An Overview on Wireless Sensor Networks

Fabian Nack
Institute of Computer Science (ICS), Freie Universität Berlin
Email: FabianNack@web.de

***Abstract*—Wireless Sensor Networks are infrastructures containing sensing, computing and communication elements that aim to give its controllers the ability to measure, collect and react to occurrences in the monitored environment. They can be seen as interfaces between the virtual and the physical worlds. Because of their widespread applications, they are one of the most rapidly developing information technologies over the last few years. This report is designed to give an overview on the field of Wireless Sensor Networks and therefore focuses on outlining the general ideas behind WSNs, the technology that is used to implement these ideas, the different strategies of routing in these wireless networks and the strong and weak points of the technology.**

I. Introduction

A. What is a WSN?

Wireless Sensor Networks are wireless networks that usually consist of a great number of far distributed devices that are equipped with sensors (instruments that measure quantities in our environment) to monitor physical or environmental phenomenons. These devices work autonomous and are logically linked by self-organizing means.

Some of the challenges for these systems are:

- **Reliability:**
  WSNs are wireless networks and are therefore vulnerable to problems like packet loss. Nevertheless, they are used in areas such as chemical attack detection, in which these problems could easily lead to serious catastrophes.

- **Power Consumption:**
  The nodes of Wireless Sensor Networks are usually battery powered because of their size. This limits the lifetime of a sensor node and raises the topic of energy-efficiency in all aspects.

- **Node size:**
  Miniaturization is the keyword in many studies about WSNs. Developing smaller nodes, with the same or even more efficiency than their bigger brothers is still a challenge, even if present sensor nodes, are hardly as big as a coin.

- **Mobility:**
  Many applications urge the factor mobility into WSN challenges. For example, commercial applications, like vehicle tracking, need networks that are able to constantly change its routing paths and infrastructure.

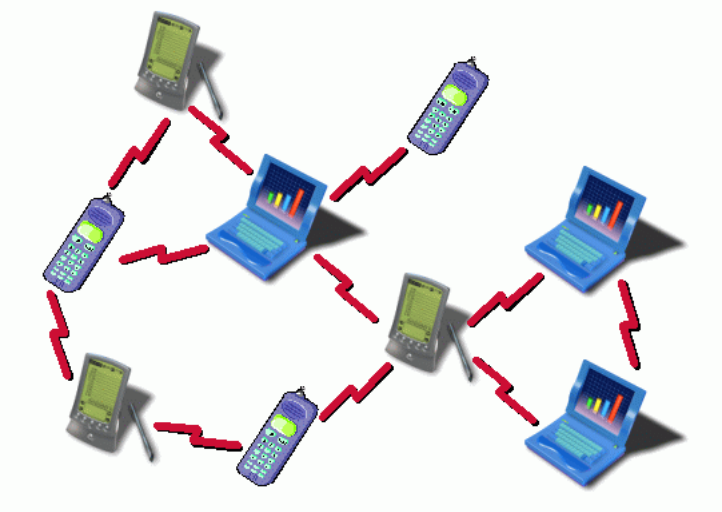
- **Privacy and Security:**
  Unlike wired channels, wireless channels are accessible to both, legitimate and illegitimate users. Therefore, several methods, like encoding the traffic, have to be discussed.

B. How does it work?

Wireless Sensor Networks is a class of special wireless ad hoc networks. A wireless ad hoc network is a collection of wireless nodes, that communicate directly over a common wireless channel. There is no additional infrastructure needed for ad hoc networks. Therefore, every node is equipped with a wireless transceiver and has to be able to act as an router, to process packets to their destinations.

A strength of these networks is their ability to self-organize the infrastructure of the routing, after they were deployed.

The following figure shows an example for a typical ad hoc network.



The main difference between common ad hoc networks and Wireless Sensor Networks is their different area of application. For WSNs, monitoring and collecting data are to the fore, while common ad hoc networks focus more on the communication aspects.

C. An overview on Sensor Networks

Similar to other (wireless) communication systems, the development of (Wireless) Sensor Networks has a variety of roots. The history can briefly be separated into four stages:

Stage 1: Cold-War Era Military Sensor Networks

During the cold war, a variety of projects that can be seen as prototypes of modern sensor networks were developed in the United States. These include the Sound Surveillance System (SOSUS), a system of acoustic sensors in the oceans used to monitor Soviet submarine movement, and several radar networks for air defense. Some of the sensors of SOSUS are still used for seismic activity surveillance.

Stage 2: Defense Advanced Research Projects Agency takes over

The impulse to researches on sensor networks was given in the early 1980s with programs initiated by the Defense Advanced Research Projects Agency (DARPA), an agency of the United States Department of Defense. They sponsored several programs, e.g. the "Distributed Sensor Networks (DSN)" research project that focused on further developments on newly invented technologies and protocols in context of their use for sensor networks. These ongoing works mainly paved the way for several modern warfare projects to take off.

Stage 3: Military Applications Development

In the late 1980s, the results of the DARPA-Research-Projects began to arouse interest of military planners. Military organizations started programs to adopt sensor network technology for warfare purposes. With these organizations spending huge amounts of money, the technology began to make progress faster and faster in the early 1990s.

Stage 4: Present-Day Research

Advances in computing and communication that were made in the late 1990s and early 2000s led to a new stage in the evolution of sensor network technology. More and more companies discovered the enormous potential of WSNs for commercial applications and standardization became important. Prominent examples for the newly introduced standards are for example ZigBee or WirelessHART which are both based on the IEEE 802.15.4 radio standard[1]. The following table gives an overview on the different generations of commercial used sensor networks and the progress in key areas, e.g. life span and size.

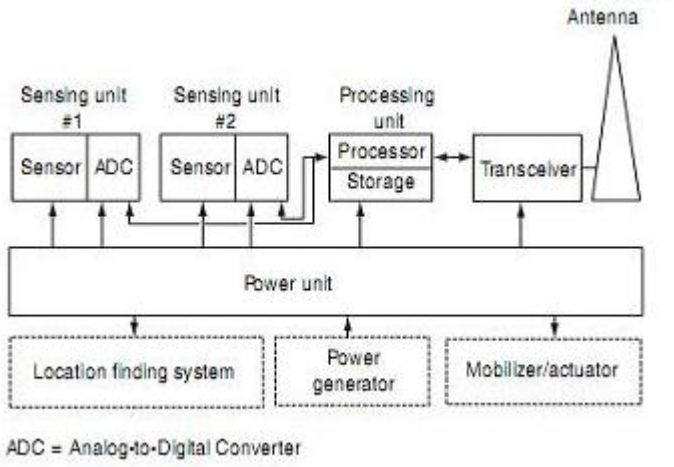
	First Generation (1980s–1990s)	Second Generation (Early 2000s)	Third Generation (Late 2000s)
Size	Attaché or larger	Paperback book or smaller	Small, even a dust particle
Weight	Pounds	Ounces	Grams or less
Deployment mode	Physically installed or air-dropped	Hand-placed	Embedded or "sprinkled," possibly nanotechnology-based
Node architecture	Separate sensing, processing, and communication	Integrated sensing, processing, and communication	Fully integrated sensing, processing, and communication
Protocols	Proprietary	Proprietary	Standard: Wi-Fi, ZigBee, WiMax, etc.
Topology	Point-to-point, star, and multihop	Client–server and peer-to-peer	Fully peer to peer
Power supply	Large batteries or line feed	AA batteries	Solar or possibly nanotechnology-based
Life span	Hours, days, and longer	Days to weeks	Months to years

II. The technology used for Wireless Sensor Networks

This chapter aims to give an overview on the technology used to implement the key features of Wireless Sensor Networks. It focuses on the hardware and software requirements, and gives a brief introduction to the network topology.[2]

A. Components of a Sensor Node (Hardware)

The figure shows a schematic of a typical sensor node hardware hierarchy.



As seen in the figure, there are several hardware components that make up a typical sensor node:

1) **Low-power embedded processor:**
The computational tasks on a WSN device include the processing of both locally sensed information as well as information communicated by other sensors. Currently, primarily due to economic reasons, the embedded processors are often substantially limited in terms of computational power (small MHz area). Due to the constraints of such processors, devices typically run specialized component-based embedded operating systems, such as TinyOS. They incorporate advanced low-power design techniques, such as sleep modes and dynamic voltage scaling to provide energy savings.[3]

2) **Memory/storage:**
In the storage, both, program memory (memory for the instruction set of the processor) and data memory (for storing measured data and other local information, e.g. the location of the node) are included. The size of the memory is often limited due to economic reasons. With the ongoing price-reduction of memory devices, the quantities of storage and memory used on sensor nodes increase over time.

3) **Radio transceiver:**
WSN devices include a low-rate, short-range wireless radio (10–100 kbps, <100m). While currently quite limited in capability too, these radios are likely to improve in sophistication over time – including improvements in cost, spectral efficiency, tun-ability, and immunity to noise, fading, and interference. Radio communication is often the most power-intensive operation in a WSN device, and hence the radio must incorporate energy-efficient sleep and wake-up modes.

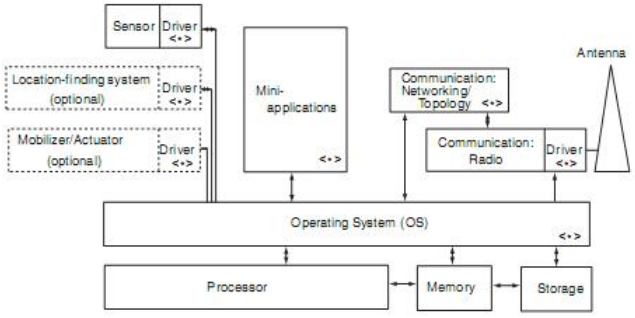
4) **Sensors with ADC unit:**
WSN devices usually support only low-data-rate sensing, because of the limitations of energy and bandwidth. In many applications, multi-modal sensing is necessary, resulting in the fact, that every device could have multiple sensors implemented. Which specific sensors are used, is application-based. The Analog-to-Digital Converter Unit translates the analog signals, provided by the sensors, to digital signals, that can be processed by the processor unit.

5) **Location finding system:**
To analyze the measured data, in many WSNs it is important to know in which location, the data was monitored. But unfortunately, only a few applications allow the designer to pre-configure the location of the sensor nodes. Particularly for randomly deployed WSNs, which are used, for example, for outdoor operations, location finding systems, normally based on satellite GPS, have to be implemented.[4]

6) **Power Source:**
Usually, the power source is a small battery. The finite battery power is likely to be the bottleneck in most WSN applications. However, in some applications, a couple of nodes may be wired to continuous power source or energy harvesting techniques may provide a small amount of renewed energy.

B. Components of a Sensor Node (Software)

The figure shows a schematic of a typical sensor node software hierarchy.



The software applications of a common sensor node, can typically be separated into five subsystems[5]:

1) **Operating System Microcode**
Operating System Microcode is also referred to as middleware. It represents the code, that is used by the high-level software modules to support a variety of functions. The middleware also covers the software from the machine-level functionality of the microprocessor. A famous example for a commonly used operating system for sensor networks is TinyOS.

2) **Sensor Drivers**
The sensor drivers are software modules that manage basic functions of the sensor transceivers. Depending on the type of the sensor, they manage to upload the right configuration and settings onto it.

3) **Communication Processors**
The communication processors manage the communication functions, including routing, packet buffering and forwarding, topology maintenance, medium access control (e.g., contention mechanisms, direct-sequence spread-spectrum mechanisms) and encryption.

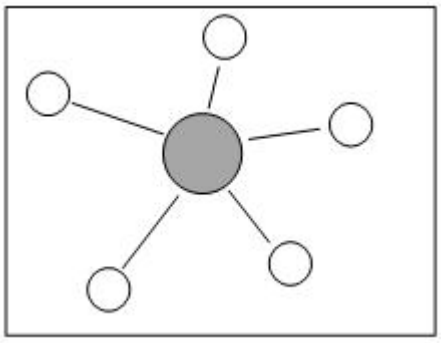
4) **Communication Drivers**
These software modules operate the details of the radio channel transmission link, including clocking and synchronization, signal encoding, bit recovery, bit counting, signal levels, and modulation.

5) **Data-Processing Mini-Applications**
Basic applications, e.g. data-processing, signal-value storage and manipulations, etc. They are supported at the node level for in-network processing.

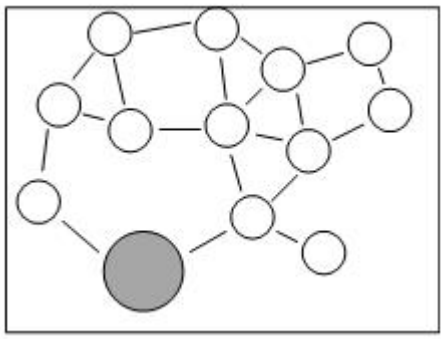
C. The Network Topology

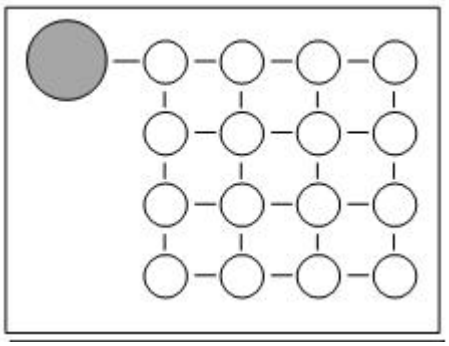
The network structure of WSNs is not limited to one design. When designing the network, the developer has several choices, which topology he wants to configure the network into.[6] Following are the different topologies:

1) Single-hop star: The single-hop star is the simplest WSN topology that is used. In this topology, every node communicates directly with the gateway. Wherever realizable, this structure can tremendously simplify design, as the networking concerns are reduced to a minimum. Unfortunately, the limitations of this topology are its poor scalability and robustness properties. For instance, in larger areas, nodes that are distant from the gateway will have low quality connections to the gateway.

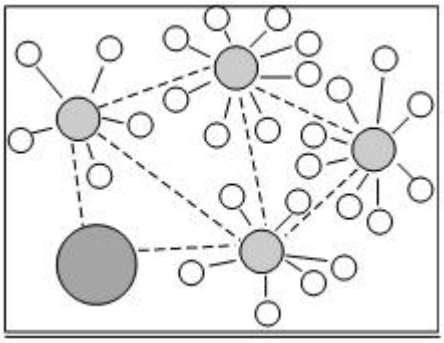


2) Multi-hop mesh and grid: For covering larger areas and networks, multi-hop routing is necessary. In this topology, the signal is transmitted from sensor to sensor until it reaches the gateway. The route of the signal is determined by a particular routing protocol (see Chapter 3). Depending on the fact, whether the WSN was structured or randomly deployed, the resulting network could look like figure 1 (random) or figure 2 (structured).





3) Two-tier hierarchical cluster: The most common architecture for larger WSNs is the two-tier hierarchical cluster architecture. In this topology, the nodes within a specified region report their data to a so-called cluster head. This cluster head forms a network with other cluster heads that are covering different regions. The network can be optional interlaced more and more, meaning that the cluster heads of tier 2 could send their data to a new cluster head that covers these tier 2 cluster heads and forms another network with other cluster heads, or finally send their data to the gateway. The advantage of this hierarchical structure is that it separates a large network into several zones within which, for example, routing can be performed locally. The cluster head nodes can also be designed more powerful in terms of computation/communication or could even be linked through a wired network, increasing transmission speed and reliability.



III. Routing Protocols

Wireless Sensor Networks are a class of wireless ad hoc networks that pose unique design challenges for their developers. The sensor nodes are normally battery-powered and therefore their lifetime is limited. Typically, these batteries also cannot be changed. Since energy is a valuable resource in WSNs, energy-efficient routing is one of the most important aspects of increasing the life span of sensors.[7], [8][9]

One of the factors, of energy-efficient routing, is the strategy of picking a route between two nodes. The challenges for the strategy are:

1) **Number of transmissions:**
   The number of transmissions until a packet reaches its destination should be as small as possible due to the fact that every transmission between two nodes uses energy. If the strategy minimizes the re-transmissions, it will also minimize the energy consumption.

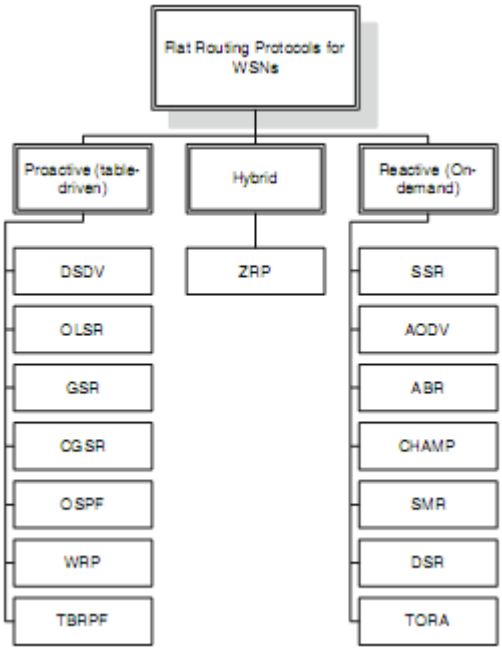
2) **Balanced use of nodes:**
   The use of the nodes for the routing has to be balanced between all the nodes. If some nodes are used distinctly more than others, their battery-power will decrease faster and will expire sooner. Too many dead sensor nodes could result in a partition of the network, which would make communication impossible.

3) **Delay:**
   For many applications of WSNs, it is important that the delay of the transmission is not too big. It is desirable, that the strategy comes to a compromise between overhead and delay.

4) **Balancing the previous aspects:**
   The routing strategy has to be aware of the energy resources that are left and has to balance all the previous aspects to produce the best possible solution.

The following section focuses on the relevant routing

techniques used in WSNs. The most common protocols can be classified in three different categories: pro-active, re-active, and hybrid. The following figure shows some popular routing protocols and to which section they belong.



A. Pro-active Protocols

Pro-active routing protocols, like Optimized Link State Routing (OLSR), Open Shortest Path First (OSPF), and Topology Broadcast based on Reverse-Path Forwarding (TBRPF), operate in a way that can be compared to wired networks. They are constantly sending routing information from each sensor node to every other node in the network and as a result are able to preserve an up-to-date map of the network with all known routes. These information are saved in tables on every node. Pro-active protocols produce a relatively high overhead due to the constant exchange but have a smaller delay than other protocols because the routes are already available on request.

B. Re-active Protocols

Re-active routing protocols are also referred to as on-demand routing protocols. Different from pro-active protocols, re-active protocols initiate route discoveries only at the request of a node. If a route to a destination is required, a search procedure will be started to find a path from the requesting node to the destination. Of course this produces a lower overhead but results in bigger delays. Existing re-active protocols are, for example, Associativity-Based Routing (ABR), Dynamic Source Routing (DSR), and Ad Hoc On-Demand Distance Vector Routing Protocol (AODV).

C. Hybrid Protocols

Hybrid Protocols are a mixture of both, re-active and pro-active routing. They aim to combine the advantages of both of these methods, by locally using pro-active and inter-locally using re-active routing. The idea behind hybrid routing is based on the fact that most communication in WSNs happens between nodes that are areal not wide apart and that changes in topology only affect nodes in the neighborhood of the change. One approach to implement hybrid routing is to divide the WSN into several zones, and use pro-active routing inside each zone, and re-active routing between them. This protocol is called Zone Routing Protocol (ZRP).

IV. Strong and weak points / Pros and Cons

A. In which areas WSNs are used

Research on Wireless Sensor Networks once began with focus on high-end-applications such as military surveillance purposes and target tracking, seismic monitoring or radiation detection systems. Lately, interest in networked biological and chemical sensors for national security applications increased and the outputs on this field are still high. Furthermore, with the advances in computation and the rising technization of normal life, interest extends also to consumer applications, which promise a high profit margin. Following is a short list to give a sense of the wide-ranging scope of WSN applications[10]:

1) **Environmental applications:**
   Forest fire detection
   Seismic Monitoring
   Flood detection
   Automated agriculture
   Ecological habitat monitoring
   etc.

2) **Military applications:**
   Monitoring equipment
   Battlefield surveillance
   Nuclear, biological and chemical attack detection
   Target tracking
   Monitoring enemy forces
   etc.

3) **Health applications:**
   Remote monitoring of physiological data
   Disease prevention
   etc.

4) **Home applications:**
   Home automation
   Home security
   Fire detection
   etc.

5) **Commercial applications:**
   Environmental control in industrial and office buildings
   Vehicle tracking
   Industrial and Commercial networked sensing
   Traffic flow surveillance

etc.

B. What are the strong points of WSNs

As the variety of applications, for which WSNs are used, indicates, there have to be a couple of strong points of WSNs that justify their utilization in all these different aspects of life. Following is a list of the advantages of Wireless Sensor Networks:

- **Robustness/Ability to withstand rough environmental conditions**
  Because of their shrinking size, their ability to communicate through a lot of materials and the possibility to cover the particular nodes in robust cases, WSNs can be used in a huge variety of environments. They are designed to defy harsh weather conditions. That is one of the reason, they are already used for things like forest fire detection or seismic monitoring

- **Ability to cover wide and dangerous areas**
  In many areas, infrastructural issues and economic considerations prevent wired networks from being used. For example, setting up a wired network on a battlefield would obviously be useless. WSNs can fill this gap, because of their lack of infrastructure and their low setup costs.

- **Self-Organizing**
  With the abilities of network discovery and multi-hop broadcast, WSNs are able to self-organize in small amounts of time, when setup. This is interesting, because someone who sets up the network by deploying the several nodes, does not have to be trained. He just needs to turn on the system and the rest should be organized by the network itself.

- **Ability to master node failures**
  WSNs are able to overcome node failures, resulting of destroyed or dead nodes, by simply using another routing path. If, for example, during war, an enemy destroys a surveillance sensor node, this will not affect the whole network.

- **Mobility of nodes**
  Mobility of nodes has been a big research field in the last few years. Sensor Nodes, that, for instance, are used to track vehicles, are permanently relocating. Modern WSN protocols and architectures are able to handle these areal shiftings and to maintain routing.

- **Dynamic network topology**
  WSNs are able to have a dynamic network topology, which means that the topology is variable and determines the neighbor relationships to be maintained by the nodes. For example, if a cluster head in the topology drops out, another sensor can jump in and take the place of the cluster head, which leads to a change of the topology.

- **Heterogeneity of nodes**
  The fact, that the monitored data of the sensors, is first converted into digital signals, and then transmitted, benefits the fact, that a special WSN can contain a variety of different sensors in one network. Every node can also have multiple different sensors implemented on it. Of course, this is interesting for a huge amount of applications, e.g. weather surveillance or disease prevention systems.

- **Unattended operation**
  Designed and configured correctly, WSNs are be able to work unattended. This saves working time and minimizes the effort that has to be done to administrator these systems. This advantage is probably very interesting for home applications, were non-trained customers want to benefit from the system with low effort.

C. What are the weak points of WSNs

- **Limited energy resources**
  With the absence of a fixed infrastructure, wireless sensor nodes are forced to manage the small amounts of battery provided power, they have, carefully. This limits their computational power and memory size, and prevents them from using full bandwidth due to higher energy costs. Working only on battery power, also means, that after a certain life span, a sensor node will die, because the battery is empty. Among other things, this fact leads to serious security issues (see point 4), that have to be kept in sight.

- **Lower data rates**
  One of the biggest problem of wireless networks in general are the low data rates. The amount of data that can be transmitted in a period of time depends on the frequency that is used. A higher frequency results in higher data rates, but at the same time causes more interference issues. This leads to the fact, that wireless networks can not be as quick as their wired brothers.

- **Communication failures**
  Wireless Networks have a higher error rate than their wired counterparts. They use electronic waves to transmit packets and these waves can be affected by phenomenons like reflection, refraction, diffraction or scattering. These phenomenons can fragment or garble the package, and that way produce error in transmission.

- **Security issues**
  Wireless Networks in general are much easier to attack from the outside, than wired systems are. The wireless channel is accessible to unwanted listeners and several passive and active attacks can be conducted. Methods like encryption are also limited by the energy resources, that tend to be small in WSNs, which strenghtens the problems.

Another WSN specific problem, are dying or malfunctioning sensor nodes. Especially in applications, dealing with life-endangering aspects, every node that falls out increases the risk, that the sensor network is not able to further on monitor data in a way security is guaranteed.[11][12], [13], [14]

D. What are the effects on privacy protection[15]

Wireless Sensor Networks have the potential to change everything in our surroundings, including the way we live, or work. With widespread applications, they could affect nearly every part of our daily life enriching and making it easier. However, there are also negative aspects, that could potentially arise from this growing surveillance industry. Privacy protectionists warn, that this development could lead into a loss of privacy of the individual.

An alarming fact is, that more and more people seem to get an attitude, that says: "I have nothing to hide, so I don't care about privacy protection!", without thinking about things like medical conditions, sexual life or bank account information. In a way, it seems like there is a lack of education on this topic.

Probably, the best way to achieve a certain understanding for the technology is to debate honestly and open in a reasoned way in public about the upcoming developments. The value of the benefits that come with WSN developments may not seduce us to blink facts like "informational self-decision"

.

V. Conclusion

In conclusion to this report, one can say that the end of research on WSNs is not within sight. Wireless Sensor Network technology has an incredible potential to enhance quality of life in all aspects and is likely to be widely used in the medium-term future.To realize the full potential of this technology, there is a lot of additional work to be done in further times. Research has to focus on security aspects and higher reliability for these systems and guidelines for aspects of privacy protection have to be discussed. With these challenges in mind, the fast speed, with which further developments of the technology flood on the field, can lead to optimism and excitement on upcoming applications.

References

[1] G. Bell, "A time and a place for standards," *Queue*, vol. 2, no. 6, pp. 66–74, 2004.

[2] M. W. Chiang, Z. Zilic, J.-S. Chenard, and K. Radecka, "Architectures of increased availability wireless sensor network nodes," *Test Conference, International*, vol. 0, pp. 1232–1241, 2004.

[3] A. E. Kateeb, A. Ramesh, and L. Azzawi, "Wireless sensor nodes processor architecture and design," *Advanced Information Networking and Applications Workshops, International Conference on*, vol. 0, pp. 892–897, 2008.

[4] K. S. Low, H. A. Nguyen, and H. Guo, "Optimization of sensor node locations in a wireless sensor network," *International Conference on Natural Computation*, vol. 5, pp. 286–290, 2008.

[5] M. A. Taleghan, A. Taherkordi, M. Sharifi, and T.-H. Kim, "A survey of system software for wireless sensor networks," *Future Generation Communication and Networking*, vol. 2, pp. 402–407, 2007.

[6] H. Chen, C. K. Tse, and J. Feng, "Impact of topology on performance and energy efficiency in wireless sensor networks for source extraction," *IEEE Transactions on Parallel and Distributed Systems*, vol. 99, no. 1, 5555.

[7] D. J. Vergados, N. A. Pantazis, and D. D. Vergados, "Energy-efficient route selection strategies for wireless sensor networks," *Mob. Netw. Appl.*, vol. 13, no. 3-4, pp. 285–296, 2008.

[8] R. S. Bhuvaneswran, J. L. Bordim, J. Cui, and K. Nakano, "Fundamental protocols for wireless sensor networks," *Parallel and Distributed Processing Symposium, International*, vol. 3, p. 30137a, 2001.

[9] N. N. Pham, J. Youn, and C. Won, "A comparison of wireless sensor network routing protocols on an experimental testbed," *Sensor Networks, Ubiquitous, and Trustworthy Computing, International Conference on*, vol. 2, pp. 276–281, 2006.

[10] E. Sabbah, A. Majeed, K.-D. Kang, K. Liu, and N. Abu-Ghazaleh, "An application-driven perspective on wireless sensor network security," in *Q2SWinet '06: Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks*. New York, NY, USA: ACM, 2006, pp. 1–8.

[11] D. Wang, Q. Zhang, and J. Liu, "The self-protection problem in wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 3, no. 4, p. 20, 2007.

[12] G. de Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," *Wireless and Mobile Computing, Networking and Communication, IEEE International Conference on*, vol. 0, pp. 580–585, 2008.

[13] Z. Zhi, "A cryptography system for wireless sensor networks based on ibe and cpk algorithms," *Pacific-Asia Workshop on Computational Intelligence and Industrial Application, IEEE*, vol. 2, pp. 857–861, 2008.

[14] H. Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, no. 10, pp. 103–105, 2003.

[15] C. Reynolds and R. Picard, "Affective sensors, privacy, and ethical contracts," in *CHI '04: CHI '04 extended abstracts on Human factors in computing systems*. New York, NY, USA: ACM, 2004, pp. 1103–1106.

[16] N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 9, no. 2, pp. 4–18, 2005.

[17] Z.-Y. Cao, Z.-Z. Ji, and M.-Z. Hu, "An image sensor node for wireless sensor networks," *Information Technology: Coding and Computing, International Conference on*, vol. 2, pp. 740–745, 2005.

[18] D. Gra?anin, M. Eltoweissy, S. Olariu, and A. Wadaa, "On modeling wireless sensor networks," *Parallel and Distributed Processing Symposium, International*, vol. 13, p. 220b, 2004.

[19] M. Hempstead, N. Tripathi, P. Mauro, G.-Y. Wei, and D. Brooks, "An ultra low power system architecture for sensor network applications," *Computer Architecture, International Symposium on*, vol. 0, pp. 208–219, 2005.

[20] B. Hurler, H.-J. Hof, and M. Zitterbart, "A general architecture for wireless sensor networks: Fisrt steps," *Distributed Computing Systems Workshops, International Conference on*, vol. 3, pp. 442–444, 2004.

[21] A. Krings, "Design for survivability: a tradeoff space," in *CSIIRW '08: Proceedings of the 4th annual workshop on Cyber security and informaiton intelligence research*. New York, NY, USA: ACM, 2008, pp. 1–4.

[22] B. Krishnamachari, *Networking Wireless Sensors*. Cambridge University Press, 2005.

[23] S. Mahfoudh and P. Minet, "Survey of energy efficient strategies in wireless ad hoc and sensor networks," *International Conference on Networking*, vol. 0, pp. 1–7, 2008.

[24] T. Pazynyuk, J. Li, G. S. Oreku, and L. Pan, "Qos as means of providing wsns security," *International Conference on Networking*, vol. 0, pp. 66–71, 2008.

[25] J. A. Stankovic, "Wireless sensor networks," *Computer*, vol. 41, no. 10, pp. 92–95, 2008.

[26] Q. Wang, T. Zhang, and S. Pettersson, "An effort to understand the optimal routing performance in wireless sensor network," *Advanced Information Networking and Applications, International Conference on*, vol. 0, pp. 279–286, 2008.

[27] M. Youssef and N. El-Sheimy, "Wireless sensor network: Research vs. reality design and deployment issues," *Communication Networks and Services Research, Annual Conference on*, vol. 0, pp. 8–9, 2007.