a physiological signal, such as ECG or oximetry. The block diagram of the internal circuits within the developed sensor node is shown in Figure 5.6.

Sensor nodes were built-in based on ZigBit-A2 (or ATZB-24-A2) modules. This device was selected because it is one of the most competitive modules, when the dimensions must be taken into account. There are many other available modules, even smaller, but they require auxiliary external circuitries, leading to larger devices. Moreover, the ZigBit module was selected because it offers the possibility of modifying the code of the MAC layer. This facility allowed that the code of the AR-MAC protocol was included in the ZigBit-A2 modules.

BS. The testbed uses the BS included in the kit available from the manufacturer. Since the BS is also built-in based on a ZigBit-A2 module, in terms of software performance the BS is identical to a sensor node.

Channel analyzer. This equipment is used to identify interferences from IEEE 802.11, ZigBee, Bluetooth, and other 2.4 GHz devices, so that a free channel can be chosen to improve the reliability of the performance tests. A channel analyzer (Wi-Spy 2.4x) connected to a USB port of the computer is shown in Figure 5.7.

Packet Sniffer. This is a very useful tool for debugging network tasks. Figure 5.7 shows the packet sniffer used in the testbed. It is a node of the kit programmed to capture packets sent to the channel without collision, including beacon frames, and on-the-fly sends to the computer data about the captured packet (e.g., source address, payload size, ACK bitmaps, used time-slot) to be shown in the computer display.

Communication cables. The object code is loaded from the computer into the sensor node through a USB-to-TTL serial converter cable (TTL-232R-3V3). An adapter was built to make the interface between this cable and the sensor node. The BS and the

packet sniffer communicate with the computer through a USB cable. Both cases are shown in Figure 5.7.

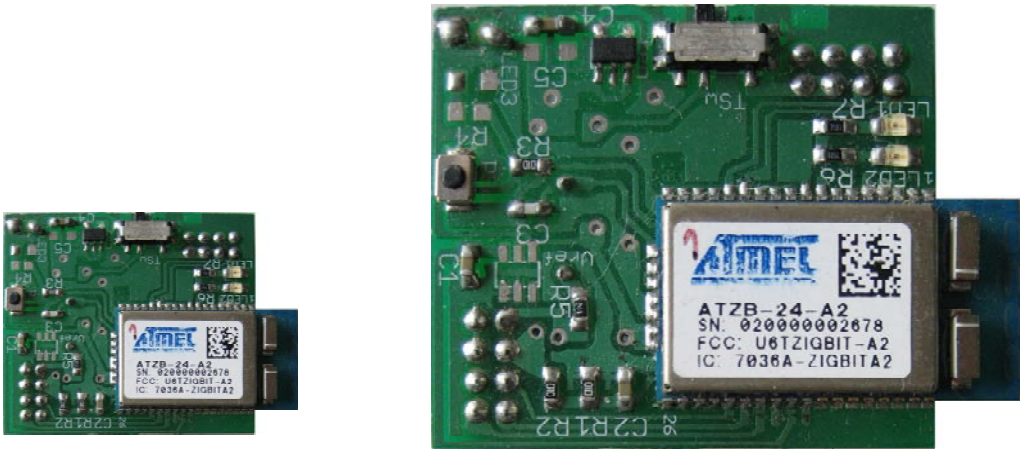

Figure 5.5 – Developed sensor node in real size (left) and magnified twice (right).

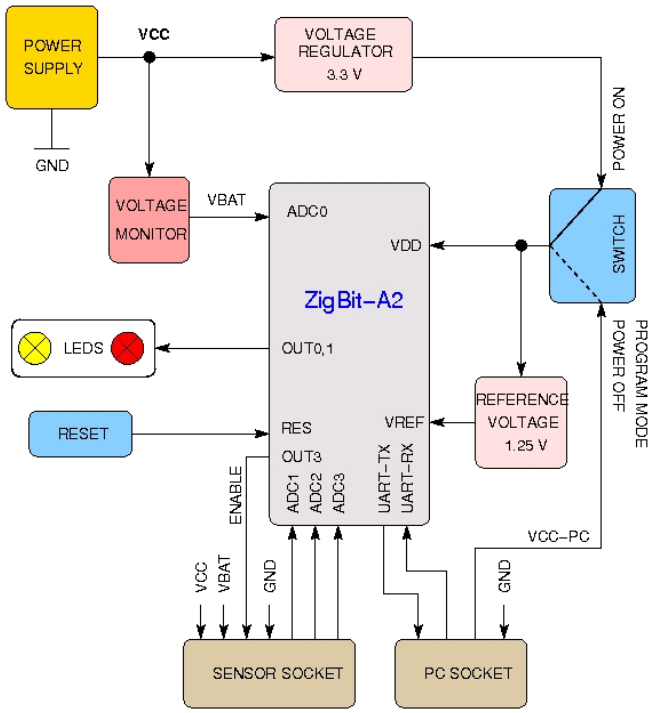

Figure 5.6 – Block diagram of the developed sensor node.

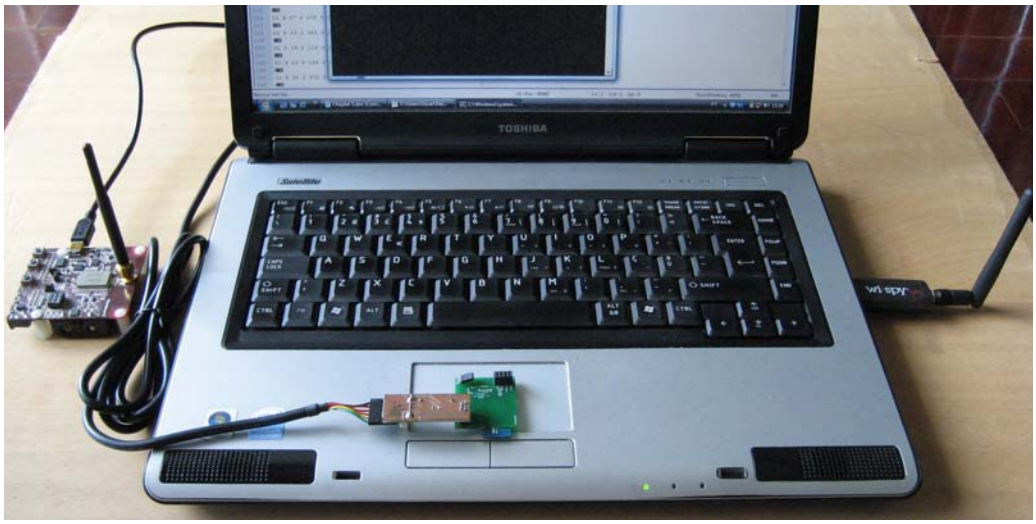

Figure 5.7 – The sniffer device (left), a sensor node coupled to the adapter (center), and the channel analyzer (right).

5.3.4 Physical Testbed

The physical testbed used in this work is shown in Figure 5.8. It is composed of a reference WSN and an interfering WSN.

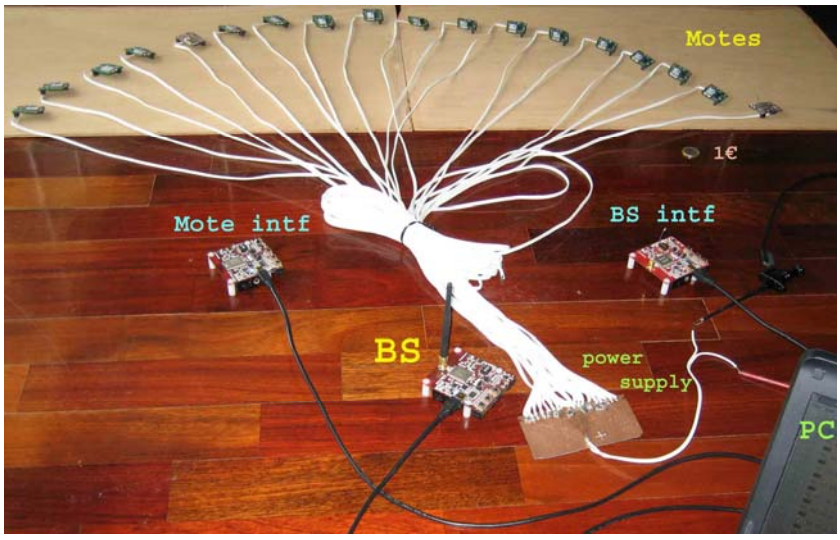

Figure 5.8 – Complete physical testbed, with the reference and interfering WSNs.

5.3.4.1 Reference WSN

The reference WSN is composed of sixteen ZigBit-A2 sensor nodes placed statically in a semi-circle around the BS. To avoid the cumbersome task of power management, the sensor nodes are energized at 4.5 V through the white cables shown in Figure 5.8. These power cables impose a maximum distance of around three meters between the sensor nodes and the BS. The reference WSN cannot admit more than sixteen sensor nodes due to the RAM memory limitation of the BS. Indeed, a minimum amount of memory in the BS is required to hold data for packet statistical analysis, and this memory size depends on the number of active sensor nodes in the WSN. The BS of the reference WSN is connected to the serial port of a computer, with a link rate of 500 kb/s.

5.3.4.2 Interfering WSN

The interfering WSN is composed of a coordinator (*BS intf*) and one sensor node (*mote intf*), as shown in Figure 5.8. This IEEE 802.15.4 network is used to inject controlled interfering traffic on the channel used by the reference WSN. Both WSNs have distinct personal area network identifications, and are close enough to sense the carrier signals mutually.

5.3.5 Testbed as Evaluation Platform

Beyond the hardware development aspects of the testbed, it was also necessary to implement the AR-MAC protocol and the application logic in the ZigBit-A2 nodes. The accomplishment of these tasks required the writing of about 245 kB of C source code for the BS and sensor nodes. Auxiliary functions were also developed to obtain network communication statistics.

Depending on whether the testbed is used to evaluate the performance of protocols and algorithms or whether it is used to deliver traffic with real-time requirements, the BS may treat the received data differently.

If the testbed is used to evaluate the performance of protocols and algorithms, then

data content is usually irrelevant. In this case, the BS may perform statistical calculations with the received data, thus avoiding forwarding important amounts of data to the computer, which improves the network scalability. Unlike the simulation platform, statistics are calculated on-the-fly since the memory capacity of the BS does not allow storing much data. The statistics for each sensor node are sent regularly to the computer. It was noted that when the BS is sending data to the computer through the USB port, the capacity of the BS to receive or transmit packets becomes significantly reduced. To reduce the influence of this aspect on the final results, the BS sends to the computer every two minutes only the relevant statistics of the traffic flow received from each sensor node relative to this time period. This transfer occurs in a time period free of data transmissions from sensor nodes.

Identically to the simulation platform, the computer registers the received statistics from the BS in a text file. Once the execution time is over, a developed auxiliary tool parses the output file in the computer, calculates the diverse statistics and creates multiple files properly formatted. A plotting tool is then invoked to show graphically the experimental results. In order to improve the user-friendliness of the testbed, a framework was developed to integrate all these procedures.

The physical platform can provide performance evaluation tests regarding the (maximum, average, minimum) packet delivery ratio, goodput, (maximum, average, minimum, deviation mean root, variance) latency, scalability, power consumption, reconfiguration metrics, as well as NRP and ERP usage metrics. This set of parameters includes the usual metrics for testing the performance of a MAC protocol in a WSN.

If the testbed is used to deliver traffic with real-time requirements (e.g., physiological data), the BS receives application data from sensor nodes and immediately forwards them to the computer, where data may be processed or stored. The BS does not perform any high-level operation or statistical calculations on the received data to ensure the real-time requirements of the e-health network. However, the network scalability is significantly affected, because larger super time-slots are required to receive data from a sensor and forward them to the computer. A tool was developed to view the physiological signal varying dynamically along time frames, as well as diverse statistical data relative to the received signals, such as the lost samples ratio, lost packet ratio, and goodput. Latency is not possible to calculate because data packets carry no time-stamps. Figure 5.9 shows a three-lead ECG signal received wirelessly with the AR-MAC protocol.

Table 5.4 presents the characteristics of the code developed to implement the physical testbed, as well as for the simulation platform.

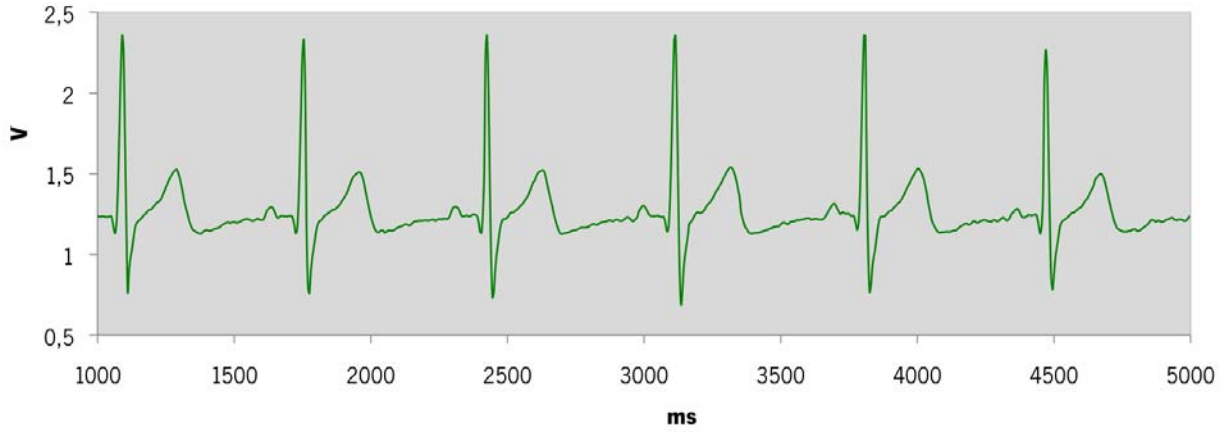

Figure 5.9 – Three-lead ECG signal sampled at 200 Hz.

platform	developed source-code	size (kB)	language
physical	BS and sniffer	135	event-driven C
	sensor nodes	110	event-driven C
	statistical + visual tool	92	C
simulation	simulator	360	C++
	statistical tool	30	C

Table 5.4 – Characteristics of the code developed for the physical and simulation platforms.

5.3.6 Testbed Use Experience

Using the physical testbed may be a fastidious and time-consuming task. For example, if the testbed needs to be used with a new set of operational parameters or if a new functionality is required, all sensor nodes must be reprogrammed. In both cases, the

sixteen nodes must be disconnected from the power supply, reprogrammed individually, and reconnected to the power supply, giving raise to the possibility of having nodes connected with the wrong polarity. The whole process takes around thirty minutes. If a bug is detected in the new functionality, the whole process must be repeated all over again after fixing the bug. Sending configuration parameters in the beacon payload alleviates the parameter redefinition problem but does not solve it, because there are many reconfiguration parameters in the testbed and the beacon payload size is very limited. The management of the MAC address may be another challenging task in the testbed, because every time a sensor node is programmed, its MAC address must be defined again, which may originate duplicate or wrong MAC addresses. Electrostatic discharge is also a serious problem, because ZigBit-A2 nodes are sensitive to it. Six sensor nodes were damaged due to this phenomenon. Moreover, a run-time of 4¼ hours is required to complete each one of the physical tests presented in the next chapter, assuming that the BS or a sensor node do not crash during the run-time; otherwise the test needs to be repeated again from the beginning.

For all these reasons, most of the evaluation tests presented in this work were carried out in the simulation platform. The physical testbed was mainly used to verify the results obtained with the simulation platform.

5.4 Summary

This chapter has described the simulation and physical platforms used in this work. The former is used to carry out evaluation and comparative performance tests of AR-MAC protocol in an e-health scenario. The latter is mainly used to corroborate the results obtained on the simulation platform.

As mentioned, Castalia and most of the generic network simulators do not model the very limited computing resources of sensor nodes, which is a key characteristic of WSNs. If ignored, this aspect may affect significantly the meaningfulness of the simulation results. This important topic will be discussed in detail in the next chapter, as well as the validation issue of the physical and simulation platforms.

Chapter 6

Parametric Model to Improve Simulation Reliability

6.1 Introduction

Network simulators are often used to study multiple aspects of data communications in distinct scenarios, including WSNs. However, simulation results may diverge considerably from the reality for diverse reasons, as pointed out next.

WSN simulation studies use frequently unrealistic assumptions, such as, flat physical environment, circular radio transmission area, equal range for all radios, channel with bidirectional symmetry, simple relation of signal strength with distance, and no fading or shadowing phenomena. A large set of measurements showed that these assumptions cause simulation results to differ significantly from experimental results [Kotz04].

Since simulators can use different models to represent the same physical phenomenon, appreciable divergences in the results may be obtained when using distinct simulators. The performance results of a simple algorithm using diverse simulators proved this fact [Cavin02]. Furthermore, models cannot represent reality with absolute accuracy [Banks96]. Simulation scenarios can also ignore diverse hardware and software aspects that may influence the final results. Examples of these aspects are the time required by the BS and sensor nodes to process the incoming or outgoing packets, the queuing delay in the transmitting and receiving buffers, the time required to switch channels between transmitting and receiving mode, and the link speed between the BS and the decision center, as explained later. Moreover, simulation tests usually do not consider any external interfering traffic on the WSN. This aspect is important when the WSN operates in license-free bands. For example, an IEEE 802.15.4 WSN operating in the 2.4 GHz band may have to share channels with IEEE 802.11 WLANs. These aspects may lead to simulation results significantly different from those obtained in a real WSN.

6.1.1 Studies on Validation of Simulators

Studies presenting experimental validation tests of simulators against results obtained in real networks are not abundant, due to the big effort usually required to implement a real testbed. The economical costs required to build a real testbed is another reason.

The accuracy of the NS-2 simulator is evaluated in [Ivanov07]. The authors compare the network characteristics of a simulated and a real IEEE 802.15.4 multi-hop mesh wireless network with sixteen stations in a static indoor environment. The results showed that the packet delivery ratio, the connectivity graph, and the packet latency are represented in the simulated model with an average error of 0.3%, 10%, and 70%, respectively.

The experimental validation results for the SWAN simulator [Perrone02] showed that the simulations with the two-ray ground radio propagation model differ from reality in around 80%, while with the shadowing model differ about 10% in an outdoor mobile IEEE 802.15.4 network [Kotz04] [Liu04].

The reliability of OMNeT++ is evaluated in [Colesanti07]. The authors consider an experimental setup made of six sensor nodes to test the performance of the flooding algorithm. The results of the testbed are compared with the results of the simulations of the same scenarios on OMNeT++. Experiments showed that simulation results tend to overestimate the metrics collected in the testbed.

To validate some high-level aspects of Castalia, the authors of this WSN simulator deployed a real network involving nine sensor nodes [Pham07]. Important differences in the results from the real network and the simulation were noted.

It is also shown in [Bergamini10] that the use of NS-2 and Castalia simulators with default configurations may produce unreliable results.

The authors of all these works were unable to justify satisfactorily the registered differences.

6.1.2 Motivation for a New Simulation Model

Aware of the difficulty that a network simulator may have in presenting accurate results, diverse tests were carried out in the physical testbed to validate the simulation results. These tests allowed identifying diverse software-related aspects of a WSN that contribute to the differences found in simulation results against real measurements. This is an important aspect that is usually neglected in WSN simulators, including Castalia. As presented in the next section, first it is evaluated in the IEEE 802.15.4 domain how the results obtained in a simulated WSN differ from those obtained in an analogous physical scenario. Then, the causes of the divergences in the results are identified.

Finally, a model using empirical software-related parameters is proposed to improve the accuracy of the simulation results. Instead of trying to present accurate values for the model parameters, which are necessarily specific to each testbed, the objective is to identify and model software-related issues which have influence on the testbed results, and which may also occur in other WSN test platforms. The proposed model is generic to be easily implemented in current WSN simulators, being also an important contribution for future development of simulation tools.

6.2 Setup of the Test Platforms

This section presents the test conditions used in the physical and simulation experimental platforms.

To evaluate the impact of software components in the performance of a WSN, a static, small-area WSN was adopted to minimize the effects of additional source of errors, such as nodes mobility, fading and shadowing phenomena. For this reason, the sixteen ZigBit-A2 sensor nodes of the reference WSN were placed statically around the BS in a semi-circle with a radius of one and half meter approximately, as shown in Figure 5.8. To study the validity of the model proposed in this work in a different test scenario, controlled traffic from the interfering WSN is admitted on the channel used in the reference WSN.

The scenario described for the physical testbed was equally implemented in the Castalia simulator. The simple collision model was used because it facilitates debugging the simulation platform. Moreover, as the considered WSN area is relatively small, the results obtained with this model are equal to those obtained with the additive interference model.

6.2.1 Test Conditions

The non-slotted CSMA-CA MAC protocol described in IEEE 802.15.4 standard [IEEE4] was used in the reference and interfering WSNs. In the reference WSN, the CSMA-CA algorithm used the default parameters: the minimum backoff exponent is

three, the maximum number of backoffs is four, and the maximum number of frame retries is three. The interfering WSN also used these parameters except the maximum number of frame retries, which is zero for the reason presented in the following.

As regards the workload in the reference WSN, each sensor node transmits to the BS a packet with a total length of 107 bytes (B) (17 B of physical and MAC overhead plus 90 B of MAC payload) every 250 ms, approximately. It should be noted that IEEE 802.15.4 standard specifies a maximum physical packet size of 133 B. In the interfering WSN, a sensor node sends a packet of fixed size (100 B of MAC payload) to the BS every 50 ms, approximately. Therefore, the maximum number of frame retries is zero to guarantee that each execution of the CSMA algorithm ends before 50 ms.

The reference WSN was configured to operate in a wireless channel free of IEEE 802.15.4 traffic. For this purpose, a channel analyzer was used to find free channels. It was selected the channel twenty five of the IEEE 802.15.4 spectrum. To reduce the impact of spurious interferences on this channel, sensor nodes transmit at maximum power (3 dBm).

The BS of the reference WSN is connected to the serial port of a computer, with a link rate of 500 kb/s. It was noted that when the BS is sending data to the computer, the capacity of the BS to receive or transmit packets is significantly reduced. To reduce the influence of this aspect on the final results, the BS was configured to send data to the computer every two minutes. Only the relevant statistics of the traffic flow received from each sensor node relative to this time period are transmitted to the computer.

Tests were carried out in the physical and simulation platforms for an increasing number of active sensor nodes in the WSN, with and without IEEE 802.15.4 interfering traffic in the selected channel. The test duration was sixteen minutes for each set of active sensor nodes. This duration was chosen as a compromise between the time required to carry out a complete test in the physical testbed (around 4¼ hours) and the time required to obtain a statistically significant set of packets. The results obtained are presented in the following.

6.3 Experimental Results

The results for round-trip delay and delivery error ratio (DER) obtained with the physical and simulation platforms are discussed next. These metrics were considered because they reflect the packet delay and loss, which are usually used to assess the QoS performance of a network. Both metrics are considered from the perspective of the application layer and, therefore, do not follow strictly the definitions provided by standardization organisms, such as IETF [IPPM-WG] or ITU-T [Glossbrenner99]. In the context of this study, round-trip delay is the time spent between sending an application data packet from a sensor node and the successful confirmation of the operation, which occurs after receiving the MAC ACK frame from the BS. As the round-trip delay of a packet is calculated using only the clock of the originator sensor node, no time synchronization mechanism is required[24]. DER expresses the probability of an application data packet sent from a sensor node to the application layer of the BS failing the delivery[25].

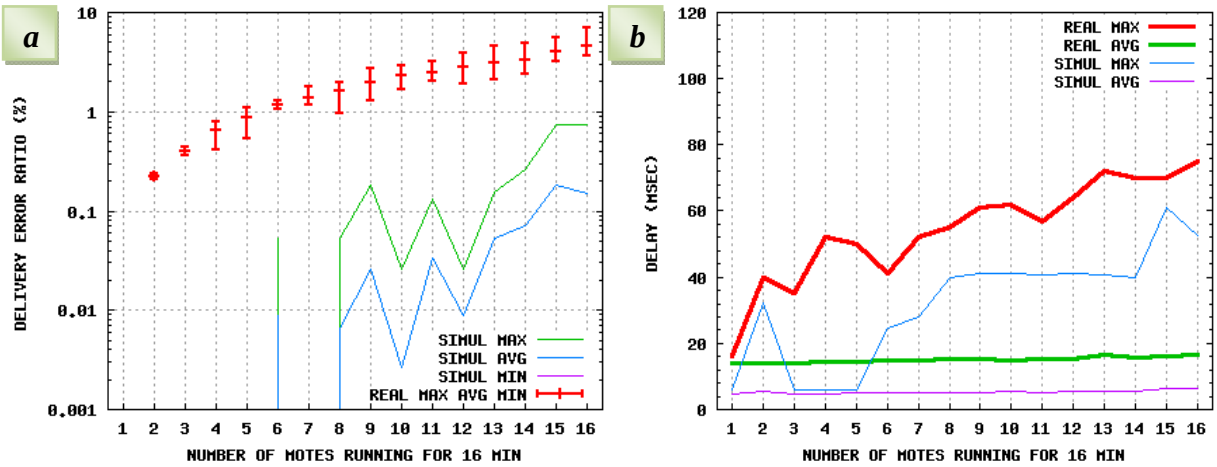

Figure 6.1 – (***a***) DER and (***b***) round-trip delay without interferences.

[24] Each packet carries in the payload the round-trip delay of the packet sent previously.

[25] The packet reception ratio (PRR) is not used to avoid ambiguity regarding the inclusion of the duplicate packets in this metric. Considering that duplicate packets are excluded, then DER = 1 – PRR.

Figure 6.1 presents the results obtained *without the presence* of interfering traffic. Figure 6.1*a* shows the simulation results for the DER when increasing the number of sensor nodes sending packets to the BS. The graphical bars correspond to the DER obtained in the physical testbed. For each number of active sensor nodes in the WSN, it is represented the maximum, average, and minimum DER values. Figure 6.1*b* shows the maximum and average round-trip delays obtained in the simulator and in the physical testbed. In Figure 6.1*a*, while the simulation results reveal a WSN scaling up to sixteen nodes with a maximum DER always below 1%, the physical testbed results show that above six active sensor nodes the maximum DER becomes higher than 1%. Figure 6.1*b* reveals that the delays obtained with the simulator are significantly distinct from the real results.

Figure 6.2 presents the DER and round-trip delay results obtained *with the presence* of interfering traffic. The results shown in both diagrams were obtained with the physical and simulation platforms. As expected, the network performance degrades before the presence of interfering traffic. The differences in the results registered in both test platforms are again considerably distinct.

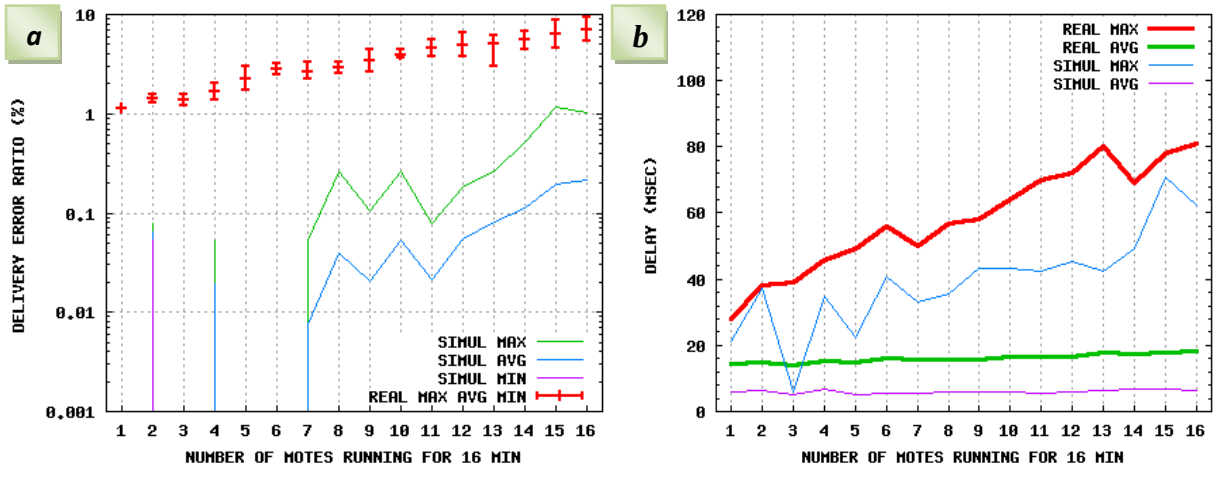

Figure 6.2 – (***a***) DER and (***b***) round-trip delay with interferences.

6.3.1 Causes of Divergence

The divergence in the results obtained with the physical and simulation platforms was identified as being caused mainly by the behavior of software components of the nodes and by the time drift, as discussed next.

Software Components. The first reason for the differences observed in the results is that the simulator does not take into consideration the behavior of the operating system used in the network devices, as well as the software execution time. As TinyOS can only schedule and handle single events and computing resources are very limited, non-negligible delays may occur in scheduling and processing those events. Processing software code of protocol stack layers also results in additional delays. Such overhead in terms of delay may be responsible for packet loss. To understand why, let us suppose that a packet has been received by the BS's transceiver. After processing it, the physical layer software triggers an event to forward the payload to the upper protocol layers. Since the delivering time to the application layer is not null, another packet may be received by the BS's transceiver during this transactional phase. In this case, TinyOS does not attend the hardware interrupt from the transceiver indicating that a new packet is ready to be transferred to the microcontroller, and the new received packet is dropped. This error situation was observed in the experimental testbed. It is possible that other operating system might attend the hardware interrupt from the transceiver signaling a new packet and drop the packet in process previously received. In both cases, an incoming packet is completely processed by the application layer of a sensor node only if its transceiver does not receive other packet during a specific time interval. Next, it is proposed a simulation model to reflect this real behavior. Its parametric nature makes the model generic and independent of the type of operating system and hardware used in the WSN.

It should be noted that TinyOS is not the most convenient operating system for implementing deterministic MAC protocols, because it uses a programming model based on split-phase operations and tasks. When the program calls a function, the call returns immediately, and the called function issues a callback when it completes. The called function may use a task for the callback, which is then placed in the task queue of TinyOS for execution. As other tasks might be already queued, there is no guarantee on how long it will take to conclude the execution of a specific task. So, TinyOS cannot

support deterministic behavior as required by TDMA-based MAC protocols [Suriyachai09].

Time Drift. The second reason for the differences in the results is that the sensor nodes present an appreciable time drift. The cause of this time drift is distinct of the CPU clock time drift, which is typically a few microseconds per second. While the latter is due to physical characteristics of the semiconductor components, the former is due to the software execution characteristics and the limited computing resources of the sensor nodes.

In summary, software components and time drift aspects may impact the reliability of the results. In order to bring simulation scenarios close to real environments, increasing the meaningfulness of simulations results, a new parametric model is proposed for inclusion in the simulator to minimize the differences to the physical testbed results.

6.4 Parametric Model

To obtain realistic results, network simulations need detailed channel and environment models, as well as detailed modeling of real properties of the nodes. This section presents a proposal to model the impact on a physical WSN of both the software components and the time drift of sensor nodes. Excluding emulators, generic simulators rarely consider any of these aspects in their simulation models [Korkalainen09].

The software components' modeling is discussed in the next section. The time drift modeling is considered in Section 6.4.2. The setting of the model parameters is discussed in Section 6.4.3.

6.4.1 Software Components' Modeling

In a single-hop network, an originator sensor node sends a packet to a recipient sensor node, which receives and processes it after a certain time delay. This latency is the sum of diverse delay components, as shown in Figure 6.3. These components, discussed in

the next section, include the delay induced by the scheduling tasks of the operating system and the software execution delays in both sensor nodes. Moreover, the time required by a sensor node to process a receiving packet may impact the packet loss ratio, because incoming packets may be dropped in a sensor node that is processing a received packet. Therefore, modeling the software components must conjugate aspects relative to the packet receiving and transmitting processes. These processes are detailed and discussed in the following sections. As consequence, a model for TDMA-based WSNs is then proposed, and its applicability for CSMA-based WSNs is also debated.

6.4.1.1 Packet Receiving Process

Let us consider that a BS received a packet from sensor node *n*. According to Figure 6.3, the delivery time parameters $T_{BS\ phy \rightarrow mac}(n)$, $T_{BS\ mac \rightarrow app}(n)$, and $T_{BS\ app}(n)$ must be considered.

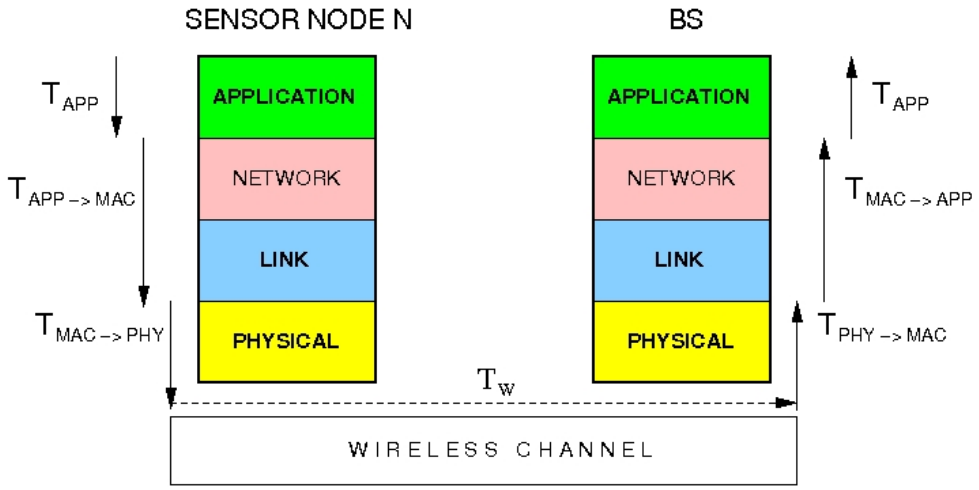

Figure 6.3 – Delay components involved in a packet transmission and reception.

The delivery time parameter $T_{BS\ phy \rightarrow mac}(n)$ reflects the time required by the BS to process the packet received from sensor node *n* at physical layer and deliver the payload to the MAC layer. Note that MAC layer tasks can be split between the transceiver and the microcontroller. In ZigBit sensor nodes, for example, address filtering, error detection, and ACK transmission operations of a receiving MAC frame are carried out

in the transceiver, but the MAC frame de-encapsulation and upper layer delivery are accomplished in the microcontroller. As the timings of the software components are very hard to be measured directly in the transceiver's firmware, the parameter $T_{BS\ phy\rightarrow mac}(n)$ is measured relatively to the MAC layer part in the microcontroller.

The parameter $T_{BS\ mac\rightarrow app}(n)$ indicates the time required by the BS to process the packet received from sensor node *n* at MAC layer and deliver the data to the application layer. Therefore, this parameter reflects both the event scheduling delay and the packet processing delay imposed by the link and network layer (the transport layer is not usually implemented in WSNs). In multi-hop networks, modeling of the routing layer is needed to evaluate the effect of the routing protocol and network topology on latency. However, in single-hop networks this aspect can be simplified to a constant delay component included in the parameter $T_{BS\ mac\rightarrow app}(n)$. The parameter $T_{BS\ mac\rightarrow app}(n)$ is measured relatively to the MAC layer part in the microcontroller.

The process time parameter $T_{BS\ app}(n)$ indicates the time required for the application layer of the BS to process the received payload from sensor node *n*. So, an incoming packet from sensor node *n* is completely processed at the application layer of the BS after a time interval $T_{BS\ totRX}(n)$:

$$T_{BS\ totRX}(n) = T_{BS\ phy\rightarrow mac}(n) + T_{BS\ mac\rightarrow app}(n) + T_{BS\ app}(n) \quad (6.1).$$

The delivery time parameter $T_{BS\ phy\rightarrow mac}(n)$ includes the following partial times: (*i*) the time required to receive the packet from sensor node *n*, $T_{RX}(n)$; (*ii*) the packet processing time in the physical layer and MAC layer part of the transceiver, $T_{BS\ phyRX}(n)$; and (*iii*) the time required by the microcontroller to read the bytes from the transceiver receiving buffer through the peripheral communication interface, $T_{BS\ pciR}(n)$:

$$T_{BS\ phy\rightarrow mac}(n) = T_{RX}(n) + T_{BS\ phyRX}(n) + T_{BS\ pciR}(n) \quad (6.2).$$

As mentioned in Section 4.4, a packet received from sensor node *n* with a physical header size PHY_h bytes, a MAC header plus trailer size MAC_h bytes, a MAC payload length $MAC_d(n)$ bytes, and a transmission rate *R* bits/s requires a receiving time:

$$T_{RX}(n) = (PHY_h + MAC_h + MAC_d(n)).8/R \quad (6.3).$$

The parameter $T_{BS\ phyRX}(n)$ is very hard to be measured directly, because it depends on the firmware performance of the transceiver. However, it can be obtained indirectly from the $T_{BS\ phy\rightarrow mac}(n)$ measurement, because $T_{RX}(n)$ and $T_{BS\ pciR}(n)$ are known.

Usually the peripheral communication interface between the microcontroller and the transceiver is a serial peripheral interface (SPI). In this case,

$$T_{pciR}(n) = (B_C + MAC_h + MAC_d(n)) \times (8/S_{clk} + T_{gap}) \quad (6.4),$$

where B_C is the number of bytes of the read command, S_{clk} is the SPI clock frequency, T_{gap} is the time gap between the less significant bit of the last byte and the most significant bit of the next byte. For ZigBit sensor nodes, B_C is 3 B, S_{clk} is 4 MHz, and T_{gap} is 250 ns. The described parameters related with the receiving process are summarized in Table 6.1.

symbol	meaning
$T_{BS\ totRX}$	time required by the BS to process completely an incoming packet.
$T_{BS\ phy\rightarrow mac}$	time required to process the packet at physical layer of the BS and deliver the payload to the MAC layer.
$T_{BS\ mac\rightarrow app}$	time required to process the packet at MAC layer of the BS and deliver the data to the application layer.
$T_{BS\ app}$	time required for the application layer of the BS to process the received payload.
T_{RX}	time required to receive a packet.
$T_{BS\ phyRX}$	packet processing time in the physical and MAC layers of the transceiver.
$T_{BS\ end}$	time instant when the BS ends processing a packet.
$T_{BS\ pciR}$	time required by the microcontroller to read the bytes from the transceiver's receiving buffer through the peripheral communication.
T_{gap}	time gap between the less significant bit of the last byte and the most significant bit of the next byte.
B_C	number of bytes of the read/write command.
S_{clk}	SPI clock frequency.

Table 6.1 – Notation associated with the receiving process.

6.4.1.2 Packet Transmitting Process

Analogously to the total receiving time, $T_{totTX}(n)$ is the total time required for sensor node *n* to complete the transmitting process of an application data packet. Hence, the application packet delay comes increased by the sum of $T_{totRX}(n)$ and $T_{totTX}(n)$, where:

$$T_{totTX}(n) = T_{app}(n) + T_{app\rightarrow mac}(n) + T_{mac\rightarrow phy}(n) + T_{conf}(n) \quad (6.5).$$

$T_{app}(n)$ is the time needed for the application layer of the sensor node *n* to prepare the data payload; $T_{app\rightarrow mac}(n)$ is the time required by sensor node *n* to deliver the data payload to the MAC layer and prepare the MAC frame; $T_{mac\rightarrow phy}(n)$ is the time required by sensor node *n* to deliver the MAC frame to the physical layer, prepare the packet and transmit it; $T_{conf}(n)$ is the time required for the application layer to obtain the confirmation of the transmission request success, as required in common MAC protocols (e.g., IEEE 802.15.4).

$T_{mac\rightarrow phy}(n)$ includes the following partial times: (*i*) the time required by the microcontroller to write the bytes in the transceiver's transmitting buffer and registers through the peripheral communication interface, $T_{pciW}(n)$; (*ii*) the packet preparing time in the physical layer and MAC layer part of the transceiver, $T_{phyTX}(n)$; (*iii*) the switching latency from listening state to transmitting state, $T_{l\rightarrow tx}(n)$; and (*iv*) the time required to transmit the packet, $T_{TX}(n)$, which is equal to $T_{RX}(n)$ in a single-hop network. So,

$$T_{mac\rightarrow phy}(n) = T_{pciW}(n) + T_{phyTX}(n) + T_{l\rightarrow tx}(n) + T_{TX}(n) \quad (6.6).$$

As for $T_{phyRX}(n)$, the parameter $T_{phyTX}(n)$ is very hard to be measured directly because it is related with the firmware performance of the transceiver. However, it can be obtained indirectly from the $T_{mac\rightarrow phy}(n)$ measurement, because $T_{TX}(n)$, $T_{BS\ pciW}(n)$, and $T_{l\rightarrow tx}(n)$ are known. $T_{l\rightarrow tx}(n)$ is obtained from the transceiver technical specifications of sensor node *n*.

If the peripheral communication interface between the microcontroller and the transceiver is a SPI, then $T_{pciW}(n)$ can be calculated using an expression analogous to Equation (6.4), being B_C the number of bytes of the write command. For ZigBit sensor nodes, B_C is 2 B, and $T_{l\rightarrow tx}$ is 0.18 ms.

After sending a packet, a sensor node must wait $T_{nextTX}(n)$ before sending another packet, where:

$$T_{nextTX}(n) = T_{totTX}(n) - T_{TX}(n) \quad (6.7).$$

This equation is important since it may limit the performance of sensor node *n* regarding data throughput or retransmission trials.

The described parameters related with the transmitting process are summarized in Table 6.2.

symbol	meaning
T_{totTX}	total time for sensor node to complete the transmitting process of an application data packet.
T_{app}	time needed for the application layer of the sensor node to prepare the data payload.
$T_{app \rightarrow mac}$	time required by the sensor node to deliver the data payload to the MAC layer and prepare the MAC frame.
$T_{mac \rightarrow phy}$	time required by the sensor node to deliver the MAC frame to the physical layer, prepare the packet and transmit it.
T_{conf}	time required for the application layer to obtain the confirmation of the transmission request success.
T_{pciW}	time required by the microcontroller to write the bytes in the transceiver's transmission buffer and registers through the peripheral communication interface.
T_{phyTX}	packet preparing time in the physical layer and MAC layer part of the transceiver.
$T_{l \rightarrow tx}$	switching latency from listening state to transmitting state.
T_{TX}	time required to transmit a packet.
T_{nextTX}	time that a sensor node, after sending a packet, must wait before sending another packet.
T_{totTX}	total time for a sensor node to complete the transmitting process of an application data packet.

Table 6.2 – Notation associated with the transmitting process.

6.4.1.3 Model for TDMA-based networks

Let us consider that the application timers of sensor node *a* and sensor node *b* trigger respectively at time T(a) and time T(b) to send application data, and that T(b) > T(a). Also, let us assume that both sensor nodes use a MAC algorithm which does not perform any clear channel assessment (CCA)[26] requests or backoff contention procedures. So, after the timer triggers, packets are directly sent to the wireless channel. This is the usual procedure in TDMA-based MAC protocols. In this context, sensor node *a* ends transmitting the bits of packet *A* into the channel at time $T_{endTX}(a)$:

$$T_{endTX}(a) = T(a) + T_{totTX}(a) - T_{conf}(a) \quad (6.8).$$

Sensor node *b* starts sending the bits of packet *B* into the channel at time $T_{startTX}(b)$:

$$T_{startTX}(b) = T(b) + T_{totTX}(b) - T_{TX}(b) - T_{conf}(b) \quad (6.9).$$

If $T_{startTX}(b) < T_{endTX}(a)$, then a packet collision occurs and both packets are lost[27]. To avoid this situation, $T_{startTX}(b)$ must occur after $T_{endTX}(a)$, which means that the application timer of sensor node *b* must trigger after T(a) the following time:

$$T(b) - T(a) > \max\{0,\ T_{TX}(b) + (T_{totTX}(a) - T_{totTX}(b)) + (T_{conf}(b) - T_{conf}(a))\} \quad (6.10).$$

In this case, if the condition:

$$T_{startTX}(b) + T_{TX}(b) > T_{endTX}(a) + T_{BS\ totRX}(a) - T_{RX}(a) \quad (6.11),$$

holds[28], then sensor node *b* finishes the transmission after the BS having completely processed the packet *A*. In this case, the BS ends processing packet *B* at time $T_{BS\ end}(b)$, where:

[26] CCA is the physical layer process of checking the status of the channel and reporting back (usually to the MAC layer) if there is activity.

[27] The medium propagation time T_w is considered negligible.

[28] $T_{RX}(a)$ is subtracted because it is included in both $T_{endTX}(a)$ and $T_{BS\ totRX}(a)$.

$$T_{BS\,end}(b) = T_{startTX}(b) + T_{BS\,totRX}(b) \quad (6.12).$$

However, if the condition on Equation (6.11) is not verified, then sensor node *b* finishes the transmission while the BS is still processing the packet *A*. Consequently, one of the packets is dropped (packet *B* in ZigBit nodes). To guarantee that packet *B* is successfully processed by the BS, it must not collide with packet *A*, and it must be totally received after the BS finishes processing packet *A*. The first condition is expressed by Equation (6.10). The second condition implies that T(b) must be incremented by $T_{BS\,totRX}(a) - T_{RX}(a)$. Additionally, if $T_{BS\,totRX}(a) - T_{RX}(a) > T_{TX}(b)$, then T(b) can be decremented by $T_{TX}(b)$, because the transceiver can receive packet *B* while the microcontroller processes packet *A*. So,

$$\begin{cases} T_{endTX}(b) - T_{endTX}(a) > T_{BS\,totRX}(a) - T_{RX}(a) - T_{TX}(b), \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad if\ T_{BS\,totRX}(a) - T_{RX}(a) > T_{TX}(b) \\ T_{endTX}(b) - T_{endTX}(a) > T_{BS\,totRX}(a) - T_{RX}(a), \quad otherwise \end{cases} \quad (6.13).$$

Let us consider that sensor node *b* is ready to transfer data from the microcontroller to the transceiver, and sensor node *a* is transmitting to the BS. The transceiver of sensor node *b* must listen packet *A* to read its physical and MAC headers. In ZigBit sensor nodes, it was observed that the transceiver of sensor node *b* can only accept data from the microcontroller after its radio circuit has finished the listening of the whole packet *A*. No channel collision occurs between packet *A* and packet *B*. This phenomenon imposes an additional delay, $T_{hdrD}(b,a)$, when sending a packet *B* to the channel due to the influence of packet *A*. This delay is less than $T_{TX}(a)$ and must be added to $T_{totTX}(b)$, expressed in Equation (6.5).

As T(b) cannot occur before T(a), it results altogether that:

$$\begin{cases} T(b) - T(a) > \max\{0, T_{TX}(b) + \left(T_{totTX}(a) - T_{totTX}(b)\right) + \left(T_{conf}(b) - T_{conf}(a)\right) + \\ \quad T_{BS\,totRX}(a) - T_{RX}(a) - T_{TX}(b) - T_{hdrD}(b,a)\}, \quad if\ T_{BS\,totRX}(a) - T_{RX}(a) > T_{TX}(b) \\ \\ T(b) - T(a) > \max\{0, T_{TX}(b) + \left(T_{totTX}(a) - T_{totTX}(b)\right) + \left(T_{conf}(b) - T_{conf}(a)\right) + \\ \quad T_{BS\,totRX}(a) - T_{RX}(a) - T_{hdrD}(b,a), \quad otherwise \end{cases} \tag{6.14}$$

If sensor node *a* and sensor node *b* are identical, run the same software, and send packets with the same size, then $T_{totTX}(a) = T_{totTX}(b)$, $T_{conf}(b) = T_{conf}(a)$, and Equation (6.14) simplifies to:

$$T(b) - T(a) > T_{BS\,totRX}(a) - T_{TX}(a) - T_{hdrD}(b,a) \tag{6.15}$$

In the ideal case of sensor node *a* and sensor node *b* present a null delay in all software components and send equal size packets, Equation (6.14) becomes simply:

$$T(b) - T(a) > T_{TX}(a) \tag{6.16}$$

The additional introduced parameters related with the transmitting process are summarized in Table 6.3.

symbol	meaning
T	time instant when application timer of sensor node triggers to send a packet.
T_{endTX}	time instant when a sensor node ends transmitting the physical packet into the wireless channel.
$T_{hdrD}(b,a)$	delay to reflect that transceiver of sensor node *b* only accepts data from the microcontroller after its radio has listened to the packet from sensor node *a.*
$T_{startTX}$	time instant when a sensor node starts transmitting the physical packet into the channel.

Table 6.3 – Additional notation related with the transmitting process.

6.4.1.4 Considerations for CSMA Networks

Let us assume that sensor node *a* and sensor node *b* use a contention-based MAC protocol. Since CCA requests and random backoffs are carried out by the CSMA algorithm to find the channel free, it is not possible to establish an equation relating T(b) with T(a). However, packet *A* and packet *B* are successfully processed by the BS only if the condition expressed in Equation (6.13) holds.

Experimental tests with ZigBit sensor nodes revealed that the BS's transceiver is able to send a MAC ACK frame to a sensor node only if a time interval T_{ack} has elapsed since the transmission of the MAC ACK frame of the last received packet.

MAC ACK frames sent by the BS's transceiver while the BS's microcontroller is processing a received packet may deteriorate the DER. To understand why, let us consider that the BS microcontroller is processing packet *A* when packet *B* is received by the BS's transceiver, and the respective MAC ACK frame arrives successfully to sensor node *b*. As BS is processing packet *A*, packet *B* will be dropped. Since no retransmission will occur at sensor node *b*, packet *B* will not be delivered to the application layer of the BS. However, if the BS does not send the MAC ACK frame, packet *B* may be retransmitted and delivered with success to the application layer of the BS, if meanwhile packet *A* has been completely processed.

6.4.2 Time Drift

The proposed model considers also the time drift of sensor nodes, since it may affect the accuracy of the simulations results. For such goal, the model includes the drift parameter D_{ab}.

Generically, if the drift between sensor node *a* and the BS is D_a, and the drift between sensor node *b* and the BS is D_b, then the drift between sensor node *a* and sensor node *b* is $D_{ab} = D_a - D_b$. This means that if sensor node *a* and sensor node *b* start transmitting separated in time by T_{ab}, and if D_a is larger than D_b, then both sensor nodes will contend for the wireless channel after sending T_{ab} / D_{ab} packets. The D_{ab} value can be calculated experimentally through the relation:

$$D_{ab} = \frac{(T_{BS}(a,\ i+1) - T_{BS}(b,\ i+1)) - (T_{BS}(a,\ i) - T_{BS}(b,\ i))}{T_{BS}(b,\ i+1) - T_{BS}(b,\ i)} \qquad (6.17),$$

where $T_{BS}(m, n)$ express the local time of the BS when this received packet *n* from sensor node *m*. It is assumed that packet *i* from sensor node *b* arrives after packet *i* from sensor node *a*, as well as all successive received packets from both sensor nodes during the time period between $T_{BS}(b, i)$ and $T_{BS}(b, i+1)$. Since T_{ab} is lower than 125 ms in the physical testbed, and assuming D_{ab} equal to 0.1%, channel contentions between a pair of sensor nodes may occur whenever 125 packets are sent, at maximum. However, no channel contention occurs if D_{ab} is zero and T_{ab} is above the full-loaded packet transmission time. In this case, the simulation results present a null DER in a WSN with more than sixteen active sensor nodes. To prevent this unrealistic situation, the simulation results in Figure 6.1 and Figure 6.2 were taken using a D_{ab} equal to 0.005%.

6.4.3 Setting the Model Parameters

The setting of the model parameters regarding the diverse software components and the time drift is presented in the following.

Software components. Whenever possible, the tuning of the model parameters was based on measurements performed in the physical testbed. Table 6.4 presents the values obtained for the diverse parameters, expressed in milliseconds, which are specific to this physical testbed. MAC payloads of 30 B and 90 B were considered. These values were measured with an analogical oscilloscope, and may present an error of +/– 0.5 ms. The values in *italic* were calculated analytically: $T_{BS\ phyRX}$ derives from Equation (6.2); T_{RX} and T_{TX} from Equation (6.3), $T_{BS\ pciR}$ and T_{pciW} from Equation (6.4), T_{phyTX} from Equation (6.6); $T_{l\rightarrow tx}$ was obtained from the transceiver technical specifications.

The computing performance of the BS in the physical testbed is similar to a sensor node. This situation is not normally found in a WSN, since a BS presents typically stronger computing resources and a more efficient operating system than sensor nodes. In this case, the values of T_{totRX} and T_{totTX} may be similar to T_{RX} and $T_{TX,}$ respectively.

However, in a multi-hop WSN the packets may be routed through the sensor nodes, and so the value of T_{totRX} and T_{totTX} can influence significantly the network performance.

	MAC_d	
	30 B	**90 B**
$T_{BS\ app}$	**1.8 ms**	**1.8 ms**
$T_{BS\ mac \rightarrow app}$	**1.0**	**1.3**
$T_{BS\ phy \rightarrow mac}$	**1.0**+T_{RX}	**1.4**+T_{RX}
T_{ack}	**3.3**	**3.7**
$T_{BS\ pciR}$	*0.10*	*0.23*
$T_{BS\ phyRX}$	*0.90*	*1.17*
T_{RX}, T_{TX}	*1.50*	*3.42*
$T_{BS\ totRX}$	3.8+T_{RX}	4.5+T_{RX}

	MAC_d	
	30 B	**90 B**
T_{app}	**1.8 ms**	**2.0 ms**
$T_{app \rightarrow mac}$	**1.2**	**2.0**
$T_{mac \rightarrow phy}$	**1.4**+T_{TX}	**2.5**+T_{TX}
T_{conf}	**4.0**	**4.0**
T_{pciW}	*0.10*	*0.23*
T_{phyTX}	*1.12*	*2.09*
$T_{l \rightarrow tx}$	*0.18*	*0.18*
T_{totTX}	**8.4**+T_{TX}	**10.5**+T_{TX}

Table 6.4 – Values of the model parameters for the BS (left) and for the sensor nodes (right).

Time drift. The parameter D_{ab}, was set by applying Equation (6.17) on values measured using the BS and pairs of sensor nodes. Measurements showed that the software time drift between sensor nodes may have values up to 0.3%, depending on the pair of sensor nodes used. The time drift between a pair of sensor nodes varies along the time too. The simulator was programmed so that each sensor node at start-up chooses an average time drift D_{ab} up to 0.3% randomly.

6.5 Model Validation

In order to validate the proposed model, tests were carried out in the physical and simulation platforms using both TDMA and CSMA-based MAC protocols. The sensor nodes used in the experiments are identical in terms of hardware and run the same software.

6.5.1 TDMA Algorithm

Validation tests of the proposed model were carried out in the physical and simulation platforms using a simple TDMA-based algorithm. The BS sends a beacon every 100 ms. This value was chosen to minimize the effect of the time drift D_{ab}. In each superframe, two or three sensor nodes transmit once with the minimum time gap that guarantees a null DER. Table 6.5 compares the time values obtained in both platforms. Simulation tests were accomplished with and without the proposed model implemented in the simulator. As illustrated, the inclusion of the proposed model in the simulator, brings the simulation outcome close to the real results, with differences below 0.5 ms. The registered differences are justified taking into account the accuracy error that affect the measured values. T_{hdrD} presented a null value in all tests, excepting the test marked with an asterisk, where T_{hdrD} was 1.0 ms.

An important conclusion taken from the real results is that time-slots should be allocated to the sensor nodes in accordance with the respective packet sizes to be transmitted. Smaller packets should be sent first to reduce the possibility of bandwidth waste. Such waste is clear in Table 6.5, when sensor node *a* sends 90 B and sensor node *b* sends 30 B.

node *a*	node *b*	node *c*	real test	simulation with the model	simulation without the model
30 B	30 B	30 B	**4.0**	3.8	1.5
30 B	30 B	-	**4.0**	3.8	1.5
90 B	90 B	90 B	**4.5**	4.5	3.4
90 B*	90 B*	-	**3.0**	3.5	3.4
30 B	90 B	-	**0.5**	0.0	1.5
90 B	30 B	-	**8.5**	8.5	3.4

Table 6.5 – Results from the physical testbed and from the simulation platform.

Validation tests of the proposed model were also carried out using the test conditions described in Section 6.2.1 in presence of interfering traffic, but running in the reference WSN the AR-MAC protocol with one beacon per BP. Figure 6.4 shows that the DER results obtained in the simulator are reasonably similar to those obtained in the physical

testbed, particularly the average DER. Each bar in the figure also shows the average value (in cyan) obtained from a second test carried out in the same test conditions. The average DER dissimilarities observed among the results of the real tests and the simulation test occurs because the values occupy a sensible region to packet loss. Indeed, considering the used test conditions, an average DER of 0.1% corresponds to a loss of just four packets per sensor node after the test conclusion (sixteen minutes[29]).

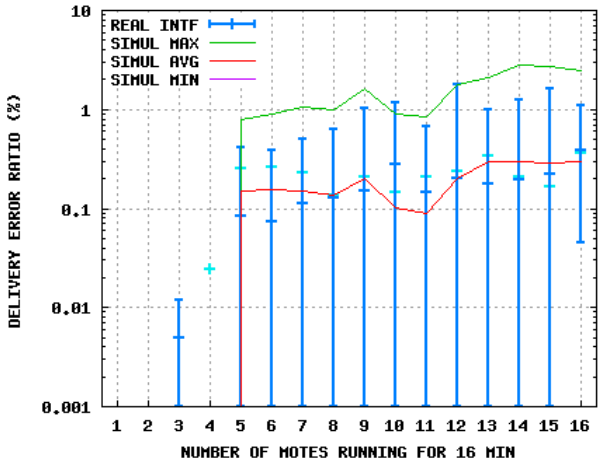

Figure 6.4 – DER with interferences.

6.5.2 CSMA Algorithm

Validation tests of the parametric model were run in the physical and simulation platforms using the IEEE 802.15.4 MAC protocol. Figure 6.5 shows the simulation results using the proposed model when IEEE 802.15.4 interfering traffic was not present. Multiple tests showed that the influence of the simulation seed on the results was not significant. It is observed that the DER simulation results approximate closely to the DER values found in the physical scenario (the corresponding physical testbed results are also replicated for better comparison). The results of the maximum and average round-trip delays become also close to those obtained in the physical scenario.

[29] Each sensor node transmits 3840 new data packets during sixteen minutes.

Simulations without using the proposed model showed that the average DER *improves* over 75% when the MAC payload decreases from 90 B to 30 B. Since the channel occupation decreases with the packet size reduction, the number of collisions diminishes, and so the DER improves. However, tests on the physical platform revealed that the average DER *degrades* about 20% when the MAC payload decreases from 90 B to 30 B. The same degradation was observed in the simulations with the proposed model, which confirms the validity of the model. As the packet size decreases, the probability of having multiple packets arriving without collisions to the BS during T_{totRX} becomes higher, and consequently the DER increases too (see Section 6.4.1.4).

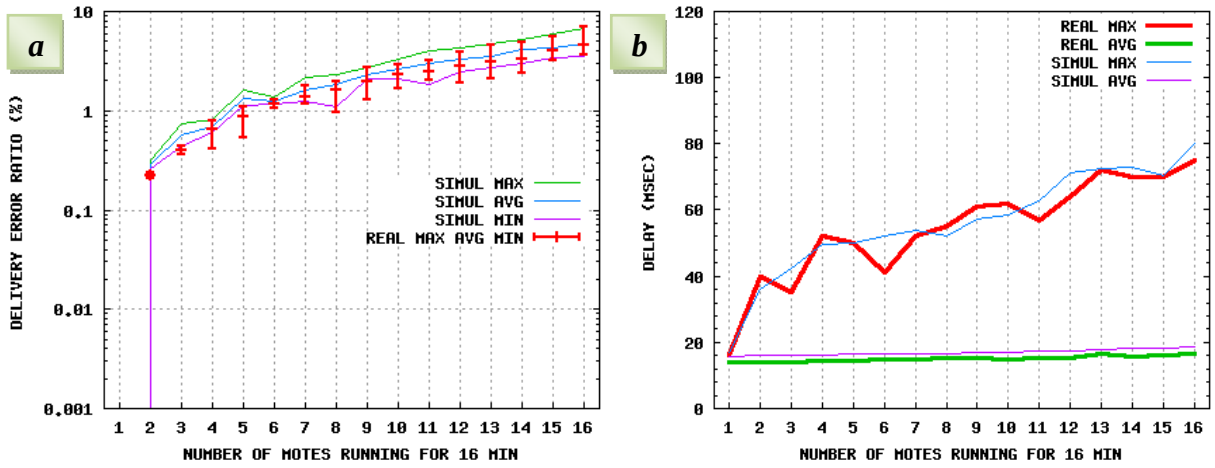

Figure 6.5 – (***a***) DER and (***b***) round-trip delay without interferences.

Figure 6.6 presents the simulation results when IEEE 802.15.4 interfering traffic was present. The DER results keep close to the DER values found in the physical scenario. The results of the average and maximum delays are also identical to those obtained in the physical scenario. It should be pointed out the notorious improvement registered in the DER when the reference WSN run the AR-MAC protocol instead of the IEEE 802.15.4 MAC protocol (cf. Figure 6.4).

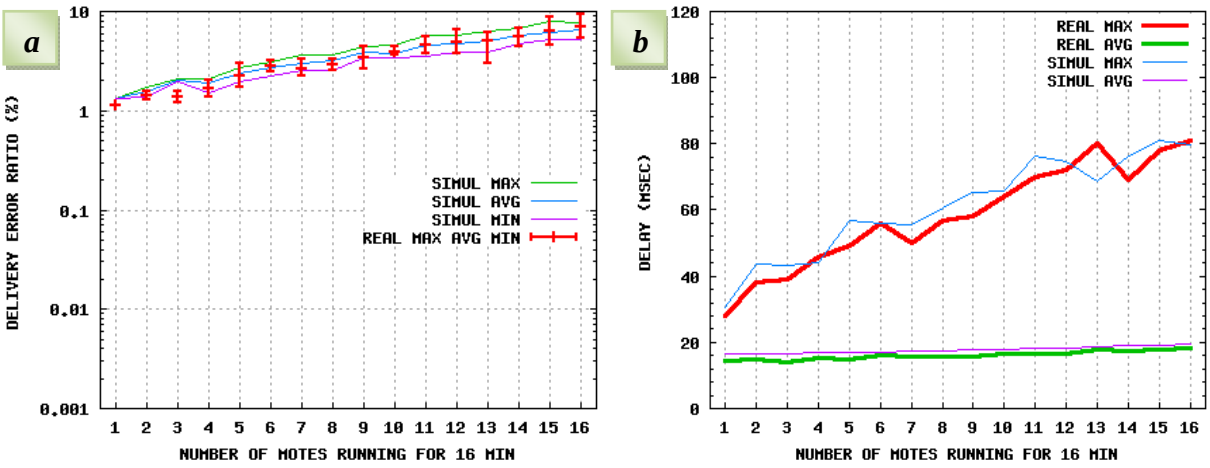

Figure 6.6 – (***a***) DER and (***b***) round-trip delay with interferences.

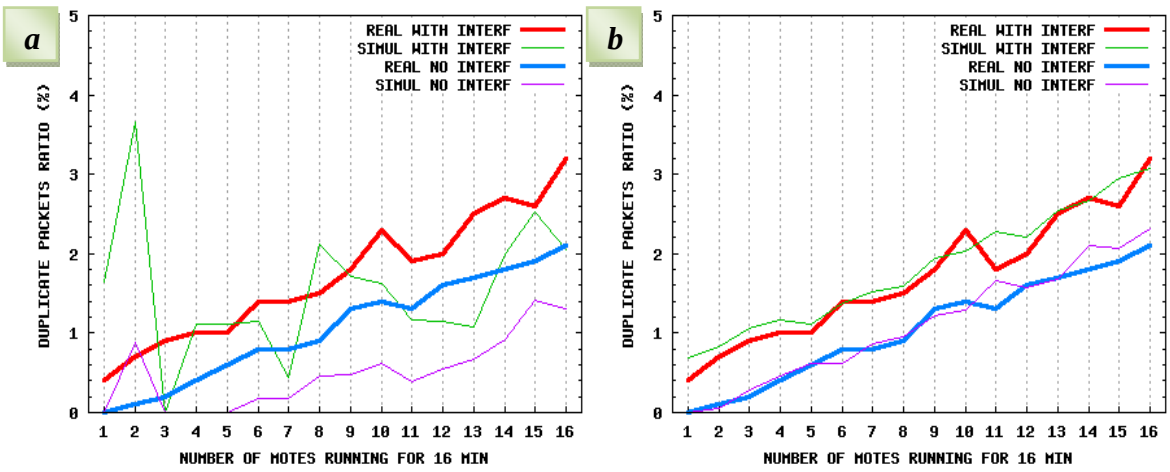

Figure 6.7 – Average DPR (***a***) without the model and (***b***) with the model.

With the CSMA-CA algorithm, a sensor node may send a duplicate packet if it does not receive the MAC ACK frame from the BS. The average duplicate packets ratio (DPR) is defined as the percentage of the total number of data packets received in duplicate by the application layer of the BS comparatively to the number of application data packets received for the first time from all sensor nodes in the WSN.

Figure 6.7*a* shows the average DPR obtained with and without the presence of IEEE 802.15.4 interfering traffic, when not using the proposed parametric model.

Figure 6.7*b* presents de average DPR using this model. In this last case, the simulation results are similar to those obtained in the physical testbed.

6.6 Validation of the Test Platforms

As mentioned in Section 6.4.3, the tuning of the model parameters was accomplished from measurements performed directly in the physical testbed using electronic instruments. Simulation tests using the model parameterized with those measured values revealed that the results match satisfactorily those obtained in the physical testbed under identical test conditions. Thus, the validation of the simulation platform is corroborated through the physical testbed. In the same way, the validation of the physical testbed can be considered corroborated through the simulation platform, because the simulation platform runs the same MAC protocol and uses the software components' parameters measured from the physical testbed. So, the simulation platform and physical testbed mutually validate each other.

6.7 Summary

Many generic network simulators, including Castalia, do not model the performance of the software components running within the network devices. This aspect is particularly important in WSNs. Since sensor nodes present typically very limited computing resources, the performance of the operating system and software components running inside the sensor nodes impose significant constrains to the overall performance of a WSN. This chapter has showed that if such software performance limitations are not taken into account, the simulation tests may produce results significantly more optimistic than those obtained under real conditions. Indeed, tests showed that it is very difficult to obtain satisfactory simulation results using uniquely the parameters of the wireless channel, the physical layer, and the MAC layer provided by the WSN simulator. This very important aspect is often neglected in many works presenting WSN evaluation studies carried out on simulators.

In order to obtain satisfactory simulation results, distinct software-related parameters were modeled, measured, and included in Castalia. Simulation tests showed that the results obtained with the new parameters match satisfactorily those obtained in real conditions. Therefore, the inclusion of the parametric model in a WSN simulator helps to improve the confidence degree on the simulation results, and it is generic enough to model distinct WSN testbeds.

Once validated the simulation platform, an e-health scenario was implemented in the simulator to test the performance efficiency of the AR-MAC protocol. The considered e-health scenario and the results of the performance tests are presented in the next chapter.

Chapter 7

AR-MAC Performance Evaluation

7.1 Introduction

In order to evaluate the efficiency of AR-MAC protocol regarding diverse service quality and design metrics, performance tests were carried out using an e-health scenario implemented in the simulation platform. The considered service quality metrics are the delivery error ratio (DER), the one-way delay, and the power consumption. The evaluated design metrics are the network scalability, in terms of number of BSNs supported, the adaptability of the network to new reconfiguration schemes, the traffic protection, and the RP usage performance. The modeling of the computation overhead of the software components running in the sensor nodes and in the BS was considered in the tests. Additionally, tests were carried out considering the BS and the sensor nodes with ideal characteristics to assess the performance boundaries of AR-MAC protocol for the metrics under analysis in the considered scenario. As discussed in the last chapter, the results obtained with the WSN simulator were corroborated by tests carried out in a physical platform.

For comparative purposes, performance tests were also carried out using the non-slotted CSMA-CA MAC protocol described in the IEEE 802.15.4 standard [IEEE4]. This standard is mostly deployed in non-beacon enabled networks and is used in many e-health systems [Chen11] [Latré11]. The motivation for choosing the non-slotted CSMA-CA MAC protocol was also reinforced by the results obtained in the preliminary performance tests presented in the next section.

Tests carried out in the physical testbed to evaluate the efficiency of AR-MAC in frequency-hopping mode, regarding the packet delivery robustness and the network reconfiguration ability, are discussed too. Finally, a set of tests is presented to assess the efficiency of the method used in AR-MAC to evaluate the interference degree on the channel.

7.2. Preliminary Performance Tests

This section presents a brief comparative performance study of AR-MAC (with channel switching disabled, one-color mode) against IEEE 802.15.4 and LPRT. Those protocols were selected because IEEE 802.15.4 is a standard used in many ambient

assistance living systems, and LPRT is a real-time MAC protocol that uses a retransmission period in the superframes, just like AR-MAC. Another important reason for selecting these protocols is that they can be easily implemented in the WSN simulator from the code developed for AR-MAC.

The experimental e-health scenario contains four BSNs, each one containing four sensor nodes to monitor the ECG, the blood pressure (ART), the oximetry (OXI), and the respiratory rate (RR). This is the scenario shown in Figure 7.2, considering four beds and the temperature (TEMP) sensor nodes off. The number of BSNs and sensor nodes was imposed by the maximum number (sixteen) of guaranteed time-slots (GTSs) available in the superframe of the slotted-IEEE 802.14.5 MAC protocol. Comparatively to IEEE 802.15.4 standard, the maximum number of GTSs was increased so that one GTS was allocated to each sensor node. The non-slotted CSMA-CA algorithm was tested with its default values. The real behavior of the software and hardware components within the WSN devices was considered in the tests, and IEEE 802.15.4 interference packets were sent regularly every 25 ms approximately. The average delivery error ratio in the WSN and the average power consumed per BSN were the considered metrics. In all tests, sensor nodes enter in sleeping mode after transmitting. To better evince the impact of the MAC protocols on the energy cost, only the microcontroller consumption (cf. Tables 5.1) and the radio consumption (cf. Table 5.2) were considered.

As shown in Figure 7.1, the results reveal a notorious data delivery robustness presented by AR-MAC, when comparing to its competitors. This good performance was achieved without aggravating the power consumption significantly. IEEE 802.15.4/GTS presented low packet delivery performance, because it does not include mechanisms to recover within the maximum delay boundary the data packets which were not delivered during the GTSs (see Section 3.4.2). The single retransmission procedure of LPRT also revealed unsatisfactory performances for e-emergency WSNs. After AR-MAC, the IEEE 802.15.4/CSMA protocol presented the best performance results, particularly when considering the BS with ideal characteristics.

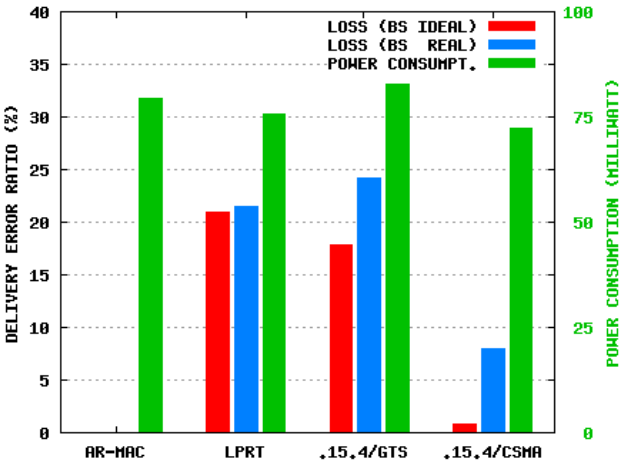

Figure 7.1 – Average power consumption per BSN and average DER in the WSN considering an ideal BS and a real BS.

7.3 Experimental e-Health Scenario

It is presented next, in the form of a case-study, the e-health scenario implemented in the simulation platform to carry out diverse studies regarding the AR-MAC protocol performance. The test conditions used in the experiments are also described.

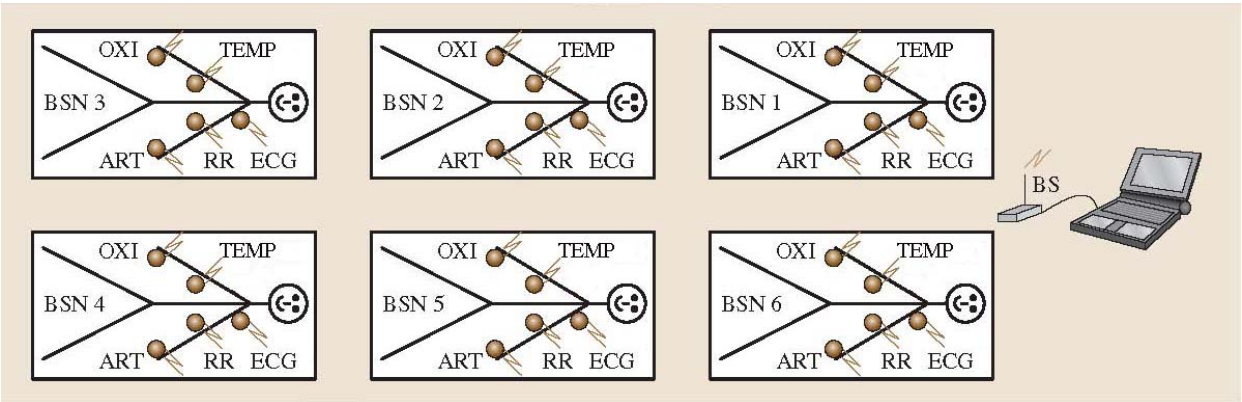

Figure 7.2 – Hospital room with a patient being monitored in each bed.

7.3.1 Case-study

Let us consider a hospital room containing several beds with one patient per bed. Each patient is monitored through a BSN, and one BS collects and analyzes the physiological signals of all patients. Figure 7.2 exemplifies this situation with six patients. This scenario is based on the intensive care unit (ICU) of an existent hospital, where the ICU is a room composed of six closed divisions, with one bed per division. A minimum area of 20 m^2 per bed must be assured in the ICUs [ACSS08].

Intensive care services should measure the ECG, the non-invasive and invasive blood pressures, the SpO_2, the heart rate, the body temperature, and the respiratory rate/CO_2 gas signals [ACSS08][30]. As the heart rate may be obtained from the SpO_2 signal, there is no need for a dedicated heart rate sensor. For simplicity, only the non-invasive blood pressure is considered, as required in emergency services. The respiratory rate is measured too. Thus, the signals being monitored are the electrocardiography (ECG), the non-invasive arterial pressure (ART), the oximetry (OXI), the respiratory rate (RR), and the body temperature (TEMP).

Each physiological signal is collected and transmitted by a dedicated sensor node to the BS at 250 kb/s. Considering the sampling rates required to obtain good quality physiological signals, ECG sensor nodes sample the physiological signal at 180 Hz, ART sensor nodes at 120 Hz, OXI sensor nodes at 60 Hz, RR sensor nodes at 20 Hz, and TEMP sensor nodes at 0.1 Hz (see Table 2.1). Each sample of every sensor node has a resolution of sixteen bits. As the maximum payload size of the data packets is 116 B, the ECG sampling rate was chosen to avoid eventual overflows caused by the inaccuracy of the timers of the sensor nodes. Data packets transmitted from ECG, ART, OXI, RR, and TEMP sensor nodes present a payload of 90 B, 60 B, 30 B, 10 B, and 1 B, respectively.

[30] As mentioned in Section 2.3.4, normal intensive care uses CO_2 gas and neonatology intensive care uses the respiratory rate.

7.3.2 Test Conditions

In order to evaluate the performance of AR-MAC protocol in the described e-health scenario under different operating conditions, simulation tests were carried out using superframes with time-slots of half millisecond. This time-slot duration was chosen as a compromise between the bandwidth granularity of the superframe and the timers' precision of typical sensor nodes. Knowing that ECG traffic must have a maximum latency of 500 ms (cf. IEEE 1073), a beacon interval of 250 ms was chosen as reference. To study how the superframe duration (SD) affects the network performance, tests were also carried out using beacon intervals of 375 ms and 500 ms. Sampling rates were adjusted so that the packet sizes did not change with the beacon interval. Tests considered the WSN operating both in one-color mode (i.e., one color attributed to all sensor nodes and superframes) and in two-color mode. All patients (i.e., BSNs) are assumed in critical health state, unless otherwise stated.

To stress the impact of the software components on the overall network performance, tests were carried out considering real and ideal software components within the sensor nodes and the BS. The devices with ideal software components present null processing time values. It is assumed that an ideal BS has negligible influence in the WSN performance. A neighbor WSN sent interference packets regularly at 12.5 ms, 25 ms, and 50 ms, with a random variation of +/-1%. Interference packets carried 100 B of data and were sent using the CSMA-CA algorithm with the following parameters: the minimum backoff exponent is three, the maximum number of backoffs is four, and the maximum number of frame retries is zero. To find the absolute maximum performance limits of the WSN, tests without any interfering traffic were run too. No fading and shadowing phenomena were considered in the tests[31]. The AR-MAC protocol was parameterized with the values presented in Table 7.1.

[31] Since the room area considered in simulator scenario is relatively small (12m x 12m), all motes work in a good connected region and, therefore, the channel BER is null. In this case, it is indifferent to use Castalia with the simple collision model or the additive interference model (see Section 5.2.2). The presence of walls, ceiling, objects, and people is not considered in the simulation model.

parameter	value
beacon interval (ms)	250, 375, 500
time-slot duration (ms)	0.5
BP duration (ms)	2.5
number of beacons in the BP	3
number of NTP safeguard slots	4
number of RP safeguard slots	2
minimum CAP size (slots)	25
max. nr. of NRP transmissions per sensor	variable
max. nr. of ERP transmissions per sensor	1
maximum number of successive NTP transmissions without receiving a beacon	2
number of used colors	1, 2
channel switching mode	off

Table 7.1 – AR-MAC configuration parameters used in the simulation platform.

As argued in Section 6.5.1, time-slots should be allocated to the sensor nodes in accordance with the packet sizes to be transmitted. Smaller packets should be sent first to reduce the possibility of bandwidth waste. For this reason, packets from the RR sensor nodes of all BSNs are transmitted first in the superframe followed by the OXI, ART, and ECG packets. As TEMP sensor nodes sample and transmit one temperature measurement every ten seconds, these data are sent in the CAP of the superframe.

For comparative purposes, tests were also carried out using the non-slotted CSMA-CA-based MAC protocol described in IEEE 802.15.4 standard. The CSMA-CA algorithm used the default parameters: the minimum backoff exponent is three, the maximum number of backoffs is four, and the maximum number of frame retries is three.

In order to study the performance boundaries of the considered MAC protocols, tests were carried out with an increasing number (up to sixteen) of patients in the intensive care unit.

7.3.3 Results

Next, it is presented the results obtained in the simulation studies regarding the packet delivery robustness, latency, traffic protection, and power consumption. Tests to the network scalability, reconfiguration ability and RP usage are also presented. In order to avoid presenting multiple graphics, the metrics were calculated taking into account all packets sent from each BSN, rather than its individual sensor nodes.

7.3.3.1 Packet Delivery Robustness

Considering all BSNs in the WSN, Figure 7.3 and Figure 7.4 show the results of the BSN which presented the highest average delivery error ratio ($\overline{\text{DER}}_{\text{max}}$), assuming the sensor nodes with real and ideal characteristics and subject to interference packets sent with an approximate period of 12.5 ms, 25 ms, and 50 ms. The BS is considered ideal. Tests were run with AR-MAC (Figure 7.3) and IEEE 802.15.4 (Figure 7.4). To exemplify how graphics should be interpreted, let us consider the one-color AR-MAC test carried out with a WSN composed of five real BSNs, superframe duration of 250 ms, and interference period of 25 ms. Accordingly to the Figure 7.3*c*, no BSN presented an average DER above 0.5%, as indicated in the bold red curve.

Observing the results obtained with AR-MAC, it is notorious the effect of the software components overhead on this metric. The $\overline{\text{DER}}_{\text{max}}$ improves significantly as the sensor nodes' characteristics tend to the ideal ones. The $\overline{\text{DER}}_{\text{max}}$ also improves as the superframe duration increases. The improvement in the $\overline{\text{DER}}_{\text{max}}$ in both cases occurs because more RP time-slots become available for the retransmission trials. It is also observed that the $\overline{\text{DER}}_{\text{max}}$ improves significantly as the load of interfering traffic on the channel becomes lower. Tests carried out without any interfering traffic presented a null $\overline{\text{DER}}_{\text{max}}$ while the number of time-slots taken by all BSNs did not exceed the total number of NTP time-slots.

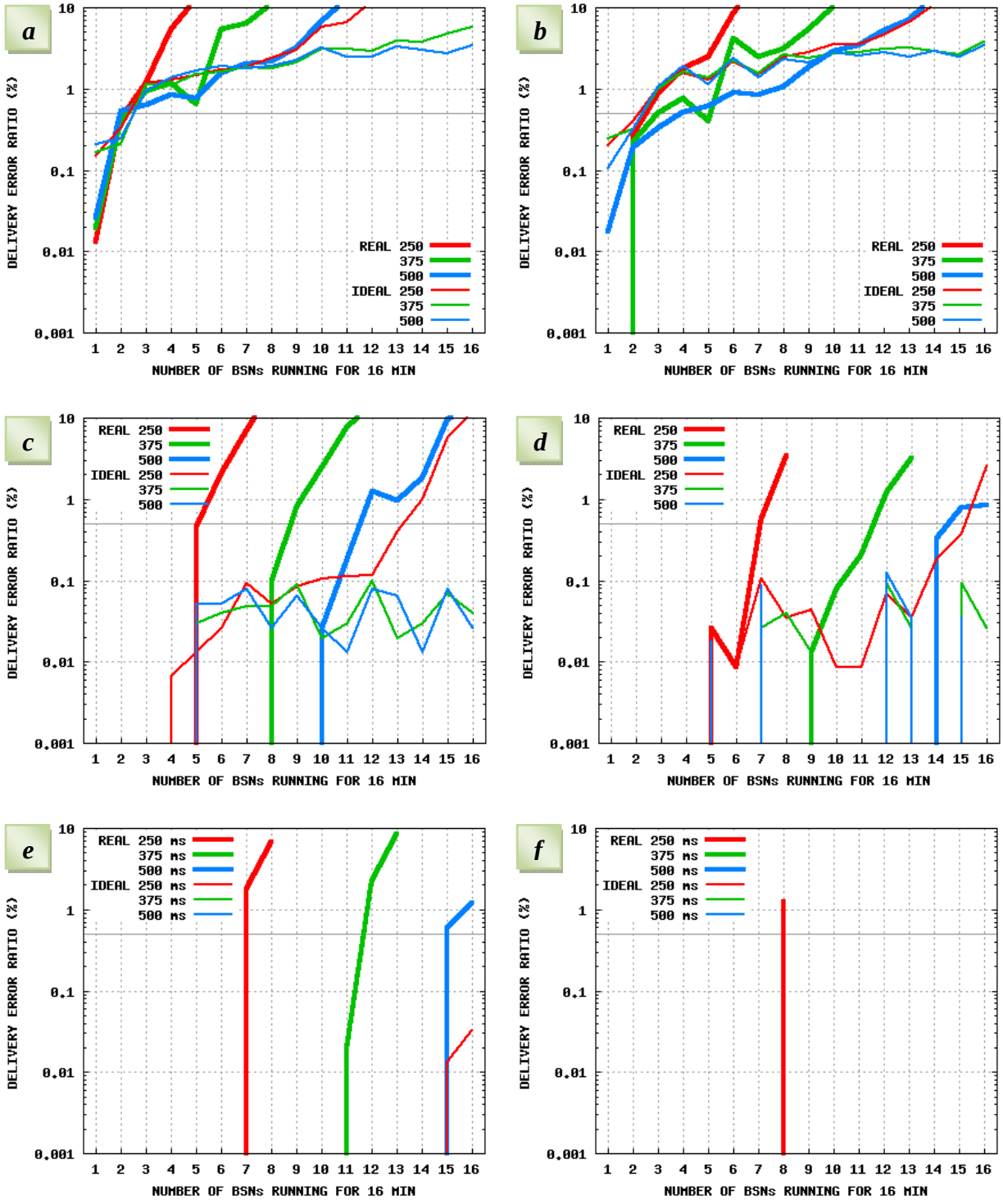

Figure 7.3 – $\overline{\mathbf{DER}}_{\mathbf{max}}$ with AR-MAC in: (***a***) one-color mode & 12.5 ms interfering traffic; (***b***) two-color & 12.5 ms; (***c***) one-color & 25 ms; (***d***) two-color & 25 ms; (***e***) one-color & 50 ms; and (***f***) two-color & 50 ms.

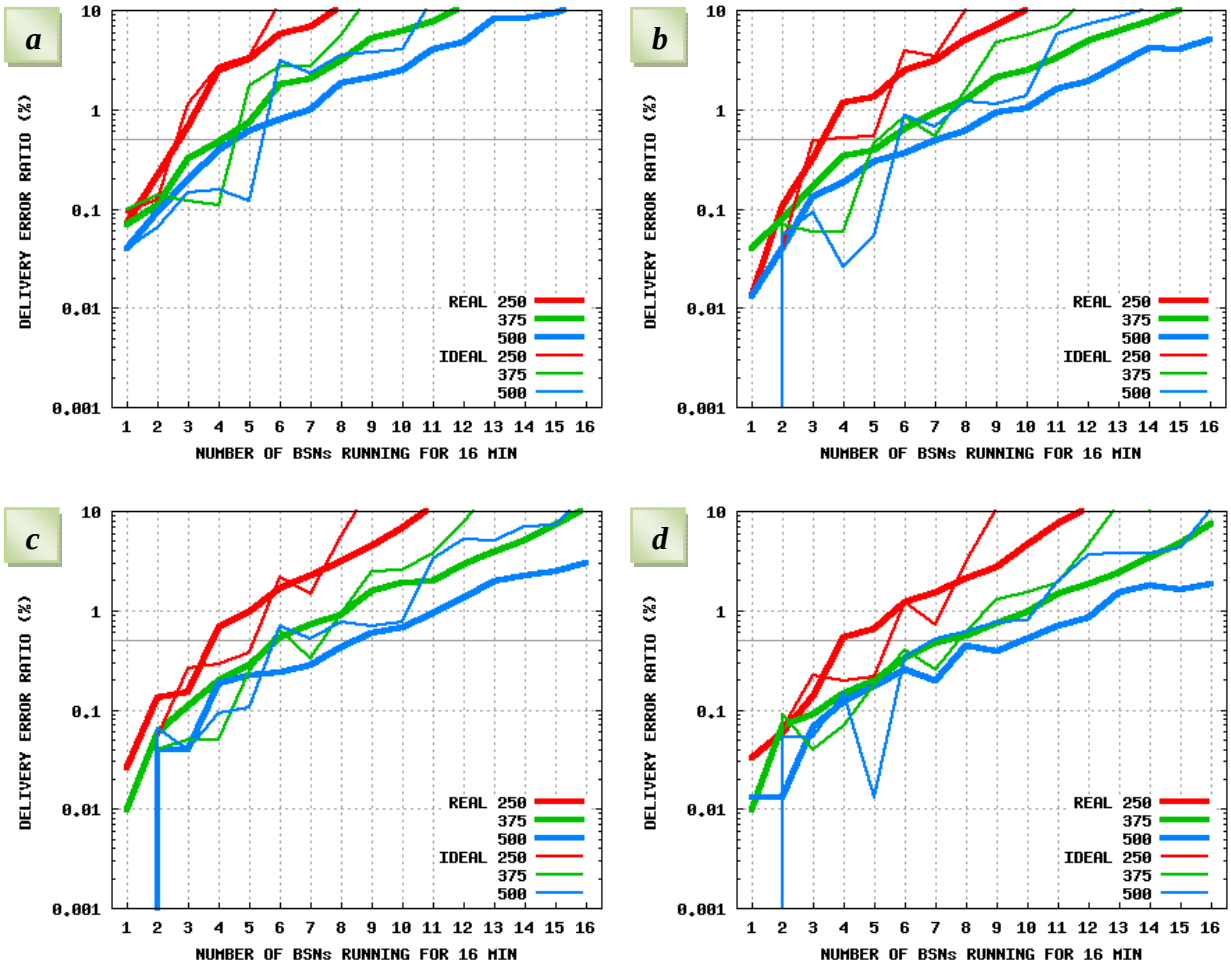

Figure 7.4 – $\overline{\mathbf{DER}}_{\mathbf{max}}$ in IEEE 802.15.4 for interference periods of: (***a***) 12.5 ms; (***b***) 25 ms; (***c***) 50 ms; and (***d***) infinite.

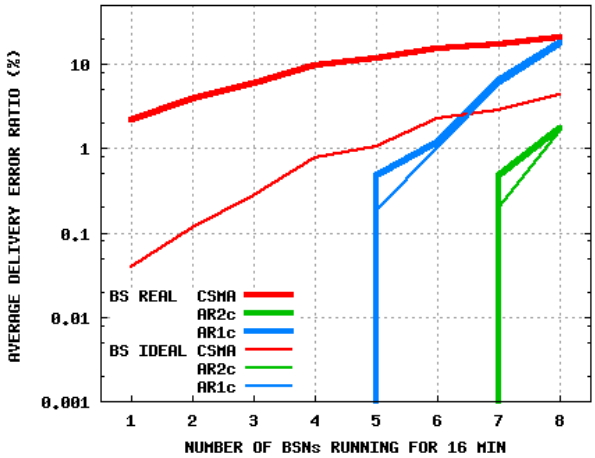

Figure 7.5 – Average DER in AR-MAC (both color modes) and IEEE 802.15.4 with 25 ms interfering traffic, considering an ideal BS and a real BS.

With IEEE 802.15.4 MAC protocol, the use of sensor nodes with ideal characteristics is not reflected in a consistent improvement of the $\overline{\text{DER}}_{\text{max}}$. Inclusively, several test situations revealed that the $\overline{\text{DER}}_{\text{max}}$ deteriorates using ideal sensor nodes, particularly when the number of BSNs reached the WSN scalability limit. Also, the $\overline{\text{DER}}_{\text{max}}$ does not improve significantly as the superframe duration increases or the interfering traffic load reduces. Even without any interfering traffic, the $\overline{\text{DER}}_{\text{max}}$ does not improve appreciably when compared with the $\overline{\text{DER}}_{\text{max}}$ obtained in the tests carried out with an interference period of 25 ms.

In order to evaluate the effect of the software components of the BS in the WSN performance, tests were also carried out assuming a BS with real characteristics, which were considered identical to a sensor node with real characteristics. This situation may occur, for example, in clustered WSNs, where cluster-heads are simple sensor nodes. Tests used sensor nodes with real characteristics and an interference period of 25 ms. AR-MAC used a superframe duration of 250 ms and tests were run for one-color mode (AR1c) and two-color mode (AR2c). Figure 7.5 shows the average DER obtained considering the traffic of all BSNs in the WSN. With IEEE 802.15.4, it is observed that the network performance is significantly affected by the real characteristics of the BS. However, AR-MAC in both color-modes revealed certain immunity, in terms of average DER degradation, regarding the real characteristics of software components of the BS.

To summarize, AR-MAC protocol in both color modes reveals, if properly tuned, immunity to the BS characteristics, which does not occur with IEEE 802.15.4. The packet delivery performance of AR-MAC tends to improve significantly as the characteristics of the sensor nodes approach the ideal characteristics, the superframe duration increases, or the interfering traffic load reduces. However, the improvement observed in the IEEE 802.15.4 was not significant, or even did not occur, when considering these aspects. Finally, the performance of the AR-MAC protocol may be significantly improved by operating in two-color mode instead of one-color mode.

It should be noted that all conclusions presented in this chapter assume that AR-MAC operates in a WSN whose characteristics are similar to those of the network used in the experimental test scenario, namely centralized, one-hop WSNs with stable topology, regular traffic pattern, and significant volumes of traffic.

7.3.3.2 Goodput

Goodput is a metric that reflects the rate at which the application data is delivered with success. The goodput *G*, in b/s, of a sensor node *m* that is sending regularly a new data packet is:

$$G = (1\text{-}DER) \times P / T_t \quad (7.1),$$

where *P* is the data payload, in bits, transmitted by sensor node *m* every T_t seconds. DER is the delivery error ratio of sensor node *m*. Note that (1-DER) represents the packet reception ratio (PRR) from sensor node *m*. Equation (7.1) is independent on the MAC protocol used in the WSN. However, for the AR-MAC protocol it can be represented alternatively as:

$$G = (1\text{-}DER) \times P / (BI \times 2^{C-1}) \quad (7.2),$$

where *P* is the data payload, in bits, sent by sensor node *m* of color *C* in a WSN using a beacon interval of *BI* seconds. The expression also holds for calculating the goodput from a group of sensor nodes with the same characteristics in terms of data payload *P* and color *C*. In this case, DER represents the average delivery error ratio of the whole group.

Goodput graphics are not showed, because goodput is correlated with the DER and so can be easily deducted from this metric.

7.3.3.3 Maximum Latency

One-way delay is defined as the time spent between sending an application data packet from a sensor node and its reception by the application layer of the BS. The one-way delay can be considered from the sample or packet's perspective. A data packet contains samples obtained at distinct times, according to the sensor node's sampling rate. If the sampling period is negligible compared to the superframe duration, the sending time of the application packet is very close to the capture time T_c of the sample obtained more recently within the packet. In such case, the one-way delay of a packet is very close to the one-way delay *D* of this recent sample. However, the capture time of the oldest sample within the packet is older than time T_c by a period ΔT equal to the product of

superframe duration and the sensor node's color. Thus, the one-way delay of the oldest sample is $D + \Delta T$. For the sake of simplicity, this study considered the one-way delay from the perspective of the packet rather than the sample.

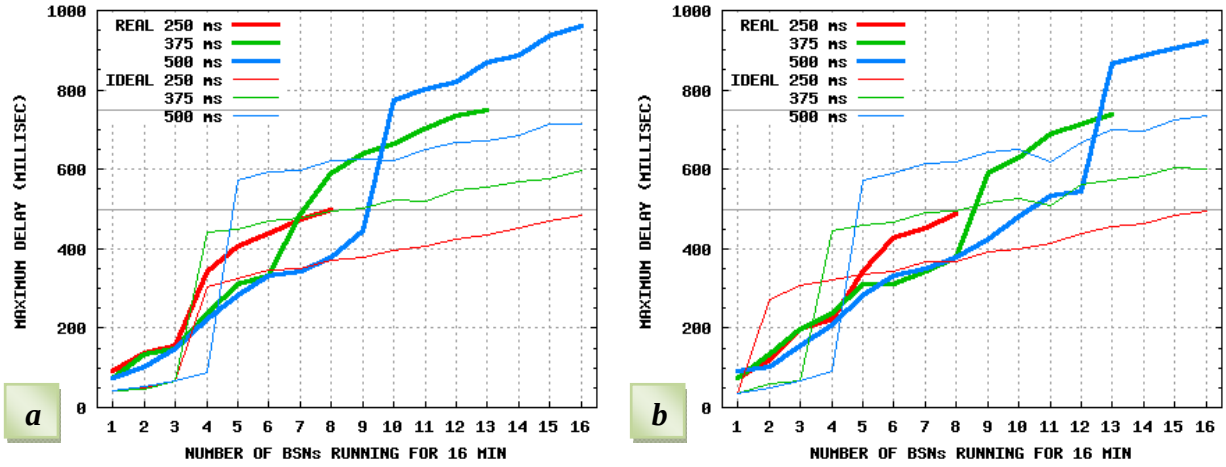

Figure 7.6 – Maximum one-way delay with AR-MAC in (***a***) one-color and (***b***) two-color mode, for an interference period of 25 ms.

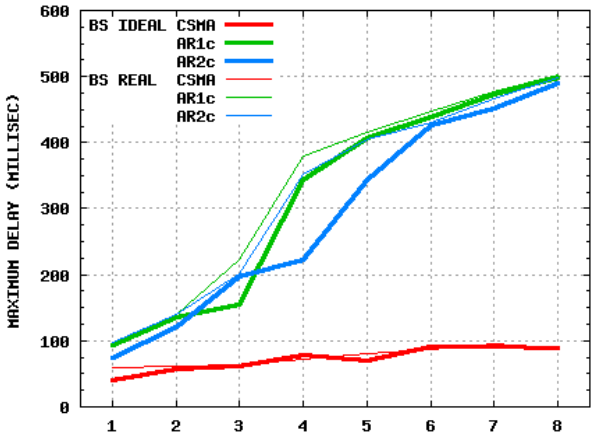

Figure 7.7 – Maximum one-way delay with AR-MAC in both color modes and IEEE 802.15.4, for a BS with ideal and real characteristics, SD = 250 ms, T_{interf} = 25 ms.

Considering the data packets received by the BS from all sensor nodes in the WSN, Figure 7.6 presents the maximum one-way delay results obtained for AR-MAC with an interference period of 25 ms. Tests considered sensor nodes with real and ideal characteristics. In all cases, the maximum one-way delay is kept below twice the superframe duration. Ideal sensor nodes present lower maximum one-way delays, because these require superframes with shorter NTP and RP periods than sensor nodes with real characteristics. With the real sensor nodes' model, the tests show that the maximum one-way delay curve tends to twice the superframe duration. When this limit is reached, the maximum number of NTP slots available in the superframes runs out, and so no additional BSNs can be admitted. This indicates that the WSN scalability reached the absolute maximum limit. With ideal sensor nodes, this saturation did not occur because the overhead of the software components is null, and so the superframe bandwidth is used more efficiently. All curves present a two-level threshold behavior. The low-level threshold indicates that retransmissions occurred uniquely in the NRP, and the up-level threshold indicates that retransmissions also occurred in the ERP.

If no retransmission occurs because the channel is free of interfering traffic, then the maximum one-way delay of a BSN is near its average one-way delay, independently of the superframe duration. Using sensor nodes with real characteristics, the maximum and average one-way delays were 10 ms and 7 ms, respectively.

Figure 7.7 shows the maximum one-way delay results obtained for IEEE 802.15.4, considering sensor nodes with real characteristics, superframe duration of 250 ms and an interference period of 25 ms. These delays are naturally lower than those obtained for AR-MAC, because AR-MAC postpone retransmissions for the next superframes. Figure 7.7 also shows the influence of the BS's characteristics on the maximum one-way delay, considering a BS with ideal and real characteristics (similar to a sensor node).

In summary, IEEE 802.15.4 MAC protocol presents a lower maximum one-way delay than AR-MAC. Nevertheless, AR-MAC in both color modes guarantees a maximum one-way delay which is bounded by twice the superframe duration, irrespectively of the characteristics of the BS and sensor nodes.

7.3.3.4 Traffic Protection

To evaluate the efficiency of the differentiated retransmission policy used by AR-MAC protocol to improve or protect the QoS of critical traffic, tests were carried out on a WSN using sensor nodes with real characteristics, superframe duration of 250 ms, and an interference period of 25 ms. An ideal BS was considered because typically a BS has more computing resources than sensor nodes. Tests were carried out for both color modes. Figure 7.8 shows the results obtained for distinct numbers of BSNs in the WSN. The graphics show the highest average DER obtained considering all critical BSNs. The same criterion also applies to the normal BSNs.

To exemplify how graphics should be interpreted, let us consider Figure 7.8*e* relative to a WSN with a size S equal to seven BSNs. Tests were carried out considering successively X critical BSNs and $(7 - X)$ normal BSNs. For $X = S$, all BSNs are in emergency state, and so no differentiation policy is applied among the diverse BSNs. This particular case is important, since it sets a reference to evaluate the efficiency of the differentiation policies on critical traffic protection. This reference is represented in Figure 7.8*e* by the horizontal line (REF1) passing at the ordinate relative to $X = S = 7$ of the one-color mode graphic. Analogously, a reference line (REF2) is also represented in Figure 7.8*e* for the two-color mode graphic. Although not explicitly represented, reference lines should also be considered in the other diagrams of Figure 7.8 for analysis purposes.

When the WSN, operating with two-color AR-MAC, has four BSNs in critical state and three BSNs in normal state, all critical BSNs present a $\overline{\text{DER}}$ below 0.12%, and all normal BSNs below 1.0%. It is also observed that if $X < 3$, all critical BSNs present a $\overline{\text{DER}}$ below 0.001% (indeed, equal to 0%), and the distance to the reference line is maximized, revealing the highest critical traffic protection. The reference line evinces that the applied policies contribute to improve the $\overline{\text{DER}}$ of the critical BSNs, while the number of critical BSNs does not prevail over the number of normal BSNs in the WSN.

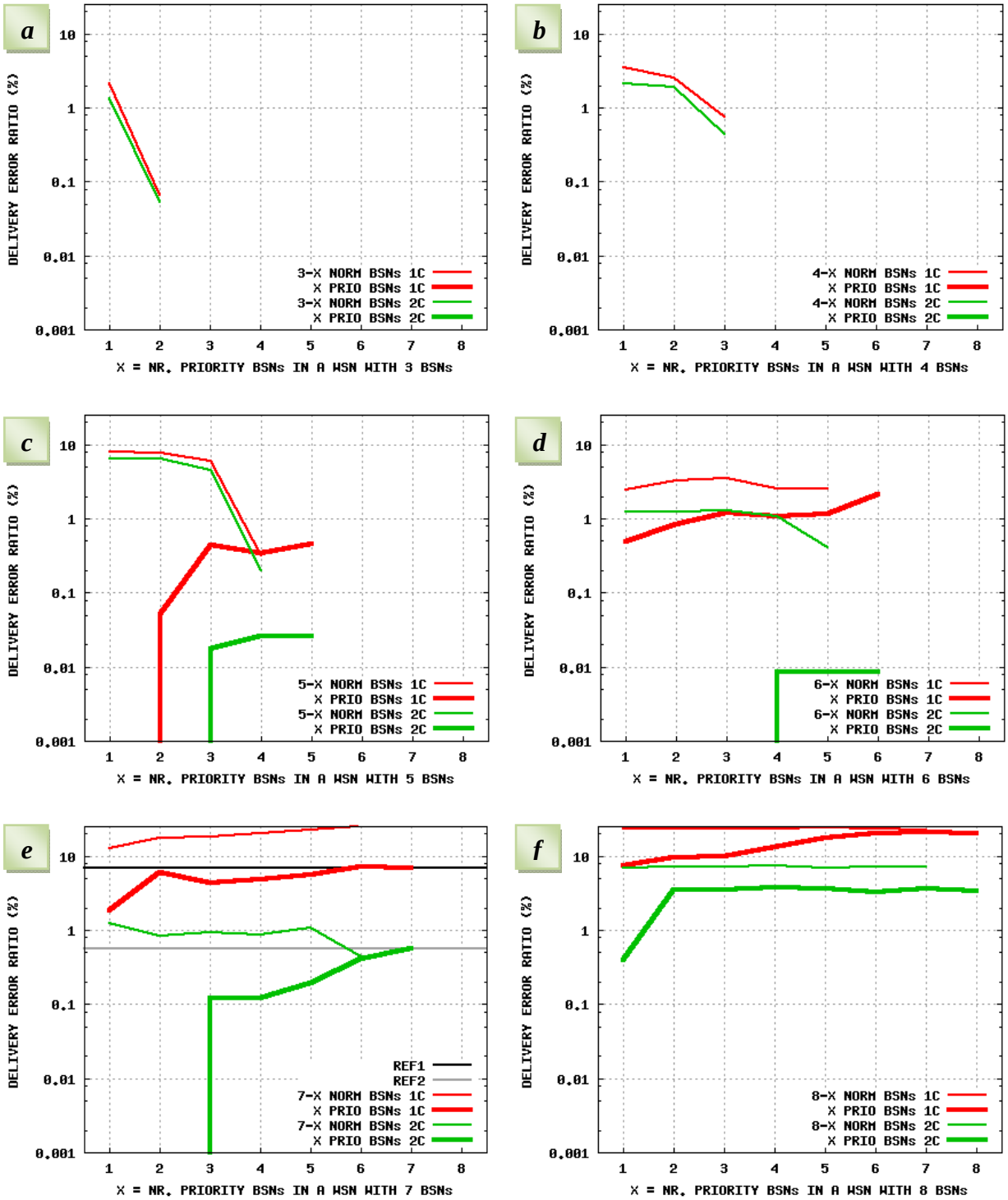

Figure 7.8 – Critical traffic protection with AR-MAC considering a WSN with: (***a***) 3 BSNs; (***b***) 4 BSNs; (***c***) 5 BSNs; (***d***) 6 BSNs; (***e***) 7 BSNs; and (***f***) 8 BSNs.

It is also observed that the differentiation policy is more effective in two-color mode than in one-color mode. This conclusion also holds for $S = 5$ and $S = 6$. For $S = 8$, the superframe bandwidth occupancy is near saturation. However, some differentiation is still possible to obtain for one critical BSN. For $S \leq 4$, all critical BSNs presented a $\overline{\text{DER}}$ null, even for $X = S$, irrespectively of the color mode in use.

In summary, the tests carried out in the experimental scenario have shown that in non-saturated WSNs the differentiation policy of AR-MAC can improve or protect the QoS of critical traffic by sacrificing the performance of normal traffic.

7.3.3.5 Power Consumption

Tests were carried out to evaluate the impact of AR-MAC protocol on the power consumption of the network. To better evince this impact, the consumption due to the samplings performed by the sensing devices is ignored. Tests were also run with the temperature sensor nodes turned off, as their contribution to the network power consumption is much lower than the contribution of the other types of sensor nodes.

The simulator was parameterized with the transceiver consumptions in sleeping, listening, and receiving mode presented in Table 5.2. The experimental tests only used the full-sleeping mode. The power consumption of the ZigBit microcontroller (15.6 mW, cf. Table 5.1) was also considered. These specifications are applied in the tests using sensor nodes with real characteristics. Tests using ideal sensor nodes assume the same power consumptions but the delay of each state transition is zero. As each BSN is composed of four active sensor nodes and because the microcontroller must be always active to collect the signal samples, this unit imposes a baseline on the power consumption of each BSN equal to 15.6 x 4 = 62.4 mW. The experimental tests measured the average power consumption taking into account all BSNs. This metric was chosen because the average power consumption of each BSN presents similar values. Figure 7.9 shows the increase in the power consumption, expressed in percentage, for diverse situations when compared with the reference case of having no interfering traffic on the WSN. The reference power consumption is 81 mW for the tests using sensor nodes with real characteristics, and 67 mW for the tests with ideal sensor nodes.

If the energy consumption of the sensing devices is not null, then the total power consumption of each BSN comes increased by a constant amount. For example, an energy consumption of 0.01 mJ/sample imposes an overhead of 4 mW in the average power consumption of each BSN. In this case, the power consumption increment does not differ significantly from the values presented in Figure 7.9, as tests actually confirmed.

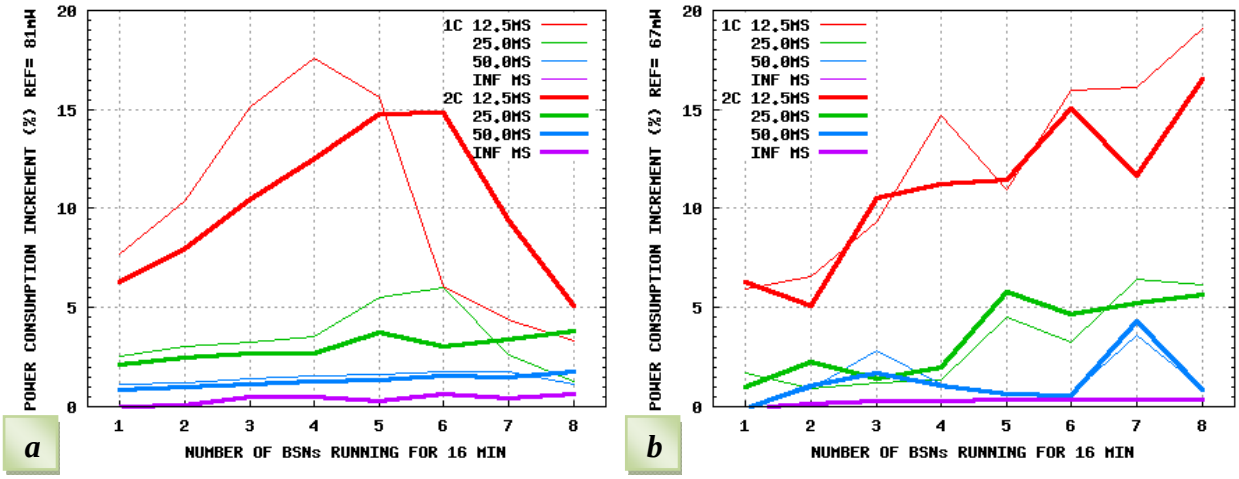

Figure 7.9 – Power consumption increment for sensor nodes with (***a***) real and (***b***) ideal characteristics, both color modes, superframe duration of 250 ms, and interference periods of 12.5 ms, 25 ms, 50 ms, and infinite.

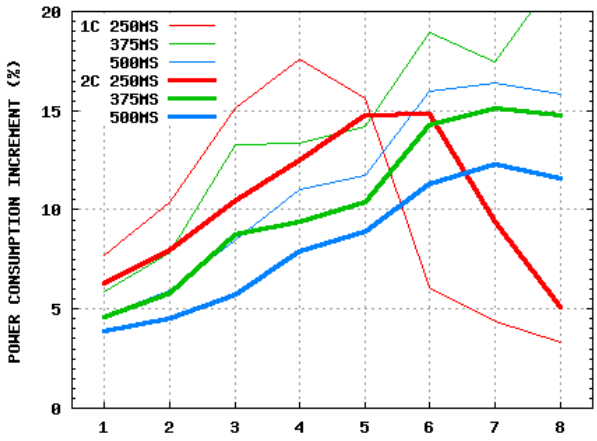

Figure 7.10 – Power consumption increment for real sensor nodes, both color modes, interference period of 12.5 ms, and superframe durations of 250 ms, 375 ms, and 500 ms.

Figures 7.9*a* and 7.9*b* illustrate that the software processing delays presented by the real sensor nodes' model do not degrade significantly the power consumption of a BSN when compared with the tests using the ideal sensor nodes' model. The external interferences have more impact, as the power consumption increases with the interfering traffic volume. The test carried out with an interference period of 12.5 ms presents an intriguing reduction of the power consumption as the WSN size increases above six BSNs. In fact, at this point the retransmission capacity of the WSN is completely saturated causing retransmission packets to be discarded at the sender, which alleviates the network power consumption. This deflective behavior should occur for a higher number of BSNs as the superframe duration is larger, because the retransmission bandwidth increases. Figure 7.10 confirms this fact illustrating the power consumption curves for both color modes and distinct superframe durations – 250 ms, 375 ms, and 500 ms. It is also noticed that, if the retransmission capacity of the network is not saturated, the increment of the superframe duration contributes to reduce the average power consumption. Figure 7.9*a* and Figure 7.10 also show that if the network retransmission capacity is near saturation, the deployment of the WSN in two-color mode contributes to reduce the power consumption.

In summary, the real characteristics of sensor nodes in an AR-MAC WSN do not degrade significantly the power consumption of a BSN when compared to ideal sensor nodes. However, external interferences may affect negatively the network power consumption, particularly if the interfering traffic volume is high. Increasing the superframe duration may reduce the power consumption if the network retransmission capacity is not saturated. If the retransmission capacity is near saturation, the operation in two-color mode may alleviate the power consumption of the WSN.

7.3.3.6 Scalability

In the context of this study, a WSN is considered scalable up to n BSNs if all these BSNs present a maximum $\overline{\text{DER}}$ not above 0.5%. In this way, the network scalability can be directly inferred from the diagrams presented in Figure 7.3 and Figure 7.4.

Table 7.2 presents the scalability level for different superframe durations, considering sensor nodes with real and ideal characteristics, and a BS with ideal characteristics. The underscored values were obtained considering a BS with real characteristics. The last row of the table presents the absolute maximum limits of the WSN scalability, determined considering no interfering traffic in the WSN - i.e., infinite (INF) interference period. In this case retransmissions never occur, and so these values were calculated theoretically to overcome the limitation of the simulation testbed regarding the maximum number of BSNs it can handle[32]. As observed in Table 7.2, the limit is nineteen BSNs. This constrain is probably imposed by the memory capacity of the computer. Tests were carried out using superframes and sensor nodes of only one color. Tests were also run with two colors: ECG and ART sensor nodes are of color one; OXI and RR are of color two. As TEMP sensor nodes transmit all data packets in the CAP, their color attribute is irrelevant. The data volume sent by each sensor node was equal in both color-mode tests. Comparing the real to the ideal case, it is clear how the processing time imposed by the software components deteriorates greatly the scalability of the e-health WSN. Indeed, the degradation can be above fifty percent.

Figure 7.11 represents graphically the data in Table 7.2 for a better comparison. Recall that INF gives the absolute maximum scalability of the WSN. Tests are identified through the notation {SD color-mode}. For example {250 1c} refers to the test carried out with the superframe duration of 250 ms and one-color mode. In Figure 7.11*a*, all graphic curves relative to one-color mode (i.e., {250 1c}, {375 1c}, {500 1c}) coincide with the blue line {500 2c}. With AR-MAC, it is notorious how sensor nodes with ideal characteristics improve appreciably the network scalability when compared with sensor nodes with real characteristics. In the case of sensor nodes with real characteristics, it is observed that using the WSN in two-color mode tends to improve the scalability comparatively to one-color mode.

[32] If the WSN operates in two-hop mode (see Section 4.2.3), the values indicated in the last row of Table 7.2 nearly duplicate. This occurs because data of ART, OXI and RR sensor nodes are transmitted aggregately in single packets to the BS.

T_{intf} (ms)	SD = 250 ms						SD=375 ms						SD=500 ms					
	real			ideal			real			ideal			real			ideal		
	1c	2c	Z	1c	2c	Z	1c	2c	Z	1c	2c	Z	1c	2c	Z	1c	2c	Z
12.5	2 2	2	2	2	2	2	2 2	3	4	2	2	4	2 2	4	4	2	2	5
25	5 4	7	3	13	15	5	8 8	11	5	≥ 19	≥ 19	5	11 10	14	7	≥ 19	≥ 19	6
50	6 6	7	3	17	16	5	11 11	13	6	≥ 19	≥ 19	7	14 14	17	8	≥ 19	≥ 19	7
INF	8	8	4	18	16	5	13	13	8	27	25	8	18	18	10	37	34	8

Table 7.2 – WSN scalability, in terms of number of BSNs supported, for AR-MAC in one (*1c*) and two (*2c*) color modes, and for IEEE 802.15.4 (*Z*).

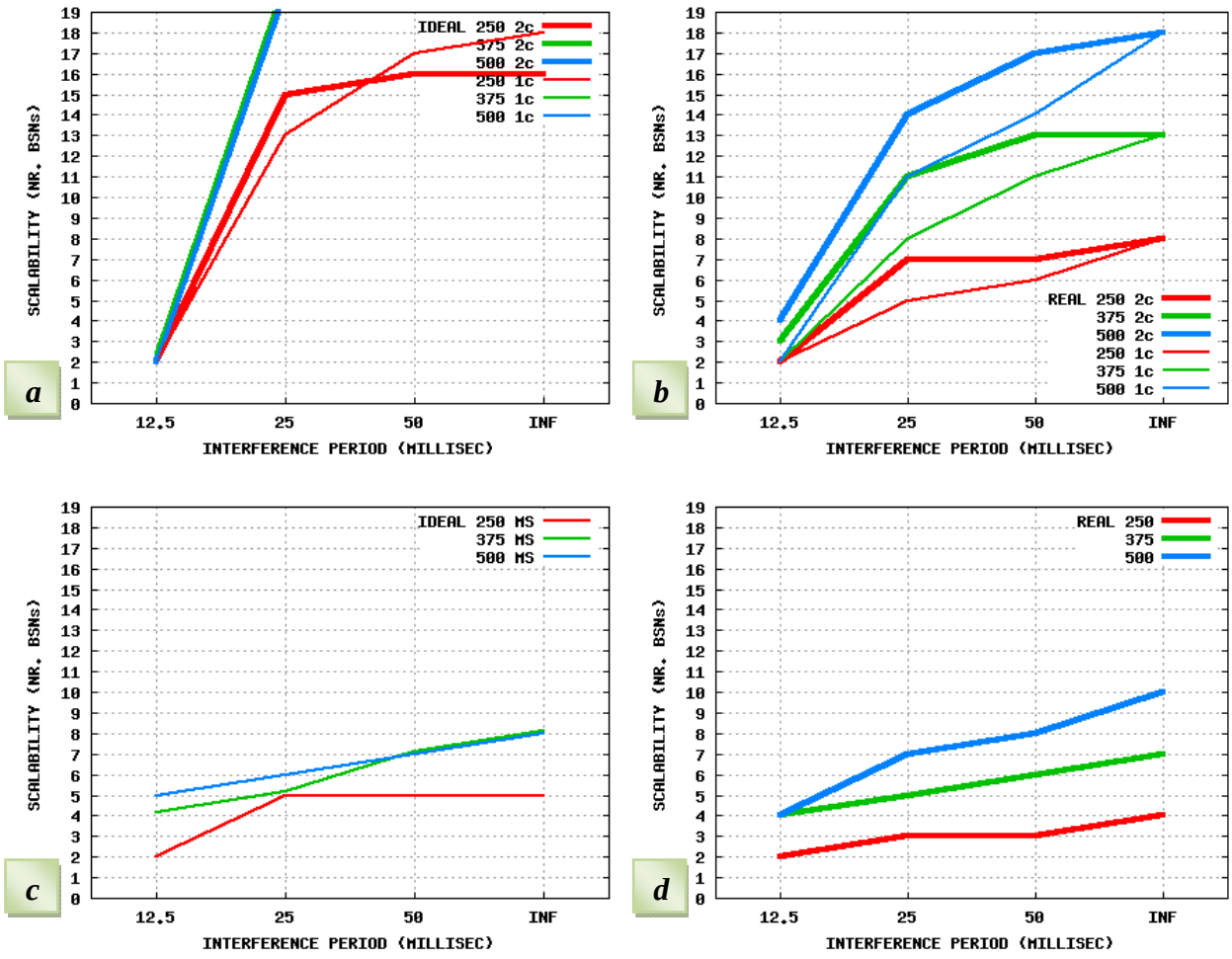

Figure 7.11 – Scalability for AR-MAC WSN, both color modes, with (***a***) ideal and (***b***) real sensor nodes; for IEEE 802.15.4 WSN with (***c***) ideal and (***d***) real sensor nodes.

With IEEE 802.15.4, the use of sensor nodes with ideal characteristics brings little benefit to the network scalability. Also, the scalability is globally lower when compared with AR-MAC.

In summary, the processing time imposed by the software components of sensor nodes deteriorates significantly the scalability of an AR-MAC WSN. The scalability of an AR-MAC WSN is not significantly affected by the real characteristics of the BS and is generically higher comparatively to an IEEE 802.15.4 WSN. The AR-MAC WSN scalability may be improved using two colors instead of one color, particularly when the interfering traffic volume is not high. Scalability may be also improved by increasing the superframe duration or reducing the interfering traffic load.

7.3.3.7 Reconfiguration Tests

Experimental tests were carried out to evaluate the performance of the reconfiguration scheme used by AR-MAC. For comparison purposes, tests were also carried out using AR-MAC with the method adopted by IEEE 802.15.4 to reconfigure a WSN regarding the allocation of new GTSs. According to this method, when the BS decides to grant GTSs to a sensor node, it broadcasts consecutively the new GTS allocation scheme for a predefined number of beacons (four).

The metric tested in the experiments was the number of superframes required to reconfigure successfully the WSN with a new set of instructions broadcasted by the BS. Once a reconfiguration process of the WSN is terminated, another one starts immediately. In the tests with the AR-MAC reconfiguration scheme, a reconfiguration process is considered successful and complete when the BS knows that all sensor nodes are aware of the new instructions. Consequently, all sensor nodes may start transmitting in the next superframe in accordance with the received instructions. In the experiments with the IEEE 802.15.4 reconfiguration method, a reconfiguration process is considered successful and complete when all sensor nodes get informed about the new instructions. In this case, the tested metric was the minimum number of superframes required to inform all sensor nodes about the new instructions.

Figure 7.12 shows the results obtained with the AR-MAC reconfiguration scheme and Figure 7.13 with the IEEE 802.15.4 reconfiguration method. Tests were run using sensor

nodes with real characteristics, superframe duration of 250 ms, and different test conditions regarding the color mode and the interference period used. The figures present the number of superframes required to reconfigure the WSN considering distinct number of BSNs present in the WSN, as well as the percentage of the reconfiguration processes that required either more than N superframes or less than N superframes to be completed successfully. The figures present one bar graphic and two curves. For each number of BSNs present in the WSN is shown in the *bar graphic* the maximum, the average, and the minimum value of the number of superframes required to reconfigure the WSN. For example, if six BSNs are present in a WSN with 12.5 ms interfering traffic (cf. Figure 7.12*a*), then the average number of superframes required to reconfigure the WSN considering all BSNs is four; the number of superframes considering only the BSN that presented the highest value is twelve; the number of superframes considering only the BSN that presented the lowest value is two. It is also presented a curve with the percentage of the reconfiguration processes that required one or two or three superframes to be completed successfully, as well as a curve with the percentage of the reconfiguration processes that required five or more superframes. The graphics do not include the case $N = 4$ to improve the quantity of information extracted from them. Indeed, it is easy to obtain the percentage of the reconfiguration processes that required four superframes. For example, if six BSNs are present in a WSN with 12.5 ms interfering traffic (cf. Figure 7.12*a*), 42% of all reconfiguration processes required five or more superframes to reconfigure the WSN, 30% of all reconfiguration processes required one, two, or three superframes, and 100 – 42 – 30 = 28% required four superframes.

It is observed that AR-MAC reconfiguration scheme presents a good performance (not above three superframes), if the number of BSNs is lower than the WSN scalability limit (cf. Table 7.2). While this condition holds, the maximum number of superframes to reconfigure the WSN is slightly higher in two-color mode than in one-color mode, which is comprehensible as sensor nodes operating in one-color mode can transmit in all superframes. Once reached the WSN scalability limit, the two-color mode revealed clearly a better performance than one-color mode. AR-MAC reconfiguration scheme also presented globally a better performance than IEEE 802.15.4 reconfiguration method.

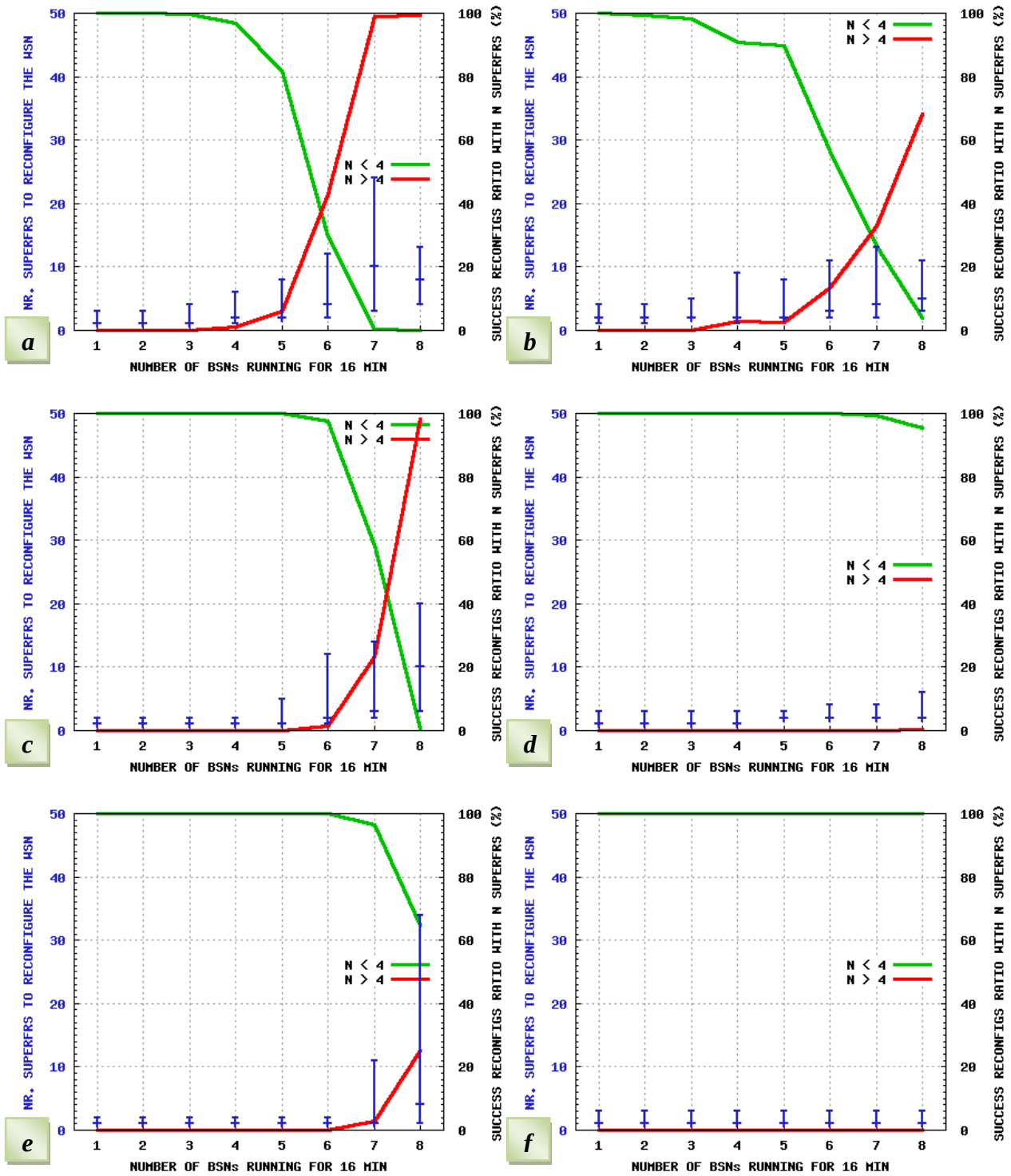

Figure 7.12 – Number of superframes to reconfigure the AR-MAC WSN for: (***a***) one-color mode and interference period of 12.5 ms; (***b***) two-color & 12.5 ms; (***c***) one-color & 25 ms; (***d***) two-color & 25 ms; (***e***) one-color & 50 ms; and (***f***) two-color & 50 ms.

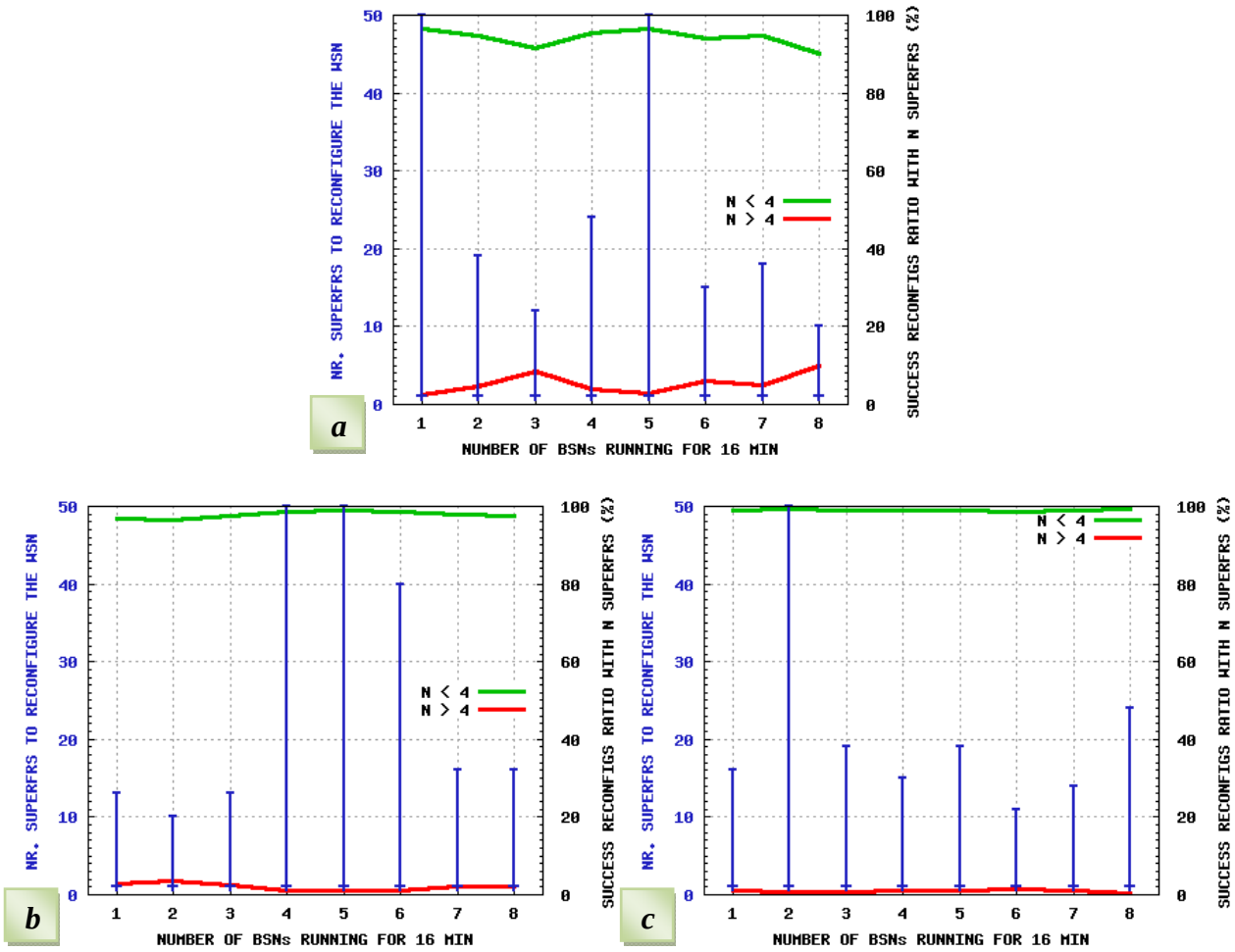

Figure 7.13 – Number of superframes to reconfigure the WSN with the IEEE 802.15.4 method for interference periods of (***a***) 12.5 ms, (***b***) 25 ms, and (***c***) 50 ms.

In summary, AR-MAC reconfiguration scheme, in both color modes, presents a good performance when the number of BSNs is lower than the WSN scalability limit. Once reached this limit, the two-color mode performs better than one-color mode. AR-MAC reconfiguration scheme generically performs better than the IEEE 802.15.4 reconfiguration method, especially in two-color mode.

7.3.3.8 RP Usage Tests

Experimental tests were carried out to evaluate the efficiency of the NRP usage and ERP usage parameters in detecting the interference level on the wireless channel. Both usage parameters are defined in Section 4.2.2.

The NRP usage parameter allows implementing a lightweight-computing, sensitive mechanism for evaluating the interference degree on the channel. This evaluation process is needed for the channel-switching mode. The NRP usage measurements are calculated in fixed time windows containing a given number of superframes. Figure 7.14*a* shows the average of all NRP usage measurements for distinct number of BSNs in the WSN, as well as the average DER considering the traffic received from all sensor nodes in the WSN. For example, if seven BSNs are present in a WSN with 50 ms interfering traffic, then the average of all NRP usage values measured (in time windows of two minutes) during sixteen minutes is 12%, and the average DER of the traffic received from all sensor nodes in the WSN is 0.5%. The same principle and explanation apply to the average ERP usage and average DER measurements represented in Figure 7.14*b*.

As shown in Figure 7.14*a*, the mechanism provides NRP usage values that vary in accordance with the interference degree on the channel, irrespectively of the number of BSNs present in the network. However, the NRP usage parameter does not consider the robustness capacity of AR-MAC protocol to deliver packets successfully in presence of moderate interference levels. For example, Figure 7.14*a* shows that, with an interfering traffic period of 25 ms, AR-MAC presents an average DER below 0.01% (indeed equal to 0%) while the number of BSNs is below five. The BS may decide to switch the WSN operating channel, if it considers uniquely the NRP usage information. However, if the impact of the interfering traffic on the WSN energy cost (e.g., due to recovery process of lost packets) is insignificant, this operation is not required in networks with less than five BSNs. To improve this aspect, the BS should take into consideration the ERP usage parameter too. As shown in Figure 7.14*b*, this parameter reflects well the packet delivery robustness capacity of AR-MAC protocol. However, it does not provide information about the interference level on the channel, as shown in the example just provided. Indeed, the ERP usage is null for less than five BSNs in the network, in spite of the existence of interfering traffic on the channel. Therefore, the BS should conjugate the

information acquired from both usage parameters to decide more properly about the channel switching need.

In summary, the NRP usage parameter reflects the interference level on the wireless channel, but not the robustness capacity of AR-MAC protocol in terms of packet delivery. On the other hand, the ERP usage parameter reflects better the AR-MAC robustness capacity than the interference level on the channel. The information collected from the ERP usage and NRP usage parameters improves the ability of the BS to decide correctly about the channel switching need.

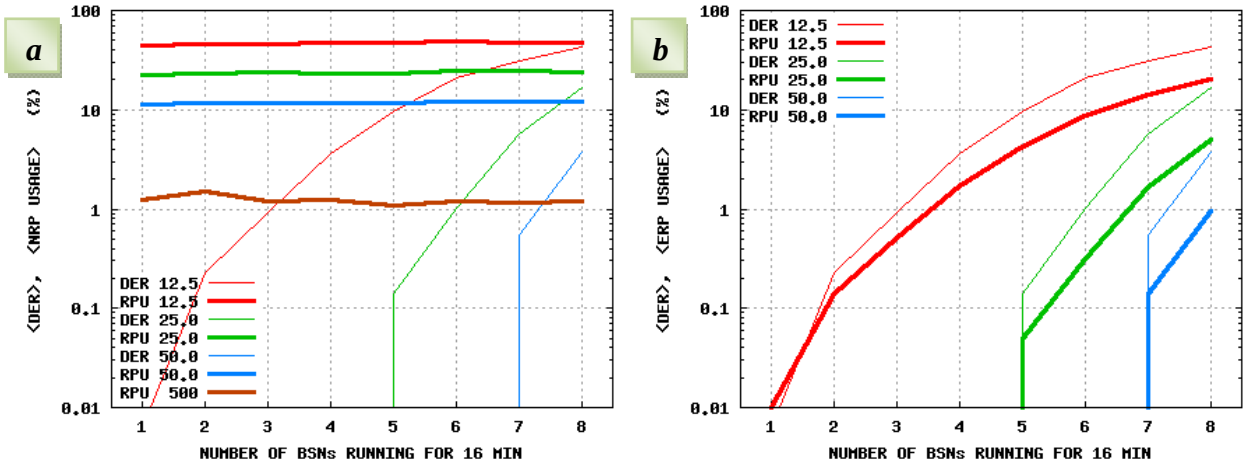

Figure 7.14 – Average DER with average NRP usage (***a***), and average ERP usage (***b***).

7.4 Tests on the Physical Platform

AR-MAC was tested in frequency-hopping mode to evaluate the impact of this communication technique on the data delivery robustness against external wireless interferences. As the simulation testbed runs only in fixed frequency mode, it is not possible to use it in frequency-hopping mode. Consequently, these tests were carried out in the physical testbed.

Tests were also carried out in the physical testbed to assess the efficiency of the method used by AR-MAC to evaluate the interference degree on the channel. The

physical testbed offers the advantage of testing with real IEEE 802.11g traffic on the operating channel.

7.4.1 Test Conditions

The WSN physical platform run AR-MAC protocol configured with the parameters presented in Table 7.3. Retransmissions in the ERP were not considered. All beacons are sent with 14 B of payload, and data packets with 90 B.

parameter	value
beacon interval (ms)	250
time-slot duration (ms)	0.5
BP duration (ms)	1
number of beacons in the BP	1
number of NTP safeguard slots	6
number of RP safeguard slots	2
minimum CAP size (slots)	125
max. nr. of NRP transmissions per sensor	2
max. nr. of ERP transmissions per sensor	0
maximum number of successive NTP transmissions without receiving a beacon	2
number of used colors	1

Table 7.3 – AR-MAC configuration parameters used in the physical testbed.

Controlled IEEE 802.11g traffic is admitted on the selected channel of the WSN. For this purpose, an FTP client downloads a file of fixed size from a remote server every fifteen seconds using a WLAN. The FTP server is located in the PC that is connected to the BS, and the FTP client is placed at an adjacent room. The operating frequency of the IEEE 802.11g WLAN is centered on the channel twenty five of the IEEE 802.15.4 band.

Three distinct experimental situations were considered: (*i*) the WSN operates in a fixed channel interfered with download traffic of 0.5 MB files; (*ii*) the WSN operates in a fixed channel interfered with download traffic of 5 MB files; and (*iii*) the WSN operates in frequency-hopping mode and downloads of 5 MB files occur in a fixed channel. In all tests, a file download occurs every fifteen seconds.

7.4.2 Frequency-hopping Mode

In frequency-hopping (FH) communication techniques, the wireless channel is physically divided up in time and frequency. Experimental tests were carried out to assess the efficiency of AR-MAC, regarding the packet delivery robustness and network reconfiguration ability, when operating in frequency-hopping mode. As ZigBit modules incorporate natively IEEE 802.15.4, a standard that operates in a fixed channel, it was necessary to modify the code of the sensor nodes to implement the frequency-hopping functionality.

It should be noted that whenever the AT86RF230 radio leaves the sleeping state to enter in listening state or transmitting state, the frequency synthesizer is turned on and settled to the channel center frequency defined in the respective register. As in AR-MAC WSNs, sensor nodes normally enter in sleeping mode when data reception or transmission operations are not required, the frequency-hopping mode does not impose additional costs to the network power consumption.

7.4.2.1 Frequency-hopping Scheme

Each superframe is transmitted in a different channel following a round-robin hopping scheme. The beacon and data packets sent in the current superframe are transmitted in the channel which is three channels away from the channel used in the last superframe. Once reached the last channel (26), it continues with the first channel (11) of the IEEE 802.15.4 spectrum band.

7.4.2.2 Results

Figure 7.15 presents the results obtained in the physical platform for distinct numbers of sensor nodes in the WSN. Note that the x-axis present the number of nodes present in the WSN, instead of the number of BSNs. Figures 7.15*a*, 7.15*c* and 7.15*e* show the average DER ($\overline{\text{DER}}$) considering respectively the WSN operating: (*i*) in a fixed channel interfered with 0.5 MB FTP traffic; (*ii*) in a fixed channel interfered with 5 MB FTP traffic; and (*iii*) in frequency-hopping mode and 5 MB FTP traffic. For each number of active sensor nodes in the WSN is presented the maximum, average, and minimum $\overline{\text{DER}}$ values. For example, if fourteen sensor nodes are operating in a fixed channel interfered with 0.5 MB FTP traffic (cf. Figure 7.15*a*), the $\overline{\text{DER}}$ considering all packets received by the BS from all sensor nodes is 0.11% (average value); the $\overline{\text{DER}}$ considering only the traffic flow from the sensor node that presented more undelivered packets is 0.5% (maximum value); the $\overline{\text{DER}}$ considering the traffic flow from the sensor node that presented less undelivered packets is below 0.001% (minimum value). Figures 7.15*b*, 7.15*d* and 7.15*f* show the results regarding the number of superframes required to reconfigure the WSN when the number of sensor nodes increase, and for the test conditions (*i*), (*ii*), and (*iii*) described above. Graphics should be interpreted as explained in Section 7.3.3.7. The curves represent the percentage of the reconfiguration processes that required more than one superframe to be completed successfully.

To confirm that the volume of uncontrolled interfering traffic on the WSN channel is negligible, a previous test was run with the FTP client disabled, so that no file transfer was carried out. It was observed that the WSN always presented a null $\overline{\text{DER}}$, even for sixteen sensor nodes.

If the FTP client downloads 0.5 MB files from the server, the $\overline{\text{DER}}$ is null while the number of sensor nodes is below twelve (cf. Figure 7.15*a*). However, if the FTP client downloads 5 MB files, the $\overline{\text{DER}}$ becomes appreciable, independently of the number of sensor nodes present in the WSN (cf. Figure 7.15*c*). Tests revealed that, in this case, increasing the maximum number of retransmissions in the RP did not improve the $\overline{\text{DER}}$ significantly, even reducing the payload size of the data packets.

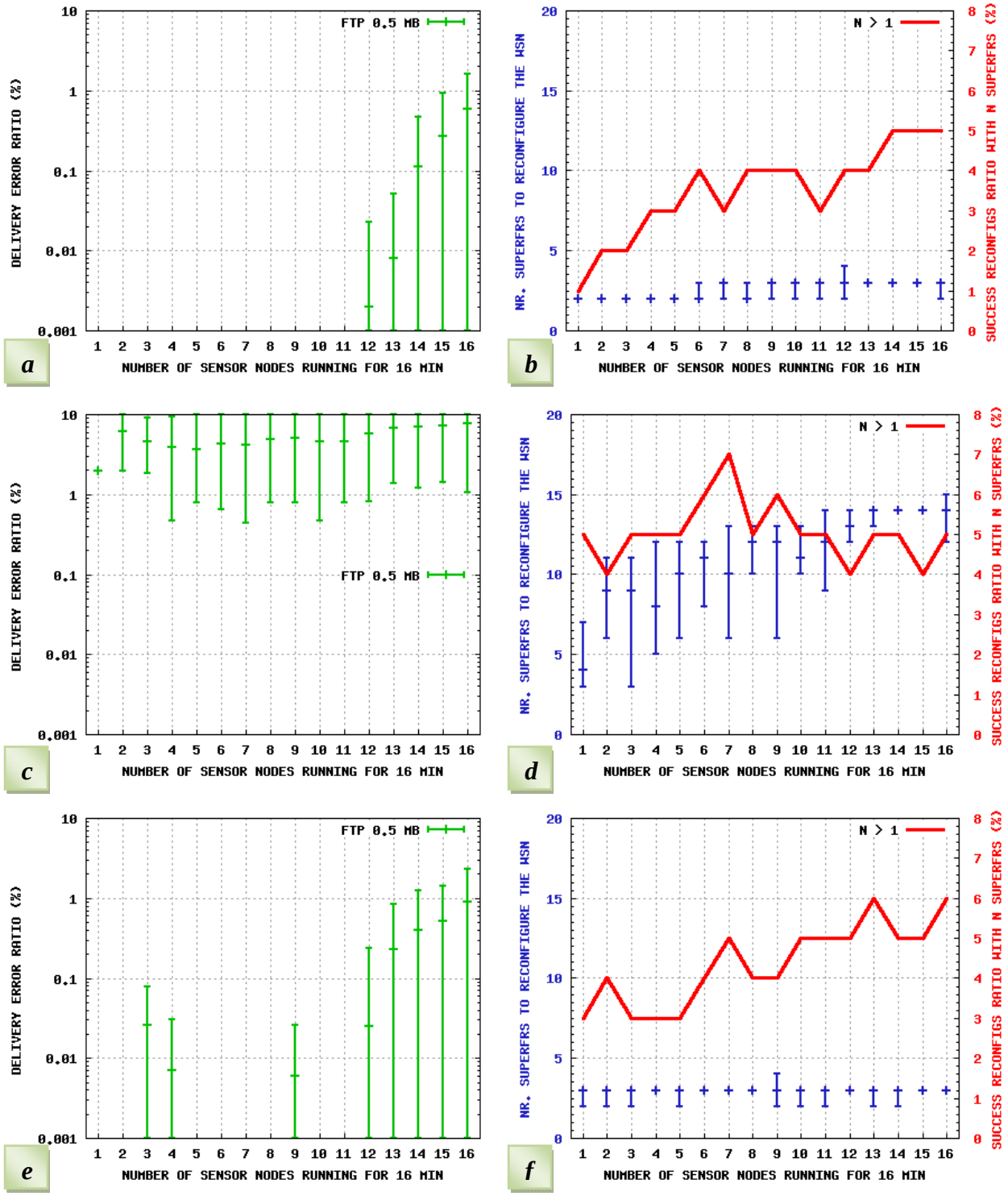

Figure 7.15 – Average DER for (***a***) 0.5 MB; (***c***) 5 MB; (***e***) FH 5 MB; and number of superframes to reconfigure the physical WSN for (***b***) 0.5 MB, (***d***) 5 MB; (***f***) FH 5 MB.

Figure 7.15*e* shows that the $\overline{\text{DER}}$ improves notoriously using the WSN in frequency-hopping mode. It should be noted that during the frequency-hopping process, some channels may present uncontrolled interfering traffic from external sources, such as IEEE 802.11 WLANs. This fact might explain the packet loss occurred with three and four sensor nodes in the WSN.

The frequency-hopping mode also presents an interesting performance regarding the reconfiguration efficiency. Indeed, if the interference level is moderate in fixed channel mode, the WSN reconfiguration occurs in less than one second (cf. Figure 7.15*b*). But if the interference level is appreciable (cf. Figure 7.15*d*), then frequency-hopping mode may be an alternative to keep the reconfiguration time below one second (cf. Figure 7.15*f*).

Figure 7.16*a* shows that the average delay improved slightly with the frequency-hopping mode. The maximum delay of the delivered packets was bounded and below 500 ms in all tests. Figure 7.16*b* shows that the duplicate packet ratio improved with the frequency-hopping mode too.

In summary, an AR-MAC WSN operating in frequency-hopping mode may contribute to improve both the network reconfiguration capacity and the packet delivery ratio, and consequently the network power consumption, principally if most of the channels used in the hopping scheme present low volumes of interfering traffic.

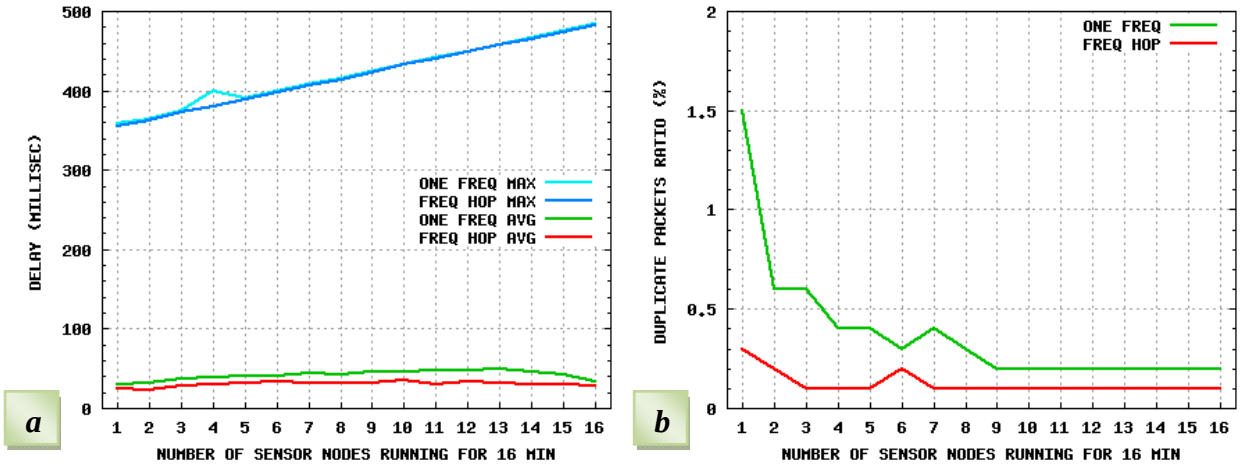

Figure 7.16 – Average and maximum delays (***a***); average duplicate packet ratio (***b***).

7.4.3 Channel Interference Assessment

Despite of frequency-hopping being a valuable technique to improve the packet delivery ratio, it is not totally efficient because interfering traffic may be present in channels addressed to the hopping scheme. A more efficient solution would be using the AR-MAC WSN in channel-switching mode. In this mode, the BS looks for a free wireless channel whenever it detects an unacceptable volume of interfering traffic in the operating channel. For this purpose, AR-MAC uses a mechanism based on the NRP usage and ERP usage parameters to assess the interference level on the channel. As retransmissions in the ERP were not used in the tests carried out in the physical platform, only the NRP usage parameter was considered.

In order to show that the NRP usage parameter is useful to evaluate the interfering degree on the wireless channel, Figure 7.17 presents the graphics obtained in two distinct tests carried out on the physical testbed when an FTP client downloads a 5 MB file from a server every fifteen seconds using an IEEE 802.11g WLAN. The TCP slow-start mechanism used by the FTP traffic had distinct behaviors in both tests, and so the graphics are not similar. These graphics present the average DER ($\overline{\text{DER}}$), considering all packets delivered to the BS from all sensor nodes, as well as the average NRP usage (NRPU) calculated using a time window of two minutes, which corresponds to four hundred and eighty superframes. This time window was chosen because the BS sends statistical data to the PC every two minutes. As shown, the NRP usage curve follows the behavior of the $\overline{\text{DER}}$ curve, while the NRP slot occupancy does not saturate. This fact can be observed in the red curves of Figure 7.17. Here, the NRP usage curve reflects relatively well the interfering degree on the wireless channel while the number of sensor nodes in the WSN is less than thirteen. Above this number, the NRP slot allocation saturates and consequently the NRP usage curve also saturates, despite of the increasing $\overline{\text{DER}}$. However, once reached this point, the BS should already be perfectly aware of the high interference degree in the channel.

In summary, the NRP usage parameter provides to AR-MAC protocol an efficient lightweight-computing mechanism to assess the interfering degree in the operating channel.

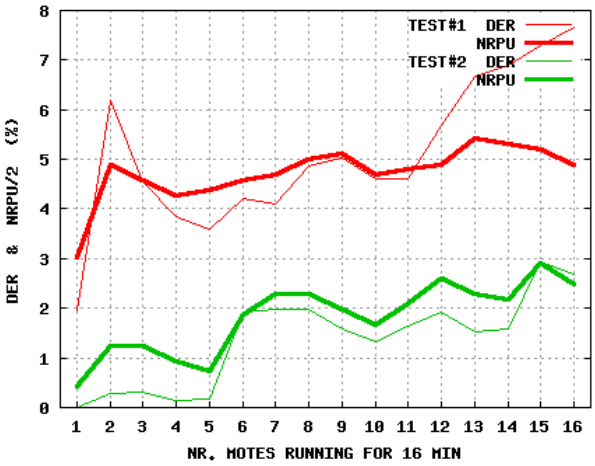

Figure 7.17 – Average DER and average NRP usage.

7.5 Summary

Tests were carried out on a physical testbed to evaluate the efficiency of AR-MAC in frequency-hopping mode. Results showed that this operating mode may contribute to improve both packet delivery and network reconfiguration efficiency. Alternatively, AR-MAC may also operate in channel-switching mode. Real tests showed that AR-MAC protocol includes an efficient lightweight-computing mechanism to assess the interference level on the channel, as required in channel-switching mode.

AR-MAC protocol was also (and mostly) evaluated in a validated e-health simulation scenario to test its performance regarding the packet delivery robustness, maximum delay, traffic protection, power consumption, scalability, and network reconfiguration. Despite of the tests having been carried out inevitably with specific interfering traffic patterns (and no fading or shadowing phenomena), generic conclusions can be inferred from the obtained results, which are presented in the next and final chapter of this thesis.

Chapter 8

Conclusions and Future Work

8.1 Introduction

In order to assure a pervasive and trustful assistance to patients under health risk, e-health systems and underlying communication infrastructures must provide QoS support, since e-emergency services demand for reliability, guaranteed bandwidth, and low delays due to their real-time nature. Energy preservation, adaptability, and scalability are also relevant characteristics in these networks. The MAC layer plays a special role in the QoS support, as the medium access and the reliability of the communication channel directly impact on the performance of upper layer protocols. However, current MAC protocols fall short in meeting those demands, as discussed in Section 3.4. To cover such shortage, the present work conceived, implemented and tested AR-MAC, a new MAC protocol presenting original concepts to assure the QoS of e-health WSNs regarding data transmission robustness and packet delivery deadline. AR-MAC provides dynamic reconfiguration and channel switching mechanisms, with the capacity of forwarding frames in two-tier network structures. This is the main contribution of this work. Another important contribution of the work was the design, implementation and testing of a new parametric model for WSN simulators. Generic conclusions regarding both contributions are presented in the following. Section 8.3 suggests directions for future research.

8.2 Conclusions

The next section presents conclusions relative to the performance of AR-MAC taken from the simulation tests. It is also discussed strategies and tradeoffs to improve the AR-MAC performance. Section 8.2.2 presents the conclusions regarding the parametric model. Section 8.2.3 discusses a few topics uncovered in the previous sections.

8.2.1. AR-MAC Protocol

As mentioned earlier, the main research accomplishment of this work has been the conception, implementation and testing of AR-MAC, a novel MAC protocol that

provides QoS regarding data transmission robustness, packet delivery deadline, and bandwidth utilization efficiency. AR-MAC is also energy efficient, because sensor nodes stay in sleeping mode when they are not scheduled to transmit or receive a packet. Moreover, AR-MAC has the capacity of reconfiguring dynamically the network in accordance with the patients' health state (adaptability), the capacity of forwarding frames in two-tier networks, and the capacity of coexistence. A MAC protocol with these properties brings an added value for e-emergency WSNs. As discussed in Chapter 3, the MAC protocols identified as being the most direct competitors of AR-MAC - namely VTS, LMAC, PEDAMACS, I-EDF, Dual-mode MAC, CR-SLF, RRMAC, LPRT, CICADA, GinMAC, TSMP, Bluetooth, and IEEE 802.15.4 - are unable to fulfill simultaneously all these requisites (see Figure 3.1). To accomplish such goal, AR-MAC uses diverse original solutions and strategies, namely ERP and NRP ACK bitmaps, criticality and activity bitmaps, coloring and reconfiguration schemes, short-size beacons, distributed slot allocation, auto channel switching, cluster mode operation, and beacon arrays (see Table 4.1).

8.2.1.1 AR-MAC Performance

In order to evaluate the AR-MAC performance in an e-emergency WSN, tests were carried out in a validated simulation platform and compared with the IEEE 802.15.4 MAC protocol (see Chapter 7), which is prominently used in diverse wireless e-health projects. The overall conclusions obtained from the results of these tests are presented next. These conclusions are based on the assumption that AR-MAC operates in a WSN whose characteristics are similar to the network characteristics used in the experimental test scenario, i.e., non-dense WSNs under regular and heterogeneous traffic.

Robustness. AR-MAC revealed packet delivery robustness while the network size does not reach the scalability limit. The results show that the packet delivery performance of AR-MAC tends to improve significantly as the characteristics of the sensor nodes approach the ideal characteristics, the superframe duration increases, or the interfering traffic load reduces. The performance of AR-MAC protocol may be appreciably enhanced by operating in two-color mode instead of one-color mode. If properly tuned, AR-MAC protocol in both color modes revealed immunity to the BS

characteristics. According to these conclusions, diverse actions can be performed to reinforce the robustness capacity of AR-MAC.

(*i*) Increasing the superframe duration and keeping the time-slot duration contribute to improve robustness, because more RP time-slots become available for retransmission trials.

(*ii*) A sensor node should use the highest color number able to guarantee the maximum delay bound. As the color mode is conditioned by the sampling rate used in the sensor node, it results that a sensor node should use the lowest possible sampling rate in accordance with patient's clinical state.

(*iii*) The sensor nodes' characteristics should be as ideal as possible, which means that the sensor nodes' computation overhead must be as low as possible. For this goal, software components should be built taking into account the specific features presented by the sensor node's components, such as the microcontroller architecture, and the requirements of the WSN application, such as the deterministic degree of the application. Operating systems for generic WSNs are not the best choice as they are not optimized for the specific architecture of a sensor node. In the eventuality of using a generic operating system and if its source code is available, then the code of the operating system should be modified in conformity with the network characteristics. For example, tasks should be avoided during the time-critical operations of the MAC layer. Also, the number of protocol stack layers should be minimized to improve the packet processing time. Cross-layer solutions are recommended to accomplish this goal.

(*iv*) Interfering traffic should be minimized. This goal may be accomplished using channel-switching or frequency-hopping techniques. Both possibilities are available in AR-MAC.

(*v*) Packet loss depends on the beacon loss, since a retransmission trial only occurs if the beacon is received. Increasing the number of beacons in the BP improves the probability of beacon delivery and consequently the packet delivery ratio.

Timeliness. AR-MAC in both color modes guarantees a maximum delay below twice the beacon interval, irrespectively of BS and sensor nodes' characteristics. This means that the maximum packet delivery delay can be controlled with the beacon interval. As the beacon interval increment contributes to improve the packet delivery ratio, the energy saving, and the network scalability, the beacon interval should be set approximately to half of the allowed maximum delay. Also, increasing the number of beacons in the BP may contribute to improve the timeliness, because the retransmission capacity is

enhanced. Indeed, a sensor node may retransmit in a superframe only if it receives the respective beacon.

Bandwidth utilization efficiency. The utilization of high-grained superframes and the enhancement of nodes' characteristics improve the bandwidth utilization. Robustness is also improved, because saving bandwidth leads to an increase in the retransmission capacity.

Scalability. Test results show that the processing time imposed by the software components deteriorates significantly the network scalability. The scalability may be improved using non-single color mode, increasing the superframe duration, and/or reducing the interfering traffic load. Since scalability is inherently correlated with packet loss, the strategies pointed out to improve packet delivery robustness also hold for scalability.

Adaptability. AR-MAC reconfiguration scheme, in both color modes, presents a good performance while the WSN scalability limit in terms of number of BSNs is not attained. After reaching this limit, the two-color mode performs better than one-color mode. Since adaptability performance is related with packet loss, the strategies indicated to improve packet delivery robustness hold for adaptability too.

Energy preservation. The energy consumption is not significantly affected by the real characteristics of sensor nodes in an AR-MAC WSN. External interferences have more impact on the deterioration of the energy consumption, especially with high interfering traffic volumes. The energy saving can be reinforced through diverse actions.

(*i*) Interfering traffic should be minimized using channel-switching or frequency-hopping techniques.

(*ii*) The use of color mode technique contributes to energy saving because the transmission overhead decreases. Moreover, the number of retransmission trials also tends to decrease, as well as the energy consumption, since the number of packets transmitted in the NTP decreases with the sensor node´s color number.

(*iii*) Increasing the superframe duration in a non-saturated network may reduce the power consumption because the number of bytes sent per time interval tends to diminish.

Coexistence capacity. This characteristic is naturally assured with AR-MAC, since every sensor node uses distinct time-slots to transmit data.

Table 8.1 summarizes the influence on the discussed parameters of diverse network aspects, namely: (*i*) the BS and sensor nodes presenting real or ideal characteristics; (*ii*)

the use of two-color mode; (*iii*) the increment (↗) of the superframe duration; (*iv*) the reduction (↘) of the interfering traffic volume; and (*v*) the use of beacon arrays. The symbols (0), (+) and (–) mean, respectively, that the considered aspect affects insignificantly (0) or contributes to improve (+) or deteriorate (–) the performance of the considered parameter.

Note that the influence of the network aspects on the packet delivery robustness, scalability, and adaptability is identical. This is not surprising because scalability and adaptability are correlated with the packet delivery performance. In addition, the real characteristics of a BS do affect not affect significantly the considered metrics, because the time required to send a packet from the application layer to the wireless channel is larger than the time to receive and deliver it to the application layer (see Table 6.4 in Section 6.4.3).

	BS real	**BS ideal**	**real node**	**ideal node**	**grained superfr.**	**color mode**	**superfr. durat↗**	**interfer traff.↘**	**beacon array**
robustness	0	0	–	+	+	+	+	+	+
timeliness	0	0	0	0	0	–	–	+	+
energy saving	0	0	0	0	0	+	+	+	0
scalability	0	0	–	+	+	+	+	+	+
adaptability	0	0	–	+	+	+	+	+	+
bandwidth efficiency	0	0	–	+	+	0	0	0	0

Table 8.1 – Influence of diverse aspects on the network parameters.

Traffic protection. Tests showed that in non-saturated WSNs the differentiation policy of AR-MAC can improve or protect the QoS of critical traffic at cost of sacrificing the performance of non-critical traffic.

Channel switching. The NRP usage and the ERP usage parameters allow for the BS to make the decision of switching the operating channel when the interference level on the channel is unacceptable. Tests revealed that the NRP usage parameter reflects the interference level on the wireless channel, but not the robustness capacity of AR-MAC protocol against interferences. This last aspect is suitably covered through the ERP usage parameter.

Comparative tests. Similar tests were carried out on a non-slotted IEEE 802.15.4 WSN, for comparison purposes regarding packet delivery robustness, maximum delay, scalability, and network reconfiguration metrics. Excepting the maximum delay, AR-MAC WSN presented globally the best performance results in all metrics.

AR-MAC also showed a notorious improvement over LPRT in terms of delivery error ratio at the cost of a minor degradation of the power efficiency.

8.2.2 Parametric Model

Castalia and most of the generic network simulators do not model the very limited computing resources of sensor nodes, which is a key characteristic of WSNs. If ignored, this aspect may affect significantly the meaningfulness of the simulation results. This work has demonstrated that if the limitations of the software components are not considered, the simulation tests may produce results significantly more optimistic than those obtained in real conditions. In order to improve the reliability of the simulation results, a generic parametric model reflecting the impact of the software components performance of real sensor nodes was developed, tuned and included in the simulator. Simulation tests showed that the results obtained with the proposed model match satisfactory those obtained in real conditions. Therefore, the inclusion of this model in a WSN simulator helps to improve the confidence on the simulation results.

8.2.3 Further Considerations

The simulation and real tests presented in this work were carried out in a relatively well-controlled environment regarding the external interferences and the characteristics of the wireless channel. This strategy was adopted in order to facilitate the analysis of the test results, since the involved traffic and network components are well identified. In this way, tests did not considered diverse important issues of the real word, such as the characteristics of the wireless channel in the immediate environment around the human body, channel fading and shadowing phenomena, mobility, and uncontrolled interferences. Modeling these aspects is a hard topic, despite of researchers having made considerable progress in the recent years, including the characterization of the body area

propagation environment [Reusens09]. In this way, simulation platforms should not be considered definitive substitutes of physical testbeds and real deployments, despite of the huge effort usually involved to study the network performance in real scenarios. Simulation platforms should be regarded mainly as auxiliary and valuable tools to perform preliminary tests and assess research directions. This is especially true in wireless scenarios, since wireless transmissions are more prone to errors than wired transmissions.

Since tests were not carried out in a real deployment, it is hard to assess if AR-MAC can really assure QoS in an e-emergency deployment. However, it is clear that QoS is easier assured in interference free environments. For this reason, e-emergency WSNs should operate in wireless channels and/or use radio technologies relatively immune to external interferences. Increasing the data transmission rate can also contribute to improve QoS since data packets are less exposed to interferences. As UWB technique can provide both interference immunity and high transmission rates, it is expectable that in a real deployment the performance of AR-MAC with UWB may improve considerably.

8.3 Future Work

This final section identifies possible directions for further research in order to improve or consolidate the AR-MAC design and performance.

The temporal variation of the wireless channel characteristics is especially pronounced in BSNs. Consequently, the physical testbed should be used to test AR-MAC in a real e-health scenario, with sensor nodes placed on human bodies. Dynamic and static scenarios should be considered in these tests.

Testing AR-MAC in a multi-hop WSN is a desirable goal, since direct transmission may be neither feasible nor energy efficient in e-health WSNs. This is particularly true in BSNs, as the propagation loss around the human body is high. Preliminary simulation tests have shown that the scalability may improve significantly in two-hop mode, as referred in Section 7.3.3.6.

In multi-hop WSNs, more than one node can transmit at the same time-slot (spatial reuse), if their receivers are not in interfering regions of the network. Therefore, the possibility of using spatial reuse techniques when AR-MAC is operating in two-hop mode should be investigated to improve the bandwidth utilization efficiency of the network.

The method of translating clinical recommendations provided by physician or automated diagnosis systems into network reconfiguration instructions should be researched in order to provide a service with the required monitoring quality. Algorithms should also be studied to help the BS detecting any change in patients' state of health. Algorithms should allow the BS to take the correct decision of reconfiguring the WSN based on the condition of the physiological parameters being sensed by the BSN.

To recover lost or corrupted data, AR-MAC uses retransmission processes. In order to reduce the number of retransmissions, and thus improve the bandwidth utilization efficiency and the power consumption of a WSN, restoration algorithms can be used to recover the missing packets that do not arrive to the BS within an acceptable delay. For example, simulation tests showed that the use of restoration algorithms to recover missing ECG packets, even for 8% of packet loss in transmission, allow reconstructing a functional ECG waveform for doctors [Henrion04]. Therefore, the inclusion of restoration techniques may reinforce considerably the robustness of AR-MAC in heavy interfered channels. This aspect can also be explored as future work. The cost on the global performance of the WSN should be evaluated and, since restoration algorithms use signal processing techniques, they should be applied only in WSNs provided with a powerful BS in terms of computing resources. It would be also interesting to explore hybrid ARQ techniques to recover lost or corrupted data.

Most of the physiological parameters from a patient are dependent and coupled. For example, when a patient gets a fever, the body temperature rises, the heartbeat rate and the blood pressure rise too, and so does the breath rate. The oxygen saturation level in the blood may change too [Li07]. In this way, it would be interesting to explore the possibility of determining the effective importance of retransmitting data of a patient's physiological signal taking into account the data received from other physiological signals. In this way, the BS may conclude from the received data that there is no need to retransmit a lost packet, which contributes to reduce the number of retransmissions.

The study of more efficient policies for traffic protection than those used in this work, which are relatively simple and possibly unfair, also deserves further attention.

Other objectives for future work also include the study of using or adapting AR-MAC to application scenarios other than e-emergency WSNs, as well as the performance evaluation of AR-MAC with other radio technologies, such as UWB. Comparing the AR-MAC performance with the IEEE 802.15.6 protocol is also a very desirable goal.

Diverse aspects of the MAC layer have been overlooked in this work, namely the association and disassociation of a BSN to the WSN. The autonomous startup of an e-health WSN without human participation was not considered too. These important aspects should be investigated.

The utilization of the simulation platform developed for this work is not intuitive for less experienced users. Diverse parameters in different configuration files require tuning before running a simulation. The development of an intuitive and user-friendly graphical interface would be convenient before making the simulation platform openly available for the research community.

Finally, AR-MAC protocol is not a definitive closed subject. Further investigation could improve the performance of the current implementation or add new capabilities.

WSNs bring new challenging opportunities and paradigms to healthcare services. New scenarios are possible to be imagined. According to the vision described in [Ren05], biodegradable nano-physiological wireless sensors will be able to move through the bloodstream for monitoring physiological changes. According to the current e-health WSN state-of-art, it is predictable that a long and tough way has still to be overcome until this futuristic scenario becomes reality.

Using a more realistic scenario and motivated with the possibility of contributing to the advancement in wireless healthcare services, the present work has proposed a MAC protocol for e-emergency WSNs. In this way, the author believes that a few steps have been given forward towards the ultimate goal of providing a pervasive and reliable assistance to patients with health risk abnormalities.

Appendix A

List of Papers

A list of publications that reflects the results achieved during the development of the research work is presented next.

1. Óscar Gama, Celso Figueiredo, Paulo Carvalho, P. M. Mendes, "Towards a Reconfigurable Wireless Sensor Network for Biomedical Applications", 1st International Conference on Sensor Technologies and Applications (SensorComm´07), Valencia, Spain, October 2007.

2. Óscar Gama, Paulo Carvalho, J. A. Afonso, P. M. Mendes, "Wireless Sensor Networks with QoS for e-Health and e-Emergency Applications", 2th Workshop on e-Health Systems and Technology (EHST´08), Oporto, Portugal, July 2008.

3. Óscar Gama, Paulo Carvalho, J. A. Afonso, P. M. Mendes, "Quality of Service Support in Wireless Sensor Networks for Emergency Healthcare Services", 30th IEEE Engineering in Medicine and Biology Conference (EMBC), Vancouver, Canada, August 2008.

4. Óscar Gama, Paulo Carvalho, J. A. Afonso, P. M. Mendes, "Quality of Service in Wireless e-Emergency: Main Issues and a Case-study", 3th Symposium of Ubiquitous Computing and Ambient Intelligence (UCAmI'08). Salamanca, Espanha, October 2008.

5. Oscar Gama, Paulo Carvalho, J. A. Afonso, P. M. Mendes, "An Improved MAC Protocol with a Reconfiguration Scheme for Wireless e-Health Systems Requiring Quality of Service", 1st Wireless Vitae´09, Aalborg, Danmark, May 2009.

6. Óscar Gama, Paulo Carvalho, J. A. Afonso, P. M. Mendes, "Trade-off Analysis of a MAC Protocol for Wireless e-Emergency Systems", S-CUBE´09, Pisa, Italy, September 2009.

7. Óscar Gama , H. Martins , C. Pereira , S. Soares , A. Valente , V. S. Ribeiro , P. Carvalho, P. M. Mendes, "A Platform with Combined Environmental and Physiological Wireless Data Acquisition for AAL Applications", International Symposium on Ambient Intelligence (IASmI), Guimarães, Portugal, June 2010.

8. C. P. Figueiredo, Óscar Gama, S. Silva, Carlos Pereira, P. M. Mendes, L. Domingues, K.-P. Hoffmann, "Autonomy Suitability of Wireless Modules for Ambient Assisted Living Applications:WiFi, Zigbee, and Proprietary Devices", 4th International Conference on Sensor Technologies and Applications (SensorComm'10), Venice, Italy, July 2010.

9. Óscar Gama, Paulo Carvalho, P. M. Mendes, "Time-slot Scheduling Algorithm for e-Health Wireless Sensor Networks", 12th IEEE International Conference on e-Health Networking, Application and Services (Healthcomm'10), Lyon, France, Jul. 2010.

10. Óscar Gama, Paulo Carvalho, P. M. Mendes, "Modelling the Impact of Software Components on Wireless Sensor Network Performance", 1st Portuguese Conference on Sensor Networks, Coimbra, Portugal, March 2011.

11. Óscar Gama, Paulo Carvalho, P. M. Mendes, "A Model to Improve the Accuracy of WSN Simulations", 9th International Conference on Wired/Wireless Internet Communications, Vilanova i la Geltru , Spain, June 2011.

12. Paulo M. Mendes, Celso P. Figueiredo, Mariana S. Fernandes, Óscar S. Gama, "Springer Handbook of Medical Technology", Part G, Electronics in medicine, 2011.

Bibliography

[Abramson70] N. Abramson, "The ALOHA system, another alternative for computer communications", Fall Joint Computer Communications - AFIPS Conf., Montvale, Nov. 1970.

[ACSS08] "Administração Central do Sistema de Saúde (ACSS) - Documento de trabalho Abril 2008 - Requisitos técnicos essenciais", pp. 31 & 34, 2008. http://www.acss.min-saude.pt/.

[Afonso06] J.A. Afonso, L.A. Rocha, H.R. Silva, J.H. Correia, "MAC Protocol for Low-Power Real-Time Wireless Sensing and Actuation", in Proceedings of 11th IEEE Conference on Electronics, Circuits and Systems, Nice, France, Dec. 2006.

[Alemdar10] H. Alemdar, C. Ersoy, "Wireless Sensor Networks for Healthcare: a Survey", Elsevier, Journal of Computer Networks 54: 2688–2710, 2010.

[Anliker04] U. Anliker, J. Ward, P. Lukowicz, G. Tröster, F. Dolveck, M. Baer, F. Keita, E. Schenker, F. Catarsi, L. Coluccini, A. Belardinelli, D. Shklarski, M. Alon, E. Hirt, R. Schmid, M. Vuskovic, "AMON: A Wearable Multi-Parameter Medical Monitoring and Alert System", IEEE Transaction on Information Technology in Biomedicine, vol. 8, no. 4, Dec. 2004.

[Arampatzis05] T. Arampatzis, J. Lygeros, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", in Proceedings of 13th Mediterranean Conference on Control and Automation, Limassol, Limassol, Cyprus, Jun. 2005.

[Arnon03] S. Arnon, D. Bhastekar, D. Kedar, A. Taubar, "A Comparative Study of Wireless Communication Network Configurations for Medical Applications", IEEE Wireless Communication, vol. 10(1), Feb., 2003.

[Astaras08] A. Astaras, M. Arvanitidou, I. Chouvarda, V. Kilintzis, V. Koutkias, E. Montón, G. Stalidis, A. Triantafyllidis, N. Maglaveras, "An integrated biomedical telemetry system for sleep monitoring employing a portable body area network of sensors (SENSATION)", 30th Conf. IEEE Engineering in Medicine and Biology Society, Vancouver, Canada, Aug. 2008.

[Bachir10] A. Bachir, M. Dohler, T. Watteyne, K. Leung, "MAC Essentials for Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, 12(2): 222–248, 2010.

[Banks96] J. Banks, J. Carson, B. Nelson, "Discrete-Event System Simulation", 2nd edition, Prentice Hall, 1996.

[Barth08] A. Barth, S. Wilson, M. Hanson, H. Powell, D. Unluer, J. Lach, "Body-Coupled Communication for Body Sensor Networks", 3rd International Conference on Body Area Networks, Tempe, Arizona, 2008.

[Batra11] A. Batra, A. Xhafa, "An Overview of IEEE 802.15.6", in Berkeley Wireless Research Center (BWRC) Sensor Workshop, Jun. 2011.

[Bergamini10] L. Bergamini, C. Crociani, A. Vitaletti, M. Nati, "Validation of WSN Simulators through a Comparison with a Real Testbed", in 7th ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks, Bodrum, Turkey, Oct. 2010.

[Bhatnagar01] S. Bhatnagar, B. Deb, B. Nath, "Service Differentiation in Sensor Networks", in Proc. of 4th Symposium on Wireless Personal Multimedia Communications, Sep. 2001.

[Bonfiglio11] A. Bonfiglio, D. Rossi, "Wearable Monitoring Systems", Springer Science+Business Media, 2011.

[Boulis09] A. Boulis, "A simulator for Wireless Sensor Networks and Body Area Networks, Version 2.3, User's Manual", Oct. 2009. Available at: http://castalia.npc.nicta.com.au.

[Braem07] B. Braem, B. Latré, I. Moerman, C. Blondia, E. Reusens, W. Joseph, L. Martens, P. Demeester, "The Need for Cooperation and Relaying in Short-Range High Path Loss Sensor Networks", 1st Conf. on Sensor Technologies and Applications, Valencia, Spain, Oct. 2007.

[Bulusu01] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, "Scalable Coordination for Wireless Sensor Networks: Self-Configuring Localization Systems," 6th International Symposium on Communication Theory and Applications, Ambleside, England, Jul. 2001.

[Buren06] T. Buren, P. Mitcheson, T. Green, E. Yeatman, A. Holmes, G. Troster, "Optimization of Inertial Micropower Generators for Human Walking Motion", IEEE Sensors Journal, 6(1), 28–38, 2006.

[Caccamo02] M. Caccamo, L. Zhang, L. Sha, G. Buttazzo, "An Implicit Prioritized Access Protocol for Wireless Sensor Networks", in 23rd IEEE Real-Time Systems Symp., Dec. 2002.

[Cavalcanti07] D. Cavalcanti, R. Schmitt., A. Soomro, "Performance Analysis of 802.15.4 and 802.11e for Body Sensor Network Applications", in 4th Inter. Workshop on Wearable and Implantable Body Sensor Networks, Aachen, Germany, Mar. 2007.

[Cavin02] D. Cavin, Y. Sasson, A. Schiper, "On the Accuracy of MANET Simulators", Proc. 2th International Workshop on Principles of Mobile Computing, Toulouse, France, Oct. 2002.

[Chen11] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, V. Leung, "Body Area Networks: A Survey", ACM/Springer Mobile Networks and Applications, 16(2): 171–193, Apr. 2011.

[Chevrollier05] N. Chevrollier, N. Golmie, "On the Use of Wireless Network Technologies in Healthcare Environments", in Proc. 5th IEEE Workshop on Applications and Services in Wireless Networks, Paris, France, Jun. 2005.

[Chung07] W. Chung, C. Yau, K. Shin, "A Cell Phone based Health Monitoring System with Self Analysis Processor using Wireless Sensor Network Technology", 29th Conference of IEEE Engineering in Medicine and Biology Society (EMBS), Lyon, France, Aug. 2007.

[Colesanti07] U. Colesanti, C. Crociani, A. Vitaletti, "On the Accuracy of OMNET++ in the Wireless Sensor Networks Domain: Simulation vs. Testbed", in Proc. of the 4th ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks, Chania, Crete Island, Greece, Oct. 2007.

[Cova09] Cova Gabriel, Xiong Huagang, Gao Qiang, Guerrero Esteban, Ricardo Ricardo, Estevez Jose, "A Perspective of State-of-the-Art Wireless Technologies for E-Health Applications", in Proc. of. Inter. Symposium on Information Technologies and Education, Ji'nan, China, Aug. 2009.

[Cui05] S. Cui, R. Madan, A. Goldsmith, S. Lall, "Energy-Delay Tradeoffs for Data Collection in TDMA-based Sensor Networks", in 40th Annual IEEE International Conference on Communications, Seoul, Korea, May 2005.

[Cui05a] S. Cui, A. Goldsmith, and A. Bahai, “Energy-constrained Modulation Optimization”, IEEE Transactions on Wireless Communications, 4 : 2349–2360, Sep. 2005.

[Curtis08] D. Curtis, E. Shih, J. Waterman, J. Guttag, J. Bailey, T. Stair, R. Greenes, L. Ohno-Machado, “Physiological Signal Monitoring in the Waiting Areas of an Emergency Room”, in Proceedings of 3rd International Conference on Body Area Networks, Tempe, Arizona, USA, Mar. 2008.

[Cypher06] D. Cypher, N. Chevrollier, N. Montavont, N. Golmie, “Prevailing over Wires in Healthcare Environments: Benefits and Challenges”, IEEE Communications Magazine, 44(4): 56–63, 2006.

[Dam03] T. Dam, K. Langendoen, "An Adaptive Energy-efficient MAC Protocol for Wireless Sensor Networks", in Proceedings of the 1st ACM International Conference on Embedded Networked Sensor Systems (SenSys), Los Angeles, U.S.A., Nov. 2003.

[Demirkol06] I. Demirkol, C. Ersoy, F. Alagoz, “MAC Protocols for Wireless Sensor Networks: a Survey”, IEEE Communications Magazine, 44(4): 115–121, 2006.

[Downard04] I. Downard, “Simulating Sensor Networks in NS-2”, Technical Report NRL/FR/5522–04–10073, Naval Research Laboratory, Washington, U.S.A., May 2004.

[Dunkels04] A. Dunkels, B. Grönvall, and T. Voigt, “Contiki – a Lightweight and Flexible Operating System for Tiny Networked Sensors”. In Proceedings of the 1st IEEE Workshop on Embedded Networked Sensors, Tampa, Florida, USA, Nov. 2004.

[e-Book11] P. Mendes, C. Figueiredo, M. Fernandes, O. Gama, “Springer Handbook of Medical Technology”, Part G, Electronics in Medicine, 2011.

[Egea-López08] E. Egea-López, J. Vales-Alonso, A. Martínez-Sala, J. García-Haro, P. Pavón-Mariño, M. Delgado, “A Wireless Sensor Networks MAC Protocol for Real-Time Applications”, Journal of Personal and Ubiquitous Computing, 12(2), Feb. 2008.

[El-Hoiydi04] A. El-Hoiydi, J. Decotignie, J. Hernandez. “Low Power MAC Protocols for Infrastructure Wireless Sensor Networks”, in Proceedings of the 5th European Wireless Conference, Barcelona, Spain, Feb. 2004.

[Ergen05] S. Ergen, P. Varaiya, “TDMA Scheduling Algorithms for Sensor Networks”, Technical Report, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Jul. 2005.

[Ergen06] S. Ergen, P. Varaiya, “PEDAMACS: Power Efficient and Delay Aware Medium Access Protocol for Sensor Networks”, IEEE Transactions on Mobile Computing, 5(7): 920–930, Jul. 2006.

[Espina06] J. Espina, T. Falck, J. Muehlsteff, X. Aubert, “Wireless Body Sensor Network for Continuous Cuff-less Blood Pressure Monitoring”, in Proc. of the 3rd IEEE/EMBS International Summer School and Symposium on Medical Devices and Biosensors, Cambridge, Massachusetts, U.S.A., Sep. 2006.

[Eysenbach01] G. Eysenbach, “What is e-health?”, Journal of Medical Internet Research, 3(2), Apr–Jun, 2001.

[Falck06] T. Falck, J. Espina, J. Ebert, D. Dietterle, "BASUMA—The Sixth Sense for Chronically Ill Patients". In International Workshop on Wearable and Implantable Body Sensor Networks, Cambridge, Massachusetts, U.S.A., Apr. 2006.

[Falck07] T. Falck, H. Baldus, J. Espina, K. Klabunde, "Plug 'n play simplicity for wireless medical body sensors", ACM/Springer Mobile Networks and Applications, 12(2): 143–153, 2007.

[Farella08] E. Farella, A. Pieracci, L. Benini, L. Rocchi, A. Acquaviva, "Interfacing human and computer with wireless body area sensor networks: the WiMoCA solution", Multimedia Tools and Applications 38(3): 337–363, 2008.

[Farshchi07] S. Farshchi, A. Pesterev, P. H. Nuyujukian, I. Mody, J. Judy, "Bi-Fi: An Embedded Sensor/System Architecture for Remote Biological Monitoring," IEEE Transactions on Information Technology in Biomedicine, 11(6), Nov. 2007.

[Figueiredo10] C. Figueiredo, O. Gama, S. Silva, C. Pereira, P. Mendes, L. Domingues, K. Hoffmann, "Autonomy Suitability of Wireless Modules for Ambient Assisted Living Applications: WiFi, Zigbee, and Proprietary Devices", 4th International Conference on Sensor Technologies and Applications, Venice, Italy, 2010.

[Firoze07] A. Firoze, L. Ju, L. Kwong, "PR-MAC a Priority Reservation MAC Protocol for Wireless Sensor Networks", in Proceedings of 2nd International Conference on Electrical Engineering, Coimbra, Portugal, Nov. 2007.

[Fort06] A. Fort, J. Ryckaert, C. Desset, P. Doncker, P. Wambacq, L. Biesen, "Ultra-Wideband Channel Model for Communication around the Human Body", IEEE Journal on Selected Areas in Communications, 24: 927–933, 2006.

[Gama08] O. Gama, P. Carvalho, J. Afonso, P. Mendes, "Wireless Sensor Networks with QoS for e-Health and e-Emergency Applications", 2th e-Health Systems and Technology, Oporto, Portugal, Jul. 2008.

[Gama09] O. Gama, P. Carvalho, J. Afonso, P. Mendes, "An Improved MAC Protocol with a Reconfiguration Scheme for Wireless e-Health Systems Requiring Quality of Service", 1st Wireless Vitae, Aalborg, Danmark, May 2009.

[Gama09a] O. Gama, P. Carvalho, J. Afonso, P. Mendes, "Trade-off Analysis of a MAC Protocol for Wireless e-Emergency Systems", 1st Inter. Conf. S-CUBE, Pisa, Italy, Sep. 2009.

[Gama10] O. Gama , H. Martins , C. Pereira , S. Soares , A. Valente , V. Ribeiro , P. Carvalho, P. Mendes, "A Platform with Combined Environmental and Physiological Wireless Data Acquisition for AAL Applications", International Symposium on Ambient Intelligence (IASmI), Guimarães, Portugal, Jun. 2010.

[Gama10a] O Gama, P. Carvalho, P. Mendes, "Time-slot Scheduling Algorithm for e-Health Wireless Sensor Networks", 12th IEEE International Conf. on e-Health Networking, Application and Services (Healthcomm), Lyon, France, Jul. 2010.

[Gama11] O. Gama, P. Carvalho, P. Mendes, "Modelling the Impact of Software Components on Wireless Sensor Network Performance", 1st Portuguese Conference on Wireless Sensor Networks, Coimbra, Portugal, Mar. 2011.

[Gama11a] O. Gama, P. Carvalho, P. Mendes, "A Model to Improve the Accuracy of WSN Simulations", 9th International Conference on Wired/Wireless Internet Communications, Vilanova i la Geltru , Spain, Jun. 2011.

[Gandham05] S. Gandham, M. Dawande, R. Prakash, "Link scheduling in sensor networks: Distributed edge coloring revisited", in Proc. of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, U.S.A., Mar. 2005.

[Gao05] T. Gao, L. Hauenstein, A. Alm, D. Crawford, C. Sims, A. Husain, D. White, "Vital Signs Monitoring and Patient Tracking Over a Wireless Network", Proc. of the 27th Annual Inter. Conf. of the IEEE Engineering in Medicine and Biology Society (EMBS), Shanghai, China, Sep. 2005.

[Gao07] T. Gao, T. Massey, L. Selavo, D. Crawford, B. Chen, K. Lorincz, V. Shnayder, L. Hauenstein, F. Dabiri, J. Jeng, A. Chanmugam, D. White, M. Sarrafzadeh, M. Welsh, "The Advanced Health and Disaster Aid Network: a Lightweight Wireless Medical System for Triage", IEEE Transactions on Biomedical Circuits and Systems, 1(3): 203–216, 2007.

[Gast02] M. Gast, "802.11 Wireless Networks: The Definitive Guide", O'Reilly, Apr. 2002.

[Gharpurey08] R. Gharpurey, P. Kinget, "Ultra Wideband: Circuits, Transceivers and Systems", Springer Book, New York, U.S.A., 2008.

[Ginseng08] http://www.ict-ginseng.eu.

[Glossbrenner99] K. Glossbrenner, Internet Protocol Data Communication Service - IP Packet Transfer and Availability Performance Parameters. ITU-T Recommendation I.380; 1999.

[Golmie05] N. Golmie, D. Cypher, O. Rebala, "Performance Analysis of Low Rate Wireless Technologies for Medical Applications", in Computer Communications", 28(10): 1266–1275, Jun. 2005.

[Guo01] C. Guo, L. Zhong, J. Rabaey, "Low Power Distributed MAC for Ad Hoc Sensor Radio Networks", IEEE Global Telecommunications Conf., San Antonio, U.S.A., Nov. 2001.

[Gyselinckx06] B. Gyselinckx, R. Vullers, C. Hoof, J. Ryckaert, R. Yazicioglu, P. Fiorini, V. Leonov, "Human++: Emerging Technology for Body Area Networks", in Proc. of International Conference on Very Large Scale Integration, Nice, France, Oct. 2006.

[Halkes07] G. Halkes, K. Langendoen, "Crankshaft: An Energy-Efficient MAC-Protocol for Dense Wireless Sensor Networks", in Proceedings of the 4th European Conference on Wireless Sensor Networks, Delft, Holland, Jan. 2007.

[Halteren04] A. Halteren, R. Bults, K. Wac, D. Konstantas, I. Widya, N. Dokovski, G. Koprinkov, V. Jones, R. Herzog, "Mobile patient monitoring: The MobiHealth system" The Journal on Information Technology in Healthcare, 2(5): 365–373, Oct. 2004.

[Hanson09] M. Hanson, H. Powell, A. Barth, K. Ringgenberg, B. Calhoun, J. Aylor, J. Lach, "Body Area Sensor Networks: Challenges and Opportunities", IEEE Computer, 42(1): 58–65, Jan. 2009.

[Hao08] Y. Hao, R. Foster, "Wireless body sensor networks for health monitoring applications," Physiological Measurement, 29(11): R27–R56, Nov. 2008.

[Henrion04] S. Henrion, C. Mailhes, F. Castanié, "Transmitting Critical Biomedical Signals over Unreliable Connexionless Channels with good QoS using Advanced Signal Processing", in Proc. of 8th WSEAS International Conf. on Communications, Vouliagmeni, Greece, Jul. 2004.

[Hoesel04] L. Hoesel, P. Havinga, "A Lightweight Medium Access Protocol (LMAC) for Wireless Sensor Networks", in Proceedings of the 1st International Conference on Networked Sensing Systems, Tokyo, Japan, Jun. 2004.

[Hussain10] M. Hussain, N. Alam, S. Ullah, N. Ullah, K. Kwak, "TDMA Based Directional MAC for BSN", in 6th Conf. on Networked Computing, Gyeongju, South Korea, May 2010.

[IEEE1] IEEE 802.15.1-2005, "Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)", 2005.

[IEEE4] IEEE 802.15.4-2003, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks", 2003.

[IEEE6] IEEE P802.15.6/D01, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs) Used in or around a Body", May 2010.

[Imran10] M. Imran, A. Said, H. Hasbullah, "A Survey of Simulators, Emulators and Testbeds for Wireless Sensor Networks," in Proceedings of International Symposium on Information Technology, Kuala Lumpur, Malaysia, Jun. 2010.

[IPPM-WG] IETF IPPM-WG. IP Performance Measurements Working Group. Available at: http:/www.ietf.org/html.charters/ippm-charter.html.

[Ivanov07] S. Ivanov, A. Herms, G. Lukas, "Experimental Validation of the NS-2 Wireless Model using Simulation, Emulation, and Real Network", in Proc. of 4th Workshop on Mobile Ad-Hoc Networks, Bern, Switzerland, Feb. 2007.

[Jeong10] J. Jeong, J. Kim, W. Cha, H. Kim, S. Kim, P. Mah, "A QoS-aware data aggregation in wireless sensor networks", in the 12th International Conference on Advanced Communication Technology, vol. 1, Gangwon-Do, South Korea, Feb. 2010.

[Jiang08] S. Jiang, Y. Cao, S. Lyengar, P. Kuryloski, R. Jafari, Y. Xue, R. Bajcsy, S. Wicker, "CareNet: an Integrated Wireless Sensor Networking Environment for Remote Healthcare", in Proc. of 3rd International Conference on Body Area Networks. Tempe, Arizona, Mar. 2008.

[Jones01] V. Jones, R. Bults, D. Konstantas, P. Vierhout, "Healthcare PANs: Personal Area Networks for Trauma Care and Home Care", in Proceedings of 4th Inter. Symposium on Wireless Personal Multimedia Communications, Aalborg, Denmark, Sep. 2001.

[Keller09] M. Keller, J. Beutel, A. Meier, R. Lim, L. Thiele, "Learning from Sensor Network Data", in Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, Berkeley, California, U.S.A., Nov. 2009.

[Kim07] E. Kim, M. Kim, S. Youm, S. Choi, C. Kang, "Priority-based Service Differentiation Scheme for IEEE 802.15.4 Sensor Networks", AEÜ – International Journal of Electronics and Communications, 61(2), 2007.

[Kim08] J. Kim, J. Lim, C. Pelczar, B. Jang, "RRMAC: A Sensor Network MAC for Real-time and Reliable Packet Transmission", Proceedings of International Symposium Consumer Electronics, Vilamoura, Portugal, Apr.2008.

[Ko08] J. Ko, R. Musaloiu, T Gao, L. Selavo, J Lim, Y. Chen, A. Terzis, W. Destler, "Demo Abstract: MEDiSN: Medical Emergency Detection in Sensor Networks", in Proc. of 6th ACM Conference on Embedded Networked Sensor Systems, Raleigh, North Carolina, U.S.A., 2008.

[Ko10] J. Ko, C. Lu, M. Srivastava, J. Stankovic, "Wireless Sensor Networks for Healthcare", Proceedings of the IEEE Special Issue on Sensor Network Applications, 98(11), Nov. 2010.

[Kohvakka06] M. Kohvakka, M. Kuorilehto, M. Hannikainen, T. Hamalainen, "Performance Analysis of IEEE 802.15.4 and ZigBee for Large-Scale Wireless Sensor Network Applications", in Proc. of 3rd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, Torremolinos, Spain, Oct. 2006.

[Köpke08] A. Köpke, M. Swigulski, P. Haneveld, H. Lichte, S. Valentin, K. Wessel, D. Willkomm, T. Parker, O. Visser, "Simulating wireless and mobile networks in OMNeT++ the MiXiM vision", In Proc. of the 1st Intern. OMNeT++ Workshop, Marseille, France, Mar. 2008.

[Korkalainen09] M. Korkalainen, M. Sallinen, N. Kärkkäinen, P. Tukeva, "Survey of Wireless Sensor Networks Simulation Tools for Demanding Applications", in Proc. of the 5th Inter. Conf. on Networking and Services, Valencia, Spain, Apr. 2009.

[Kotz04] D. Kotz, C. Newport, R. Gray, J. Liu, Y. Yuan, C. Elliott, "Experimental Evaluation of Wireless Simulation Assumptions", in Proc. of the 7th ACM/IEEE Inter. Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Venice, Italy, Oct. 2004.

[Krames02] E. Krames, "Implantable Devices for Pain Control: Spinal Cord Stimulation and Intrathecal Therapies", Best Practice & Research Clinical Anaesthesiology, 16(4): 619–649, 2002.

[Krishnamachari02] L. Krishnamachari, D. Estrin, S. Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks", in Proceedings of the 22nd Inter. Conf. on Distributed Computing Systems Workshops, Vienna, Austria, Jul. 2002.

[Kumar08] S. Kumar, K. Kambhatla, F. Hu, M. Lifson, Y. Xiao, "Ubiquitous Computing for Remote Cardiac Patient Monitoring: A Survey", International Journal of Telemedicine and Applications, (2008), 2008.

[Kurkowski05] S. Kurkowski, T. Camp, M. Colagrosso, "MANET Simulation Studies: the Incredibles", ACM Mobile Computing and Communications Review, 9(4):50–61, 2005.

[Kwak10] K. S. Kwak, S. Ulah and Niamat U. "An Overview of IEEE 802.15.6 Standard", 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies, Rome, Italy, Nov. 2010.

[Kyriacou03] E. Kyriacou, S. Pavlopoulos, A. Berler, M. Neophytou, A. Bourka, A. Georgoulas, A. Anagnostaki, D. Karayiannis, C. Schizas, C. Pattichis, A. Andreou, D. Koutsouris, "Multi-purpose HealthCare Telemedicine Systems with Mobile Communication Link Support", BioMedical Engineering OnLine", 2(7), Mar. 2003.

[Kyriacou07] E. Kyriacou, M. PattichiS, C. Pattichis, A. Panayides, A. Pitsillides, "m-Health e-Emergency Systems: Current Status and Future Directions", IEEE Antennas and Propagation Magazine, 49(1), Feb. 2007.

[Latré07] B. Latré, B. Braem, I. Moerman, C. Blondia, E. Reusens, W. Joseph, P. Demeester, "A Low-delay Protocol for Multihop Wireless Body Area Networks", in Proc. 4th Annual Conf. on Mobile Ubiquitous Systems Networks and Services, Philadelphia, U.S.A., Aug. 2007.

[Latré11] Benoît Latré, Bart Braem, Ingrid Moerman, Chris Blondia, Piet Demeester, "A Survey on Wireless Body Area Networks", in Wireless Networks, 17: 1–18, Springer Netherlands, 2011.

[Lee08] E. Lee, N. Kim, N. Trang, J. Hong, E. Cha, T. Lee, "Respiratory Rate Detection Algorithms by Photoplethysmography Signal Processing", in Proceedings of the 30th Annual International IEEE EMBS Conference, Vancouver, Canada, Aug. 2008.

[Levis03] P. Levis, N. Lee, M. Welsh, D. Culler, "TOSSIM: Accurate and Scalable Simulation of entire TinyOS Applications", in Proc. International Conference on Embedded Networked Sensor Systems, Los Angeles, California, U.S.A., Nov. 2003.

[Li05] H. Li, P. Shenoy, K. Ramamritham, "Scheduling Messages with Deadlines in Multi-Hop Real-Time Sensor Networks", in Proc. of 11th IEEE Real-time and Embedded Technology and Applications Symposium, San Francisco, U.S.A., Mar. 2005.

[Li07] H. Li, J. Tan, "Medium Access Control for Body Sensor Networks", in Proceedings of the 16th International Conference on Computer Communications and Networks, Honolulu, Hawaii, U.S.A., Aug. 2007.

[Liang07] X. Liang, I. Balasingham, "Performance Analysis of the IEEE 802.15.4 based ECG Monitoring Network", Proc. of 7th IASTED Conferences on Wireless and Optical Communications, Montreal, Canada, May 2007.

[Liolios10] C. Liolios, "An Overview of Body Sensor Networks in Enabling Pervasive Healthcare and Assistive Environments", in 3rd International Conference on Pervasive Technologies for Assistive Environment, Samos, Greece, 2010.

[Liu04] J. Liu, Y. Yuan, D. Nicol, R. Gray, C. Newport, D. Kotz, L. Perrone, "Simulation Validation using Direct Execution of Wireless Ad-hoc Routing Protocols", in Proceedings of 18th Parallel and Distributed Simulation Workshop, Kufstein, Austria, May 2004.

[Liu05] Y. Liu, I. Elhanany, H. Qi, "An Energy-efficient QoS-aware Media Access Control Protocol for Wireless Sensor Networks, in IEEE International Conference on Mobile Ad hoc and Sensor Systems, Washington, U.S.A., Nov. 2005.

[Liu06] Z. Liu, I. Elhanany, "RL-MAC: A QoS-aware Reinforcement Learning based MAC Protocol for Wireless Sensor Networks", in Proc. of IEEE Inter. Conference on Networking, Sensing and Control, Ft. Lauderdale, Florida, U.S.A., 2006.

[Mao07] J. Mao, Z. Wu, X. Wu, "A TDMA Scheduling Scheme for Many-to-One Communications in Wireless Sensor Networks", in Journal of Computer Communications, 30(4): 863–872, Feb. 2007.

[Montón08] E. Montón, J. Hernandez, J. Blasco, T. Hervé , J. Micallef, I. Grech, A. Brincat, V. Traver, "Body Area Network for Wireless Patient Monitoring", Telemedicine and E-Health Communication Systems, 2(2): 215–222, 2008.

[Mundt05] C. Mundt, K. Montgomery, U. Udoh, V. Barker, G. Thonier, A. Tellier, R. Ricks, R. Darling, Y. Cagle, N. Cabrol, S. Ruoss, J. Swain, J. Hines, G. Kovacs, "A Multiparameter Wearable Physiological Monitoring System for Space and Terrestrial Applications", IEEE Transactions on Information Technology in Biomedicine, 9(3):382–391, Sep. 2005.

[Ng04] J. Ng, B. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, G. Yang, "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)", Proc. of Conf. on Ubiquitous Computing, Nottingham, England, Sep. 2004.

[Nguyen06] K. Nguyen, T. Nguyen, C. Chaing, M. Motani, "A Prioritized MAC Protocol for Multi-hop, Event-driven Wireless Sensor Networks", in Proc. of 1st Inter. Conf. on Communications and Electronics, Hanoi, Vietnam, Oct. 2006.

[Nunes07] M. Nunes, A. Grilo, M. Macedo, "Interference-Free TDMA Slot Allocation in Wireless Sensor Networks", in: Proceedings of the 32nd IEEE Conference on Local Computer Networks, Dublin, Ireland, Oct. 2007.

[Oh05] H. Oh, C. Rizo, M. Enkin, A. Jadad, "What is eHealth (3): a Systematic Review of Published Definitions", Journal of Medical Internet Research, 7(1), Jan.–Mar., 2005.

[Österlind06] F. Österlind, A. Dunkels, J. Eriksson, N. Finne, T. Voigt, "Cross-Level Sensor Network Simulation with COOJA". In Proc. of 1st IEEE Workshop on Practical Issues in Building Sensor Network Applications, Tampa, Florida, U.S.A., Nov. 2006.

[Paksuniemi05] M. Paksuniemi, H. Sorvoja, E. Alasaarela, R. Myllylä, "Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit", Proceedings of 27th Annual International Conference of IEEE Engineering in Medicine and Biology, Shanghai, China, Sep. 2005.

[Pantazis08] N. Pantazis, D. Vergados, N. Miridakis, D. Vergados, "Power Control Schemes in Wireless Sensor Networks for Homecare e-Health Applications", in Proc. of 1st International Conference on Pervasive Technologies for Assistive Environment, Athens, Greece, Jul. 2008.

[Pantelopoulos09] A. Pantelopoulos, N. Bourbakis, "A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis", IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews, 40(1), Jan. 2010.

[Paradiso05] J. Paradiso, T. Starner, "Energy scavenging for mobile and wireless electronics", IEEE Pervasive Computing, 4(1):18–27, 2005.

[Park00] S. Park, A. Savvides, M. Srivastava, "SensorSim: A Simulation Framework for Sensor Networks." In Proc. ACM Modeling, Analysis and Simulation of Wireles and Mobile Systems, Boston, U.S.A., August 2000.

[Park03] S. Park, S. Jayaraman, "Enhancing the Quality of Life through Wearable Technology", IEEE Engineering in Medicine and Biology Magazine, 22(3):41–48, 2003.

[Pattichis06] C. Pattichis, E. Kyriacou, M. Pattichis, A. Panayides, A. Pitsillides, "A Review of m-Health e-Emergency Systems", in Proc. of the International Special Topic Conference on Information Technology in Biomedicine, Ioannina, Greece, Oct. 2006.

[Pediaditakis10] D. Pediaditakis, Y. Tselishchev, A. Boulis, "Performance and Scalability Evaluation of the Castalia Wireless Sensor Network Simulator", 3rd Inter. Conference on Simulation Tools and Techniques, Torremolinos, Spain, 2010.

[Pentland04] A. Pentland, “Healthwear: Medical Technology Becomes Wearable”, in IEEE Computer, vol. 37, nr. 5, May 2004.

[Perillo05] A. Perillo, W. Heinzelman, “Wireless Sensor Network Protocols”, in Fundamental Algorithms and Protocol for Wireless and Mobile Networks”, CRC Hall 2005.

[Perrone02] F. Perrone, D. Nicol, “A scalable simulator for TinyOS applications”, In Proceedings of the Winter Simulation Conference, San Diego, California, U.S.A., 2002.

[Pham07] H. Pham, D. Pediaditakis, A. Boulis, “From Simulation to Real Deployments in WSN and Back”, In Proc. of 8th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Helsinki, Finland, Jun. 2007.

[Pister08] K. Pister, L Doherty, “TSMP: Time Synchronized Mesh Protocol”, Proc. of Inter. Symposium Distributed Sensor Networks, Orlando, Florida, U.S.A., Nov. 2008.

[Polastre04] J. Polastre, J. Hill, D. Culler, “Versatile low power media access for wireless sensor networks”, in 2nd ACM Conf. on Embedded Networked Sensor Systems (SenSys), Baltimore, Maryland, U.S.A., Nov. 2004.

[Prokkola06] J. Prokkola, “OPNET – Network simulator”, VTT Technical Research Center of Finland, 2006.

[Rappaport96] T. Rappaport, “Wireless Communications: Principles and Practice”, Prentice Hall, 1996.

[Ray11] S. Ray, ,S. Dash, N. Tarasia, A. Ajay, A. Swain, “Energy Efficient Token Based MAC Protocol for Wireless Sensor Networks”, International Journal of Computer Science and Information Technologies, 2(2): 747–753, 2011.

[Ren05] H. Ren, M. Meng, X. Chen, “Physiological Information Acquisition through Wireless Biomedical Sensor Networks,” Proc. of IEEE Inter. Conf. on Information Acquisition, Macau, China, Jun. 2005.

[Reusens09] E. Reusens, W. Joseph, G. Vermeeren, L. Martens, B. Braem, C. Blondiam, B. Latré, I. Moerman, “Characterization of on-body communication channel and energy efficient topology design for wireless body area networks,” IEEE Transactions on Information Technology in Biomedicine, 13(6): 933-945, Nov 2009.

[RFsafety99] “IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz”, 1999.

[Rhee05] I. Rhee, A. Warrier, M. Aia, J. Min, “Z-MAC: a Hybrid MAC for Wireless Sensor Networks”, in 3rd ACM Conference on Embedded Networked Sensor Systems (SenSys 2005), San Diego, U.S.A., Nov. 2005.

[Roelens06] L. Roelens, S. Bulcke, W. Joseph, G. Vermeeren, L. Martens, “Path loss model for wireless narrowband communication above flat phantom”, Electronics Letters, 42(1): 10–11, 2006.

[Saxena08] N. Saxena, A. Roy, J. Shin, “Dynamic duty cycle and adaptive contention window based QoS-MAC protocol for wireless multimedia sensor networks”, Computer Networks 52 (13): 2532–2542, 2008.

[Shastry05] N. Shastry, J. Bhatia, R. Adve, “A Theoretical Analysis of Cooperative Diversity in Wireless Sensor Networks”, in Proc. of IEEE Global Telecommunications Conference, St. Louis, Missouri, U.S.A., Nov. 2005.

[Shih01] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, A. Chandrakasan, “Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks”, in Proc. of the ACM 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, Jul. 2001.

[Shin07] S. Shin, H. Park, W. Kwon, “Mutual Interference Analysis of IEEE 802.15.4 and IEEE 802.11b”, Computer Networks: The International Journal of Computer and Telecommunications Networking, 51: 3338-3353, Aug. 2007.

[Shnayder05] V. Shnayder, B. Chen, K. Lorincz, T. Fulford-Jones, M. Welsh, “Sensor Networks for Medical Care”, in 3rd International ACM Conference on Embedded Networked Sensor Systems (SenSys), San Diego, California, U.S.A., Nov. 2005.

[Singh08] C. Singh, O. Vyas, M. Tiwari, “A Survey of Simulation in Sensor Networks”, in Proceedings of the IEEE Conference on Computational Intelligence For Modelling Control & Automation, Washington, U.S.A., Dec. 2008.

[Sobeih05] A. Sobeih, J. Hou, L. Kung, N. Li, H. Zhang, W. Chen, H. Tyan; H. Lim, “J-Sim: a Simulation and Emulation Environment for Wireless Sensor Networks”, IEEE Wireless Communications, 13(4): 104-119, Aug. 2006.

[Sridharan04] A. Sridharan, B. Krishnamachari, “Max-min Fair Collision-Free Scheduling for Wireless Sensor Networks”, IEEE Workshop on Multihop Wireless Networks, Phoenix, Arizona, U.S.A., Apr. 2004.

[Suriyachai09] P. Suriyachai, U. Roedig, A. Scott, “Implementation of a MAC Protocol for QoS Support in Wireless Sensor Networks”, Proceedings of IEEE Conference on Pervasive Computing and Communications, Washington, USA, 2009.

[Suriyachai10] P. Suriyachai, J. Brown, U. Roedig, “Time-critical data delivery in wireless sensor networks”, in Proceedings of Conference on Distributed Computing in Sensor Systems, Santa Barbara, California, Jun. 2010.

[Szewczyk04] R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson, D. Culler, “An Analysis of a Large Scale Habitat Monitoring Application”, in Proceedings of Conference on Embedded Networked Sensor Systems, Baltimore, Maryland, U.S.A., Nov. 2004.

[Tan08] J. Tan, M. Chan, H. Tan, P. Kong, C. Tham, “A Medium Access Control Protocol for UWB Sensor Networks with QoS Support”, in Proc. of 33rd IEEE Conference on Local Computer Networks, Montreal, Canada, Oct. 2008.

[Teng10] Z. Teng, K. Kim, “A Survey on Real-Time MAC Protocols in Wireless Sensor Networks”, Journal of Communications and Network, 2: 104–112, 2010.

[Timmons04] N. Timmons, W. Scanlon, “Analysis of the performance of IEEE 802.15.4 for medical sensor body area networking”, IEEE Annual Conference on Sensor, Mesh and Ad Hoc Communications and Networks, New Orleans, U.S.A., 2004.

[TinyOS] “TinyOS: Open-Source Operating System for Wireless Embedded Sensor Networks”. Available at: http://www.tinyos.net.

[Togabi75] F. Togabi, L. Kleinrock, “Packet switching in radio channels: part I carrier sense multiple access modes and their throughput delay characteristics”, IEEE Transactions on Communications, 23(12): 1400–1416, Dec. 1975.

[Torfs06] T. Torfs, V. Leonov, C. Hoof, B. Gyselinckx, “Body-heat powered autonomous pulse oximeter”, in Proc. of the Intern. IEEE Conference on Sensors, Daegu, Korea, Oct. 2006.

[Varga00] A. Varga. “The OMNeT++ discrete event simulation system”, in European Simulation Multiconference, Prague, Czech Republic, Jun. 2001.

[Virone06] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, J. Stankovic, “An Advanced Wireless Sensor Network for Health Monitoring”, in Proc. 1st Transdisciplinary Conf. on Distributed Diagnosis and Home Healthcare, Arlington, Virginia, U.S.A., Apr. 2006.

[Wang01] A. Wang, S. Chao, C. Sodini, A. Chandrakasan, “Energy Efficient Modulation and MAC for Asymmetric RF Microsensor System”, in International Symposium Low Power Electronics and Design, Huntington Beach, California, U.S.A., Aug. 2001.

[Watteyne06] T. Watteyne, I. Augé-Blum, S. Ubéda, “Dual-Mode Real-Time MAC Protocol for Wireless Sensor Networks: a Validation/Simulation Approach”, in Proceedings of 1st Conference in Integrated Internet Ad Hoc and Sensor Networks, Nice, France, May 2006.

[Werner06] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, J. Lees, “Deploying a Wireless Sensor Network on an Active Volcano”, IEEE Internet Computing, 10(2): 18–25, 2006.

[WHART07] http://www.hartcomm2.org.

[Wood06] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, J. Stankovic, “ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring”, Technical Report CS-2006-11, Department of Computer Science, University of Virginia, 2006.

[Ye02] W. Ye, J. Heidemann, D. Estrin, “An Energy-Efficient MAC Protocol for Wireless Sensor Networks”, In Proc. of 21st Inter. Annual Joint Conference of the IEEE InfoCom Computer and Communications Societies, New York, U.S.A., Jun. 2002.

[Yick08] J. Yick, B. Mukherjee, D. Ghosal, “Wireless Sensor Network Survey”, Elsevier, Journal of Computer Networks, 52(12): 2292–2330, 2008.

[Yigitel11] M. Yigitel, O. Incel, C. Ersoy, “QoS-aware MAC Protocols for Wireless Sensor Networks: a Survey”, Elsevier, Journal of Computer Networks, 2011.

[Ylisaukko04] A. Ylisaukko-oja, E. Vildjiounaite, J. Mantyjarvi, “Five-Point Acceleration Sensing Wireless Body Area Network Design and Practical Experiences”, in Proc. of 8th IEEE International Symposium on Wearable Computers, Arlington, Virginia, USA., Oct. 2004.

[Yoon07] S. Yoon, C. Qiao, R. Sudhaakar, J. Li, T. Talty, “QoMOR: a QoS-aware MAC Protocol using Optimal Retransmission for Wireless Intra-Vehicular Sensor Networks”, in IEEE InfoCom Workhop on Mobile Networking for Vehicular Environments, Anchorage, Alaska, U.S.A., May 2007.

[Yu06] J. Yu, W. Liao, C. Lee, “A MT-CDMA based Wireless Body Area Network for Ubiquitous Healthcare Monitoring”, in Proceedings of IEEE Biomedical Circuits and Systems Conference, London, England, Nov. 2006.

[Zasowski03] T. Zasowski, F. Althaus, M. Stager, A. Wittneben, G. Troster, "UWB for Non-Invasive Wireless Body Area Networks: Channel Measurements and Results", in Proc. of IEEE Conf. on Ultra Wideband Systems and Technologies, Reston, Virginia, U.S.A., Nov. 2003.

[Zasowski05] T. Zasowski, G. Meyer, F. Althaus, A. Wittneben, "Propagation Effects in UWB Body Area Networks", IEEE Conf. on Ultra-Wideband, Zurich, Switzerland, Sep. 2005.

[Zhou, 2007] B. Zhou, C. Hu, H. Wang, R. Guo, "A Wireless Sensor Network for Pervasive Medical Supervision", in 1st Conf. on Integration Technology, Shenzhen, China, Mar. 2007.

[ZigBee07] The ZigBee Alliance. http://www.zigbee.org.

[Zimmerman96] T. Zimmerman, "Personal Area Networks: Near-Field Intra-Body Communication", IBM Systems Journal, vol. 35, nr. 3 & 4, 1996.

[Zuniga04] M. Zuniga, B. Krishnamachari, "Analyzing the Transitional Region in Low Power Wireless Links", in Proceedings of 1st IEEE Annual Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, U.S.A., Oct. 2004.