Chapter 7
Wireless Sensor Networks: A Key Enabling Technology for Remote Healthcare

Steffen Ortmann, Peter Langendoerfer, Marcin Brzozowski, and Krzysztof Piotrowski

Abstract Recent advances in ICT and sensing technologies have created exciting options for individualised sensing and health monitoring. Wireless Sensor Networks (WSN) that are built of lightweight and autonomous devices called sensor nodes are a concrete example of such technologies. Each sensor node typically combines individual sensing, processing and wireless communication features into one small device. This chapter motivates the use of WSN as a key enabler for remote health care by introducing the manifold facilities and use cases of that technology. Based on that, it discusses the architectural basics and provides insights into practical system design issues, especially in view of reliability, energy efficiency and security of the system. After that an assessment of design goals and most critical challenges for applying WSN in health care is given. The chapter finally closes with presenting several selected solutions that successfully tackle introduced challenges.

7.1 Motivation

The prevalence of ageing in modern societies leads to an increased number of people suffering from Stroke, Cancer or Chronic Diseases (CDs) such as Cardiovascular Diseases (CVD), Diabetes, Asthma, Chronic Obstructive Pulmonary Disease (COPD) etc. Alarming numbers published recently stated that over 100 million people or 40 % of the European population aged over 15 years suffer from at least one type of a "chronic disease" whereas 2 out of 3 people aged over 65 years are already affected by at least two chronic conditions.[1,2] The World

[1] http://www.eupha.org/repository/publications/EU_HPF_Answer_to_Consult_on_CDs_Jan12.pdf.

[2] http://ec.europa.eu/research/innovation-union/pdf/active-healthy-ageing/steering-group/operational_plan.pdf and European Chronic Disease Alliance, WHO Europe.

S. Ortmann (✉) • P. Langendoerfer • M. Brzozowski • K. Piotrowski
IHP GmbH—Innovations for High-Performance Microelectronics, Frankfurt (Oder), Germany
e-mail: Ortmann@ihp-microelectronics.com; langendoerfer@ihp-microelectronics.com

K. Maharatna and S. Bonfiglio (eds.), *Systems Design for Remote Healthcare*,
DOI 10.1007/978-1-4614-8842-2_7, © Springer Science+Business Media New York 2014

Health Organization (WHO) "considers the rise in chronic diseases an epidemic and estimates that this epidemic will claim the lives of 52 million people in the European Region by 2030".[3] As another example, Stroke is hitting about two Million people per year in Europe (Kirchhof et al. 2009) and the German Aerztezeitung predicts these numbers to increase by even 2.5 times until 2050.[4] Stroke is a leading cause of acquired disability and is also one of the main reasons for the need of care for elder people. In Germany, Stroke meanwhile is the third main cause of death (Heuschmann et al. 2010).

What all of the major diseases have in common is that their socio-economic implications are enormous. It is widely acknowledged that 70–80 % of healthcare costs are spent on chronic diseases—approximately equalling to 700 billion €—and the cost is expected to rise in the coming years.[5] According to the estimates of World Economic Forum and Harvard School of Public Health chronic diseases will cause a 47 trillion US $ global economic output loss over the period of 2011–2030.[6] Recent analysis also showed that productivity loss due to Cancer in UK alone in 2008 is approximately 15 billion[7] € and the cost associated with mental health problem is estimated to be 3–4 % of the Gross National Product (GNP).

The list of health impacts and respective social-economic implications can be easily extended by many other facts. However, the following major aspects require developing new means to cope with the effects of continuously increasing number of patients:

1. The reduction of quality and length of life of millions of people.
2. The enormous pressure for the socio-economic system in terms of health care costs, long time care as well as productivity loss.
3. According to statistics, the chance that a European citizen suffers from a major disease and/or a NCD in her/his life converges up to 100 %.
4. Constant aging of the society and increasing urbanization exacerbates the problem of adequate and good-quality care for all people, especially in rural areas.

Given these facts, there is a strong need for a radical change in disease management. Suitable approaches need to shorten or even avoid stationary hospitalisation and to improve the ambulant care model, in particular, at the home settings. The patients need to be involved into the care pathway to achieve a maximal outcome in terms of clinical treatment as well as quality of life. Wireless sensor networks are considered as a key enabler for novel telemedical concepts and implementations ensuring an adequate supply with little or no additional personal efforts.

[3] United Nations General Assembly 19 May 2011 Report by the Secretary-General on the prevention and control of non-communicable diseases (A/66/83).

[4] http://derstandard.at/1259281485986/Neuer-Gesundheitsbericht-Risiko-einer-Schlaganfall-Krise-in-Europa.

[5] See http://www.oecd.org/dataoecd/43/9/48245231.pdf and "The future of healthcare in Europe", The Economist Intelligence Unit Limited 2011.

[6] http://www.hsph.harvard.edu/news/features/features/noncommunicable-diseases-report.html.

[7] Policy Exchange, The Cost of Cancer, Featherson and Whitman, 2010.

The concept of telemedicine pursues letting patient health data "travel" around instead of the patients themselves. That means, instead of visiting the doctor directly, the patient is provided with technical equipment that monitor and assesses the patient's actual health state, for example by measuring blood pressure, heart rate or even body weight. Gathered data is submitted to the doctor via internet, who can then assess the data without the need to really "see" the patient. Thus, telemedicine offers remote health care applications for patients at home and during daily life (Ortmann et al. 2011).

The advances in ICT and sensor technologies have developed novel means for personalised sensing and health monitoring. Wireless Sensor Networks (WSN) are a prime example of such technologies. WSN consist of small sensor nodes that in principle are lightweight and autonomous mini-computers. Sensor nodes combine latest sensing, processing and wireless communication features into small autonomous systems that can be used to execute a common respectively distributed task. Given that, WSNs are ideally usable for personal health monitoring due to the following key facts:

- Customised monitoring of patients and their environment becomes feasible using sensor nodes. Sensor nodes may be attached to the patient's body, build into equipment or wearable garment or be installed in a fixed infrastructure, for example the home of the patient.
- Sensor nodes provide great flexibility due to the fact that these may be equipped with a variety of sensors, such as motion, biomedical or environmental sensors, or can be used for signal processing, assessment or forwarding of data etc.
- Due to their autonomous nature, sensor networks provide mobility by default. Equipped with portable power supply, for example a portable battery, these are enabled to independently carry out their tasks for weeks, months or even years depending on the power consumption.
- Wireless communication means on each node enable to communicate amongst sensors themselves or to public infrastructure such as the UMTS or GSM network. Thus, remote data access becomes feasible.
- Sensor nodes are low cost devices. The costs for single sensor nodes even decreases rapidly when several hundreds or thousands are used.
- WSN can provide so called self-X properties that are key for ease of use. This means sensor nodes can be programmed to react autonomously and flexibly on changing operational conditions. Therefore they are capable of learning and optimizing their behaviour during operation, e.g. to self-organise to changes in the environment, to self-heal the network in case of failing nodes, to self-coordinate distributed processing according to available resources etc.

The benefits of applying WSNs as health care technology are manifold. WSNs can play an important role while developing the next generation of health care technology by contributing to:

- *Ambient health care solutions* that enable a better and safer control almost anywhere at any time. Hence, medical monitoring will no longer be bound to a physical place such as a clinic. Instead, smart and ambient systems will overtake many of the tasks that are currently provided by health care professionals.

- *Improved well-being of patients* when being monitored or "treated" during daily life. Sensor networks worn throughout the day or installed in the daily environment, e.g. the patient's home, can control the patient's health state continuously even outside a clinical environment.
- *Reduction of stationary treatment* due to inherent flexibility of sensor nodes. Being small, lightweight and wearable, autonomous sensor nodes can amongst other things overtake patient specific monitoring tasks in the post-acute phase to shorten hospitalisation as well as for detection of future acute phases or ensuring well-being respectively to prevent future stationary treatment.
- *Reduction of costs* in many ways. In addition to the reduction of expensive stationary treatment, WSN also allow transferring regular evidence-based treatment means into home services or to support rehabilitation means and thereby empower patients to faster return home and to their job again. WSN might further reduce costs of future health monitoring devices too.
- *Enriched data sets* of patient's health states and disease progress. Monitoring solutions outside a clinical environment provide clinical experts with great long-term data sets not available today. This will lead to a better understanding of disease management and effective treatment.

Featuring such great potential and flexibility, wireless sensor networks are already used for different application fields in modern e-health technologies and telemedicine scenarios. Amongst many others, current research focusses on the following four main application areas:

Acute care: Sensor networks or lightweight sensing boards that are used to gather various bio-signals and health parameters such as ECG, EMG, blood pressure, breath rate, O_2 saturation etc. on demand or in emergency cases. Taken data is then not only accessible by the paramedic but can in parallel be submitted to the next clinic for proper preparation of equipment or surgery if necessary.

Rehabilitation: After stationary or acute care, sensor networks can still be used to monitor the recovery process. That does not only cover bio-signals. In fact, they can also be used for activity monitoring or training supervision to measure the progress of rehabilitation for example for stroke survivors[8] (Ortmann et al. 2012) or people suffering from Parkinson's disease[9] (Edwards 2012).

Prevention: Preventive collection of bio-signals mostly concerns continuous monitoring of people suffering from chronic diseases. For example, the most known case are Cardiovascular diseases (CVD), which are monitored with mobile ECG and daily taken body weight (Chen et al. 2012).

Mobile diagnostics: Mobile and lightweight diagnosis means are obviously part of all three application scenarios mentioned above. However, there exists many more

[8] www.strokeback.eu.

[9] www.cupid-project.eu.

technical solutions ranging from mobile and instantaneous measuring of blood parameters with Lab-on-Chips (2011) over monitoring of fire fighters in action (Piotrowski et al. 2010) up to implantable devices measuring the blood glucose level continuously (Birkholz et al. 2009; Fröhlich et al. 2012). In combination with communication and flexibility means provided by WSN's, these approaches can provide novel value-added e-health services.

7.2 Background

Wireless sensor networks have been introduced in research about 15 years ago. The core idea was that extremely cheap devices can be deployed in a very large number and which are then forming a network without human intervention. The sensor network is then gathering data about its environment. In order to facilitate such an idea the devices to be used need to be extremely cheap and battery powered to keep the coats at a reasonable level and to enable autonomous operation. The standard sensor node is built of a microcontroller, volatile and non-volatile memory, a wireless communication interface i.e. a transceiver and an interface to the sensing device, see Fig. 7.1.

Table 7.1 shows common sensor node platforms including their micro-controllers, available memory and radio interfaces. Most of the micro controllers come with very limited computing resources and memory, resulting in serious challenges for software developers. The other limiting factor of sensor nodes is the fact that they need to run out of a battery i.e. they may use very little energy in order to ensure long lifetime.

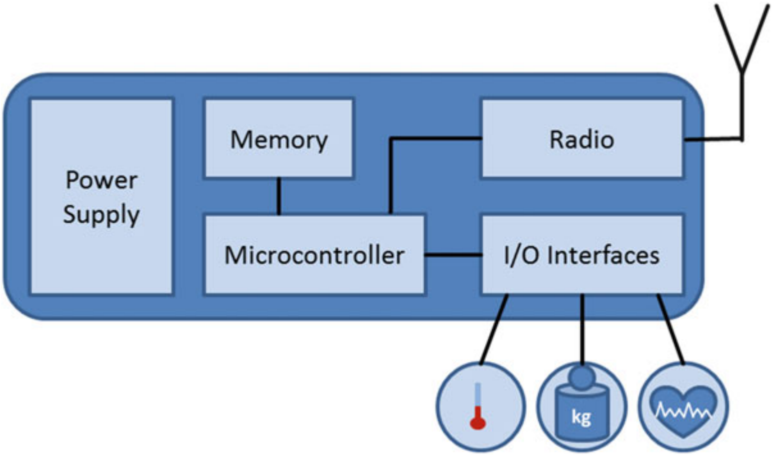


Fig. 7.1 General assembly of a sensor node that can integrate various external sensors

Table 7.1 Overview of existing sensor platforms and their basic features

Platform	μC	f_{max} [MHz]	RAM [KB]	Code [KB]	Storage [MB]	Radio
MICAz	ATmega128L (ATMEL 2011)	8	4	128	0.5	CC2420 (TI Inc. 2007a)
MICA2	ATmega128L	8	4	128	0.5	CC1000 (TI Inc. 2007c)
IRIS	ATmega1281 (ATMEL 2010b)	8	8	128	0.5	CC2420
TelosB	MSP430F1611 (TI Inc. 2011)	8	10	48	1	CC2420
IHPNode	MSP430F5438A (TI Inc. 2010c)	25	16	256	4	CC1101 (TI Inc. 2010a) CC2500 (TI Inc. 2009) CC2520 (TI Inc. 2007b)
Chronos	CC430F6137 (TI Inc. 2010b)	20	4	32	–	CC430F6137 (CC1101)
Sun Spot	AT915SAM9G20 (ATMEL 2010a)	400	1,024	8,192	–	CC2420
Imote2	PXA271 (Marvel 2010)	416	256 + 32,768	32,768	–	CC2420
Shimmer (Burns et al. 2010)	MSP430F1611	8	10	48	µSD-card	BT RN-42 CC2420

7.2.1 Original Application Areas

WSN's have originally been developed out of the vision of pervasive intelligent environments that may surround and serve us at any place and any time (Weiser 1991). Long time ago in the early nineties, this computing paradigm already predicted computing devices to be embedded in everyday objects, e.g. in coffee cups (Gellersen et al. 2000) or garment (Patel et al. 2012), allowing information technology to fade into the background and become nearly invisible to their users. As one of the first real world examples enabling pervasive computing, WSNs have become a rising star in this research field. Envisioned to be distributed like "Smart Dust" (Kahn et al. 1999, 2000), these networks support a broad range of applications (Aboelaze and Aloul 2005; Akyildiz et al. 2002) and may become the perfect service and surveillance tool (Bohn et al. 2004). Based on their capabilities to identify physical phenomena, sensor networks can be applied for environmental and structural control (Dikaiakos et al. 2007; Mainwaring et al. 2002; Sun et al. 2005; Werner-Allen et al. 2005), context-awareness for personal services (Robinson and Beigl 2003), military applications (Gillies et al. 2009) and ubiquitous healthcare (Morchon et al. 2009), to mention a few. As a particular variant of WSNs, Body Area Networks (BANs) that utilise sensor nodes attached to the human body have emerged rapidly for a broad range of novel e-health applications. The following paragraphs will therefore focus on applying wireless sensor nodes for body area networks.

7.3 Architecture

Wireless body area networks can be used to monitor vital parameters of patients and even healthy persons. These networks can in addition monitor also the environmental conditions of the monitored persons. While under normal conditions such monitoring is a task that can be performed locally and even the assessment of the measured parameters can be done by the BAN itself, it is important to allow for reporting features to make full benefit out of such a solution. There are two reasons to aim for an always connected solution:

- If vital parameters are above/below a predefined threshold the BAN can send the measured values directly to a telemedicine centre so that appropriate actions can be triggered immediately.
- The measured values should be stored even while being in the allowed range of values to enable anamneses later on if necessary, or to allow the patient to do kind of self-assessment. Due to the limited resources of the BAN devices they cannot be used as long term storage i.e. they need to be connected to a more powerful device.

For providing connectivity to a BAN a lot of different networking solutions can be used. It ranges from wireless LAN and standard Internet to GSM/UMTS communication. Figure 7.2 illustrates these possibilities and depicts the communication end point i.e. the BAN and a telemedicine centre. The protocols used for ensuring the always connected feature are out of the scope of this chapter. The only issue to be considered when designing the BAN is the specification where the bridging functionality between the BAN and the cellular network or the Internet is

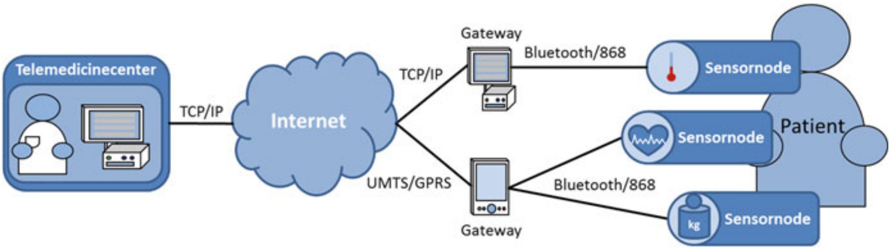


Fig. 7.2 Main principle of BAN applications. Sensor nodes attached to the patient's body wirelessly communicate to a gateway device that is connected to a global network over which it can reach the telemedicine center

to be placed. It can be allocated inside the BAN or outside the BAN, e.g. when a Smartphone is used. For practical reasons, i.e. the design of Smartphones normally won't be heavily influenced by BAN designers, the bridging functionality will be placed inside the BAN that then has to provide a communication link that is compatible with those provided by Smartphones. Here low-power Bluetooth (Bluetooth 4.0) is a highly probable candidate. Whether or not the Smartphone as the most probable gateway to the outer world then uses a cellular network or the Internet, may depend on:

- Features of the Smartphone i.e. supported communication devices
- Availability of the one or the other type of network
- Emergency consideration
- Certifiability as a medical product[10]

This short discussion of the integration of the BAN into a telemedicine service architecture should show that we are aware of those problems, and that there are solutions at hand, whereas a detailed discussion of these issues is out of scope of this chapter.

7.3.1 Centralized vs. Distributed BAN Architecture

When designing BANs a lot of decisions need to be taken. One of the first decisions and one with an extremely high impact on the final design is, whether or not the BAN will be centralized or distributed. In addition, there are a lot of design goals such as dependability of the BAN that need to be ensured independent of the type of the BAN network. But please note that the decision whether the BAN is centralized or distributed has considerable impact on the approaches to be applied for ensuring features of the BAN such as dependability, availability, power supply etc.

While there are good reasons for both approaches—centralized and distributed—which we will discuss here, we will focus on distributed architectures when going into a more detailed discussion of design goals and means to achieve these goals.

7.3.2 Centralized BANs

The basic idea of a centralized BAN solution is that there are more or less dumb sensor devices that are capable to measure and send parameters such as heart beat, temperature etc. All computation is then done on a central intelligent BAN node that comes with a processor and that knows how to assess the raw data sent by the sensing nodes. The right side of Fig. 7.3 illustrates this approach. Such a centralized model has the following benefits. The central device e.g. the Body Central Unit

[10] Designers should be aware of the simple fact that an increased number of features and capabilities provided by the device directly lead to a more complex certification procedure.

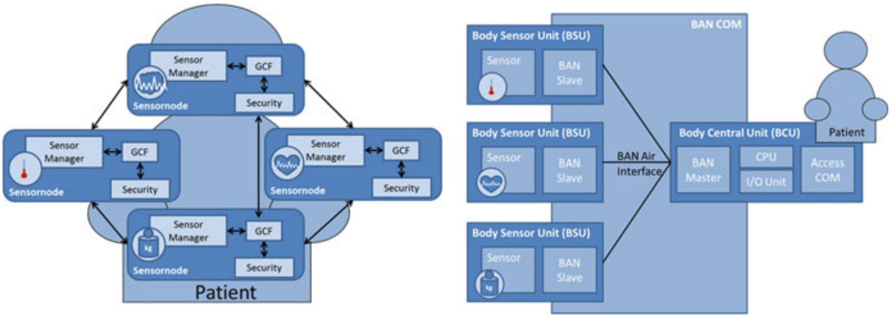


Fig. 7.3 Conceptual design of distributed and centralized BAN architectures. Whereas a distributed approach allows all nodes to communicate independently to each other (left side of the figure), the centralized approach forces all nodes into one-way streaming to a central unit (right side of the figure)

(BCU) in Fig. 7.3 can be used as a scheduler for medium access. This allows using relatively simple Medium Access Control (MAC) protocols since only the BCU can initiate communication, i.e. all other devices are actively polled by the BCU. This in addition helps to reduce the memory needed for the software that is deployed on the sensor nodes. Such a centralized approach also facilitates pretty simple management of sleep cycles that are used to reduce the energy consumption of the sensor nodes. The open issue here is the synchronization of the wake-up times. These issues will be discussed in detail later in this chapter. Last but not least, the implementations of centralized BANs may be easier to certify as medial product. This assumption is based on the fact that the majority of the devices used in the BAN are relatively simple and equipped with little software only, i.e. the amount of components—hardware and or software—is small.

But this approach comes with some drawbacks. All measured data need to be transferred to the central unit for assessment. This puts a serious communication load on the sensing devices. Here data and not information is transferred. Since transmitting data is more power consuming than processing data it seems reasonable to do evaluation of measurement data directly after measuring it instead of sending it to the central unit. The central unit is a single point of failure, i.e. if it fails the whole BAN can no longer provide its service. Such failure may put the patient's health at serious risk. The raw data will no longer be assessed and it is even impossible to communicate it to a telemedicine centre. From a security and privacy point of view the centralized approach is extremely challenging. If the sensing devices really come with extremely limited resources—less than normal sensor nodes have—it is infeasible to run cipher algorithms or other protection means. This means that the measured values are send in plain to the central unit, which in turn means that these values are accessible by any potential attacker in the vicinity of the BAN user, rising serious privacy concerns. Security questions as well as feasible solutions will be detailed later in this chapter.

7.3.3 Distributed BAN

The left side of Fig. 7.3 illustrates the distributed BAN approach in which all sensor nodes in the BAN are equally equipped with respect to processing capabilities, transceivers etc. Here the major difference in the sensor nodes are the sensing devices attached to the sensor node. Due to the concept of almost identical sensor nodes a kind of distributed intelligence can be realized. I.e. in such a system each of the sensor nodes can do an assessment of the values measured by itself, so that raw data does not need to be send so the energy consumption can be reduced compared to the centralized model. The fact that all sensor nodes are identical provides kind of resilience since the nodes can replace each other. Thus if one of the sensor nodes fails the BAN can still work and provide measurements at least for those values for which the sensors are functioning. The processing features on each of the BAN nodes enable the use of proper cipher means to protect the data from eavesdropping when being exchanged in the BAN. The realization of security and privacy features is an essential and non-trivial task, on which we will elaborate later in this chapter.

The improved dependability of the distributed BAN concept comes with some drawbacks. All sensor nodes are more or less equal, i.e. a kind of distributed control is required. This affects the protocol stack especially the MAC layer. Here no centralized scheduler, such as the BCU before, is available so that the MAC protocol needs to be able to cope with contention based medium access, while trying to allow for energy efficiency etc. This requires a more complex software to be installed an all nodes, consuming additional memory which is a scarce resource on senor nodes.

7.4 Design Goals and Challenges

In the originally addressed application areas the holy grail for designers was—and still is—energy efficiency since here the sensor nodes are expected to work unattended for years. This situation changes in the area of BAN design. The sensor nodes are easy accessible and reloading /exchanging of batteries can be afforded. But even if the intended lifetime of a BAN does not need to be years, often exchanges of batteries will have significant and negative impact on usability and acceptance of BANs, so energy efficiency is still an important design goal. Not to mention that less power consumption certainly allows using smaller and more lightweight battery packs of course. But other features are considered to be equally important for convincing BAN designs. As human being lives might depend on BANs the following features are essential:

Safety: this means the BAN may not put the patients' health at risk. To ensure this is tricky but as long as the BAN is used for monitoring only, i.e. no actuators are included, only a few features need to be considered. Radio transmission is one of these features. Here the exposure of the patient should be kept minimal which can be achieved in the design by reducing the communication frequency and transmit power. As long as the hardware works according to its specification there should not be any problem. In order to ensure this the hardware needs to be measured from time to time. Another challenge might occur due to possible (over-)heating of electrical components and battery packs during operation or charging. Here the usage of Negative Temperature Coefficient Thermistors (NTC) is common to monitor the temperature of devices or partial components. NTCs are available as single parts but are also available as fully integrated solutions e.g. in enhanced battery packs.

Reliability/Availability: this means the BAN need to work correct at every point in time when in use. There is a certain probability for any component in the BAN to fail be it permanently or transient. Redundancy is a means to increase the overall reliability. It should be applied for all parts of the BAN. So it should be taken into account when designing individual sensor nodes, e.g. by integrating more than one transceiver and micro controller, but also when designing the BAN by integrating two or more nodes providing the same functionality. Also for software redundancy should be considered. Software can also be used to provide redundancy if replication strategies are supported by the software used in the BAN. We will introduce such a concept later on. Even though redundancy is a key concept to achieve reliability/availability, energy efficiency of the overall design is nearly as important as redundancy if not more important. If one of the nodes run out of battery supply it can be replaced by another one using redundancy, but energy efficiency can help to even avoid the failure of the node.

Security: or more precisely confidentiality and data integrity are essential in BANs used for health care applications. Here all data is extremely sensitive and needs to be protected against eavesdropping. While this might be considered as convenience feature, data integrity is required to ensure correct behaviour of the telemedicine system. If measurement values are falsified during transport, this may have significant impact e.g. emergency situations are not detected, negatively affecting the patient's health status. In Halperin et al. (2008) the authors have shown that eavesdropping and even manipulating of a pacemaker can be easily done. The problem with integrating reasonable security functions is that most cipher algorithms require significant computation effort and by that consume energy. Both are scarce resource so that the design of the cipher means i.e. selection and implementation needs special attendance.

Privacy: For acceptance of telemedicine solution ensuring privacy is a core issue. Protecting the patients' data requires strong cryptographic means to ensure confidentiality whenever data is transmitted. This holds true for the communication inside the BAN but also for data transport via open networks to the telemedicine centre. The most secure and advanced solution is having a real end-to-end security in which the sensor nodes use the same crypto system as the telemedicine centre. Ortmann (2011a, b) introduce such an architecture. That way transmitted data is protected regardless whether or not unknown or public devices/gateways are used as communication hop (Ortmann and Maaser 2011). But the more tricky issue is to protect the data after it is received in the telemedicine centre or stored in patients' health records. Here different types of access model that take the current role of the data user into account can be applied, i.e. whether it is a nurse or physician (Maaser and Ortmann 2010). A very interesting concept for privacy protection is proposed in Scheffler et al. (2011). Here not only the patient is considered to be a data owner, but also the physician who did the examination and updated the health record is considered to be data owner. These privacy enhancing techniques are mainly related to the back end, where patient data is processed. Even though privacy protection is a major concern there might be conflicting situations in which privacy might put the patient at risk. Consider kind of emergency situation in which the patient suffers from a heart attack or similar. First aid arrives but may not access the patients vital data stored in the BAN due to privacy settings and still on-going encryption of measurements values. Conflict resolution techniques have gained some interest in the recent past (Naqvi et al. 2010). But in this chapter we will focus on the basic security techniques that need to be available inside the BAN to allow for privacy at all.

Usability: Despite clinical/therapeutical advances and opportunities, usability is by far the most crucial acceptance factor! That means a comfortable and easy way to use the sensor nodes is the key to success in the real world beyond any research trials. The idea that patients are going to use BANs at home requires usability in several aspects. First, almost none of the patients will be computer experts, which means the BAN may not need any kind of configuration, at least not after a first set-up phase. In fact the BAN design is required to ensure that a single push button is going to bring the BAN into a full operation mode. Here the self-healing and self-configuring features of wireless sensor network are providing a solid basis to do such a design. Wireless sensor network have been considered to run unattended and by that need to do kind of network bootstrapping without human intervention. Nevertheless, body worn sensors should work nearly “invisible” and must not hinder the patient in her/his daily life activities. The sensors should be small and lightweight but still allow for monitoring the patient for several hours or the whole day respectively. The latter is certainly a trade-off between power consumption and an appropriate battery supply, which grows in size and weight with the amount of energy that is needed. The second point is physical handling. Some patients may be elderly people some suffer from physical handicap so that attaching the sensor node of the BAN might be difficult to those patients. This requires that the BAN shall come with some help to apply it properly. This can be achieved for example by integrating the sensor node in clothes, or by appropriately selecting easy to reach parts of the body for attaching the sensor node etc. This aspect will not be detailed further in this chapter, since it is more an ergonomics than computer science issue.

7.5 Selected Solutions

After discussing design issues and challenges we are going to introduce some solutions for the before mentioned challenges. The selection of the solutions is done mainly on our own experiences with those solutions so we are not aiming at a full survey. There are for sure more approaches that are most probably equally suited, without being mentioned.

7.5.1 Redundancy for Improved Availability and Reliability

Redundancy is a key feature when it comes to reliability issues. Redundancy means using several equal components in parallel to detect and overcome failures. Redundancy allows substituting functionalities, components or even complete sensor nodes during operation. The latter has been discussed in the previous section of distributed BAN architectures, where more or less all nodes provide the same hardware and can therefore overtake tasks from other nodes. In the following, we will therefore focus on two approaches providing reliability in wireless communication and by data redundancy.

Reliable Communication

Wireless communication is inherently prone to errors such as link failures, packet errors during transmission, physical disturbances e.g. caused by water or metal, or blocked frequencies due to other devices such as microwave ovens at 2.4 GHz. The various radios available at the market certainly offer significant differences in power consumption, communication distances and reachable data rates. In addition, the physical destruction of radios or whole sensor nodes, e.g. in case of falls, need to be taken into account as well. In summary, there exists dozens of issues that might hinder the wireless communication to work properly at least for a certain time period.

Since we target on availability and reliability of wireless communication, i.e. ensuring that communication is always feasible, integrating more than one radio into one sensor node might be a suitable solution. To again increase resilience against failures, all nodes used in such BAN architecture should be equally equipped. To show evidence that such approach really works, we here report on the *IHPNode* sensor platform originally developed for monitoring vital and environmental of fire-fighters in action (Piotrowski et al. 2010). This means, the BAN of *IHPNodes* locally gathers all data and then needs to transfer it to the head of mission who is usually outside of the emergency area, e.g. outside of the burning building. While the pure reporting of data from moving persons is a challenge as such, we have faced almost the worst case scenario for wireless sensor networks because of

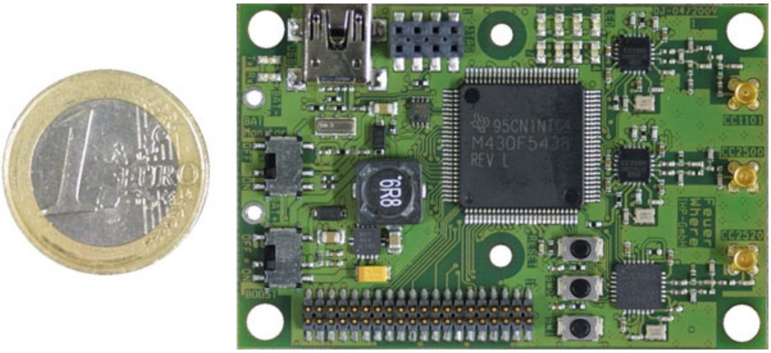


Fig. 7.4 Top view of IHPNode in comparison to the size of a 1 Euro coin

the harsh environmental conditions, i.e. heat, fire, acids, 100 % humidity (water steam) etc.

However, to cope with communication errors, we have integrated the following transceivers in parallel on each to provide redundancy in radio connectivity:

- TI CC1101: Low cost transceivers working in the 868 MHz band
- TI CC2500: Low cost transceivers working in the 2.4 GHz band
- TI CC2520: ZigBee$^{\text{TM}}$ Transceiver working in 2.4 GHz band

We applied two pin and logic compatible transceiver chips working in different radio frequency bands, i.e. the first in the European 868 MHz band and the second in the 2.4 GHz. The third transceiver (ZigBee) is also working in the 2.4 GHz band and provides 802.15.4 support. It was applied to be able to communicate with other known node platforms. The IHPNode is empowered by the MSP430F5438 Microcontroller from TI. The complete sensor node is depicted in Fig. 7.4.

Redundant Data Storage

Protecting from data loss by applying redundancy in data storages is of common use for decades in server applications, e.g. by using RAID systems. However, full redundancy in sensor nodes is counterproductive due to the enormous additional efforts in terms of processing power and energy consumption. On the other hand, mere redundancy at single nodes will not be helpful when complete sensor nodes fail. To still cope with potential data loss or failed sensor nodes, we have investigated how to provide redundant data storage means in a comfortable way in sensor networks. As a result, we will report on the *tinyDSM* middleware approach that introduces the concept of Distributed Shared memory (DSM) to sensor networks. The tinyDSM middleware:

- Provides a data storage model that not only supports replication of measurements but ensures also consistency of data,

- Supports storing of historical data up to a specified number to facilitate anamnesis,
- Provides an event detection mechanism based on the shared data.

Compared to passive data storage approaches, like tinyDB (Madden et al. 2005), cougar (Yao and Gehrke 2002) or tinyPEDS (Girao et al. 2007), tinyDSM provides an active data monitoring. There are also other approaches that support distributed computation and data storage for WSN, like (Abdelzaher et al. 2004; Costa et al. 2007; Gummadi et al. 2005), but they are usually tied to a specific operating system. Our middleware is implemented in pure C programming language and provides a clear interface to both, the underlying operating system and the application on top of it. Encapsulated in an OS adaptation layer (wrapper) it can work with all C based operating systems, and thus, it supports heterogeneity in both, hardware and software (or OS) dimension.

The tinyDSM middleware provides means that allow sensor nodes to autonomously share their data in an application dependent way. Moreover, tinyDSM middleware supports an event mechanism based on the shared data. Therefore a predefined set of shared variables is known to all nodes in the network. There are two types of variables—local variables and global variables. A variable defined as local has as many entities as many nodes are in the network, i.e., each node owns an entity of a local variable. Each global variable has only one entity existing in the whole network. In this context, an entity is a unique and independently addressable data unit in the shared memory space. Thus, to address a variable defined as global, only a reference to the variable is needed. In case of addressing a local variable it is necessary to point at a specific node—the owner—to address the right entity of the variable.

There are two operations that the application can perform on a variable, i.e. the WRITE operation and the READ operation. If an operation requires multiple nodes to interact, there is a need to exchange messages to fulfil the task. For example, since the sharing of the variables is based on data replication, once a new value is written to an entity of a variable in a WRITE operation, an UPDATE message is broadcast to all the nodes that hold a copy of the entity. Updates are autonomously handled by the underlying middleware layer without the need of extra programming effort. Data replication makes the system robust against data loss caused by lost nodes and reduces the overhead of the read access if the data is available locally on the nodes. The span of the data replication and its density is controlled by a policy chosen at the compile time.

The integrated event mechanism allows the application developer to define runtime events at compile time that shall be detected during operation. Each event is described as a logical equation evaluated each time any variable included in this equation changes. The result of this evaluation is stored in a variable that is automatically created for each event. From the application perspective, these event variables are read only and store only logic values, i.e., true or false. According to the event definition, the application is notified about the evaluation result. For more details about configuration of variables, events and the middleware interfaces please refer to Piotrowski et al. (2009, 2010).

Table 7.2 Percentage of tinyDSM messages delivered between node pairs inside the BAN

NodeID	1	2	3	4	5	6
1		87.2	93.7	86.3	83.2	85.5
2	86.1		94.3	92.1	79.7	89.0
3	89.3	92.0		85.9	82.8	86.6
4	85.9	89.0	87.1		80.8	88.9
5	88.6	87.2	93.9	88.1		86.4
6	86.1	87.5	88.1	94.4	79.8	

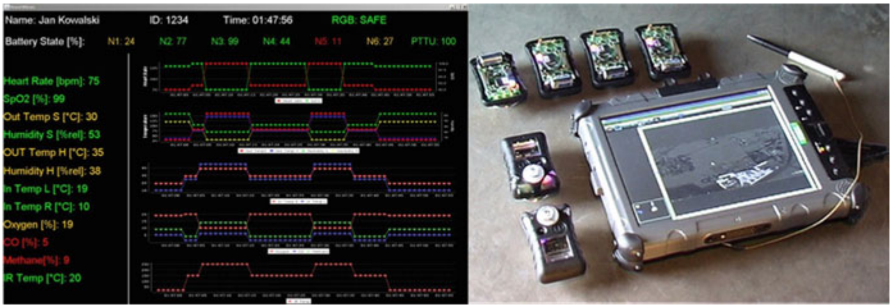
In order to verify the distributed mechanisms we ran five over 2 h-long tests of our system with focussing on the weakest point of this distributed system, i.e., the networking in general and the packet loss rate in particular. The middleware in its basic configuration does not include the network protocols and relies on external ones, i.e., the medium access controlled by the transceiver only. The BAN consisted of six nodes, each randomly generating the values of 2–7 parameters, resulting in a total of 26 updates per second. An UPDATE message was 120 bits long, while the data rate was set to 400 kbps.

Based on that we could estimate the quality of the replication in the system. In order to provide a reliable replication, the copies of the entities need to be updated frequently, i.e., it is important that the packets are not missing in series. Table 7.2 shows the percentage of middleware requests that were delivered. The columns represent the packets sent and the rows the packets received by each node. The average number of packets missing in a series was below 1 and the maximal length of a series was 18, which is less than 1 s in time.

Using the *IHPNode* and the *tinyDSM* data storage concept we have been able to provide a proof of concept by testing the nodes in a real fire drill. Therefore the sensor nodes together with a couple of sensors have been packaged into fireproofed cases. The local BAN sensors have communicated amongst each other using the CC2500 transceivers at 2.4 GHz while at the same time actual vital parameters have been reported to the squad leader outside of the burning building via the CC1011 transceiver at 868 MHz. If single BAN nodes had no direct link to the squad leader’s device, one of the other BAN nodes has been used as communication hop. Similarly, nodes equipped with inactive redundant sensors observe the primary nodes and in case the value is not updated for 5 s they take over the management of the parameter variable and provide the data. Note that such self-healing feature is only feasible when all BAN nodes provide similar or redundant resources and features as previously introduced as decentralized BAN approach. The graphical user interface and the basic equipment used in the fire drill are shown in Fig. 7.5.

7.5.2 Ensuring Data Integrity and Privacy

When it comes to providing security in wireless sensor networks two core problems have to be solved, i.e. key distribution and energy efficient implementation of the selected cipher algorithms. For key distribution in WSNs a lot of proposals have



Name: Jan Kowalski ID: 1234 Time: 01:47:56 RGB: SAFE

Battery State [%]: N1: 24 N2: 77 N3: 99 N4: 44 N5: 11 N6: 27 PTTU: 100

Heart Rate [bpm]: 75
SpO2 [%]: 99
Out Temp S [°C]: 30
Humidity S [%rel]: 53
OUT Temp H [°C]: 35
Humidity H [%rel]: 38
In Temp L [°C]: 19
In Temp R [°C]: 10
Oxygen [%]: 19
CO [%]: 5
Methane[%]: 9
IR Temp [°C]: 20

Fig. 7.5 Tactical screen of the squad leader with vital parameters of a single fire fighter in action (left side) and a set of packaged BAN sensors with the squad leader device (right side)

been made that fully rely on lightweight secret key cryptography such as SPINS (Perrig et al. 2001) and the system proposed in Chang et al. (2007), but there are also proposals that use public key cryptography such as those presented in Karlof et al. (2004), Shaikh et al. (2006). But in the field of telemedicine where the number of nodes is very limited and deployment is done in a controlled way the key distribution is not as important as it is in standard WSN application fields since keys can even be manually programmed into each device. But energy consumption of the applied crypto system is crucial for the lifetime of the BAN. Here especially the fact that data integrity is a core issue since it almost directly requires using public key cryptography to ensure integrity and non-repudiation. In principle two public key scheme could be applied, RSA and Elliptic Curve Cryptography (ECC). The resource restrictions rule RSA out since it requires a key length of at least 1024 bits which is extending ten the messages sent by the BAN extremely, requiring not only significant processing but also transmission power. In contrast to this, ECC can provide the same level of security with key length of 160–233 bits. But even ECC puts a serious burden on the micro-controller. Here serious efforts have been made to reduce the energy consumption of the ECC processing see for example (Ugus et al. 2009). But also the memory consumption needs to be taken into account on a micro controller a space optimized implementation was proposed in Uhsadel et al. (2007). The core problem with software implementations of ECC (as well as with any other algorithm) is that memory can be traded versus speed and vice versa. In other words, if the implementation is fast and by that energy efficient the memory provided by the sensor nodes might not be sufficiently large enough to install all needed software modules. If the implementation is very small it will most probably drain down the battery quickly. Here efficient hardware implementations help to cope with both issues. They require almost no energy for processing the underlying mathematical functions of the crypto system, and do not allocate memory for the implementation. To the best of our knowledge the most efficient hardware implementation of ECC with a key length of 233 bits was proposed in Dyka and Langendoerfer (2005), a preliminary but still very efficient implementation was integrated with a 16-bit microcontroller (Panic et al. 2011). Hardware

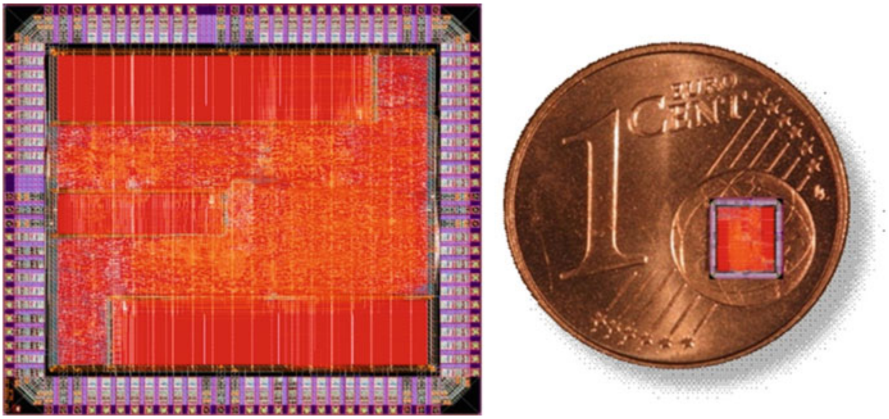


Fig. 7.6 Layout of the IHP-crypto-microcontroller (www.ihp-microelectronics.com) with a 128-pins pad frame. Additionally the size of the chip is compared to the size of a 1 Euro cent coin

implementations of specific functions such as crypto operations are often considered as too costly for sensor nodes but their impact on the total cost of a telemedicine system is negligible. Their size is about 2.5 mm^2 in an old fashioned 250 nm technology resulting in an additional prize in the range of several 10 Euro cents, and without any recognizable effect on the form factor, see Fig. 7.5 for an example of our 16 bit microcontroller enhanced with hardware accelerators for AES, ECC, SHA-1. An interesting software based approach is presented in Sojka et al. (2010). Here the authors propose a lightweight security approach based on modification of elliptic curves cryptography. The reduction of the length of the security parameters influences the security level but also helps to save the energy needed for computation and especially for communication, which is not achieved with the hardware based approaches (Fig. 7.6).

The performance and the energy consumption of the accelerators integrated into the IHP-crypto-microcontroller are given in Table 7.2. For the ECC component the elliptic curve B-233 (standardized by NIST) was hard-coded. As expected, the AES and ECC versions implemented in hardware consume orders of magnitude less power while boosting the performance at the same time. Since performance efficiency and energy consumption are two of the main factors for usage on sensor nodes and the protection of gathered private data is mandatory in the medical domain, integrated hardware accelerators provide the ideal solution for cipher means on resource constrained devices like sensor nodes.

Even with the encryption of data on their way from sensor source to the sink in the e-health centre and an according effective access control (e.g. by appropriate key management), the privacy of patients is still not fully protected (Table 7.3). The patient remains in control of who may access her/his data. Nevertheless, the patient cannot control the extent to what the data is communicated (compare to the definition of privacy in Westin (1967)) to those that may in principle be entitled. That is, with the mere access control and encryption, a doctor or admitted

Table 7.3 Comparison of the performance and the energy consumption of AES and ECC implemented in hard- and software. The software variants have been implemented in native C code

Variant	Duration	Energy consumption
AES (software) 8 MHz/3 V	9,090/19,500 cycles (Encoding/Dec.)	8.5/18.3 μWs
AES (hardware)	78 cycles	16.957 nWs
ECC (software) 8 MHz/3.3 V	82,436 ms	454.3 mWs
ECC (hardware) 33 MHz	180–810 μs	25.1–10.6 Ws

paramedic could access more data than actually required for the current treatment. A role based access control may limit potential privacy risks stemming from exploited authority but in general it is hard if not even impossible to autonomously decide about the need of accessing certain data for treatment. If it was possible to objectively determine the medical necessity to access particular (maybe historic) vital data in the current medical context, we could introduce a context-aware access control approach.

Unfortunately, in the medical domain this is not objectively possible (through an autonomous computing system) without putting the patient at risk. This is still a very important open issue that especially concerns the handling of data access in emergency cases, where it is not reasonable to obstruct the paramedic's or emergency doctor's access to current and historic vital data. In principle free access to the stored and currently measured data should be given in case of danger to life so that acute health problems can be cured by medical or even non-medical helpers. In the simplest form, an emergency situation may be detected if a health parameter exceeds or falls below a pre-configured threshold. Unfortunately that only works fine under certain conditions. For example if the heart rate falls below 10 or exceeds 200 beats per minutes (bpm), it is almost certain that a danger to life exists. However, such simple assumption can e.g. not be taken for monitoring blood pressure that significantly depends on the actual activity of the patient and many other constraints. In other words, even a high blood pressure level may be ok when doing sports but of course not while sleeping. To the best of our knowledge, a highly-reliable and useful monitoring approach that correctly correlates many various vital and physical parameters is still missing.

A means to at least discourage a privacy breaching use by an accessing entity is discussed in Maaser and Ortmann (2010). The system proposed herein logs every data access automatically. The logging includes also rejected access attempts. Therefore, each data access or access attempt is associated with a timestamp and the ID of the accessing entity retrieved from the certificate given in the credentials. In case of complaints of the affected patient, data access e.g. on a data history stored in the sensor node, is documented. The idea is based on using an incremental secure logging functionality as known from other application fields (Sandler et al. 2008; Crosby and Wallach 2009) but the implementation efforts are still too heavy to be used on sensor nodes.

7.5.3 Energy Efficient Protocols

As already mentioned, energy is a scarce resource and thought to be the most important factor when it comes to wireless sensor network lifetime and applicability. Transmitting and receiving are the most power hungry actions on a sensor node. Since most of the time nothing is to be sent or received the coordination of communication is a well-researched field. Most work has been done on Medium Access Control (MAC) protocols. Here the major challenge is to reduce the energy consumed during idle listening. The focus is on allowing sensor nodes to keep the radio powered off as often and as long as possible and to switch it on rarely to send short data frames, dubbed low duty cycle. By doing so, they can achieve a theoretical lifetime of 2 or 3 years with state-of-the-art hardware (Brzozowski et al. 2010c). However, to send data, both the sender and the receiver must be awake at the same time. The problem of synchronizing wake-up time is referred to as "rendezvous" and can be solved in the following ways (Lin et al. 2004):

1. Asynchronous: wake-up radio
2. Pseudo-asynchronous: preamble sampling and similar approaches such as BMAC (Polastre et al. 2004), STEM (Schurgers et al. 2002) and Koala (Liang and Terzis 2008)
3. Synchronous: schedule based wake-ups, e.g. S-MAC (Ye et al. 2002), Dozer (Burri et al. 2007), or DLDC-MAC (see below).

The ideal solution would be a wake up radio, i.e. a transceiver that consumes almost no energy but can be used to indicate a planned transmission. Such solutions are still under investigation.[11] The major advantage of pseudo-asynchronous protocols is their simplicity. The code size is quite small, even ten times smaller than those of synchronous protocols, and they do not suffer from clock drift problems. However, as nodes send a long preamble or plenty of wake-up beacons before data transmission, it may lead to a high collision risk in many WSN scenarios. On the contrary, synchronous approaches deal with the collisions problem well thanks to TDMA schedule. However, such protocols suffer from the clock drift problem, and must precisely synchronize wake-up times of many nodes.

Currently, more stable solutions are based on MAC protocols that rely on a "rendezvous" principle in which sensor nodes agree on a specific time when to wake up for data exchange. Well known approaches to reduce energy consumption on the MAC layer are e.g. STEM (Schurgers et al. 2002), Dozer (Burri et al. 2007), solutions taking energy as parameter for routing decisions have as well been researched HEED (Younis and Fahmy 2004), EECMT (Shemshaki and Shahhoseini 2009), MR-Leach (Farooq et al. 2010). None of these solutions take Quality of Service into account, but monitoring applications such as those to be researched in SAID are requiring QoS e.g. in the sense of minimum latency etc. First steps in this direction have been researched and realized in the FP7 project

[11] www.aet-projekt.de.

WSAN4CIP in which we developed the DLDC-MAC protocol that can be tuned to guarantee certain latency (Brzozowski et al. 2009, 2010a, b, c, 2012). The routing layer can contribute to enhance the lifetime of a sensor network if it takes energy into account when selecting the routes. Here several energy aware routing protocols and metrics have been analysed by Stecklina et al. (2013). In BANs the routing layer is not really needed all nodes should reach each other directly. Therefore we will not provide details on routing here.

Even though many solutions have been proposed already, there are still some basic questions that always need to be considered by the application developer and system designer when it comes to efficient wireless (remote) monitoring applications.

First, at least one node needs to know the gateway to the internet except the gate can become part of the BAN, which might be the most convenient solution.

Second, nodes in a BAN need to learn who else is there and when do they awake or are listening respectively. Therefore coordination of communication activities is needed, which can be executed by some kind of master device (centralized approach) or by the nodes themselves (distributed approach). The latter can be realised by neighbourhood discovery protocols. These are more complex than the centralized approaches indeed, but allows for ease of use and self-set-up means that might become a very important usability issue. Then the sensor nodes stay awake for at least one sleep period and listen on the communication channel to detect all other BAN nodes. Based on that information, they agree on wake-up periods in dependence of the availability of the next hops or the receiving node. In ideal case each sensor node listens at one period during the sleeping time only.

Third, sensor nodes have to cope with overhearing, which means they may receive packets that are not addressed to them and hence processing them is useless and wastes resources not to mention that the communication channel is blocked. This problem does not longer exist if redundant data storage is used in the WSN (BAN) as introduced before. Then all nodes shall get measurement values and store them. However overhearing caused by other BAN's in the vicinity is still an open issue. The currently applied solutions do not fit, since they are meant for cooperating nodes in a common network. A potential approach to solve that may be shifting the sleep cycles in such a way to ensure the own BAN is sleeping while others are communicating, but that is still under research.

7.6 Open Issues

In summary, even with considering all mentioned aspects properly, there is much space left for potential improvements in hardware and software design of body area networks. For example power gating technologies for integrated circuits (Panic et al. 2008) may be facilitated to optimize power consumption e.g. of the microcontroller and the communication module. The focus here lies on minimising the internal power dissipation in times the devices are not used. The software can further be optimized up to certain extend when it is fully adapted to a single hardware platform and a single task rather than using a multi-purpose operating system. There even exist approaches where the operating system itself implements power management techniques, e.g. the IQLevel OS (Stecklina et al. 2013) where the driver implementations themselves select the deepest possible sleeping mode of components right on a single command.

Looking ahead, additional challenges will arise when the sensor nodes shall be implanted into the human body, which has already been investigated in some selected solutions such as defibrillators (Kao et al. 2010) and glucose monitoring (Fröhlich et al. 2012). However, it is quite obvious that such application has to deal with even more aggravated energy issues Basmer et al (2012) and the form factor of the senor node platform plays a very important role due to missing space inside the human body of course. Even with a fully integrated single chip sensor node, which would then feature smallest dimensions e.g. less than a 2 Euro coin (depending on its capabilities), the overall size will mainly be driven by the power consumption and hence, by the size of the battery. Nevertheless, the domain of implantable devices holds a lot more legal and biological restrictions in terms of device heating and communication. The heating of the device must be limited to around 1 °C during operation. In other words, the device temperature must not exceed 37.5 °C even if the normal body temperature yet is around 36 °C to protect from potential health risks. Also, there exist a couple of legal restrictions in particular for the use of wireless communication. In Germany, wireless communication of implantable devices is restricted to a certain mixed signal band around 403 MHz. This means, you cannot simply put some Bluetooth or any other widely used radio onto such platform, not to mention that communication in the 2.4 GHz band is useless since it will be blocked by water and other body liquids too.

Last but not least, bio stability issues need to be considered. Any kind of implantable device needs to cope with the non-ideal environment (from the technical point of view) of body liquids, blood and natural body defences of course. This may not only lead to processes harming the implanted device itself, e.g. by oxidising or short cuts, but may also cause unwanted reactions repelling the device in the end that can put the patient at serious risks. That does not only concern the sensor nodes but especially holds true for the sensing devices themselves since those most probably need to directly interfere with or contact to the body.

7.7 Conclusions

Wireless sensor nodes are lightweight and autonomous devices that can be applied for individualised sensing and health monitoring. Being used in small networks worn on a person's body, they enable the implementation of various remote health care applications. However, a lot of requirements have to be considered in WSN system design for e-health use. First, the very basic network architecture has to be determined. Centralised architectures are easier to implement but provide less flexibility and often feature single points of failures. In contrast to that, centralized architectures—in which all sensor nodes provide same or similar capabilities—are more reliable and fail-safe while in addition providing various self-X properties such as self-organisation, self-configuration and self-healing.

These mentioned basic considerations may be sufficient to make the application running properly, but nevertheless many more design challenges have to be included for e-health use of WSN. In such application area the running system needs to meet all technical and also legal demands of the health domain. That raises further critical design challenges in particular in view of reliability, security and privacy of the system. In addition, the holy grail for WSN design is the energy efficiency of the system since the whole set of features, the size and the weight of the sensor nodes and hence, the usability of the system depend on it. Especially if the latter is not sufficiently given, even a good working system may not be used by patients and clinicians. In this chapter we have presented several selected solutions that successfully tackle the introduced challenges. Finally, we are also aware of the fact that there still exist a lot of open issues and much space for future research as we have discussed at the end of the chapter.

References

Abdelzaher TF et al (2004) EnviroTrack: towards an environmental computing paradigm for distributed sensor networks. In: Proceedings of the 24th international conference on distributed computing systems (ICDCS 04), IEEE CS Press, pp 582–589

Aboelaze M, Aloul F (2005) Current and future trends in sensor networks: a survey. In: Proceedings of second IFIP international conference on wireless and optical communications networks WOCN, Dubai, pp 551–555

Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Comput Netw 38:393–422

Basmer T, Genschow G, Fröhlich M, Birkholz M (2012) Energy budget of an implantable glucose measuring system. Biomed Technol 57:259–262

Birkholz M et al (2009) Mikroviskosimeter zur kontinuierlichen Glucosemessung bei Diabetis mellitus. In: Proceedings of Mikrosystemtechnik-Kongress. VDE-Verlag, Berlin, 124p

Bohn J, Coroama V, Langheinrich M, Mattern F, Rohs M (2004) Living in a world of smart everyday objects—social, economic, and ethical implications. J Hum Ecol Risk Assess 10:763–786

Brzozowski M, Salomon H, Langendoerfer P (2009) Completely distributed low duty cycle communication for long-living sensor networks. In: Proceedings of the 2009 international conference on computational science and engineering (CSE '09), vol 2. IEEE Computer Society, Washington, DC, pp 109–116

Brzozowski M, Salomon H, Langendoerfer P (2010a) On efficient clock drift prediction means and their applicability to IEEE 802.15.4. In: Proceedings of the 2010 IEEE/IFIP international conference on embedded and ubiquitous computing (EUC '10). IEEE Computer Society, Washington, DC, pp 216–223

Brzozowski M, Salomon H, Langendoerfer P (2010b) ILA: idle listening avoidance in scheduled wireless sensor networks. In: Osipov E, Kassler A, Bohnert TM, Masip-Bruin X (eds) Proceedings of the eighth international conference on wired/wireless internet communications (WWIC'10). Springer, Berlin, pp 363–374

Brzozowski M, Salomon H, Langendoerfer P (2010c) Limiting end-to-end delays in long-lasting sensor networks. In: Proceedings of the eighth ACM international workshop on mobility management and wireless access (MobiWac '10). ACM, New York, NY, pp 11–20

Brzozowski M, Salomon H, Langendoerfer P (2012) Support for a long lifetime and short end-to-end delays with TDMA protocols in sensor networks. Paper presented at the International Journal of Distributed Sensor Networks, Article ID 651748

Burns A et al (2010) SHIMMER™—a wireless sensor platform for noninvasive biomedical research. IEEE Sens J 10(9):1527–1534

Burri N, Rickenbach P, Wattenhofer RR (2007) Dozer: ultra-low power data gathering in sensor networks. In: Proceedings of the sixth international conference on Information processing in sensor networks (IPSN ‘07). ACM, New York, NY, pp 450–459

Chang N, Zhang QY, Cungang Y (2007) A lightweight security protocol for wireless sensor networks. In: Proceedings of the international workshop on telecommunications—IWT/07

Chen T, Mazomenos E, Maharatna K, Dasmahapatra S, Niranjan M (2012) On the trade-off of accuracy and computational complexity for classifying normal and abnormal ECG in remote CVD monitoring systems. In: Proceeding of the IEEE workshop on signal processing systems (SiPS), Quebec, pp 37–42

ATMEL Corporation (2010a) AT91SAM9G20 preliminary. http://www.atmel.com/dyn/resources/prod documents/doc6384.pdf. Accessed May 2013

ATMEL Corporation (2010b) ATmega640/1280/1281/2560/2561 preliminary. http://www.atmel.com/dyn/resources/proddocuments/doc2549.pdf. Accessed May 2013

ATMEL Corporation (2011) ATmega128(L). http://www.atmel.com/dyn/resources/proddocuments/doc2467.pdf. Accessed May 2013

Costa P, Mottola L, Murphy AL, Picco GP (2007) Programming wireless sensor networks with the TeenyLIME middleware. In Proceedings of the eighth ACM/IFIP/USENIX international middleware conference (Middleware 2007), Newport Beach, CA, pp 26–30

Crosby SA, Wallach DS (2009) Efficient data structures for tamper evident logging. In: Proceedings of the 18th USENIX security symposium, Montreal, CA

Dikaiakos MD, Florides A, Nadeem T, Iftode L (2007) Location-aware services over vehicular ad-hoc networks using car-to-car communication. IEEE J Sel Areas Commun 25(8):1590–1602

Dyka Z, Langendoerfer P (2005) Area efficient hardware implementation of elliptic curve cryptography by iteratively applying Karatsuba’s method. In: Proceedings of design, automation and test in Europe, IEEE

Edwards J (2012) Wireless sensors relay medical insight to patients and caregivers [special reports]. IEEE Signal Process Mag 3(29):8–12

Farooq MO, Dogar AB, Shah GA (2010) MR-LEACH: multi-hop routing with low energy adaptive clustering hierarchy. In Proceedings of the 2010 Fourth international conference on sensor technologies and applications (SENSORCOMM ‘10). IEEE Computer Society, Washington, DC, pp 262–268

Fröhlich M et al (2012) Biostability of an implantable glucose sensor chip. IOP Conf Ser Mater Sci Eng 41:012022

Gellersen HW, Schmidt A, Beigl M (2000) Adding some smartness to devices and everyday things. In: Proceedings of third IEEE workshop on mobile computing systems and applications, Monterey, CA, pp 3–10

Gillies D, Thornley DJ, Bisdikian C (2009) Probabilistic approaches to estimating the quality of information in military sensor networks. Comput J

Girao J, Westhoff D, Mykletun E, Araki T (2007) Tinypeds: tiny persistent encrypted data storage in asynchronous wireless sensor networks. Ad Hoc Netw J 5(7):1073–1089

Gummadi R, Gnawali O, Govindan R (2005) Macro-programming wireless sensor networks using kairos. In: Proceedings of the international conference on distributed computing in sensor systems (DCOSS 05), LNCS 3560, Springer, Heidelberg, pp 126–140

Halperin D et al. (2008) Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: Proceedings of IEEE symposium on security and privacy, Washington, DC, pp 129–142

Heuschmann PU et al (2010) Schlaganfallhäufigkeit und Versorgung von Schlaganfallpatienten in Deutschland. Aktuelle Neurol 7:333–340

Hoon CL (2009) Practical broadcast authentication using short-lived signatures in WSNs. Information security applications, Lecture Notes in Computer Science 5932:366–383

Kahn JM, Katz RH, Pister KSJ (1999) Next century challenges: mobile networking for “smart dust”. In: Proceedings of international conference on mobile computing and networking (MOBICOM), Seattle, pp 271–278

Kahn JM, Katz RH, Pister KSJ (2000) Emerging challenges: mobile networking for smart dust. J Commun Netw 2(3):188–196

Kao CW, Friedmann E, Thomas SA (2010) Quality of life predicts one-year survival in patients with implantable cardioverter defibrillators. Qual Life Res 19(3):307–315

Karlof C, Sastry N, Wagner D (2004) TinySec: a link layer security architecture for wireless sensor networks. In: Proceedings of the second international conference on embedded networked sensor systems, Baltimore, MD, Nov 2004, pp 162–175

Kirchhof P, Adamou A, Knight E, Lip GYH, Norrving B, de Pouvourville G (2009) How can we avoid a stroke crisis? ISBN 978-1-903539-09-5

Lab-on-Chip-System (2011) Lab-on-Chip-System. Medizin&Technik, http://www.medizin-und-technik.de/home/-/article/27544623/35089533?returnToFullPageURL=back. Accessed May 2013

Liang CJM, Terzis A (2008) Koala: ultra-low power data retrieval in wireless sensor networks. In: Proceedings of the seventh international conference on Information processing in sensor networks. IEEE Computer Society

Lin E-YA, Rabaey JM, Wolisz A (2004) Power-efficient rendez-vous schemes for dense wireless sensor networks. In: IEEE international conference on communications, vol 7, Enschede

Maaser M, Ortmann S (2010) Remote medical treatment at home using the using the Java mobile sensor API. In: Proceedings of the third international workshop on smart homes for tele-health (SmartTel ‘10), Miami, USA

Madden SR, Franklin MJ, Hellerstein JM, Hong W (2005) TinyDB: an acquisitional query processing system for sensor networks. ACM Trans Database Syst 30(1):122–173

Mainwaring A, Culler D, PolastreJ, Szewczyk R, Anderson J (2002) Wireless sensor networks for habitat monitoring. In: Proceedings of the first ACM international workshop on wireless sensor networks and applications (WSNA ‘02). ACM, New York, NY, pp 88–97

Marvel (2010) PXA27x Specification update. http://www.marvell.com/products/processors/applications/pxafamily/pxa27x emts.pdf. Accessed April 2013

Morchon OG, Falck T, Heer T, Wehrle K (2009) Security for pervasive medical sensor networks. In: Proceedings of sixth annual international conference on mobile and ubiquitous systems (MobiQuitous 2009), Toronto, Canada

Naqvi S, Dallons G, Michot A, Ponsard C (2010) Assuring privacy of medical records in an open collaborative environment—a case study of Walloon Region™ eHealth platform. Privacy and identity management for life, vol 320. Springer, Berlin, pp 146–159. ISBN:978-3-642-14281-9. http://dx.doi.org/10.1007/978-3-642-14282-6_12

Ortmann S, Maaser M (2011) Enabling secure and privacy-aware mobile sensing and e-health applications on everybodys smartphone. In: First IEEE international conference on consumer electronics-Berlin (ICCE-Berlin 2011), Berlin

Ortmann S, Maaser M, Parandian B, Schultz M (2011) Telemedizinisch assistierte ambulante Betreuung von Patienten, vol 4. Deutscher AAL-Kongress, Berlin

Ortmann S, Langendoerfer P, Sik-Lanyi C (2012) Telemedical assistance for ambulant rehabilitation of stroke patients. In: Proceedings of the ninth world congress on brain injury, Edinburgh, Scotland

Panic G, Dietterle D, Stamenkovic Z (2008) Architecture of a power-gated wireless sensor node. In: Proceedings of 11th EUROMICRO conference on digital system design architectures, methods and tools (DSD’08), IEEE, Parma

Panic G, Basmer T, Schrape O, Peter S, Vater F, Tittelbach-Helmrich K (2011) Sensor node processor for security applications. In: Proceedings of the 18th IEEE international conference on electronics, circuits and systems (ICECS 2011), Beirut

Park T, Shin KG (2004) LiSP: a lightweight security protocol for wireless sensor networks. ACM Trans Embed Comput Syst 3(3):634–660

Patel et al (2012) A review of wearable sensors and systems with application in rehabilitation. J Neuroeng Rehabil 9(12):1–17

Perrig A, Szewczyk R, Wen V, Culler D and Tygar JD (2001) SPINS: Security protocols for sensor networks. In: Proceedings of seventh annual international conference on mobile computing and networking, Rome, Italy, Aug 2001, pp 188–189

Piotrowski K, Langendoerfer P, Peter S (2009) tinyDSM: a highly reliable cooperative data storage for wireless sensor networks. In: Proceedings of the 2009 international symposium on collaborative technologies and systems (CTS '09), Washington, DC, pp 225–232

Piotrowski K, Sojka A, Langendoerfer P (2010) Body area network for first responders: a case study. In: Proceedings of the fifth international conference on body area networks (BodyNets '10), ACM, New York, NY, pp 37–40. doi:10.1145/2221924.2221933

Polastre J, Hill J, Culler D (2004) Versatile low power media access for wireless sensor networks. In: Proceedings of the second international conference on embedded networked sensor systems. ACM, New York

Robinson P, Beigl M (2003) Trust context spaces: an infrastructure for pervasive security in context-aware environments. In: Proceedings of first international conference of security in pervasive computing. Springer, Berlin, pp 157–172

Sandler D, Derr K, Crosby S, Wallach DS (2008) Finding the evidence in Tamper-Evident logs. In: Proceedings of third international workshop on systematic approaches to digital forensic engineering (SADFE '08), Berkeley, pp 69–75

Scheffler T, Schindler S, Lewerenz M, Schnor B (2011) A privacy-aware localization service for healthcare environments. In: Proceedings of the fourth international conference on pervasive technologies related to assistive environments (PETRA '11). ACM, New York

Schurgers C, Tsiatsis V, Ganeriwal S, Srivastava M (2002) Optimizing sensor networks in the energy-latency-density design space. IEEE Trans Mob Comput 1:70–80

Shaikh, R. A., Lee, S., Khan, M. A., & Song, Y. J. (2006). LSec: Lightweight security protocol for distributed wireless sensor network. In Personal Wireless Communications (pp. 367–377). Springer Berlin Heidelberg.

Shemshaki M, Shahhoseini HS (2009) Energy efficient clustering algorithm with multi-hop transmission. In: Proceedings of the 2009 international conference on scalable computing and communications; eighth international conference on embedded computing (SCALCOM-EMBEDDEDCOM '09). IEEE Computer Society, Washington, DC, pp 459–462

Sojka A, Piotrowski K, Langendoerfer P (2010) ShortECC: a lightweight security approach for wireless sensor networks. In: Proceedings of INSTICC international conference on security and cryptography, SECRYPT

Stecklina O, Langendoerfer P, Goltz C (2013) A fair energy trade multi-hop routing in wireless sensor networks. In: Proceedings of the sixth joint IFIP wireless & mobile networking conference (WMNC2013), Dubai

Sun T, Chen LJ, Han CC, Gerla M (2005) Reliable sensor networks for planet exploration. In: Chen LJ (ed) Proceedings of IEEE networking, sensing and control, Tucson, USA, pp 816–821

Texas Instruments Inc. (2007a) 2.4 GHz IEEE 802.15.4 / ZigBee-Ready RF Transceiver. http://www.ti.com/lit/gpn/cc2420. Accessed May 2013

Texas Instruments Inc. (2007b) 2.4 GHz IEEE 802.15.4/ZIGBEE RF TRANSCEIVER. http://www.ti.com/lit/gpn/cc2520. Accessed May 2013

Texas Instruments Inc. (2007c) Single-chip very low power RF transceiver. http://www.ti.com/lit/gpn/cc1000. Accessed May 2013

Texas Instruments Inc. (2009) Low-cost low-power 2.4 GHz RF transceiver. http://www.ti.com/lit/gpn/cc2500. Accessed May 2013

Texas Instruments Inc. (2010a) CC1101 low-power Sub-1 GHz RF transceiver. http://www.ti.com/lit/gpn/cc1101. Accessed May 2013

Texas Instruments Inc. (2010b) CC430F613x, CC430F612x, CC430F513x MSP430 SoC with RF core. http://www.ti.com/lit/gpn/cc430f6137. Accessed May 2013

Texas Instruments Inc. (2010c) MSP430F543xA, MSP430F541xA Mixed signal microcontroller. http://www.ti.com/lit/gpn/msp430f5438a. Accessed May 2013

Texas Instruments Inc. (2011) MSP430F15x, MSP430F16x, MSP430F161x mixed signal microcontroller. http://www.ti.com/lit/gpn/msp430f1611. Accessed May 2013

Ugus O et al (2009) Optimized implementation of elliptic curve based additive homomorphic encryption for wireless sensor networks. arXiv preprint arXiv:0903.3900

Uhsadel L, Poschmann A, Paar C (2007) Enabling full-size public-key algorithms on 8-bit sensor nodes. Security and privacy in ad-hoc and sensor networks. Springer, Berlin, pp 73–86

Wei Y, Heidemann J, Estrin D (2002) An energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of the twenty-first annual joint conference of the ieee computer and communications societies (INFOCOM 2002), vol 3, IEEE, New York

Weiser M (1991) The computer for the twenty-first century. Sci Am 265(3):66–75

Werner-Allen G, Johnson J, Ruiz M, Lees J, Welsh M (2005) Monitoring volcanic eruptions with a wireless sensor network. In: Proceedings of the second European workshop on wireless sensor networks, Istanbul, pp 108–120

Westin AF (1967) Privacy and freedom. Atheneum, New York

Yao Y, Gehrke JE (2002) The cougar approach to in-network query processing in sensor networks. ACM Sigmod Rec 31(2):9–18

Younis O, Fahmy S (2004) HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans Mob Comput 03(4):366–379