International Telecommunication Union

ITU-T Technical Paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(28 February 2014)

SERIES Y.2000:
NEXT GENERATION NETWORKS

Applications of Wireless Sensor Networks in Next Generation Networks

International Telecommunication Union

Foreword

This Technical Paper is developed by Messrs. Valery Butenko, Anatoly Nazarenko, Viliam Sarian, Nikolay Sushchenko and Aleksandr Lutokhin.

Abstract

Wireless sensor networks (WSNs) are one of the most rapidly developing information technologies and promise to have a variety of applications in Next Generation Networks (NGNs).

The major goal of this technical paper is to give recent advances and state-of art results covering both fundamental principles and use cases of WSNs in NGNs. This technical paper presents design techniques and guidelines, overview of existing and emerging standards for the subject area, modeling principles for WSNs. It gives also a comprehensive reference to ITU-T developments concerning WSNs, including Ubiquitous Sensor Networks (USNs), sensor control networks (SCNs), machine-oriented communications (MOC) concerns. In addition, this technical paper covers important particular issues: efficiency estimation and application of WSNs for critical tasks such as emergency management and healthcare.

This technical paper should appeal to ITU-T contributors working on NGNs development, researchers, networking designers, engineers and graduate students interested in WSNs.

Table of contents

Preface

The following technical paper is concerned with such rapidly developing information and communication technologies (ICT) directions as Next Generation Networks (NGNs), Wireless Sensor Networks (WSNs), as well as their convergence. Specialists from study groups of International Telecommunication Union, Telecommunication Standardization Sector (ITU-T) examine new contributions on different NGNs and WSNs aspects every ITU-T meeting. The *Internet of Things* (IoT) has become the most potential catalyst of this convergence, and has also become the object of global standardization.

So, due to NGNs, WSNs and IoT, ICT got a new point of development. Besides, it got a new way of cardinal increase of human's adaptive capacities in case of facing the globalizing world with declining human-made environment. With the help of intellectual customer devices (e. g., computers, mobile phones, etc.), the extension of inter personal informational communication led to interaction between items and the natural environment, if equipped with relevant soft- and hardware. That leads to clear and longstanding perspective, which is very attractive for businessmen and specialists, as it allows developing all the ICT directions further.

The discussed convergence processes have set the additional vector of development for other actively developing and still quite independent ICT directions. Among them, there are radio-frequency identification (RFID), "smart car" and "smart house" projects, mechatronics, etc. Such circumstance is very important for global world creation and also for elaborating such world's standards.

The following statement is becoming generally accepted: the development and inoculation of NGNs, WSNs and IoT convergent solutions, as well as "drawing in" the impressive leap-ahead results in the area of cognitive and nanotechnologies (connected with inorganics and bioorganics convergence — i. e., the integration of modern technologies abilities and nature-made formations), marks a new qualitative step in the building of the unified *information and communication environment* and a new stage in further creation of the global *information society*.

Every ICT specialist often has to face different terms and concepts concerning modern society and the problems it has or will have in the future. We'd like to touch up just a few of them, such as:

- Cognitive revolution, which scale is being compared with the informational revolution;
- Risk society;
- Knowledge society;
- Decrease in non-renewable resources;
- "Green" ICT;
- The new Sixth Technological Order;
- Social claims, such as the decisions on social issues of the improvement of living standards with phasing-out *"digital gap"*, etc.

We'd like to mention, that though these terms and concepts are complementary, their connection with ICT development is not always obvious, and sometimes special explanations are requested.

Having so many materials and directions and being limited by the size of this technical paper, the authors meet a hard task to find the criteria for setting up and selecting the materials. Another task is to find the way of extending their "longevity" somehow. For the main contents, the authors have selected long-time relevant descriptions of decisions, methods, protocols and standards.

Nowadays, the global society is making the first step to the new *technological order* (TO), the sixth one [1]. Any TO is formed by a cluster of its basic innovations. Basically, there are nanotechnologies, biotechnologies, genetic engineering, cognitive and info communication

technologies that will provide the intercommunication of a huge number of objects. Besides human machine and machine systems, there will be milliards of new objects among them — the objects of IoT. The sixth TO will modify the objective world, but also the relationships between people by changing the structures of the modern global society's institutional matrix. In comparison with the previous technological orders, the advantages of the sixth TO are individual production and individual consumption development (while preserving the advantages of mass production technologies), the raise of production's flexibility, sharp decrease in power-consuming and materials consumption and the construction of materials and organisms with preset qualities.

There is one more expected and most important point in the new TO that should be mentioned — the progress in the production, distribution and accounting of human activities will lead to service sector as the main transforming factor of the society.

According to the results of the authors' research, transferring to the individualization of public IC services will become an important characteristic for the sixth TO. This will not only demand for radical changes in the IC services contents, but also supposes the inclusion of a new element in the IC infrastructure. This element is *individualized decision support services*. This point has become the basement for a new WSN category — *sensor control networks* (see Section 6.4).

The individualized decision support service is able to extend the areas of personal contentment and safety regarding to wide life domains. The loss of control that many of us feel in regard to some life circumstances is quite objective, unless these decision support systems are implied.

Due to the ICT development, our way of life will cardinally change in the 20 years to come. Powerful embedded microchips will raise the level of systems' intellect, and cloud computing guarantees the growth of its effectiveness. Moreover, further integration will erase the technologies' boundaries.

To avoid enormous losses, the move to the sixth TO shouldn't last too long and shouldn't happen spontaneously. To achieve this goal, a rational cross-subject strategy for the service market organization is to be elaborated. This should be definitely done with the support of state structures. The aim of this strategy is to provide a rational integration of separate innovative technologies that would be included into the new TO.

That's what the ITU (and mostly ITU-T) is promoting by working on the proper Recommendations.

Chapter 1
Introduction to Wireless Sensor Networks

1.1 History

It is possible to say that history of sensor network technology originates in the first distributed sensing idea implementations. The continuous work of researchers and engineers over sensor networks which lately became wireless sensor networks (WSNs) has started exactly with this idea. Like many other technologies, distributed sensing was firstly introduced by the military. The first system which has all the characteristics of sensor networks (distribution, hierarchical data processing system) is *Sound Surveillance System* (SOSUS), which was made to detect and track submarines. SOSUS consisted of the acoustic sensors (hydrophones) settled on the ocean bottom [2].

In 1980s Defense Advanced Research Projects Agency (DARPA) is working over *Distributed Sensor Networks* (DSN) program [3 ,2]. The main task of the program was to test applicability of a new approach to machine communications, introduced for the first time in Arpanet (predecessor of the Internet). The task of researchers was to engineer a network of area-distributed sensors. At the same time, sensors had to be inexpensive, work autonomously and exchange data independently. Such demands are still made for developing sensor networks for modern applications. Hence, it is possible to say that the DARPA research was a base for modern WSNs. A sensor network of acoustic sensors tracking aircrafts appeared as a result of collaboration of researchers from Carnegie Mellon University (CMU), Pittsburgh, PA, and Massachusetts Institute of Technology (MIT), Cambridge. For a demonstration there was a platform made to passively detect and track low-flying aircraft. Connection between mobile nodes and a central computer was implemented through wireless transmission channel. Certainly, this system included not so many wireless nodes, and it was necessary to transport mobile nodes in the lorries, also system was able to track only low-flying objects with simple trajectory in rather short distance [4]. However, this work was well in advance of that time and gave a considerable impetus to sensor networks developing.

But for practical use distributed sensing with a great number of sensor nodes is of much more interest. The first steps to creating such systems were the following projects: *Wireless Integrated Network Sensors* (WINS), which started in 1993, and *Lowpower Wireless Integrated Microsensors* (LWIM), which started in the mid-1990s.

WINS combine sensor technology, signal processing, computation, and wireless networking capability in integrated systems [5]. The project was carried out in the University of California at Los Angeles in collaboration with the Rockwell Science Center. The project elaboration included working over various aspects of WSNs: sensing elements (*micro-electro-mechanical system (MEMS) sensor*), closer integration between transceiver and other elements in order to reduce the size, signal processing points, network protocol design. The researchers have aimed at distributed network and Internet access to sensors. The network from WINS supported a great number of sensor nodes with small transceiver coverage area and low-speed data transmission (1-100 kbps) [6]. The first WINS devices had been demonstrated in 1996, and then work continued as the project WINS NG (new generation).

Sensor node's hardware platform, worked out in the framework of the WINS project, included sensitive element, analog-to-digital converter, spectrum analyzer, buffer memory. This platform was meant for continuous measurements. In addition to that, sensor nodes included digital signal processor and low power transceiver. All the sensor node's components mentioned above have been worked out with tight restrictions on energy consumption, because every sensor node's supply was provided by a simple Li-Ion battery which had a diameter 2.5 cm [7], wherein the sensor nodes had to be working on one battery for a long time. Such an efficient energy use was achieved by reducing

speed of signal processing, decreasing sensor nodes connection range, reducing radio channel data throughput, applying MEMS and CMOS (*Complementary metal–oxide–semiconductor*) technologies for sensing elements and integration circuits production, and also by reducing the demands on WSN response delays.

WINS technologies have offered the brand-new opportunities for distributed sensing and controlling. A range of low-power integrated circuits have been worked out: interface, signal processing and communicative circuits. Its results allowed the researchers to create a great number of new ways to use WSNs for both military and civil tasks.

The LWIM project by University of California at Los Angeles (UCLA) was funded by DARPA [8]. The aim of the project was to create low-power wireless sensor network modules. Researchers wanted to work out compact wireless measurement devices that may be installed immediately and anywhere. As a result a module was created which included vibration sensor, infrared sensor, low power transceiver which provided communication range in 30 m, data transmission speed about 1 kbps [9]. The possible transceiver's frequency range was 902-928 MHz. The supposed fields for developed modules were monitoring and control applications: manufacturing processes (wireless presence monitoring), vehicle condition monitoring (wireless motor maintenance), medicine (wireless patient monitoring), defense (size reduction).

Elaborations in the framework of *SensIT* project gave new opportunities for WSNs. WSNs became interactive and programmable, and this gave a possibility to make demands and change tasks dynamically. A multitasking feature in the system allows multiple simultaneous users. Also, short distances between sensor nodes reduce distance between threat object and the nearest sensor node, improving the accuracy of the target identification and tracking. The system was designed in such a way which made both software and hardware able to support energy-saving functioning, short term response, autonomy and high survivability.

SensIT developers and researchers have conducted two experiments in 2000 and 2001. The U.S. Marine Corps took the part in those experiments. The aim of them was to check collaborative signal processing capabilities at the Marine Corps Air Ground Test Facility at Twentynine Palms, California. As a result of the SensIT project, sensor nodes supporting targets detection, identification and tracking have been produced. Also the network had an additional function of connectivity on the battlefield.

Another important development work in the WSN field was the study of the University of California at Berkeley, which had started PicoRadio [10] program in 1999. The goal of the program was to support the assembly of an ad hoc (application specific) WSN of low-cost, low-energy sensor nodes, able to operate on the natural sources of energy, such as solar energy. Development started not with hardware, as usually, but with software, what made it possible to provide the platform flexibility for various applications due to extensive opportunities of PicoRadio protocol. [11].

It is worth mentioning that Berkeley was also working over one more elaboration — *"Smart Dust"* program. The goal of this program was to create unusually small sensor nodes which could be dropped from the air like the dust, could move with air masses and cooperate during a few hours or days. The authors of the project planned to integrate a sensor, laser diode and MEMS mirror in a single compact MEMS case in order to receive and transmit optical radiation [12].

Within the framework of this project the ways of data transmitting with the help of the light rays reflected from the micromirror have been developed and tested. The following results were achieved: temperature, humidity, barometric pressure, light intensity, tilt and vibration, and magnetic field sensors all in a cubic inch package, including the bi-directional radio, the microprocessor controller, and the battery, 20 meter communication range, one week lifetime in continuous operation, 2 years with 1% duty cycling [13]. This project finished in 2001, but many additional projects have grown out of it. Among these are: Berkeley Webs, Network of Embedded

Systems (NEST), Center for Embedded and Networked Sensing at UCLA.

In 1999 Massachusetts Institute of Technology (MIT) has set to work over AMPS project (*micro-Adaptive Multidomain Power-aware Sensors*). The project includes a whole range of challenging issues in design and implementation of WSNs [14]. The researches focuses on low-power hardware and software components for sensor nodes, including the use of microcontrollers capable of dynamic voltage scaling and techniques to restructure data processing algorithms to reduce power requirements at the software level [15]. Two key elements drive μAMPS project [14]:

- To achieve a satisfactory lifetime, an extreme focus needs to be placed on energy efficiency, both at the level of the individual sensor nodes and of the entire network;
- Unattended operation under hard to control conditions requires intelligence that is pushed far into the network, allowing self-configuration, reconfigurability and flexibility.

In the framework of the project it was planned to work out two versions of sensor nodes: μAMPS-I and μAMPS-II. The latter had to be based on *application-specific integrated circuit* (ASIC) and operate on novel system architectures and design techniques to achieve the desired energy efficiency and reconfigurability.

A result of this work was the elaboration of a sensor network communication protocol, which was named *Low Energy Adaptive Clustering Hierarchy* (LEACH). The main feature of LEACH is node-clustering algorithm, which randomly distributes the functions of the network's coordinator node. Since the coordinator node is the main power consumer in WSN, random giving a role of the coordinator node to different sensor nodes aligns energy consumption among the WSN. And this, in turn, increases the lifetime of LEACH WSN, if we compare it with WSNs managed by other protocols, where the coordinator node is permanent and runs down the battery faster than other nodes; as a result, such WSNs fail and their lifetime is decreasing.

In the beginning of 2000s Institute of Electrical and Electronics Engineers (IEEE) have released the first version of IEEE 802.15.4 standard "*Low-Rate Wireless Personal Area Networks*", developed especially for low-power devices [16]. Nowadays the standard has been significantly extended and revised for a few times. This standard regulates construction of low levels of sensor node protocols, which are the *physical level* and *medium access control* level. The higher levels (from *network layer* to *application layer*) are regulated by other standards additional to this one.

All these benefits in combination with excellent technical characteristics of IEEE 802.15.4 transceivers caused appearance of numerous standards which used IEEE 802.15.4 as a low level. Among these standards we can mention ZigBee [17], WirelessHART [18], and 6loWPAN [19] (IPv6 over Low power Wireless Personal Area Networks), and each of them, in turn, offers own solution for WSNs. Herewith, the last offers an implementation of a WSN based on IP protocol.

Special attention should be given to ZigBee which is the most widely used standard for WSNs. ZigBee is a suite of high level communication protocols used to create personal area networks, developed by the ZigBee Alliance (group of companies that maintain and publish the ZigBee standard). ZigBee builds upon the physical layer and media access control layers defined in IEEE 802.15.4 standard. The most part of sensor nodes producers have ZigBee modules in their product lines.

The history of WSN has a lot of discoveries, trials and tasks still unsolved. But the researches of academic organizations which took place in 1990s – the beginning of 2000s allowed to achieve the current level of WSN availability and flexibility.

1.2 General information

1.2.1 Definitions

In the ITU-T Recommendation Y.2221 [20] there is the following definition of sensor network and sensor node.

Sensor network: A network comprised of interconnected sensor nodes exchanging sensed data by wired or wireless communication.

Sensor node: A device consisting of sensor(s) and optional actuator(s) with capabilities of sensed data processing and networking.

Sensor node consists of a great number of nodes of the same type (sensor nodes), which are spatially distributed and cooperate with each other. Each such node has a sensing element (sensor), a microprocessor (microcontroller), which process sensor signals, a transceiver and an energy source. Distributed over the object, sensor nodes with the necessary sensors make it possible to gather information about the object and control processes which take place on this object.

1.2.2 Overview of applications

From the point of view of practical application, WSNs offer unique opportunities for monitoring and data collecting from a number of spatially distributed sensor nodes. In addition to providing distributed sensing of one or a few parameters of a big object like a building or open space, WSNs also allow to control the processes in the object.

For example, WSN may be installed in a building for automatic control of load-bearing constructions' conditions. For this reason engineers determine the places on the building most appropriate for data measuring. In these places autonomous sensor nodes with necessary sensing elements are installed. After installation they start to interact and exchange data. Receiving these data from the sensor nodes and comparing measurement data from each of the sensor node with its position, building structure specialists can in real time mode supervise, control and predict emergency situations.

For the last twenty years researchers groups and industry representatives have been showing a lot of interest in WSNs. This interest is caused by the fact that WSN applications are highly promising and help to solve a wide range of problems which are to be described below. Also, technological progress in the microelectronics made it possible to produce rather small, productive, energy effective and cheap sensor nodes, and it allows to introduce and use advantages of WSN technology everywhere and right now.

WSNs technologies started to actively develop in mid 1990s, and in the beginning of 2000s the microelectronics development made it possible to product rather inexpensive elementary base for sensor nodes. It also became possible due to the rapid development of wireless technologies and microelectromechanical systems. Constant wireless devices price decreasing, their operating parameters improving make it possible to gradually migrate from using wireline technologies in telemetric data collecting systems, remote diagnostics techniques, data exchange. A lot of branches and market segments (production, constructing, different types of transport, life support, security, warfare) are interested in WSNs deployment, and their number is permanently increasing. It is caused by technological processes complication, production development, increased needs in security field and resources use control. In emergency management, sensor nodes can sense and detect the environment to forecast disasters before they occur. In biomedical applications, surgical implants of sensors can help monitor a patient's health. For seismic sensing, ad hoc deployment of sensors in volcanic areas can detect occurrence of earthquakes and eruptions [21]. With the development of semiconductor technology there are new WSNs practical applications appearing in industry, household and also in military field. The usage of inexpensive wireless sensor devices for remote monitoring opens up new fields for telemetry and control systems applications, such as:

- Military target tracking and surveillance [22 ,23];
- Timely detecting of possible mechanism failure, when controlling such parameters as vibration, temperature, pressure, etc. (see Section 3.4);
- Control of access to remote monitoring object systems in real time mode;
- Buildings and constructions condition control automation (see Section 3.3);
- Smart house (see Section 3.2);
- Energy saving and resource saving (see Section 3.4);
- Biomedical health monitoring [24 ,25] (see also Section 5.4 and Section 6.5);
- Ecological parameters of environment control;
- Natural disaster relief [26] (see also Section 5.2);
- Hazardous environment exploration and seismic sensing [27] (see also Section 3.4).

1.2.3 Overview of engineering problems

While choosing or developing a WSN platform for particular application, developers make a rather wide range of demands to the sensor nodes. Generally, high demands for autonomy, cost and size are made. These and others technical requirements often can be contradictory. For example, increasing in power of sensor node's transmitter leads to increasing of energy consumption and decreasing of autonomy, causing a bad influence on WSN lifetime. At the same time, WSNs (unlike other kinds of networks) have some rigid restrictions, such as a limited amount of energy, short communication range, low bandwidth, and limited processing and storage in each sensor node. Also, WSN has to be sustainable to elements failures, support self-organization; moreover, sensor nodes have not to require service and special installation. So, finding a balance between demands which are made and sensor nodes' cost is a very special task for each specific application.

It is possible to improve WSN technical characteristics without significant increasing of its cost only by means of technologies development. There are certain researches aimed for improving existing WSNs characteristics and technologies, and also expanding their field of application. These researches are being conducted in the following directions:

- Development of the new sensing elements which are inexpensive, low-power, have low noise level and small size;
- Integrating sensors and signal processing circuits;
- Integrating sensors into sensors arrays in order to reduce inherent noise;
- Development of sensor nodes able to process signals and having different communication radio interfaces;
- Integrating WSNs into information systems in order to provide new services;
- Development of the new communication protocols which improve reliability and sustainability to interferences, distributed data processing algorithms, synchronization algorithms, sensor nodes spatial positioning methods, algorithms of energy-effective data exchange in the network.

In addition to technical challenges related to sensor node design, there are other problems to be solved in WSN field. They arise when a WSN has a great number of sensor nodes.

Network deployment. Reliable connection between the nearest nodes is necessary to provide normal operation of the network. So the distance between the nearest nodes should not exceed a

certain value. If WSN is deployed on an infrastructural object, this condition is feasible due to the fact that this deployment is made by means of embedding every mote to a certain specific place. In this way it is possible to tune a location if there are some communication problems. But deployment of such a system requires more time. A lot of WSN applications in agriculture, environment monitoring and emergency management are deployed in the places without any specially prepared infrastructure, and require easier and more rapid ways of sensor node installation. In the most cases under these circumstances dissemination (e. g., scattering, dropping) of sensor nodes with the help of some moving vehicle, such as car, airplane etc. is used. In such cases sensor nodes get in rather difficult conditions, and establishing connection with other sensor nodes is not easy. Thus, successful WSN deployment depends on both the hardware characteristic and the network self-organization protocols which are used.

Unattended operation. The major part of applications requires operation of WSN during the whole lifetime without human intervention. This requirement is natural because of the great number of sensor nodes. Under these circumstances maintenance of WSN would have been very labor-intensive. In addition, some applications don't make it possible to detect the precise location of the sensor node which needs service. Being developed, unattended operation requires using of reliable hardware components and protocols, resistant to noise and errors. Sensor nodes themselves are responsible for reconfiguration in case of any changes.

Autonomy. Sensor nodes are not connected to any energy source. So network lifetime depends on economical and effective use of energy efficiency by each sensor node. In WSN the most part of energy is consumed by data reception and transmission, so the key energy-saving technique is finding a balance between reducing the amount of transmitted data and necessity to ensure the WSN integrity.

Reliability. Self-organization is the main characteristic of WSN. It was the ability of modern WSN for self-organizing what has become the key factor which made it possible to design WSNs with thousands of nodes. Also, self-organizing allows WSN to save the integrity if connection between some nodes is suddenly lost. It makes WSN more reliable. New approaches to WSN using include integration of WSNs with converged communication networks for providing services to a wider range of customers. Because of this fact many other tasks are becoming relevant, such as administration of services in WSNs.

Chapter 2
Implementation details of WSNs

2.1 Architectures

2.1.1 Overview of the network architecture

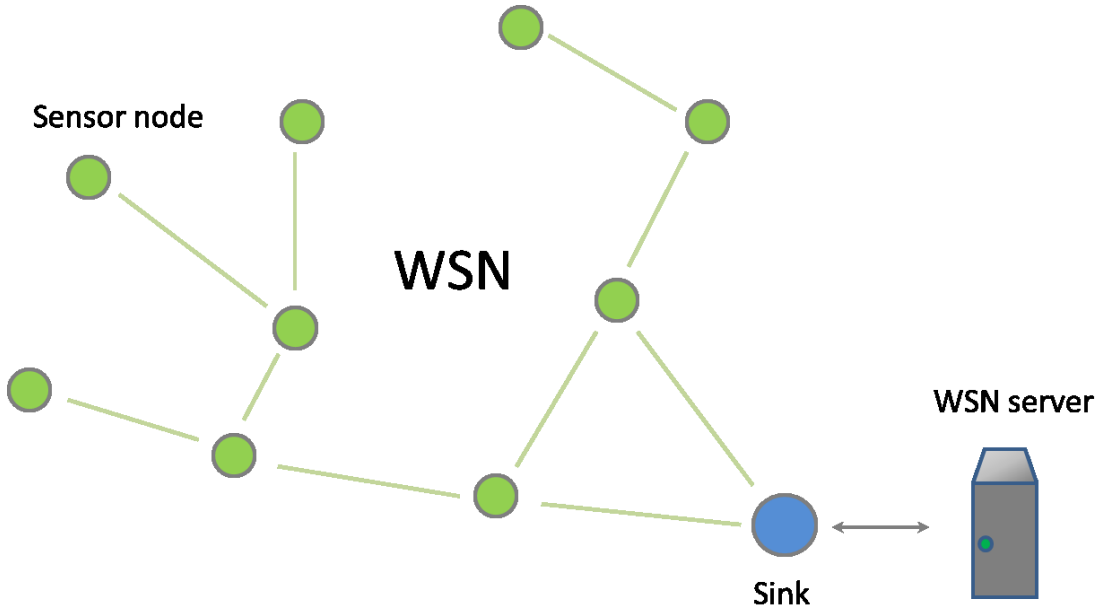

Figure 2.1: An example of a WSN

WSNs are spatially distributed systems which consist of dozens, hundreds or even thousands of sensor nodes, interconnected through wireless connection channel and forming the single network. Figure 2.1 represents an example of a WSN. Here we can see a WSN which consists of twelve sensor nodes and a *network sink*, which also functions as a *gate*. Each sensor node is a device which has a transceiver, a microcontroller, and a sensitive element (Figure 2.2). Usually sensor node is an autonomous device. Each sensor node in WSN measures some physical conditions, such as temperature, humidity, pressure, vibration, and converts them into digital data. Sensor node can also process and store measured data before transmission. Network sink is a kind of a sensor node which aggregates useful data from other sensor nodes. As a rule, network sink has a stationary power source and is connected to a *server* which is processing data received from WSN. Such connection is implemented directly, if server and WSN are placed on the same object. If it is necessary to provide a remote access to WSN, network sink also functions as a gate, and it is possible to interact with WSN through global network such as the Internet.

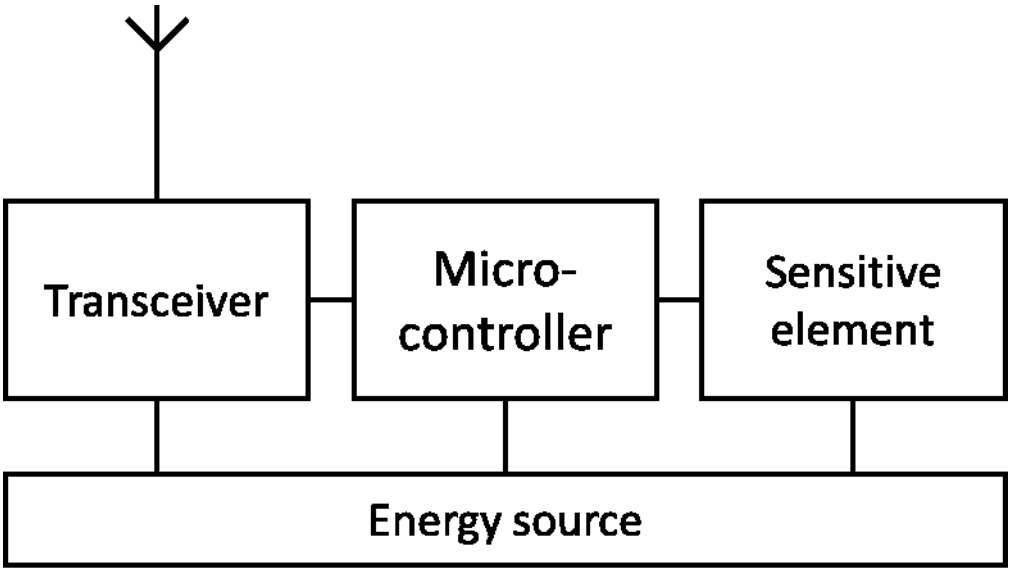

Figure 2.2: Sensor node inner structure

In WSNs communication is implemented through wireless transmission channel using low power transceivers of sensor nodes. Communication range of such transceivers is set up in the first place for reasons of energy efficiency and density of nodes spatial disposition, and, as a rule of thumb, this quantity is about a few dozens meters. Sensor node's transceiver has limited energy content, and this fact makes it impossible for the most spatially remote sensor nodes to transmit their data directly to the sink. So, in WSN every sensor node transmits its data only to a few nearest sensor nodes which, in turn, retransmit those data to theirs nearest sensor nodes and so on. As a result, after a lot of retransmissions data from all the sensor nodes reach the network sink.

Inside the sensor node a microcontroller (more precisely, its firmware) accounts for data collecting and connection with other sensor nodes. Microcontroller firmware has a set of algorithms to control the transceiver and the sensing element. These algorithms make it possible to provide sensor node functioning. At the same time, in addition to data collecting and transmitting their own measurements, sensor nodes takes a part in data transmission from other remote sensor nodes, i. e. in providing connectivity of the whole WSN. Also, microcontroller firmware is monitoring the sensor node's battery and in the case of its running down it changes all its components' operation mode to expand sensor node uptime as much as possible.

Another important characteristic of WSN is self-organization of intra-network connectivity.

Network self-organization makes it possible for randomly spatially distributed sensor nodes and sinks to form a WSN automatically. Furthermore, when network is in use and there are connection problems with some sensor nodes, it doesn't make the whole system fail. In that case WSN simply changes its mode of operation in order to not use the lost nodes for data transmission. This feature of WSNs noticeably simplifies their installation and maintenance, and also allows to create WSNs with thousands of nodes because there is no need to change the network's mode manually when adding new nodes. WSN's self-organization feature in general makes WSN more reliable because network reconstruction can be done in real-time mode, and it allows the WSN to quickly react to the environment changes or sensor nodes failures. In addition, self-organization algorithms can provide optimization of energy consumption for data transmission.

Data collected by all the sensor nodes are usually transmitted to the server which provides the final processing of all the information collected by the sensor nodes. In general, a WSN includes one or a few sinks and gates which are collecting data from all the sensor nodes and transmitting these data for further processing. At the same time, gate forwards the data from the WSN to other networks. In this way communication between WSNs and other external networks, like the Internet, is being provided.

2.1.2 WSN structure

WSN sink

Sensor nodes are the basis of a WSN. They collect and exchange data necessary for WSN functionality. Data collected by sensor nodes are the raw information and require processing. Depending on application, such data can be averaged statistical information or detailed measurements of parameters which define the condition of some object. A separate group of WSN applications is detecting and tracking of targets, for examples, vehicles, animals etc. Each of these cases requires processing of data provided by WSN. Usually it is impossible to perform this processing on sensor nodes themselves, by reason of energy saving and low computing power of sensor nodes. That is why in WSNs the final part of data processing is usually made beyond sensor nodes, on WSN server. WSN server is connected to only one sensor node which is called *sink* or *base station*. Sink is a collecting point of all data in the WSN and interact both with the sensor nodes and the WSN server.

WSNs with the cluster structure

Since energy content of sensor nodes is limited and non-renewable, it is important to use it in the most economical way. Figure 2.3 illustrates the data streaming from sensor nodes to sink. Sink collects data from all the sensor nodes periodically. On the figure, every arrow between sensor nodes shows a transfer of a portion of measurements for a single period of data collection.

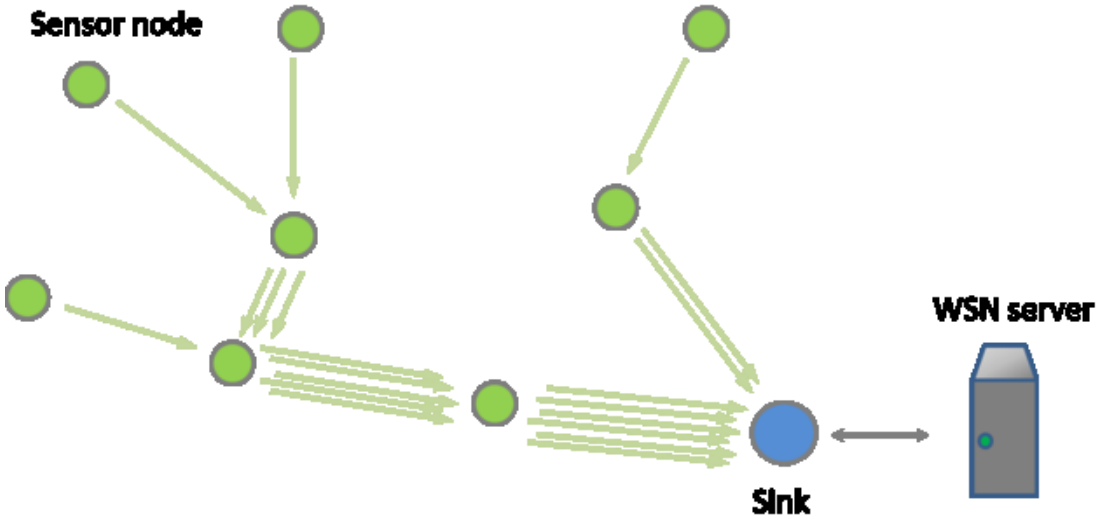

Figure 2.3: Data streaming from sensor nodes

Data is collected from all the sensor nodes; in result, the sensor nodes located closer to sink have to receive and transmit not only their own measurements, but also measurements from other sensor nodes which are further from sink. So, transceivers of the nearest sensor nodes retransmit much more information, and hence they consume more energy than remote sensor nodes. And since sensor nodes are usually all of the same type and have equal energy content, it leads to the fact that the nearest sensor nodes fail much earlier than remote ones, and so the former disrupt the work of the rest of WSN.

So, if WSN application provides periodical data collecting (and it happens in the most cases), it turns out that time of autonomous operating of sensor nodes which are the nearest to sink is much reduced because of more frequent retransmitting. In the long run, traffic from all the sensor nodes is going through one sensor node that is nearest to sink. And the more sensor nodes are in a WSN, the higher is this traffic. From the point of view of energy saving, big WSNs with only one sink cannot consume resources effectively.

To solve this problem it is necessary to divide the WSN into clusters. Each cluster has its own sink and, in fact, is a separate, but smaller, WSN. And each sink communicates with the server directly. Figure 2.4 represents a network with two sinks. On the figure the arrows also used to represent the amount of transmitted data. As we can see, the number of retransmissions is significantly decreased, and it reduces the load on the nearest to sinks sensor nodes.

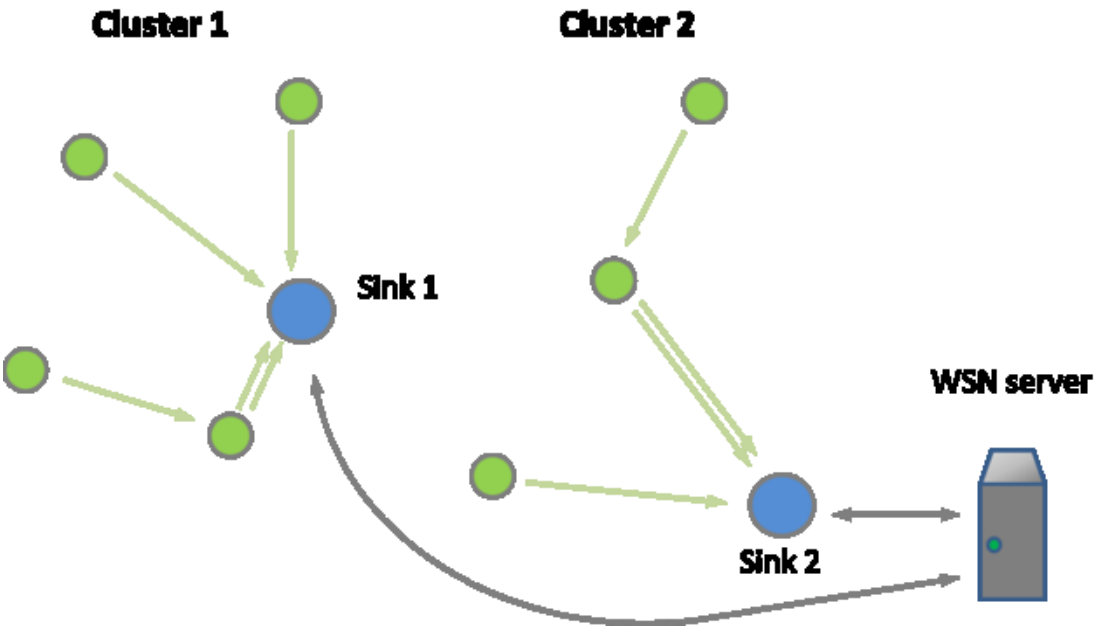

Figure 2.4: Multiple-sink WSN

Multiple-sink WSN is not a random division of one WSN into parts [28]. In the most cases such division is made automatically when WSN is deployed and used. Sensor nodes automatically choose the sink to which they send data. This choice is made according to the algorithm of WSN protocol. Depending on requirements of the application, different criteria may be used, for example, the minimum time for data delivery, the minimum number of retransmissions, achieving the optimal traffic distribution in WSN and others.

WSN gate

WSN organization schemes considered above suppose placement of all WSN elements in the same location. In practice, there is often necessary to have a remote access to WSN data. For example, WSN can be deployed in woodland in suburbs, and collecting and processing of WSN data have to be done in the office in a city. To organize data transmission from WSN to a remote server one uses specialized gates which receive sensor network data from sink and retransmit them using other (i. e. non-WSN) communication standard, wired or wireless. Figure 2.5 represents such a network, which transmit collected data to server through the Internet using a gate.

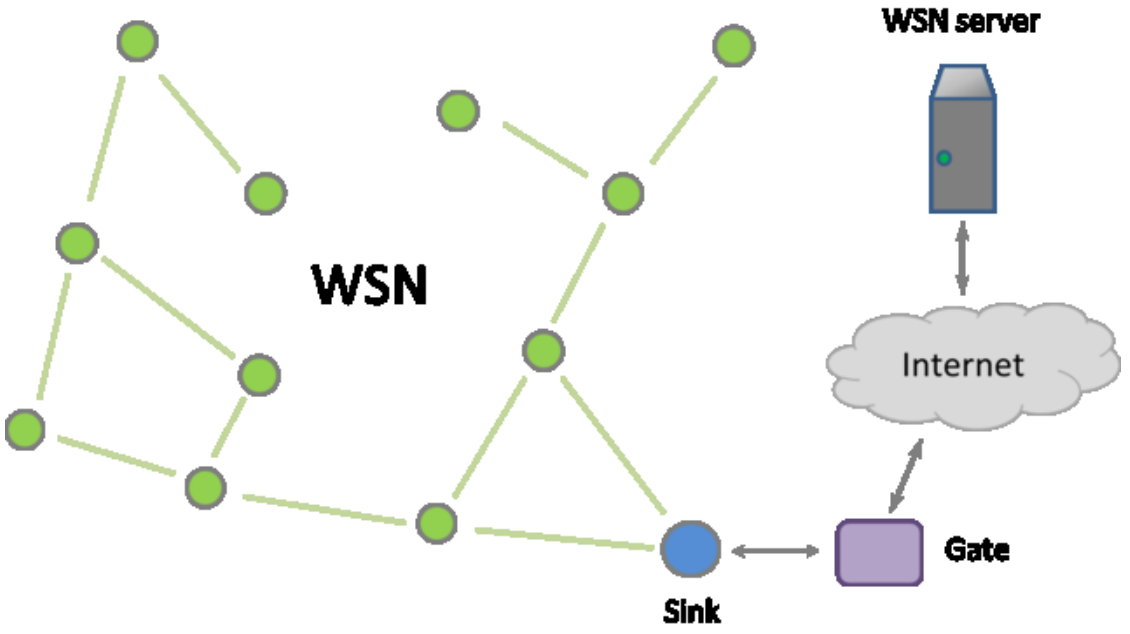

Figure 2.5: WSN server is connected via the Internet

Gates also provide the possibility to organize service provision. Nowadays, when access to the Internet via cellular, cable and satellite networks is available almost in any place in the world, connection of WSNs to the Internet in most cases is easy to implement. Figure 2.6 represents the scheme of possible interaction between a user and a WSN.

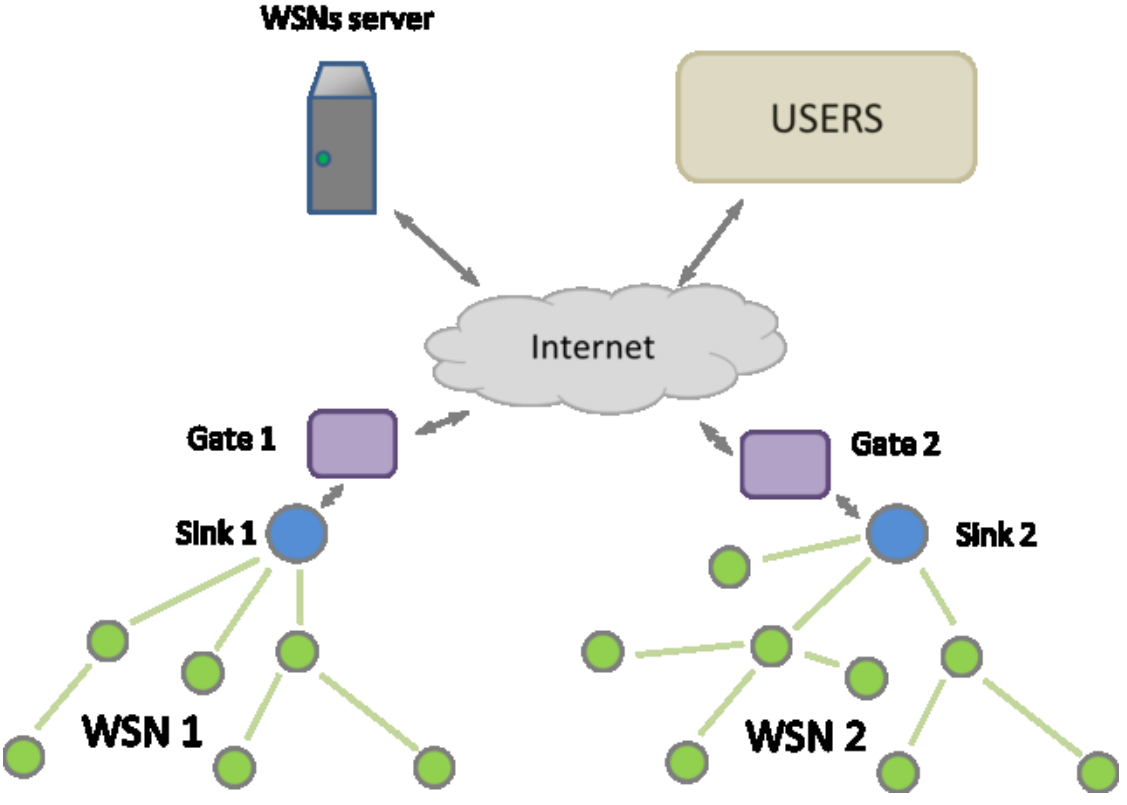

Figure 2.6: Scheme of provision of WSN services

2.1.3 Network topology

Previously we have described traditional applications of WSN for data collecting and processing. Such applications have a special feature: they have one data collecting point, namely sink. But there are also applications where sensor nodes have not only to send information to sink, but to exchange data between themselves. That is why there are different schemes of organization of interaction between sensor nodes within WSN. These schemes are called network topologies. The main types of network topologies for WSNs are: *star*, *tree* and *mesh*. Different WSN standards support different types of network topologies.

Star

The star topology is widely used in computer networks, so when WSN appeared, it started being used also for organization of interaction between sensor nodes. The main characteristic of the star topology is connecting of all the sensor nodes to sink directly. Figure 2.7 schematically represents this topology. In such cases sensor nodes are not connected between themselves, and all interactions between sensor nodes are taking place only via sink. Disadvantage of this topology is limited number of sensor nodes in such WSN. This limitation appears because all the sensor nodes have to be placed in the vicinity of sink, in order to connect to it directly. Another limiting factor is sink's performance, i. e. the maximum number of supported connections.

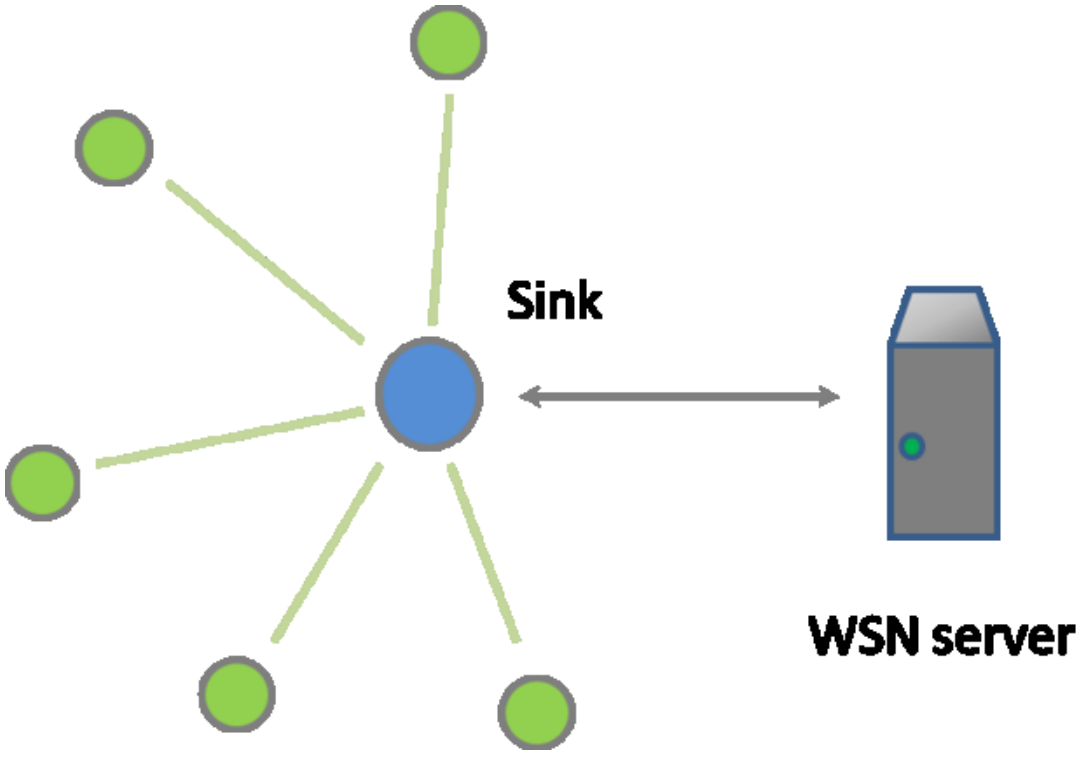

Figure 2.7: The star topology

Tree

The tree topology, in contradiction to the star topology, is much better suitable for WSN with the large number of sensor nodes. It has a hierarchical structure, as it is illustrated on Figure 2.8. Sensor nodes which are the nearest to sink interact with the sink directly. And more remote sensor nodes interact with the nearest ones according to the rules of the star topology. The tree topology also does not provide direct data exchange between all the sensor nodes. Data transmissions only from any sensor node to the sink and in the opposite direction are allowed. Also, in this topology data flow

from the levels with greater numbers (i. e. “leaves”) can be delivered only through the levels with smaller numbers (i. e. “root” and “branches”). So, if on the first level there are only two sensor nodes, and the whole WSN consists of eleven sensor nodes, traffic will be delivered through these two sensor nodes much longer, because of data retransmission from nine sensor nodes on lower levels. Such network can fail quickly, because of energy consuming by the nearest to sink sensor nodes.

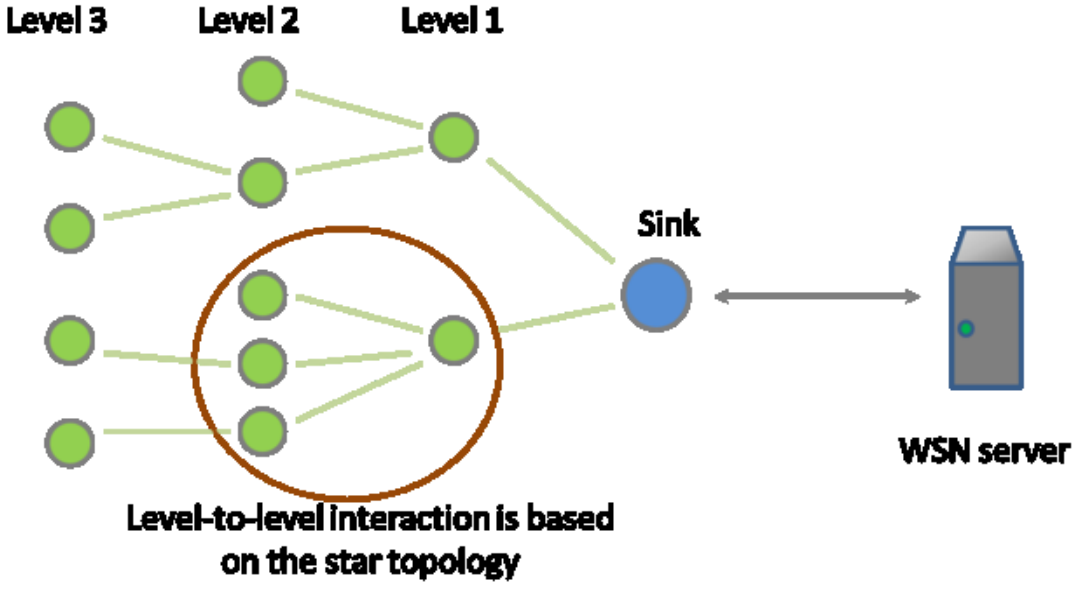

Figure 2.8: The tree topology

Mesh

The mesh topology is the most difficult one for implementation, but it provides much more opportunities for data exchange between sensor nodes. In WSN with the mesh topology interaction between sensor nodes is taking place according to the principle “with every nearest one”, as shown on Figure 2.9. It means that every sensor node cooperates with other sensor nodes, which are in its transceiver’s proximity. In such WSN data exchange between sensor nodes goes through the shortest ways and with the smallest number of retransmissions, what has a positive effect on the energy consumption of the sensor nodes.

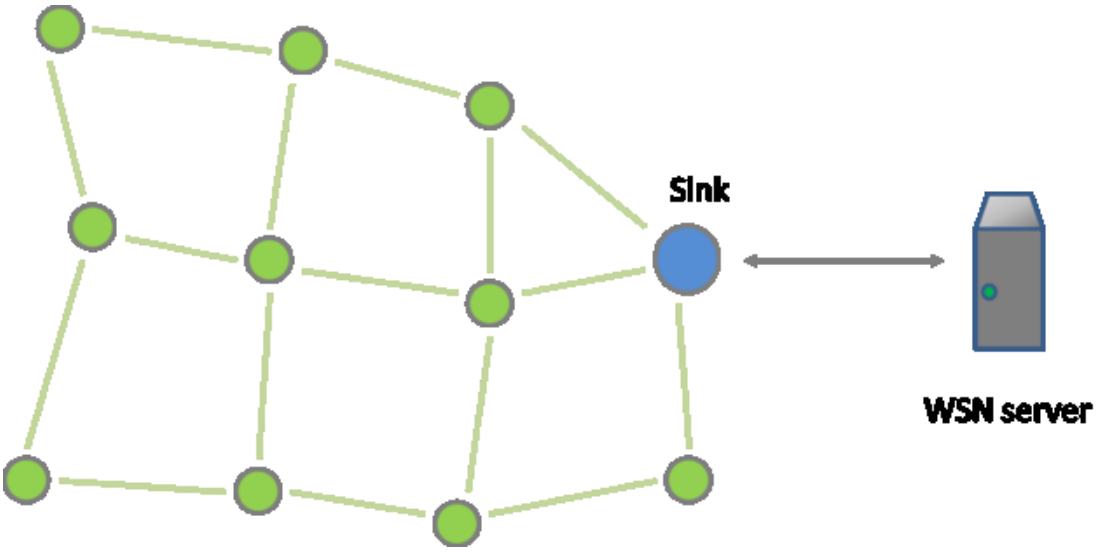

Figure 2.9: The mesh topology

2.2 Hardware

2.2.1 General design issues

One of the most important tasks which have to be solved when working out a WSN for a specific application is the choice of the hardware platform which will serve as a basis for creating a sensor node. There are a lot of sensor nodes implementations from different vendors, but all the platforms have common elements. Choosing one or other existing platform or development of a new one from scratch have to be made in order to meet WSN functional requirements. Any hardware platform provides its own set of sensor node parameters. Variety of available platforms is caused by a wide range of WSN applications, and each existing platform has its own features according to the set of the tasks it is meant for. Also we have to understand that the current level of technology makes it necessary for the researchers to constantly find a balance between such parameters as size, productivity, battery lifetime, communication range, coverage, reliability, functionality, cost etc. Figure 2.10 illustrates the correlation between the primary sensor node parameters. The arrows link directly related parameters, so improving a parameter in one end of the arrow will lead to worsening of the parameter in the other end of the arrow. For example, refinement of functionality (such as increasing the number of controlled parameters , improving the microcontroller performance) will inevitably cause an increase in cost, a decrease in battery lifetime and/or an increase in the size of a sensor node. So, the task of developing new hardware/software platforms which would support new technologies, expand the application scope, facilitate the deployment of WSNs is still relevant.

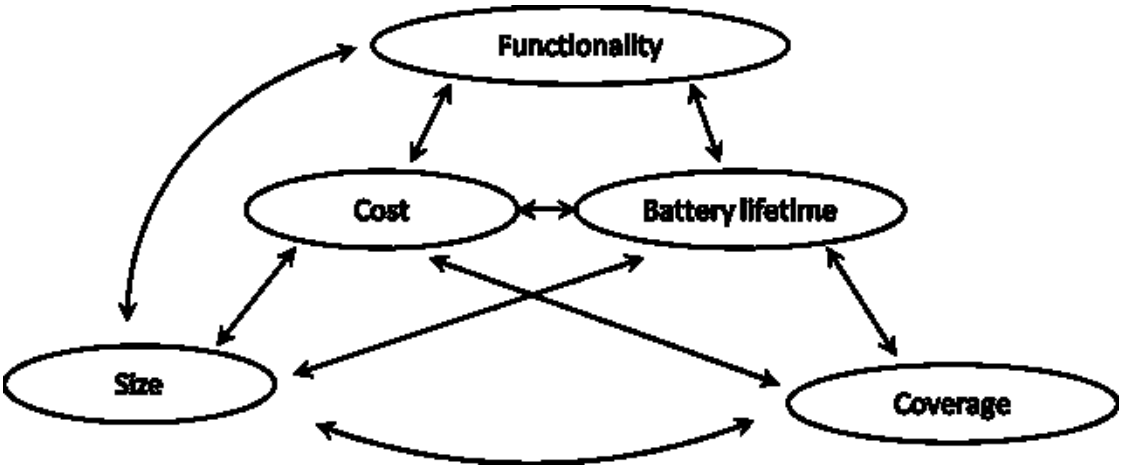

Figure 2.10: Relationships of the primary sensor node parameters

In the next sections we are going to consider the internal structure of a sensor node as well as the main problems of sensor node development more precisely.

2.2.2 The key features of sensor nodes

Before starting the consideration of the sensor node's structure in more detail, we should pay more attention to the main features of sensor nodes. They directly affect the capabilities of the whole WSN. That is why the requirements made to a WSN by a concrete application can always be converted to requirements for sensor nodes.

Energy efficiency (autonomy)

Unlike other common battery-powered mobile devices, sensor nodes deal with much more stringent requirements on energy efficiency, and it imposes restrictions on the all sensor node components. For example, for a mobile phone it is acceptable to keep working autonomously for a few days because the user usually have the possibility to charge the battery if necessary. But with sensor nodes we have another situation. The WSN parts may be spatially distributed on the area of many kilometers, especially if a WSN user is managing it via the Internet. At the same time, sensor nodes can be located in the inaccessible places, or the concrete location of each sensor node can be unknown. Also, a WSN may consist of dozens, hundreds or even thousands of sensor nodes. Under these conditions charging of sensor nodes by the user is out of question. That is why a sensor node must have high energy efficiency in order to keep working on small and inexpensive battery for a few months and even years. This ultra-low-power operation can only be achieved by using low-power hardware components.

Also, one of the key techniques extending the sensor node battery life is reduction of duty-cycle. This parameter is defined as the ratio of the sensor node active functioning time and the time when it is in the low power mode (the sleep mode). In WSNs with long lifetime sensor nodes most of the time are in the sleep mode, where sensor node power consumption is reducing in 3-4 times due to switching off all the main components excepting the part which is responsible for returning from the sleep mode when needed. After returning from the sleep mode the sensor node exchanges data with surrounding sensor nodes, takes readings from sensing elements, and then the sleep mode in turned on again.

Platform flexibility

The majority of real applications require flexibility and adaptability of the WSN platform. In one application a user may need a WSN able to keep working for a few years, and herewith data update speed and data transmission delay won't play a significant role. For example, to monitor the soil temperature and humidity there is no need of frequent readings update and fast data transmission (because the soil temperature cannot change quickly), but it is very important that WSN which performs these functions keeps working as long as possible. In other applications such as monitoring of the spread of forest fires, fast detecting and fast data transmission will be more important, and the WSN lifetime will be less important parameter. So, each sensor node platform must have ability to be adjusted to meet the requirements of a specific application.

Reliability

Certainly, every WSN developer and manufacturer is interested in cost reduction of sensor nodes taking into consideration that every WSN has a great number of sensor nodes. Nevertheless, each concrete sensor node has to be reliable to such extent that it could work without breaking from the moment of turning on until the complete using of battery supply. In addition to increasing reliability of each sensor node, to provide the whole WSN reliability one may use adaptive protocols of data transmission management (*adaptive routing*). They are meant for providing WSN general robustness when certain sensor nodes are failing. For example, if traffic from one or a few sensor nodes is going through the other sensor node and it suddenly fails, as it is illustrated on Figure 2.11, the WSN will change its structure and reconnect the "lost" node through the others nearest to it. It is worth mentioning that the main modern WSN platforms support this function.

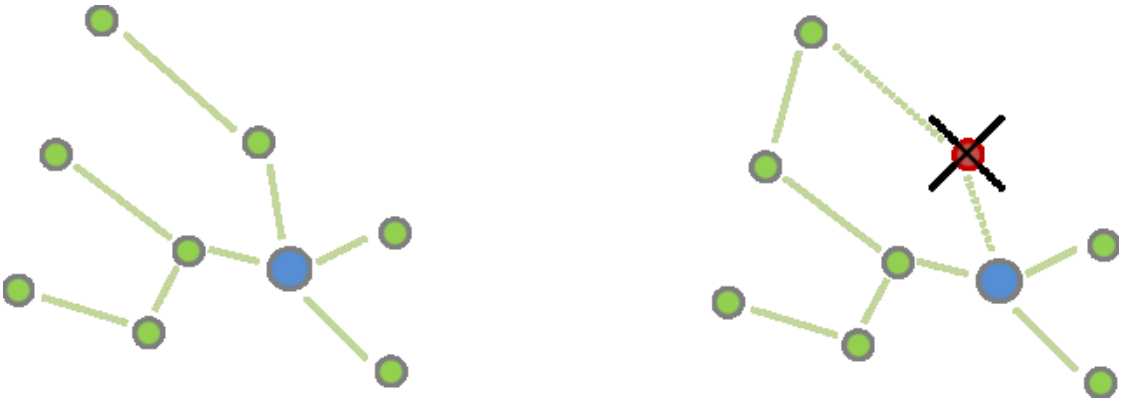

Figure 2.11: Wireless links in WSN. On the left there is representation of network before one of the sensor nodes failing, on the right – after failing

There is also another common threat to WSN reliability which doesn't deal with reliability of any concrete sensor node. It is interference with the signals of other wireless networks and household or industrial devices' radiation. WSNs are often fully or partially located in places with significant electromagnetic fields of other wireless connection systems and appliances. In such cases these electromagnetic fields interfere with low-power transmitters in sensor node. This interference can be significant if it falls on radio spectrum in operation frequency range of sensor nodes' transmitters. In this case connection between nodes in the interference area can get much worse or even break down, and here even operable sensor nodes cannot transmit collected data. In such situations to increase the system's robustness to a node failure, a wireless sensor network must also be robust to external interference. The robustness of wireless links can be greatly increased through the use of *multi-channel and spread spectrum radios*. Figure 2.12 represents principal of operation of the sensor nodes which support multi-channel radios. So, the possibility to change frequency channel for data transmitting is a necessary function for WSNs that are supposed to be deployed in a harsh electromagnetic environment.

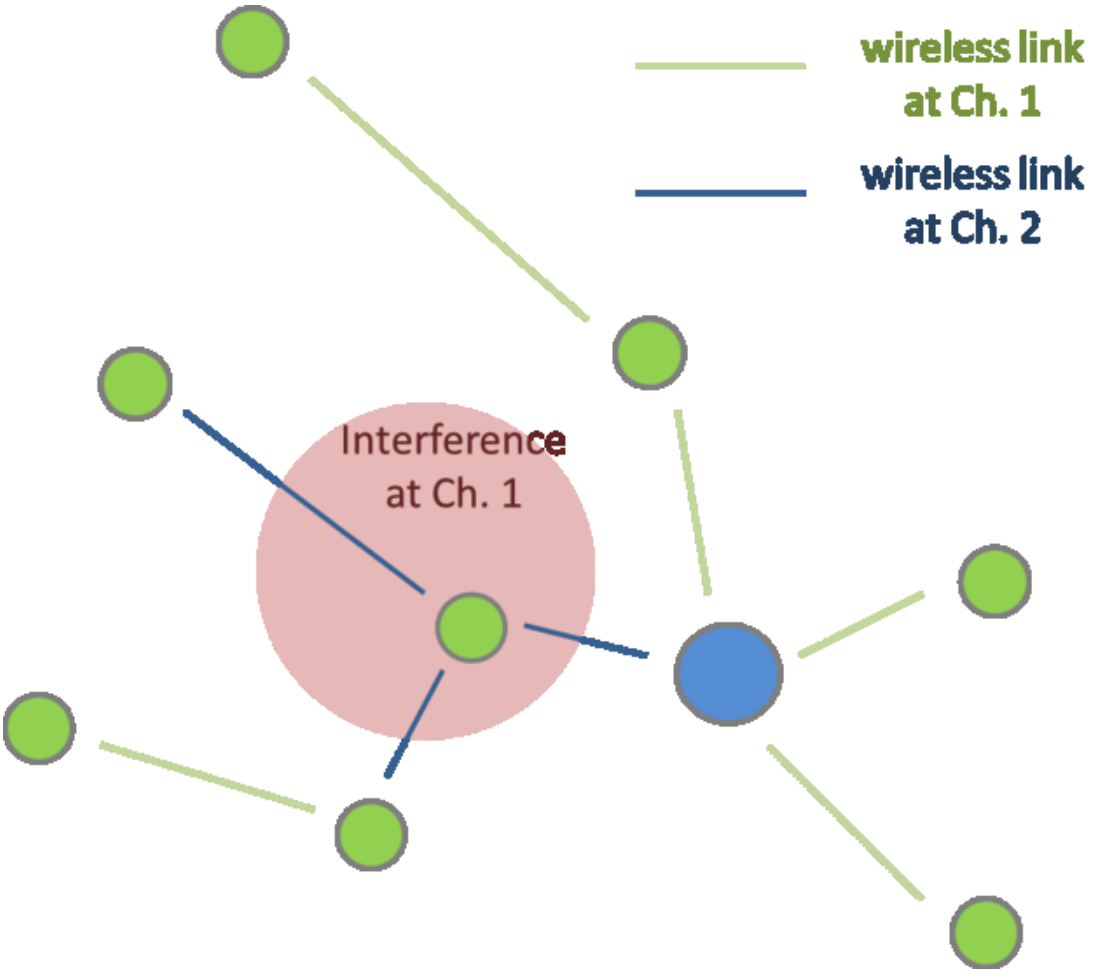

Figure 2.12: WSN working under conditions of strong interference on communication channel 1

Information security

Certain WSN applications make stringent requirements to information security. And this requirement becomes increasingly important, by reason of growth of cybernetic threats when WSNs are connected to the Internet [20]. In order to meet the security requirements, sensor nodes must be capable of performing complex encrypting and authentication algorithms. In fact, radio communication channels can be easily tapped and become available for intruders. The only way to avoid it is encrypting of all data transmitted in the WSN. Many modern sensor nodes make it possible to flexibly set traffic encryption in the network. In some platforms it is made by means of software, but some sensor nodes include special hardware encryption blocks. But in any case, encryption requires additional expenditure of energy, and it has negative impact on WSN lifetime.

Another aspect of information security in WSNs is protection of sensor nodes' internal memory. Sensor node internal memory includes not only information meant to be transmitted in the WSN, but also private keys for traffic encryption. So it must be reliably protected from external intervention.

These information security aspects have to be taken into account simultaneously. On the one hand, weak protection of internal memory will make WSN private keys available making it possible to "crack" the WSN no matter how complex encryption algorithm is. On the other hand, weak traffic encryption will make data transmitted in the network available for sniffing and alteration by the intruder, even if internal memory of each sensor node is well protected.

The security issues in WSNs will be considered in detail in Section 6.3.

Transceiver performance

One of the key sensor node characteristics is transceiver performance. The main parameters of transceiver performance which affect the sensor node characteristics are maximum data transfer rate, frequency range, modulation method, receiver sensitivity and transmitter power.

All these sensor node technical parameters affect such main WSN characteristic as reliability, the minimum spatial density of sensor nodes, the maximum readings update rate and lifetime. So, sensor node transceiver parameters are one of the main characteristics of WSN platform.

Above we have considered how the interference affects WSN reliability on a qualitative level. It is possible to estimate quantitatively how interference affects wireless link between sensor nodes with the help of the mentioned transceiver characteristics. For estimating the impact of noise on the quality of signal reception, in information theory the *signal-to-noise ratio* (SNR) is used. This ratio shows in how many times the wanted signal (signal from other sensor node) received by the sensor node receiver exceeds the power level of interference. The higher the SNR is, the more powerful is useful signal as compared with noise, and the higher is probability to receive the signal correctly. For every method of signal modulation there is a special SNR value at which or above which communication between receiver and transceiver is possible. Also, in information theory there is a fundamental principle [29], which can be expressed (in a simplified form) by the following statement: the higher SNR is, the higher is maximum data transfer rate.

Now it is obvious that the SNR affects reliability and quality of wireless link between two sensor nodes. And the higher SNR is, the better is the quality of communication. So, the more powerful is emission of the first sensor node's transmitter, the higher is SNR of receiving sensor node, and the higher is wireless link quality, hence the whole WSN reliability. In addition, the closer the sensor nodes to each other are located, the better is the SNR for both of them. It means that the maximum distance between sensor nodes in WSN is inextricably linked with power of sensor node transmitter, and the maximum distance between sensor nodes specifies the minimum number of sensor nodes necessary for covering the given space by WSN.

Sensor node receiver *sensitivity* represents the ability to receive weak signals, for example, at a great distance from other sensor nodes, and it, as well as transmitter power, affects the maximum distance between the sensor nodes. It is worth mentioning that increasing the power and sensitivity of sensor node transmitter and receiver leads to higher energy consumption and cost of the sensor nodes. But this dependence is not linear, and the benefit in increasing the range of sensor node is not so great. That is why the most common characteristics of transceivers measure up with ones mW of power, which is acceptable in terms of energy consumption and provides reliable wireless connection between sensor nodes at the distance of about 10 meters.

Frequency range of transceiver affects the maximum possible rate of data exchange and the maximum possible distance between the sensor nodes. At the heart of this dependence are the physical laws of the radio signal. According to these laws, the higher is frequency used as carrier, the stronger is the signal attenuation with the distance. That is why the sensor nodes platforms which operate in lower frequency ranges allow to have higher value of the maximum distance between sensor nodes in WSN. But the basic physical laws don't allow to use very low frequencies for connecting sensor nodes in the majority of WSNs, because the size of the transceiver's antenna has to be the bigger, the lower is the frequency, and it affects the size of the sensor nodes.

The maximum speed of data transmission and reception by sensor node transceiver restrains the maximum speed of data gathering in the WSN. In addition, the higher is the maximum speed of data transmission, the higher is the energy consumption of transceiver during transmission and reception. On the other hand, the higher is speed of transmission, the less time is necessary for transmitting the same data; hence, transceiver will be switched on for less time. But high speed of transmitting also requires more computing power and energy for this computing, which is not always acceptable.

So, performance of the sensor nodes transceiver affects the main characteristics of the WSN

which utilizes such sensor nodes.

Computing power

Sensor node's microcontroller (and hence, consumes battery energy) uses its computing powers for two kinds of tasks. First kind of these tasks deals with supporting WSN functioning, the second task is reading and processing measurements of sensing element. Both kinds of tasks require certain computing power and take the time of the microcontroller. When the micro controller is busy, its energy consumption becomes significant.

The task of supporting WSN functioning, in the first place, is implementation data reception and further transmission algorithms that are part of the WSN communication protocol. Every sensor node is permanently receiving data from other surrounding sensor nodes. Microcontroller identifies these data and depending on the content transmits to the nearest sensor nodes, ignores them or saves to internal memory for further processing. All it happens in accordance with the WSN communication protocol. Computing power of sensor node microcontroller has to be the higher, the higher is the maximum rate of data exchange, so that to have time for data decoding.

We can see the same situation with computing powers necessary for reading and processing of sensor measurements. Sensitive elements can produce a plenty of data which have to be timely processed. And the types of necessary processing can vary a lot, from simple averaging, digital filtration, tracking of some threshold exceeding to calculation of autocorrelation and spectral analysis. The last two operations are the example of the especially resources-consuming ones.

Size and cost

Miniaturization, price reduction, and improvement of other parameters are the most important priorities from the very first researches in WSNs. The good example is the SmartDust project which took place in the end of 1990s and the beginning of 2000s [13]. Miniaturization and price reduction of sensor were constantly expanding the possibilities of WSN applications, and in future they can lead to the widespread use of WSNs and to uprising of ubiquitous WSNs.

Above we have already considered the dependence between different WSN characteristics, and now, after considering the additional characteristics, it is possible to imagine how difficult is to find balance between them when developing the sensor nodes.

2.2.3 Inner structure of a sensor node

Figure 2.13 illustrates the most common scheme of sensor node layout. Also the main inner blocks of each component are represented. Let's consider each of these components.

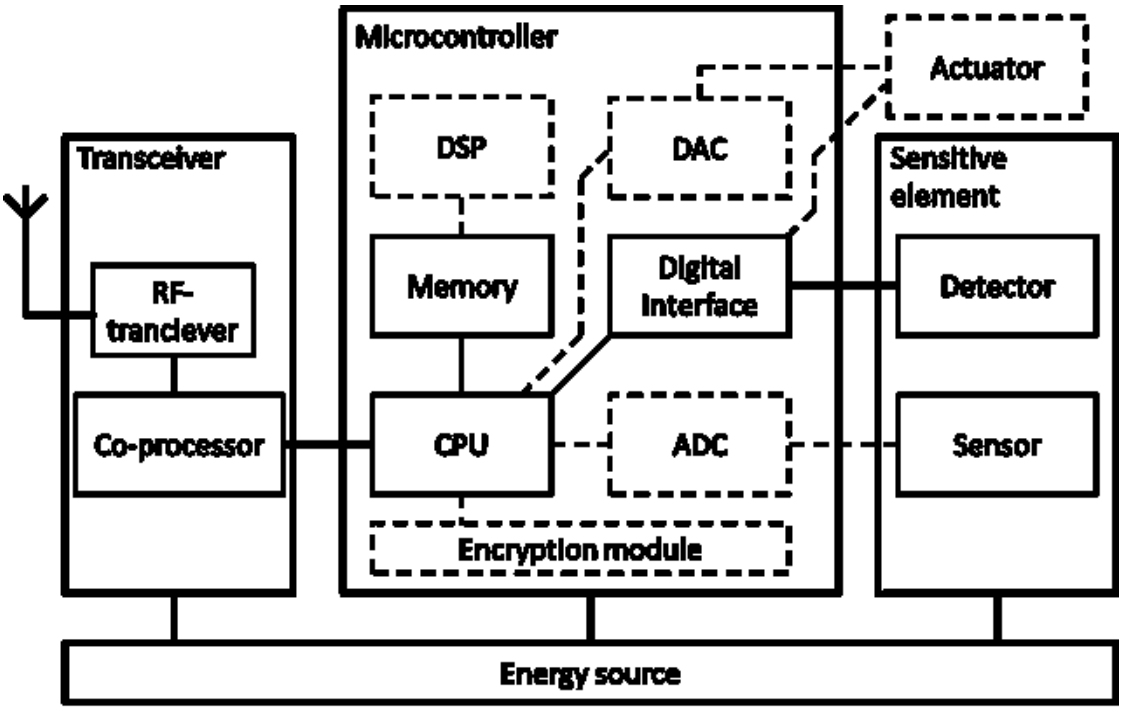

Figure 2.13: Basic layout of a wireless sensor node

Microcontroller performs the function of controlling all the components, and also process data received from sensing element of this sensor node, as well as data received from other sensor nodes.

Microcontrollers are widely used as control elements in a sensor node, by the reason of their low cost, low energy consumption, small size. An important reason by which microcontroller can be taken as a basis of sensor node was a wide range of produced microcontrollers. Researchers can easily find microcontroller with any additional modules (e. g. analog-to-digital converter (ADC), encryption module), with various digital and even wireless interfaces, and also with the necessary performance. All this provides flexibility necessary for developments. In addition to that, microcontrollers are mainstream devices, so it makes them also easier to use.

In the most cases microcontroller, which serves as a basis of sensor node, includes all the modules necessary for its correct functioning. Such modules can be the following ones, depending on applications:

- central processing unit (CPU),
- memory,
- ADC,
- digital interfaces (i2c, UART, 1-wire, SPI, USB, GPIO etc.),
- encryption module,
- digital-to-analog converter (DAC),
- Digital Signal Processor (DSP), etc.

But some of these modules can be designed not on the same crystal with microcontroller, but be externally connected. But in any case, microcontroller controls them. On the figure the optional modules are marked with dotted lines.

To reduce cost and energy consumption of a sensor node, microcontrollers are made severely

limited in productivity. The most common are 8-bit and 16-bit microcontrollers with clock frequency to 16 MHz. Because of limiting productivity of microcontrollers, they typically run specialized component-based embedded operating systems, such as TinyOS [30]. Also, microcontroller can operate in the energy-saving mode (or the *sleep mode*). It can shout down most of its internal blocks and then turn them on again. Power consumption can be reduced up to 1000 times in this mode.

In addition to microcontrollers, other types of embedded processors are used in sensor nodes as control elements, including DSP and Field Programmable Gate Array (FPGA). These types of embedded processors can be more productive than microcontrollers in solving specialized tasks. Specialization of such decisions gives significant benefits to productivity, cost and energy consumption. At the same time, specialization prevents them from being widespread. Nevertheless, let's consider each of these versions in more detail.

Digital Signal Processor is a kind of processor meant for making certain operations with received data according to the pattern. It allows to reach higher productivity in solving of such tasks as processing of audio and video data, spectral analysis, the pattern recognition. But DSP is unable to solve the other type of sensor node tasks, i. e. WSN protocol implementation.

Field Programmable Gate Array, as well as DSP, has advantages in sequential processing, also FPGA is more flexible in using than DSP, and are able to do parallel processing, that is impossible for both DSP and microcontrollers. But because of its construction, FPGA makes it possible to realize only limited number of logical elements, and it is impossible to realize such modules as ADC in FPGA. In addition, they are more difficult to learn, and cost of developing and production of decisions on the FPGA base is rather high.

Radio transceiver. Sensor nodes are interacting with each other through the radio channel. Access to this channel is provided by radio transceiver. In stringent conditions of energy saving, transceivers in the most cases have to be low-rate and short-range. Modern transceivers used in sensor nodes operate at a transfer rate to 250 kbps [31] and distances about 10 m. Herewith, radio transceiver keeps being the most energy consuming part of a sensor node. Radio transceiver managed by a microcontroller goes to the sleep mode and comes back, allowing to reduce the total amount of energy consumption. Another way to reduce energy consumption of radio transceiver is reducing the traffic in the network, for example, by the means of moving some part of sensing elements signals processing to the sensor node's microcontroller.

Chapter 3
Use cases of WSNs

In this chapter we are going to consider the main WSN use cases which are available on the market or are discussed in scientific and technical literature as potentially possible. From the great variety of WSN applications we have chosen those ones which, in our opinion, will be in the greatest demand in the next decade: home automation, building control, agriculture, civil and environmental engineering, emergency management.

It should be mentioned that this dividing into scopes is rather approximate, because these WSN applications intersect each other. For example, WSN applications made for heating and lightening control, can be used in smart homes as well as in office space; sensors used for building control or for various civil and environmental engineering tasks, can also be used for forecasting of emergency situations. Nevertheless, in every section which deals with one or the other scope, we will try to describe the most typical way of using WSNs, and also to analyze the promising applications which can become popular in the future.

3.1 Agriculture

3.1.1 Overview

Agriculture is one of the most interesting fields where WSNs can be used. That is due to the agriculture specific tasks which make it possible to use in practice almost all modern developments in WSN:

- To monitor vast areas it is necessary to create networks which consists of dozens thousands of sensors;
- The existence of several kinds of measured values (temperature, humidity, chemical composition of the soil) makes it necessary to operate with heterogeneous networks;
- The necessity to work with mobile objects for animal husbandry tasks;
- Emerging of automatically controlled agricultural machinery creates a wide range of applications for machine-oriented communications and sensor control networks (to learn more about these technologies, see Sections 6.5 and 6.4);
- The difficulty of battery changing in the field makes it necessary to create energy effective sensors and radio transceivers;
- Good opportunities for data mining application.

WSN applications are closely related with a term “precision agriculture” which now becomes more and more popular. It is based on the idea of distributing such resources as water, seeds and fertilizers not evenly or by pieces, as it is done in traditional agriculture, but in dosage according to conditions (temperature, light, composition of the soil) of each specific spot. It allows to reach two goals: on the one hand, consumption of resources is reducing, on the other hand, productivity of a land site is increasing. In addition, it is rather important that implementing of this idea leads to reducing environmental damage.

Among the precision agriculture technologies we can name the following ones:

- Selective irrigation;
- Fertilizers distribution control;
- Productivity mapping;

- Weeds detecting;
- Soil mineralization detecting;
- Optimal planning of irrigation systems, tracks, protective planting and surveying the territory according to the soil peculiarities.

Let's consider the examples of successful WSN deployment in agriculture.

3.1.2 Wireless sensor network for precision agriculture in Malawi

Wireless sensor network for precision agriculture in Malawi (WiPAM) is a project intended to automate irrigation in order to assist small scale farmers in the rural areas of developing countries. For this purpose a network of sensors was made; these sensors detect humidity and temperature of soil and transmit measurement results to the center every half an hour. When the measurements are reaching some threshold values, automatic irrigation procedure is activated, and in this case measurement results are being transmitted twice per minute.

The WiPAM project uses ZigBee modules as hardware which are working under IEEE 802.15.4 standard at frequency 2.4 GHz. Watermark 200SS was chosen to be a sensor, because it has the best relation between cost, reliability, ease of interfacing to a signal processing device, accuracy, and soil texture. To form sensor nodes with these components the project developers have used open source sensor device, powered with a lithium battery which can be recharged through a special socket dedicated for a solar panel. Also, custom software has been designed in the frameworks of the project.

It is worth mentioning that as a potential risk of the project was considered deterioration of the radio link between sensor nodes in consequence of plants growing. But these fears didn't come true in practice, and an experiment showed the even dense vegetation doesn't have much influence on the signal level in this frequency band.

But during the project implementations other problems have appeared. Firstly, it became obvious that it was impossible for the ZigBee modules to work simultaneously with GPRS by reason of violation of electromagnetic compatibility conditions. Secondly, the researchers have faced with the problem of fast battery resources consuming which was partially solved by increasing the data measuring and transmitting interval. Thirdly, it was proved that remote monitoring of the system condition is very important because there were failures appearing from time to time when system was in work. Physical search of these failures would have taken too much time.

As a result of the project it was shown that WSN deployment can provide significant resources economy even for small farms.

3.1.3 "Smart" agricultural machinery managing

WSN applying benefits can significantly increase in integration with other modern agricultural machinery. In this regard, one of the most advanced industries is wine-making, because exactly in this field even insignificant change of the product quality may have a great influence on the incomes, and farmers have an interest in new technologies implementing for achieving the best possible result.

In the work [32] there is a review of tools and techniques meant for so-called precision viticulture. As one of the most promising ICTs, along with WSN, they regard high-precision positioning based on the global satellite navigation systems. Now there are two systems of this kind: GPS (USA) and GLONASS (Russian Federation), also, Chinese Beidou and European Galileo are actively developing. At the moment usage of only these two systems allows to achieve the positional accuracy in a few meters. But using some satellite navigation systems additions (as a rule, offered at extra cost), such as Differential GPS (DGPS), Real Time Kinematic (RTK), Precise Point Positioning (PPP), makes it possible to achieve accuracy in decimeters or even centimeters. It offers

good opportunities for using agricultural machinery operating with no or little human intervention and makes it very promising.

On the market only for wine-making there is offering of automatic machinery for inter-row cultivation, weed control, pruning, planting. It is possible to automate the most part of operations of grape growing, and, in this way, reduce the cost of the product. When using data from WSNs in a correct way for management, planning and decision making, it is possible to enhance this effect and provide productivity unattainable for manual labor.

3.1.4 Cows monitoring

WSNs can be used for cows monitoring. Sensors can determine if cows are ill of pregnant, and inform a farmer about it.

It is interesting that, according to words of the company's founder [33], the main problems of this idea realization have taken place not by reasons of the technical limitations, but due to difficulties connected with the law. To store the measurements of cows, a foreign cloud service has been used. But privacy providing legislation of European countries doesn't take into account peculiarities of cloud services work where it is impossible to predict the way of data transmitting and the place of their storage. As a result, in certain countries such systems application may cause problems with the law.

This example makes it clear that technologies development has to go along with changing of legal and regulatory framework to make implementation of these technologies possible.

3.2 Home automation

3.2.1 Overview

Home automation is a general name for technologies for automation of maintenance of residential buildings. As a synonym of home automation a more 'marketing' term *smart home* is often used. The first ideas of smart home appeared in the science fiction, but the most part of these ideas came true recently. Largely it was facilitate by WSNs development.

Home automation solves a lot of various tasks which include:

- Monitoring of different parameters, such as temperature, turning on the light, opening of locks in rooms;
- Remote managing of all available in the house systems by the owner: lightening, heating, security systems, water supply, air conditioners, home entertainment systems, though the control panel, computer or smartphone or from any place via the Internet.
- Automatic management of systems in the house according to the monitoring data;
- Efficient resources consumption (water, electricity, heat);
- Different tasks on protection from criminals, including access control, audio and video surveillance;
- Monitoring condition of aged and ill people presenting in the house;
- Emergency detecting and automatic taking actions to cope with it;
- Taking care of pets;
- Managing domestic robots.

The examples of WSN applications for home automation are interesting most of all because they have a huge commercial potential and are very likely to become in the coming years the mass phenomenon in the developed countries.

3.2.2 Smart home and machine-oriented communications

One of the examples of the smart home application is considered in the Appendix of Recommendation Y2061 [34], which deals with *machine-oriented communications* (MOC). The term MOC means technical systems construction principle where interaction of two or more entities and at least one entity does not necessarily require human interaction or intervention in the communication process. So, the main part of the modern smart home functions relates to the scope of MOC.

In Y.2061 the typical cases of using smart home applications in various situations (normal conditions, an attempt to enter into the house made by a criminal, ignition) are described. In the present technical paper this example is discussed with more details in Section 6.5 which deals with MOC, where also are considered the requirements to NGN and MOC devices for support of this application.

3.2.3 WSN and service robots integration

In the work [35] there a description of probably the most futuristic WSN application for home automation — domestic *service robots* control.

The service robots can be considered to be mobile nodes that provide additional sensorial information, improve/repair the connectivity and collect information from wireless sensor nodes. On the other hand, the WSN can be regarded as an extension of the sensorial capabilities of the robots and it can provide a smart environment for the service robots.

Usage of service robots in this example allows to solve the task of providing full supervision over the whole house while keeping low cost of the equipment. Cameras, ultra-violet and ultrasound sensor make it possible to give to a user complete information about what's happening in his house when he is absent. But equipping every room with these sensors costs a lot. The authors of the paper offer to equip rooms only with inexpensive sensors able to detect ignition of other emergency situation; after detection a service robot, which has sensors of various kinds, is directed to a place of probable danger.

Of course, in future there will be robots able not only monitor, but also to act in so that to minimize damage of emergency situation, and also solve other, less critical tasks.

3.3 Building control

3.3.1 Overview

Building control is the expanding of the smart home idea. But it deals with not only residential houses, but also with industrial, office and commercial buildings. In this case one of the main tasks is not only to enhance comfort and safety, but also to save resources.

In these applications WSNs have a key role, because building control efficiency depends upon good organization of processes, measurements gathering, data processing and decisions making.

According to the information given by Waide Strategic Efficiency [36], the total techno-economic optimal savings potential can reach 22% of all building energy consumption by 2028 and to maintain that level thereafter as an optimal scenario on a rational and perfectly functioning market. According to this scenario, using building control systems leads to some 2 099 Mtoe of cumulative energy savings from 2013 to 2035 which equates to estimated cumulative CO_2 savings of 5.9 gigatonnes over the same period, with annual savings of 184 million tonnes of CO_2 in 2020 and 380 million tonnes in 2035.

3.3.2 Future Smart Rotating Buildings

The work [37] offers an interesting application. Recently there is a huge trend to build high rise

"*dynamic buildings*". As each floor rotates separately, the form of the building changes constantly. The innovation for such buildings would be to create a system that optimizes its rotation in order to maximize the benefits of solar panels installed at the various building surfaces (vertical and horizontal). Using WSNs in such building is becoming a trend given the tremendous benefits which such system provides. Researches managed to build a model and to determine the algorithm of each building surface rotation, which will be able to provide the most effective using of solar energy. These results will be used in constructing of Da Vinci Tower, 80-floor moving skyscraper, which is supposed to be build in Dubai (United Arab Emirates).

3.4 Civil and environmental engineering

3.4.1 Overview

WSN applications for civil and environmental engineering first of all deals with monitoring condition of the objects created by human, as well as the environmental objects. For a researcher these applications are interesting first of all because of a great number of various types of sensors used, and also because of variety of places where it is necessary to implement a network.

3.4.2 Structural health monitoring

Structural health monitoring is the process of identification and localization of failures in different engineering systems with the help of the statistical analysis of the periodic measurements of various physical parameters. For the large objects where parameters have to be measured at the same time in a great number of places, WSNs are becoming indispensable.

One of the most typical WSN applications for structural heath monitoring is bridges condition control. On famous Golden Gate Bridge in San Francisco Bay there is implemented a network of 64 sensors (piezoelectric accelerometers) which measure ambient vibrations with accuracy of 3 μG sampled at 1 kHz [38]. The goal is to determine the response of the structure to both ambient and extreme conditions and compare actual behavior to design predictions. The network measures ambient structural accelerations from wind load at closely spaced locations, as well as strong shaking from a possible earthquake, all at low cost and without interfering with the operation of the bridge.

3.4.3 Volcanic Earthquake Timing

Predicting of eruption is a very difficult technical problem. One of the ways to solve this problem is monitoring of so called *primary waves* (P-waves) with the help of seismic sensors network. Specific algorithms are worked out which can detect hypocenter and seismic tomography, but they need fine-grained data to operate, more precisely sensor signals which are sampled at high frequencies (e. g., 50 to 200 Hz), collected upon a large territory; moreover, the data have to be transmitted in real time. It settles extremely stringent requirements to sensor network capacity that, in turn, has a negative effect at the cost and energy consumption of sensor nodes.

Another problem is the difficulty of network deployment because sensors have to be installed in a volcano crater, what is not just costly, but also risky. Also, after installation sensors have to operate in a harsh weather conditions.

n the project *Autonomous Space In-situ Sensorweb* (OASIS) [39], where monitoring of the Mount St. Helens (Pacific Northwest region of the USA) was carried out, the problem of WSN deployment was solved due to sensor nodes being air-dropped and self-organizing a network. Also the researchers have used a special hardware design for sensor nodes. It were 3-leg "spider" sensor nodes, which are about 4-foot (122 cm) tall including the lifted antenna and weigh about 70 pounds (32 kg). Such design was able to support air-drop deployment and survive in the harsh volcano environment.

In the work [40] it was suggested to reduce the cost and increase energy efficiency of WSN in the

following way. Instead of transmitting raw measurements to the central point, it was proposed to implement hierarchical architecture where a large number of inexpensive sensors were used to collect fine-grained, real-time seismic signals while a small number of powerful coordinator nodes process collected data and pick accurate P-phases. This approach was successfully implemented for the OASIS project, and made it possible to increase the sensor nodes lifetime from 2 to 6 months.

3.5 Emergency management

The previous use case shows that WSN can solve the problems on which can depend lives and security of a large number of people. It is possible to say that one of the most critically important WSN applications is *emergency management*. This term means not only emergency detecting, as in the previous example, but also people and equipment management meant for minimizing damage caused by a disaster. Emergency management applications are the ones where WSN peculiarities such as decentralization, possibility of autonomous power supply, self-healing and self-organizing become critically important. In addition, mass mobile devices, such as smart phones, tablet computers and laptops, can be used by WSN applications in the case of the disaster to control people individually, what is impossible when the traditional resources of emergency warning are used.

Since emergency management is very important, in present technical paper it will be individually considered in Section 5.2.

Chapter 4
Decision making and efficiency assessment in WSNs

4.1 Introduction: decision making in WSNs

While deploying a WSN, the system designer has to take care of many issues which require selection between several alternatives. He or she needs to determine:

- network topology,
- number of sensor nodes,
- relative position of elements,
- security model,
- hardware and software for both sensor nodes and servers.

The final goal of these choices is making the WSN solve all the problems that are set for it effectively. At the same time, the expense of the limited resources (e.g. financial costs of deploying and maintenance of a WSN) should be kept within established limits.

In the same way, during WSN maintenance many decisions have to be made, for example:

- placement of new sensors in case of WSN expansion,
- procedure of battery replacement in the sensor nodes,
- necessity of software update and hardware upgrade.

Moreover, while designing the WSN elements, it is also required to choose electronic components, modulation methods, cryptographic schemes, frequency channels, etc.

Finally, the operating of every WSN itself is connected with decision making on the level of sensor nodes and servers:

- route selection for data delivery (routing),
- decisions about sleep mode or active mode transition,
- sensor node identification and evaluation of the trust level of the sensor nodes.

The algorithms able to make such decisions are built into the sensor nodes' firmware.

Thus, during designing a WSN, its deployment and maintenance various decisions have to be made at the following levels:

- System level: the decisions made while deploying, upgrading, modifying and maintaining a WSN;
- Element level: the decisions made by the developers of WSN elements' software and hardware;
- Operation level: the decisions made automatically by the WSN elements' software/firmware.

As these three levels have different *decision making units* (DMUs): it can be both people (system analytics, developers, designers) and software/firmware working automatically, — it is very important to provide the consistency of their decisions.

For that reason, it is required that DMUs at all levels use the same set of efficiency criteria for assessment of alternatives. All the requirements to WSN or its individual components have to be expressed in terms of these criteria.

As soon as this is done, different alternatives can be compared using the selected criteria to find the one that fits best for the task to be solved. Thus, working out the set of efficiency criteria allows to formalize the decision making process and, thus, to make it more objective. The set of efficiency criteria together with the rules of application of these criteria forms an *efficiency assessment system*.

This chapter is dedicated to the problem of finding a common efficiency assessment system for WSNs. First, the efficiency criteria used by different WSN applications are analyzed. Next, the analytic hierarchy process (AHP) is considered, as it allows to merge several criteria into one. Finally, the ideas on developing a general framework for making decisions on all levels of WSNs, applicable to all network and service types, are explained. After that, the orientation of further work is determined.

4.2 Existing efficiency criteria

Let's consider the efficiency criteria that are used in various articles and other scientific and technical materials in the WSN field. Four groups of efficiency criteria can be marked out:

4.2.1 Group 1. Network lifetime

Battery replacement is a complex and expensive operation almost in every WSN, because the sensor nodes are numerous and they can be situated in places that are difficult of access. That is why one of the most important WSN efficiency criteria is the network lifetime, i. e. the time the WSN remains alive after the deploying of [41]. Network lifetime can be defined in various ways, because the meaning of the statement "the network is alive" depends on the requirements for this network. In the [41] work some of the most frequently used definitions are given:

- The time before the failure of the first sensor node;
- The time before the failure of a certain fraction β of total number of sensor nodes;
- The time before one of the following events happen (which is earlier): failure of one of the so-called "critical" sensor nodes or failure of k "non-critical" sensor nodes.
- The time before the failure of one of the sinks;
- The time before the failure of all the sensor nodes;
- k-coverage: the time while the whole service area is covered by at least k sensor nodes. The "service area" can mean some area, volume or a discrete set of points which the DMU would like to monitor;
- α-coverage: the time while α percent of the service area is covered by at least one sensor node;
- An important special case of the previous two definitions: the time while the whole service area is covered by at least one sensor node;
- The number of successfully transmitted packets. As opposed to other definitions, this value is measured not in hours or days, but in dimensionless units;
- The time before the fraction of the sensor nodes that have a path to the base station is below some threshold value α;
- The time before the probability of some specified event detection by the WSN is below some threshold;
- The time while the maximal connected subgraph of the network graph contains more nodes when N.

Network lifetime, defined in any of the following ways, belongs to the system level of decision making. But network lifetime is related in many respects to the lifetime of individual components of

the network, which, in its turn, depends on the energy content of batteries and power consumption in different modes: transmission, reception, idle and sleep. Moreover, network lifetime depends on algorithms and protocols for data transfer, processing, routing and other operations. For instance, the choice of more efficient routing protocol can result in significant increase in network lifetime without modifying the hardware implementation of the sensor nodes. That makes it possible to use different parameters related to network lifetime as efficiency criteria both on the element level and the operation level.

In the former case that means that the firmware can take into account the amount of energy that should be needed to execute every action.

4.2.2 Group 2. Criteria related to data processing

In many WSN applications the sensor nodes do not just make measurements and send the results to the central node, they perform data processing, too. The algorithm of this processing strongly depends on the application, but it always involves two basic operations: data storage and retrieval. Thus, expenses to these operations can be used as efficiency criteria of a WSN.

To calculate the numerical value of the criterion, we can measure either the mean time needed for one operation of data storage and search, or the amount of messages sent to the network during the operations. Although all of these criteria are used for assessing the efficiency of data storage and processing in a WSN, there are differences between them: the meantime is directly connected with the speed of processing the users' requests, and the amount of messages mostly assesses the efficiency of spending the resources during the operations.

To achieve the best values for these criteria the DMU should take care of choosing the best network topology and the best way of organizing data storage (e. g. indexing, data replication, optimization of requests), which would provide high speed of data reading and data recording. Moreover, there may be need of using or developing the request algorithms that minimize the amount of messages sent to the network.

On the element level, one may need integrating faster storage devices into the WSN. On the operation level, the WSN elements can, for example, give priority to the packets related to storage or searching the data and their responses. That would reduce the mean time of data processing.

4.2.3 Group 3. Criteria related to data transfer

Every WSN can be regarded as a data transfer network, and the corresponding efficiency criteria could be applied to it. The choice of a certain criterion depends on the tasks the WSN is used for, but usually one of the following two is used.

On the one hand, if a guaranteed delivery of all the network messages is needed, we can calculate the *mean time that the WSN needs to transfer a message* of some typical fixed length from one point to another, e. g. from a peripheral sensor node to the base station. On the other hand, we can fix the maximal time of message transfer, and calculate the *fraction of messages that are delivered in time*. This kind of criterion is preferable for the real-time applications, especially the ones connected with the automatic control of devices, audio and video transfer.

The considered criteria related to data transfer could also be used on all the levels of decision-making. With the fixed hardware and software parameters of the WSN the value of the criterion depends on the size of the network and its topology. On the element level, to get better values, the DMU can choose high-speed computation modules, optimize the time of switching to the sleep mode, use more powerful transmitting devices. On the operation level, different methods of priority traffic processing can be used.

4.2.4 Group 4. Other efficiency criteria related to the quality of service

All the parameters of the *quality of service* (QoS) used for other networks could be applied to WSN:

data throughput, the level of bit and packet losses and errors, the reliability availability ratios [41]. In a number of applications connected with real-time transferring and processing of information the delay variation (jitter) may be important.

Among the efficiency criteria, the service area should be mentioned particularly. Depending on the problem, either the volume, area, or length of the service area can serve as an efficiency criterion; in some cases, it can be more convenient to choose several objects the WSN should observe and express the size of the service area through the amount of objects covered by the network.

As in the previous cases, each efficiency criterion related to the QoS on the system level has a corresponding criterion on the element level. The WSN service area is a function of the service areas of single sensor nodes. The service area, the error probability, the reliability and availability indexes, the jitter can all be determined for single sensor nodes, for communication links between them, and sometimes for different algorithms.

On the operation level different indicators can serve as corresponding efficiency criteria (the signal level, the distance between different sensor nodes, the level of battery charge, etc.). Such indicators serve for the automatized making of such decisions as choosing the best route, estimating the priority of different kinds of traffic or choosing the degree of data compression.

4.3 Analytic Hierarchy Process

4.3.1 Overview

With the growing difficulty of the problems solved with the use of WSN, the need of simultaneous consideration of different efficiency criteria has arisen.

One of the most frequent ways to solve this problem is the use of the Analytic Hierarchy Process (AHP). Due to its universality, this method is widely used for many different problems, from strategic planning to automatized operating control [42]. AHP deals with hierarchies consisting of:

- goal that the decision making unit is interested in,
- alternatives between which the DMU needs to choose the best one
- the criteria used to assess the alternatives from the point of view of the goals (see Figure 4.1).

In its calculations, AHP uses three types of values:

- **The priority of the criterion.** The importance of the criterion shows how great is the impact of the criterion on the achieving of the goal.
- **The local priority of the alternative by a certain criterion.** The priority of an alternative by some criterion shows how relevant is a particular alternative by this criterion.
- **The global priority of an alternative.** The global priority of an alternative is equal to the sum of local alternatives by different criteria, multiplied by the priorities of the criteria. This value is the index of efficiency calculated in AHP.

4.3.2 AHP procedure

The description of the AHP procedure is given by [43].

To compute the global priorities using the AHP, we first must obtain the input data for given problems comprising judgment matrices of pairwise comparisons of the decision elements in one level that contribute to satisfying the objectives of the decision elements in the next higher level. The pairwise comparison process elicits qualitative judgmental statements that indicate the strength of the decision makers' preference when making a particular comparison. In order to translate these qualitative statements into numbers to be manipulated to establish required relative weights, a

reliable scale has to be established. This scaling process is necessary because it provides the input to be utilized in evaluating the weighting values of the decision factors.

The relative weights of the decision elements are estimated with the combined judgment matrices by using Saaty's eigenvalue method. The estimation of relative weights can be obtained from equation:

$$A_{n\times n}W = \lambda_{max}W,$$

where A is the observed matrix of pairwise comparisons, λ_{max} is the largest eigenvalue of A, and W is its right eigenvector.

Finally, the weighting values of the respective decision factors at the bottom level of a hierarchy are computed by aggregating the relative weights of various elements in the hierarchy.

4.3.3 Usage of AHP for efficiency assessment in WSN

Below we consider a few remarkable works related to usage of AHP for efficiency assessment in WSN on different levels.

System level

The paper [44] develops a rational and comprehensive five-layer indicator model which incarnates system efficiency of WSNs. Target layer the ultimate goal indicates system efficiency; criterion layer is composed of QoS, energy consumption, network management, and other crucial factor in view of system application; subcriterial layer represents significant task of each monomial efficiency; evaluation indicator layer designates primary aspects of each task; scale parameter layer reflects inherent characteristic of WSNs. The model can render assistance to system design, development, and optimization.

The paper [45], is not directly related to AHP, but all the same can be useful for WSN researcher, because it deals with the issue of optimal network topology. The following criteria are considered: the number of nodes, the total link length, the total path length weighted by path traffic, the amount of traffic on the maximally loaded link. To evaluate the values of criteria, computer simulation is used. It allows to examine 83,868 candidate topologies.

Element level

The paper [46] is devoted to performance analysis key management schemes to enable encryption and authentication in WSN for different application scenarios. The following five performance criteria are considered: scalability, key connectivity, resilience, storage overhead and communication overhead. As all permutations of five performance criteria include 120 types' situations, experimental analyses on 43 key management schemes for the optimum selection are presented.

The article [47] is an example of AHP application for some concrete technical question. It deals with Cooperative *Multi-In Multi-Out* (MIMO) schemes that are aimed to reduce both transmission energy and latency in WSNs. In this paper a comparison study of three cooperative MIMO schemes is presented. From the analysis, the authors have found a scheme that outperforms other schemes in term of energy-efficiency and lower packet latency.

Operation level

In the paper [48] a mechanism based on AHP is proposed that allows to select the appropriate cluster head of a network automatically in real time. With the goal of prolonging the network

lifetime, three factors are considered: energy, mobility and the distance to the cluster centroid. The message exchanging procedures to implement the mechanism are also proposed. The simulation results demonstrate that the proposed cluster head selection approach can improve the network lifetime remarkably, especially for differentiated initial energy of nodes.

The article [49] proposes a method for behavior trust evaluation of WSN nodes. As people's subjective judgments has uncertainty and ambiguity in comparing judgment among elements, with triangular fuzzy number the paper proposed the trust evaluation for nodes in WSNs which based on observing the behavior of them. It also utilizes and extension of AHP called *Fuzzy Analytic Network Process* (F-ANP). Its has a network structure which is more complex than hierarchy structure used in the "classical" AHP and uses using a more profound application of mathematical knowledge. The method allows to make automatic decisions if the center should trust the measurements of some specific sensor.

4.3.4 General framework for efficiency assessment in WSNs

In all the above mentioned articles, the authors performed the same sequence of steps for AHP:

1. Building the hierarchy of the problem to be solved;
2. Defining the criteria to assess the alternatives;
3. Evaluating the priorities of the criteria;
4. Evaluating the local alternatives' priorities according to the criteria;
5. Calculating the global alternatives' priorities according to the goal.

Often the work is doubled, as for many problems the results of these steps (especially the first two of them) turn out to be the same. It would have been more effective if there was one general framework serving as a template where the questions that are common for all the problems of efficiency assessment in WSN would be solved already, and the researcher could pay more attention to the peculiarities of every certain problem. Along with making the problem easier, it would provide the comparability of the results gotten by different researchers and the possibility to use the results that had already been gotten beforehand if the problem is slightly modified, e. g. if new alternatives arise.

To realize that practically, we need to add one more level to the hierarchy on Figure 4.1 — the service requirements level.

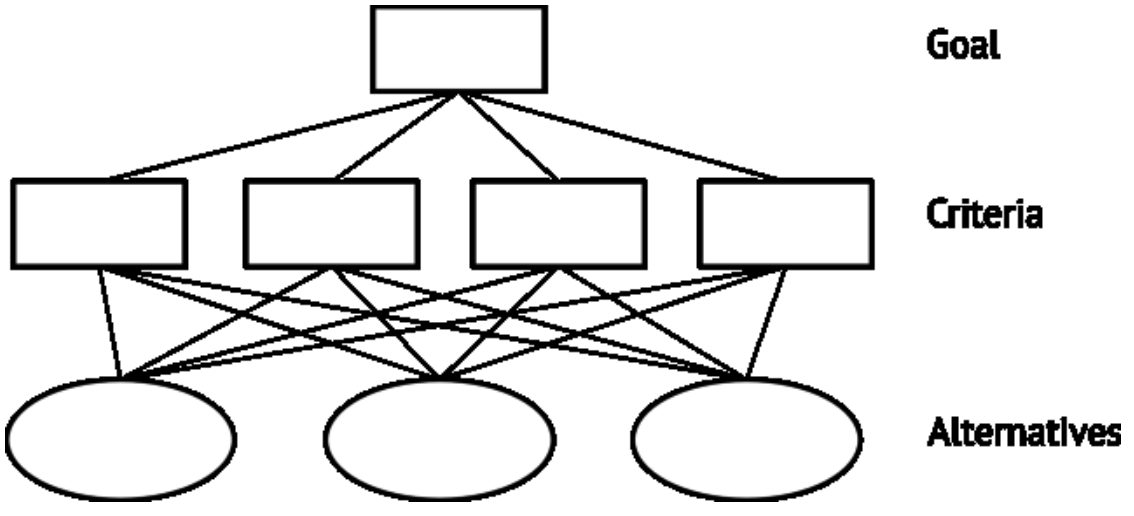

Figure 4.1: General AHP hierarchy

Each service requirement is a functionality which can be useful for several applications at a time. Any service requirement can be "compatible" or "incompatible" with certain alternatives. And the alternatives that are compatible with some service requirement can differ in the degree of correspondence to it, depending on the values of the criteria.

On the other hand, for each problem there can be both "obligatory" and "desirable" service requirements. The former ones determine the alternatives that can be considered, and the latter ones should be used for choosing the most preferable of the possible alternatives.

So, there are two types of AHP problems to be solved:

1. Determining the degree of correspondence of alternatives to the service requirements, depending on the values of the criteria (see Figure 4.2);
2. Determining the degree of correspondence of alternatives to the global goal, depending on the degree of their correspondence to the service requirements (see Figure 4.3).

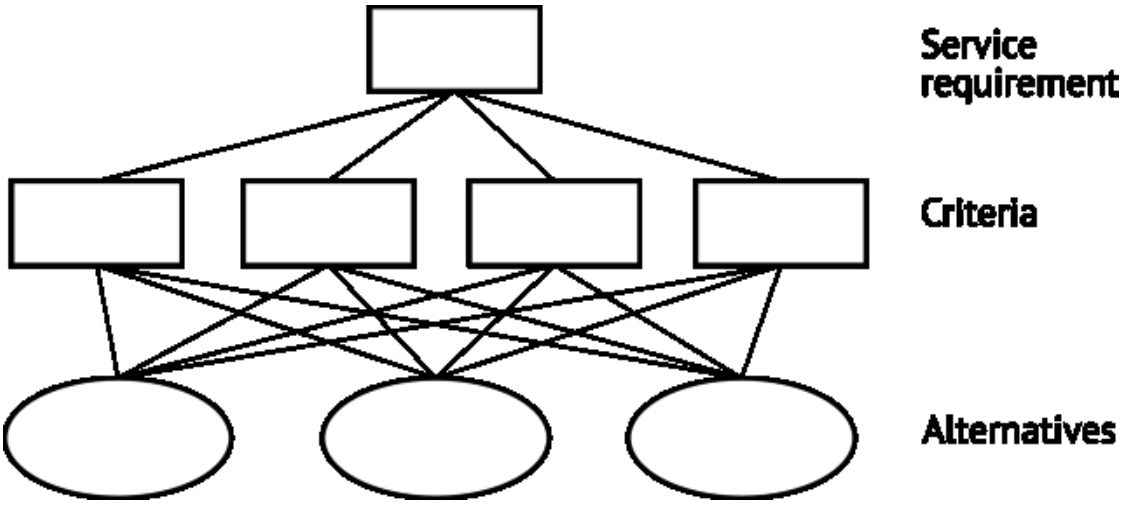

Figure 4.2: AHP hierarchy for service requirements

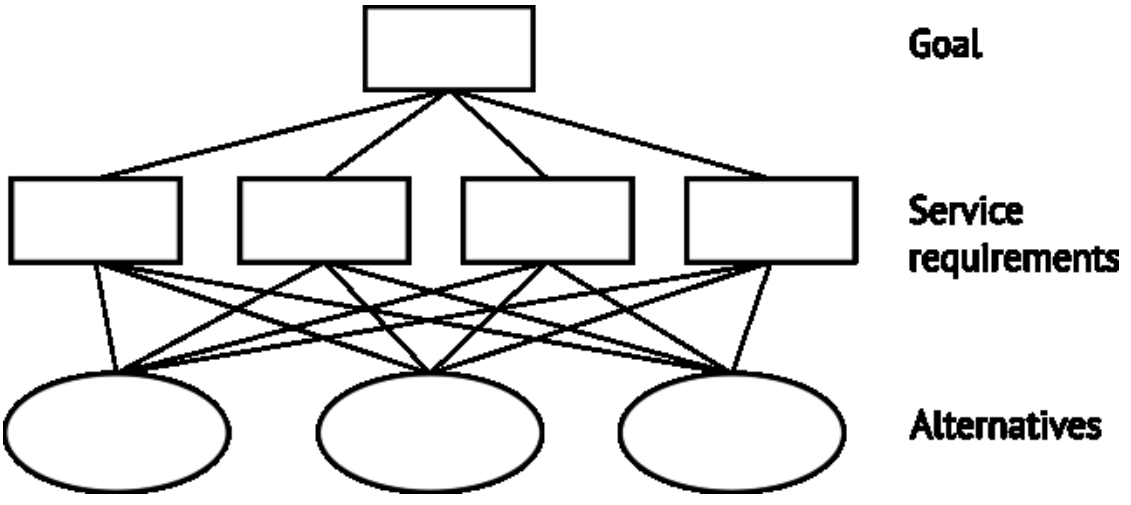

Figure 4.3: AHP hierarchy for the global goal

In result, the following procedure should be realized for different problems:

1. Determining the obligatory service requirements;
2. Determining the desirable service requirements and their priorities;
3. For every service requirement:
   (a) Determining the alternatives compatible with it and assessing their priorities;
   (b) Determining the priorities of the criteria;
   (c) Assessing the priority of each alternative compatible with the requirement;
4. Determining the set of the alternatives compatible with all the obligatory service requirements.
5. Calculating the global priority of each alternative of this set.

The steps 3.1 – 3.3 can be fulfilled independently, as they don't depend on the global goal. That gives us the possibility to distinguish the assessment of the degree of relevance of the alternative to the service requirements from the assessment of the service requirements for every certain problem, which allows us to simplify the researchers' work, and to make the results comparable and applicable for repeated use, as mentioned above.

4.4 Future work

The task of efficiency assessment in WSNs is extremely complex, and it is far from complete solution. In particular, none of the existing approaches is fully applicable to sensor control networks (SCNs, see Section 6.4).

Like in other converged networks, in SCNs every element can have several role functions simultaneously. In particular, a sensor node in a WSN can perform gathering, processing, transferring and routing of data, and fulfill some part of the decision making process, too. That is why any choice on, for instance, data transfer method affects in WSNs the process of data processing; hence, different choices should be made in different conditions. This means that the priorities of criteria are no more constant, as in AHP; and each alternative has its own set of priorities of criteria.

Thus, a new, more general framework should be developed, that would be applicable for recently appeared types of networks, such as SCNs.

Chapter 5
Usage of WSNs for critical tasks

Consistency of decisions, discussed in the previous chapter, is a desired design goal for every use case of WSNs. However, there are a number of tasks where every decision is required to be well-founded and validated, because they have a direct impact to human life, health and security. These tasks are considered separately, because they have problems and issues as well as design approaches that are not relevant for common tasks.

5.1 Problems and issues

5.1.1 Overview

The limited capabilities of a sensor node, such as restricted processing capabilities and a limited amount of energy, have an impact on all the parameters of a WSN. Taking into account the energy characteristics of transmitters in sensor nodes and their high susceptibility to interference, the quality of communication between sensor nodes can vary significantly with time. That is why the information loss and substantial delays often occur in WSNs. And their impact is closely associated with the size of a WSN.

Also, in order to save energy, sensor nodes in most WSNs are in the low power state (the sleep mode) most of the time, as mentioned in Section 2.2. At the low power state, all the components of a sensor node except the microcontroller are switched off and inside the microcontroller only a small portion of internal blocks are switched on. Moreover, in most applications, the amount of calculations, performed by the microcontroller at a sensor node, is reduced to minimum. This technique allows to extend the WSN lifetime up to several months or even several years.

For a typical monitoring applications information losses and shortage of the processing capabilities are not crucial, because dropping of one or several measurements does not have a strong influence on the result of the processing of the data from the whole WSN.

Tolerance to partial loss of information due to the low communication quality is the main difference between common WSN applications and WSN applications for critical tasks. The critical tasks here and later will reference to such applications where the data received from the WSN is used as basis for responsible decision-making. The exact criteria for determining whether task is critical or not, are out of scope of this technical paper. This we describe only the main peculiarities and give a few examples of critical tasks.

Applications of WSNs for critical tasks in comparison with applications for common tasks have stronger reliability, information security and quality of service (QoS) requirements. Clauses 7.2, 7.3 and 7.4 describe some relevant applications of WSNs for critical tasks.

5.1.2 Security and privacy

Wireless media is much more vulnerable than wired media for attackers. In critical tasks information security problems are particularly important since a security breach can result in a variety of negative effects. WSN applications for critical tasks are required to support integrity and confidentiality of the data exchanged during the application operations. These applications are required to provide security of exchanged data against malicious attacks. It is recommended to provide a secure channel to protect the data flows.

Data encryption and authentication are common information security techniques used in WSNs [50]. Restriction of access to the WSN settings and to the collected information is also a necessary measure of protection. These techniques in conjunction with the appropriate organization of interaction of sensor nodes in the WSN allow to achieve required level of security and privacy.

5.1.3 Fault tolerance

Errors in a WSN can occur for the following reasons: malfunction of one or more of sensor nodes, the change of environmental conditions, the actions of the attacker. According to most common practices, sensor node can be considered as failed if it sends measurements which significantly deviate from the results of the neighbor sensor nodes [51]. A faulty sensor node can be identified by the WSN as workable but provide bad measurement results.

A WSN intended for critical tasks has to operate well even if some nodes fail. In order to ensure a given level of fault tolerance, appropriate error correction mechanism must be provided. Besides, the WSN is required to ensure reliability and availability of the WSN infrastructure in order to handle a single sensor node failure. In case of such failures, the capabilities of the failed sensor nodes can be dynamically delegated to sensor nodes in order to provide consistent functioning and to prevent failure of the critical task.

5.1.4 Context Awareness

Context involves the information which can be used to describe the state of some physical object. This information has to be considered when making responsible decisions based on WSN measurements. For example, many of the processes are affected by temperature and time of day (especially in e-health applications). Without consideration of such dependencies, the data obtained from the WSN can be interpreted incorrectly.

Data processing and decision-making systems of the WSN should also take into account the natural noise in sensor nodes, possible node failures and other sources of context information. For this purpose, context information is required to be collected, stored and used for decision making.

5.1.5 Quality of Service

The strict reliability requirements are often a key challenge for WSN utilization for critical tasks. Some applications require low latency in updating sensor readings, others may require high accuracy of measurements. Time response and accuracy characteristics of a WSN affect the accuracy and timeliness of the decision-making. Critical tasks ordinary need high levels of both of these parameters. Appropriate QoS mechanism must be implemented to make sure that QoS requirements are satisfied [52].

5.2 Emergency management

Emergency management is a good example of critical tasks where WSN can find its application [53]. Telecommunications during an emergency play crucial role in rescue coordination. And WSNs, and, in particular, sensor control networks (SCNs) which are considered in Section 6.4, are well applicable in this field because of easy deployment and self organization features. Besides monitoring the state of emergency and providing communication in emergency situations, WSNs have another potentially important application concerning emergency situations and saving people's lives. This application was described in [54].

An indoor emergency management system is based on SCNs. The main goal of the system is to provide everyone in the building with instructions concerning the appropriate way of evacuation. The system uses a personal mobile phones or tablet computers to deliver information to their owners. So every mobile device turns into a terminal of the rescue system in case of emergency. It is very reasonable due to the wide spread of mobile devices and because of the presence of additional communication channels in today's mobile devices.

At the entrance to the building a mobile user terminal automatically connects to the SCN infrastructure and obtains data from the SCN motes. While normal operation, system uses SCN motes to observe the physical conditions inside the building (temperature, smoke, etc.) as shown in Figure 5.1. When an emergency occurs, SCN motes automatically detect it. Then the information

about the detection of signs of disaster spreads throughout the SCN and user terminals. Each user terminal automatically launches software for guidance in emergency cases. It gives instructions on the safest way of self-evacuation from the building. For example it can show one of the following: evacuation plans or maps; step-by-step sound commands and visual hints (e. g. interior photos with arrows towards the exit overlaid); videos showing how to use safety equipment. Especially important that the information displayed varies depending on the location of the user.

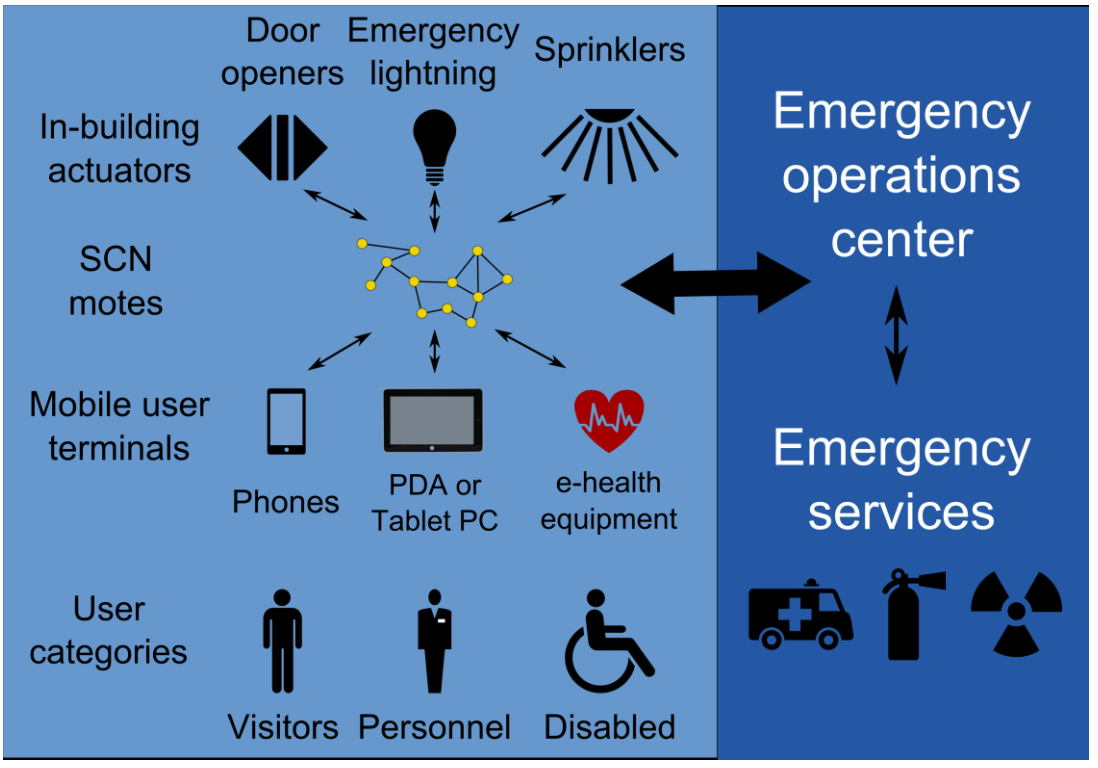

Figure 5.1: Emergency management system

The content of the instructions, which the system gives through the device to the owner, depends on various factors, for example:

- State of the building like accessibility and hazard level of rooms and escape routes. The state is determined by SCN motes;
- Position of the user determined by the nearest network node or using the GPS or GLONASS;
- User's health state determined by the e-health equipment.

User peculiarities awareness is a crucial feature of system. It means that while the personal mobile equipment is used the owner can chose appropriate customization options in software. These options will have impact on the instructions shown by the system. For example, a person with disabilities will receive special self-evacuation route, equipped with necessary facilities. Another example of customization is special instructions for building personnel. The system will remind them if they have specific duty responsibilities in case of emergencies. Also, the system will point to location of people with disabilities who need help.

In-building actuators (e. g. automotive door openers, emergency lightning and sprinklers) should also be equipped with SCN motes. Such actuators will also get commands from the system and start working if necessary.

5.3 Verification networks

Verification networks [55] are intended for the systems that operate automatically without human intervention. For a machine actuation unit in such automated system there exists a set of critical operations. Such operations can cause considerable negative consequences when carried out in improper system state. To avoid this for each critical operation a set of verification rules should be defined, which must be checked up before this operation and/or while the operation is in progress. Verification network can be designed to test these conditions. This type of critical task can be solved by using WSNs or SCNs. In this case the WSN should provide some kind of addition context awareness for automated systems.

To check verification rules the values of a number of parameters must be determined. Such parameters can be:

- Aggregate values, reference values, sensor readings presenting in SCN as part of normal flow of decision-making;
- Aggregate values, reference values, sensor readings presenting in SCN which are only intended to support verification;
- Sensor reading obtained from the machine actuation unit's own sensors;
- Values obtained by request from SCN server or other servers in NGN.

Verification network may have much more strict requirements concerning the reliability, security and performance. Data processing and transmission in a SCN for the purpose of verification may have higher priority in QoS in comparison with other activities in the SCN.

In Figure 5.2 a normal SCN decision-making flow is shown (see Section 6.4), but as soon as decision sets a machine actuation unit in motion, the verification process starts up by the verification network. If some of the check-ups of the verification process fail, some safe action (or no action) is performed instead of the action supposed in the decision.

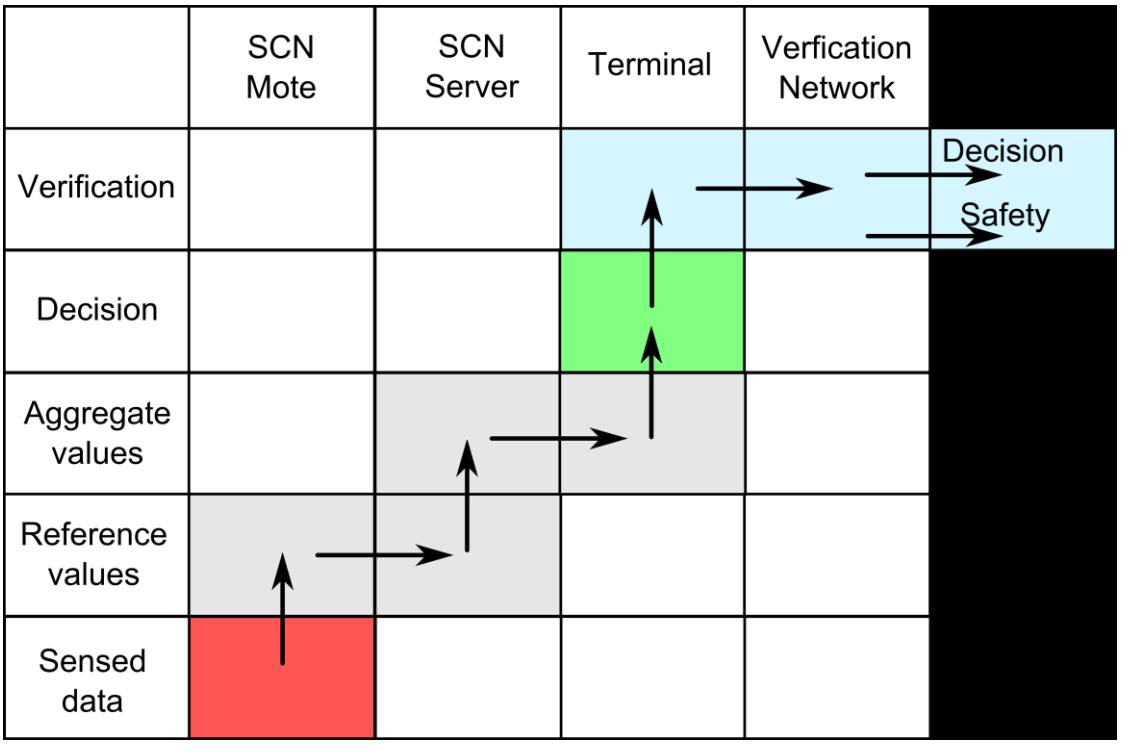

Figure 5.2: Verification network's decision-making flow

5.4 E-health

5.4.1 Overview

There is a wide variety of e-health applications for WSNs. Most of them have been proposed during last ten years. Some of these applications include: patient monitoring, emergency informing of physicians and emergency services, and providing user-friendly home environment. The majority of e-health applications use WSNs as a part of a complex system which includes also a global communication channel, system of remote processing of collected data and more comprehensive and complex health and rescue systems. General scheme of an e-health WSN-based system is shown in Figure 5.3. Patient is equipped with wearable or implantable sensor nodes, which perform continuous measurements of the patient health state (e.g., blood sugar level, body temperature, blood pressure). Sensor nodes form a WSN, which transmits the gathered measurements to user's mobile terminal, e.g. notebook or smart phone. The user's mobile terminal performs measurements processing, result indication and transmitting of the results to the attending doctor using a wide area network (e.g. a cellular network).

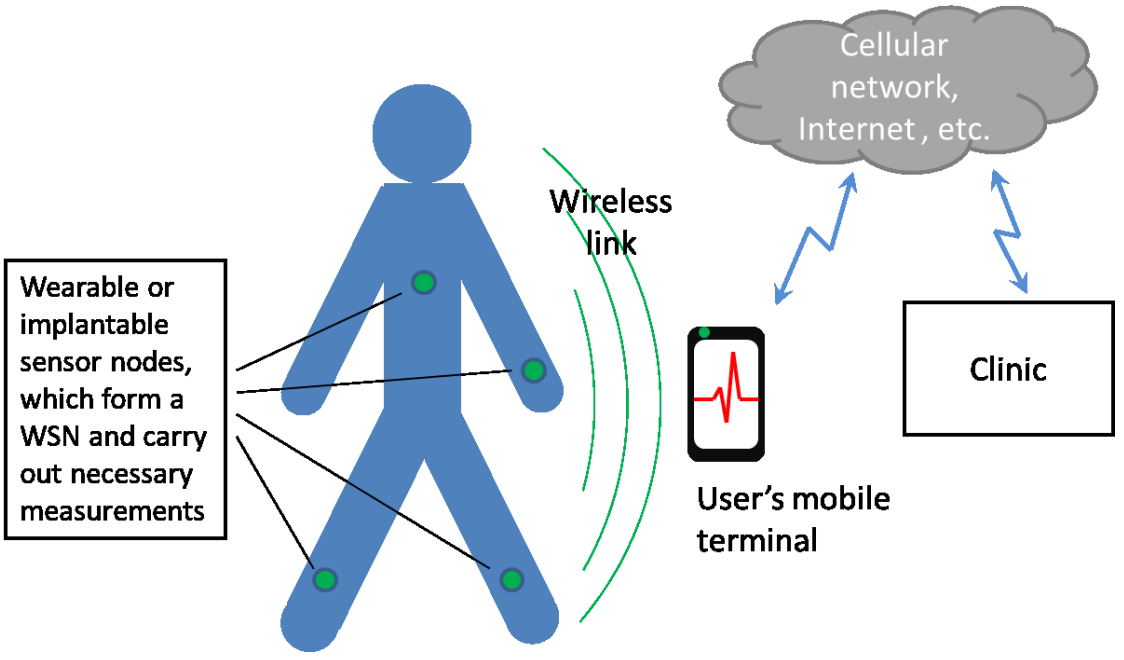

Figure 5.3: General scheme of e-health system

There are also patient continuous monitoring systems which don't interact with the patient's mobile devices. Such systems are equipped with an independent transceiver, running on a dedicated wireless communication channel of the direct link with the clinic. This independent communication channel brings travel restrictions, because the patient should be within the range of the used channel. However, such an approach can help to avoid the data loss and unexpected delays by choosing special design techniques for channel planning. The independent communication channel ensures the reliability for e-health system communication, including during global emergency situations when cellular network may be unavailable.

5.4.2 Relevance of e-health applications

E-health applications are very relevant for several reasons. The first reason is convenience. For example, remote monitoring allows patients to reduce the number of visits to their physician. This is important, because sometimes patients prefer not to have a regular health examination in order save their time. This leads to complication of their diseases. Many patients miss scheduled visits to clinic

also because of fear of overexertion or transportation cost. The second reason is the completeness of the data gathered by the e-health systems. For example, the remote monitoring system cannot replace expensive equipment in hospitals and inspections by a professional doctor. However, such systems may perform measurements of some of the major health parameters (temperature, heart rate, etc.) of a patient during a long time. This system provides the physician with additional information that cannot be obtained from one-time visits. This can greatly improve the accuracy of diagnosis and adjust the dosage of drugs. In addition, an e-health system can automatically inform the attending physician about unacceptable values of the patient's health parameters. In case of exceeding body temperature, blood pressure, an abrupt change of the patient's pulse, the e-health system can immediately send this information to the attending physician. Herewith an ambulance call can be sent automatically. This ensures prompt response of medical services to changing of health of the patient and reduces the risk of adverse effects to him or her.

Continuously collected data from different patients can make up significant statistics on various diseases. This statistics could help in medical research. E-health systems are also able to save labor costs for care and examination of patients, and therefore reduce the cost of treatment.

5.4.3 Opportunities of e-health

Due to the development of the MEMS technology for sensitive elements of sensor nodes and the miniaturization of sensor nodes, WSNs become more and more attractive for e-health applications. WSNs can be used to create wearable systems, which would provide necessary monitoring of the health status but would not restrict normal lifestyle of the patient. The active work of the researchers in this area has led to creation of a number of sensing elements, which become available for e-health applications. The list of available sensitive elements includes: blood pressure sensors, temperature sensors, blood flow sensors, oximeters (blood oxygen level sensor), pulse oxygen saturation sensor, electrocardiogram (ECG), electromyogram (EMG), respiration sensor [51], glucose level sensor [56]. Created on the basis of these sensitive elements designs affect many areas of medical care. Some of WSN applications for e-health applications will be described below.

5.4.4 CodeBlue

CodeBlue is a project of Division of Engineering and Applied Sciences of Harvard University. This work was one of the largest academic researches in the WSN applications for medical care. One of the solved problems of this research was creation of protocols providing high QoS for WSNs [57]. The requirements of the field of the research impose high characteristics in miniaturizing of sensor nodes, communications reliability, mobility, information security. CodeBlue proposes the protocols for device discovery and publish/subscribe routing, as well as a simple query interface that is tailored for medical monitoring [57].

Also some healthcare-specific sensor nodes have been developed:

- Pulse oximeter (a sensor for non-invasive reliable meter of key patient health metrics: heart rate and blood oxygen saturation);
- Electrocardiograph that uses measurements of the differential across a single pair of electrodes;
- Motion analysis board that incorporates accelerometer, gyroscope and surface electrodes for EMG recordings.

5.4.5 Monitoring of patients with Parkinson's disease

WSNs were proposed for monitoring patients with Parkinson's disease (PD) in the papers [58 ,59]. The main goals of the research were augmenting or entirely replacing a human observer and to help the physician to fine-tune the dosage of medication. Balanced medication is necessary for PD, it helps to achieve normal movements free of tremor for patient [59].

A wearable system was developed that can reduce personnel cost and help a physician to fine-tune the medication dosage [51 ,59]. This system provides 17 hours of continuous measurements of

patient movements. Sensor node was equipped with 3D accelerometer and provides sample at a rate of 40 Hz. The report reveals that the system was able to identify the occurrence of exaggerated involuntary movements cased by highest concentration of medication at the rate of 80% [51].

A more modern system operating by the similar principle [58] is capable of storing data from the accelerometer continuously for more than 80 days at a sampling frequency of 50 Hz. In addition to the 3-axis accelerometer, the sensor node platform provides interfaces for gyroscope, ECG, EMG, tilt and vibration sensors, and a passive infrared (PIR) motion sensor.

5.4.6 Monitoring of heart diseases

Electrocardiogram (ECG) is the most widely used technique for capturing rhythm disturbances. In addition to providing continuous monitoring and analysis of physiological parameters, the *body sensor networks* (BSN) incorporates context aware sensing for increased sensitivity and specificity [60].

BSN provides a number of sensors nodes for ECG and pulse oxygen saturation measurements. Context awareness is provided by sensor nodes equipped with accelerometers, temperature and humidity sensors. WSN signals are gathered, displayed and analyzed by the personal user terminal. All measured data is transferred using Wi-Fi or GRPS networks for storage and analysis if necessary.

5.4.7 Summary

This section does not cover the whole list of studies in the field of WSN applications for e-heath. However, it is obvious that WSN technology is of great interest for practical medicine. The major manufacturers and academic institutions were taken a lot of research activities and experiments on the use of WSN for e-health applications. Despite the fact that during these research works a variety of platforms have been developed, WSNs are not widespread in this area. A lot of work had to be done in future to achieve high cost-efficiency and QoS characteristics for WSN-based e-health systems [52].

Chapter 6
ITU-T Recommendations related to WSNs

Standardization is part and parcel of ICT effective development, so it's useful to consider the basic standards and recommendations while studying wireless sensor networks. In this chapter we're going to consider the recommendations created by the International Telecommunication Union (ITU). All ITU recommendations related to WSNs define the high-level requirements applicable to every type of WSN irrespective of the underlying hardware and protocol stack. That is why the recommendations we're going to consider in this chapter don't intersect but supplement the protocols specification previously described in this technical paper.

6.1 Requirements for support of Ubiquitous Sensor Network (USN) applications and services in the NGN environment

As clear from history overview, in the mid 2000's WSNs were already widely used for solving various practical tasks, such as industrial automation, monitoring and control, home automation, environmental/agricultural, e-health, etc. At the same time the first practical WSN protocols connected with data transfer via radio, routing, self-organizing, self-healing had been created. The essence of the next WSNs development level was integration of various types of networks within the frameworks of common platform, transition from a great number of uncoordinated sensor networks to intelligent information infrastructure of advanced e-Life society. This process was reflected in the Ubiquitous Sensor Network (USN) concept.

6.1.1 Origin

The discussion on USNs was started in February 2007 by Electronics and Telecommunications Research Institute (ETRI) (Korea) on the TSAG meeting. The meeting considered the idea with interest and reached the consensus of the importance of USN study, so that it was noted that some activities related to USN were already undertaken in the framework of several Study Groups of ITU-T. It was therefore felt necessary to reinforce the coordination in order to progress the studies on USNs, and in this respect it was decided to start a new work item on general USN issues in Study Group 13. In January 2010, after almost three years of active work, Recommendation had been approved and got the number Y.2221.

6.1.2 USN description and characteristics

Recommendation Y.2221 [20] defines the USN as a conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness. In this definition "physical networks" means not only various types of WSNs, but also wired sensor networks and RFID readers.

Figure 6.1, which represents the plan of USN structure, illustrates a few intermediate essences in addition to previously mentioned in USN definition physical networks and services. Let's consider theirs details.

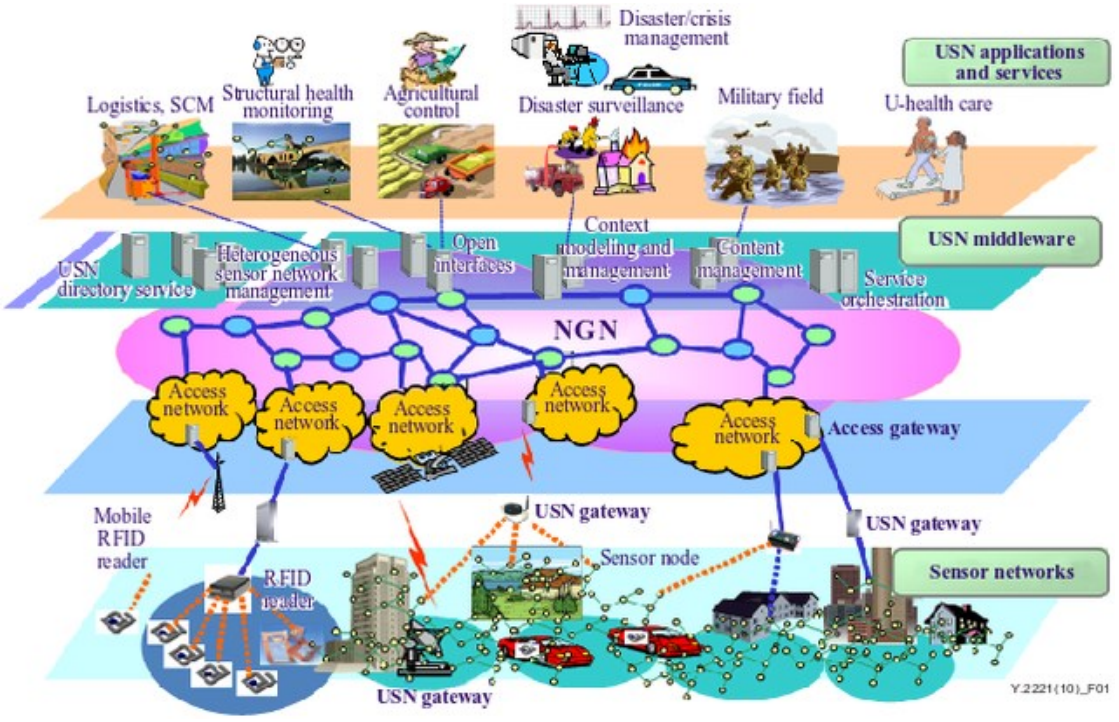

Figure 6.1: An overview of the USN

First of all, an additional layer *USN middleware* is being introduced. The USN middleware is software on a special server which works as a mediator between physical network and its users. It is intended to hide all the complications of physical networks from a developer and to give convenient API which can help to control network and get access to sensed data and related information: sensor location, network structure, devices' health and battery level. Moreover, middleware can be responsible for specific elements examination, organizing of query plans, fault detection and elimination, control of devices' power supply, authentication, encoding, providing of confidentiality, data storage, data filtering, data mining and other similar tasks which are common for different services and applications. As a result, applications can be developed in loosely-coupled way, i. e. disregarding peculiarities of specific physical networks. This offers the following advantages:

- From the physical network vendor's point of view – expansion of service range supported by the sensor networks produced by the vendor;
- From the service provider's point of view – increasing the number of target platform, i. e. physical networks produced by various vendors, which can be used for service providing;
- From the applications developer's point of view – easier development which helps to reduce expenses on the new features addition, problem detection and recovery, porting applications to various platforms (for example, creation of new mobile and web interfaces);
- From the commercial point of view – changing from the vertical business model to the horizontal one, when instead of one big company which gives the full range of solutions there can be a few different providers and vendors competing in the market.

In USNs *NGN* serves two functions: transport and service. The transport function means providing connection between separate sensor networks and users from any place in the world. Also these sensor networks can be connected with each other creating a common structure. Separate clusters of sensor networks can connect to NGN *access network* both directly and through the *USN gateway*. The use of USN gateway is necessary when sensor network works with a protocol

incompatible with IP.

The service function of NGN consists of providing for the users the same possibilities in sensor network services that in other NGN services: access to services through various terminals, intuitive and consistent user interface, providing QoS across different provider networks. By comparison with other NGN services USN services have a range of specific features. As a result, NGN have to keep on enlarged capabilities set to answer USN-specific service requirements. List of these requirements and their rationale along with corresponding NGN capabilities are the matters of the rest of the Recommendation Y.2221.

6.1.3 Service requirements of USN applications and services

The following paragraphs deals with the requirements of USN applications and services. Recommendation Y.2221 considers for the most part only requirements affecting extensions to the set of NGN capabilities. Other requirements, which don't have any influence on NGN capabilities, are given in the Recommendation's appendix for informative purposes and will not be considered in this technical paper.

USN applications and services require the following NGN capabilities:

Sensor network management, configuration and reconfiguration. In USN environment, it is required to manage diverse types of sensor networks. Configuration and reconfiguration of sensor networks may require different mechanisms than traditional network management, as sensor networks are normally a group of nodes. A sensor network must not lose its connectivity or its functionality despite the loss of a connection to a single node in the network due to link or hardware failure, which has a high probability of occurrence in sensor networks. Configuration and reconfiguration of a sensor network are used to support assurance of connectivity and lifetime management.

Service/device profiles. Here profile means a record in database which contains information about services offered by the USNs and devices functioning in a network. Service profile information may include service identifier, data types, service provider, and location information. A standard set of USN service profile makes it possible for the user to orientate oneself quickly while connecting to new networks and to select services according to one's demands. Device profile is used for ensuring functioning of various types of sensor networks made by different producers in a certain USN. The information of device profiles may include sensor network identifier, device identifier, device types, capabilities and location. Thus, service/device profiles are used to simplify working in heterogeneous networks which may contain a large number of coexisting devices and be providing different types of services at the same time.

Building of open service environment. The concept of open service environment is described in details by Recommendations Y.2020 and Y.2234 [61 ,62]. The OSE's main idea is to apply standard application network interfaces (ANIs) for accessing application and services. Due to standardization, application providers and developers are able to create and introduce applications quickly and seamlessly. OSE offers various capabilities. For USNs the most important of them are as follows:

- Service registration — managing the information about services (i. e. service profiles, described in the previous item).
- Service discovery — searching by the user against all registered services and giving him related service information.
- Service composition — capability of creating new services from other existing services by the reuse of existing resources. Service composition can occur in a static or in a dynamic way. While in static composition, composite services are defined in advance, dynamic composition sends the request for service discovery using the service description to find the needed services and composes the services during run time.

- Service coordination — the ability to manage the relationships and interactions among services to provide a "service chain", i. e. a set of interconnected services which have to be offered in a specific sequence.
- The use of service description language (SDL) for formal (i. e. understandable for machines) describing of functionality, offered by the services. Example of SDL used in practice is XML-based web services description language (WSDL), created by World Wide Web Consortium. It is necessary to use for USN its own SDL in accordance with its peculiarities.

Differentiated QoS and data prioritization. Different types of services have different demands on transport capabilities of a network. For example, if sensed data are used to take decisions immediately, it is possible to make demands on latency. If urgent and important data transmission through a certain channel is planned, its full capacity or a part of it can be reserved. For example, emergency notification of a fire incident must be delivered in a timely and reliable way to the appropriate disaster monitoring systems. Less important data can be transmitted on a best-effort basis, meaning obtaining unspecified variable bit rate and delivery time, depending on the current traffic load. Each requirement, similar to those previously mentioned, will be defined by *quality of service (QoS)*. Many network protocols make it possible to specify the type of QoS one or other data relate to, and hence define priority of their transmission and processing.

USN services have unique characteristics in terms of service priority. For example, sensed data may be sent to central node not immediately, it is possible that measuring results at first are being gathered by a sensor node or by a few nodes, and then be sent with other measuring results within one transaction. The application transaction volume may be very high. So, particular demands on QoS can be made in order to manage the transaction volume generated by USN applications and services and to make it possible to avoid access concentration to a single resource.

Support of different types of connectivity and networking. In USNs sensor nodes can be IP-based or non-IP-based. In the first case, although the underlying wired and/or wireless media access control manages the connectivity, connections between USN end-users and sensor networks are implemented through the IP. In this type of sensor networks, it may be possible that a single sensor node is directly connected to the infrastructure networks without a USN gateway. In non-IP-based sensor networks, sensor nodes do not have IP addresses, and the connections between USN end-users and sensor networks are possible only through the USN gateways. Non-IP-based network interface can be used for different reasons, such as impossibility to give its own IP address to each node of sensor network, limited computational capability of sensor network's nodes which don't provide IP-stack support, battery's energy saving owing to refusing of processing IP-package operation which requires high computational capacity.

Both types of networking have to be supported, moreover, various types of wired and/or wireless media connections can be used for connectivity between sensor networks and infrastructure networks.

Location management. Location management capability is specified in the Recommendation Y.2201 [63] regarding the location of *users and devices* within networks. In this document location management means possibility to use information regarding the physical position of objects, hence enhancing applications with local context and relevance. Besides, in USNs the location of *sensor networks and individual sensor nodes* needs to be maintained and managed in order to support context awareness with location information for USN applications and services. In addition, service and device discovery can be facilitated by the usage of the location information.

Mobility support. Mobility, as specified in the Recommendation Y.2201, involves the ability of mobile objects, such as users, terminals and networks, to be able to roam between different networks. Two types of mobility are considered: *personal mobility* where users can use registration mechanisms to associate themselves with a terminal that the network can associate with the user and *terminal mobility* here registration mechanisms are used to associate the terminal to the network.

Providing terminal mobility in USNs may prove to be a difficult task. Existing IP mobility technologies can be adapted for IP-based sensor networks. However, to port heavy IP mobile mechanisms into very low-power, low-rate sensor networks pose various challenging issues.

In addition to above-mentioned classification, in USNs there can be three more types of mobility:

- Intra-sensor network mobility: a sensor node moving within a sensor network.
- Inter-sensor network mobility: a sensor node moving across multiple sensor networks.
- Network mobility: A sensor network moving across infrastructure networks (e. g., across NGN and non-NGN).

A scenario illustrating mobility requirements can be found in the healthcare application domain. For instance, medical check-up data of a patient may be monitored via a sensor network. Several sensors may be attached to the patient, resulting in a body area sensor network. The sensors periodically gather the medical check-up data and send them to patient's doctor via a home-gateway when the patient is at home; while moving, the data can be sent via an access gateway in a network-enabled car, bus, train, or subway. Various cases of mobility may occur in such an application scenario.

Security support. In general, USN applications and services require strong security, due to very sensitive sensed data. That is why ITU has created a set of Recommendations on security in USNs, which is going to be considered in details below in this technical paper.

Identification, authentication and authorization. Identification (procedure of subject recognition), authentication (procedure of verification), authorization (conceding rights to do some actions) are often considered together, because they all are intended to prevent unsanctioned network using and data accessing. In USN applications and services, data can have different levels of authentication requirements. For example, in military systems, raw sensed data are as important as service data which are derived from raw sensed data by processing and manipulation from service providers or applications, while this may not be the case for other systems (e. g., hospital systems). Thus, different levels of authentication for different types of data based on the requirements of USN applications and services should be supported.

Privacy support. When using USNs, there is a danger that unauthorized parties can get access to the critical information. For example, the mere observation when and where events within a USN occur may compromise the security of the USN itself as well as the security of USN end-users. In this connection, special privacy measures are required in USN. These measures will be considered in the part of his technical paper which deals with USN security Recommendation series.

Support of different accounting and charging policies. General NGN accounting and charging capabilities are specified in Y.2233 [64]. USN may require support of different accounting and charging policies according to different data transaction types. As an example, there are USN applications and services whose sensed data do not have to be continuously transmitted to the application systems, but it is sufficient if they are transmitted, at least once, within a certain period of time. In these scenarios, the network connections may stay in an idle state for a long time. On the contrary, some other USN applications and services may continuously generate and transmit streaming data. It is obvious that each of these cases requires a special approach to accounting and charging.

6.2 Service description and requirements for Ubiquitous Sensor Network middleware

6.2.1 Origin

In 2008 a lot of the most advanced researches in the field of WSNs (and USNs in particular) were concentrated in Korea. In Electronics and Telecommunications Research Institute (ETRI) and

Sejong University the experiments on using WSN for offering services to mass consumer have been conducted. One of the key technical problems, which had arisen, was gluing together the network hardware, operating systems, network stacks and applications [65]. Solving that task was the goal of COSMOS (Common System for Middleware of Sensor Networks) Project [66 ,67], a middleware platform developed by ETRI. As a result, in January 2008, at Rapporteur meeting in Seoul, January 2008, the decision was made that the work on USN middleware could be started at ITU-T Study Group 16 ("Multimedia coding, systems and applications"). In April 2008 the initial text of the Recommendation "Service description and requirements for ubiquitous sensor network middleware" had already been presented. Afterward that work item had been referred to Study Group 16, which dealt with multimedia. Recommendation was received in 2009 under number F.744.

6.2.2 Description of USN middleware

F.744 [68] defines the USN middleware as a set of logical functions to support USN applications and services. The reason of using USNs is the fact that to offer various services in a USN it is often necessary to solve the same tasks, such as:

- finding appropriate sensor networks to obtain sensed data;
- requesting raw sensed data and/or processed data;
- processing received sensed data;
- activating actuators;
- monitoring sensor network status;
- controlling sensor networks;
- authenticating sensor networks;
- providing appropriate services to users.

Concerning complexity, scalability and cost-effectiveness, it would be beneficial to support functions by a separate entity rather than by each USN application and service. The USN middleware is exactly such an essence. It receives requests from USN applications and delivers those requests to appropriate sensor networks. Similarly, the USN middleware receives sensed data or processed data from sensor networks and delivers them to appropriate USN applications. The USN middleware can provide information processing functions such as query processing, context-aware processing, event processing, sensor network monitoring and so on.

6.2.3 Service providing in USNs

An important part of F.744 deals with the description of use cases of USN services. For each of them there is a description of sequence "steps" for service providing. Before considering concrete examples, it is useful to take a look at these steps in general. Of course, one or other service providing process may not require all given steps, also some steps can be added according to concrete needs.

- **Generating rules.** Managers or operators of an application should generate appropriate rules to determine a course of action to deal with various events whose arising can be detected. For example, a healthcare application may react to pulse rate measuring and call a doctor in the case of a critical aberration from the norm. The rules can use context information, such as residents' medical histories. When the rules are generated, they have to be registered to the USN middleware.
- **Sensor network authentication.** When a sensor network tries to connect to the USN middleware, the USN middleware authenticates the connecting sensor network to protect itself against deceptive sensor networks. This authentication step is very important to protect the USN services from fraudulent data.

- **Application authentication.** When the application requires connection to the USN middleware, the USN middleware authenticates the connecting application to protect itself from unauthorized application.
- **Sensing.** Sensor nodes are installed on the objects which require monitoring. After being turned on, each sensor node senses physical parameters then periodically sends that sensed data to the USN middleware.
- **Access to metadata.** The USN middleware can offer metadata directory service, i. e. to give various metadata to find appropriate resources such as components or sensor networks. If some services are required to monitor an area, then the USN metadata directory service can help to look them up. The USN directory service offers all relevant information such as location, wireless protocol, sensor type, number of sensor nodes, sensor network lifetime, etc. [65]
- **Collecting of sensed data.** The USN middleware collects sensed data from the appropriate sensor networks, based on the requests of USN applications. The USN middleware may send the requests to the target sensor networks and RFID readers to collect data, or they may periodically send sensed data to middleware without any requests. Sensed data aggregation (e. g. averaging of temperature in building monitoring application) may be performed.
- **Activating of actuators.** If certain rules have been generated as a reaction to events whose arising is detected by a sensor network, actuators can be activated. For example, in cold chain management application meant for monitoring food delivery conditions the refrigerator (actuator within the sensor network) can be activated to decrease the temperature when it exceeds certain level.
- **Displaying the status.** In a control center operator can see on the screen all the information relevant to USN status. Furthermore, operator can receive alarm notification if some abnormal conditions arise. To increase the amount of information some additional facts can be reported. For example, instead of numeric sensor id in healthcare application the resident's name can be used, and, if it is necessary, information on his patient case history may be given.
- **Stopping.** When the application is about to stop its service, it may request the USN middleware to no longer collect data from the sensor networks.

6.2.4 Use cases of USN services

According to Recommendation F.744, USN services can be categorized into three groups, based on the above observations:

- using only sensed data (e. g., healthcare applications);
- activating one or more actuators, based on the sensed data (e. g., cold chain management applications);
- monitoring and/or controlling sensor networks (e. g., sensor network monitoring applications).

To illustrate how USN services and USN middleware work together in these three situations, there are three use cases given as an example.

Healthcare applications. A healthcare application continuously monitors the location and the health status of the persons within the range of a sensor network in buildings, in order to handle possible emergencies. Every resident wears a sensor node on his/her wrist, which looks like a wristwatch. The sensor node senses body temperature, pulse, momentum, and electrocardiogram (ECG) of the resident and then periodically transmits the sensed data to the USN application. A healthcare application displays the current location and health condition of the resident based on the sensed data. Emergency notifications are delivered to the related authorities such as a hospital, a police station and the relatives or family to handle the situation appropriately.

Cold chain management application. A cold chain management application uses sensed data to

monitor the condition of a delivery system. Sensor nodes are installed in delivery vehicles and storage buildings of distribution centers. They sense temperature and send the data to a cold chain management application to report the current status of the delivery environment. If unusual conditions are detected, then a cold chain management application alerts operators to such unusual conditions.

Sensor network monitoring application. A sensor network monitoring application monitors the various sensor networks. The purpose of a sensor network monitoring application is to check and to control current state of sensor networks. If a sensor network monitoring application detects abnormal conditions, it may request USN middleware to reset the sensor network.

6.2.5 Functional model of the USN middleware

Functional model given in Recommendation F.744 proposes the following classification of functions offered by the USN middleware:

- **Open application interface processing.** Access to all USN middleware functions is provided by means of application interface. Implementing new functionalities can be difficult if the interface is proprietary, that's why the condition of openness is very important.
- **Sensor network metadata directory service.** As described previously, metadata directory service provides access to information on sensor network, such as number and location of sensor nodes, sensor network lifetime, etc.
- **Application-independent data filtering.** Data filtering is provided to ensure that a program operates on clean, correct and useful data. Data filtering function may use validation rules that check for measurement units, data types and value ranges of sensed data to make it certain that there were not any mistakes in data receiving.
- **Sensor network management.** Network management is the process of monitoring and controlling the behavior of a network. Monitoring functions include collecting information about node states (e. g., battery level and communication power), network topology, wireless bandwidth, link state, and the coverage and exposure bounds of USNs. Control tasks are, for example, based on the collected network states controlling sampling frequency, switching node on/off (power management), controlling wireless bandwidth usage (traffic management), and performing network reconfiguration in order to recover from node and communication faults (fault management) [69]. Also the USN middleware can provide a possibility of remote software update for sensor nodes.
- **Query processing.** Amount of radio transmissions, as well as amount of energy used, can be reduced by means of transmitting queries on measurement results along with responses not immediately, as soon as they appear, but combining them in lines and reasonably planning processing of these lines. Query processing functions are responsible for creating query plans to request data, simultaneous scheduling for requests as well as processing for responses.
- **Sensor data mining processing.** The term "data mining" combines a lot of methods of intellectual processing of information. The main task of data mining can be defined as detecting in raw data previously unknown, nontrivial, practically useful information which can be interpreted and is necessary for making decisions. Outliners filtering is one of the simplest but still very important examples of data mining use cases. From time to time measurements may give incorrect results in every sensor network. Such errors can arise accidently, by reason of the statistic nature of measured quantity, as a result of a software failure of equipment error. Data mining methods make it possible to detect such errors and give to the user the "refined" quantities.
- **Event processing, context-aware rule processing.** One of the ways which makes working with a great amount of raw sensor information easier is using event models. Each event is a message which occurs when some conditions are being fulfilled. Event rules are used to solve

the task the application deals with. These rules describe the operations which have to be made when one or other event arises. What kind of operation it will be depends not only on the event itself, but also on the status of relevant entities, which forms a coherent environment as a context. The functions which belong to this group are responsible for generation of events based on raw sensed data and processing application-dependent context-aware rules.

- **Service discovery.** This group of functions is responsible for possibility of registration and searching of services provided by the USN and the USN middleware.
- **Sensor network common interface processing.** Sensor network common interface is made for connecting of creation of the abstraction which could make it possible to hide from the application developer the peculiarities of a concrete sensor node realization and also could make it possible to work with them as with the standardized objects.
- **Security service.** Security service functions include access control, secure channel provision, protecting the USN middleware from malicious attacks, etc. The matters connected with security in USNs are going to be considered in the next section.

6.3 Ubiquitous Sensor Network security Recommendation series

6.3.1 Security in WSNs

Providing security from attackers is a very important task in the field of WSNs, as well as in every computer network. Successful security problem solving defines if one or other technology will be used for crucial tasks (such as medicine, emergency management, military applications) or its applications will be used in laboratory researches and high-tech entertainment only.

A number of WSN peculiarities complicate the task of security providing. A part of these peculiarities deals with the physical level of WSNs. Data transmission via radio makes it possible for a attacker to capture transmitted information (eavesdropping), to misrepresent it (man-in-the-middle attacks), to disable the whole network or a part of it (denial-of-service, DoS attacks). Herewith, many information protection technologies (for example, complicated plans of key distribution) can't be used by reason of the cost and energy consumption of sensor nodes.

Another part of WSN peculiarities which affect security deals with the applications and services. Such applications as environmental monitoring intend installation of sensor nodes across immense areas. It makes physical protection of every node impossible, so, there is a danger of tempering by a perpetrator. Such conditions contradict assumptions of many "classical" information security tasks which are based on the fact that a perpetrator does not have an access to network objects.

Finally, security providing has become more difficult when Ubiquitous Sensor Networks (USNs) and Internet of Things (IoT) have been created. These both conceptions intend availability of a huge amount of sensor nodes and, therefore, the same amount of potential threat sources. In USNs all this quantity of objects can be distributed over the whole world. In IoT, in addition to this, some nodes can be connected not only to the objects of unanimated nature, but also to human organs. As a result, any, even the less significant, weak point may lead to global catastrophic consequences. In this connection, information security task in WSNs keeps being unsolved, so there is a huge amount of work to be done by researchers in this field.

6.3.2 Origin

One of the first research institutions dealing with security issues in sensor networks, was Carnegie Melon University (Pittsburgh, United States). Already in the early 2000s, this university conducted researches where privacy issues and the possible types of attacks on WSNs [70 ,71] were considered. Once this issue became widely discussed, proposals on how to ensure data encryption, authentication, key distribution as well as software and hardware implementations began to appear. There was a need for high-level standards which would formulate security requirements for WSNs, and in particular, for USNs.

That is why in 2007 TSAG of ITU-T proposed to start work on this subject. Study Group 17 supported this proposal and created three work items covering USN security:

1. X.1311: Information technology – Security framework for Ubiquitous Sensor Networks [72],
2. X.1312: Ubiquitous Sensor Network middleware security guidelines [73],
3. X.1313: Security requirements for wireless sensor network routing [74].

X.1311 is a basic document in a series of Recommendations considering security in WSN, and historically work on it was started first. The original text was proposed by representatives of the Korea Information Security Agency and was based on research conducted at Carnegie Melon University (see [71]). The initially proposed version of the text considered attack models, and classified the key management schemes. As a result of SG 17 work, in 2011 a document covering at a high level all the major security issues was simultaneously approved as an ISO/IEC Standard and an ITU-T Recommendation.

Recommendation X.1312 was approved at the same time, X.1313 — a year and a half later.

6.3.3 Threats in sensor networks

General threats in computer/telecommunication networks are described in Rec. ITU-T X.800 [75]. Rec. ITU-T X.1311 in addition to them lists sensor node-specific threats:

- **Vulnerability of sensor nodes:** Sensor networks are expected to consist of hundreds or thousands of sensor nodes. Each node represents a potential point of attack, rendering the monitoring and protection of each individual sensor from either a physical or a logical attack impractical. The networks may be dispersed over a large area, further exposing them to attackers capturing and reprogramming individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the attacker can then mount a variety of attacks such as falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service.
- **Eavesdropping:** In wireless sensor network communications, an adversary can gain access to private information by monitoring transmissions between nodes. For example, a few wireless receivers placed outside a house may be able to monitor the light and temperature readings of sensor networks inside the house, thus revealing detailed information on the occupants' personal daily activities.
- **Secrecy of sensed data:** Sensor networks are tools for collecting information; an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary gaining access to both indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and consequently extract details of the inhabitants' private activities. However, the fact that sensor networks enable the collection of information that would otherwise be impossible to collect is not the main privacy problem. In fact, a lot of information from sensor networks could probably be collected through direct site surveillance. Sensor networks exacerbate the privacy problem because they make large volumes of information easily available through remote access. Thus, attackers need not be physically present to maintain surveillance. They can gather information in a low-risk, anonymous manner. Remote access also allows a single adversary to monitor multiple sites simultaneously.
- **DoS attacks:** As safety-critical applications use more sensor networks, the potential damage of operational disruptions becomes significant. Defending against denial-of-service attacks – which aim to destroy network functionality rather than subverting it or using the sensed information – is extremely difficult. DoS attacks can occur at the physical layer, e. g., via radio

jamming. They can also involve malicious transmissions into the network to interfere with sensor network protocols or physically destroy central network nodes. Attackers can induce battery discharge in sensor nodes – for example, by sending a sustained series of useless communications that make the targeted nodes expend energy in processing them and forwarding them to other nodes as well. More insidious attacks can occur from inside the sensor network if attackers can compromise the sensor nodes. For instance, they could create routing loops that will eventually exhaust all nodes in the loop.

- **Malicious use of commodity networks:** The proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For example, thieves can hack home automation sensors or even simply eavesdrop on their activity to gain private information on the presence, location, etc., of the owners and act accordingly. If the sensors are small enough, they can also be planted on computers and cell phones to extract private information and passwords. Such widespread use will lower the cost and availability barriers that are supposed to discourage such attacks.
- **Routing-specific threats:** Rec. X.1311 specifies seven types of attacks that are specific to sensor network routing protocols: spoofed, altered, or replayed routing information; selective forwarding; sinkhole attacks; sybil attacks; wormholes; HELLO flood attacks; acknowledgement spoofing. These attacks are described in the paper [76] which is free available online.

6.3.4 Security dimensions for USNs

A security dimension is a set of security measures designed to address a particular aspect of network security to protect against all major security threats; it is not limited to the network but extends to applications and end user information as well. Rec. X.1311 adopts security dimensions, described in Recommendation X.805 [77]:

- **Data confidentiality:** The standard approach for keeping sensitive data confidential is to encrypt the data with a secret key that only the intended receivers possess, thus ensuring confidentiality.
- **Data authentication/identification:** Data authentication allows a receiver to verify that the data was really sent by the sender claiming to be such. Identification aims at proving the identity of the entity or sensor node. Along with the two-party communication authentication, it is very important to provide authenticated broadcast in sensor networks, since routing tree construction, network query, software updates, time synchronization, and network management all rely on broadcast.
- **Data integrity:** Data integrity assures the receiver that the received data is not altered in transit by an adversary.
- **Access control:** Access control ensures that only the authorized user or entity is allowed to gain access to information, resource, or services.
- **Non-repudiation:** Non-repudiation ensures that the entity or user cannot deny the activities in the network he/she has done.
- **Communication security:** Communication security ensures that the information only flows from the source to the destination.
- **Availability:** Availability ensures that information, service, and application are available to legitimate users anytime.
- **Privacy:** Privacy ensures that the identifier of the user or entities and network usage is kept confidential.

Rec. X3211 identifies additional security dimension — **resilience to attacks**, which is applicable

only for sensor networks. Resilience to attacks refers to the measures for recovering from the various attacks against the USN. It ensures that the USN is able to recover from attacks so that it is capable of detecting/remaining resilient to various attacks through the appropriate design of PHY/MAC/Routing protocols.

6.3.5 Security techniques for USNs

Key management. Key management refers to the generation, distribution, sharing, rekeying, and revocation of cryptographic keys. The security of key management forms the foundation of the security of other security services. In general, there are three types of key management: trusted server scheme, self-enforcing scheme, and key pre-distribution scheme. But the trusted server scheme (e. g. Kerberos) is not adequate for the sensor network since there is no trusted infrastructure in the sensor network; the self-enforcing scheme which uses the public key algorithm (e. g. Diffie-Hellman or RSA key transport algorithms) cannot be employed in the sensor network due to the limited memory and computational complexity of the sensor node. The key pre-distribution scheme pre-distributes the key information among all sensor nodes prior to deployment. This scheme is the most suitable for the wireless sensor network since it has low communication overhead, is resilient to node compromise, and does not rely on the trust of the base station. Rec. X.3211 identifies the following requirements to key management:

- Ability to support large sensor networks and flexibility to handle a substantial increase in sensor nodes even after the deployment of the sensor node.
- Efficiency of memory size to store the key in the sensor node, efficiency of computation complexity required to establish the key, efficiency of communication overhead, i. e., number of messages exchanged during the key generation process.
- High probability for pair-wise key establishment if random key management algorithms are utilized.
- Capability to resist compromised nodes and not to reveal even the minimum information on the security of other links in the sensor network.

Authenticated broadcast. Due to the nature of wireless communication in sensor networks attackers can easily inject malicious data or alter the content of legitimate messages during multi-hop forwarding. Sensor network applications need authentication mechanisms to ensure that data from a valid source will not be altered during transmission. Two kinds of techniques can be used according to the type of cryptographic algorithm. In the case of public key cryptography, a digital signature can be used. If symmetric cryptography is used, there is a need to append to the data the verifiable authentication data (i. e., message authentication code) based on the multiple shared secret between the base station (sink node) and sensor node. Due to the properties of the sensor network, the broadcast authentication method is preferred in broadcast message authentication based on symmetric cryptography. There is a typical scheme for enabling broadcast authentication in sensor networks, called TESLA (timed efficient stream loss-tolerant authentication) (see [78]). TESLA supports delayed per-packet data authentication and integrity checking. The key idea is the delayed disclosure of symmetric keys. The delayed key disclosure results in authentication delay. TESLA has the following properties: low computation overhead for the generation and verification of authentication information, low communication overhead, limited buffering required for the sender and the receiver, high robustness to packet loss, scales to a large number of receivers, and protection of receivers from denial of service. Annex B of Rec. X.3211 describes μTPC — improved version of TESLA.

Secure data aggregation. Secure data aggregation refers to an in-network process performed on the aggregator node to transfer securely the aggregation value to the sink node (i. e., a base station) by combining the sensed values sent by a number of sensor nodes. In this scheme, each sensor node sends an encrypted sensed value to the aggregator, which then calculates the encrypted aggregator results using aggregation functions such as summing function, average function, median function,

and maximum value or minimum value; the sink node obtains the aggregation value by decrypting the encrypted aggregator results.

Data freshness. Since all sensor networks stream some forms of time-varying measurements, guaranteeing confidentiality and authentication is not enough; one must also ensure that each message is fresh. Data freshness implies that the data is recent and ensures that no adversary replayed old messages.

Tamper-resistant module. The best well-known technique to protect against sensor node compromise is to use the tamper-resistant module in the sensor node. If each sensor node is equipped with a tamper-resistant module, protecting the storage of sensitive data, e. g., key data, may be possible; otherwise, damage can be trigged in case of capture of sensor nodes. Another possible technique in protecting against a compromised sensor node is to limit the amount of information obtained by the attacker after reading data from the captured sensor nodes. The cryptographic module (FIPS PUB 140-2) is an example of a tamper-resistant module that ensures sensitive data without storage damage.

USN middleware security. Rec. X.1312 describes the following security techniques:

- **Access control:** The USN middleware blocks the access of unauthenticated and unverified USN applications as well as sensor networks elements (e. g. sensor nodes and base stations). Details of authentication mechanisms for the sensor node are also described in Annex C of Rec. X.1311.
- **Stored data protection:** The USN middleware utilizes identity management and database security to keep sensing data, ID and authentication information of sensor networks and the USN applications securely.
- **Transmission/receipt data security:** The USN middleware uses encryption/decryption and integrity check when exchanging sensitive data (e. g. passwords) with USN applications and sensor networks elements.
- **Secure channel:** The USN middleware establishes a secure channel to protect the data exchange between applications and middleware and between the sensor network and middleware.

Routing-specific techniques. At the early stages of development routing protocols in WSNs were optimized for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security [76]. However, for today a few rather effective algorithms have already been developed. Appendix I of Rec. 1313 gives an overview of wireless sensor routing protocols.

Privacy protection in sensor networks. Along with data encryption and access control a typical approach for ensuring privacy preservation in a sensor network is to limit the network capability to collect the sensed data in such level of detail that the privacy of the individuals concerned could be compromised. For example, the sensor network might report the aggregate temperature over a large area instead of a small area. Annex D of Rec. 1311 describes an algorithm of secure data aggregation in sensor networks.

6.4 Sensor control networks

6.4.1 Shortcomings of the existing service providing models in WSN

In the very beginning of WSNs' development they were considered just as the method for measuring physical parameters in large spaces. In such a model (see Figure 6.2) readings collected by sensor nodes are transferred to a certain *center*, where these readings are processed and decisions are made. For example, in the enemy's submarines detection system the center on the base of data given by the sensors disposed in the ocean identifies and classifies moving underwater objects, and,

in the case of discovering suspicious activity, can give orders to send ships for a reconnaissance.

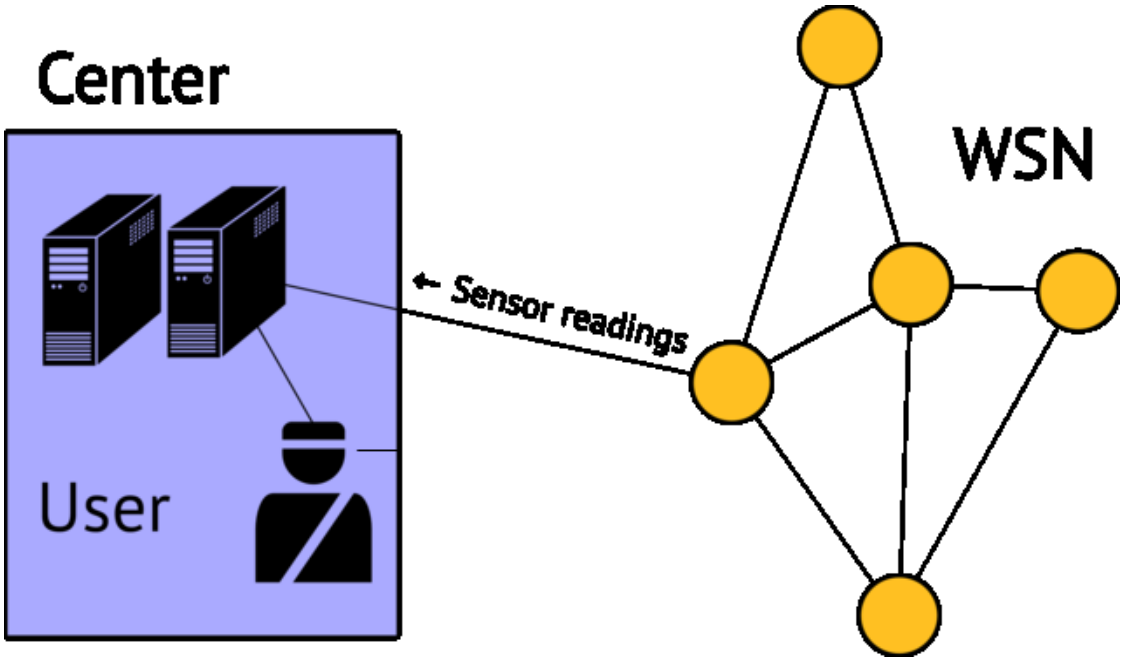

Figure 6.2: Original WSN service providing model

It is decisions making what WSN deployment is meant for. The borderline between what we have to consider as decision and consequence of decision is very relative. If we regard the center just as software and hardware which deals with sensor data processing, then possible decisions are "there is a submarine" or "there are no submarines" in one or other observed area. But if we include to the center definition headquarters with the officers responsible for dynamic response in the case of enemy invasion, then decision can be regarded as orders given by the headquarters.

When WSN started to be used for mass services providing, the model has undergone some changes (see Figure 6.3). A new essence appeared in it – a group of *users*: people, machines or mechanisms, each of them is a user of decision made in center. With it all, decision can be common for all users or individual for each of them. The example of the first case is notification of a city population about earthquake coming; the example of the second case is a medical system which notifies the medical staff and relatives about possible attack if the patient's blood pressure or pulse rate is reaching the critical point.

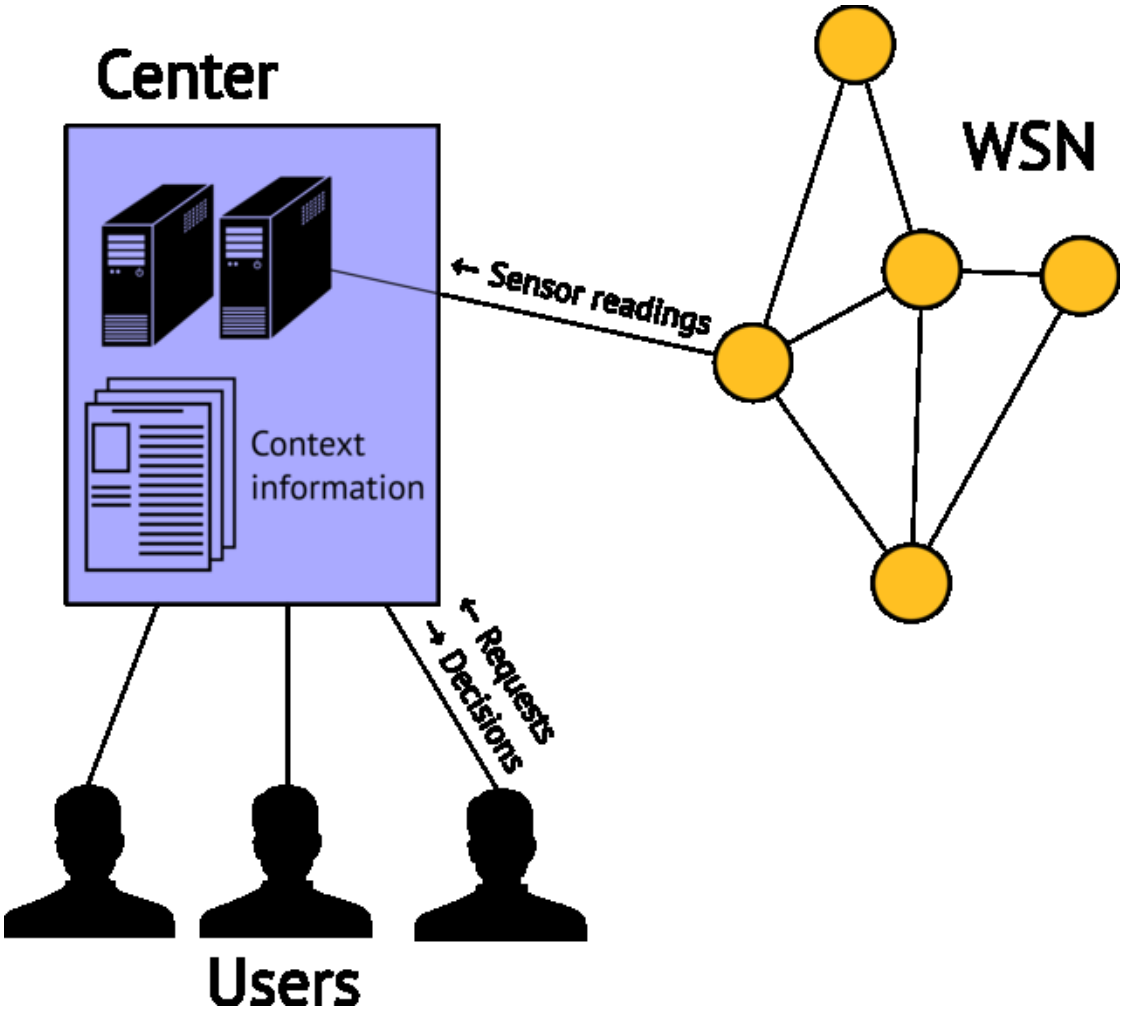

Figure 6.3: Multi-user WSN providing model

If decision is individual for every user, the center makes decisions not only basing itself on the data given by sensors, but also according to the *context information*, such as patient's case-history, which defines some rules for making decisions for a concrete user.

However, in some applications this model has a range of shortcomings:

- **Low scalability.** Increasing number of WSN leads to increment of load on the center. When sensor nodes are being added, it requires calculating resources for processing large amount of readings. But increasing number of users has even bigger influence here. While this number is small, the center can easily make decisions for everyone. Since every user has individual peculiarities and needs, to take them into account the center has not only to enlarge amount of context information according to the size of user base, but also to expand its structure, and, consequently, its volume attached to every user. For example, when WSN with healthcare application is used for controlling condition of patients ordered to bed rest, the application can raise an alarm every time when any patient's pulse rate exceeds some threshold. If the application is meant to be used by both ill and healthy persons, it is necessary to analyze if palpitation is connected with illness or normal physical activity and if current condition is permissible for the concrete person. In this case the center needs a database with medical indicators of all the users and have to use a complicated system of decisions making. Together with extremely heavy reliability demands imposed on e-health applications, it may lead to inadmissible charges necessary to equip the center.
- **Insufficient reliability.** The model represented in Figure 6.2, is a centralized one, in the sense that all decisions are made by the center. It means that if the center is disabled, the network

will become totally unserviceable. Besides, the center is not the only single point of failure. Even if the center is in good working condition, there is a need of some *central communication channel* to transmit decisions to the user.

The failure of the center or the central line of communication can be caused by both the internal overloading (unplanned growth of data stream from sensors or requests of service from the users) and the external reasons (electric power cut off, physical destruction of equipment, actions of attackers). In addition, the causes of both types arise in the time when WSN services are needed most of all. For example, the population notification about natural disasters system can function normally while being tested or used for monitoring. But when the real disaster comes, the rescue services and ordinary citizens begin to strenuously use all available communication channels, what leads to their failure; the building in which the center is located can be damaged. There is another example: an attacker along with invading a guarded object is executing an assault on the WSN center which provides monitoring service.

Of course, the problem of low reliability can be solved by means of dividing the center functions between a few geographically dispersed objects. But here we again face the WSN cost question: in addition to the charges on constructing supplementary centers, it is necessary to increase complexity of sensor nodes to provide their work with a few centers. For the reason that the number of nodes in WSN can be very large, budgetary limits can make getting necessary level of reliability impossible.

- **Problems real-time applications.** In some applications time interval during which decisions stays valid is very short. It happens in the cases when the users need continuous controlling of theirs actions, for example, if there is a need in navigation in unknown and quickly changing environment: on the road, in the time of combat operations or emergency situations. Such applications are called real-time applications.

  In most cases, in such applications decisions making requires readings of sensors located in immediate proximity of the user. The delay between changing of some physical parameters which has to evoke response from the user, and bringing appropriate decision from the center to the user, is composed with the time of detecting this change by a sensor node t_1, transmission of this information through WSN t_2, data processing in the center t_3 and transmitting decision through the central communication channel to the user t_4. When number of sensor nodes is increasing, of these four constituents t_3 is increasing the most quickly, because amount of hops from a node to the center depends on the extent of the network. Besides, all temporary elements are arising along with the number of users. As a result, if the extent of network is large, decisions made by the center may be no longer valid when the user receives them.

These problems cause searching for other service providing models for the cases when there is a need for scalability and supporting real-time applications.

6.4.2 SCN features

First of all, such a model has to be decentralized. It means that importance of the center has to be as small as possible, and at least a certain number of decisions have to be made without it. This approach reflected in the sensor control networks (SCNs) concept.

The idea of this conception for the first time was declared in 2010 in ITU-T by the Communication Administration of Russian Federation. The contribution presented for discussion at Study Group 13 was based on researches of Radio Research & Development Institute (Moscow) which were produced while elaborating Customized Emergency Management System (CEMS). Finally, the work of Study Group 13 ended in the production of Recommendation Y.2222 “Sensor control networks and related applications in next generation network environment” [55].

CEMS was designed in such a way which could provide navigation for people in buildings in the case of fire or other emergency situations even when the electrical power is cut off, some network nodes are disabled and central communication channels such as wired Internet and GSM/3G/4G are unapproachable. So, all three previously described shortcomings didn't allow to use the "ordinary" centralized model of service providing. Instead of it the model shown on Figure 6.4 was used. In contrast to previous figures, this one doesn't illustrate which kind of information is transmitted from one object to another. It is connected with the fact that every object can play different roles, as it will be described later.

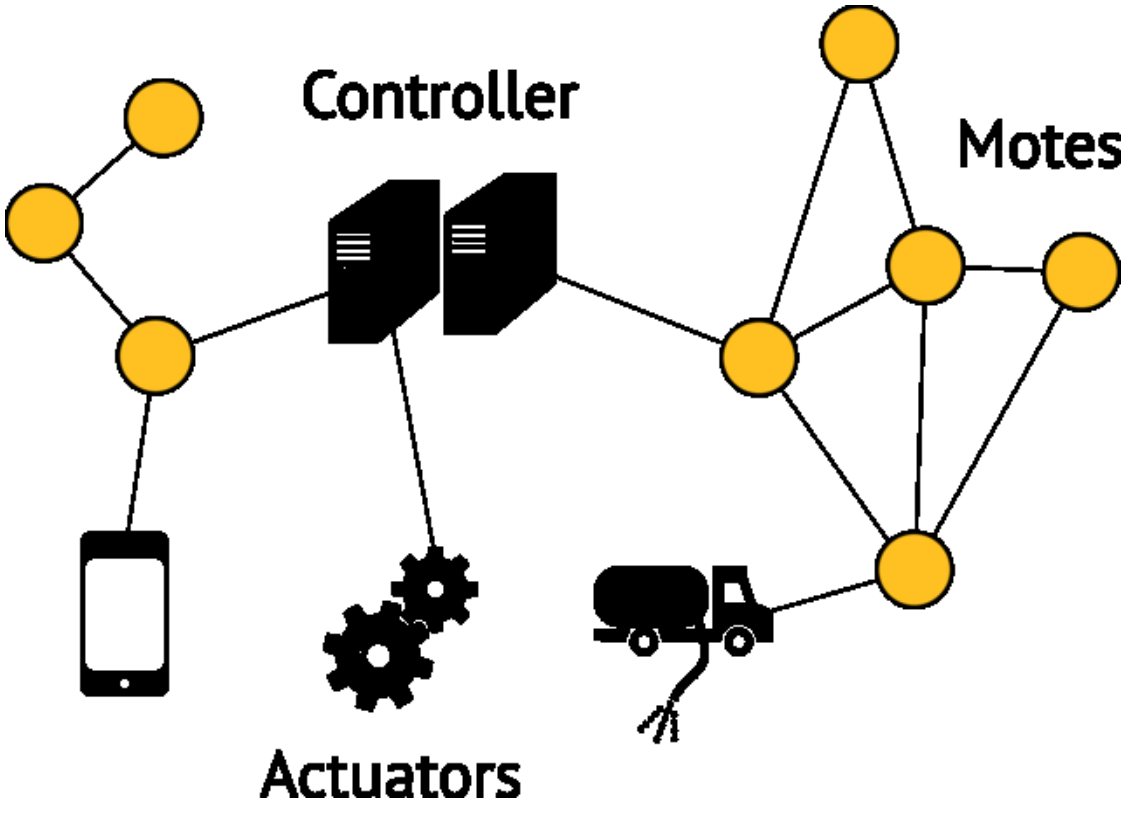

Figure 6.4: SCN service providing model

Besides, a new entity appears in the model, namely, an *actuator*, a certain electronic or electromechanical device which can interact with other SCN entities and be controlled by them. An actuator is a device which actually solves the tasks SCN was deploys for, for example, activates mechanisms or shows messages for the user on the display. There are three types of actuators: information actuators, which are intended to provide visual, audio, sensory interaction with the human user; gateway actuators, which are intended to forward management commands given by SCN to other networks; machine actuators, which are electromechanical devices intended for physical interaction with the external environment. In other WSN service providing models such devices play passive role: they just carry out the orders given by the center. In SCN actuator receives not decisions but data which allows to make decisions; it has software and hardware which make it possible to select the best action scenario, taking into account, from the one hand, these data, from the other hand, peculiarities and needs of the user.

The same statement is valid for the sensor nodes. In SCN, in addition to sensing element and radiomodule intended for connection with other nodes, they have a microcontroller or microprocessor which allow to provide data processing. Such "smart" sensor nodes are called *motes*. Due to enlarged possibilities the mote in some situations is able to make decisions without a center, cooperating with other motes if it's necessary. To underline the less important part of the center, in

SCN center is called *controller*.

6.4.3 SCN decision-making process

In most typical use cases in SCN it's impossible to say that decision is made by a single entity: a mote, an actuator or the center. Usually decision is made by different essences in a few stages. To present the decision-making process clearly, the charts like those shown on Figure 6.5 are used.

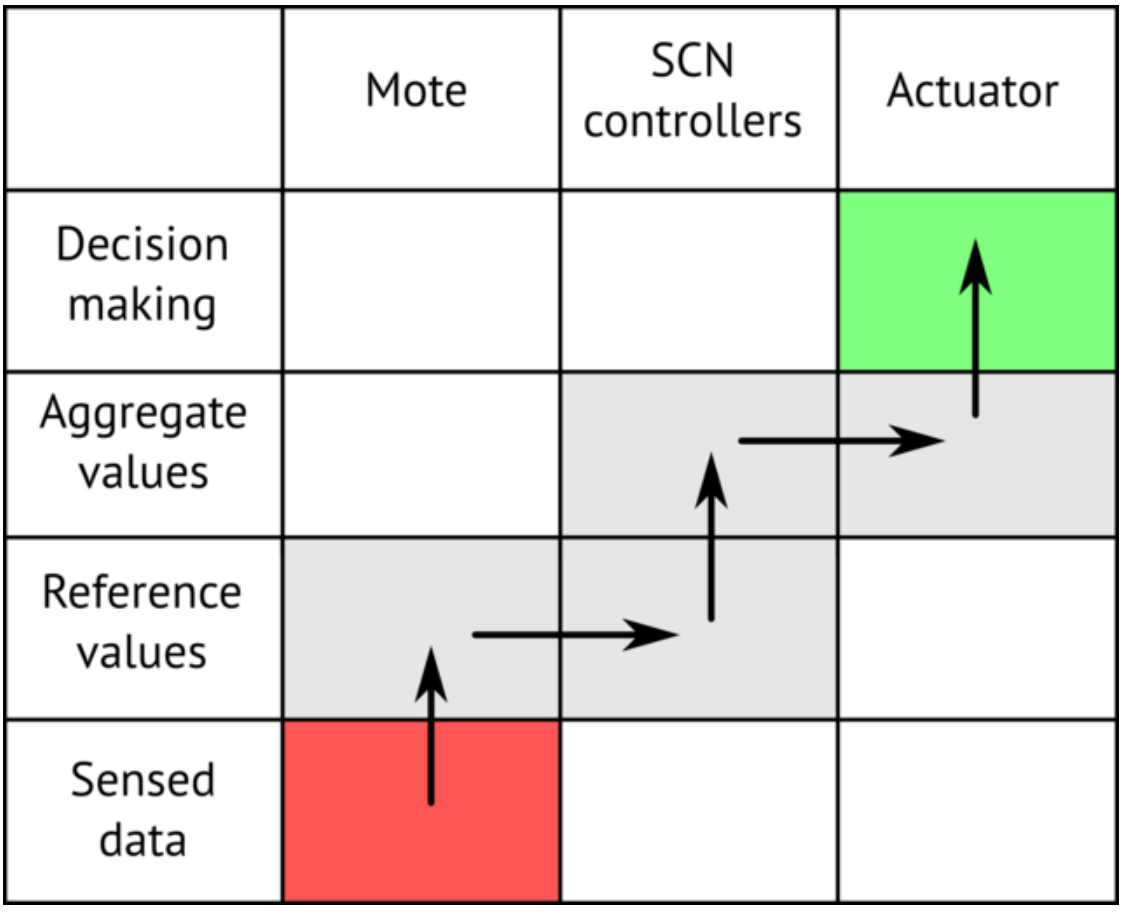

Figure 6.5: Example of a flow chart

Columns of such chart represent entities of SCN and rows represent data types. The set of data types can differ in various applications, but usually it is possible to define the following four types:

1. Fetching of sensed data (shown as Sensed data in figures);
2. Calculation of reference values by combining (e. g. averaging) the sensed data of one or several closely situated motes (shown as Reference values in figures). The aim of calculation of reference values can be, for example:
   - comparison of sensed data readings with thresholds for the purpose of filtering sensed data and taking them into account during calculations of aggregate values and/or decision making,
   - auxiliary pre-calculations for the purpose of quicker calculation of aggregate values and/or decision making,
   - synchronous analysis of multiple sensed data readings.
3. Calculation of aggregate values by combining (e. g. averaging) the sensed data of several spatially distributed motes, reference values and other data (shown as Aggregate values in

figures). Also aggregate values may be received from external networks or from the operator;

4. Decision making (shown as Decision making in figures). During this process a specific control command for the actuator is formed. It can use fetched aggregate values.

The rows of such chart represent the above listed operations and the columns represent elements participating in the decision making process. Data transmission flows are depicted as horizontal arrows whose endings correspond to the sending and receiving elements of the actual transmission stage, while data computational flows are depicted as vertical arrows corresponding to the above described operations. Any operation sequence which allows to form decisions from raw sensor data on an actuator, is called *decision flow*.

The choice of the concrete decision flow can be based on different reasons. For example, if decision depends only on the situation and the environment condition in the immediate proximity of the user, it can be made by the actuator in cooperation with the nearest sensors without SCN controller. But if in some place within the SCN service range some event arises and is so important that all the users have to respond to it, decision can be made by the SCN controller. Moreover, the choice of decision flow depends on the actuator possibilities, it will be different for the actuators which can communicate with the sensor nodes directly through the sensor network protocol, and for the actuators which work just with the centralized communication channel. Different types of decision flow organization will be regarded later. Before it's necessary to consider how SCNs are being integrated in NGN infrastructure.

6.4.4 High-level SCN infrastructure

Figure 6.6 gives an overview of SCN and its applications including their relationship with NGN.

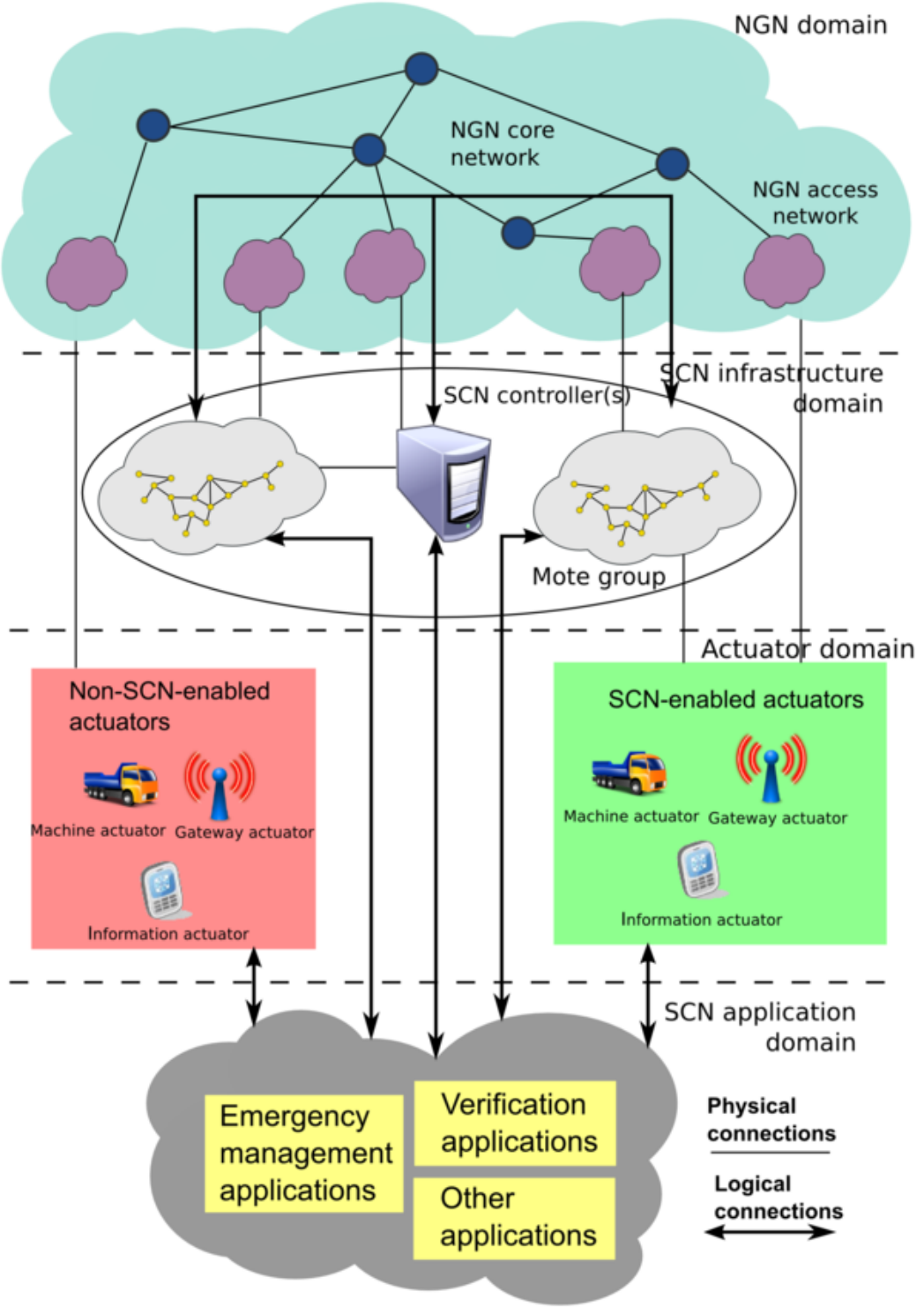

Figure 6.6: Overview of SCNs and its applications

Figure 6.6 picks out four domains:

1. NGN domain: the connectivity via NGN fulfills two objectives. Firstly, NGN provides access to SCN applications for both non-SCN-enabled and SCN-enabled actuators when direct communication of actuators with motes is not possible or desirable (e. g. when an actuator is a mobile phone and its owner doesn't want his/her location to be exposed due to privacy reasons). Secondly, NGN is used to unite spatially distributed mote groups and the SCN controllers into a single network.

2. SCN infrastructure domain: the SCN infrastructure includes one or several SCN controllers and *mote groups*. They may be spatially distributed: in that case, NGN is used to unite them into a single network. Authorized personnel may use the SCN controllers for SCN monitoring and administration. Motes can allow direct access to SCN applications of SCN-enabled actuators, while direct access via motes to SCN applications of non-SCN enabled actuators is not possible.
3. Actuator domain: the actuators can be of three different types: machine actuators (e. g. car, water sprinkler, door lock), information actuators (e. g. screen, loudspeaker, mobile phone, PDA, notebook) and gateway actuators (e. g. computer with telephone private branch exchange software).
4. SCN application domain: it consists of SCN applications, e. g. emergency management applications (see Section 5.2). Different parts of SCN applications can reside in different SCN objects according to the specific application requirements.

So, the typical SCN is a group of motes located in different places and at least one controller. Technically, e. g. from the point of view of the traffic transmitting, separated mote groups and the controller are connected via NGN; organizationally, e. g. from the point of view of management, they are connected by *SCN provider*, which is a juridical person responsible for service providing and managing, billing, customer relationship management and other administrative tasks. The actuators, SCN-enabled as well as non-SCN-enabled, are the part of the network, but not a constant part, because they can be disconnected from one network and connected to the other one. As for SCN applications, they are distributed, theirs separated parts are located in controllers, motes and actuators.

6.4.5 Configurations for SCN applications

The following paragraphs deals with considering the ways of decisions-making process organization in SCN applications depending on the actuators capabilities. There are a lot of configuration types in addition to those mentioned here; moreover, in practice it is often more preferable to combine a few configurations at once in a single application, in order to provide better flexibility. Nevertheless, the configurations offered here are rather multipurpose and can serve as a base for more complicated variants.

Decentralized configuration for SCN applications

The decentralized configuration is the most universal configuration for SCN applications in terms of flexibility, expansibility and reliability. It is called so because it makes minimal demand to the central communication channel and the SCN controllers. This provides the possibility of ubiquitous usage of such configuration in a wide range of applications, including emergency management applications (due to the high risk of failure related to centralized entities in case of disaster or emergency).

Roles in the decentralized configuration are distributed as follows:

- SCN controllers:
  - It receives from the actuators via the central communication channel requests about aggregate values, which are necessary for making decision but cannot be calculated by the actuators themselves.
  - It requests transmission of sensed data and reference values from the appropriate motes via the SCN infrastructure and regularly calculates the necessary aggregate values.
  - It transmits to each actuator via the central communication channel the aggregate values requested by that actuator.

- It interoperates with external systems (e. g., a different application server) and the authorized personnel administrating the SCN.

- Actuator:
  - It requests the necessary sensed data and reference values from the motes via the SCN infrastructure.
  - It requests from the SCN controllers via the central communication channel the aggregate values which are necessary for making decision but cannot be calculated by the actuator itself.
  - It receives from the motes via the SCN infrastructure the requested sensed data and reference values and calculates the other necessary reference values and aggregate values.
  - It receives from the SCN controllers via the central communication channel the requested aggregate values.
  - It forms the appropriate control commands.
  - It transmits to the SCN controllers information about its own status via the central communication channel.

- Mote:
  - It receives requests from the SCN controllers and the actuators via the SCN infrastructure about sensed data or reference values.
  - It transmits the requested data to the SCN controllers and the actuators via the SCN infrastructure.

The decision making process should hold the following procedure:

1. The necessary sensed data, reference values and aggregate values are kept in the SCN controllers' memory and regularly updated.
2. Each actuator sends requests for sensed data and reference values to the motes, and then stores the received ones in memory. The data requests can be of different types, such as broadcast request (all motes send data on demand to actuators via the SCN infrastructure), threshold-exceeding request (only motes whose sensed data exceed some thresholds send data), etc.
3. Some other reference values can be computed as needed by the actuators based on received sensed data and reference values.
4. Each actuator needs to have the up-to-date aggregate values necessary to make decision. These aggregate values can be computed by the actuator itself or fetched from the SCN controllers.
5. Each actuator forms a control command depending on the aggregate values.

Two examples of flow chart for decentralized configuration are shown in Figures 6.7 and 6.8.

In the first example, actuators use aggregate values received from the SCN controllers (data flow 2) and aggregate values calculated using reference values received from motes (data flow 1).

In the second example, actuators use only aggregate values calculated using reference values received from motes (data flow 1). There is no influence of the SCN controllers on the decision making process. The SCN controllers only calculate (data flow 2) and store in memory aggregate values for the purpose of interoperation with external systems and the authorized personnel administrating the SCN.

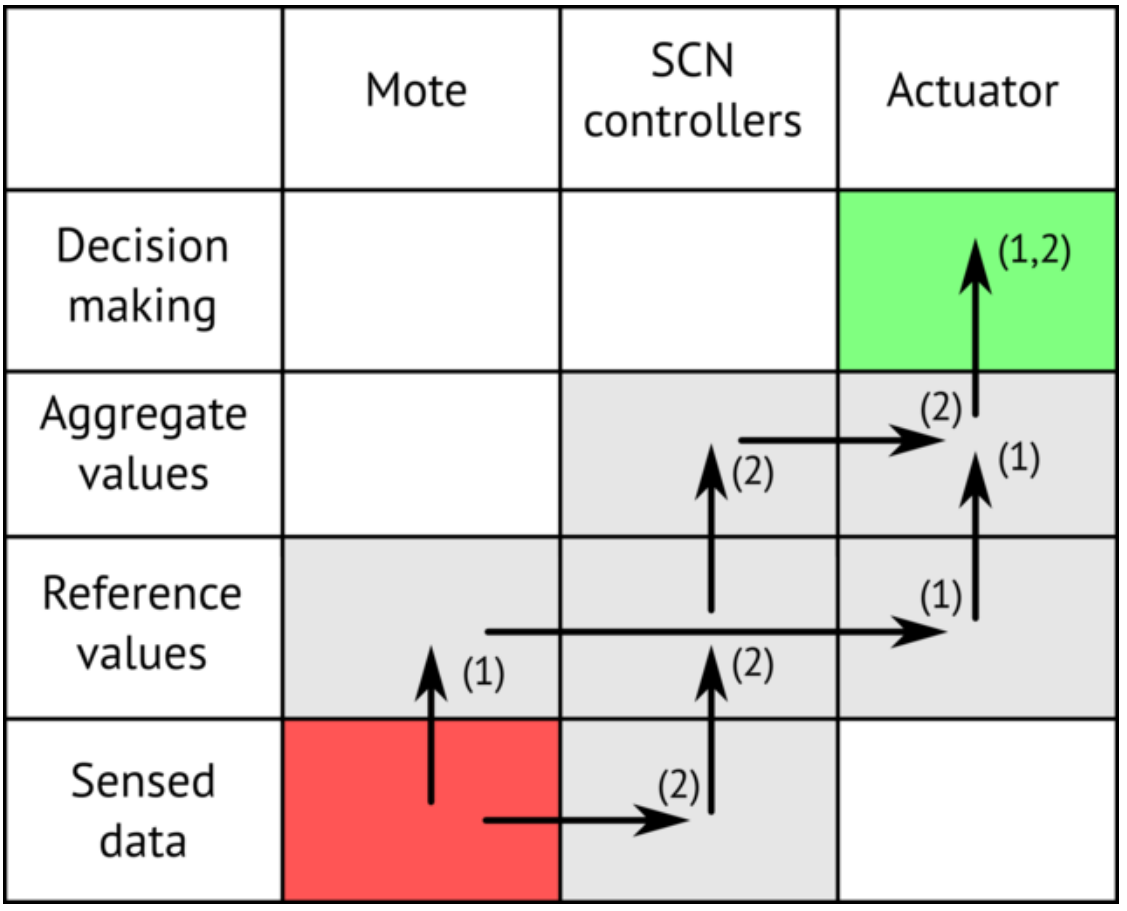

Figure 6.7: Example of a flow cart for decentralized configuration for SCN applications

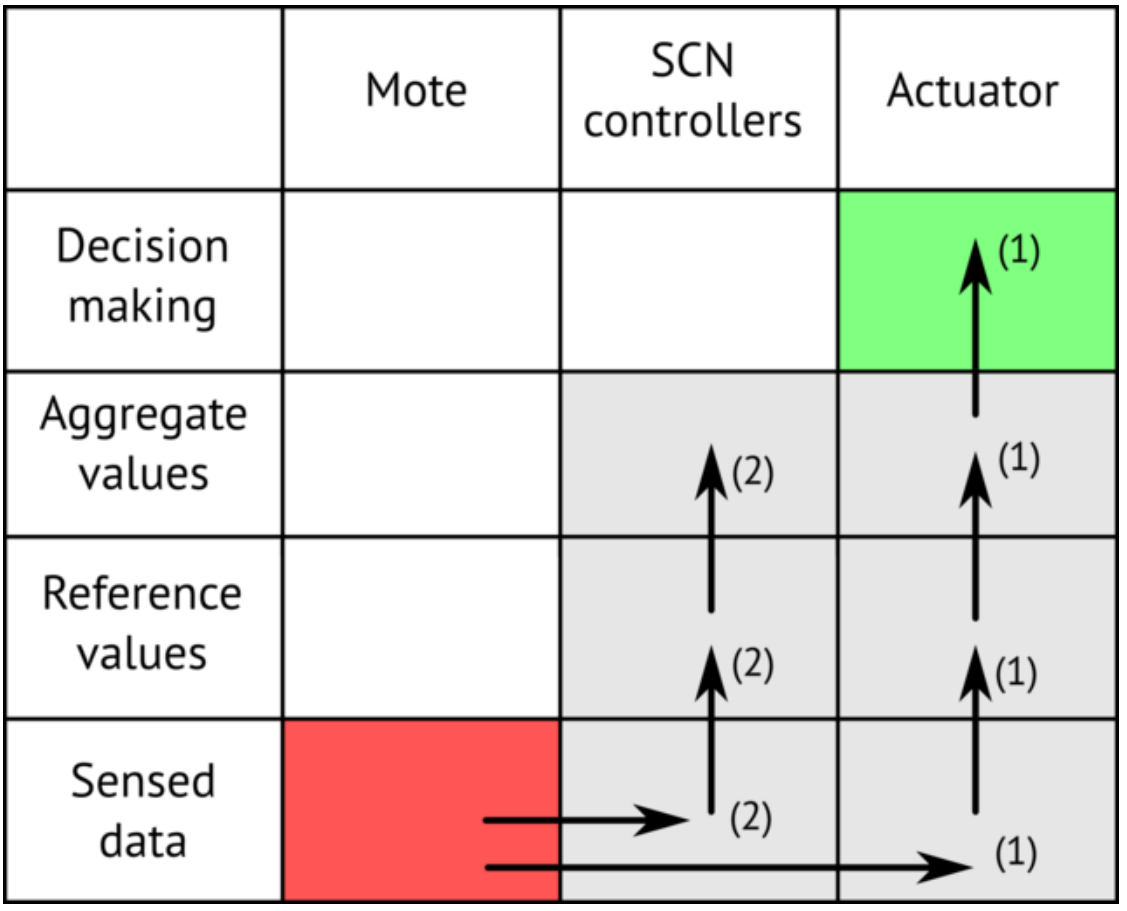

Figure 6.8: Example of a flow cart for decentralized configuration for SCN applications

As mentioned above, decentralized configuration is the most acceptable configuration for SCN applications. However, nowadays most of mass mobile user actuators such as mobile phones, PDAs, netbooks etc. have no technical possibility of direct data exchange with existing mote infrastructures because of difference in transceiver kinds and transmission standards. Thereby transitional configurations are needed to provide a possibility of working in SCNs for mass mobile user terminals.

Centralized configurations for SCN applications

This configuration is called so because the data for every decision made by SCN are transferred through the SCN controllers and are delivered to the actuators via a central communication channel. It should be employed when actuators can only communicate via the central communication channel and/or it is not desirable to change the existing infrastructure of motes and actuators to enable SCN applications.

Roles in centralized configuration are distributed as follows:

- SCN controller:
  - It receives from the actuators requests via the central communication channel about aggregate values.
  - It requests transmission of sensed data and reference values from the appropriate motes via the SCN infrastructure and regularly calculates the necessary aggregate values.
  - It transmits to each actuator via the central communication channel the aggregate values

requested by that actuator.

- It interoperates with external systems (e. g. a different application server) and the authorized personnel administrating the SCN.

- Actuator:
  - It requests from the SCN controllers via the central communication channel aggregate values, which are necessary for making decision.
  - It receives from the SCN controllers via the central communication channel the requested aggregate values.
  - It forms the appropriate control commands.
  - It transmits information about its own status to the SCN controllers via the central communication channel.
- Mote:
  - It receives requests from the SCN controllers via the SCN infrastructure about sensed data or reference values.
  - It transmits to the SCN controllers the requested data via the SCN infrastructure.

The decision making process should hold the following procedure:

1. The necessary sensed data, reference values and aggregate values are kept in the SCN controllers' memory and regularly updated.
2. Each actuator needs to have the up-to-date aggregate values necessary to make decision. These aggregate values are fetched from the SCN controllers.
3. Each actuator forms a control command depending on the aggregate values.

An example of flow chart for centralized configuration is shown in Figure 6.9. In this example actuators use only aggregate values received from SCN controller.

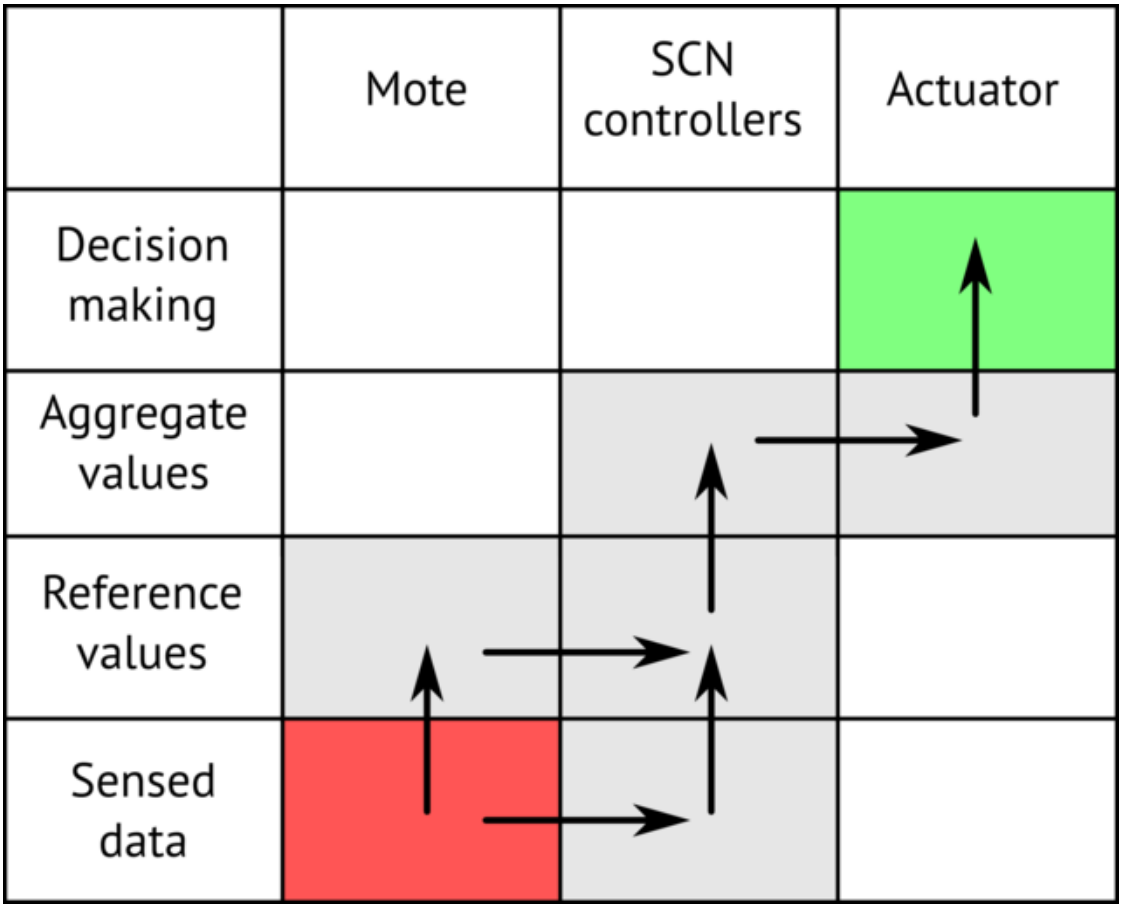

Figure 6.9: Example of a flow cart for centralized configuration for SCN applications

Ad hoc configuration for SCN applications

This configuration is called so because it utilizes ad hoc networks (e. g. based on Bluetooth or Wi-Fi technologies) to deliver data to actuators. It should be employed when there is the possibility to expand the existing SCN infrastructure and the actuators have some ad hoc wireless network capabilities. Some intermediate devices called gates are used to provide a communication channel between actuators and one or several nearby motes.

Roles in ad hoc configuration are distributed as follows:

- SCN controller:
  - It receives from the actuators via the central communication channel requests about aggregate values, which are necessary for making decision but cannot be calculated by the actuators themselves.
  - It requests transmission of sensed data and reference values from the appropriate motes and regularly calculates the necessary aggregate values.
  - It transmits to each actuator via the central communication channel the aggregate values requested by that actuator.
  - It interoperates with external systems (for example, a different application server) and the

authorized personnel administrating the SCN.

- Gate:
  - It receives requests from the actuators via the ad hoc network about sensed data and reference values and forwards them to the motes via the SCN infrastructure.
  - It transmits the requested data to the actuators via the ad hoc network.
- Actuator:
  - It requests the necessary sensed data and reference values from the gates via the ad hoc network.
  - It requests from the SCN controllers via the central communication channel aggregate values, which are necessary for decision but cannot be calculated by the actuator itself.
  - It receives from the gates via the ad hoc network the requested sensed data and reference values and calculates the other necessary reference values and aggregate values.
  - It receives from the SCN controllers via the central communication channel the requested aggregate values.
  - It forms the appropriate control commands.
  - It transmits to the SCN controllers information about its own status via the central communication channel.
- Mote:
  - It receives requests from the SCN controllers and the gates via the SCN infrastructure about sensed data or reference values.
  - It transmits the requested data to the SCN controllers and the gates via the SCN infrastructure.

The decision making process should hold following procedure:

1. The necessary sensed data, reference values and aggregated values are kept in the SCN controllers' memory and regularly updated.
2. Each gate forwards sensed data and reference values from the motes to the actuators.
3. Each actuator sends requests for sensed data and reference values to the gates, and then stores the received ones in memory. The data requests can be of different types, such as broadcast request (the gates send data of all motes on demand to the actuator), threshold-exceeding request (gates send data only of the motes whose sensed data exceed some thresholds), etc.
4. Some other reference values can be regularly computed as needed by the actuators based on received sensed data and reference values.
5. Each actuator needs to have the up-to-date aggregate values necessary to make decision. These aggregate values can be computed by the actuator itself or fetched from the SCN controllers.
6. Each actuator forms a control command depending on the aggregate values.

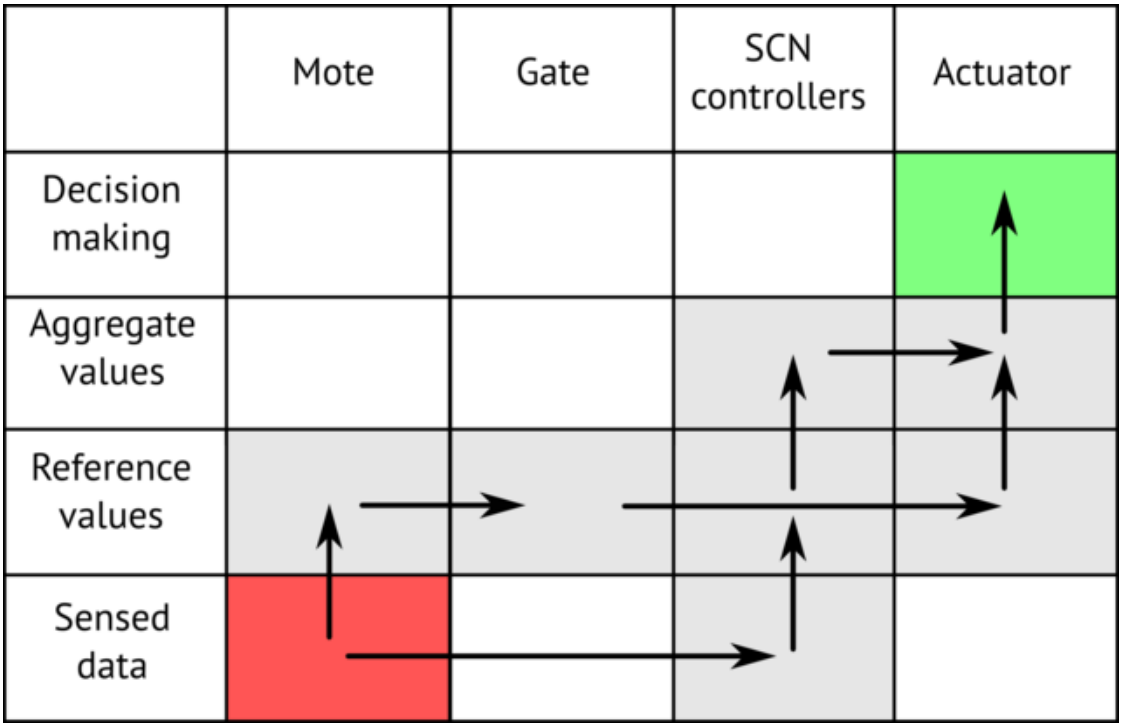

Figure 6.10: Example of a flow cart for ad hoc configuration for SCN applications

6.4.6 Conclusion

SCNs are one of the most promising line of development WSN. They allow to deploy reliable, robust and scalable applications for various tasks including real-time ones. SCNs also have a high return of investments, because a huge and growing market of mass mobile devices forms a base for SCN user equipment. All these factors make it possible to solve large-scale critical problems such as enhancing of personal security in man-made environment during disasters. Countries that, on the one hand, are most at risk from natural disasters (e. g., drought, floods, storms, coastal flooding, etc.) and, on the other hand, have a developed ICT infrastructure may be the main users of SCN technology in the short and mid-term.

6.5 Machine-Oriented Communications (MOC)

Machine-Oriented Communications (MOC) is one of the most developing trends not only in the WSN field, but also in ICT in general. Often the other term is used: *machine-to-machine communications* or M2M. This term means not some concrete technology but a design principle of technical systems where interact two or more entities and at least one entity does not necessarily require human interaction or intervention in the communication process.

In this definition “entity” means not only traditional terminals used in other networks, such as telephones, personal computers and servers, but also different electromechanical devices. In particular, it can be sensing devices (e. g. sensors, meters, surveillance cameras), actuators (e. g. dimmer, relay) and data capturing/carrying devices such as RFID terminal.

So, common WSNs composed of a lot of sensors which are collecting and automatically processing physical parameters measurements are the example of MOC. On the other hand, in MOC a great attention is paid to the questions which are beyond the scope of WSN, such as work with a great number of heterogeneous devices, integration with proprietary actuators, restricting access to

certain functions of devices for different users etc.

Cisco's Internet Business Solutions Group (IBSG) predicts some 25 billion devices will be connected by 2015, and 50 billion by 2020 [79]. According to the information given by ABI Research company, market of just MOC security applications by 2018 will reach $198 million.

In ITU-T *Internet of Things Global Standards Initiative* and Study Group 13 have dealt with MOC. In 2012 SG13 has worked out and approved Recommendation Y.2061 "Requirements for the support of machine-oriented communication applications in the next generation network environment" [34]. The following part of this section will concern the description of this Recommendation, because it deals with the network aspects of MOC systems: data delivery, mobility, quality of service, etc. — i. e. questions related to WSN as well. It is possible to say that Recommendation Y.2061 considers the problems which arise with using WSNs in practice for solving a particular task – providing cooperation between machine objects which does not necessarily require human interaction. Also, in this Recommendation important WSN use cases are considered, such as e-health, warning service, motorcade management, smart home.

In Recommendation Y.2061 the following questions are considered:

- Terms and determinations related to MOC;
- General information about MOC: network overview, types of machine-oriented communications, MOC ecosystem,
- characteristics of MOC;
- Service requirements of MOC applications;
- Requirements of NGN capabilities and MOC devices/gateways capabilities, which deals with these requirements;
- Reference framework for MOC capabilities;
- MOC use cases (in Appendix which does not form an integral part of the Recommendation).

To make it easier to understand, we are going to change the order of presentation and will start with the use cases, take a look at service requirements made in each case, and according to these requirements we'll determine the required set of capabilities of NGN and MOC devices.

6.5.1 Use Case 1: e-health monitoring

Overview

Various types of devices are involved in the provisioning of e-health services. Some of these devices only collect data and interact with the network (e. g., heartbeat sensors), others can interact bidirectionally (e. g., cameras), some devices usually generate small amounts of data (e. g., thermometers), while others may deal with multimedia streaming (e. g., cameras) or, deal with call session control (e. g., SIP terminals supporting video calls). Some devices may even work as both gateway and sensor-like service platforms.

The e-health devices gather data and send them to the relevant parties, such as the e-health center in Figure 6.11. Hospitals, doctors and families can subscribe to the service to get raw or processed data.

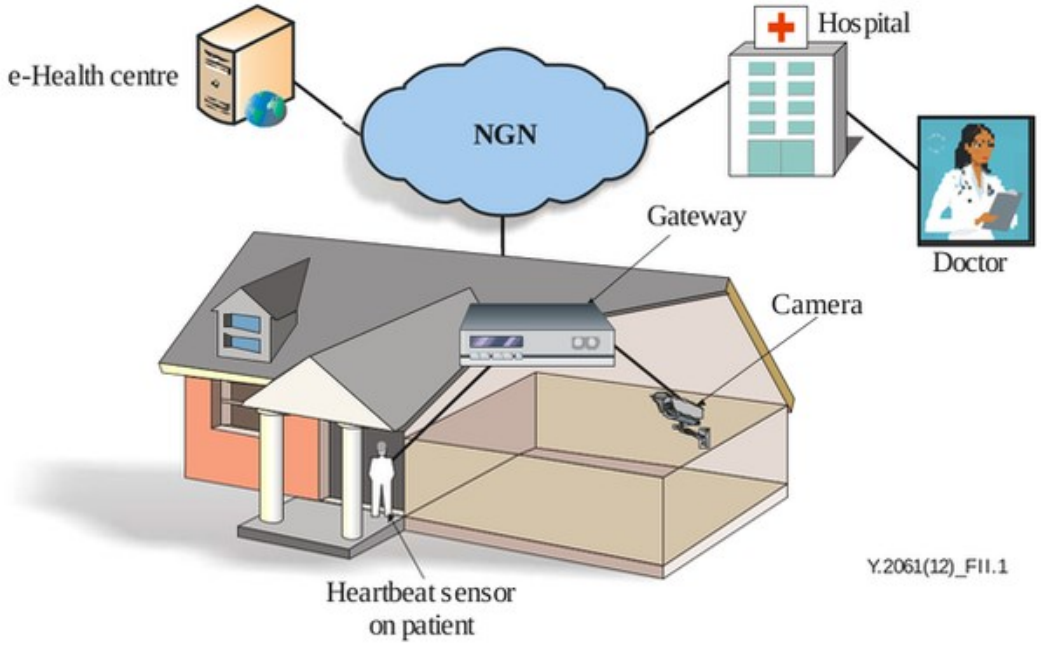

Figure 6.11: Typical e-health monitoring service configuration

Requirements

Use case technical challenges	**Service requirements**	**NGN requirements**	**MOC devices/gateways requirements**
Grouping should be supported. This is useful, for instance, for multiple patients with the same type of disease, or in the case of a single patient, to manage a set of devices which can be managed in group mode.	1) Support of data transmission to/from one or all members in an MOC group using group identifier. 2) Support online and offline accounting and charging based on groupings. 3) Support of the group based QoS policy. 4) Support of MOC group management, including display/creation/modification/deletion of MOC groups, group	1) Group based addressing mechanisms according to the NGN provider's policy. 2) Map of the MOC group identifier to network addresses of MOC devices. 3) Per group level QoS policy, in parallel with, or instead of, a per device level QoS policy. 4) Optimized handling of group communications in order to save	MOC gateways are required to support mapping between the identification of an MOC device group and one or more MOC local network addresses for each MOC device within the group.

	members and associated attributes.	network resources and to prevent network congestion. 5) Support of group-based accounting and charging.	
Optimized traffic control should be supported. For example, the detected data may be very small and need to be reported to the network every hour: in such a case, it is a waste of resources to be permanently connected to the network. Additionally, devices on a patient might stay in sleep mode and wake up when the doctor needs to diagnose the patient remotely.	1) Mechanisms for application traffic management, e. g., to limit the maximum number of application transactions per second. 2) MOC devices enter or stay in sleep mode in order to save power (especially for devices using a battery) and save network resources (especially for devices with wireless network access).	Allow MOC end users' access (e. g., attachment to the network or establishment of a data connection) during a defined granted network communication access time interval; otherwise reject it or allow it with different charging parameters.	1) MOC devices are required to go offline when no data transmission is required and then to go into sleep mode according to the necessary policies. 2) MOC gateways are required to allow the setting and modification of granted/forbidden network communication access time schedules and durations.
Different mobility levels should be supported. For instance, in the case of patients with poor mobility (moving infrequently and not very far), it is a waste of resources to activate full mobility management capabilities.	Support of mobility management for different mobility levels in order to reduce resource usage (e. g., the timer of periodic location update should be reduced for the MOC devices which have infrequent movement).	Support of different mobility level management according to the mobility requirements of MOC devices and gateways, such as reducing the frequency of the mobility management procedures for MOC devices and MOC gateways with low mobility.	MOC gateways and MOC devices are required to support enhanced mobility management capabilities in order to support different levels of mobility.
Remote device activation and management should be supported. For example, devices in sleep mode would be woken up only when	1) Support of monitoring the state of various aspects of MOC devices and gateways including abnormal behavior, the attachment	Support of managing and controlling MOC devices and gateways, including monitoring MOC devices and gateways'	1) MOC gateways are required to act as a management proxy for MOC devices of the connected MOC local network. 2) MOC gateways

the doctor needs to diagnose the patient remotely.	information, the connectivity. 2) Support of mechanisms to perform simple and scalable pre-provisioning of MOC devices and gateways, enable and disable features, report errors from devices, and query device status.	operations, monitoring changes, and related actions, related to the network attachment points of MOC devices and gateways, monitoring MOC devices and gateways' network connectivity.	and MOC devices are required to support configuration management. 3) MOC gateways are required to support fault and performance data collection and storage.
Device profiles should be supported. Patient may buy new devices and connect them to the network dynamically: device related information should be included in the device profile and be updated dynamically to enable the network authentication and control of the newly-added devices and also their removal.	Using and managing standard device profiles for MOC devices and gateways, including their registration and discovery. The MOC device profile is a set of information related to MOC devices and MOC gateways.	Support of standard device profiles with enhancements for MOC devices and gateway's specific information.	—
Devices behind a gateway should be able to be identified by the network. The gateway might provide only a bearer channel and act as a data aggregator for the devices connected to it or might provide service control for the devices connected to it. In the first case, the devices connected to the gateway should be controlled by the network, or by both the network and	1) Support of mechanisms for managing gateways acting as traffic aggregators (a gateway aggregates traffic and acts as a channel). 2) MOC devices may communicate with different MOC applications via a single MOC gateway or via multiple gateways. 3) MOC devices may support non-IP addresses when they connect to the network via MOC	—	1) MOC gateways are required to support mapping between the identification of an MOC device and one or more MOC local network addresses. 2) An MOC gateway can optionally use temporary identifiers for MOC devices connecting and disconnecting to the network dynamically. 3) MOC gateways are required to identify and authenticate MOC

gateway.	gateways. 4) Support of a mechanism for authentication and authorization of MOC devices which are in an MOC local network (connected via an MOC gateway).		applications, other MOC devices and MOC end users. 4) MOC gateways are recommended to support different accounting and charging methods for the connected MOC devices.
Proprietary devices should be supported. There are plenty of proprietary devices and gateways running in networks: adaptation to existing proprietary devices and gateways should be supported.	1) Interoperability with proprietary devices through appropriate means, e. g., MOC gateways. 2) Support of the effective hiding of proprietary devices' operations.	—	MOC gateways are recommended to support communication with proprietary devices (e. g., devices with proprietary interfaces for inter-working with network entities).
Service profile should be supported. Patients are usually not very familiar with the services offered by different hospitals, they can usually just logon to the e-health center's portal and access services, whereas the e-health center is usually familiar and can determine the target hospitals based on their professional knowledge.	Using standard service profiles for registration and discovery. The service profile of a specific MOC application is composed by a set of information specific to that MOC application. It may include, but it is not limited to, the MOC application identifier, MOC application provider identifier and application data types.	Support of standard service profiles with enhancements for MOC applications' specific information.	—

6.5.2 Use case 2: Tsunami warning service

Overview

The tsunami warning system is used to detect tsunamis and issue warnings to prevent loss of life and property.

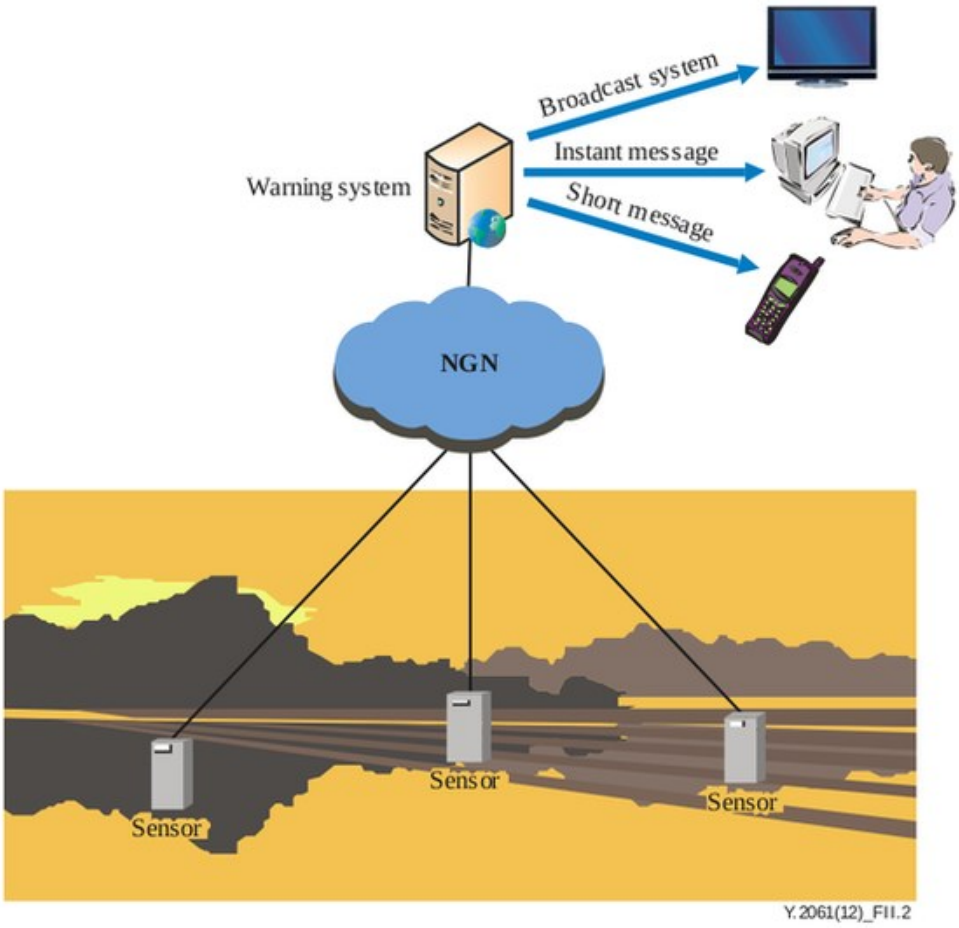

Figure 6.12: Typical tsunami warning service configuration

As shown in Figure 6.12, it consists of two equally important components: a network of sensors to detect tsunamis and a communications infrastructure to issue timely alarms to help evacuation of coastal areas. Detection and prediction of tsunamis is only half the work of the system. The other equal importance is the ability to warn the populations of the areas that will be affected. To save lives more certainly, proper guidance for escape according to their situation in danger (e. g., time, place, and occasion) should be considered. For a visitor who comes to an unfamiliar area at night, a simple alarm is not enough to escape to a safe place. All tsunami warning systems feature multiple lines of communications (such as SMS, e-mail, fax, radio, text and telex, often using hardened dedicated systems) enabling emergency messages to be sent to the emergency services and armed forces, as well to population alerting systems (e. g., sirens).

Requirements

Use case technical challenges	**Service requirements**	**NGN requirements**	**MOC devices/gateways requirements**
Grouping should be supported. This is useful, for instance, for multiple patients with the same type	1) Support of mechanisms in the network and MOC capabilities in the NGN domain for	—	—

of disease, or in the case of a single patient, to manage a set of devices which can be managed in group mode.	load balancing. 2) Robustness of network and MOC capabilities in the NGN domain, whilst also ensuring a sufficient level of QoS under given circumstances, e. g., emergency scenarios.		
Prioritized delivery of emergency information, i. e., emergency message for an earthquake, should be prioritized compared with other service messages.	1) Ability to set the prioritization of data (within a single application or among different applications). 2) Ability to manage different data according to their prioritization. 3) Ability to immediately transmit high priority data which are collected in network performance sensitive applications.	1) Ability to identify data according to relevant categories. 2) Ability to apply different data handling (e. g., caching and/or forwarding) based on data identification.	1) MOC gateways and MOC devices are recommended to support application prioritization. 2) MOC gateways and MOC devices are required to support QoS differentiation according to different categories of traffic.

6.5.3 Use case 3: Motorcade management

Overview

Figure 6.13 shows a typical service configuration for motorcade management.

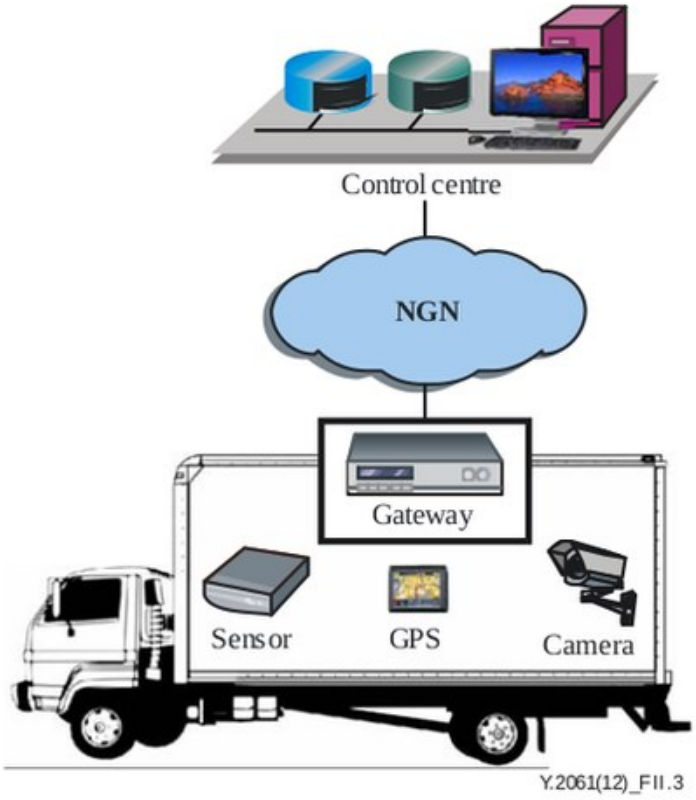

Figure 6.13: Typical motorcade management service configuration

Every bus is equipped with devices and gateways which have the same characteristics. The control center gathers data related to location, speed and the situation given from the sensors, global positioning system (GPS) terminal and cameras of the bus. Data aggregated through a gateway located on the bus are transmitted to the NGN using wireless access.

The dynamic timetable can be forwarded to the monitor screen on the bus stop by the control center according to the location information collected from the bus.

When a sensor on the bus detects an abnormal situation, such as the smell of gasoline, an alarm indication is sent to the control center.

The bus always has a fixed route which means it should not move out of the pre-defined roads. When a bus moves out of a particular area, an application should be triggered. For example, a call may be made to the bus driver, or an alert indication may be made to the bus administrator while the bus moves out of the area.

Requirements

Use case technical challenges	**Service requirements**	**NGN requirements**	**MOC devices/gateways requirements**
Location based service: an application should	1) Awareness of the location of MOC devices.	—	

be triggered when devices are in or out of a particular area;	2) Maintaining and managing different types of location information of both a single MOC device and a set of MOC devices behind an MOC gateway. Location management capability which determines and reports information regarding the location of users and devices within the NGN.		
Prioritized service level, for example, alarm indication should be prioritized compared with other data.	*See "Prioritized delivery of emergency information" in Use Case 2*	*See "Prioritized delivery of emergency information" in Use Case 2*	*See "Prioritized delivery of emergency information" in Use Case 2*
Group management for devices with the same characteristics.	*See "Grouping" in Use Case 1*	*See "Grouping" in Use Case 1*	*See "Grouping" in Use Case 1*

6.5.4 Use case 4: Smart home

Overview

Smart home usually involves a mix of different devices and applications, such as real-time or near real-time sensors, power outage notification and power quality monitoring.

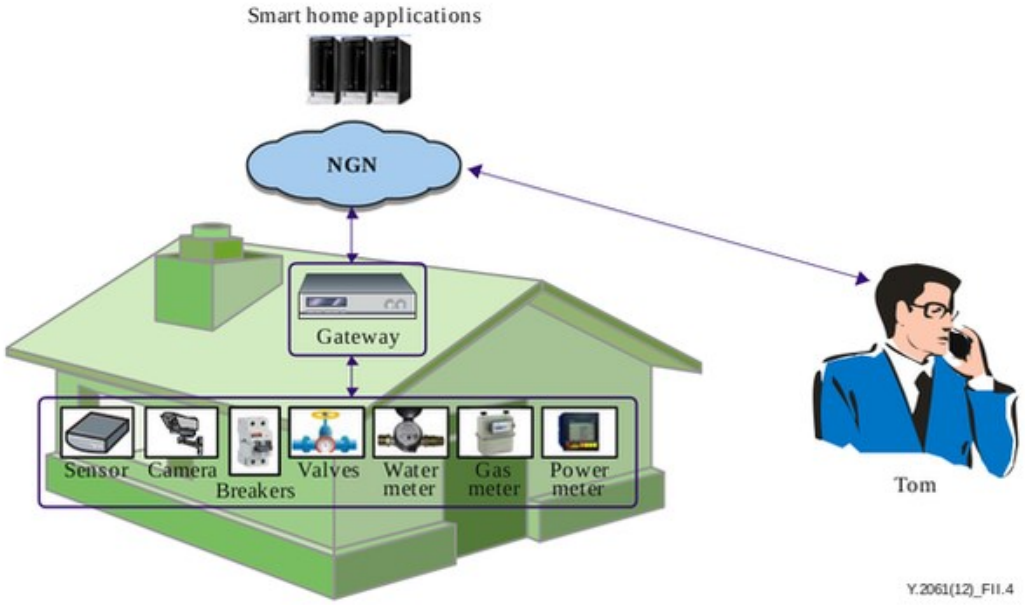

Figure 6.14: Typical smart home service configuration

As shown in Figure 6.14, a "smart home" scenario often refers to devices (e. g., smoke sensor, electricity meters, gas meters, etc.) which are connected to a smart home application platform via a gateway located in the smart home. The data center collects data from the "smart home" devices and is able to control these devices remotely via the gateway. In this scenario, Tom's house information related to power, gas and water consumption can be collected and reported to the smart home applications platform. At the same time, Tom can manage the application related policy of his home using the smart home applications and the application related policy can be sent to MOC devices in order to be executed according to Tom's requirements.

Let us now consider that Tom is out of his house while a fire occurs in his kitchen where his son is cooking. When detecting this event, the MOC device (i. e., the smoke sensor) sends an alarm message to Tom directly. Upon receipt of this information, Tom initiates a video communication with the camera to check the status of the kitchen, and to tell his son how to use the fire extinguisher or to exit. For privacy and security reasons, the camera is only connected and controlled by members of Tom's family.

Requirements

Use case technical challenges	**Service requirements**	**NGN requirements**	**MOC devices/gateways requirements**
Enhanced video/audio based capabilities, such as concurrent video streaming and local-breakout.	Prevention of access concentration into a single resource when QoS is impacted by high application traffic.	Support the following QoS policies and corresponding traffic parameters: packet transfer delay, packet delay variation, packet loss ratio, packet error ratio.	—

Group management for MOC devices with the same characteristics, for example, power meters in different smart homes.	*See "Grouping" in Use Case 1*	*See "Grouping" in Use Case 1*	*See "Grouping" in Use Case 1*
Message broadcasting and multicasting based on specific characteristics, such as group and location, to support functions such as firmware upgrading.	—	Support of broadcasting and multicasting for MOC groups (with MOC devices and gateways directly or indirectly connected to NGNs).	MOC gateways are required to support broadcasting and multicasting.

Chapter 7
Conclusions

In the conclusion part of the work, we'd like to concern the problems, strongly connected with organization, provision management and administration of public services, or technological structure of the global information society, which will already include NGN and IoT objects. The number of interacting subjects and objects, that can access the global networks, has increased tremendously. This will lead to noticeable and probably even full destructuring of the existent world-perception. Besides, this will demand working out new ideas on the world imagery. This process will naturally influence on services contents while organizing these services and providing with them, as well as on their administration's effectiveness. The systems of IoT sensors, implied in the environment (e. g., multisensor systems), will provide us with new opportunities, but also will bring new troubles.

Now, there are a few problems that can be defined already. These problems are waiting for their decision, so an effective administration of public services could be performed. The main questions are:

- How will the new sensors be standardized, checked up and integrated with the existing measurement instrumentation?
- How will they react in the case of emergency?
- How will Big Data from the sensors be organized using ICT resources?
- How one can use Big Data aggregated by global sensor networks to construct a new perception of the world (which borders are constantly changing)?
- Will broadly adopted sensors (including nanosensors) become a new source for the pollution of the environment? Although wireless sensors are kind of tiny and low energy devices, their lifetime is short enough and typical applications use big arrays of such sensors. After short lifetime these arrays may cause pollution of environment like any other electronical wastes.

All these questions prove that such tendencies, appeared via the convergence of IoT, NGNs, nano- and cogitotecnologies, create the opportunities that previously were not accessible.

Bibliography

[1] S. Glazyev, “The global economic crisis as a process of technological shifts,” *Problems of Economic Transition*, vol. 52, no. 5, pp. 3–19, 2009.

[2] C.-Y. Chong and S. P. Kumar, “Sensor networks: evolution, opportunities, and challenges,” *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[3] W. Dargie and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice*. Wiley. com, 2010.

[4] R. T. Lacoss, “Distributed mixed sensor aircraft tracking,” in *American Control Conference, 1987*, pp. 1827–1830, IEEE, 1987.

[5] G. J. Pottie, “Wireless integrated network sensors (WINS): the web gets physical,” in *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2001 NAE Symposium on Frontiers of Engineering*, p. 78, National Academies Press, 2002.

[6] G. J. Pottie and W. J. Kaiser, “Wireless integrated network sensors,” *Communications of the ACM*, vol. 43, no. 5, pp. 51–58, 2000.

[7] S. Vardhan, M. Wilczynski, G. Portie, and W. J. Kaiser, “Wireless integrated network sensors (WINS): distributed in situ sensing for mission and flight systems,” in *Aerospace Conference Proceedings, 2000 IEEE*, vol. 7, pp. 459–463, IEEE, 2000.

[8] W. J. Kaiser, K. Bult, A. Burstein, D. Chang, *et al.*, “Wireless integrated microsensors,” in *Technical Digest of the 1996 Solid State Sensor and Actuator Workshop*, 06 1996.

[9] G. Asada, A. Burstein, D. Chang, M. Dong, M. Fielding, E. Kruglick, J. Ho, F. Lin, T. Lin, H. Marcy, *et al.*, “Low power wireless communication and signal processing circuits for distributed microsensors,” in *Circuits and Systems, 1997. ISCAS’97., Proceedings of 1997 IEEE International Symposium on*, vol. 4, pp. 2817–2820, IEEE, 1997.

[10] J. Rabaey, J. Ammer, J. da Silva Jr, and D. Patel, “PicoRadio: Ad-hoc wireless networking of ubiquitous low-energy sensor/monitor nodes,” in *VLSI, 2000. Proceedings. IEEE Computer Society Workshop on*, pp. 9–12, IEEE, 2000.

[11] J. Da Silva Jr, M. JS, C. G. Ammer, S. Li, R. Shah, T. Tuan, M. Sheets, J. Ragaey, B. Nikolic, A. Sangiovanni-Vincentelli, *et al.*, “Design methodology for Pico Radio networks,” *Berkeley Wireless Research Center*, 2001.

[12] J. M. Kahn, R. H. Katz, and K. S. Pister, “Next century challenges: mobile networking for Smart Dust,” in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, pp. 271–278, ACM, 1999.

[13] K. S. Pister, J. M. Kahn, B. E. Boser, *et al.*, “Smart dust: Wireless networks of millimeter-scale sensor nodes,” *Highlight Article in*, p. 2, 1999.

[14] “µAMPS research.” URL: http://www-mtl.mit.edu/researchgroups/icsystems/uamps/research/overview.shtml, 2004. Accessed: 2013-11-08.

[15] B. H. Calhoun, D. C. Daly, N. Verma, D. F. Finchelstein, D. D. Wentzloff, A. Wang, S.-H. Cho, and A. P. Chandrakasan, “Design considerations for ultra-low energy wireless microsensor nodes,” *Computers, IEEE Transactions on*, vol. 54, no. 6, pp. 727–740, 2005.

[16] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, “IEEE 802.15. 4: a developing standard for low-power low-cost wireless personal area networks,” *network, IEEE*, vol. 15, no. 5, pp. 12–19, 2001.

[17] “The ZigBee alliance.” URL: http://www.zigbee.org/About/AboutAlliance/TheAlliance.aspx, 2014. Accessed: 2014-02-26.

[18] “HART communications foundation official website.” URL: http://www.hartcomm.org/, 2014. Accessed: 2014-02-26.

[19] “6LoWPAN working group.” URL: http://www.ietf.org/dyn/wg/charter/6lowpan-charter.html, 2014. Accessed: 2014-02-26.

[20] “Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.” ITU-T Recommendation Y.2221 (2010).

[21] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[22] G. Simon, M. Mar´oti, ´ A. L´edeczi, G. Balogh, B. Kusy, A. N´adas, G. Pap, J. Sallai, and K. Frampton, “Sensor network-based countersniper system,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 1–12, ACM, 2004.

[23] J. Yick, B. Mukherjee, and D. Ghosal, “Analysis of a prediction-based mobility adaptive tracking algorithm,” in *Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on*, pp. 753–760, IEEE, 2005.

[24] T. Gao, D. Greenspan, M. Welsh, R. Juang, and A. Alm, “Vital signs monitoring and patient tracking over a wireless network,” in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pp. 102–105, IEEE, 2006.

[25] K. Lorincz, D. J. Malan, T. R. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, “Sensor networks for emergency response: challenges and opportunities,” *Pervasive Computing, IEEE*, vol. 3, no. 4, pp. 16–23, 2004.

[26] M. Castillo-Effer, D. H. Quintela, W. Moreno, R. Jordan, and W. Westhoff, “Wireless sensor networks for flash-flood alerting,” in *Devices, Circuits and Systems, 2004. Proceedings of the Fifth IEEE International Caracas Conference on*, vol. 1, pp. 142–146, IEEE, 2004.

[27] G. Wener-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Walsh, “Deploying a wireless sensor network on an active volcano. data-driven applications in sensor networks (special issue),” *IEEE Internet Computing*, vol. 2, pp. 18–25, 2006.

[28] C. Buratti, A. Conti, D. Dardari, and R. Verdone, “An overview on wireless sensor networks technology and evolution,” *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[29] R. Hartley, “Transmission of information,” *Bell System Technical Journal*, 1928.

[30] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, *et al.*, “TinyOS: An operating system for sensor networks,” in *Ambient intelligence*, pp. 115–148, Springer, 2005.

[31] “Wireless Medium Access Control (MAC) and physical layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).” IEEE 802.15.4 Standard. Part 15.4 (2006).

[32] D. R. Green, “Geospatial tools and techniques for vineyard management in the twenty-first century,” in *The Geography of Wine* (P. H. Dougherty, ed.), pp. 227–245, Springer Netherlands, 2012.

[33] A. Galloway, “An Internet of Cows (and Sheeps!),” *Design Culture Lab*, 07 2011. URL: http://www.designculturelab.org/2011/07/20/an-internet-of-cows-and-sheeps/.

[34] “Requirements for the support of machine-oriented communication applications in the next

generation network environment." ITU-T Recommendation Y.2061.

[35] W. Huiyong, W. Jingyang, and H. Min, "Building a smart home system with WSN and service robot," in *Measuring Technology and Mechatronics Automation (ICMTMA), 2013 Fifth International Conference on*, pp. 353–356, IEEE, 2013.

[36] P. Waide, J. Ure, G. Smith, and B. Bordass, "The scope for energy and CO2 savings in the EU through the use of building automation technology," final report, Waide Strategic Efficiency, 08 2013.

[37] K. Jaafar and M. K. Watfa, "Sensor networks in future smart rotating buildings," in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, pp. 962–967, IEEE, 2013.

[38] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, "Health monitoring of civil infrastructures using wireless sensor networks," in *Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on*, pp. 254–263, 2007.

[39] W.-Z. Song, R. Huang, M. Xu, A. Ma, B. Shirazi, and R. LaHusen, "Air-dropped sensor network for real-time high-fidelity volcano monitoring," in *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pp. 305–318, ACM, 2009.

[40] G. Liu, R. Tan, R. Zhou, G. Xing, W.-Z. Song, and J. M. Lees, "Volcanic earthquake timing using wireless sensor networks," in *Proceedings of the 12th international conference on Information processing in sensor networks*, pp. 91–102, ACM, 2013.

[41] I. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 5, no. 1, p. 5, 2009.

[42] T. Saaty, *Decision Making with Dependence and Feedback: The Analytic Network Process: the Organization and Prioritization of Complexity*. Analytic hierarchy process series, Rws Publications, 2001.

[43] L. Yu and Z. Heng, "Measuring agility of enterprise using analytic hierarchy process and bayesian belief networks," in *Management Science and Engineering, 2006. ICMSE'06. 2006 International Conference on*, pp. 551–556, IEEE, 2006.

[44] C.-x. Chen, Z.-w. He, J.-g. Jia, J.-m. Kuang, and Z.-y. Zhang, "Fuzzy evaluation algorithm for system effectiveness of wireless sensor networks," in *Global High Tech Congress on Electronics (GHTCE), 2012 IEEE*, pp. 43–48, IEEE, 2012.

[45] N. Kamiyama and D. Satoh, "Network topology design using analytic hierarchy process," in *Communications, 2008. ICC'08. IEEE International Conference on*, pp. 2048–2054, IEEE, 2008.

[46] N. Ruan, Y. Ren, Y. Hori, and K. Sakurai, "Performance analysis of key management schemes in wireless sensor network using analytic hierarchy process," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pp. 1739–1744, IEEE, 2011.

[47] M. R. Ahmad, E. Dutkiewicz, *et al.*, "Performance analysis of MAC protocol for cooperative MIMO transmissions in WSN," in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, pp. 1–6, IEEE, 2008.

[48] Y. Yin, J. Shi, Y. Li, and P. Zhang, "Cluster head selection using analytical hierarchy process for wireless sensor networks," in *Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on*, pp. 1–5, IEEE, 2006.

[49] N. Yang, T. Liqin, S. Xueli, and G. Shukai, "Behavior trust evaluation for node in WSNs with

fuzzy-ANP method," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, vol. 1, pp. V1–299, IEEE, 2010.

[50] I. M. Khan, N. Jabeur, M. Z. Khan, and H. Mokhtar, "An overview of the impact of wireless sensor networks in medical health care," in *The 1st International Conference on Computing and Information Technology (ICCT)*, pp. 576–580, 2012.

[51] W. Dargie and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice*. Wiley. com, 2010.

[52] M. Souil and A. Bouabdallah, "On QoS provisioning in context-aware wireless sensor networks for healthcare," in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, pp. 1–6, IEEE, 2011.

[53] A. Meissner, T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner, "Design challenges for an integrated disaster management communication and information system," in *The First IEEE Workshop on Disaster Recovery Networks (DIREN 2002)*, vol. 24, 2002.

[54] "Personal safety in emergencies." ITU News, 3 2012.

[55] "Sensor Control Networks and related applications in Next Generation Network environment." ITU-T Recommendation Y.2222 (2013).

[56] T. Gao, C. Pesto, L. Selavo, Y. Chen, J. G. Ko, J. H. Lim, A. Terzis, A. Watt, J. Jeng, B.-r. Chen, *et al.*, "Wireless medical sensor networks in emergency response: Implementation and pilot results," in *Technologies for Homeland Security, 2008 IEEE Conference on*, pp. 187–192, IEEE, 2008.

[57] D. of Engineering and H. U. Applied Sciences, "Sensor networks for medical care," in *Technical Report TR-08-05*, 2005.

[58] K. Lorincz, B.-r. Chen, G. W. Challen, A. R. Chowdhury, S. Patel, P. Bonato, M. Welsh, *et al.*, "Mercury: a wearable sensor network platform for high-fidelity motion analysis.," in *SenSys*, vol. 9, pp. 183–196, 2009.

[59] J. A. Weaver, *A wearable health monitor to aid parkinson disease treatment*. PhD thesis, Massachusetts Institute of Technology, 2003.

[60] B. Lo, S. Thiemjarus, R. King, and G.-Z. Yang, "Body sensor network-a wireless sensor platform for pervasive healthcare monitoring," in *The 3rd International Conference on Pervasive Computing*, vol. 13, pp. 77–80, 2005.

[61] "Open service environment functional architecture for next generation networks." ITU-T Recommendation Y.2020.

[62] "Open service environment capabilities for NGN." ITU-T Recommendation Y.2234.

[63] "Requirements and capabilities for ITU-T NGN." ITU-T Recommendation Y.2201.

[64] "Requirements and framework allowing accounting and charging capabilities in NGN." ITU-T Recommendation Y.2233.

[65] Y. B. Kim, "u-healthcare service based on a USN middleware platform," *Networked Computing and Advanced Information Management, International Conference on*, vol. 0, pp. 673–678, 2009.

[66] M. Kim, Y. Lee, and J. Park, "Trend of USN middleware technology," *ETRI: Trend Analysis of Electronic & Telecommunication*, vol. 22, pp. 67–79, 06 2007.

[67] Y. Kim, M. Kim, and Y. Lee, "COSMOS: A middleware platform for sensor networks and a u-

healthcare service," in *ACM SAC'08*, (Brazil), pp. 512–513, 03 2008.

[68] "Service description and requirements for ubiquitous sensor network middleware." ITU-T Recommendation F.744.

[69] W. Lee, A. Datta, and R. Cardell-Oliver, "Network management in wireless sensor networks," *Handbook of Mobile Ad Hoc and Pervasive Communications: American Scientific Publishers*, 2006.

[70] A. Smailagic, "Location sensing and privacy in a context-aware computing environment," *Wireless Communications, IEEE*, vol. 9, pp. 10–17, 10 2002.

[71] H. Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, pp. 103–105, 10 2003.

[72] "Information technology – Security framework for ubiquitous sensor network." ITU-T Recommendation X.1311.

[73] "Ubiquitous sensor network middleware security guidelines." ITU-T Recommendation X.1312.

[74] "Security requirements for wireless sensor network routing." ITU-T Recommendation X.1313.

[75] "Security architecture for Open Systems Interconnection for CCITT applications." ITU-T Recommendation X.800.

[76] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[77] "Security architecture for systems providing end-to-end communications." ITU-T Recommendation X.805.

[78] *Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction*.

[79] D. Evans, "The Internet of Things. how the next evolution of the internet is changing everything," tech. rep., Cisco Internet Business Solutions Group (IBSG), 04 2011.