2016 IEEE 40th Annual Computer Software and Applications Conference

Communication and Security in Health Monitoring Systems - A Review

Hossein Fotouhi, Aida Čaušević, Kristina Lundqvist, Mats Björkman
Mälardalen University, Västerås, Sweden
{hossein.fotouhi, aida.causevic, kristina.lundqvist, mats.bjorkman}@mdh.se

***Abstract*—The fast development of sensing devices and radios enables more powerful and flexible remote health monitoring systems. Considering the future vision of the Internet of Things (IoT), many requirements and challenges rise to the design and implementation of such systems. Bridging the gap between sensor nodes on the human body and the Internet becomes a challenging task in terms of reliable communications. Additionally, the systems will not only have to provide functionality, but also be highly secure. In this paper, we provide a survey on existing communication protocols and security issues related to pervasive health monitoring, describing their limitations, challenges, and possible solutions. We propose a generic protocol stack design as a first step toward handling interoperability in heterogeneous low-power wireless body area networks.**

I. Introduction

Advancements in the radio hardware and the wireless communication protocols enable tremendous changes in relaying sensor measurements. Various applications are gaining on wireless sensing devices for monitoring and controlling purposes. Remote health monitoring is one of the emerging applications that has attracted system designers to devise efficient and reliable communication protocols.

If we consider predictions that the world population of elderly people (65 and older) will double in 2025, compared to numbers in 1990 [1], then it is obvious that providing an efficient and reliable healthcare, at lower or at the same price as today, becomes a major challenge. Almost 30% of all deaths worldwide are related to cardiovascular diseases that can be easily detected and prevented by reliable and timely remote health monitoring systems. Consequently, health monitoring systems are about to revolutionise the human life by providing fast detection and real-time monitoring of patients. However, when employing the enabling technologies, we have to consider the well-being of the patients, since it is unacceptable to employ solutions that mismatch standards of current best practices in healthcare.

In this paper, we investigate recent research related to health monitoring systems, focusing on the wireless communication and the relevant security requirements. We focus on low-power wireless networks (LPWNs) for monitoring of human vital signs. To be fully functional, the system should be flexible and scalable, while providing sufficient levels of reliability and timeliness. Providing interoperability between different networks is also a challenging topic. Security, privacy and trust are other key issues that affect the functionality of health monitoring systems. With an increasing number of devices connected to the Internet in health monitoring systems, the possibility for security threats and adversary attacks increases. In addition, LPWNs come at the price of low-power, limited memory, and computational capabilities, which limits the use of already existing security solutions. To be concise, our contributions include:

- Investigating relevant communication technologies, and identifying challenges.
- Reviewing security and privacy issues within the LPWN technologies, together with some of the existing solutions.
- Devising a generic health monitoring system, considering the limitations and possible solution, focusing on the design of a generic protocol stack for heterogeneous LPWNs.
- Overviewing the state-of-the-art communication frameworks, designed for health monitoring applications.

The paper is organized as follows. Section II describes the main wireless communication technologies and standards, used in health monitoring applications. Section III provides details on the security issues in LPWNs. We propose a generic health monitoring framework in Section IV, followed by reviewing well-known health monitoring frameworks in Section V. The final remarks are given in Section VI.

II. Communication networks in health monitoring systems

There are two types of non-invasive body sensors; classified as *implantable sensors* (e.g., biosensors that measure metabolite levels for diabetes [2], pacemakers and endoscope capsules), and *wearable sensors* (e.g., blood pressure, ECG, SpO2 and breath sensors). The communication requirements and prerequisites depend on the type of sensors. In this work, we focus on a wireless body area network (WBAN) as it is the most common type of network within a health monitoring system, responsible for collecting measurements from sensors with low-power radios using short range communication through unreliable links. We also briefly describe the high-power networks within a health monitoring system.

We categorize the communication strategies in health monitoring systems into: intra-WBAN communication (i.e., data exchange between sensing devices and the coordinator, located on the human body), and beyond-WBAN communication (i.e., communication from the WBAN coordinator, located on the body of primary end-user towards the secondary end-user). In this section, we consider the possible wireless standards/technologies for intra-WBAN and beyond-WBAN communications. We also explain some of the quality of service (QoS) communication requirements, followed by the main challenges from a communication architecture point of view.

A. Intra-WBAN communication networks

Intra-WBAN communication, which is also known as WBAN, covers a wide variety of applications, such as health-

0730-3157/16 $31.00 © 2016 IEEE
DOI 10.1109/COMPSAC.2016.8

Table I: Comparing different standard wireless technologies in terms of network topology, transmission range, frequency band, data rate, transmission power and their security support.

Wireless technology	Standard	Network topology	Transmission range	Frequency	Bit rate	TX power	Security
ZigBee	802.15.4	star, cluster-tree, mesh	10 - 20 m	2.4 GHz	250 kb/s	-25 - 0 dBm	✓
Bluetooth	802.15.1	piconet, scatter net	10 - 30 m	13.56 MHz, 2.4 GHz	2.1 Mbit/s	0, 4, 20	✓
Bluetooth low energy	802.15.1	star	$\approx$ 50 m	2.4 - 2.5 GHz	1 Mbit/s	0, 4, 20 dBm	✓
IEEE 802.15.6	802.15.6	star	$<$ 100 m	NB, UWB, HBC	75.9 kb/s - 15.6 Mb/s	-25 - 0 dBm	✓
UWB	802.15.4a	piconet, peer-to-peer	10 m	3.1 - 10.6 GHz	480 Mb/s	-41.3 dBm/MHz	✓
WiFi	802.11	mesh	100 m	2.4 GHz	54 Mb/s	0 - 10 dBm	✓
Low-power WiFi	802.11ah	single-hop	100 - 1000 m	780, 868, 915, 950 MHz	150 kb/s	$<$ 10 dBm or $<$ 30 dBm, depending on the country	✓

care, fitness, and entertainment. It is usually used for collecting, processing and forwarding the data over a long period of time. Each WBAN consists of a number of sensing devices with processing and communication capabilities. Even if WBANs share many challenges with wireless sensor networks (WSNs), there are several specific design questions that require a new line of research.

Wearable sensors that are placed on the human body are usually used for long-term health monitoring and can prevent life threatening events. The main LPWN standards for on-body communication are: IEEE 802.15.4 [3], IEEE 802.15.6 [4] and Bluetooth [5]. However, the IEEE 802.15.6 radio is unavailable to be employed within WBAN applications. Table I summarizes the main features of these standards and technologies, comparing them with some higher power consuming wireless networks, such as WiFi and Low-power WiFi [6].

IEEE 802.15.4 [3] defines Physical (PHY) and medium access control (MAC) layers for LPWNs. It provides three frequency bands of 868 MHz, 915 MHz and 2.4 GHz, with a data rate of 250 kbps. The 2.4 GHz Industrial, Scientific and Medical (ISM) band is available worldwide and is therefore most commonly used. IEEE 802.15.4 defines two topologies: star topology (all sensor nodes communicate directly with the coordinator (single-hop)), and peer-to-peer topology (any sensor node can communicate with other sensor node), where star topology is more common in health monitoring applications.

ZigBee [7] is an open specification that complements the IEEE 802.15.4 standard with network and security layers, as well as application profiles. ZigBee supports mesh topology, where each node can communicate with any other node, through a single- or multi-hop, by relaying the transmission through multiple additional nodes. The network then can spread out over a larger area. To secure transmitted data, ZigBee networks use the advanced encryption standard (AES) encryption algorithm, which is one of the most secure, robust, and reliable algorithms that encrypts 128-bit blocks of data, using multiple substitution and permutation operations.

6LoWPAN [8] is an open standard, developed by IETF (RFC 6282) for supporting IPv6 for LPWNs, which has been integrated within IEEE 802.15.4 standard protocol. It basically adapts the long IPv6 addressing into an abstract and short frame suitable for IEEE 802.15.4 standard packet format. 6LoWPAN provides an adaptation model that provides network management, routing strategy, security, application interface, and network discovery. This open standard is also under integration within other networks, including Sub-1 GHz low-power radios, such as BLE and low-power WiFi [9].

IEEE 802.15.1 or Bluetooth [5], is designed and implemented for short-range wireless communication. It supports different frequency bands, such as 13.56 MHz, 2.4 GHz and 2.5 GHz, with the data rate 1 to 2.1 Mb/s. Two types of topologies have been defined: *piconet* and *scatternet*. A piconet is formed by the master node and one or more Bluetooth devices as slaves. A clock is set by master node in order to obtain synchronization, and frequency hopping is applied to reduce the probability of interference. Slaves have point-to-point communication with their master node. However, a master node can either unicast or multicast to slaves within the piconet. A scatternet is a collection of some piconets. A Bluetooth unit can be a member of different piconets, i.e., it can be slave in many piconets.

Bluetooth low energy (BLE) [10] was introduced as a part of the Bluetooth Core Specification version 4.0. BLE expands the functionality and applicability of Bluetooth, and makes it a suitable choice for health monitoring systems. BLE involves several changes compared to traditional Bluetooth. It operates in the spectrum band 2402-2480 MHz, divided as 40×2 MHz channels instead of 79×1 MHz channels in Bluetooth. In BLE, three advertising channels are dedicated to broadcast messages, using frequencies 2402, 2426, and 2480 MHz to mitigate interference from other technologies working in same frequency band. BLE employs a frequency hopping mechanism that reduces the risk of eavesdropping on transmitted packets. In BLE, timing requirement in frequency hopping is more relaxed due to the longer stay in each channel. Security requirements are covered by advanced encryption standards, pairing to create shared secrets, and bonding to enable trusted device pair and device authentication.

IEEE 802.15.6 [4] defines a MAC layer that supports several PHY layers, such as narrowband (NB) with frequencies 400, 800 and 900 MHz, ultra-wideband (UWB) with frequencies 2.3 and 2.4 GHz, and human body communication (HBC) with 10-50 MHz, while the data rate varies from 75.9 kb/s to 15.6 Mb/s. Selecting a proper PHY layer with accompanying frequency band should be influenced by the application requirements and limitations. With 802.15.6, sensor nodes are organised in a one- or two-hop star topology, communicating to a single coordinator or hub. In a two-hop topology, special nodes with relay capability are supposed to be placed in order to forward the data from sensor nodes towards the coordinator. The IEEE 802.15.6 standard divides the time into beacon periods or super frames with the equal length. The coordinator defines boundaries of the super frame that is separated into a number of slots, used for data transmission. Beacons are transmitted periodically for synchronisation purposes among all sensor nodes [11]. The IEEE 802.15.6 supports three security levels with different security properties, protection levels, and frame formats, which are known as (*i*) unsecured

communication level (low security level), (*ii*) authentication level (medium security level), and (*iii*) authentication and encryption (high security level).

B. Beyond-WBAN communication network

In a health monitoring system, measurements are usually forwarded from a WBAN through a gateway towards the cloud. The gateway is used to bridge two different network technologies, from low-power to high-power wireless network, or from a wireless network to a wired network. The high-power networks are out of the scope of this work, as they provide more reliable and secure way of data communication. The possible high-power wireless networks are described below.

IEEE 802.11 or WiFi that operates in the 2.4 and 5 GHz bands is the most popular wireless technology for indoor environments. The main features of WiFi are: high data rate, easy deployment, low cost and high power consumption (compared with LPWNs)[1]. Due to the increasing demands for ubiquitous devices with low-power consumption, low power WiFi (IEEE 802.111ah) [6] was designed. This radio that works at 780, 868, 915 and 950 MHz is a potential solution for relaying data from body sensors towards the cloud. IEEE 802.11ah is scalable, supporting more than 8,000 devices, and it brings seamless connectivity with WiFi. In general, WiFi enables security via WiFi Protected Access that includes both access control and privacy for the communication.

Cellular networks unlike LPWNs have a fixed infrastructure of base stations, which are connected through wires and have unlimited power. There are various cellular network technologies, such as GSM, UMTS, LTE and LTE advanced. Each one has its own features and they are progressing in terms of data rate, reliability, connectivity and more importantly security. This network guarantees reliability and security issues for beyond-WBAN communications.

C. QoS requirements

In terms of QoS, a health monitoring system should provide a long-term collection and analysis of physiological data to ensure comprehensive feedback to professionals. In order to provide a good diagnosis, the system should be dependable in the sense that it especially offers reliable, timely and secure services.

Dependability can be defined as a systems capability to consistently perform the expected behaviour in order to provide a service, while minimising the fault [12], meaning that patient-related data must be available in case of any individual node failure, sensor compromises or adversary attacks. It is one of the most critical concerns in WBANs, due to the fact that failure to retrieve correct data when needed, might cause life critical events. In order to be able to say that a system satisfies the dependability requirements, the following attributes should be guaranteed: reliability, availability, maintainability, safety, confidentiality, and integrity [13]. However, one has to bear in mind that the overall dependability in systems like this, is under huge impact of error sources, such as; failures of complex softwares existing in the system, network size that is in the constant increase due to the number of small sensor devices and technological solutions involved, and the overall complexity of the system. Additionally, knowing the fact that WBANs are designed to integrate various solutions such as; different types of communication, communication protocols, and security mechanisms, it is important to be able to assess their impact on system's properties (i.e., reliability, security, availability). In order to enable the satisfying level of dependability in complex systems such as WBANs, we have to agree on certain trade-offs (i.e., by integrating technological solutions aiming at increasing one of the properties of the system; one might minimise failures of the system, while increasing the dependability, or ensuring another property, while having negative impact on the dependability).

Reliability of a message transmission is defined as the probability of successfully delivery of a message from the sender (sensor node) to the receiver (server). Considering the existence of unreliable links in LPWNs employed in WBAN, achieving reliable data transmission is very challenging. Also, the presence of the human body, and frequent node mobility are recognized as two major sources of interference that affect link quality.

Timeliness is defined as collecting data in real-time, which is crucial in critical applications such as health monitoring, where human life might be in danger. Hence, emergency data that requires predictable feedback from the health service provider, should be delay bounded. The message transmission delay is defined as the amount of time needed to transfer a message from the source to the sink, and it is measured from the time the message is passed down to the MAC layer, traveling through multi-hops, until it reaches the upper layers at the sink node. The transmission delay includes queuing delay, MAC delay, propagation delay and processing delay at the link layer. Timeliness is particularly difficult to achieve in WBAN due to the unreliable wireless links with time-varying quality.

Security requirements for health monitoring are described in Section III.

D. Communication challenges

Modelling a transmission channel is imperative when it comes to wireless devices. There have been some effort to model the human body as a communication channel for WBANs [14]. In communication through the human body, the signal is transmitted through galvanic coupling, which is so-called *inductive coupling*. The transmitter injects the signal into the body such that an electromagnetic field is generated in the body. At the remote end, the receiver senses this electromagnetic field. In this channel, the data rate is low in the kbps range as the body effectively attenuates the signal. RF communication is also used to collect data from implantable sensors. Since the human body as a medium poses numerous wireless challenges, the results may vary according to different human body situations, such as age, gaining/losing weight and changing posture. Implanting sensing devices in a good location during surgery drastically improves the link reliability.

In this paper, however, we mainly focus on wearable sensors for on-body communications, which implies intra-WBAN. We will describe some communication challenges, such as interference, scalability and resource management.

Link unreliability. There are three major reasons for link unreliability in LPWNs. First, the nature of sensor devices that are usually equipped with low-gain antennas. These antennas, which are often omnidirectional, have an irregular pattern

[1]The maximum transmission power of a regular LPWN device (e.g., TelosB) is 1 mW, while in WiFi access points (APs) is in the range of 30 mW to 800 mW, in WiFi mobile nodes (laptops) is 32 mW, in cellular APs is $\approx 10^5$ mW and in cellular phones varies from 500 mW to 2 W.

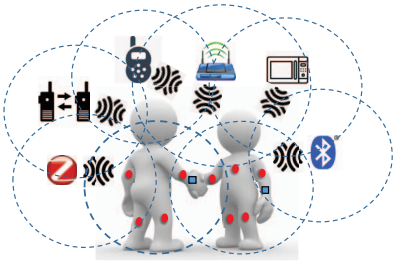

Figure 1: All types of interference in a WBAN, consisting the co-existence of another WBAN, Bluetooth devices, ZigBee devices, Microwave oven, WiFi access point, walkie talkie, and baby monitors.

during radiation. Thus, they have non-uniform communication ranges and asymmetric links. Second, the environmental factors, such as temperature and humidity drastically affect the quality of the links. Third, inaccurate radio hardware that causes link asymmetric, and eventually affects network performance.

Interference. LPWNs share the same frequency band (2.4 GHz) with many other wireless devices, such as WiFi, Bluetooth, IEEE 802.15.4, baby monitors, walkie-talkies, and microwave ovens. All external devices in addition to the WBAN devices that use the same frequency are sources of *cross interference*[2]. Figure 1 depicts all the possible sources of interference for a WBANs. The neighbouring WBANs are also considered as other major sources of interference, specially in some environments like hospitals, where many patients are monitored remotely. The interference generated by other WBAN devices is known as *mutual interference*.

Scalability is one of the major challenges in remote health monitoring applications. For some patients, it is necessary to monitor various vital signs, and collect different parameters from different sensors. Moreover, in some cases to collect a physiological parameter, it is required to employ more than a sensor node. In some cases, sensing parameters may increase according to the condition. The wireless technology should be scalable and able to self-organise the network even after increasing the number of nodes within a WBAN.

Resource management in LPWNs with limited battery power and channel bandwidth should be considered when designing a health monitoring system. For long-term patient monitoring, a wise solution would be to report emergency and high priority messages fast, but enter sleep cycles when there is no data to transmit. The low priority messages can be buffered and transmitted with low intervals.

III. Security in Health Monitoring System

In case of health monitoring systems, security threats might endanger the health state of a patient, or in the most extreme cases cause a death. In order to prevent this, strict and scalable security mechanisms are required to prevent any malicious interaction in the system. An efficient security framework for health monitoring applications must therefore ensure basic security services, such as privacy, confidentiality, authentication, authorization, availability, etc. These security services are imposed and required by different legal directives including European directive 95/46 on data protection [15] and HIPAA [16] in the United States, and should guarantee patient safety and privacy. To establish foundations for development and use of different types of WBAN applications, including medical applications, in a secure way, IEEE 802 working group for standardisation of WBANs, has produced the IEEE 802.15.6 standard [4]. Additionally in WBAN, the security mechanisms must operate fast to avoid any latency and at the same time enable high-level of scalability.

In the following, we focus on security requirements related to privacy and data access security, network communication security and data storage security as the main potential targets for security attacks.

A. Application data security requirements

Data confidentiality means that the collected, transmitted, and stored medical information is kept strictly private, and therefore can be accessed by authorised people only. On the other hand, an adversary can monitor the communication within the system and eavesdrop the transmitted information. Data confidentiality is usually achieved by encryption/decryption. *Data access control* defines a privacy policy and prevents possible unauthorised access to patient information. In WBAN, patient records could be accessed by physicians, nurses, or insurance companies. For example, based on the health condition described in a patient record, an insurance company might offer an expensive premium for health insurance [17]. Therefore, data access roles should be defined at the application level, enforcing different access privileges [18]. Besides role-based access control, one has to ensure a comprehensive set of control rules applicable within the communication framework. *Non-repudiation* is a way to guarantee that a participant in the communication network cannot deny sending or receiving a message. A common way to ensure non-repudiation is the use of digital signatures while communicating.

B. Network communication security requirements

When developing a secure WBAN, one should account for secure network communications. In this section, we describe some of the requirements related to security at this level.

Data integrity ensures that no data changes have been done by any adversary before reaching the storage. In WBANs, a failure to obtain correct data might lead to incorrect medical treatment that can have disastrous consequences. One of the mechanisms to achieve data integrity is to use a message authentication code, employed at the sender and receiver sides to verify that the data is not modified by an adversary. *Data authentication* should guarantee that the data is sent by a trusted sender. In case of absence of such a mechanism, it might happen that a false sender, appearing as a legitimate one, sends false data to the storage or gives incorrect treatment instructions to a patient, possibly causing harm to the patient. Similarly as with data integrity one can use a message authentication code with a shared secret key. *Data freshness* guarantees that all received data is fresh, i.e., all data frames are in correct order, and not replicated for disruption purposes. There are two types of data freshness guarantees, both needed in WBANs; weak and strong freshness. The first guarantees just the ordering of frames, not tackling possible delays, while the latter makes guarantees on both order and delay. Weak freshness in WBANs is required by low-cycle body sensors, such as blood pressure, while strong freshness

[2]Cross interference takes place between different network technologies working in a same frequency band.

is required during synchronising measurements with higher duty cycle, for instance in ECG [19]. *Availability* enables patient data to always be available to the physician. In case of loss of availability of one node in the system, redundancy that enforces switching operation from a disabled node to an available node can be used. In this case, it is important to use forward and backward secrecy. The first makes sure that a node leaving a network will no longer be able to read future messages, while the second ensures that the new node joining the network should not be able to read previously transmitted messages.

C. Security requirements on data storage

In WBANs, it is important to address data confidentiality and integrity, as well as dependability of data storage security. *Dependability* is one of the most critical properties when it comes to storage accessed by WBANs. It ensures quick retrieval of patient data, even in case of individual node failure and malicious modifications. So far, in the literature, dependability has been given limited attention. However, some works propose error correcting code techniques [17] that add redundancy to the original source data, while they increase network overhead in terms of packet payload size, but enhance data reliability for LPWNs with unreliable links.

D. Security challenges

Due to the resource constrains, a WBAN is required to be highly efficient. Wearable sensors are small and come at the price of low-power supply, making them incapable to carry out larger computations and to store larger amounts of data. Thus, cryptographic mechanisms used by sensors should be as light-weight as possible, in terms of computation and low storage overhead. Additionally, a denial of service attack might overwhelm the WBAN if the authentication protocol is not sufficiently fast.

The safety of a patient can be endangered if their records are not available at any time. In case of too strict data access control being introduced, providing a prompt medical care might be a problem. On the other hand, having a loose access control makes more room for malicious attacks.

If we assume that sensing devices in the health monitoring system would be used by non-expert patients, then we should make it as easy to use as possible, but at the same time provide an acceptable level of security. Possible problems might occur in cases when the patient has to give an access to his/her data to an emergency physician that has not been initially authorised, even though the strong security mechanism is used at the device. Sensor nodes might origin from different manufactures, and therefore, it might be a problem to share cryptographic materials. Consequently, it becomes very difficult to establish data security mechanisms and provide common settings compatible with a wide range of WBAN devices.

E. Existing security solutions

There are several techniques available to secure communications in WBANs based on the use of *biometrics*. Such techniques use the unique features of the human body to generate and maintain cryptographic keys used in the system. The cryptographic keys are obtained using electrocardiogram (ECG) signals, timing of the heartbeat, or using a group of similar random numbers obtained from a combination of biometrics of the human body and further distributed throughout the network [20], [21], [22]. Another suitable approach for WBANs is proposed by Shanthini et al. [23]. Their approach uses the receiver's fingerprint to generate cryptographic keys and preserve data integrity and patient's privacy. These approaches usually require less memory and computational power and thus makes them suitable for WBANs.

More traditional approaches to obtain a secure sensor network is based on the public key *cryptography*. The main disadvantage of this method is a high resource consumption, making it unsuitable for WBANs. Therefore a number of novel light-weight approaches have been proposed. The authors in [24] present a light-weight approach that includes key management, random number generation, and a three step security model. The approach is based on using a bio-channel in combination with a wireless channel to establish secure communications, as well as on the usage of physiological data to establish a secure system. In [25], a light-weight secure sensor association and key management scheme for WBANs was proposed. A group of sensor nodes establish an initial trust via group device pairing (GDP) without prior secret sharing before the meeting. The GDP protocol does not require any extra hardware devices, supports batch deployment, and relies on symmetric key cryptography. A secure sensor allocation for WBANs is described in [26]. Nodes in the system are equipped with public key-based authentication one-by-one, by a central controller, and are verified by the user through a comparison among LED blinking patterns. The disadvantage of this approach is the long time period needed for association and lack of batch deployment. Additionally, nodes with pre-distributed public keys from a trusted authority are often not practical. Authors in [27] present a secure, lightweight user authentication scheme, called Securing User Access to Medical Sensing Information (SecMed). The approach is based on elliptic curve cryptography (ECC), and provides an authentication protocol between physicians and nurses and a sensor node or PDA device. The approach uses public key codes that makes it highly scalable, requires less memory in comparison with other symmetric key-based schemes, and has good performance. Another approach based on ECC is presented in [28]. The scheme consist of setup, registration, verification and key exchange, and use of the patient's phone SIM card number as an identification code. To prevent the replay attack, they provide a counter number at every process of authenticated message exchange to resist.

IV. Proposed health monitoring framework

In Sections II and III, we stated that the main features of LPWNs (i.e., low-power radios, link unreliability, low-processing capability, single radio, and limited bandwidth) imply reliability and timeliness guarantees, while application-specific requirements (i.e., health monitoring applications) demand security support. We also need to provide the following issues while designing a health monitoring system: (*i*) interoperability to support IoT applications, (*ii*) scalability, (*iii*) light-weight security on the application, network and storage levels, and finally (*iv*) it should work in any environment, indoors, as well as outdoors, and thus, requires intra- and beyond-WBAN communications.

In this section, we propose a generic system model for health monitoring systems that provides reliable, timely and wireless secure communications and considers the future IoT demands, scalability issues, and suitability for any environment, indoors as well as outdoors. Figure 2 illustrates our proposed system design, with classification based on the limitations of each wireless technology and its security demands.

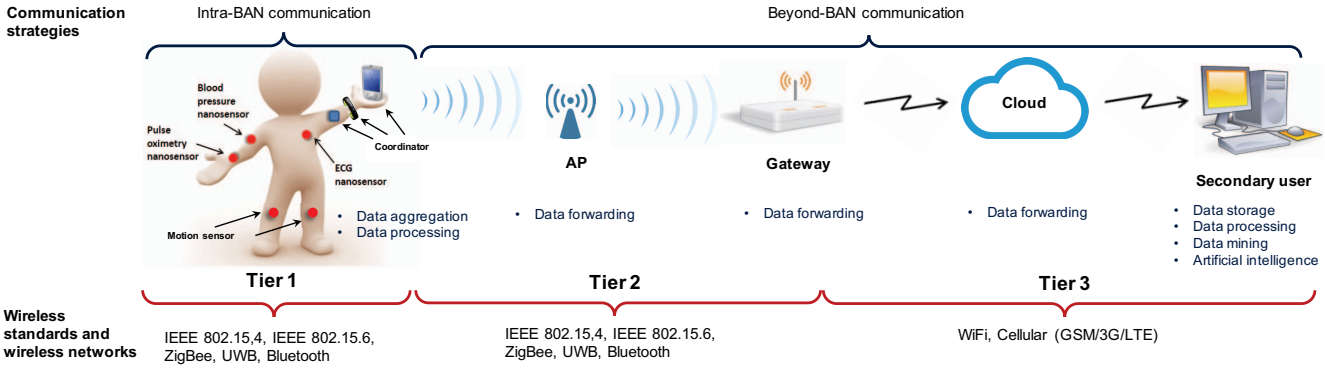

Figure 2: A generic health monitoring system, consisting of three tiers with respect to the possible wireless technologies.

A. *System design considerations*

As can be concluded from Section II, selecting a wireless network technology affects system performance in terms of *reliability*, *timeliness* and *security*. The system architecture should be designed based on the type of sensor devices, location of sensors, and the number of sensor nodes. Sensor devices record data periodically with low or high sampling rate. High sampling rate requires a radio that supports higher data rate (e.g., Bluetooth). Large attenuation of the signal during communication with the implanted sensor requires a radio that overcomes channel restrictions (e.g., UWB and IEEE 802.15.6). Increasing the number of sensor nodes on the human body requires a radio that is scalable (e.g., IEEE 802.15.4 and ZigBee). In environments where patients are more prone to security threats and attacks, it is important to employ wireless networks that guarantee some security levels (e.g., 6LoWPAN on top of IEEE 802.15.4). A multi-standard radio module is useful for supporting connectivity in different environments based on the existing wireless infrastructure [29]. Moreover, this radio module supports various data rates based on the frequency of measurements and application specific requirements. Hence, to enable data collection from a range of different sensors, a health monitoring framework should support at least IEEE 802.15.4, IEEE 802.15.6, UWB and Bluetooth to enable enough flexibility.

We propose a health monitoring system, which includes the following components: (*i*) *Coordinator* – a simple sensor node located on the human body that collects the data from all sensor nodes. Both sensing nodes and the coordinator are equipped with the same low-power radio. (*ii*) *Access points (APs)* – nodes that have the same radio as sensor nodes, which are static nodes attached on the walls, known as infrastructure. APs collect and forward data towards a Gateway. (*iii*) *Gateway* – a device that provides connection between the WBAN and the Internet, and receives the data directly from either sensor nodes or the coordinator, which is then forwarded to the cloud. We assume two types of users in these system: *primary end-user*, defined as the patient that holds sensors, and *secondary end-user*, a physician, whom analyses and makes decisions based on the processed information. We define *a three tier system architecture* for health monitoring, where low-power radios are employed in Tier 1 and Tier 2, while high-power radios are used in Tier 3. This system architectures supports various radio and network technologies that establishes a heterogeneous network.

Tier 1 supports intra-WBAN communication, i.e., data transmission from sensor nodes toward a coordinator. This short range communication is supported by IEEE 802.15.4, ZigBee, 6LoWPAN, IEEE 802.15.6, Bluetooth, BLE and UWB.

Tier 2 is classified as a beyond-WBAN communication, where it covers data transmission from the coordinator within WBAN to the APs, and then from APs toward the Gateway. The coordinator and APs have one of the aforementioned low-power radio technologies (i.e., 802.15.4, ZigBee, 6LoWPAN, 802.15.6, Bluetooth, BLE or UWB). This tier is beneficial for special patients and environments. Holding a smartphone as a Gateway for elderly people and patients with Alzheimer disease would be difficult and sometimes impossible. In some environments with the possibility of deploying low-cost low-power radios, it is possible to provide direct communication from the coordinator (i.e., one of the selected sensors within the WBAN) to one of the neighbour APs[3] (i.e., a low-power radio node) [30]. These static APs with low-power radio provide an infrastructure to relay data toward a Gateway that supports multi-radio. In outdoor environments, due to the lack of AP infrastructure, Tier 1 and Tier 2 are merged together. Thus, person should hold the Gateway node in order to collect WBAN information and relay toward the cloud.

Tier 3 is also considered as a beyond-WBAN communication, which covers data transmission from Gateway through cloud towards the sink node (server) [31]. The server is responsible for data processing before it reaches to the secondary end-user (physicians/nurses) for possible actions. Each of the aforementioned tiers would be sufficient to collect data from sensor nodes. However, in order to support connectivity in different indoor/outdoor environments, depending on the possible infrastructure, we assume three levels, where each of these levels may become inaccessible in special environments.

B. *Solutions for the identified existing challenges*

In Sections II and III, we have identified a set of challenges. The proposed generic health monitoring system design enhances network inter-operability, scalability, connectivity and security. In addition, we propose the following solutions that

[3]The term AP in our proposed framework, unlike WiFi APs, stands for a simple low-power static node that collects and forwards data from WBAN via APs towards a powerful node, known as Gateway (i.e., a node with multi-radio (low-power and WiFi/cellular radios), which is connected to a wired power source).

would further benefit the network in terms of increased QoS regarding reliability, timeliness and security.

There exists various **link quality estimators** (LQEs) for LPWNs, which are designed based on various parameters, such as packet delivery ratio, signal strength and link symmetry. However, most of them consider static nodes. In healthcare applications, the human body and mobile nodes are the two major sources that create dynamic environments, which eventually affect the LQE metric. Link quality directly affects packet delivery rate in wireless media.

Providing sufficient QoS levels in unreliable LPWNs requires a **mobility management framework** that considers both link quality (LQE parameters such as RSSI, SNR, LQI) and network parameters (e.g., local traffic, number of hops). There are different strategies to tackle mobility in wireless networks, such as *(i)* localisation algorithms, where they defines how to estimate the position or spatial coordinates of a wireless device. *(ii)* Software defined radio techniques that controls the path of a packet to an individual router. *(iii)* Hand-off or hand-over[4] mechanisms that select the best router for data communication [32]. For instance, in Tier 2, it supports network connectivity by selecting the best access point for data reliability based on an LQE parameter. A mobile IPv6-based (6LoWPAN) hand-off mechanism provides guarantees on data security.

There are different solutions proposed in the literature that address **interference awareness** in WBANs. [33] classifies these solutions into five groups: *(i)* time spacing, *(ii)* frequency spacing, *(iii)* code diversity, *(iv)* standards adaptation, and *(v)* hybrid solutions.

The idea of *time spacing* is to avoid simultaneous transmissions that causes collision in networks with single channel. TDMA techniques within MAC protocols are used to schedule data packet transmission. These solutions are useful for cases with interference from other WBAN devices. Thus, it will not be effective to obtain better performance with WiFi interference, where it uses a contention-based MAC protocol. Major problems with TDMA-based protocols are the large delays in dense sensing networks and the complex process of re-scheduling in networks with high dynamics. The re-scheduling process have been targeted in many works, by cooperative scheduling in [34] and horse race scheduling in [35].

In *frequency spacing or frequency hopping* solutions, channel assignment strategies are employed that change the channel after detecting interference. These strategies are limited to the number of available channels, and they are not very accurate in estimating the interference level in each channel. With dynamic channel selection, interference is detected by using packet error rate [36]. Channel scheduling is also used to reduce mutual interference between adjacent WBANs [37]. Frequency hopping allows communication among two or more antennas by synchronous hopping over a set of predefined channels that are traditionally selected in a pseudo-random fashion. This strategy has been implemented in Bluetooth and BLE. Hence, an adaptive frequency hopping model is required to change the dedicated channels [38]. By applying a frequency hopping strategy, it is possible to deliver the data over a more reliable link, which in turn results in higher reliability and less delay. In addition, frequency hopping makes eavesdropping and malicious monitoring more difficult, and the adversary first needs to acquire the correct pseudo-random hopping sequence.

[4]Hand-off (or hand-over) is the process where mobile nodes select the best AP available to communicate.

The *code diversity or network coding* targets CDMA techniques for data communication, where orthogonal codes of the interfering networks is used. However, these techniques require high amount of packet exchanges and complex algorithms. One solution is a parallel interference cancelation that utilises direct sequence CDMA and targets mutual interference [39]. Another solution is multi-user detection in CDMA networks for interference cancelation, where Gaussian noise and Rayleigh fading channels were considered [40]. In network coding, more than one path is selected in a routing protocol, but instead packets are combined when sent over individual links. It is a technique that is useful for saving energy consumption and enhancing the network scalability. This technique allows nodes in the network to perform algebraic operations, but requires more computational resources. Thus, network coding is likely not possible in the low-power sensors, but in the Tier 2 part of the framework, it can be used to increase scalability, redundancy and availability.

With *standard adaptation* solutions, MAC protocols are usually revised and restructured in order to enhance the coexistence of interference. One example is to select a special modulation scheme, data rate, and duty cycle (active and inactive periods) based on the level and duration of interference [41]. There are also solutions that do not modify standards, which are based on transmitting fake packets. For instance, a fake WiFi data packet with preamble duration that is sufficient for a WBAN [42], or a fake RTS packet to reserve the medium for WBAN nodes and avoid WiFi nodes to interfere [43], or fake CTS packets with specific duration, which is sufficient for WBANs and prevents WiFi nodes to send data over the medium [43].

A combination of the above four solutions is called *hybrid solutions*, which keeps the benefits of all these schemes. In [44], a distributed mutual interference mitigation method based on data packets transmission and channel scheduling was proposed. In this method, based on the information collected from the interfering networks, the WBAN either re-schedules data transmissions or enters idle state until the interference ends.

Generic protocol stack is a protocol design requirement for the future health monitoring systems that require using various radio technologies. We propose this solution as an initial solution to enable heterogeneous LPWNs for health monitoring systems. In a traditional homogeneous network, all network entities are functioning in a same protocol stack, where each layer has its specific features. Integrating various technologies with different capabilities in a health monitoring system would degrade network performance, since the inter-operability issues have been neglected in protocol stacks. In the literature, there are two main solutions that provide inter-operability within a heterogeneous network [45]:

1) Mobile IP-based techniques, which are used as network architecture to integrate different networks [46], [47]. This approach requires fundamental changes in non-IP-based network protocol stacks.
2) Gateways are used to establish connection between different networks. These devices are intermediate nodes that transfer information between different networks. However, this approach is easy to implement.

The first solution — mobile IPv6 — is a more common way to attain inter-operability in LPWNs [48], [49]. Many adaptation techniques have been defined to integrate IPv6 in different networks. For instance, 6LoWPAN was designed to

carry IPv6 datagrams over the IEEE 802.15.4 and recently under development within BLE. Web services such as REST and CoAP are tailored within the application layer. A light version of XML and SOAP are under IETF implementation for the security purposes.

The aforementioned adaptation techniques based on mobile IPv6 are targeting one of the layers specifically and customised for a network design or standard. Providing a seamless communication with good performance using different devices and networks is still a challenging topic. Conventional generic protocol stacks consist multiple physical, data link and medium access control (MAC) layers, and network, transport, and application layers [45]. Thus, based on the requirement, a specific combination of lower layers is selected, while all networks are supposed to have similar upper layer protocol designs. However, these conventional protocol stacks are very heavy in terms of memory footprint. There is a need to design novel protocol stacks that provide common features of all networks, while adding additional features to obtain a reasonable network performance.

Security enhancements, can be addressed using a lightweight encryption solutions to prevent possible eavesdropping of the transmitted data and attacks to a patient's privacy. Unauthorised access to a patient data can be solved by strict data access roles, and enforcing access privileges. Additionally, a message authentication code can be used to prevent data modification and to guarantee that the data is sent from a trusted node, but we have to keep in mind that it does not provide guarantees on timeliness. Availability can be ensured via redundancy mechanisms that enforce mode switch in case a node becomes unavailable. So far dependability-related issues are the least addressed, but we see as a possibility to include existing error correcting code techniques to bridge this gap. Note also that redundancy mechanisms and error correcting codes not only enhance security, but also increase reliability.

V. Health monitoring frameworks

In this section, we provide a description of the most representative examples of well-known system architectures for health monitoring, including both research and commercial solutions, enlisted in a chronological order of their appearance. Table II illustrates a qualitative comparison between the most common system architectures for health monitoring applications compared with our proposed system architecture with heterogeneous LPWNs. We argue that our system model can outperform the other systems in terms of security, scalability, real-time, infrastructure, hand-off and heterogeneity. However, there is a need to provide appropriate solutions for all these issues to provide the requirements for a generic system suitable for health monitoring applications.

CodeBlue [51] is a low-power wireless infrastructure, intended for emergency medical care. It is designed to operate both with a small number of devices under almost static conditions, such as hospitals, as well as in ad-hoc deployments at a mass casualty site. CodeBlue utilises a set of medical sensors integrated with some commercial-off-the-shelf platforms (i.e., Mica2, MicaZ, and Telos motes). The sensing units measure the vital signs and transmit their data directly to APs, attached on walls. Physicians subscribe to the network by multicasting. This system architecture is very scalable with self-organising capabilities. Literature related to this monitoring system recognises the need of data security and privacy protection and suggests the use of ECC approach [52] for the key generation and TinySec [53] for symmetric encryption. However, none of the suggested approaches have never been implemented within the system. CodeBlue supports scalability, timeliness and security, but it fails in terms of reliability. The results in [51] indicate that packet delivery ratio drops drastically in a (*i*) multi-hop network and (*ii*) with high sampling measurements.

The **AID-N** [54] health monitoring architecture is designed in three layers. Layer 1 consists of an ad-hoc network for collecting vital signs and running lightweight algorithms, able to operate on a limited memory and computing capabilities. Layer 2 includes servers that are connected to the Internet to forward information to a central server, located in Layer 3. The intermediate servers are laptops and PDAs that send the data. Intra- and beyond-WBAN communications is supported via IEEE 802.15.4 and IEEE 802.11, respectively, while a flexible security level is provided (i.e., from low to high level). AID-N is a real-time system architecture that fails in terms of reliability in LPWNs with unreliable links and also in networks with high sampling measurements.

The **CareNet** [55] system architecture builds a heterogenous network infrastructure and provides a two-tier wireless network for data sensing, collection, transmission, and processing. The intra-WBAN communication uses IEEE 802.15.4 wireless standard to send the data from Telos motes, while a multi-hop IEEE 802.11 wireless network provides a high performance backbone structure for packet routing. This architecture comes with a scalable software platform and built-in security communication mechanisms, which enable a reliable and privacy-preserving data transmission within the system. CareNet supports intra- and beyond-WBAN communications with a reasonable reliability, scalability and security. However, CareNet neglects the real-time issue in critical health monitoring applications.

The **MobiHealth** [56] system is designed for ambulant patient monitoring that employs cellular network (i.e., UMTS and GPRS). The patient is provided with a number of sensors, measuring the vital signs and communicating with a mobile base unit (collects the data) via Bluetooth and ZigBee. Thus this architecture supports both intra- and beyond-WBAN communication, however, mechanisms for security are not provided. MobiHealth provides reliability and inter-operability issues, while it fails in terms of security and data privacy.

MEDiSN is a wireless sensor network used to automate the process of patient monitoring in hospitals and at disaster scenes [57], developed in a collaboration of John Hopkins University Hospital, University of Latvia, University of Maryland Medical Center and Aid Networks. The system consist of a number of a mobile sensor-based physiological monitors that collect the medical data of a patient, temporarily store the data and transmit it to the nearest relay points. Relay points are self-organised into bidirectional routing tree and they transmit the patient's medical data to gateways. In the final phase, the data is stored within the back-end databases and is available to authorised personnel only. Security protection includes encryption for each physiological monitor and authentication and user authorisation. However, the details regarding the implemented security mechanism have not been revealed in the existing literature.

LAURA is a wireless sensor based lightweight system for monitoring of patients within nursing institutions [58]. Architecturally, the system consist of (i) a localisation and tracking engine to locate patients based on the samples of the received signal, (ii) a personal monitoring module that classifies the movements of the patients eventually detecting

Table II: Qualitative comparison between the related works on system architectures for health monitoring with our proposed generic health monitoring system architecture.

System architectures	Radio	Security	Scalability	Real-time	Infrastructure	Hand-off	Heterogeneous
CodeBlue	802.15.4	✗	✓	✓	✓	✓	✗
AID-N	802.15.4	✓	✓	✓	✗	✗	✗
CareNet	802.15.4	✓	✓	✗	✓	✓	✓
MobiHealth	802.15.4 or Bluetooth	✗	✗	✓	✗	✗	✗
MEDiSN	802.15.4	✓	✓	✗	✓	✗	✗
LAURA	802.15.4	✗	✓	✗	✓	✓	✗
eCare Campanion	n/a	✓	✗	✗	✓	✗	✗
[50]	802.15.4 or Bluetooth	✗	✗	✗	✓	✗	✗
Proposed system	Low-power radios	✓	✓	✓	✓	✓	✓

hazardous situations, and (iii) a wireless communication infrastructure to deliver the information remotely. The benefit of the approach is its ability to be quickly deployed, due to adopted self-calibration method. Authors address the need of security and privacy preserving mechanisms, however they omit to provide any details on the existing implementations.

eCare Companion is a health monitoring system from Philips [59]. The system provides a patient portal, accessible via PDA or tablet, where patients can enter medical information such as weight, blood pressure, etc., but also to answer questionaries about their current health condition. The system is able to connect to sensor devices such as pulse oximeter, weight scale, blood pressure meter, and medicine dispenser to collect the data automatically. In the system description Philips claims that they provide security and privacy protection of the patient's data, but do not provide details on mechanisms used. In 2014, in partnership with Salesforce Philips constructed a connected, multi-point and collaborative data platform for healthcare similar to eCare Companion [60]. It is a cloud-based information technology that enables different devices to be connected.

In [50], authors present a distributed system architecture for fall detection by identifying human postures, and detecting harmful activities. The system constitutes of multiple tiny sensor nodes attached on human body with IEEE 802.15.4 radio. Two types of communication between sensor nodes and the remote server was defined. For indoor environments, sensors communicate with access points through 802.15.4 enabled radios, while for the outdoor environment, sensor nodes send data through smartphone using Bluetooth radio. Thus, each sensor node is equipped with two radios of Bluetooth and 802.15.4.

VI. Concluding remarks

In this paper, we review the ongoing research within health monitoring systems in terms of wireless communication infrastructure, QoS requirements, security and safety issues. We identify the main challenges regarding wireless communication technologies and security threats. We also propose a generic framework, classified into three tiers based on the specific advantages and limitations of wireless technologies together with the application demands, and provide a set of solutions to the main communication challenges and security requirements related to these tiers. We have identified security as a critical point in health monitoring-related applications, and therefore it is paramount to select LPWNs that provide sufficient security guarantees.

Acknowledgments

Authors would like to thank to associate professor Elisabeth Uhlemann for discussions and valuable comments on the early versions of the paper. This work is funded by the Swedish Knowledge Foundation (KKS) throughout research profile Embedded Sensor System for Health (ESS-H), the distributed environments Ecare@Home, and Research Environment for Advancing Low Latency Internet (READY).

References

[1] S. Ullah, H. Higgin, M. A. Siddiqui, and K. S. Kwak, "A study of implanted and wearable body sensor networks," in *Agent and Multi-Agent Systems: Technologies and Applications*. Springer, vol. 4953, 2008.

[2] S. Vaddiraju, I. Tomazos, D. J. Burgess, F. C. Jain, and F. Papadimitrakopoulos, "Emerging synergy between nanotechnology and implantable biosensors: a review," *Elsevier Biosensors and Bioelectronics*, vol. 25, 2010.

[3] "Ieee standard for local and metropolitan area networks - part 15.4: Low-rate wireless personal area networks (lr-wpans), ieee std 802.15.4-2011 (revision of ieee std 802.15.4-2006)," IEEE, 2006. [Online]. Available: http://standards.ieee.org/getieee802/802.15.html

[4] C. S. IEEE, "Ieee standard for local and metropolitan area networks part 15.6: Wireless body area networks," 2012.

[5] "Bluetooth, sig, bluetooth specification," 2010.

[6] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "Ieee 802.11 ah: the wifi approach for m2m communications," *IEEE Wireless Communications*, vol. 21, 2014.

[7] "Zigbee specification, version 1.0," ZigBee Alliance, 2004. [Online]. Available: http://www.zigbee.org/

[8] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, 2011.

[9] T. I. Jonas Olsson. (2014) 6LoWPAN demystified. [Online]. Available: http://www.ti.com/lit/wp/swry013/swry013.pdf

[10] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," *Sensors*, vol. 12, 2012.

[11] S. Ullah, M. Mohaisen, and M. A. Alnuem, "A review of ieee 802.15. 6 mac, phy, and security specifications," *Hindawi International Journal of Distributed Sensor Networks*, 2013.

[12] Y. Hovakeemian, K. Naik, and A. Nayak, "A survey on dependability in body area networks," in *5th International Symposium on Medical Information Communication Technology (ISMICT)*, March 2011.

[13] W. Elghazel, J. Bahi, C. Guyeux, M. Hakem, K. Medjaher, and N. Zerhouni, "Dependability of wireless sensor networks for industrial prognostics and health management," *Computers in Industry*, 2015.

[14] M. S. Wegmueller, A. Kuhn, J. Froehlich, M. Oberle, N. Felber, N. Kuster, and W. Fichtner, "An attempt to model the human body as a communication channel," *IEEE Transactions on Biomedical Engineering*, vol. 54, 2007.

[15] E. Parliament and of the Council. (1995) Directive 95/46/ec of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[16] U. S. Congress. (1996) Health insurance portability and accountability act. [Online]. Available: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

[17] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, 2010.

[18] M. Evered and S. Bögeholz, "A case study in access control requirements for a health information system," in *Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation*, ser. ACSW Frontiers, vol. 32. Australian Computer Society, Inc., 2004.

[19] S. Irum, A. Ali, F. A. Khan, and H. Abbas, "A hybrid security mechanism for intra-wban and inter-wban communications," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[20] S. M. K.-u.-R. Raazi, H. Lee, S. Lee, and Y.-K. Lee, "Bari+: A biometric based distributed key management approach for wireless body area networks," *Sensors*, vol. 10, 2010.

[21] H. Wang, H. Fang, L. Xing, and M. Chen, "An integrated biometric-based security framework using wavelet-domain hmm in wireless body area networks (wban)," in *IEEE ICC*, 2011.

[22] T. Hong, S.-D. Bao, Y.-T. Zhang, Y. Li, and P. Yang, "An improved scheme of ipi-based entity identifier generation for securing body sensor networks," in *IEEE Conference on Engineering in Medicine and Biology Society (EMBC)*, Aug 2011.

[23] B. Shanthini and S. Swamynathan, "Genetic-based biometric security system for wireless sensor-based health care systems," in *International conference on Recent Advances in Computing and Software Systems (RACSS)*, april 2012.

[24] S.-D. Bao and Y.-T. Zhang, "A design proposal of security architecture for medical body sensor networks," in *BSN*, 2006.

[25] M. Li, S. Yu, W. Lou, and K. Ren, "Group device pairing based secure sensor association and key management for body area networks," in *IEEE INFOCOM*, 2010.

[26] S. L. Keoh, E. Lupu, and M. Sloman, "Securing body sensor networks: Sensor association and key management," in *IEEE PerCom*, 2009.

[27] R. Sankar, X. Le, S. Lee, and D. Wang, "Protection of data confidentiality and patient privacy in medical sensor networks," in *Implantable Sensor Systems for Medical Applications*, ser. Woodhead Publishing Series in Biomaterials, A. Inmann and D. Hodgins, Eds. Woodhead Publishing, 2013.

[28] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ecc algorithm for patient's medical information in healthcare system," in *International Conference on Information Networking (ICOIN)*, Feb 2014.

[29] Y.-H. Liu, X. Huang, M. Vidojkovic, A. Ba, P. Harpe, G. Dolmans, and H. de Groot, "A 1.9 nj/b 2.4 ghz multistandard (bluetooth low energy/zigbee/ieee802. 15.6) transceiver for personal/body-area networks," in *IEEE ISSCC*, 2013.

[30] H. Fotouhi, M. Zúñiga, M. Alves, A. Koubâa, and P. Marrón, "Smarthop: A reliable handoff mechanism for mobile wireless sensor networks," in *EWSN*, 2012.

[31] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 2010.

[32] H. Fotouhi, D. Moreira, and M. Alves, "mrpl: Boosting mobility in the internet of things," *Elsevier Ad-Hoc Networks*, 2015.

[33] T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in wban: analysis and open research issues," *Wireless Networks*, vol. 20, no. 8, 2014.

[34] E.-J. Kim, S. Youm, T. Shon, and C.-H. Kang, "Asynchronous inter-network interference avoidance for wireless body area networks," *The Journal of Supercomputing*, vol. 65, no. 2, 2013.

[35] L. Wang, C. Goursaud, N. Nikaein, L. Cottatellucci, and J. Gorce, "Cooperative scheduling for coexisting body area networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, 2013.

[36] R. C. Shah and L. Nachman, "Interference detection and mitigation in ieee 802.15. 4 networks," in *Proceedings of the 7th international conference on Information processing in sensor networks*. IEEE Computer Society, 2008, pp. 553–554.

[37] W. Lee, S. H. Rhee, Y. Kim, and H. Lee, "An efficient multi-channel management protocol for wireless body area networks," in *Information Networking (ICOIN)*. IEEE, 2009.

[38] L. Stabellini and M. M. Parhizkar, "Experimental comparison of frequency hopping techniques for 802.15. 4-based sensor networks," in *UBICOMM*, 2010.

[39] W.-B. Yang and K. Sayrafian-Pour, "A ds-cdma interference cancellation technique for body area networks," in *Personal Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2010.

[40] K. Ghanem and P. S. Hall, "Interference cancellation using cdma multi-user detectors for on-body channels," in *Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2009.

[41] W.-B. Yang and K. Sayrafian-Pour, "Interference mitigation using adaptive schemes in body area networks," *International Journal of Wireless Information Networks*, vol. 19, no. 3, 2012.

[42] Y. Wang, Q. Wang, Z. Zeng, G. Zheng, and R. Zheng, "Wicop: Engineering wifi temporal white-spaces for safe operations of wireless body area networks in medical applications," in *32nd Real-Time Systems Symposium (RTSS)*. IEEE, 2011.

[43] J. Hou, B. Chang, D.-K. Cho, and M. Gerla, "Minimizing 802.11 interference on zigbee medical sensors," in *Proceedings of the 4th International Conference on Body Area Networks*, 2009, p. 5.

[44] W. Sun, Y. Ge, and W.-C. Wong, "A lightweight inter-user interference mitigation method in body sensor networks," in *8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2012.

[45] A. Gani, G. M. Nayeem, M. Shiraz, M. Sookhak, M. Whaiduzzaman, and S. Khan, "A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing," *Journal of Network and Computer Applications*, vol. 43, 2014.

[46] P. Feder, R. Isukapalli, and S. Mizikovsky, "Wimax-evdo interworking using mobile ip," *Communications Magazine*, vol. 47, no. 6, 2009.

[47] M. Bernaschi, F. Cacace, G. Iannello, S. Za, and A. Pescapé, "Seamless internet working of wlans and cellular networks: architecture and performance issues in a mobile ipv6 scenario," *Wireless Communications*, vol. 12, no. 3, 2005.

[48] M. Durvy, J. Abeillé, P. Wetterwald, C. O'Flynn, B. Leverett, E. Gnoske, M. Vidales, G. Mulligan, N. Tsiftes, N. Finne *et al.*, "Making sensor networks ipv6 ready," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, 2008.

[49] N. B. Priyantha, A. Kansal, M. Goraczko, and F. Zhao, "Tiny web services: design and implementation of interoperable and evolvable sensor networks," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, 2008.

[50] F. Felisberto, R. Laza, F. Fdez-Riverola, and A. Pereira, "A distributed multiagent system architecture for body area networks applied to healthcare monitoring," *BioMed research international*, vol. 2015, 2015.

[51] V. Shnayder, B.-r. Chen, K. Lorincz, T. R. F. Jones, and M. Welsh, "Sensor networks for medical care," in *SenSys*, vol. 5, 2005.

[52] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on*, April 2008.

[53] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, ser. SenSys '04. ACM, 2004.

[54] T. Gao, T. Massey, L. Selavo, D. Crawford, B.-r. Chen, K. Lorincz, V. Shnayder, L. Hauenstein, F. Dabiri, and J. Jeng, "The advanced health and disaster aid network: A light-weight wireless medical system for triage," *IEEE Biomedical Circuits and Systems*, vol. 1, 2007.

[55] S. Jiang, Y. Cao, S. Iyengar, P. Kuryloski, R. Jafari, Y. Xue, R. Bajcsy, and S. Wicker, "Carenet: an integrated wireless sensor networking environment for remote healthcare," in *ICST*, 2008.

[56] K. Wac, R. Bults, B. Van Beijnum, I. Widya, V. Jones, D. Konstantas, M. Vollenbroek-Hutten, and H. Hermens, "Mobile patient monitoring: the mobihealth system," in *IEEE EMBC*, 2009.

[57] J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson, T. Gao, W. Destler, L. Selavo, and R. P. Dutton, "Medisn: Medical emergency detection in sensor networks," *ACM Trans. Embed. Comput. Syst.*, no. 1, Aug. 2010.

[58] A. Redondi, M. Chirico, L. Borsani, M. Cesana, and M. Tagliasacchi, "An integrated system based on wireless sensor networks for patient monitoring, localisation and tracking," *Ad Hoc Netw.*, vol. 11, Jan. 2013.

[59] "Philips heathcare," http://www.hospitaltohome.philips.com/, accessed: 2015-11-27.

[60] "Philips and salesforce.com announce a strategic alliance to deliver cloud-based healthcare information technology," http://www.newscenter.philips.com/us_en/standard/news/press/2014/20140626-Philips-and-Salesforce-announce-a-strategic-alliance-to-deliver-cloud-based-healthcare-information-technology.wpd#.VlgUlN-rRUM/, accessed: 2015-11-27.