Untethered Health - Radio Technologies in a Health Monitoring Context

Dipl.-Inform. Kirsten Terfloth, Prof. Dr.-Ing. Jochen Schiller
Institute of Mathematics and Computer Science, Freie Universität Berlin, Germany

Abstract

Within the past decade, wireless technologies have become a crucial part of our day to day life, generally allowing us to overcome inconveniences caused by spatial dependencies of services or devices. Especially in the domain of health monitoring, patient supervision and care for the elderly the possibility to physically decouple health parameter acquisition from data analysis by substituting wires with wireless links has a great impact on the quality of life of patients.
This paper targets to supply an overview of available wireless technologies that may be used in a health monitoring context. Since this domain includes a rich set of different applications, essential parameters shared by a majority of current or envisioned applications are pinpointed and used as a basis for an evaluation of the decision on the usage of a particular wireless standard.

1 Introduction

Wireless communication in combination with the ability to build small, portable but powerful devices opened up a magnitude of possible application domains. Handheld computers, mobile phones or car navigation systems nowadays commonly integrated in our everyday life are only the tip of the iceberg of technological solutions currently in progress or yet to come.
A very promising area where the benefits of replacing unwieldy wires by communication over wireless channels has a great impact on the actual freedom of users is the domain of personal health monitoring. Parameters that indicate the state of health of a person may be measured by various sensors attached either directly to the skin or integrated into personal objects that are worn close to the body such as watches or clothes. The obtained data can then be processed locally in case the embedded hardware allows for the requested operations or send to a central processing unit. Wireless communication can literally untie a patient from a monitoring entity, which is especially valuable in case the supervision has to take place for a longer period of time.
From a technological point of view, one necessary choice is to decide which wireless technology to use for communication. A plethora of wireless standards and therefore radio transceivers is available or currently under review to enable data transmission via wireless links, each of them initially designed with different application areas in mind. Therefore, characteristic attributes such as e.g. data rates and transmission ranges should be carefully evaluated before the actual implementation of a new system. To ease this evaluation process this paper surveys the wireless standards most commonly used in this context and points out the relevant parameters that should be included in an evaluation process.

2 Personal Health Monitoring

A tremendous amount of research and industrial effort has been put into supporting medical applications with new communication primitives and technological improvements. Dependent on scale, scope and field of application, this intersection area of medicine and telematics is referred to using terms such as eHealth [2], which denotes the usage of Internet-related technologies with health services, or telemedicine [3][4], which is concerned with any clinical patient/doctor interaction on a remote basis. Personal health monitoring, hence monitoring multiple physiological signals of a person by means of different sensors, is an area that greatly benefits from current technological advancements: miniaturization of sensors and radio chips and their integration into wearable accessories and textiles [5] allow to literally untether patients from formerly wired solutions, thus opened up a new domain of intersection.
Prominent vital parameters that are monitored include ECG data, blood pressure and body temperature or motion. This data can be used to be able to react immediately to life-threatening conditions of a person or to aggregate data over time for later analysis. Systems build to achieve such monitoring consist of application specific sensors, placed on or near the patients' body and radio transceivers to transmit sampled data. Usually, data is sent for further processing or forwarding to a central unit which is situated in the vicinity of the patient.

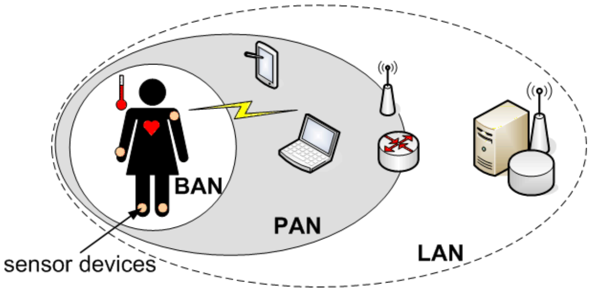

Figure 1: Scope of Network Technologies

This paper will focus on radio technologies that operate in a BAN (body area network) or WPAN (wireless personal area network) context, see Figure 1. For additional forwarding, e.g. to a remote site for medical evaluation or to a patient database for persistent storage, a hierarchical model including a gateway node is usually applied [6] [7]. This way, the according radio technologies are decoupled, and BAN/WPAN communication may rely on standards that target intrinsic requirements of the health monitoring domain.

Demands that have to be met on the networking side are a low energy consumption scheme of transceivers to guarantee user comfort, support for patient mobility and security mechanisms, a low complexity in terms of software stack and protocol overhead and a flexible network organization scheme. Since data samples taken from sensors are rather small, supported data rates may be low. A higher transmission range allows for more flexible placement of gateway devices but comes at the price of higher energy expenses, a trade-off that has to be evaluated in the application context. The application that will be used as an exemplary scenario for evaluation involves multiple, mobile patients, each equipped with body sensors whose values are transmitted to a central entity for monitoring.

3 Wireless Standards

3.1 Bluetooth

Bluetooth [8], as specified in the industrial specification IEEE 802.15.1, is a standard targeting short range radio communication for personal area networks (PANs). It has been introduced in the 1990's primarily to interconnect devices such as cell phones, PDAs, Laptops, workstations and peripheral devices, overcoming the line-of-sight requirement and point-to-point connectivity of Infrared that has been widely adopted in this domain beforehand.

Bluetooth has been designed to provide a low-cost, low-power solution for ad-hoc radio connectivity working in the license-free frequency band at 2.4GHz. While traditionally 802.x standards provide a specification only for the lower layers (physical and data link), Bluetooth has been designed from a more holistic viewpoint, thus covers specifications from physical to application layer. Since the development of Bluetooth has been driven by the usage in different application scenarios, e.g. to connect a PDA to a laptop or to use a headset with a specific cell phone, the specification of so called profiles reflects this approach. A profile defines a set of parameters to be used with a protocol, thus provides application-specific tuning of the hardware.

To avoid interference with other technologies that also rely on the 2.4 GHz frequency band (such as WLAN), Bluetooth divides the band into 79 channels with each being 1 MHz wide. Frequency hopping in combination with a time division duplex MAC scheme add to the robustness of the data transmission. Different modulation schemata, varying in the Bluetooth specifications, yield different data rates: A binary frequency modulation that provides a theoretical data rate of 1 MBit/s as specified in Blutooth Specification 1.1 [9], which is commonly considered as the basic rate, has to be implemented by all bluetooth devices for compatibility reasons. Bluetooth Specification 2.0 + EDR, which stands for Enhanced Data Rate, proposes two other modulation schemes, a quarternary phase modulation providing an upper bound for a data rate of 2 MBit/s and a phase modulation resulting in a data rate of 3 MBit/s. The obtainable data rates in practise differ depending on the chosen data link. Bluetooth offers a synchronous, circuit-switched connection (SCO) used voice between two devices. The asynchronous counterpart (ACL) provides a connectionless link between participants. This packet-switched data link protocol achieves 723 kBit/s for asymmetric communication in one direction, and 58kBit/s in the other or 434 kBit/s in a symmetric setting. These values may be tripled with the help of EDR.

The transmission range of Bluetooth chips highly depends on antenna characteristics and maximal permitted power. Class 3 devices, equipped with chips allowing for a maximal transmission power of 100 mW have an approximate range of up to 100 m. More commonly spread are chips of Class 2 with a transmission range of up to 10 m with an energy consumption of 2.5 mW or Class 1 at 1 m using 1 mW since Bluetooth devices most often operate on batteries.

Any Bluetooth device can send an inquiry to find other devices in its range and initiate a connection, and will then automatically become the master node of the piconet. A 48-Bit address, the bluetooth device Address, serves to uniquely identify a device, thus after the inquiry, all addresses of surrounding devices that are activated for communication configured as discoverable are obtained. A so called paging request send by the master will then establish either a unicast or a multicast connection. Up to 7 slaves can communicate with the master node at the same time simply by following his channel hopping sequence, while 255 devices can inactively participate in a piconetwork. Multiple piconets can be interconnected to form a scatterweb, a network topology that features several masters.

Eavesdropping or man-in-the-middle attacks are typical attacks that wireless links are exposed to. The Bluetooth Specification has defined several security mechanisms to defeat these vulnerabilities, all of which are based on cryptographic methods using Link Keys [10]. Upon the first connection of two Bluetooth devices (pairing), this key is generated using their unique addresses in combination with a pseudo-random number, a PIN, which is either provided by the device itself, or the user, and a cryptographic function. Both, authorization and encryption of data between two devices will afterwards depend on the generated link key. The decision whether to enable encryption can be configured via the profile a bluetooth device is chosen to use, and therefore is integrated into the bluetooth stack.

3.2 Ultra Wideband (UWB)

According to the Federal Communications Commision (FCC) radio technologies that either utilize a frequency spectrum of over 500 MHz or whose bandwidth exceed 20 % of the arithmetic centre frequency are called ultra-wideband [11]. Instead of modulating the data to be transmitted between devices onto a carrier frequency, data will be encoded via pulses over a larger frequency band. These pulses have to be very narrow to prevent other radio technologies already authorized to use a frequency band from being harmfully disturbed.

Due to strict regulations in terms of maximal permitted transmission power and covered frequency bands, Ultra-Wideband is dedicated to small communication ranges but at the same time enables high data rates. Currently, the commercial use of UWB is not possible since it is not yet fully approved in Europe. Nevertheless, there is a strong indication that it will be approved in the near future, as license-free usage is already permitted in the USA.

Pulse radio techniques such as UWB have the main advantage that they are able to share a spectrum already assigned to other technologies without imposing significant interference as long as this additional noise is strictly regulated. Throughout the following only the proposed technical standards by the FCC for communication and measurement systems will be discussed although two other classes of devices are available. The FCC is requiring that –10 dB bandwidth of indoor UWB systems must be between 3.1 GHz and 10.6 GHz for data communication. Furthermore, harmful interference with other technologies is avoided by restricting the transmission emission, called the EIRP to -41.3 dBm/MHz (equivalent to 0,56 mW transmission power) for in- and outdoor usage. Due to this very low transmission power setting it is not possible to obtain high data rates and a large transmission range at the same time. UWB provides a very high bandwidth which is especially preferable for devices running on batteries, since high data rates may be achieved with low costs in terms of energy. In practise, current chips can supply data rates of 480 MBit/s, targeting a rate of 2 Ghz in the future.

The technical development of Ultra-Wideband is split into two competing technologies, Direct Sequence UWB (DS-UWB) and the Multiband OFDM (MB-OFDM). The Task Group IEEE 802.15.3a discussed both alternatives but did not agree on a single standard but instead stopped its work. Both technologies are currently implemented in parallel and supported by different industrial partners.

While the data rate is extremely high, the transmission range for UWB devices is with a maximum of 10m relatively small. This can be accounted to the fact that the energy of the signal is very low to not interfere with other technologies transmitting on a given frequency, thus the farther devices are apart, the more erroneous the reception of a data stream will be. The future application domain of UWB can therefore be anticipated to centre around Personal Area Networks, e.g. to substitute wired USB connections.

The proposal of the IEEE 802.15.3a task group does not specify anything beyond the physical layer for DS-UWB, thus medium access schemes and higher layer issues have not been discussed. The ECMA-368 (European Association for Standardizing Information and Communication Systems) specifies a distributed medium access control (MAC) sublayer and a physical layer (PHY) in the spirit of MB-OFDM. Though this standard exists, it does not cover any regulatory requirements of any country or region. Without going into too much detail, the standard provides two medium access schemes, a distributed, reservation-based and a prioritized, contention-based channel access mechanism and specifies further duties of the second layer, e.g. a synchronization facility for coordinated applications and a mechanism for measuring distances between devices. No requirements and services for upper layers are specified.

Security mechanisms are speccified in the ECMA standard for MB-OFDM, all of them relying on a symmetric, secret key, the Pairwise Master Key (PKM). Temporary keys for point-to-point as well as for multicast connections will be generated relying on this key and a 4-way handshake, and may afterwards be used to encrypt transmitted data via the Advanced Encryption Standard (AES). The exchange or creation of the PKM is not denoted by the standard.

3.3 Zigbee

The IEEE technical standard 802.15.4 specifies the lower two layers of Zigbee [12], a standard especially designed for a low data rate with multi-month to multi-year battery life and very low complexity. Application areas are envisioned to be Wireless Personal Area Network such as sensor networks, interactive toys, remote controls, and home automation. Zigbee has been approved in May 2003 and officially published in October the same year, with the Zigbee Alliance, a consortium of manufacturers, distributors and users providing a specification for the upper layers.

Generally, Zigbee is specified to be used in the industrial, scientific and medical bands (ISM), which has the advantage that no licensing is necessary for its usage. Three frequency bands are therefore denoted: While the 2.4 GHz band allows for world-wide service, Zigbee may also be used in the 868 MHz band in Europe or in the 902 MHz to 928 MHz band in the US. On the downside, Zigbee and IEEE 802.11 or Bluetooth are prone to interfering with one another [12], a problem that has to be tackled on the medium access layer.

Using Zigbee in the 2.4 GHz domain yields a data rate of 250 kBit/s. In Europe, a BPSK modulation scheme at 868 MHz is capable of supplying 20 kBit/s, whilst American Zigbee devices will provide 40 kBit/s. Before transmission, data will be spread with the help of the DSSS approach.

As stated above, the IEEE 802.15.4 standard has been proposed for Personal Area Networks which commonly feature battery powered devices. The expected transmission power is therefore set from 0,5 mW up to 10 mW, which in return will result in an operational range of 10 m to 70 m under optimal conditions.

To organize the access to the medium and to be able to integrate devices of different complexity according to their capabilities, the IEEE 802.15.4 standard differentiates two classes of devices, Full Functional Devices (FDD) that implement all functionalities needed for setting up a WPAN and Reduced Functional Devices (RDD) that are only able to communicate directly with a FDD. One dedicated FDD device in a Zigbee network has to take the role of the PAN coordinator, a task assigned to the first FDD becoming active. The coordinator is in charge of keeping track of devices registered to the WPAN, regulating the medium access and maintaining its identification. Beacon frames are sent out by all coordinators and the PAN coordinator itself with this WPAN identification on a regular basis. The time between receptions of two beacons is divided into two phases, each of which allows for a different medium access mechanism. In the first phase, the medium access scheme is CSMA/CA, thus access is based on competition. The second, optional interval can be used for guaranteed time slots. Their assignment to eligible users will be posted by the PAN coordinator in its beacon packets.

A node can participate in a Zigbee network as a Zigbee Coordinator, or as a Zigbee Router, which provides routing of packets between nodes and is equivalent to a coordinator on the second layer, or as a simple Zigbee End Device. While a Zigbee network has no predefined topology, thus may take the form of a tree, a star or a mesh with redundant links, in case of mobility no end-to-end connectivity will be guaranteed by the protocol. The IEEE 802.15.4 standard clearly targets static networks as can be found in home automation or manufacturing.

The Zigbee standard provides methods for the exchange of keys and for data encryption and decryption of messages on the different layers of the stack. Zigbee devices rely on 128 Bit symmetrical Link Keys for unicast and a Network Key for broadcast messages, which has to be known to all devices. The link key can either be derived this from a Master Key, or is distributed via the network as can be the network key. For key distribution, Zigbee defines a Trust Centre that resides at the PAN Coordinator.

Tabelle 1: Comparison of Bluetooth, UWB and Zigbee

	Bluetooth	UWB	Zigbee
Energy Consumption	2,5 – 100 mW	0,5 mW	0,5 mW
Frequency Band	2,4 GHz	3,1 – 10,6 GHz	868 MHz /902-928 MHz, 2,4 GHz
Transmission Range	1 – 100 m	<. 10 m	10 – 70 m
Data Rates	high	very high	low
Network Topology	Master/Slave, Star	not specified	Star/Tree/Mesh
Security	Link keys, high overhead	Pairwise master key	Link/Network key
Complexity	high	medium	depends on device type
Mobility	not supported	not specified	partially possible

4 Evaluation

All wireless standards described above have been designed for BAN/WPAN applications, each of them with a different focus. To determine their applicability to a personal health monitoring system, we evaluated them based on quantitative and qualitative measures.

Although Bluetooth has been used previously in a health monitoring context [7], this wireless technology is the least favourable for the simple reason that it is overly complex for the target application domain. Bluetooth devices have to be able to serve both as a master and a slave, a fact that is reflected in a large protocol stack (250 kB in a standard implementation). The achievable high data rate Bluetooth devices are able to provide is not needed to forward data samples. High complexity is also observable when it comes to pairing of devices and secure data transmission due to the necessity to store link keys. Furthermore, the network size is restricted to eight active participants, mobility of participants is not explicitly supported by means of handover mechanisms or ad-hoc routing, so that the range of a piconet can be depicted as the effective range of a Bluetooth master device.

Utilization of UWB in future personal health monitoring systems, due to lack of regulation UWB is currently not an option, is not the best choice, either. The main reasons are that once again the high data rate provided will not be used, but comes at the cost of a very small transmission range. This constraint can be overcome by using additional devices to relay information, but will add unnecessary complexity to a system. Network or routing issues are neither part of the specification or a dedicated working group.

UWB has been designed to allow for transmission of multi-media data over a short distance, so that design rationals differ from demands of health monitoring systems.

Among all wireless technologies described in this paper, Zigbee is the most adequate choice. The general parameters such as low the data rate, the low energy consumption and the medium data transmission range conform to the application context. With its possibility to integrate different classes of devices, the devices operating in a personal health monitoring system can be clearly mapped accordingly.

However, user mobility and interference with other wireless protocols using the 2,4 Ghz domain are two major points of criticism: Although the availability of having a meshed network topology and a modified version of the AODV routing protocol allows for multi-hop routing, thus user mobility, this is only applicable for FDDs. Issuing route requests and route replies is restricted to routers and the PAN coordinator, a fact that is problematic since low-power modes are not defined for these devices in Zigbee v1.1.

5 Conclusion

In this paper, we briefly surveyed three wireless technologies and evaluated their applicability in a health monitoring context. In a target application involving embedded devices, user mobility as well as low data rates, it has been shown that Zigbee is the most applicable choice, but still lacks major features to sufficiently build the envisioned application. This gap motivates further developments that allow for mobility support and flexible usage in health monitoring.

6 Literatur

[1] Jovanov, E. et. al.: A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation, Journal of NeuroEngineering and Rehabilitation, March 1, 2005

[2] Eysenbach, G. What is E-Health? Editorial of the Journal of Medical Internet Research 2001.

[3] Wootton R. Telemedicine: A Cautious Welcome. *BMJ* 1996;313:1375-7

[4] Mair FS, Haycox A, May C, Williams T. A review of telemedicine cost-effectiveness studies. *J Telemed Telecare* 2000;6(suppl 1):S38-40

[5] J. Ottenbacher et. al., Integration of a bluetooth based ECG system into clothing, *Proceedings of ISWC'04*, Arlington, 2004, pp. 186–187.

[6] Homepage "Body Area Networks", Fraunhofer Gesellschaft, last accessd: 12.11.2007 http://www.ban.fraunhofer.de/index.html

[7] Homepage "Personal Health Monitoring", http://www.itiv.unikarlsruhe.de/opencms/opencms/de/research/projects/mst_pm/

[8] Core Specification of the Bluetooth System Specification. Availalble online at: http://ieee802.org/15/Bluetooth/index.html

[9] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), IEEE 802.15.1, Juni 2002.

[10] Bundesamt für Sicherheit in der Informationstechnik: Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte, 2006, http://www.bsi.de/literat/doc/drahtkom/index.htm

[11] New public safety applications and broadband Internet Access among uses envisioned by FCC Authorization of Ultra-Wideband-Technology, http://www.fcc.gov/Bureaus/Engineering_Technology/News_Releases/2002/nret0203.html,

[12] The Zigbee Specification. Available online at: http://www.zigbee.org/en/spec_download/zigbee_downloads.asp