Advances and Challenges of Wireless Body Area Networks for Healthcare Applications

Craig A. Chin*, Garth V. Crosby*, Tirthankar Ghosh*, Renita Murimi*, * *Member, IEEE*

***Abstract*—The term wireless body area network (WBAN) is used to describe a network of devices connected wirelessly for communication on, in and near the body. In this paper, we survey the current state of various aspects of WBAN technologies that are being used in healthcare applications. In particular, we examine the following areas: monitoring and sensing, power efficient protocols, system architectures, routing, and security. We conclude by discussing open research issues, their potential solutions and future trends.**

Keywords- Wireless body area network, body sensor network, healthcare, WBAN survey

I. Introduction

Rising healthcare costs and the increase in average life expectancy of individuals in many developed nations represent two of the primary motivating factors for innovation in health care. One such innovation is the continuous monitoring of patients via sensors connected as a WBAN. This will enable improved analysis and modification of treatment regimes, computer-assisted rehabilitation and early detection of life-threatening events. The likelihood of user acceptance of WBAN technologies has increased with advances in miniaturization of electronic devices, sensing, battery and wireless communication technologies. The key components of a WBAN are smart miniaturized devices (motes) that are able to sense, process and communicate. They are designed such that they can be worn or implanted, and are able to monitor and transmit physiological signals to specialized medical servers without much interference to the daily routine of the patient.

In section II we review monitoring and sensing devices used in WBANs. Section III presents an examination of power efficient protocols. In section IV we explore the WBAN system architectures. Approaches to routing in WBAN are presented in section V. In section VI we present various security techniques and protocols. We conclude in section VII with a discussion of open research problems and future trends.

II. Monitoring and sensing

In this section we describe two categories of sensors (*wearable* and *implantable*) that are used for monitoring and sensing in WBANs. Wearable sensors have been used to monitor several physiological parameters. A pulse oximeter is a medical device that indirectly measures the oxygen saturation levels (SpO_2) in an individual's blood as well as the changes in blood volume in the skin that coincide with the cardiac cycle. The quasi-periodic signal that is output is called a photoplethysmograph (PPG), and can be used to determine heart-rate. A wearable PPG biosensor in the form of a ring has been developed by Yang and Rhee [1].

A wearable ECG sensor for WBAN has been described in [2]. The electrocardiogram (ECG) is a waveform that represents the propagation of electric potentials through the heart muscle with respect to time. Therefore, the ECG waveform provides a non-invasive means for investigating heart function. Fulford-Jones *et. al.* designed an ECG sensor that is supported by a Mica2 mote hardware platform [2]. A network of wearable wireless blood pressure monitors has been studied in [3]. It has been observed that ambulatory blood pressure (BP) is more closely related to target organ damage and cardiovascular events than BP readings taken in a clinical environment [3]. This fact provides the motivation for the creation of wireless BP sensors. Poon et. al. have created a cuff-less BP watch sensor, based on the pulse transit time (PTT) method for measuring BP [4].

Wearable sensors have also been used for activity/motion detection. The level of activity or the nature of motion of an individual can be detected by a system that combines an accelerometer with a gyroscope. An example of an integrated accelerometer/gyroscope is presented in [5]. An EEG monitor as a wearable sensor has been described in [6]. Electroencephalography (EEG) is a representation of the electrical activity of the brain. Farshchi *et. al.* have introduced a wireless neural interface, using Mica2 and Mica2dot systems as the wireless sensor platforms, which is capable of acquiring two channels of EEG data [6].

Implantable sensors have been studied in [7]. In [7], implantable neural stimulators send electrical impulses into the brain or spinal cord for the treatment of Parkinson's disease, intractable epilepsy and chronic pain. An example of such a device is given in [7].

III. Power efficient protocols

Wireless body area sensor nodes, due to their size, use miniaturized batteries. Hence, WBANs must sense, process and communicate data in a power efficient manner in order to preserve battery life. Power efficiency is a key emphasis of design efforts for WBAN protocols. The majority of work in this area has been on developing energy-efficient medium access control (MAC) protocols. The main sources of energy waste in the design of a MAC protocol for a WBAN have been identified as collision, overhearing, control packet overhead, and idle listening [8]. Currently, there are two main schemes

978-1-4673-0009-4/12/$26.00 ©2012 IEEE

used for MAC protocols of sensor networks. Contention-based MAC protocols, such as carrier sense multiple access/collision avoidance (CSMA/CA), have their nodes contend for channel access prior to transmission. The advantages of these protocols are scalability, adaptability to network changes and no time synchronization constraint. In schedule-based MAC protocols, such as TDMA, access to the channel is divided into time slots that are of fixed or variable duration. Each node is assigned a time slot(s) by a controller, and it will only transmit within that time window. TDMA-based protocols eliminate collision, overhearing and idle listening, and are typically utilized in some form in energy-efficient MAC protocols.

It has been found that IEEE 802.15.4 does not meet all the energy efficiency requirements for WBAN applications [9]. It is because of these shortcomings that the IEEE 802.15 Task Group 6 (BAN) has begun developing a communication standard optimized for low power devices and operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics / personal entertainment and other [10].

In the absence of a standard, several energy efficient MAC protocols specifically designed for WBAN applications have been presented. An energy-efficient MAC protocol that uses clear channel assessment and collision avoidance with time division multiplexing (CCA/TDMA) is presented in [11]. Marinkovic et. al. [12] present an energy-efficient, low duty cycle MAC protocol based on TDMA. A novel TDMA-based protocol for BSNs, called H-MAC, is proposed in [13]. This protocol improves energy-efficiency by using the heartbeat rhythm to perform TDMA synchronization, avoiding energy consumption associated with transmitting time synchronization beacons. In [14] a TDMA-based MAC protocol called BodyMAC is proposed. Timmons et. al. [15] introduce an adaptive TDMA-based MAC protocol called MedMAC. MedMAC incorporates a novel adaptive TDMA synchronization mechanism in which only a multi-superframe beacon has to be listened to by the nodes. Otal and Alonso proposed an energy-saving MAC protocol, DQBAN (Distributed Queuing Body Area Network) for WBAN in [16]. The proposed DQBAN is a combination of a cross-layer fuzzy-logic scheduler and energy-aware radio-activation policies.

IV. System architectures

A. Network Architectures

The network architecture of WBANs can be broadly classified into two major categories: flat architectures and multi-tier architectures. Flat architectures comprise of a single data-gathering unit that sends its data to a personal computer or a personal server application running on a PDA. Multi-tier architectures are widely used to achieve large data gathering of multiple physiological signals using multiple nodes in the base tier, a gateway at the second tier that acts an interface between first tier and a server at the third tier.

The rest of this section focuses on various multi-level architectures with an emphasis on specific topologies for parameter optimization of security, energy efficiency and node locations.

Security-Centric Architectures

In [17], the authors have studied the design of WBAN architecture with an emphasis on security and cross-layer operation. The main components of the WBAN are the network of nodes, external networks and back-end server. Security is enforced during node initialization using a secure key which is generated by back-end servers uniquely for each node in each session. When a node leaves or rejoins the WBAN, it triggers a network topology update which generates a new key for each node. This ensures that nodes which leave the network cannot read/modify the patient data.

Energy Efficient Architectures

In [18], the authors described an energy efficient TDMA-based MAC protocol for a multi-tier architecture of a WBAN. The architecture consists of sensor nodes at the first tier, a set of master nodes that collect data from first tier nodes, and a monitoring station in the highest (third) tier that encompasses the monitoring and data access functionalities at the user level. By exploiting the features of a fairly stationary network of first tier nodes with fixed data collecting functions and smaller distances between the first tier nodes and second tier master nodes, the authors develop a MAC protocol that is energy efficient.

In [19], the authors presented a WBAN that measures stress through the heart-rate variability parameter. The BAN is organized as a network of (**W**ireless **I**ntelligent **Se**nsor) WISE sensors (clients) that connect to a personal server (PS). In order to reduce the power consumption of the wireless transceiver on the PS the authors introduce the concept of a mobile gateway (MOGUL) that establishes wireless communication with the PS and downloads data. Energy efficiency is implemented using energy efficient communication protocols and low-energy radio layer 900 MHz RF modules. Increased on-board data processing at sensor nodes reduces the size of the transmitted packets to the PS. The system architecture is a master-slave architecture, where the MOGUL acts as the master and downloads data from WISE sensors when it is in within its communication range. The architecture allows for multiple sessions of communication with WISE sensors. All data obtained from these sensors is aggregated in a central device that is connected to the multiple mobile gateways generating these sessions.

Node Locations

WBAN architectures can be wearable or implanted on/within the human body. Capsule endoscopy discussed in [20] is an example of implantable WBAN architecture. Most of the WBAN architectures and applications discussed in this section are wearable architectures. An additional example is [21]. Here, the authors described wearable WBAN (WWBAN) for health monitoring. The proposed WWBAN architecture is a multi-tier architecture, where the first tier comprises of sensors, the second tier is an application-specific layer (e.g. a personal server (PS) running on a PDA) and the third tier includes data accessibility through servers connected to the Internet.

V.Routing

A. Routing Protocols

The principal characteristics of a Wireless Body Area Network (WBAN) that necessitate the design of a routing protocol are frequent network partitioning due to postural mobility of the on-body sensors, high propagation loss across the human body, low transmission power of the sensors, and low reliability of end-to-end path from source to sink.

Traditionally, there have been two approaches to routing in BANs. One approach is to integrate the routing functions with the MAC layer, with a fundamentally cross-layer approach. The other is to design a routing layer on top of the MAC layer, where link qualities are measured based on selected parameters, and taken into path computation.

The first approach has been studied and was proposed in [22, 23]. The authors in [23] have proposed a cross-layer CICADA protocol that sets up a spanning tree and uses time slots for controlling each node's transmission and reception cycles. The protocol lacks an approach to define link metrics and use those metrics for finding effective multihop routes. This can be a compelling argument for necessitating a separate routing layer on top of MAC that would provide the basis for computing efficient multihop paths based on link quality metrics.

The second approach has been investigated in [24], where the authors have proposed a probabilistic packet routing protocol, Probabilistic Routing with Postural Link Cost (PRPLC), using a stochastic link cost. The proposed protocol, based on postural link cost formulation, uses time-varying costs formulated for each link based on the locality in the connectivity patterns of the links. The protocol uses postural link costs to compute probabilistic forwarding of data packets. The authors have reported a significantly low end-to-end packet delay using PRPLC, as the protocol can successfully capture the locality in postural movements.

VI.Security

A. Security Requirements of WBAN

The WBAN and supporting infrastructure must implement security operations that guarantee the security, data integrity, privacy and confidentiality of the patients' medical records. In addressing privacy issues it must be ensured that the Health Insurance Portability and Accountability Act of 1996 [25] is observed. The following security requirements must be attained: authentication, data integrity, confidentiality, availability, and privacy.

B. Proposed Security Solutions

TinySec

TinySec is proposed in [26] as a security solution in biomedical sensor network to achieve link-layer encryption and data authentication. TinySec [27] is a software based security architecture that implements link-layer encryption.

IEEE 802.15.4 Security

Several security suites can be implemented under the IEEE 802.15.4. The IEEE 802.15.4 security suite modes can be classified into two basic modes: unsecured mode and the secured mode. The unsecure mode simply means no security suite has been selected. The standard defines 8 distinct security suites.

ZigBee Security Services

ZigBee is a consortium of industry players which came together to define a new standard for ultra-low power wireless communication [28]. The ZigBee network layer (NWK) is designed to operate on top of the IEEE 802.15.4 defined PHY and MAC layers. The ZigBee standard defines extra security services including processes for key exchange and authentication, in addition to the security services of IEEE 802.15.4, upon which it is built.

Hardware Encryption

Instead of using software encryption as done in TinySec, hardware encryption can be implemented utilizing the ChipCon 2420 ZigBee compliant RF Transceiver. The CC2420 is able to execute IEEE 802.15.4 security operations with AES encryption using 128-bit keys. These operations include the counter (CTR) mode encryption and decryption, CBC-MAC authentication and CCM encryption plus authentication. Hardware encryption has been implemented in a WBAN project with off-the-shelf ZigBee platform [29]. The drawback of this method is that it is dependent on the specific sensor platform. Not all sensor node hardware offers hardware encryption support.

Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) has emerged as a viable option for public key cryptography in wireless sensor networks. The main reason for this is its comparatively fast computation, small key size and compact signatures. There has been several noteworthy contributions in the past few years [30, 31].

Although ECC has been successfully implemented in several variations it is still not a top choice for WBAN. This is because its energy requirements are still significantly higher than symmetric systems. This being the case, others have proposed that ECC be implemented only for infrequent and security-sensitive operations such as key establishment during the initial setup of the network or code updates. In line with this thinking, Malasri *et al.* [32] proposed a solution for medical sensor networks that uses: (i) an ECC-based secure key exchange protocol to set up shared keys between sensor nodes and base stations, (ii) symmetric encryption and decryption for protecting data confidentiality and integrity, and (iii) an authentication scheme for verifying data source.

Identity-Based Encryption

Oliveira *et al.*[33] proposed TinyTate, a lightweight Identity-Based Encryption (IBE) security solution for traditional wireless sensor networks. Tan *et al* [34] proposed an Identity-Based cryptographic security solution for WBAN. In their work, the sensor nodes compute public keys by applying a hash function on an arbitrary number of application dependent self-generated keys. These keys are stored on their flash memory and are used to execute elliptic curve encryption/decryption using Elliptic Curve Digital Signature Algorithm (ECDSA).

Biometrics

Biometrics has emerged as a useful mechanism to use in the key establishment and authentication of body sensor nodes [35, 36]. This method uses measurement of physiological characteristics of the body itself as an important parameter in a symmetric key management system.

VII.Discussion: open research problems

In this section, we provide an overview of open research problems in WBANs and suggest some potential solutions.

Extended Power Supply Lifetimes

Micro-fuel cells provide high energy efficiency and density and refueling simply requires a cartridge replacement. These characteristics make fuel cells attractive for portable applications such as WBANs [37]. Energy scavenging of solar, heat or vibration from the ambient environment also has the potential to extend the life of the power supply. A self-powered wireless sensor node that is powered solely by human body heat was designed in [38].

Low Power Consumption

The majority of the power consumption budget is dedicated to wireless communication. Possibilities for reducing communication-based power consumption are the use of ultra wideband (UWB) transceivers, because of the high data rates and low power consumption they provide [39]. Use of energy-efficient data compression algorithms [40] to reduce the number of bits that would need to be transmitted by the transceiver.

Biocompatibility

In the context of implantable sensors, biocompatibility encompasses the reactions the sensor undergoes once being placed within the body (sensocompatibility) and the reaction the body experiences in response to the sensor. One aspect of a sensor's reaction to being placed within the body is called biofouling, which refers to the accumulation of proteins, cells and other unwanted biomaterials on a surface. Biofouling of the active surface of an implantable sensor will result in a fall in the sensor current and may eventually result in sensor failure. Nine sensor modifications to mitigate the effects of biofouling are presented in [41]. The body's reaction to an implantable sensor involves two factors: mechanical and chemical disruption [42]. Mechanical disruption may involve tissue distortion and occlusion of blood vessels. To minimize tissue damage, it is recommended that the sensor be blunt and rounded instead of sharp [42].

Unobtrusiveness

The largest component of a sensor in terms of size and weight is usually the battery. Therefore, methods that may result in the reduction in battery size, such as the adoption of fuel cell technology, have the potential to make wireless sensors less obtrusive [42]. Also, the utilization of ASIC technology will produce greater levels of integration than would be obtained by adapting commercial off-the-shelf (COTS) motes to a specific sensor application, and this would result in a reduction in sensor size.

Optimization of network resources

A key concern is the development of network protocols that use ultra-low radio power levels for transmission and reception that are safe for human use. With increasing number of WBANs, the radio layers used by the 802.15.4 networking standard need to be optimized to increase the throughput and minimize interference between multiple networks and users of the frequency bands.

Security

As computing and technology inches closer to the human body, it is important to protect the privacy of the data collected and disseminated by these networks. Complex security mechanisms require more computational and power resources, and optimizing the tradeoff between these is crucial for the widespread use of WBANs.

Preventative Healthcare

Present WBAN technology is mostly developed on-demand; WBANs are developed in response to specific physiological requirements. Using dynamic programming environments and cognitive interfaces, we should be able to measure multiple parameters in the human body and use this data to aid in preventive medicine and diagnosis.

Computational and Economic Perspective

Since WBANs comprise of networks of sensors performing specialized detection of physiological data, the cost and size of these devices impose limitations on their use. Creating networks that seamlessly interface with the human environment will be an interesting area of research.

Routing

The main challenges in designing any efficient routing protocol would be to address network partitioning with postural mobility, the design an energy-constrained protocol, and to ensure end-to-end path reliability.

References

[1] B. H. Yang and S. Rhee, "Development of the ring sensor for healthcare automation," *Robotics and Autonomus Systems,* vol. 30, pp. 273-281, 2000.

[2] T. R. F. Fulford-Jones, *et al.*, "A Portable, Low-Power, Wireless Two-Lead EKG System," in *26th Annual International Conference of the IEEE EMBS* San Francisco, CA, USA, 2004, pp. 2141-2144.

[3] K. Kario, *et al.* (2003) Ambulatory Blood Pressure Monitoring for Cardiovascular Medicine. *IEEE Engineering in Medicine and Biology Magazine*. 81-88.

[4] C. C. Y. Poon, *et al.*, "M-Health: The Development of Cuff-less and Wearable Blood Pressure Meters for Use in Body Sensor Networks," in *Proceedings of IEEE/NLM Life Science Systems and Applications Workshop*, 2006.

[5] V. Shnayder, *et al.*, "Sensor Networks for Medical Care," Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University, 2005.

[6] S. Farshchi, *et al.*, "A TinyOS-Based Wireless Neural Interface," in *Proceedings of the 26th Annual International Conference of the IEEE EMBS*, 2004.

[7] M. Ghovanloo, *et al.*, "A BiCMOS Wireless Interface Chip for Micromachined Stimulating Microprobes," in *Proceedings of IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology*, 2002, pp. 277–282.

[8] S. Ullah, *et al.*, "A Study of MAC Protocols for WBANs," *Sensors* vol. 10, pp. 128-145, 2009.

[9] D. Cavalcanti, *et al.*, "Performance Analysis of 802.15.4 and 802.11e for Body Sensor Network Applications," in *4th International Workshop on Wearable and Implantable Body Sensor Networks* Aachen, Germany, 2007.

[10] *IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks*. Available: http://www.ieee802.org/15/pub/TG6.html

[11] O. Omeni, *et al.*, "Energy Efficient Medium Access Protocol for Wireless Medical Body Area Sensor Networks " *IEEE Transactions on Biomedical Circuits and Systems,* vol. 2, December 2008.

[12] S. J. Marinkovic, *et al.*, "Energy-Efficient Low Duty Cycle MAC Protocol for Wireless Body Area Networks," *IEEE Transactions on Information Technology in Biomedicine,* vol. 13, November 2009.

[13] H. Li and J. Tan, "Heartbeat-Driven Medium-Access Control for Body Sensor Networks," *IEEE Transactions on Information Technology in Biomedicine,* vol. 14, January 2010.

[14] G. Fang and E. Dutkiewicz, "BodyMAC: Energy efficient TDMA-based MAC protocol for Wireless Body Area Networks," in *9th International Symposium on Communications and Information Technology (ISCIT 2009)*, 2009, pp. 1455-1459.

[15] N. F. Timmons and W. G. Scanlon, "An Adaptive Energy Efficient MAC Protocol for the Medical Body Area Network," in *1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace(Wireless VITAE2009)* Aalborg, Denmark, 2009, pp. 587-593.

[16] B. Otal and L. Alonso, "Highly Reliable Energy-Saving MAC for Wireless Body Sensor Networks in Healthcare Systems," *IEEE Journal on Selected Areas in Communications,* vol. 24, pp. 553-565, May 2009.

[17] D. Singelée, *et al.*, "A Secure Cross-Layer Protocol for Multi-hop Wireless Body Area Networks," in *7th international Conference on Ad-Hoc, Mobile and Wireless Networks*. vol. 5198, ed Berlin: Springer-Verlag, 2008, pp. 94-107.

[18] S. Marinkovic, *et al.*, "Energy-Efficient TDMA-Based MAC Protocol for Wireless Body Area Networks," in *Third International Conference on Sensor Technologies and Applications*, 2009, pp. 604-610.

[19] E. Jovanov, *et al.*, "Stress Monitoring Using a Distributed Wireless Intelligent Sensor System," in *IEEE Engineering in Medicine and Biology Magazine*, May/June 2003, pp. 49-55.

[20] R. C. Santiago, *et al.*, "Architecture of an Ultra Wideband Wireless Body Area Network for Medical Applications," in *IEEE 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, 2009, pp. 1-6.

[21] A. Milenkovi, *et al.*, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Computer Communications,* vol. 29, pp. 2521-2533, 2006.

[22] B. Braem, *et al.*, "The Wireless Autonomous Spanning Tree Protocol for Multihop Wireless Body Area Networks," in *3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops*, San Jose, CA, USA, 2006, pp. 1-8.

[23] B. Latré, *et al.*, "A Low Delay Protocol for Multihop Wireless Body Area Networks," in *the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MobiQuitous)*, 2007, pp. 1-8.

[24] M. Quwaider and S. Biswas, "Probabilistic Routing in On-Body Sensor Networks with Postural Disconnections," in *7th ACM International Symposium on Mobility Management and Wireless Access*, Tenerife, Canary Islands, Spain, 2009, pp. 149-158.

[25] "The Health Insurance Portability and Accountability Act of 1996 (HIPAA)," ed: Centers for Medicare and Medicaid Services, 1996.

[26] S. S. Marci, *et al.*, "Security and Privacy Issues with Health Care Information Technology," in *28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS 06)*, New York City, NY, USA, 2006, pp. 5453-5458.

[27] C. Karlof, *et al.*, "TinySec:A Link Layer Security Architecture for Wireless Sensor Networks," in *Second ACM Conference on Embedded Networked Sensor Systems (SenSys '04)*, Baltimore, Maryland, USA, 2004, pp. 162-175.

[28] "ZigBee Specification v1.0," ZigBee Alliance, San Ramon, CA, USA2005.

[29] S. Warren, *et al.*, "Interoperability and Security in Wireless Body Area Network Infrastructures," in *IEEE Engineering in Medicine and Biology 27th Annual Conference*, Shanghai, China, 2005.

[30] D. J. Malan, *et al.*, "A Public Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography," in *IEEE Sensor and Ad Hoc Communications and Network (SECON '04)*, Santa Clara, California, USA, 2004.

[31] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," in *International Conference on Information Processing in Sensor Networks (IPSN '08)*, St. Louis, Missouri, USA, 2008.

[32] K. Malasri and L. Wang, "Addressing Security in Medical Sensor Networks," in *ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments (HealthNet '07)*, San Juan, Puerto Rico, USA, 2007.

[33] L. B. Oliveira, *et al.*, "TinyTate:Identity-Based Encryption for Sensor Networks," *Cryptology ePrint Archive,* vol. 2007/020, 2007.

[34] C. C. Tan, *et al.*, "Body Sensor Network Security: An Identity-Based Cryptography Approach," in *Frist ACM Conference on Wireless Network Security (WiSec '08)*, Alexandria, Virginia, USA, 2008.

[35] C. C. Y. Poon, *et al.* (2006, April) A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health. *IEEE Communications Magazine*.

[36] F. M. Bui and D. Hatzinakos, "Biometric Methods for Secure Communications in Body Sensor Networks: Resource-Efficient Key Management and Signal-Level Data Scrambling," *EURASIP Journal on Advances in Signal Processing,* vol. 8, pp. 1-16, 2008.

[37] A. Heinzel, *et al.*, "Fuel cells for low power applications " *Journal of Power Sources,* vol. 105, pp. 250-255, 2002.

[38] V. Leonov, *et al.*, "Thermoelectric Converters of Human Warmth for Self-Powered Wireless Sensor Nodes," *IEEE Sensors Journal,* vol. 7, pp. 650-657, 2007.

[39] A. Alomainy, *et al.*, "UWB on-body radio propagation and system modelling for wireless body-centric networks," *IEE Proceedings Communications,* vol. 153, pp. 107-114 2006.

[40] L. Schwiebert, *et al.*, "Research challenges in wireless networks of biomedical sensors," in *7th Annual International Conference on Mobile Computing and Networking* Rome, Italy, 2001, pp. 151 - 165.

[41] N. Wisniewski and M. Reichert, "Methods for Reducing Biosensor Membrane Biofouling," *Colloids and Surfaces B: Biointerfaces,* vol. 18, pp. 197-219, 2000.

[42] G.-Z. Yang, Ed., *Body Sensor Networks*. Springer, 2006, p.^pp. Pages.