Wireless Sensor Networks: Status and Trends

Fischerauer, Gerhard; Stöber, Ralf
Lehrstuhl für Mess- und Regeltechnik, Universität Bayreuth
D-95540 Bayreuth

Abstract

Wireless Sensor Networks (WSN) are distributed systems comprising a (possibly large) number of intelligent, energetically self-sufficient sensors communicating by radio waves. With them, the vision of an "intelligent environment" created by man could come true. The present contribution gives an overview of the fundamental challenges to be overcome when wireless sensor networks are to be realized, of the state of the art, and of current trends.

I. INTRODUCTION

Technical progress in the last decades is marked by the decentralization and ubiquity of computing power and information. While the computational ubiquity has been enabled by microprocessors, more than 90 % of which are built into embedded systems, the wide availability of information is due to mobile communication and the internet. At the same time, the importance of automatic control techniques has led to a wide distribution of sensors, for instance in automotive technology. It goes without saying that computing power, radio communication, and sensors are already combined to create complex systems, such as when a decentralized measurement unit sends alarm messages in text form via a GSM or UMTS cell phone.

The functional density of microprocessors, microsystems technology, hybrid integration techniques, and modern radio communication technologies have arrived at a level which makes conceivable an even denser integration of computing power, radio communication, and sensors. In other words, a distributed system consisting of a high number of intelligent, energetically self-sufficient, or energy-autarkic, sensors communicating by radio waves appears quite feasible. Such *wireless sensor networks* (WSN) command a lot of attention in the current literature [1, 2].

The vision is to create an „intelligent environment“ by letting hundreds or thousands of sensors and embedded processors interact with each other. This would pave the way for novel solutions in areas such as environmental monitoring, early disaster warning, remote monitoring of patients, machines, and plants, room climate control, or the management of energy consumption in buildings.

II. HARDWARE AND SOFTWARE REQUIREMENTS IN WIRELESS SENSOR NETWORKS

The communication needs in WSNs are quite different from those in networks supporting human communication. The cell phone networks GSM and UMTS, for instance, have been designed to transmit information between two subscribers as much unchanged as possible and at a high data rate. The dominant criterion is information per time and bandwidth (in bit/s/Hz). In contrast, data traffic in a WSN must be limited to prevent flooding of the central node with raw data and to save energy. The dominant criterion is information per cost and energy consumed (in bit/€/J). Hence, WSN nodes must transmit condensed, preprocessed information. For this reason, the sensors are likely to communicate much more often with each other than with a central node. The fundamental challenges are the following:

- The sensor nodes should not require the wired connection to a central power source, but rather be equipped with a power source of their own (otherwise, the need for wireless communication can be questioned). Energy autarky then requires energy efficiency to extend operating lifetime. This precludes the use of many established, but computationally and thus energetically expensive algorithms for signal processing, database search, data encryption etc.
- The majority of the available energy is used up by communication. This calls for new hardware and software solutions which will make the RF frontend more energy-efficient and will help to reduce the amount of data to be transmitted.
- Large networks cannot be configured and maintained by human operators. Instead, they have to be self-configuring and adapt automatically to changes in the network such as the failure of nodes.

The average power consumption of a sensor node must not exceed 100 µW per cm³ of battery volume if a minimum operating lifetime of one year is required (the best available batteries, of the lithium ion type, feature an energy density of 3000 J/cm³). Wireless communication, however, consumes 10 to 100 mW at a transmission power of 0 dBm and a receiver sensitivity of –100 dBm, as do the storage and processing of data. Consequently, a sensor node must spend 99 to 99.9 % of the time in an energy-saving idle mode, which is to be supported by the hardware [2].

With today's battery technology, if a small sensor node is to operate for five or ten years, it must tap additional sources of energy in its environment, a process called energy harvesting. Physical effects that could be exploited to this end are photovoltaics (energy from light), thermoelectricity (energy from temperature gradients), piezoelectricity (energy from vibrations), and others. Both estimates and laboratory demonstrators suggest that energy harvesters with areas of 1 cm² or volumes of 1 cm³ are capable of delivering average powers in excess of 100 µW, depending on the field of application (Fig. 1; see also Fig. 1 in [2]). Still, as of now, no one has been able to deploy a WSN with truly energy-autarkic sensor nodes. It should also be mentioned that energy harvesting is about more than just energy conversion. Since the energy harvested from the environment varies with time, sometimes very fast so, one also needs energy management strategies and intermediate energy storage units such as batteries or capacitors. The optimization of the overall efficiency of such an energy harvesting system is by all means an area of active research.

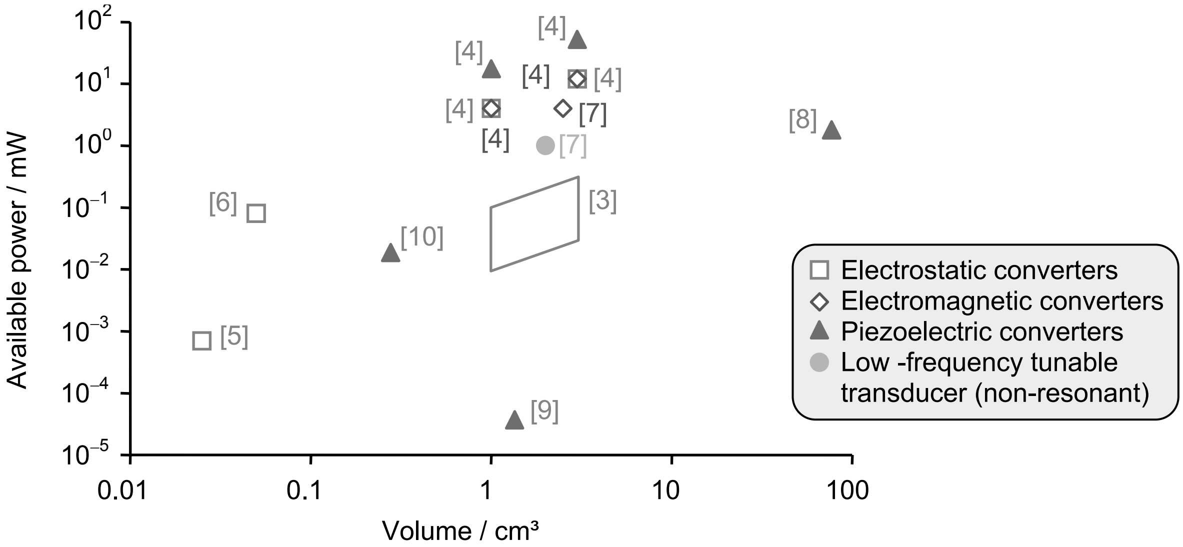

Figure 1. Volume and available power of dedicated hardware converting vibrational energy to electrical energy.

Although the nodes in a WSN will likely not transmit many data and could make do with an average data rate of much less than 10 kbit/s, the small ratio of active-to-inactive time mentioned above leads to data rate requirements of up to several 100 kbit/s.

Finally, if a large WSN is to be economically feasible, the price tag attached to a single sensor node should read 1 € or less. This is one to two orders of magnitude below current prices.

III. Network Protocols

A. Overview

In view of the energy restrictions in a WSN, the node-to-node distance has to be kept below about 10 m (100 m at most). Such networks are called w*ireless personal area networks* (WPAN). Fig. 2 compares the characteristics of some protocols meeting the range and data rate requirements discussed above. Among these network protocols, Bluetooth, Wi-Fi, and DECT are widely used in the office (and therefore lack energy efficiency). The former two are also becoming more widespread in industrial automation, and a Bluetooth variant by ABB called WISA (*wireless interface for sensors and actuators*) specifically targets real-time industrial control applications. Bluetooth, based on IEEE standard 802.15.1 [11], is limited to smaller networks with five to seven nodes and has been reported to struggle with data security problems. Intel's early wireless sensor nodes of the *Mote* series supported Bluetooth.

Wi-Fi (w*ireless fidelity*), the technology of today's WLANs, is based on the IEEE 802.11 family of standards [12]. The protocol has been designed for rather high data rates unnecessary in WSNs, but could be useful for the wireless connection of selected master nodes in different WSNs.

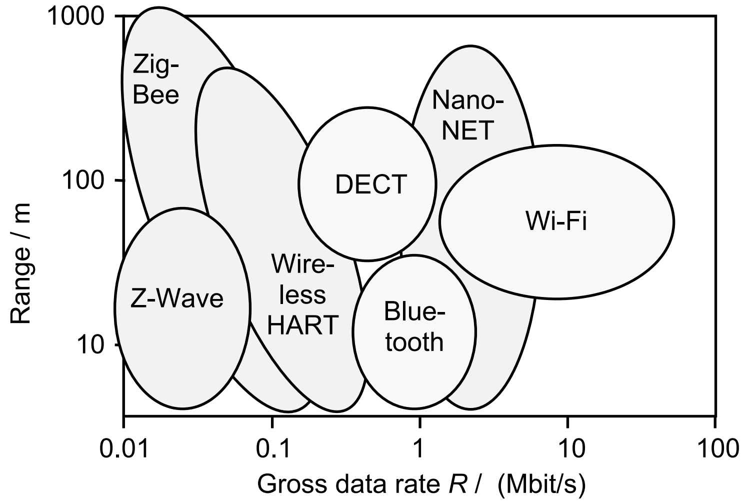

Figure 2. Data rates and ranges of selected wireless networks. A lighter shade indicates general-purpose networks known from office applications, a darker shade refers to special wireless sensor networks.

The European standard for cordless digital phones, DECT (*digital enhanced cordless telecommunications*), has also been allocated a frequency band in the U.S.A. in 2005, but no sensor applications have become known so far.

Among the dedicated WSN protocols, one finds both proprietary and standardized solutions. Examples of the former are:

- Z-Wave (Zensys and Z-Wave Alliance) with more than 225 home automation products in the American market;
- EnOcean (EnOcean and EnOcean Alliance) with more than 500’000 installed energy-autarkic sensor nodes in more than 300 building automation products;
- SimpliciTI (Texas Instruments), launched in September 2007 as a competitor to Z-Wave.

Ultra-wideband (UWB) technologies are also considered candidates for wireless sensor networks. They work with a very low power spectral density by spreading the signal energy over a wide bandwidth. In Germany, for instance, the frequency band from 30 MHz to 10.6 GHz has been opened up to UWB applications in January 2008. The exact implications of UWB for wireless sensing are not yet clear.

Currently, the single most important technology for standardized WSN solutions appears to be IEEE standard 802.15.4 [13]. All protocols likely to dominate the market for commercial solutions are based on it:

- ZigBee (hardware, e. g., by Intel, Texas Instruments, Crossbow [more than 500’000 installed nodes] or Ember [in Siemens products]) [14];
- NanoNET (Nanotron) with chirp spread spectrum modulation [15];
- WirelessHART (HART Foundation) [16].

Table I characterizes some network protocols which are of particular interest in the present context.

Table I. Network protocols designed for wireless sensor networks.

Item	Protocol			
	Z-Wave	ZigBee	NanoNET	WirelessHART
Standard (IEEE …)	—	802.15.4	802.15.4a	802.15.4
Modulation by [1]	BFSK	BPSK; OQPSK	CSS	OQPSK
Multiple access by [2]	CSMA	CDMA/DSSS	TDMA	TDMA + CDMA/DSSS
Frequency band [3]	A; B	A; B; C	C	C
Data rate / (kbit/s)	20	20; 40; 250	250, 1000	250
Range in m	30…100	75…1600	60…900	200

[1] BFSK = binary frequency shift keying; BPSK = binary phase shift keying; CSS = chirp spread spectrum; OQPSK = offset quadrature phase shift keying.

[2] CDMA/DSSS = code division multiple access with direct sequence spread spectrum; CSMA = carrier sense multiple access; TDMA = time division multiple access.

[3] A = 868… 868.6 MHz (EU); B = 902...928 MHz (U.S.A.); C = 2.4…2.48 GHz (global).

B. *ZigBee*

By way of an example, let us consider ZigBee, the most widely distributed WSN standard [14]. A ZigBee network may comprise 216 nodes in theory. One of the nodes, the ZigBee coordinator, transmits beacon frames at a regular interval to synchronize and organize the network. The other nodes are either capable of routing messages between devices (routers) or communicate with just one other node (end devices). All sensor nodes proper belong to the latter device type. The network forms by itself in an ad-hoc manner in one of several possible topologies (star, mesh, cluster; Fig. 3). When a node in an established network path fails, messages are automatically rerouted via alternative paths.

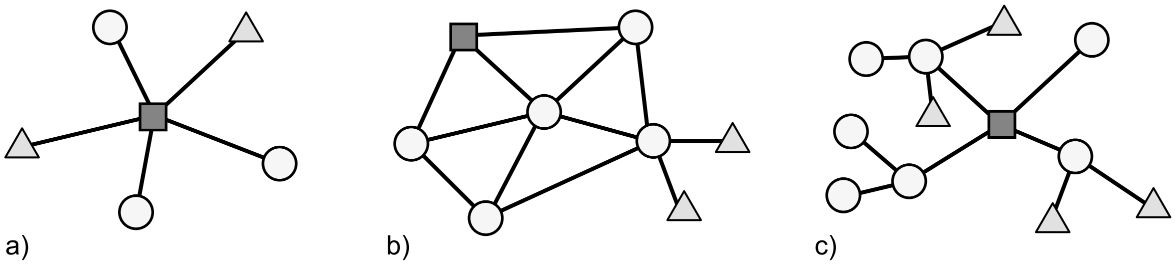

Figure 3. ZigBee network topologies. a) Star. b) Mesh. c) Cluster. ■ = coordinator; ○ = router; △ = end device.

The physical and the media access layers of the ISO OSI seven-layer reference model are set out in IEEE 802.15.4 while the network and application layer definitions are part of the ZigBee specification. The network layer organizes the network by adding and removing nodes, assigning addresses to newly associated devices, ensuring data security on the frame level, discovering and maintaining routes between devices, and routing frames to their intended destinations via multihopping.

The application layer comprises the application support sublayer (APS), the application frame with vendor-specific application objects (up to 240), and the ZigBee Device Object (ZDO) (Fig. 4a). The latter defines the role of a device within the network, discovers devices on the network, determines which application services they provide, initiates and/or responds to requests for the creation of a logical link between two devices (a process called binding), and establishes a secure relationship between network devices. The APS provides an interface to data and security services for both application objects and the ZDO. For example, it maintains tables for binding and handles 128-bit encryption keys.

Both IEEE 802.15.4 and ZigBee aim at low cost and maximum energy efficiency by, e. g., avoiding telegram collisions which would require messages to be sent repeatedly, idle listening to data traffic, and limiting telegram overhead.

ZigBee is supported by more than 230 companies, among which one encounters semiconductor suppliers, software developers, end device manufacturers, and service providers. They agree on public or vendor-specific application profiles to define what messages are to be exchanged for a given application such as home automation or industrial plant control. Devices with the same application profile interoperate end to end. All standard-compliant platforms, of which there exist more than 30 at the moment, are based on such application profiles (Fig. 4b).

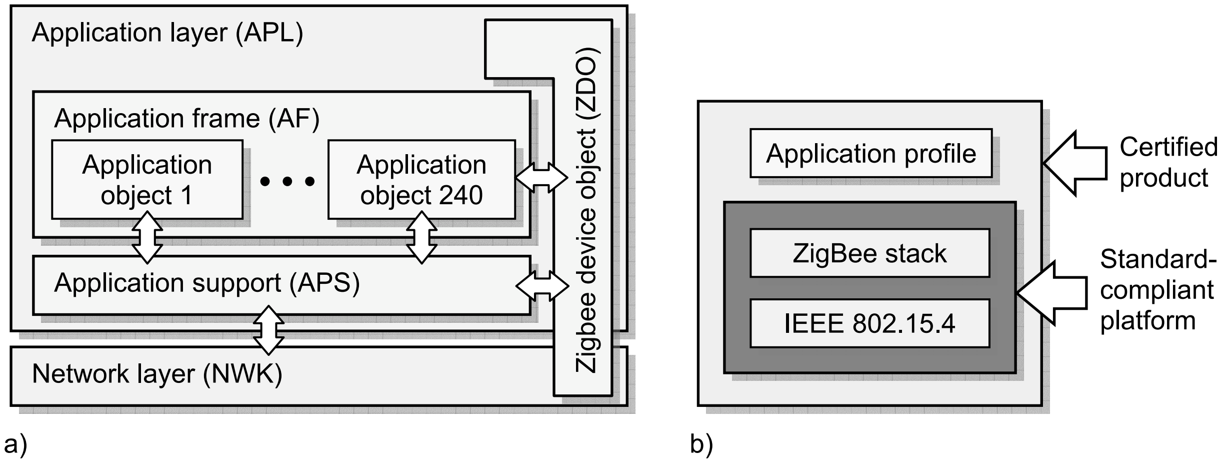

Figure 4. ZigBee standard [14]. a) Protocol stack architecture. b) Co-operation between IEEE standard 802.15.4 (ISO OSI layers 1 and 2), the ZigBee standard (layers 3 and 7), and end user products.

IV. Hardware

A WSN node consists of the sensor proper supplemented by the processor and communication hardware. The latter is often called *mote* as a reminder to the original miniaturization vision and at least comprises a radio transceiver, a microcontroller, and memory. Quite often, the open-source operating system TinyOS is used. Some of the commercially available motes and corresponding development kits are:

- MICAz by Crossbow (for ZigBee);
- eZ430-RF2500 by Texas Instruments (for ZigBee and SimpliciTI);
- XBee-PRO ZNet 2.5 by Digi International, based on a ZigBee transceiver by Ember and featuring a line-of-sight range of 1.6 km at a data rate of 1200 bit/s (for ZigBee);
- Lime CM09 by GreenPeak, based on the Emerald GP500XC chipset (for ZigBee or GreenPeak);
- nanoNET Atmega DK by Nanotron (for NanoNET).

These and similar products enable one to become familiar with WSNs and gain quick experimental insight into their characteristics.

V. Coexistence

No one frequency band is exclusively reserved for WSNs. In particular, the globally available ISM frequency band at 2.45 GHz (intended for the unlicensed operation of industrial, scientific, or medical equipment) is crowded with WLAN, WSNs, and proprietary systems, which therefore interfere with each other. This makes it important to characterize the ability of a network to coexist with other networks and to quantify the quality-of-service restrictions in a network brought about by the existence of interfering sources [17, 18]. Figs. 5 and 6 show the results of such a characterization for a NanoNET communication channel.

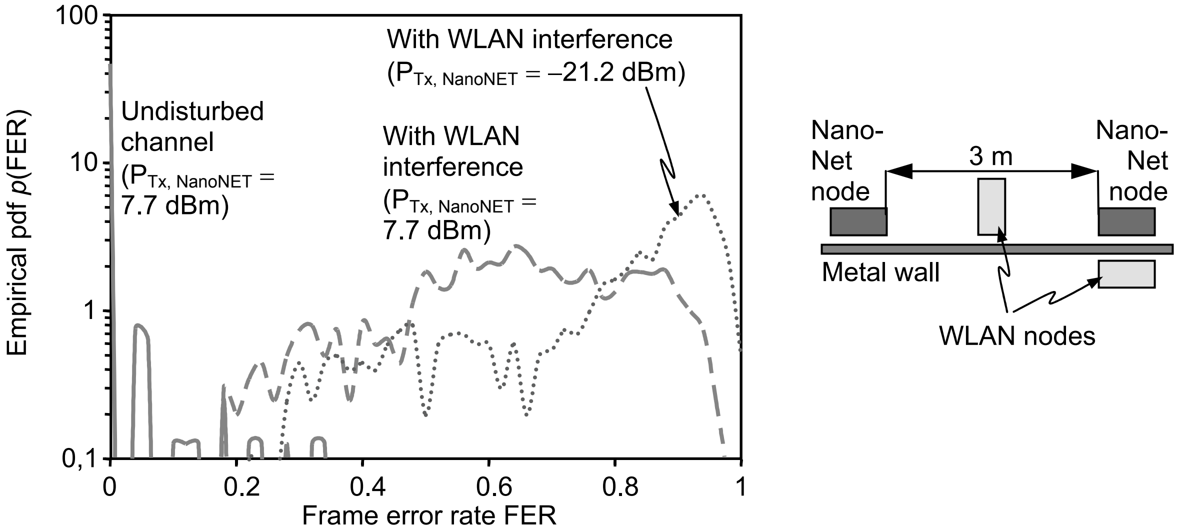

Figure 5. Measured probability density function of the frame error rate on a NanoNET communication channel.

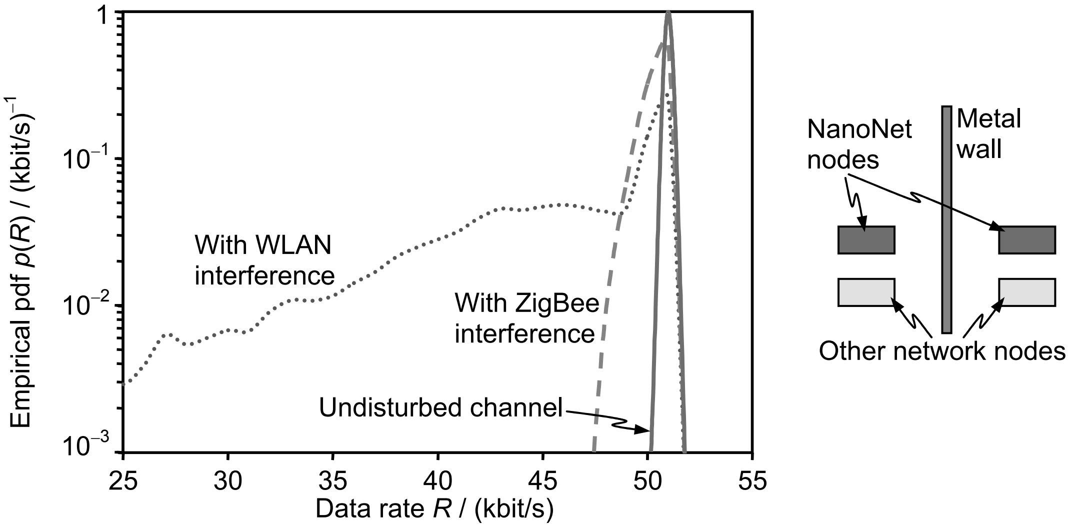

Figure 6. Measured probability density function of the data rate on a NanoNET communication channel.

The frame error rate (FER) in a WSN of course depends on the signal-to-noise ratio. It increases with the ratio of the interfering RF power to the Tx power of the disturbed network. For instance, the analysis of the probability density functions (pdf) shown in Fig. 5 reveals that the expected FER increases from 0.68 % (undisturbed NanoNET channel) to 61.1 % (NanoNET with Tx power of 7.7 dBm disturbed by WLAN) and even 80.3 % (NanoNET with Tx power of −21 dBm disturbed by WLAN). Similar comments apply to the effective data rate: it is lower for higher interfering RF power. The experimental results plotted in Fig. 6 are described by expected values for the data rate of 51.0 kbit/s (undisturbed NanoNET channel), 50.5 kbit/s (NanoNET disturbed by ZigBee), and 44.7 kbit/s (NanoNET disturbed bei WLAN).

As the measurement results in a network depend heavily on the actual situation (network layout, vicinity of interfering networks, multipath propagation, fading, etc.), the design of a WSN involves the solution to application-specific problems. Measurements in typical networks show that a suitable choice of parameters can help to tune selected network characteristics such as the energy efficiency (see, e. g., [18]). Also, the ability of a network to coexist with others may be strengthened by increased Tx power, special coding schemes, or antenna directivity (space diversity).

VI. Conclusion

The currently available commercial hardware, software, and network technologies are a sound basis for the implementation of WSNs. There already exist products, mainly for building automation. Nevertheless, the state of the art must be improved when it comes to the cost, size, and energy autarky of sensor nodes if many nodes are to be deployed to “make the environment intelligent”. Our knowledge about WSNs is currently expanding by practical experience, which, together with the convergence to the de-facto standard IEEE 802.15.4, will lead to higher volumes and lower cost.

References

[1] E. Callaway, Jr., *Wireless Sensor Networks.* Boca Raton: Auerbach 2004. — C. Raghavendra et al., *Wireless Sensor Networks*. New York: Springer, 2004. — N. Bulusu, S. Jha, *Wireless Sensor Networks*. Boston: Artech House, 2005. — R. Shorey et al., *Mobile, Wireless, and Sensor Networks*. Hoboken: Wiley 2006. — B. Otis, J. Rabaey, *Ultra-Low Power Wireless Technologies for Sensor Networks*. New York: Springer, 2007. — P. Baronti et al., “Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards,” *Computer Communications*, Vol. 30, No. 7, pp. 1655–1695, 2007. — J. Sammarco et al., “Information Circular 9496,“ *DHHS (NIOSH) Publ. No. 2007-114*, Apr. 2007.

[2] G. Fischerauer, “Funksensornetzwerke”, *Proc. Dresdner Sensorsymposium*, Dresden, pp. 65–73, Dec. 10–12, 2007

[3] J. Rabaey et al., “PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking,” *IEEE Computer*, Vol. 33, No. 7, pp. 42–48, July 2000

[4] S. Roundy, “Energy scavenging for wireless sensor nodes with a focus on vibration to electricity conversion,” *PhD thesis*, Univ. of California, Berkeley, May 2003

[5] R. K. Kotlanka et al., ”Inertial MEMS energy harvester using rotary comb,” *Proc. Eurosensors XXII*, Dresden, pp. 1412–1415, Sept. 8–10, 2008

[6] Ch. Lee et al., “Theoretical comparison of energy harvesting mechanisms based on electrostatic scheme,” *Ref. [5]*, pp. 1403–1407

[7] D. Spreemann et al., “Innovative ‘Energy Harvesting’ Prinzipien zur Wandlung von kinetischer Energie”, *4. GMM-Workshop Energieautarke Sensorik*, Karlsruhe, pp. 7–12, Sept. 14–15, 2006

[8] Th. Albach et al., „Entwurfskonzept und Realisierung eines autarken elektromechanischen Energiewandlers als Energiequelle für drahtlose Sensoranwendungen“, *Ref. [7]*, pp. 13–20

[9] S. L. Kok et al., “A novel piezoelectric thick-film free-standing cantilever energy harvester,” *Ref. [5]*, pp. 395–399

[10] S. Matova et al., “Modeling and validation of AlN energy harvesters,” *Ref. [5]*, pp. 1482–1485

[11] N. N., *IEEE Std 802.15.1-2005 […]*. New York: IEEE, June 2005.

[12] N. N., *ANSI/IEEE Std 802.11, 1999 Edition (R2003) […]*. [And:] *IEEE Std 802.11b-1999 (R2003) […]*. [And:] *IEEE Std 802.11g-2003 […]*. New York: IEEE, June 2003.

[13] N. N., *IEEE Std 802.15.4-2006 […]*. New York: IEEE, Sept. 2006.

[14] N. N., *ZigBee Specification* (ZigBee Document 053474r13). [And:] *ZigBee-PRO Stack Profile* (ZigBee Document 074855r05). San Ramon: ZigBee Alliance, Dec. 2006; Jan. 2008.

[15] N. N., *nanoNET Chirp Based Wireless Networks. V. 1.04*. Berlin: Nanotron Tech., Feb. 20, 2007.

[16] N. N., *White Paper : Why Wireless HART?* Austin: HART Foundation, Oct. 2007.

[17] N. N., *Koexistenz von Funksystemen in der Automatisierungstechnik*. Frankfurt: ZVEI, Nov. 2008.

[18] R. Stöber, G. Fischerauer, “Interaction of WLAN and NanoNET sensor networks,” *Ref. [5]*, pp. 1540–1543