Wireless Body Area Network (WBAN): A Survey on Reliability, Fault Tolerance, and Technologies Coexistence

MARWA SALAYMA, AHMED AL-DUBAI, and IMED ROMDHANI, Edinburgh Napier University
YOUSSEF NASSER, American University of Beirut

Wireless Body Area Network (WBAN) has been a key element in e-health to monitor bodies. This technology enables new applications under the umbrella of different domains, including the medical field, the entertainment and ambient intelligence areas. This survey paper places substantial emphasis on the concept and key features of the WBAN technology. First, the WBAN concept is introduced and a review of key applications facilitated by this networking technology is provided. The study then explores a wide variety of communication standards and methods deployed in this technology. Due to the sensitivity and criticality of the data carried and handled by WBAN, fault tolerance is a critical issue and widely discussed in this paper. Hence, this survey investigates thoroughly the reliability and fault tolerance paradigms suggested for WBANs. Open research and challenging issues pertaining to fault tolerance, coexistence and interference management and power consumption are also discussed along with some suggested trends in these aspects.

CCS Concepts: • **Computer systems organization** → **Sensor networks**; **Reliability**; **Fault-tolerant network topologies**; *Sensors and actuators*; • **Hardware** → **Wireless devices**; **Wireless integrated network sensors**; **Fault tolerance**; *Sensors and actuators*; *Sensor devices and platforms*; *Analysis and design of emerging devices and systems*

Additional Key Words and Phrases: Wireless body area networks, QoS, medical, channel access, fading, WBAN standards

ACM Reference Format:
Marwa Salayma, Ahmed Al-Dubai, Imed Romdhani, and Youssef Nasser. 2017. Wireless body area network (WBAN): A survey on reliability, fault tolerance, and technologies coexistence. ACM Comput. Surv. 50, 1, Article 3 (March 2017), 38 pages.
DOI: http://dx.doi.org/10.1145/3041956

1. INTRODUCTION

The first decades of the last century heralded a revolution in wired communication: they brought about an almost magical technological evolution especially sensing data and communications. It did not take long for people to realise however that this technology was inefficient, especially when it comes to wiring costs, mobility and independent connections. Such inefficiencies have been the key driving forces towards the evolution

Authors' addresses: M. Salayma, School of Computing, Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, UK; email: m.salayma@napier.ac.uk; A. Al-Dubai, School of Computing, Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, UK; email: a.al-dubai@napier.ac.uk; I. Romdhani, School of Computing, Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, UK; email: i.romdhani@napier.ac.uk; Y. Nasser, ECE Department, American University of Beirut, Beirut, Lebanon; email: yn10@aub.edu.lb.

DOI: http://dx.doi.org/10.1145/3041956

of wireless technology [Akyildiz et al. 2002; Boukerche 2005]. Wireless communication has revolutionised our daily lives as it pervades most technological applications such as controlling, tracking, monitoring and automation [Selavo et al. 2007; De Oliveira et al. 2009]. It was not long before the wireless sensor networking (WSN) revolution shifted its direction to a technology that suited human mobility by devising a technology that can be wearable or even implanted in the human body. This technology is characterized by low-cost, energy-constrained, tiny, heterogeneous sensor nodes that form a special type of WSN, namely, the Wireless Body Area Network (WBAN) [Movassaghi et al. 2014]. A WBAN comprises sensors that capture physiological information and send it to a central base station through wireless communication. WBAN replaces complex and wired healthcare equipment as it is able to continuously monitor the body's vital statistics [Movassaghi et al. 2014]. WBAN sensor devices are supposed to provide real-time feedback without causing any discomfort, thereby providing a greater deal of flexibility and mobility to the user [Otto et al. 2006]. More importantly, the data provided by WBAN gives doctors a better view of a patient's situation as this data is gathered during a patient's normal activities in his/her natural environment. WBAN devices are characterised by their heterogeneity [Mahapatro and Khilar 2011], i.e., they vary in their capabilities, tasks, sizes, sampling rates, required resources and levels of intelligence. The criticality of WBAN applications, the dynamic environment within which they operate (limited to the human body) and the heterogeneity of the deployed sensor devices confirm that WBAN has special characteristics that impose key challenges in designing an efficient and resilient WBAN. For instance, a WBAN has to be reliable as any fault could be life threatening for the person dependent on this technology. One of the requirements of a reliable system is that it has to be fault tolerant, that is, it needs to have the ability and the capability to self-heal if a fault occurs regardless of the type or nature of fault [Liu et al. 2009]. Despite ongoing research studies that tackle technical issues in WBAN, such as energy, mobility, security, routing and sensor design, however, fault detection and recovery in WBANs is still in their infancy. These observations motivate us to place a great deal of emphasis on this concept in this study.

In fact, there have been several surveys pertaining to WBANs. We briefly introduce these surveys in chronological order and then we demonstrate how our survey differs from existing literature surveys. For instance, the MAC layer protocols of WBANs are surveyed in Gopalan et al. [2010]. The survey provided in Latré et al. [2011] covers the network layers and some existing projects related to the WBANs deployment. The survey conducted by Barakah and Ammad-uddin [2012] focuses on the role of the virtual doctor server (VDS) in current WBAN architecture. The healthcare applications are surveyed in Crosby et al. [2012] and the WBAN layers are covered in Ullah et al. [2012]. As for the routing protocols, [Movassaghi et al. 2013] provided a review of protocols deployed in WBANs. The design properties of WBANs are covered in Cavallari et al. [2014] and the coexistence problem was explored in Hayajneh et al. [2014]. The architecture, routing, channel modelling, PHY layer, MAC layer, security and applications are covered in Movassaghi et al. [2014]. The security related issues have been tackled in the survey of Mainanwal et al. [2015]. Moravejosharieh and Lloret [2015] have focused on IEEE 802.15.4 standard. Although the previous studies shed some light on various important issues and concepts in WBANs, this technology is still unexplored in different aspects and dimensions. To the best of our knowledge, there has not been any survey study reported on fault tolerance, reliability and interferences management. To fill in this gap, this survey makes these major contributions.

—Unlike existing surveys, this survey emphasizes on two major issues lightly addressed before, namely, fault-tolerance- and reliability-related issues.

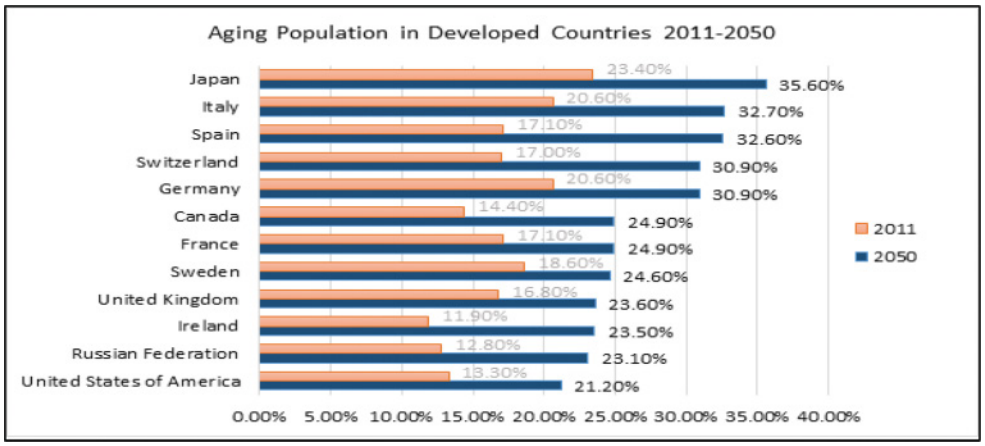

Fig. 1. Statistics of population aging in developed countries [Rutherford and Socio 2012].

—It provides an overview of some of the key challenges presented in the recent literature regarding reliablity and provides a summary of related research work. Moreover, we explore both the hardware and software faults.
—It presents the need for better reliable solutions and integration among different layers. It presents the interferences management and illustrate how the different mobility models can affect the network reliability and possible solutions to mitigate interferences.

The structure of this survey is as follows: Section 2 presents an overview about WBAN, it discusses the possible motivation for adopting this technology, its potential applications, the proposed standards and its devices. Section 3 illustrates the challenges of the WBAN technology. It focuses on fault tolerance, as it is one of the major WBAN reliability requirements, it classifies faults and failures and illustrates the fault tolerance life cycle. Section 4 presents the proposed mechanisms and schemes that targeted towards achieving a reliable WBAN. This survey is ended in Section 5 with a summary of the main points revealed in the survey and a conclusion of the literature reviewed.

2. WIRELESS BODY AREA NETWORKS (WBANs)

Our world is facing a rapid growth in population which is accompanied with an increase in the average lifetime expectancy of individuals, especially in the developed countries, leading to an increasing number of people who are over 65 years old [Rutherford and Socio 2012]. Given the population chart shown in Figure 1, 23.6% of United Kingdom's population is expected to be over 65 by 2050. Figure 1 reveals that not only the United Kingdom is characterised with population aging, but the majority of the developed countries lead this phenomenon. The ratio of people of age 16–64 to those who are over 65 will be 2.5:1 in the United Kingdom.

Unfortunately, chronic and fatal diseases such as cancer and cardiovascular and asthma diseases are often diagnosed too late. Consequently, this increases the death rate of individuals who are diagnosed with such diseases. Early detection would mitigate the impact of such diseases and increase the sufferers' life expectancy. Furthermore, traditional monitoring systems do not provide a complete picture of a patient's status as the bodily functions are monitored too infrequently. The lack of early detection and effective monitoring of diseases affect increases health care cost and adds a huge

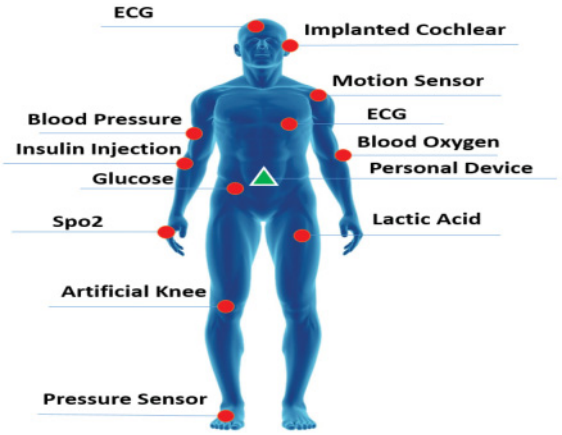

Fig. 2. Typical WBAN.

load to health care systems with limited financial resources. This calls for more affordable and scalable systems that are able to move current health care in the direction of early disease diagnosis and proactive wellness management. Wireless technologies, including WSN and Wireless Personal Area Networks (WPAN), nanotechnologies, and the Internet provide the means through which economical solutions could be found for health care systems. Such technologies suggest the idea of using tiny, smart, low-power, microsensors and actuators to sample physiological data and then forward it to a remote server through wireless communication. While WPAN devices operate within very small range area (less than 10m), the communication range of WBAN devices would be narrower than that of WPAN as they are limited to the human body area where they could be worn or implanted [Latr'e et al. 2011]. Actually, WBAN is considered to be the next generation of WPAN. A typical WBAN is shown in Figure 2. Though WBAN comprises the typical characteristics of both WSN and WPAN, it also has its own characteristics and thus its own requirements. WBAN saves lives by allowing early detection of abnormal situations through wearable and implanted monitoring devices. It allows continuous and real-time monitoring with no human or mechanical intervention, which improves the quality of the achieved results. Moreover, WBAN offers patients the ability to carry out their normal activities without interruption while their vital signals are monitored, as they are no longer required to stay in hospital or stick to a medical service [Movassaghi et al. 2014]. The adoption of WBAN should reduce the cost of healthcare, by minimizing the need for expensive in-hospital care monitoring. Such benefits have motivated practitioners in other fields, such as sports, the military and the entertainment field to adopt it in their systems [Patel and Wang 2010].

A classification of the various applications that can be facilitated by WBAN is presented next, followed by the four popular standards proposed for WBAN, the main WBAN devices and finally the most important WBAN challenges featured in the literature to its special nature.

2.1. Applications of WBAN

WBAN applications span from the health care and entertainment fields to sport and the military among others. According to (TG6) [2012], WBAN applications are categorised as either medical or non-medical. This section classifies WBAN applications according to their target domain of application. Each application is further classified into medical,

Table I. Fields and Applications of WBAN

WBAN fields	Applications types		Examples of applications
Healthcare	Medical	Wearable	Electrocardiogram (ECG), electroencephalogram (EEG), Electromyography (EMG), Saturation of Peripheral Oxygen (SPO2), temperature, blood pressure, drugs delivery
		Implant	Diabetes control
	Non-medical	Motion detection	
		Secure authentication	
Military and defense	Medical wearable	Asses solider fatigue, detect life threatening situations	
	Non-medical wearable	Fire detection, poisonous gas	
Sports	Medical wearable	heartbeat, temperature, blood pressure, motion sensor	
Entertainment	Non-medical wearable	Real time streaming: Video streaming by camera, audio streaming by headsets	
		Consumer electronics: MP3 player, microphone, camera	
		Gaming purposes, virtual reality, ambient, intelligence areas, personal item tracking and social networking	

non-medical, implanted, and wearable. WBAN fields of applications are summarised in Table I. They are further classified into medical and non-medical applications. Table I also gives some examples for each WBAN field.

2.1.1. Healthcare. This is one of the most promising fields for using WBAN. Implanted and wearable sensors are used to collect biomedical signals remotely and continually [Malik and Singh 2013; Cavallari et al. 2014]. This continual monitoring allows a proactive fatal and anomalies detection which is vital for diagnosing heart and brain activities. Actuators help in automatic drug delivery. Some applications such as cochlear implants, hearing aids, and artificial retinas help enhance the life style of human beings [Barakah and Ammad-Uddin 2012; Malik and Singh 2013]. Additionally, given that medical accidents can and do happen, WBAN applications help to reduce them and increase public safety by using profiles of previous medical accidents to alert medical personnel before similar accidents occur. Consequently, WBAN is expected to improve the management of illnesses and reaction to crisis which will increase the efficiency of health care systems. WBAN health care applications can be further classified as follows.

2.1.1.1. Medical Applications. WBAN medical applications enable the continual monitoring of physiological parameters such as the heartbeat, the body temperature, and blood pressure [Movassaghi et al. 2014]. The data collected can be sent through a cell phone, which acts as a gateway, to a remote location such as an emergency centre so that the relevant action can be taken [Barakah and Ammad-Uddin 2012; Malik and Singh 2013; Movassaghi et al. 2014]. WBAN is considered key to the early detection and treatment of patients with serious cases such as diabetes and hypertension. Medical applications of WBAN can be further divided according to the position of the medical sensors as follows:

—*Wearable Applications*. Medical wearable healthcare applications include temperature monitoring, blood pressure monitoring, glucose level monitoring, ECG, EEG, EMG, SpO_2, drugs delivery. Other applications can be found in Movassaghi et al. [2014].

—*Implant Applications*. These applications comprise nodes implanted either under the skin or in the stream of the blood such as in diabetes control systems, cardiovascular diseases and cancer detection.

2.1.1.2. Non-Medical Applications. These applications are considered to fall within the wearable sensor class of applications and include two applications which are Movassaghi et al. [2014]:

—*Motion Detection*. This application is used to detect, capture, recognise and identify body gestures and motions and send alerts to the owner of the application. For example, fear increases heartbeat, which leads to sweating and other symptoms. Thus, emotional status can be measured and monitored [Movassaghi et al. 2014].
—*Secure Authentication*. This is a very promising WBAN application as it is the core of both multi-modal biometrics and electroencephalography. This application harnesses physiological and behavioural human body biometrics such as fingerprints and facial patterns.

2.1.2. Sports. Sport activities and fitness can be improved by keeping a log of vital physiological data such as temperature, heart beat and blood pressure. The data can be used to avoid sport accidents and injuries and to plan for future training [Barakah and Ammad-Uddin 2012; Malik and Singh 2013; Cavallari et al. 2014]. According to Movassaghi et al. [2014], WBAN sport applications are considered to be medical wearable applications. Such applications enhance professional and amateur sport training especially for athletes. For example, they provide the necessary information to enable training schedules of professional athletes to be adapted to make them more effective.

2.1.3. Entertainment. Entertainment is also a very promising field for WBAN. The film industry, for example, benefits from motion capturing and post production mechanisms to produce movies in which actors perform the objects roles [Cavallari et al. 2014]. Using the on-body accelerometers and gyroscopes for capturing motions facilitates the possibility of tracking the different positions of body parts [Cavallari et al. 2014]. According to Movassaghi et al. [2014], WBAN entertainment applications are considered to be wearable non-medical applications. WBAN can be used in three types of entertainment applications, presented below.

—*Real-Time Streaming*. This includes video streaming, as well as audio streaming such as voice communication for headsets that are used for listening to explanations, illustrations, and multicasting (for example, conference calls).
—*Consumer Electronics*. These applications include appliances/devices such as microphones, MP3-players, cameras and other advanced interfaces such as neural interfaces.
—Gaming, virtual reality, ambient intelligence areas, personal item tracking and social networking [Malik and Singh 2013].

2.1.4. Military and Defense. WBAN provides new capabilities to improve performance of individual and teams of soldiers in military situations. To avoid threats at the individual tier, a group of sensors sample important information on the surrounding emerging actions and environment. At the team level, the taken information enables the commander to coordinate team tasks efficiently. Inter-WBAN communications and security play a key role in preventing critical data from being hacked by enemies [Cavallari et al. 2014]. WBAN applications can be considered as either medical wearable or non-medical wearable as follows:

2.1.4.1. Medical Military WBAN Applications. These types of applications are used to assess soldier fatigue and battle readiness and for safeguarding uniformed

personnel. For example, sensors surrounding soldiers, firefighters or policemen can foresee a life-threatening situation by monitoring the level of air toxins.

2.1.4.2. Non-Medical Military WBAN Applications. Such applications involve off-body sensors (on buildings) that are used for emergencies. Such sensors are capable of, for example, detecting a fire in the home or a poisonous gas and must directly send this information to on- and in-body devices to notify the wearer of the emergency situation.

2.2. WBAN Communication Standards

There are several reasons behind the motivation of wireless communities to standardise their technologies. Standardisation allows interoperability which enables wide use of the products since manufacturers depend on common fixed specifications in developing their products. Additionally, customers need not to depend on a certain vendor. This saves the costs for both the vendors and customers [Cavallari et al. 2014]. It is worth to mention that WBAN often follows a star topology and due to the body nature, the majority - if not all- the WBAN challenges are related to the reliability of the channel access mechanisms. In this regard, this section presents the main technologies that are proposed to serve WBAN and focuses on the MAC techniques adopted by those technologies to support WBAN. A comparison between the WBAN supported technologies is presented in Table II.

2.2.1. IEEE 802.15.4 Standard. The IEEE 802.15 Task Group 4 (TG4) proposed a communication standard that is geared toward WPANs [TG4 2003]. This technology, called IEEE 802.15.4, has become the de facto standard that supports both WSN and WBAN. Many studies on the design of WSN power-aware algorithms and standards based on IEEE 802.15.4 have emerged recently [Salayma et al. 2013a, 2013b]. Notice that, the IEEE 802.15.4 standard considers both physical and MAC layers. Due to WBAN challenges, the design of these networks necessitates the need for new protocols. In this regard, IEEE 802.15 community has proposed amendments to the physical and MAC layers of IEEE 802.15.4 protocol stack to overcome the drawbacks of the legacy IEEE 802.15.4 in achieving the requirements of WBAN, which are the IEEE 802.15.4a [TG4a 2007] and IEEE 802.15.4j [TG4j 2012]. In addition, IEEE 802.15 has proposed a new standard that is geared towards WBAN, specifically, namely the IEEE 802.15.6 this standard among with the two amendments on IEEE 802.15.4 are presented in the following subsections.

2.2.2. IEEE 802.15.6 Standard. The existing standards (e.g., IEEE 802.15.4) do not meet the regulations of medical communication as they fail to support the needs of applications in terms of key issues such as reliability, low power, the variety of traffic flows and coexistence. The IEEE 802.15 Task Group 6 (TG6) has proposed a communication standard that is geared toward applications in the vicinity of, or inside, the body, such as in medical, sports and military applications [TG6 2012]. It supports low cost, low complexity, very short range, and highly reliable and ultra-low power wireless communication. It aims to support an array of applications with a range of requirements such as data rates and channel bandwidths. To support various applications, the standard offers three bandwidths defined in three different physical layers: Narrow Band (NB), Human Body Communication (HBC) and UWB [Cavallari et al. 2014; Movassaghi et al. 2014]. These physical layers share only one MAC layer. The supported data rate ranges between 75.9Kbps in NB and 15.6Mbps in HBC. As the range, it is limited to 3m for in-body communication and has to be at least 3m for body-to-body communication patterns. The standard allows star and 2-hops tree topologies [Movassaghi et al. 2014]. IEEE TG6 provides two classifications for devices, according to their position in the body: implanted nodes, body surface nodes and external nodes.

Table II. A Comparison between the Aforementioned Technologies Discussed in this Section

Standard/ Criteria	IEEE802.15.4	IEEE802.15.4a	IEEE802.15.4j	IEEE802.15.4.6
Network type	WPAN	UWB WBAN	MBAN	WBAN: NB, UWB and HBC
MAC modes	Beacon/Non-Beacon mode with/without superframe	Superframe Beacon mode enabled	Superframe Beacon mode enabled	Superframe with beacon mode Superframes with non-beacon mode Non-beacon mode without only
Access mechanisms	Random access (with Contention: CAP) Scheduled access (without Contention: CFP)	Random access (Contention-based: CAP) Scheduled access (Contention free: CFP)	Random access (with contention CAP) Scheduled access (Contention free: CFP)	Contention-based random access: EAP1,RAP1,EAP2, RAP2,CAP) TypeI/II) Connection oriented contention-free: TypeI/II)
Contention access resource allocation procedure	Slotted and un-slotted CSMA/CA in beacon mode and in non-beacon mode (in CAP)	Slotted or unslotted Aloha (CSMA is optional) (in CAP)	Slotted CSMA/CA (in CAP)	CSMA/CA/a slotted Aloha (in EAP1,RAP1,EAP2, RAP2,CAP)
Contention free access resource allocation procedure	Schedule access by allocating static GTS Allocation persists in the upcoming superframes. (1-periodic) (in CFP)	Schedule access by allocating static GTS Allocation persists in the upcoming superframes. (1-periodic) (in CFP)	A multi-periodic scheduled access by allocating static GTS (m-periodic) (in CFP)	Two access modes: 1-Schedules the allocation of slots: one/ multiple upcoming superframes single-periodic or m-periodic) allocations. 2-In unscheduled access: unscheduled polling/posting
Specific Access for prioritised (emergency) traffic	No	No	No	Yes exclusive access (EAP1,EAP2).

More detail about this classification is provided in TG6 [2012]. The IEEE TG6 proposes only one shared MAC to manage the channel access above the three physical layers. It combines both contention and contention-less access techniques to support the variety of data flaws that might occur in WBAN, such as burst, continuous and periodic traffic. The coordinator splits the time or the channel into a successive number of Superframes [TG6 2012; Cavallari et al. 2014; Movassaghi et al. 2014]. To access the channel, the coordinator chooses one of three access modes, these are illustrated in the following:

(1) *Beacon Mode with Beacon Superframe Periods*. Here, the coordinator sends successive beacon frames to specify the beginning and the end of the Superframe, which is referred to as the beacon period. The Superframe structure of this mode is presented in Figure 3. Table II provides more details about the MAC eaccss mechanisms that are offered by this access mode.
(2) *Non-Beacon Mode with Superframes*. No beacon frame is used in this access mode, and the superframe may only comprise either Type I phase or Type II phase as expained in Movassaghi et al. [2014].

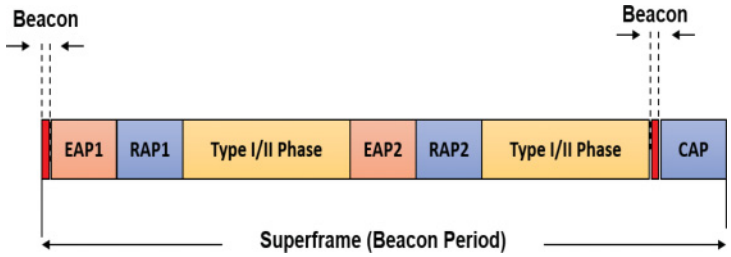

Fig. 3. IEEE802.15.6 beacon mode superframe structure.

Table III. WBAN Devices

WBAN devices	Functionality	Examples	
Sensor node	Samples and communicates physiological attributes and provides a response to the information through wireless communication for anybody, anywhere and anytime.	Wearable: added to clothes or placed on the body to collect vital signs.	Spo2, ECG, EEG
		Implantable: injected under the skin or in the blood stream.	In Parkinson's disease, sensors send electrical impulses to the brain through neural simulators
Actuators	Administer medicine to a patient when a sensor detects an abnormality according to the doctor's decision.		Control blood pressure, the body's temperature and to treat many other illnesses
Personal Device (PD)	Set up communication between a cellular phone sensors, actuators wirelessly.		Can be a specialised dedicated unit, PDA or a smart phone

(3) *Non-Beacon Mode without Superframes*. A coordinator follows an unscheduled allocation using unscheduled Type II poll allocation. Thus, each node specifies its time schedule in a distributive manner considering either Exclusive Access Period1 (EAP1) or Random Access Period1 (RAP1) as access phases, during which it competes for channel access following CSMA/CA.

From this brief description, it can be seen that these diverse channel access mechanisms offer the flexibility to support a variety of WBAN applications. However, the parametrization of the Superframe and the selection of the optimal solution is not an easy task and requires further study.

2.3. Types of WBAN Devices

As the name indicates, WBAN comprises tiny devices with communication capabilities. Based on their functions and roles, these devices are divided into three classes. This section presents a brief taxonomy of WBAN devices according to their functionality. This taxonomy is summarised in Table III.

2.3.1. Wireless Sensor Node. It comprises four components: transceiver, battery, microprocessor, and the sensor component. WBAN sensor nodes provide wireless monitoring for anybody, anywhere and anytime. These nodes can be physiological sensors, ambient sensors or bio kinetic sensors [Barakah and Ammad-Uddin 2012].

2.3.1.1. Wearable Sensors. These devices are added to clothes or positioned on the body to gather vital signs, such as the SpO_2 that measures the oxygen saturation

level in the human blood, which coincides with the cardiac cycle. The ECG sensor that investigates the heart function by sampling the heart muscle propagation electric waveform with respect to time. The EEG sensor that detects brain electrical activity and the motion detection sensors that combine both accelerometer and a gyroscope to monitor and analyse a person's movements [Khan and Yuce 2010; Crosby et al. 2012].

2.3.1.2. Implantable Sensors. These devices are injected under the skin or in the blood stream [Crosby et al. 2012]. In Parkinson's disease, for example, these sensors are used to send electrical impulses to the brain through neural simulators. Other applications for implantable sensors can be found in Garg et al. [2004] and Maloney and Santini Jr [2004].

2.3.2. Actuators. Actuators are used to administer medicine to a patient. The required drug is administered directly in a predefined manner when a sensor detects an abnormality or when it is triggered by an external source, according to the doctor's decision. Similar to a sensor node, an actuator consists of a transceiver, battery, memory, and the actuator hardware that holds and manages the drug. The drugs could be used to control blood pressure, the body's temperature and to treat many other illnesses. The actuator is activated upon receiving data from the sensors [Barakah and Ammad-Uddin 2012; Movassaghi et al. 2014].

2.3.3. Wireless Personal Device (PD). It is responsible for establishing communication between sensors, actuators and a cellular phone in a wireless fashion. Its main components are: a transceiver, a rich power source, a large processor and a large memory [Barakah and Ammad-Uddin 2012; Movassaghi et al. 2014].

3. CHALLENGES OF WBAN

As WBAN is a special type of WSN, it inherits many of its challenges. However, a number of new challenges characterise WBAN and a number of problems require better solutions. A survey of the differences between WBAN and WSN is given in Latr'e et al. [2011]. Practical adoption of WBAN could not be achieved without tackling the various technical, ethical and social challenges this type of networks faces. The main objective is to achieve a reliable, fault-tolerant network with minimum delay and maximum throughput while considering power consumption by reducing unnecessary communication. User requirements such as privacy, safety, ease of use, security and compatibility are also of great importance. The most challenging issues concerning WBAN are detailed in this section. This survey considers a wide range of challenges in WBANs. However, it is worth indicating that this survey will put a great deal of emphasis on the reliability challenges.

3.1. Power Consumption

Devices in WBAN are generally battery powered. WBAN has fewer and smaller nodes with smaller batteries compared to the other WSN, which adds more constraints on power consumption in communication [Wu et al. 2010]. The power required by nodes in WBAN varies according to the application type. All implanted nodes are required to operate for multiple years. Pacemakers, for example, need to operate for at least 5 years [Cavallari et al. 2014]. Therefore, it is essential to design ultra-low power radio transceivers. WBAN protocols have to be able to minimise power consumption without sacrificing reliability. A common technique is to allow devices to sleep for most of the time and thus lower the duty cycle. However, balancing between power consumption and average end-to-end delay should be considered. The first point to consider when choosing a wireless technology for WBAN is the power usage. WBAN peak power demands in idle mode vary between 0.001mW and 0.1mW and requires up to 30mW in

active mode [Movassaghi et al. 2014]. Wireless technologies focus on minimising the average current drawn from the battery by different means and techniques. Further improvements are necessary to reduce the drawn peak current in sensing technologies, radio hardware and integrated circuits. The issue of minimising interference and increasing WBAN lifetime by adopting transmit power control requires further attention. Some studies reviewed in the literature focus on scavenging energy from body heat or motion. Power consumption challenge is deeply discussed in Cavallari et al. [2014] and Movassaghi et al. [2014].

3.2. Heterogeneity of Devices

Since sensors in WBAN capture different kinds of data, reliability is a key issue. For instance, sensors vary in their sensed traffic rate as this depends on the application type and data to be sent. Bit rate values vary between less than 1kbps to 10Mbps [Cavallari et al. 2014]. Inherently, some sensors sense more critical data than others. Moreover, the same sensor might be in different states that vary in their criticality. Hence, the reliability grade may change dynamically at runtime [Wu et al. 2010]. For example, human temperature might be normal and requires a normal level of reliability, but when the temperature suddenly goes over or under the natural limit, the reliability requirement becomes much more rigorous. As a consequence, WBAN needs to dynamically guarantee reliability for the sensor nodes. Assuring a dynamic level of reliability for different sensors is a challenge of great importance. These factors, as well as sensor limitations, breakdowns and interference change the network operational conditions, which consequently leads to incomplete and erroneous sensor data [Ullah et al. 2012].

3.3. Reliability

A WBAN demands a high degree of reliability as it directly affects the quality of patient monitoring. Undetected life-threatening situations can lead to fatality. A main requirement is that the health care professionals receive the monitored data correctly. Thus, reliability is a crucial issue in WBAN. Reliability can be measured by the quality of the link or by the efficiency of end-to-end communication. In order to meet user expectations and achieve a reliable network, there are three basic characteristics that any network technology, programmed service and protocol needs to address: fault tolerance, QoS and security [C.N.A.P Staff 2013]. Designing protocols for unforeseen problems is an essential element of WBAN design because it is necessary that the WBAN operates continuously for users who rely on it. This requires that the architecture of a WBAN and its design techniques should be fault tolerant. A fault-tolerant network is the one that limits the effect of a failure, so that the fewest number of network components are affected [Kshirsagar and Jirapure 2011; Mishra et al. 2012; C.N.A.P. Staff 2013]. It is also built in a way that enables quick recovery when such a failure occurs. However, WBAN medical applications create higher expectations for the quality of the delivered services as for such applications any constant breaks, pauses, delays or packet loss could be fatal especially in emergency situations [Khan and Yuce 2010; C.N.A.P. Staff 2013]. Hence, QoS becomes an ever-increasing requirement of WBAN. Reliable QoS could be acquired by proposing well-designed protocols that can prioritise network traffic. Reliable QoS also means that that all packets arrive on time and in their correct order. This requires mechanisms that avoid or could manage traffic congestion. Network bandwidth measures the capacity of the medium to carry data that is the amount of transmitted information through the channel during a specific time.

When there are simultaneous multiple attempts in using the medium, the demand for the bandwidth outstrips its availability as the medium has to carry more than what the bandwidth can deliver. This leads to channel congestion. In most cases, when

the volume of packets is greater than what can be carried across the medium, data can be queued or saved in temporary memory until the resources become available. However, if the memory or queues become full, packets will be dropped causing packet loss. Packet loss could occur due to collisions in simultaneous packet transmission. For a WBAN, packet loss might lead to erroneous output and a life-threatening failure. It is understood that achieving the required fault tolerance and QoS by managing faults, the delay and the packet loss parameters on a WBAN becomes the secret to providing a successful solution for end-to-end application quality [Khan and Yuce 2010; C.N.A P. Staff 2013]. It can be concluded that, for WBAN, fault tolerance and QoS are correlated, and that in order to provide a successful and reliable solution for WBAN end-to-end applications, both fault tolerance and QoS should be considered side by side. The third requirement that should be addressed to achieve a reliable WBAN is security. Security in WBAN is fully addressed in Barakah and Ammad-uddin [2012], Chin et al. [2012], and Movassaghi et al. [2014].

3.3.1. Threats: Faults, Error, Failure. A threat is a violation of one or more of the system requirements. Some threats could be noticed without affecting the functionality of the system. Others could be noticed but negatively affect the system functionality as they violate the needs of the system. To understand the concept of fault tolerance, three types of threats should be differentiated, that is fault, error and failure. Any threat starts out as fault, it could be a physical hardware defect or a software defect. It could occur intentionally or accidentally [Mishra et al. 2012; Raghunath and Rengarajan 2013; Alrajei and Fu 2014].

If the fault is noticed, then it is called an active fault. One example of an active fault is the dead battery of a sensor [Alrajei and Fu 2014]. If the fault cannot easily be noticed, then it is called a *passive fault*, such as a bug in the code [Alrajei and Fu 2014]. If a fault occurs and remains unconsidered, it is possible that it extends and affects other system components and consequently becomes an error. The error is a noticed threat, which, once it occurs drives the system into the state of behaving wrongly [Bellalouna and Ghabri 2013; Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. In other words, an error is an active fault. If errors propagate, they can cause system failure. In this case, the system does not achieve the correct service it is supposed to offer. A service is a number of coherent system's external states. Suppose that one external state, at least, of the system deviates from the correct service state, a service failure is generated and the deviation is the error. For example, when a node depletes its energy due to a dead battery fault, a loss of connection with other nodes error occurs [Alrajei and Fu 2014]. The dead node is now not able to operate in the network and other nodes are not able to receive data from it. This means that an error is propagated within the network, leading to an abnormality in the network behaviour, which causes network failure. However, not all errors lead to an overall system failure as they are not able to affect the external state of the system, leading to other forms of failure that cause various modes of service failure.

Though the occurrence of faults does not necessary lead to system failure, it is essential to control faults from propagation to avoid system failure especially if system recovery, maintenance and repair are complex or impossible. When the system fails to offer a functional requirement, then it fails to offer one or more of its non-functional requirements [Alrajei and Fu 2014]. Thus, it is essential that the system continue working according to its non-functional requirement despite the occurrences of functional faults. This is the definition of fault tolerance.

To get a complete understanding of the concept of fault tolerance in WBAN, this section focus on the fault tolerance. It discusses and differentiates between different terms used in this field, namely faults, errors and failures. It presents a taxonomy of

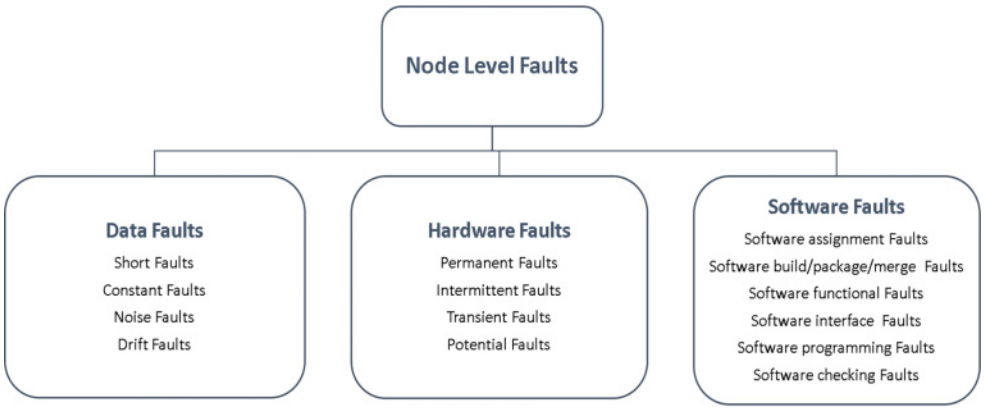

Fig. 4. Faults at node level in wireless communication.

different types of faults and failures that could occur in wireless communication. The management of the fault tolerance lifecycle is also illustrated in detail.

3.3.2. Classification of Faults. Like other wireless networks, a WBAN consists of nodes and communication links. Nodes are built from hardware components and software components. Limited resources and a harsh environment are just two examples of factors that can make sensor nodes prone to failure [Wu et al. 2010]. For a better understanding of the types of faults that might occur in a WBAN, faults are categorised into two general classes according to where they might occur: the node level and the channel level.

3.3.2.1. Node-Level Faults. The node is the basic network entity that is comprised of hardware components such as the transceiver, memory and microcontroller as well as the software components, such as the actual application programme installed in the microcontroller, MAC protocols, routing algorithms and so on [Mahapatro and Khilar 2011; Alrajei and Fu 2014]. Faults associated with nodes in wireless networks include data faults, hardware faults and software faults [Yu et al. 2007; Mishra et al. 2012; Bellalouna and Ghabri 2013; Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. Each one of those faults is depicted in Figure 4.

(A) *Data Faults*. This fault is related to an abnormality in sensor readings [Galzarano et al. 2012; Mishra et al. 2012; Raghunath and Rengarajan 2013]. Various reasons might cause data faults, for instance:
—*Short Fault*. This fault has a minor impact on the system and is noticed in the presence of a spike. It is called short because it is just a short-lived oscillation on the sensor reading signal [Mishra et al. 2012; Raghunath and Rengarajan 2013; Alrajei and Fu 2014].
—*Constant Fault*. This is an invariant repetition of random values, which are noticed as constant flat signals of sensor readings.
—*Noise*. This kind of fault makes sensors lose their data input and thus reduces the signal to noise ratio.
—*Drift*. When reading signals deviate from the original specification and persist, the error is considered as a drift error, which distorts the sensor data.
Data faults can be reduced by applying signal processing mechanisms that provide services to validate sensor readings [Galzarano et al. 2012].
(B) *Hardware Faults*. Hardware faults can be categorised in various ways, for example according to their duration. They can be classified into permanent, intermittent,

transient and potential faults [Mahapatro and Khilar 2011; Mishra et al. 2012; Bellalouna and Ghabri 2013; Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. These faults are described below:

—*Permanent Faults*. Permanent faults are continuously present and their effect remains stable until the source of the fault is removed, fixed or replaced. Manufacturing defects on sensor hardware components is an example of such faults.

—*Intermittent Faults*: These faults do not persist continuously, they occur and vanish frequently. Such faults cause a repeated faulty state of the network and, thus, diagnosing them is not a trivial process. They normally occur due to non-environmental conditions, for example, when a sensor loses link communication with others due to an aging sensor component.

—*Transient Faults also known as "soft faults"*. These faults occur due to environmental reasons such as temperature, humidity, pressure and so on. They occur less frequently than the intermittent faults as they present themselves one time and then vanish after which the system behaves normally. For instance, a sent packet might not be received by the sink due to some environmental reason, but it is very likely to be received successfully if it is retransmitted.

—*Potential Faults*. These faults occur when any of the node hardware resources diminish. They disable the functionality of the system as a whole. The system will not work again unless the deleted resource is substituted. An example of a potential fault is when a node dies when its battery is depleted and is considered useless unless its battery is recharged or replaced [Raghunath and Rengarajan 2013].

(C) *Software Faults*. The hardware of a sensor device works through software components. Analysing software faults is necessary as any bug in software functionality may disallow the sensor from completing the desired purpose [Raghunath and Rengarajan 2013]. However, such faults are rarely considered in the literature. In general, software faults are classified into six types of faults:

—*Software Assignment Fault*. This happens when the initialisation phase is handled incorrectly.

—*Software Build / Package / Merge Fault*. One example of this fault is the fault that occurs in system libraries.

—*Software Functional Fault*. Such faults happen due to errors in the design process of the system that allows it to misbehave, failing to offer the required functions.

—*Software Interface Fault*. This is a communication error between transmitter and receiver.

—*Software Programming Fault*. This is the deadlock which occurs in simultaneous operations.

—*Software Checking Fault*. This occurs due to wrong data code validation or bugs in software math.

3.3.2.2. Channel-Level Faults. Different factors can affect the communication channel between sensor devices. This includes interference, obstacles, weather conditions and signal strength [Wu et al. 2010]. The human body absorbs RF electromagnetic rays, this energy absorption leads to channel fading which adversely affects propagation paths [Ullah et al. 2012]. Transmission paths are also affected by reflection, diffraction, shadowing that occurs due to rapid body movement, body structure and posture. Body motion causes frequent changes in the network topology [Ren and Meng 2006; Ullah et al. 2012]. All of these factors lead to communication link errors which cause channel impairment. Channel impairment might lead to insufficient use of channel. This effect increases in an emergency because physiological information is normally correlated and in an emergency situation a group of sensors might be involved in

transmission. Even if every component of the WBAN is working properly when the emergency occurs, simultaneous transmission leads to collision and consequently to packet loss and maybe to a fatality [Liu et al. 2011; Rezvani and Ghorashi 2013]. As a conclusion, faults associated with channel in WBAN can be classified according to their causes into two boarder classes: channel faults due to human body nature and channel faults due to interference.

Human Body Nature. The human body can absorb RF electromagnetic waves that heat the surrounding tissues [Ullah et al. 2012; Movassaghi et al. 2014]. The body usually absorbs RF at a certain rate, namely the Specific Absorption Rate (SAR) that should be recognized under the umbrella of the regulations of the Federal Communications Commission (FCC) [Ntouni et al. 2014]. Besides tissue heating, energy absorption causes fading, which adversely affects propagation paths. Transmission paths are also affected by reflection, diffraction, shadowing due to rapid body movement, body size and posture [Ren and Meng 2006; Ullah et al. 2012; Movassaghi et al. 2014]. Body movement causes frequent change in network topology, which is a very complicated issue, as nodes might move with regard to each other due to the correlation between some moving parts of body. Fading effects lead to channel impairments. This affects sensor channel allocation strategies and even the common coding mechanisms mentioned in the literature to mitigate interference might not be sufficient. Channel impairments increase Bit Error Rate (BER) and cause unreliable data transmission as critical data might not be sent as expected and the doctor might mistakenly diagnose the patient which could be fatal [Movassaghi et al. 2014]. Moreover, the packet loss increases data retransmission which increases power consumption. In order to avoid this eventuality, the transmitting power must be as low as possible. Another important challenge is the antenna design in terms of height, size and material shape.

(A) *Interference and Coexistence*. Interference is one of the drawbacks of WBAN that crucially needs to be addressed. The requirement to support per body up to 256 devices in the WBAN, and the coexistence of up to 10 WBANs in $6\times6\times6$ meters (TG6) [2012] lead to critical interference scenarios in WBANs due to the presence of diifrent sensors the belong to different bodies within the same range [Alam and Ben Hamida 2015]. Another interference issue in WBANs rises from the coexistence of other signals related to, for instance, Wi-Fi, Zigbee, and Bluetooth etc. This can take place in a small volume and within the same frequency band used by WBANs, e.g., ISM band [Lo Bello and Toscano 2009]. Therefore, limited number of channels has to be shared between these different technologies and this will lead to severe inter-network interference that may affect the neteork reliability and deteriorate the performance of the network when used in E-Health related applications [Dakun et al. 2015]. Hence, the life of a patient whose health status is being monitored may be in danger in emergency scenarios where a triggered alarm should be sent from the sensors connected to the body of the patient to a monitoring application at a remote location. This issue motivates the need to fully understand the network coexistence problem and the impact of Interference on WBANs in different bands of frequency used by the IEEE 802.15.6 standard in order to provide efficient and effective interference mitigation and coexistence schemes [Wang and Cai 2011].

Erroneous outputs due to channel faults might result in life-threatening situations. These conditions adversely affect WBAN reliability and performance.

3.3.3. Classification of Failures. As explained in Section 3.3.1, failures are a normal consequence of faults that might occur at node and channel levels [Mishra et al. 2012; Bellalouna and Ghabri 2013; Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. The overall system might stop working due to one of the following failures:

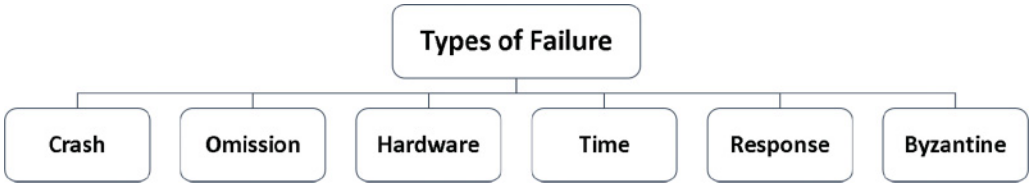

Fig. 5. Types of failures in wireless communication.

—*Crash Failure*. When there is no response to a certain request, it is likely that the network has suffered a crash failure. This might occur due to messages loss or due to physical damage, which disjoins the sensors from the network. When this type of failure occurs, there is no further output as the process remains halted.
—*Omission Failure*. This occurs as a result of transmission faults when the system fails to respond to incoming queries due to a limited buffer size. Incoming and outgoing messages fail to be processed. Receive and send omissions are called channel omissions.
—*Hardware Failure*. This is a consequence of hardware faults that occur in hardware components mostly due to environmental reasons as mentioned previously. Hardware failure might lead to node software failure.
—*Time Failure*. This is a periodic operational behaviour of the network. In this case, the nodes successfully respond with a message but the message is received too late or too early according to the specified message time interval. Thus, the synchronous real-time system responds outside the range of the required time interval.
—*Response Failure*. This failure occurs when nodes send messages successfully and in time but the message contains incorrect reading information. This might happen due to malicious attacks, noise, software malfunction and many other reasons as specified previously. Consequently, the accumulated results would be inaccurate which will reduce application reliability. There are two types of response failure. If the system responds with faulty replies, then this is a value failure. If the system responds with unintended action at wrong time to handle a collapsed control flow, then this is called a *state transition failure*. It generates irrelevant information as a response.
—*Byzantine Failure*. If the system generates random values at random times, then it is considered as byzantine failure. Managing such failures is messy, as during processing, this failure neglects the required processing measures and follows unintended processing. This consequently produces corrupted messages or concurrent channel usage due to multiple message transmission. Types of failures are summarised in Figure 5.

3.3.4. Fault-Tolerance Life Cycle. Eliminating the occurrences of threats in the system could not be achieved without predicting the occurrences of faults that could potentially happen in the system [Alrajei and Fu 2014]. Eliminating faults will prevent system failure. Fault tolerance requires fault prediction. First, the possibility of a fault occurring needs to be predicted and an attempt made to prevent it [Yu et al. 2007; Mishra et al. 2012; Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. If it cannot be prevented, then at least a guarantee should be built into the system to allow it to operate in the presence of that fault. This is the second level and requires the system to be aware of how to react in the presence of faults so as to avoid the failure of the overall system services. This level comprises fault detection, isolation, fault identification and fault recovery [Yu et al. 2007; Mishra et al. 2012; Raghunath and Rengarajan 2013; Alrajei and Fu 2014].

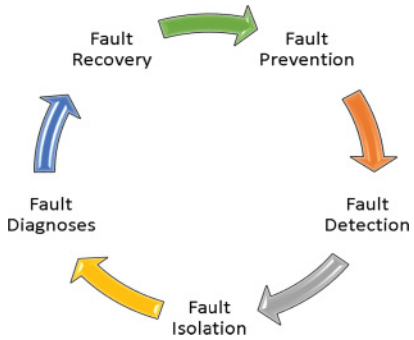

Fig. 6. Fault tolerance life cycle.

Fault tolerance aims to eliminate threats of the system by finding ways to allow the system to survive and to continue operating in the presence of errors according to its design goals without deteriorating the performance of the services it is supposed to offer. Fault tolerance could be achieved through two methods. The first method is fault masking, that is to hide faults and prevent them from extending to errors [Alrajei and Fu 2014]. The second method is fault isolation that is to remove the fault or the source of fault from the system either manually or automatically. Each step in the lifecycle of fault tolerance as well as in choosing the method is considered to be a research topic on its own and depends on the application and the criticality of faults. This subsection illustrates each step in the fault tolerance life cycle. The steps of fault tolerance life cycle in wireless communication are depicted in Figure 6.

3.3.4.1. Fault Prevention. This avoids the occurrences of faults and takes place in three stages of the WBAN application, as follows [Mishra et al. 2012; Raghunath and Rengarajan 2013]:

—*Specification Phase*. This phase must ensure that incomplete and equivocal specifications are avoided.
—*Design and Deployment Phase*. The design of the network topology, connectivity and link coverage must be insured during this phase. This phase also includes the necessity of choosing RF and hardware components with a suitable wireless standard in terms of quality, reliability and flow.
—*Monitoring Phase*. To constantly watch out for the status of the network for functional degradation and incorrect usage of resources by monitoring node status, link quality and the level of congestion and take reactive action when necessary.

3.3.4.2. Fault Detection. Due to the dynamic nature of wireless communication, fault prevention does not guarantee 100% prevention of faults [Yu et al. 2007; Mishra et al. 2012; Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. Therefore, a detection phase is required to identify the unexpected fault in the network. Basically, fault detection can be categorized as online and offline detection.

—*Offline Detection*. This is often applied in wired networks using special programmes during the idle time of the network.
—*Online Detection*. Online detection is real-time detection and is adopted in wireless networks. It is classified into explicit and implicit detection.
  (A) *Explicit Detection*. This is an application-specific fault-detection technique. It is performed by sending an alarm when the event/action is detected. For example, in WSN, there is a predefined threshold used to detect the misbehaviour

of sensing applications [Yu et al. 2007]. These conventional threshold tests are unsuitable for WBAN fault detection, since WBAN is characterised by the complexity of a heterogeneous sensing environment [Mahapatro and Khilar 2011]. The hybrid resource capabilities of nodes in terms of their resource capabilities, installed software, and data rates limits the adoption of a fixed threshold to check their status in WBAN. For example, ECG and SpO_2 sensors sample different readings and detection of the faulty nodes by comparing energy levels might deliver inaccurate results. Moreover, medical sensors might be introduced under various situations, such as normal situations and emergency situations. For example, temperature readings might be higher or lower than the average normal temperature, which could be life, threatening. Consequently, WBAN has two levels of variation in the reliability requirements of its sensors: amongst heterogeneous sensors and within the same sensor, as it might run in different situations. In addition, high threshold values lead to several missed detections, while values that are too low result in false positives. Thus, adopting a constant or fixed threshold value for overall WBAN components may not function well if the properties of the sensors vary, or if the scene and the environment change, because it generates faulty observations, which produce unsatisfactory results. For WBAN, explicit detection can be classified in to two types which are:

—*Anomaly Detection of Abnormality due to Malfunction of Sensor Node*. Detection can be done by measuring the average receiving rate of the previous data and comparing the result to a predefined dynamic threshold. It is necessary to classify the level of critically of the malfunction sensor because action is taken according to its level [Jeong et al. 2014].

—*Anomaly Detection due to Human Body Abnormality*. This kind of detection reflects that there is a problem in the human body that could be life threatening. This requires a detailed set up since each medical situation has its own parameters and requires a different response. This kind of detection can be further classified into: detection of an accidental change in the body medical data and the detection that medical data reached a threshold or a reference value [Jeong et al. 2014].

(B) *Implicit Detection*. This type of detection requires overall network management because it targets faults that happen due to abnormal phenomena such as vulnerable environment conditions [Yu et al. 2007]. There are two ways to adopt implicit detection: active and passive detection which are discussed below:

—*Active Model (Proactive)*. In this model, nodes send continuous messages to a central controller to indicate that they are still alive. If a certain specified time period has elapsed without receiving a message from a node, the controller can tell that the node is dead [Yu et al. 2007; Mishra et al. 2012; Alrajei and Fu 2014].

—*Passive Model (Reactive)*. In this model, a node sends the alarm to the controller only when a fault or network corruption is detected. In this case, nodes save energy as they are requested to send keep alive messages constantly to the controller, thus they stay inactive most of the time.

Figure 7 summarises different types of online fault detection in WBAN in particular.

3.3.4.3. Fault Isolation. After the fault is detected, it is necessary to analyse the nature of that fault in terms of its type, behaviour, and characteristics. A procedure should be followed to isolate that fault [Yu et al. 2007; Mishra et al. 2012; Raghunath and Rengarajan 2013].

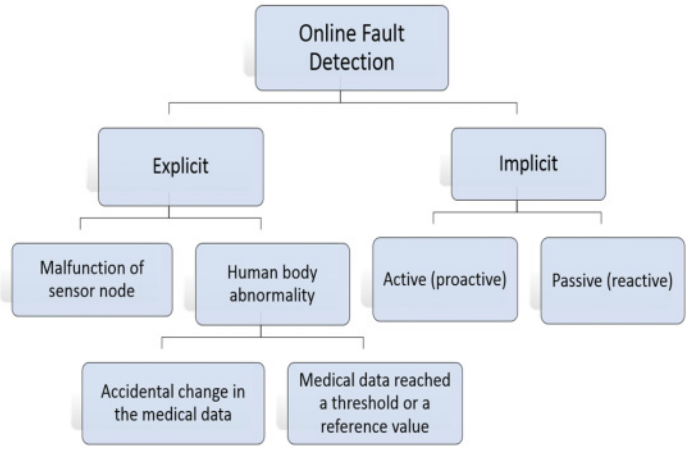

Fig. 7. Fault detection in WBAN.

3.3.4.4. Fault Diagnosis. Fault diagnosis is essential to properly identify the isolated faults in terms of their characteristics and behavioural nature. Faulty nodes should also be distinguished from suspicious nodes and from other irrelevant triggers. This could be achieved by applying historic data and sharing knowledge. The state-of-art fault solution models either manage faults at the component level of the node or at link communication level between nodes. However, although there are several accurate fault detection techniques, there is no comprehensive model to comprise accurate fault diagnosis and fault recovery approaches [Yu et al. 2007; Abedi et al. 2011; Mishra et al. 2012; Raghunath and Rengarajan 2013].

3.3.4.5. Fault Recovery. In this phase, the network is restructured and reconfigured to minimise or stop the detected faults from generating further impact on the network. Fault recovery techniques are classified into two broad areas according to the type of fault: the recovery of faults that might occurred at sensor node level and the recovery of faults that might occur at channel level [Yu et al. 2007; Mishra et al. 2012, Raghunath and Rengarajan 2013; Alrajei and Fu 2014].

(A) Node-level recovery: In this case, the first approach is to directly isolate the failed node from the network, such as isolating it from routing communication [Yu et al. 2007; Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. In clustered networks, if the failure occurs in the cluster head (CH), then its nodes members join the neighbour clusters. Conventional WSN fault tolerance techniques follow sensor replication by deploying redundant sensors through following appropriate redundancy mechanisms. For example, WSN was commonly used to sense a region and emit the sensed data to the sink. If a node fails to provide the correct data, the sink receives the correct data from the redundant deployed nodes [Liu et al. 2009]. However, unlike WSN, WBAN is considered a sparse communication network because of the short area communication space and the limitations on the number of nodes, thus, there is no way to establish packet redundancy. Moreover, adding extra sensors increases the interference among sensors and might be stressful [Mahapatro and Khilar 2011]. Nevertheless, it is worth indicating that our types of redundancies that are commonly followed in WSN, are as follows:
—*Hardware Redundancy*. This is achieved by adding extra physical components, such as additional sensors, additional batteries and so on [Raghunath and Rengarajan 2013; Alrajei and Fu 2014].

—*Software Frequency*. This is done by replicating software code. For example, software components can be allowed to reconfigure the management of the software. Another technique is using mobile code technology.

—*Time Redundancy*. This is done by repeating the required processes multiple times.

—*Information Redundancy*. Two ways to achieve information redundancy are:

—*Active Replication*. This technique allows all replicas to process all requests. A failed node is recovered by duplicating its information by distributing redundant sensed data to other nodes. Thus, each node requires extra memory space to buffer its own data and even the data and the replicas for other nodes. Redundant copies are used to recover the failed sensor data. Beside the extra memory hard requirement, this approach is prone to high message communication overhead in sending the update messages [Mishra et al. 2012; Raghunath and Rengarajan 2013].

—*Passive Replication*: This allows only a single replica to process a single request, and other replicas are allowed to process the request only when the current replica fails to.

(B) *Channel-Level Recovery*. A fault-tolerant system should be able to tolerate channel impairments. Finding ways to coordinate channel usage among nodes according to their criticality is one solution. Distinguishing nodes' criticality means assigning them different priority levels [Wu et al. 2010]. Sensors that are used in WBAN are usually classified into two parts: medical sensors that are used to sense physiological information and non-medical sensors that are used to sense environmental information [Liu et al. 2011; Rezvani and Ghorashi 2013]. It is always the case that, while some medical sensors work in their normal situations, other medical sensors might suddenly require high QoS and exclusive resources when emergent situations occur. In this case, it does not make sense to provide all sensors in WBAN identical conditions and resources because less important data might be achieved before the critical one resulting in unreliable and an untrustworthy, erroneous WBAN. To avoid this, nodes in emergency situations must transmit their data as fast as possible and should be assigned enough bandwidth to allow the complete information achieved in a real time, even if this would be at the expense of other less important information sensed by those nodes which work in normal situations or which sense environmental information. What makes the problem worse is that, despite the heterogeneity of WBAN sensor nodes, their sensed data is correlated. For example, both the ECG and hemodynamic signals, such as blood pressure, have information mutually correlated due to the physiological inter-relation of the mechanical and electrical functions of the heart [Mahapatro and Khilar 2011]. Moreover, physiological information also has a direct correlation with environmental information. It is mentioned early in this section that due to this correlation nodes might produce erroneous results in emergency situations as nodes will try to transmit simultaneously. This all-at-once data transmission leads to collisions, which consequently increases packet loss and produces erroneous results. This could lead to fatal situations. This emphasises the necessity of prioritising nodes according to their situation, and according to the type and the criticality of the data they sense [Wu et al. 2010]. Various approaches can be adopted to assign priorities for heterogeneous nodes in different situations. The commonly used one is to check the nodes' situation according to a specified threshold [Mahapatro and Khilar 2011]. To overcome the channel interference problem, other adaptive channel allocation approaches are required to enable successful coexistence between the various communication technologies that might coexist in the area [Zhou et al. 2011; Wu et al. 2010]. Dynamic channel switching can be followed according to the standards adopted. Adaptive channel allocation to solve coexistence problem is beyond the remit of this research.

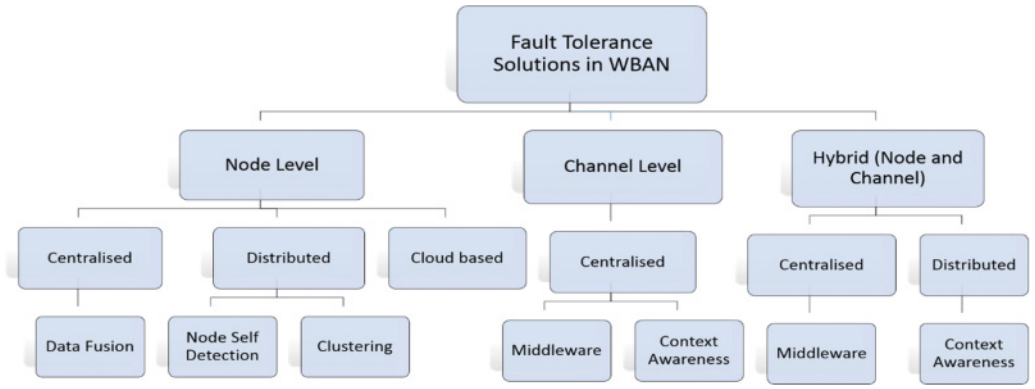

Fig. 8. Fault tolerance solutions in WBAN.

4. SOLUTIONS FOR FAULT TOLERANCE

WBAN should provide measurable, predictable and, when necessary, guaranteed services. To ensure this and improve the reliability, a tremendous amount of work has been proposed in the literature. Studies to date typically seek to improve QoS and find ways to achieve a secure WBAN, however, few works addressed the fault tolerance issue. Each proposed approach aims to tackle fault tolerance from its own perspective. Nevertheless, there is no work standing firmly enough to address all types of faults or the entire life cycle of fault tolerance in WBAN. The taxonomy of WBAN fault-tolerance solutions which are going to be illustrated in this section are depicted in Figure 8. This section examines recent literature pertaining to achieving a fault tolerant and high QoS WBAN. Interference is classified earlier as one of the sources that causes channel faults and which has a huge impact on WBAN reliability. Interference however, is a wide topic and has huge research directions by its own. Therefore, interference management solutions are added as separated subsection in this section. As detailed in Section 3, fault prevention is considered in reference to network specification and topology deployment during the early design stage when developing a network [Raghunath and Rengarajan 2013; Alrajei and Fu 2014]. The proposed protocols aim to prevent faults by monitoring node status, link quality and level of channel congestion [Alrajei and Fu 2014]. The majority of work focuses on proposing fault detection techniques, omitting the necessity of fault recovery [Zhou et al. 2011; Otal et al. 2009; Ali et al. 2010; Wu et al. 2010; Liu et al. 2011; Rezvani and Ghorashi 2013]. Literature varies between proposing generic algorithms [Zhou et al. 2011; Wu et al. 2010; Mahapatro and Khilar 2011; Galzarano et al. 2012; Abarna and Venkatachalapathy 2014], MAC protocols and enhancements to existing wireless standards such as IEEE 802.15.4 [Otal et al. 2009; Rezvani and Ghorashi 2013], IEEE 802.15.4a [Liu et al. 2011], and IEEE 802.15.6 [Liu et al. 2011]. A number of the proposed fault tolerance approaches are targeted towards node faults in WBAN, others are geared towards coping with channel vulnerability regardless of nodes abnormality, but very little consider both node and channel levels impairments. According to the literature reviewed, this survey classifies fault tolerance approaches in WBAN into three broadbands according to the type of fault level they consider, namely fault tolerance approaches at node-level, fault tolerance approaches at channel level, and fault tolerance approaches at both node and channel levels. Each one of these three classes is further classified into two major categories: Centralised approaches and Distributed approaches. Several techniques that follow the centralised manner have been suggested, such as performing data fusion [Mahapatro and Khilar 2011],

adopting a specialised layer [Zhou et al. 2011; Mahapatro and Khilar 2011, Galzarano et al. 2012], following clustering techniques [Abarna and Venkatachalapathy 2014] and developing context awareness [Liu et al. 2011; Rezvani and Ghorashi 2013]. Yet, there are also a distributed middleware and context aware techniques that are classified under the category of the distributed approaches. A new trend that is neither centralised nor distributed, which is based on the cloud is also considered in this survey as one of the fault tolerance techniques proposed to cover node-level faults.

Due to the limited communication space of WBAN, it is inappropriate to adopt sensor replication as a recovery technique, thus, the majority of those techniques consider isolating and replacing faulty nodes as a recovery method [Mahapatro and Khilar 2011; Galzarano et al. 2012; Abarna and Venkatachalapathy 2014; Jeong et al. 2014]. This review emphasises that achieving both fault tolerant and high QoS is a key concern in WBAN. It also suggests some trends to adopt in order to achieve more accurate, feasible, real time and efficient fault tolerance framework for WBAN.

4.1. Fault Tolerance Approaches at Node Level

Approaches that fall within this band are typically limited to those which occur in WBAN nodes. Those approaches do not consider channel vulnerability due to body or surrounding environment, they however, detect and deal with abnormalities that occur at the node level due to data faults, hardware faults as well as the abnormality in body physiological information. Approaches followed in literature in this realm are categorised into centralised, distributed, and cloud-based approaches. WBAN studies that have adopted such techniques are presented in the following subsections.

4.1.1. Centralised Node Fault Detection using Fusion Centre. In the centralised approaches, network faults are managed by one node, which is the central controller, sink or base station. In this way, complex computations and processes are shifted from resource constrained nodes and performed by a resource rich node, in order to increase power efficiency [Yu et al. 2007; Kshirsagar and Jirapure 2011]. Active detection is normally considered a centralized approach as the central node receives periodic and constant messages that indicate the situation of the nodes and network by sending queries to make inferences about the network and the individual nodes' statuses used by the controller to identify both failed and suspicious nodes.

One centralised node fault detection is based on data fusion techniques. In this approach, a specific node aggregates the decisions from the remaining network nodes [Yu et al. 2007]. This so-called data fusion node can determine the abnormal status of other nodes by comparing data from a set of nodes. This technique is very efficient, especially for data centric applications that require detection precision, to manage the number of recovered sensors and the communication costs. However, there must be a balance between the accuracy of the detection and the network's energy consumption.

The work in Mahapatro and Khilar [2011] is the only work found in literature that is based on a centralised data fusion fault detection in WBAN. A PDA provides continuous data transmission and performs real-time analysis of physiological sensor data. PDA derives relevant physiological information from sensor data, according to which it diagnoses faulty nodes. Time redundancy can be used to address the detection of intermittent and permanent errors. Mahapatro and Khilar [2011] observed a tradeoff between choice of the time detection parameter T, and the latency and accuracy of the error detection. However, it is important to note that there must be some level of context awareness before the data fusion centre can generate results. For example, an increase in heart rate does not necessarily mean a patient is having a cardiac episode, the patient might be engaged in some form of sport (for example, running) and that causes a change in their physical activity level. Such critical issues

were neglected in this work. Changes in the internal and external states of the body can be analysed according to triggering events [Korel and Koo 2007]. Moreover, as a centralised technique, this technique is prone to a single point of failure, as the error detection is performed by a centralised PDA, and no discussion was made of what would happen if the PDA crashes or produces faulty results. There can be several fusion sensors, the number of which depends on the requirements of the area, in terms of the communication range between nodes and the region of the application of interest. Although the physiological information extracted is used to decide the occurrences of faulty nodes, it could be argued that the information extracted could be used for temporary recovery, such as by substituting one piece of information for another, allowing a temporary flow of information. This temporary recovery continues until permanent action can be taken such as node isolation and replacement.

Although centralisation is considered an accurate and efficient approach, its major drawback is the failure of a single central node to manage everything. This is because the central node is prone to data traffic concentrations, which leads to rapid energy depletion in the controller [Yu et al. 2007; Kshirsagar and Jirapure 2011]. Moreover, in multi-hop communication, nodes close to the central node will forward more communication messages to the central node, which will also cause early energy depletion in those nodes leading to what is called the hot spot problem. The single point of failure problem requires adoption of a distributed fault detection model.

4.1.2. Distributed Node Fault Detection. To relax the pressure of duties, the central controller is responsible for avoiding the problem of single point of failure, level of fault detection is shifted to local nodes by allowing them to report the awareness of their status, thereby enabling them to take decisions [Yu et al. 2007; Kshirsagar and Jirapure 2011]. Obviously, this minimizes the number of messages the nodes are required to transmit to the central node, which reduces the energy consumption and network congestion. Generally, distributed techniques can be fully adopted selflessly at each node, by allowing the node to diagnose malfunctions in its physical hardware components. Distributed fault detection can be adopted by following clustering techniques. A common distributed detection approach in WSN, is the coordination between neighbours. However, such a technique has yet to be considered in WBAN. The three distributed fault tolerance techniques in the literature are given in the following discussions.

4.1.2.1. Node Self-Detection. Nodes are allowed to self-detect faults, taking decisions about their own status without the need to consult the coordinator [Yu et al. 2007; Kshirsagar and Jirapure 2011]. One approach presented in literature for distributed self-detection in WBAN is by adopting a middleware layer in each node to be responsible for detecting and possibly recovering faulty status, without the need to rely on a certain node to perform complex computations. A middleware is a layer that acts as a bridge between the conventional network stack layers, to perform some functionality and provide some services that are not provided by the current stack layers, without violating the traditional layers' tasks [Wikipedia The Free Encyclopedia 2015]. In this technique, a set of software modules are used in each sensor node to perform tasks beyond those the legacy stack layers perform.

One work that uses a separated layer for node fault detections is presented in Galzarano et al. [2012]. Galzarano et al. [2012] concentrated on data faults in WBAN, by analysing the level of decreased accuracy after applying four types of data faults to readings acquired by sensors in a human activity recognition application. Galzarano et al. [2012] studied the impact of faults on the quality of that application. Those faults are: short faults, noise, constant faults, and accumulative faults. Galzarano et al. suggest that the reliability of WBAN can be enhanced by adding autonomic elements that perform self-healing operations, and thus enhance data fault tolerance.

The idea is realised by adopting a self-healing layer with the aim of detecting and recovering from such situations. The layer is based on the Signal Processing In-node Environment (SPINE) framework [Bellifemine et al. 2011], which is built on top of the existing SPINE2 framework [Galzarano et al. 2012]. Experimental results confirm that the defined autonomic elements can mitigate faults affecting the sensor data, and improving the system behavior correctness [Galzarano et al. 2012]. However, this technique is based on image-processing algorithms that require complex processing capabilities, and resource rich devices which are not suitable for energy constrained sensor nodes. Moreover, Galzarano et al. [2012] considered only one type of data fault, short faults. The accuracy and performance of the self-healing layer should be proven by testing it in reference to the occurrence of other types of data faults.

4.1.2.2. Clustering Detection. This technique distributes fault management, by dividing the network into groups of clusters where distributed fault management is adopted for each group. Thus, a virtual Skeleton communication is created [Yu et al. 2007]. Centralisation is adopted in each cluster head (CH), which is then becomes responsible for detecting faults by exchanging messages with the members of its group. Identification of faulty nodes can be achieved by applying a pre-defined failure detection rule to each CH. The information detected can be propagated to all other clusters through a gateway, which is considered a neighbour to two CHs from different clusters. Hence, the overall network is managed through self-aware clusters [Yu et al. 2007]. A study following this approach in WBAN is presented in Abarna and Venkatachalapathy [2014]. Abarna and Venkatachalapathy [2014] tried to alleviate a drawback of single of point of failure, as presented in Zhou et al. [2011] and Wu et al. [2010]. To achieve this aim, Abarna and Venkatachalapathy [2014] followed a cluster-based approach to fault tolerance in WBAN. Abarna and Venkatachalapathy [2014] applied a hierarchal architecture, where each group of physiological nodes are connected to one CH. The CHs are interconnected and connected with a Wireless Local Gateway (WLG), which is linked with a Hospital Gateway (HG). Then, each CH assigns priority values to its nodes that reflect their fault tolerance level according to three pieces of aggregated information: physiological collected information, environmental information, and the node's physical status. The three values collected are then compared with three threshold values and node priorities are assigned accordingly. Nodes with a high priority are processed first. A scheme for CH fault detection and recovery is also proposed. However, although this work considers three threshold values, it has not been shown why, how and what the chosen values are. Once again, the threshold test is not suitable for fault detection in WBAN, as it is characterised by the complexity of heterogeneous sensors that might follow different critical cases requiring different dynamic thresholds. Moreover, it considers WBAN as a homogenous network comprising homogenous sensors in terms of data rate, packet size, capabilities and physical status. For this reason, Abarna and Venkatachalapathy [2014] suggested that, in case of a CH failure, its members can associate with any other CH, as all CHs achieve identical processing and capabilities and are all provided with the same threshold values. However, this assumption is irrational for WBAN, as it has a characteristically heterogeneous nature. On homogenous networks, when a fault occurs, all the CHs might discover the faulty node, and thus will send failure information simultaneously, leading to collision and packet loss. The increased use of control packets between CHs adds an extra overhead, which might cause congestion on the channel.

While Abarna and Venkatachalapathy [2014] claimed that their technique reduced control overheads and energy consumption rates significantly, they have not considered the power consumption in their performance evaluation. Clearly, this work adopts a level of redundancy to recover the controller failure by adopting several CHs. Adopting

such an approach in WBAN, which is considered a very short scale network, is not trivial. Indeed, an intensive study and in depth analysis is required concerning the optimal number of CHs, their position on the body, as well as the number of maximum sensors in each cluster. In addition, this work does not specify the action to be taken after assigning priorities to nodes, if the only action was to wait for faulty node isolation, there would be a huge delay before the faulty node could be replaced which could be fatal in an emergency situation. Thus, there must be a real-time recovery mechanism in place, even if this is considered as temporary solution, such as the previously presented data fusion technique.

4.1.3. Cloud-Based Node Fault Detection in WBAN. Cloud-based fault detection in WBAN is neither a centralised nor a distributed approach, as both the node and the controller are not responsible for tracking the node's status or performing a reactive response. A third party, outside the WBAN, achieves fault tolerance, i.e., the cloud-computing Infrastructure as Service (IaaS)-based application. Jeong et al. [2014] proposed a visual monitoring system (VMSFT) to monitor patient's conditions and to tolerate sensor failures immediately. The work presented in Jeong et al. [2014] differs from other works, as it considers a large number of WBAN adopted by multiple patients simultaneously, therefore, it is considered a local monitoring system for a group of people within target area. VMSFT obtains patient's data through the IaaS application and according to this data, it can infer sensor failure. This work performs two types of explicit anomaly detection, anomaly because of sensor failure, and anomaly because of a problem in the human body. VMSFT can provide three responses according to the criticality of the detected sensor anomaly. The level of criticality is assigned according to the position of the sensor in the body. A high level is assigned for sensors close to the heart, and a low level is assigned to hands and leg sensors. All other sensors are assigned to the middle level. If VMSFT is connected to an emergency room, it is possible to care for patients proactively. High-level cases are sent to emergency room as well as to managers, middle-level incidents are sent to managers, but if a delayed response is expected according to a specified time, calls are sent to the emergency room, whereas a low-level response incidents are monitored periodically by the manager. However, for abnormalities in the human body, if data changes abruptly, status is sent as an emergency directly, but if the body data approaches a specified reference threshold, the GP is informed to prompt a suitable proactive response. A hierarchical scheme is suggested for management within a cloud service infrastructure. However, Jeong et al. [2014] considered the position of the sensor as a criterion to decide the criticality of the data readings. Sensors positioned on the body extremities have a lower priority in triggering an emergency response, as their readings are of lower criticality than other sensors, for example, those placed close to the heart. It is very popular, however, for sensors being used to detect heart rate to be placed on the hand. Thus, other criteria must be applied to decide the level of criticality. Moreover, cloud computing–based applications for WBAN cannot be adopted, unless there is a full guarantee of trustworthiness, which is still a major drawback of cloud computing, as level of privacy and security are not wholly determined.

4.2. Fault Tolerance Approaches at Channel Level

The approaches that fall within this band are typically limited to channel-level impairments that occur in response to the body and environmental changes, and does not consider node-level faults. In other words, they consider nodes as fault free. Approaches found in literature for detecting and dealing channel vulnerability are generally centralised. Some approaches enable the controller to perform some level of context awareness to classify traffic according to the importance of the sampled data, to

improve network QoS and to tolerate channel impairments [Ali et al. 2010; Liu et al. 2011; Rezvani and Ghorashi 2013]. In other approaches a controller might adopt an extra layer or middleware that prioritises traffic, tolerate and manage the channel's vulnerability [Zhou et al. 2011; Wu et al. 2010]. Such techniques are presented in the following subsections.

4.2.1. Centralised Context Aware Fault Detection. According to Korel and Koo [2007], context refers to any information that characterises an entity's situation. Context awareness is the ability to diagnose entities' internal or external states. To achieve a fault tolerant WBAN, the entity for which the context needs to be analysed is the sensor node. More generally, context-aware WBAN is a network in which wearable and implanted sensors' situations can be described in accordance with the surrounding environment, according to which, their behaviour can be modified. As stated previously, WBAN has several challenging characteristics, one of which is its vulnerability to context and environmental changes [Wu et al. 2010]. Contextual changes include the body's motion and activity, and the temperature of the surrounding environment among others. Such factors affect the reliability of the network. Context awareness can assist in the interpretation of any physical and physiological data being monitored, and accounts for the current situation as it affects the body and the surrounding environment. Thus, it can be used as a method to determine tolerance to impairments that might occur in the network channel. Therefore, context awareness plays a key role in WBAN, by enhancing reliability and helping to facilitate long-term system monitoring. Supervision of the context awareness process in terms of data gathering, classification of context, transitions and events, and extraction of context recognition, can either be centralised at a single resource rich sensor node (usually the controller), or implemented in a distributed manner to a certain level at the resource constrains nodes. This subsection presents literature that has adopted centralised context awareness for fault tolerance in WBAN at the channel level.

Rezvani and Ghorashi [2013] studied the channel impairments that might occur in WBAN, because of fading and body postures which cause packet loss in a star topology. Rezvani and Ghorashi [2013] considered both medical and other types of applications, proposing an adaptive channel allocation superframe-oriented MAC protocol for WBAN. The proposed protocol supports the heterogeneous characteristics of different applications by separating medical and non-medical applications. Moreover, Rezvani and Ghorashi [2013] considered correlations that may occur in medical traffic in emergencies and splits that traffic into normal and emergency medical traffic. The separation between non-medical, normal medical, and emergency medical traffic is adaptive, according to channel condition and the user's medical situation. As medical data is usually periodic, and in order to improve the efficiency, medical nodes can follow TDMA synchronisation. However, because non-medical data is flexible, it follows that there is a contention-based access mechanism for traffic transmission. Moreover, according to the condition of channel deep-fading, the interval between consecutive transmissions changes adaptively. To summarise, the proposed protocol tolerates channel faults by adapting the channel allocation to the classified sampled data that consider fading effects. The proposed algorithm outperforms both IEEE 802.15.4 and IEEE 802.15.6 MAC in terms of reliability, channel utilisation, and power consumption; this is because of the successful data packets transmission due to the adaptive resource allocation.

However, although Rezvani and Ghorashi [2013] considered emergency traffic, it does not explain the classification process applied for different types of traffic (for example, if they followed a threshold comparison mechanism). The proposed protocol still follows the CSMA mechanism in emergency situations, and while it is considered a smart solution for WSN, it does not guarantee collision avoidance in WBAN, which

would adversely affect reliability and therefore be fatal in emergency situations, and thus other channel access mechanisms must be proposed for contention-based channel access in WBAN. Moreover, context awareness computation is centralised and performed by a slot sent by the hub itself, this leads to the common problem, namely a single point of failure. Notice that, the slot in the hub examines the channel to check if it is busy or not. If it is busy, then it decides there is an emergency situation. This mechanism, however, must be sufficiently robust to consider all types of nodes in the network. For example, context awareness can be performed in a distributed manner throughout all WBAN nodes; this cannot be achieved unless nodes are allowed to adopt cross layering approaches to a certain level, at all stack layer levels. The core problem discussed is the occurrence of collisions in emergencies, due to the correlation in medical data. However, data correlation could also be considered as a feature to harness to improve WBAN fault tolerance. For example, the data fusion technique discussed in the previous subsection can be adopted to provide a temporary solution to recover information from some faulty nodes.

Liu et al. [2011] proposed a hybrid superframe-based MAC protocol (CA-MAC) that allocates transmission bandwidth according to WBAN context. CA-MAC adjusts the transmission priority and access strategy according to the traffic and channel status, respectively. The CA-MAC protocol changes the duty cycle according, adaptively, to human activity, or environmental conditions, while also considering power consumption to prolong the network's lifetime. CA-MAC comprises three parts: the beacon frame, the contention-based period that adopts the slotted CSMA/CA and which changes dynamically according to the level of fading in the channel, and the third part is the contention free period which follows the TDMA mechanism. The TDMA part comprises two slots types. This first one is schedule-based slots and the second is polling-based slots. Schedule-based slots are adaptively allocated for nodes based on traffic intensity. However, polling-based slots are assigned by the nodes' coordinator, which requests them through poll messages, a situation which might occur in emergency situation; thus, such slots are normally inactive. Under normal situations, each node sends data to the coordinator, and to its allocated slot, after which it enters a sleep state. All the nodes should wake up at the beginning of a new superframe to check for a new beacon frame. The coordinator analyses the data, and if it detects anomalies, it sends a new beacon frame in the next superframe to inform the emergency context. Nodes that work in a specific context will have an increased sampling rate and will assign more transmission slots to accommodate emergency requirements. Other sensors, might acquire fewer slots and a lower sampling rate to reduce energy consumption. The CA-MAC performance outperforms both 802.15.4 MAC and H-MAC in terms of delay and power consumption, especially in emergencies.

Apparently, the proposed protocol inherits the basics of the IEEE 802.15.4 beacon enabled superframe structure. In addition, although the proposed algorithm can tolerate an emergency delay, it still does not guarantee reliable data transmission in real time entirely. This is because nodes are not informed about emergency situations directly, as they have to wait for subsequent superframe structures, according to which they can then change their remission slots and sampling rates. Thus, there would be some delay handling such situations, which might lead to critical packet loss. Moreover, a centralised coordinator performs the entire context awareness procedure, thus, it is prone to a single point of failure.

4.2.2. Centralised fault Detection Using Middleware. Zhou et al. [2011] are the first to propose a middleware layer, called BodyQoS that tolerates channel faults and impairments by performing an adaptive channel allocation strategy through which the QoS of WBAN is improved. BodyQoS is mainly a collection of software modules, which reside

between MAC and transport layers Zhou et al. [2011]. BodyQoS comprises a virtual MAC (VMAC) that makes the system radio-agnostic when following an abstraction technique [Zhou et al. 2011]. It schedules bandwidth adaptively, without knowledge of the implementation details of the underlying MAC protocols. Thus, the VMAC can be easily ported from one radio platform to another, allowing it to support an array of different MACs, including Time Division Multiple Access (TDMA), CSMA, and hybrid approaches. VMAC re-allocates resources adaptively, to meet QoS requirements. BodyQoS guarantees a statistical bandwidth for reliable data transmission when channel impairments occur because of radio interference or body fading effects. If the wireless resource available is not able to satisfy all QoS reservations, packets with the higher priority will be processed before the lower priority ones. A resource rich aggregator is responsible for the majority of channel scheduling computations, and can be used to minimise the load on resource constrained sensor nodes. BodyQoS performance outperforms conventional solutions, as it tolerates channel impairment with a minimum overhead. However, although the proposed technique should guarantee reliable data communication under channel impairments, it does not consider the dynamic change in the reliability requirements of sensors, as it assigns a specific fixed priority to sensor nodes based on the level of criticality and data type. In addition, BodyQoS is prone to single points of failure, as the entire channel's fault detection, traffic prioritisation and classification is managed by one central node.

4.3. Fault Tolerance Approaches at both Node and Channel Level

The approaches that fall within this band comprehend abnormalities that might occur at both nodes and channel levels in WBAN. Two Approaches have been found, one follows a centralised middleware while the other adopts a context aware technique implemented in a distributed manner. The WBAN studies that have adopted such techniques are presented in the following subsections.

4.3.1. Centralised Fault Detection Using Middleware. The work in Wu et al. [2010] aims to improve BodyQoS that is presented in Zhou et al. [2011]. Wu et al. [2010] suggested an adaptive and flexible fault-tolerant communication middleware (AFTCS). AFTCS is made to tolerate channel impairments by adjusting the priority queue of each sensor node adaptively, according to three pieces of sensor information: physiological, environmental and physical status of the sensor. According to the information received, a central node allocates the channel resources adaptively after considering the priority level of the sensor nodes and their current data criticality level. The resource computation and effective bandwidth calculation approach was inspired by the work in Zhou et al. [2011]. Simulation results revealed that AFTCS can tolerate channel impairments by reducing the rate of packet loss and the delay in critical data transmission. However, the centralised controller checks the three sources of information for each node according to a single specified activation threshold, which has the value 0.4, and according to which the priority for each sensor will be adjusted. It was not demonstrated why this threshold value was chosen. Additionally, a fixed threshold test is not suitable for fault detection in WBAN, as it is characterised by the complexity of heterogeneous sensors. Furthermore, each sensor might encounter different situations that change its criticality. For instance, two settings are considered critical for a body temperature sensor, e.g., to determine if the temperature is below a specific value and if it is higher than another certain value. Therefore, choosing as single threshold is not a realistic option for all cases of sensors. As channel computations and adaptive resource allocations are performed by one central node, this technique is prone to a single point of failure. It can be argued that, although the controller receives information about the node's physical status, it does not consider the effect of node-level faults.

4.3.2. Distributed Context Aware Fault Detection. Context awareness can be applied in each resource constrained sensor nodes, without the need to rely on the controller. Several approaches can be adopted to achieve this aim. Otal et al. [2009] explored the QoS and reliability in WBAN and presented a novel cross-layer based on a fuzzy logic technique to schedule transmissions in WBAN. The Distributed Queuing Body Area Network (DQBAN) protocol was proposed by Otal et al. to modify the beacon enabled IEEE 802.15.4 MAC protocol, and improve the efficiency in terms of delay, reliability and power consumption. DQBAN is adaptable to the heterogeneity of traffic load, number of sensor nodes and interference. A fuzzy-rule–based system is implemented in each sensor node to handle input variables that relate to node status. DQBAN violates the first-come-first-served packet transmission policy because it allows the node, according to its status, to occupy the next frame collision-free "data slot", even if that node has already achieved the first location in the queue. A node can also chose to temporarily stop transmission if it detects channel impairments. DQBAN protocol performance was evaluated according to two different realistic hospital scenarios following a star topology. This revealed that DQBAN achieves higher reliabilities than other possible MAC protocols, when considering battery limitations and latency demands. Thus, Otal et al. ensure that all packets are treated within specific delay parameters, and with a particular BER, while conserving power. Although the mechanism provides some solutions for fault-tolerance in WBAN and avoids single point of failure, it does not consider differences in the reliability and requirements of the heterogeneous sensor nodes. Moreover, Otal et al. [2009] achieved self-monitoring, by adopting two queues to detect the physical status of the node. This means deploying specialised hardware and software to resource constrained nodes, which adds extra resources and increases the computation complexity of the network. Thus, when using this technique, the trade-off between the level of required reliability and processing complexity should be investigated. As shown, some primary efforts have been undertaken to try to address fault tolerance challenges in WBAN. These efforts have varied between designing new protocols to target network stack layers such as Medium Access Control (MAC) layer [Otal et al. 2009; Ali et al. 2010; Liu et al. 2011; Rezvani and Ghorashi 2013], and proposing the injection of a middleware or new layer responsible for fault diagnosis [Zhou et al. 2011; Wu et al. 2010; Galzarano et al. 2012], or new generic techniques that do not follow the stack-layering concept [Zhou et al. 2011; Wu et al. 2010; Mahapatro and Khilar 2011; Galzarano et al. 2012; Abarna and Venkatachalapathy 2014]. Others make enhancements to the proposed standards to improve their fault tolerance capabilities [Otal et al. 2009; Ali et al. 2010; Liu et al. 2011; Rezvani and Ghorashi 2013]. However, the majority of work follows centralised detection techniques [Zhou et al. 2011; Ali et al. 2010; Wu et al. 2010; Liu et al. 2011; Mahapatro and Khilar 2011; Rezvani and Ghorashi 2013], neglecting the issue of a single point of failure, and while most consider techniques for an overall fault tolerance approach, fault recovery, which is a crucial second component of fault tolerance, is not considered, thus, these efforts cannot be considered complete solutions to fault tolerance in WBAN. Table IV provides a summary of fault tolerance techniques in WBAN. It classifies the proposed solutions according to the categorization presented in Figure 8.

Table V categorizes fault tolerance solutions further. For those solutions that are geared toward node-level faults, it shows whether they consider hardware faults, data faults or both. It shows which work considers channel-level abnormality, and whether the proposed solution considers abnormality in emergency situations due to the correlation in medical data.

Table VI classifies the proposed solutions for fault tolerance in WBAN according to other four criteria. It shows whether a prioritising approach is considered in each proposed solution discussed in Section 4 along with the priotrisation technique adopted,

Table IV. A Summary of Fault Tolerance Techniques in WBAN

Solutions for node-level faults			
Technique		Solution	Summary
Centralised (Fusion centre)		[Mahapatro and Khilar 2011] (Generic)	Fusion centre (PDA) derives relevant physiological information from sensor data, according to which it diagnoses faulty nodes. This technique is efficient for data centric applications that require detection precision.
Distributed	Middleware	[Galzarano et al. 2012] (Generic based on SPIN*)	Adopts a middleware layer in each node to detect data faults and possibly recover faulty status. Suggests adding autonomic elements that perform self-healing operations. Avoids single point of failure and reduces the messages between nodes and the central node, so reduces energy consumption and network congestion.
	Clustering	[Abarna and Venkatachalapathy 2014] (Generic based on AFTCS)	CH assigns priority values to its nodes that reflect their fault tolerance level. Collected values from sensors are compared with three threshold values and node priorities are assigned accordingly. A scheme for CH fault detection and recovery is also proposed. Tries to alleviate a drawback of single of point of failure.
Cloud based		VMSFT [Jeong et al. 2014] (IaaS cloud based application)	A visual monitoring system that monitors patient's conditions and tolerates to sensor failures immediately. Considers a large number of WBAN adopted by multiple patients simultaneously. Collects patient's data through the IaaS application according to which it can infer sensor failure. Performs two types of explicit anomaly detection and provides three responses according to the position of the sensor in the body.
Solutions for channel-level faults			
Technique		Solution	Summary
Centralised	Context aware	[Rezvani and Ghorashi 2013] (Based on IEEE802.15.4)	Studies the channel impairments in WBAN due to fading and body postures in a star topology. Considers correlations that occur in medical traffic in emergencies and splits that traffic into normal and emergency medical traffic adaptively, according to channel condition and the user's medical situation. Tolerates to channel faults by adapting the channel allocation to the classified sampled data that consider fading effects.
		CA-MAC [Liu et al. 2011] (Based on IEEE 802.15.6)	Hybrid superframe-based protocol that adjusts the transmission priority and access strategy according to the traffic and channel status. It changes the duty cycle of the nodes according to human activity, or environmental conditions, while considering power consumption.
	Middleware	BodyQoS [Zhou et al. 2011] (Generic)	A middleware layer, called BodyQoS tolerates to channel faults and impairments by performing an adaptive channel allocation strategy through which the QoS of WBAN is improved.
Solutions for hybrid (node and channel) faults			
Technique		Solution	Summary
Centralised (Middleware)		AFTCS [Wu et al. 2010] (Generic based on BodyQoS)	Each node is assigned a queue with a set of multiple priorities. Tolerates to channel impairments by adjusting the priority queue of each node adaptively, according to three pieces of sensor information. Accordingly, a central node allocates the channel bandwidth adaptively after considering the priority level of the nodes and their data criticality level.
Distributed (Context awareness)		DQBAN [Otal et al. 2009] (Based on IEEE 802.15.4)	A cross-layer and fuzzy logic–based mechanism that schedules transmissions in WBAN. Adaptable to the heterogeneity of traffic load, number of sensors and interference. A fuzzy-rule–based system is implemented in each node to handle input variables that relate to node's status. Adopts two queues that violates the first-come-first-served packet transmission policy. A node chooses to temporarily stop transmission if it detects channel impairments. Avoids single point of failure.

Table V. A Classification for the Centralized and Distributed Approaches Fault Tolerance Approaches in WBAN

Fault Type/Solution		Centralized			Distributed			Cloud based
		Data fusion	Middleware	Context aware	Node-self detection	Clustering	Context aware	
Node level	Hardware		AFTCS [Wu et al. 2010]			[Abarna and Venkatacha-lapathy 2014]	[Otal et al. 2009]	VMSFT [Jeong et al. 2014]
	Data faults (including physiological information)	[Mahapatro and Khilar 2011]	AFTCS [Wu et al. 2010]		[Galzarano et al. 2012]	[Abarna and Venkatacha-lapathy 2014]		VMSFT [Jeong et al. 2014]
Channel Level Body/ interference			BodyQoS [Zhou et al. 2011] AFTCS [Wu et al. 2010]	CA-MAC [Rezvani and Ghorashi 2013]			[Otal et al. 2009]	
Medical correlation (emergency)				CA-MAC [Rezvani and Ghorashi 2013]		[Abarna and Venkatacha-lapathy 2014]	[Otal et al. 2009]	VMSFT [Jeong et al. 2014]

it also shows whether the proposed solution follows a recovery approach and whether the proposed approach is a generic based or based on a standardized protocol.

The following section summarises some interference solutions presented in this section. It highlights the strengths and the drawbacks of the presented approaches and suggests trends that can be adopted in the future to achieve a more reliable WBAN by overcoming the drawbacks of the literature presented.

4.4. Interference Mitigation Techniques

For interference analysis and modelling, when building reliable interference models, a challenging task could be in the assessment of future e-Health applications while considering the increasing heterogeneity of networks, devices, services, user requirements and conditions. Thus, classical deterministic approaches that are characterized by limited scalability and high complexity can barely characterise such highly dense networks. As an alternative, emerging stochastic geometry techniques has recently been used to obtain tractable evaluations and suitable expressions to capture and optimize the total effect interference in co-existing scenarios. A very recent application of stochastic geometry technique in modelling intra and inter WBANs interference was proposed in Sun et al. [2015]. However, it was limited to unrealistic assumptions where each node in the network was assumed to follow the same MAC protocol at a given period of time. This is despite all WBANs use hybrid MAC structure as given in the IEEE 802.15.6 standard.

There are two major schemes for interference mitigation namely, *collaborative* and *non-collaborative* schemes [Le and Moh 2015]. In the former one, multiple WBANs interact with each other to manage the co-existence problem while in the latter WBANs can manage the coexistence issue without any interaction. The work in this area is very limited and the majority of the proposed schemes depend on unrealistic assumptions. In addition, they do not consider performance metrics that are essential to measure and monitor reliability in such networks. Hence, there is a need for new efficient versions of coexistence schemes where simplicity, reliability are key elements. For example, in de Francisco et al. [2009], Martelli and Verdone [2012], Dong and Smith [2013], and Hayajneh et al. [2014], the authors proved that there is a dominant interferer from other networks in WBANs such as, for instance, IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4, etc. However, their interference analysis was limited to intra-BAN communication where nodes transmit with the same power to the coordinator.

Table VI. Priority and Recovery Mechanisms Proposed by Fault Tolerance Approaches in WBAN

Protocol/ Criteria	Prioritization	Fault recovery mechanism	Solution	Algorithm
BodyQoS [Zhou et al. 2011]	Specific and fixed priority based on level of criticality of sensor and data type.	N/A	Dynamic Chanel Allocation	Generic (VMAC)
AFTCS [Wu et al. 2010]	Default priority statically configured by the clinician. Based on the perceived fault-related information it adjusts the priority.	N/A	Dynamic Chanel Allocation	Generic Based on BodyQoS
[Mahapatro and Khilar 2011]	N/A	Isolation	Feature-level Fusion	Generic
[Rezvani and Ghorashi 2013]	It adjusts the priority based on the Physician's recognition and health condition of the user and	N/A	Dynamic Chanel Allocation	MAC based on IEEE 80.15.4 and IEEE 802.15.6
CA-MAC [Rezvani and Ghorashi 2013]	Adaptive priority according to traffic and channel status.	N/A	Dynamic Scheduling	MAC Based on IEEE 802.15.6
[Otal et al. 2009]	Adaptive priority according to node physical status.	N/A	Distributed Queues	MAC Based on IEEE 802.15.4
[Galzarano et al. 2012]	N/A	Isolation	Autonomic Elements	Generic Based on SPIN*
[Abarna and Venkatachalapathy 2014]	Adaptive priority according to a specified fixed threshold.	Isolation of faulty node. Nodes under faulty CH re-cluster themselves and elect new cluster head.	Dynamic Priority	Generic based on AFTCS
VMSFT [Jeong et al. 2014]	Priority according node position on body.	Isolation by emergency response	Three levels of response based on abnormality criticality	IaaS cloud-based application

On the other hand, few studies have focused on inter-BAN communication where, in Davenport et al. [2009], the authors conduct a study on the measurement of coupling between 10 nodes within a WBAN. This was done in a single room using the 2400–2500MHz frequency band and within a hospital environment. Note that, although the measurements were interesting, yet it did not consider the mobility of the nodes which is an important characteristic of WBANs. In addition, the authors didn't show the effect of the measured interference on the degradation of the application performance and the coexistence strategies proposed were limited to the packet delivery ratio performance only. Furthermore, the effect of interference in Dotlic [2011] was studied when using both of the chirp and the sampling receivers. Finally, in Alasti et al. [2014], the authors addressed co-channel interference between co-located multiple WBANs where couple of uncoordinated schemes were presented. In both approaches, the coordinator node re-allocates slots in the TDMA scheme. However, such approaches are limited since they use several unrealistic assumptions including lack of mobility and absence of computation or estimation of actual interference. Nonetheless, there is still a need for IEEE 802.15.6-compliant radio transceivers that are available commercially. In addition, communicating WBANs form a very complex network that cannot be

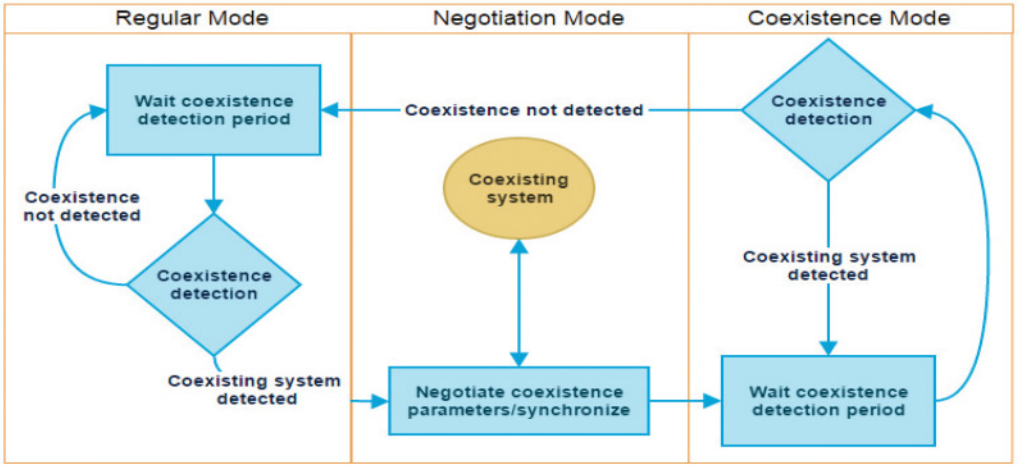

Fig. 9. Generalized coordinated coexisting algorithm.

analyzed analytically due to huge number of possible combinations thus simulation-based approaches are considered.

The performance evaluation of any proposed co-existence mechanism should be done under realistic environment to simulate real deployment and operating assumptions [Ben Hamida et al. 2009] where there is a need for accurate intra- and inter-WBAN mobility and physical layer modeling (e.g., radio link modelling, realistic channel and path loss modelling) to ensure reliability. A challenging task that affects the interference in WBANs is the modelling of both intra and inter-WBANs mobility so as to capture the postural behaviors of real-time motion of human bodies. Perhaps, either sensor nodes within a WBAN move individually or they may move in a group resulting in extra interference effect. In addition, several WBANs sharing the same activity may move in a group into another location where they may enter other WBANs communication range and interfere with their transmissions or be subject to interference from dominant interfering signals coming from other communication technologies.

As detailed earlier, WBANs are expected to coexist with other technologies such as WiFi, Bluetooth, and ZigBee which leads to performance degrading challenges due to the uncoordinated operation of these multi-Radio Access Technologies (multi-RATs) and their uncontrolled interference. In general, a solution to the coexistence problem will follow either coordinated or uncoordinated approaches. In Al-Khansa and Artail [2015], different coexistence techniques in the context of LAA-WiFi coexistence has been presented, where LAA stands for "Licensed-Assisted Access to the unlicensed spectrum" for the Long Term Evolution (LTE) systems [Rupasinghe and Güvenç 2015]. However, this work is not directly applicable to WBAN. Hence, we can summarize the two approaches as follows.

4.4.1. The Multi-RAT Coordination Approach. Through coordination protocols, the different technologies exchange traffic information and negotiate system parameters for optimal system performance. In a WBAN-ZigBee coexistence scenario, for example, the WBAN coordinator node (a.k.a the hub) will coordinate with the ZigBee coordinator node; coordination occurs through a predefined coordination protocol and dedicated interfaces. In general, a coordinated system follows the algorithm shown in Figure 9, where the coordinating technologies switch between regular modes and coexistence modes. This approach has proven to be useful in several scenarios, however, it is not suitable for

WBANs because of the coordination overhead which cannot be tolerated by WBAN nodes that are of limited range and power capabilities.

4.4.2. The Uncoordinated Approach. The coexisting technologies implement techniques to avoid interference with each other while operating independently (i.e., without coordinating with each other). For example, cognitive radio, least-congested channel selection, and power control are uncoordinated techniques. The CSMA/CA protocol is another example for uncoordinated protocols. A drawback of carrier sense mechanisms is that they often suffer from energy-detection inaccuracies due to the uncertainties of noise variance. Moreover, these uncoordinated techniques are time-inefficient, where most of the modes time is spent in listen-modes sensing the medium and often backing-off for exponentially growing durations when collisions occur, and the higher the level of interference, the worse the performance gets. As an illustration of this problem, Nokia has conducted simulations on LTE-WiFi coexistence [Almeida et al. 2013], and the results have shown that when LTE interferes with WiFi without implementing any coexistence techniques, the WiFi nodes consumed "over 99% of the time listening to the wireless medium and backing off" [Almeida et al. 2013]. Thus, significant system time and energy resources are wasted in interfering networks with uncoordinated protocols, which again is not suitable for WBANs.

5. CONCLUSIONS AND RESEARCH DIRECTIONS

Improved efficiency and reliability are vital to guarantee the success of the next generation of WBANs and their ability to host a rich portfolio of applications. Although different surveys have been found in the literature covering different concepts and applications, resilience and reliability and their related issues have been addressed lightly. Thus, unlike existing surveys, this article surveys outlines and discusses the state-of-the-art fault tolerance models and reliability related issues and challenges such as coexistence and interferences. In addition, this survey emphasized the importance of the various technology aspects such power efficiency and heterogeneity. Indeed, the increasing heterogeneity of networks, devices, services, and coexistence of different WBANs and other communication technologies within the same range impose potential challenges in reliability of WBANs. The majority of work proposed in the literature for fault tolerance in both WSN and WBAN focuses only on fault detection techniques, supposing that the only recovery approach is node isolation and replacement [Mahapatro and Khilar 2011; Galzarano et al. 2012; Abarna and Venkatachalapathy 2014; Jeong et al. 2014]. Such a solution could be sufficient for WSN where there is node redundancy, due to the huge number of homogenous nodes. However, in WBAN, waiting for node isolation and replacement results in a huge delay in response, while critical data needs to be transmitted immediately. The framework for fault tolerance in WBAN cannot be considered complete if it only allows fault detection, ignoring real-time fault recovery. Thus, proposing real time recovery techniques for WBAN is necessary, such that the critical data of erroneous nodes could be achieved even though the node is faulty.

One technique followed in this work is to exploit the data correlation in sensor readings. Despite the problems mentioned as possibly occurring due to data correlation in WBAN, existing interconnections can be harnessed by performing data fusion. Mahapatro and Khilar [2011] was found to be the first and only study to mention this technique but for fault detection. Data fusion can be considered an initial step towards fault recovery. In other words, a central node can achieve data of some faulty sensors by performing some derivations from other available data that has been sent by other sensors. This could be considered a temporary solution, until node isolation and replacement takes place.

Moreover, new technologies might encounter opportunities in this arena, such as cloud computing and sensor clouds. Through these technologies, fault detection and recovery can be achieved in real time simply by exploiting the services such technologies offer. Virtual sensors in the sensor cloud, for example, could be considered a valuable alternative to sensor redundancy [Alamri et al. 2013]. Certainly, adopting such technologies requires the implementation and installation of fault tolerance applications in the cloud. Such applications can be used by patients and medical staff, each with different responsibilities and capabilities. However, privacy and security is still a primary concern potentially limiting the level of adoption of such technologies at the current time. Yet it is still beneficial to consider them. It is also found that, to satisfy the emerging applications, there is a need for new cross-layer interference mitigation schemes, considering different mobility and coexistence paradigms.

Finally, regarding WSN, we used to claim: the lifetime of a sensor determines the lifetime of WSN, but in relation to WBAN we claim instead: the behaviour of a sensor determines lifetime of the human. Hence, if we cannot achieve the highest degree of reliability with 0% error as an acceptable QoS in WBAN, then it is better to shift to wired e-health networks despite their limitations on individual's movements. We must always remember that the main objective of WBAN is to improve and extend human life, it is not intended to offer luxury.

REFERENCES

K. T. Meena Abarna and K. Venkatachalapathy. 2014. Cluster based failure detection and recovery technique for wireless body area networks. *Research Journal of Applied Sciences, Engineering and Technology* 7, 17 (2014), 3458–3465. DOI:10.19026/rjaset.7.697

Raza H. Abedi, Nauman Aslam, and Sayeed Ghani. 2011. Fault tolerance analysis of heterogeneous wireless sensor network. In *Proceedings of the 24th Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 000175-000179. DOI:10.1109/CCECE.2011.6030433

Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. 2002. A survey on sensor networks. *IEEE Communications Magazine* 40, 8 (2002), 102–114. DOI:10.1109/MCOM.2002.1024422

Rasha Al-Khansa and Hassan Artail. 2015. A semi-distributed LTE-WiFi system design for future LTE-unlicensed: Deployments in small-cell environments. In *Proceedings of the 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 43–50. DOI:10.1109/WiMOB.2015.7347939

Muhammad Mahtab Alam and Elyes Ben Hamida. 2015. Interference mitigation and coexistence strategies in IEEE 802.15.6 based wearable body-to-body networks. In *Proceedings of the International Conference on Cognitive Radio Oriented Wireless Networks*. Springer International Publishing, 665–677. DOI:10.1007/978-3-319-24540-9_55

Atif Alamri, Wasai Shadab Ansari, Mohammad Mehedi Hassan, M. Shamim Hossain, Abdulhameed Alelaiwi, and M. Anwar Hossain. 2013. A survey on sensor-cloud: Architecture, applications, and approaches. *International Journal of Distributed Sensor Networks* 2 (2013), 18. 917923. DOI:10.1155/2013/917923

Mehdi Alasti, Martina Barbi, and Kamran Sayrafian. 2014. Uncoordinated strategies for inter-BAN interference mitigation. In *Proceedings of the 25th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*. IEEE, 2150–2154. DOI:10.1109/PIMRC.2014.7136528

Khaled A. Ali, Jahangir H. Sarker, and Hussein T. Mouftah. 2010. Urgency-based MAC protocol for wireless sensor body area networks. In *Proceedings of the IEEE International Conference on Communications Workshops*. IEEE, 1–6. DOI:10.1109/ICCW.2010.5503911

Erika Almeida, André M. Cavalcante, Rafael C. D. Paiva, Fabiano S. Chaves, Fuad M. Abinader, Robson D. Vieira, Sayantan Choudhury, Esa Tuomaala, and Klaus Doppler. 2013. Enabling LTE/WiFi coexistence by LTE blank subframe allocation. In *Proceedings of the IEEE International Conference on Communications (ICC)*. IEEE, 5083–5088. DOI:10.1109/ICC.2013.6655388

Nancy Alrajei and Huirong Fu. 2014. A survey on fault tolerance in wireless sensor networks. In *Proceedings of the 3rd International Conference on Sensor Technologies and Applications, 2009 (SENSORCOMM'09)*. 366–371.

Deena M. Barakah and Muhammad Ammad-uddin. 2012. A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. In *Proceedings*

of the 3rd International Conference on Intelligent Systems Modelling and Simulation. IEEE, 214–219. DOI:10.1109/ISMS.2012.108

M. Bellalouna, and A. Ghabri. 2013. A priori methods for fault tolerance in wireless sensor networks, In *Proceedings of the 2013 World Congress on Computer and Information Technology (WCCIT)*, IEEE, 1–6.

Monia Bellalouna and Afef Ghabri. 2013. A priori methods for fault tolerance in wireless sensor networks. In *Proceedings of the 2013 World Congress on Computer and Information Technology (WCCIT)*. IEEE, 1–6. DOI:10.1109/WCCIT.2013.6618654

Fabio Bellifemine, Giancarlo Fortino, Roberta Giannantonio, Raffaele Gravina, Antonio Guerrieri, and Marco Sgroi. 2011. SPINE: A domain-specific framework for rapid prototyping of WBSN applications. *Software: Practice and Experience* 41, 3 (2011), 237–265. DOI:10.1002/spe.998

Lucia Lo Bello and Emanuele Toscano. 2009. Coexistence issues of multiple co-located IEEE 802.15.4/ZigBee networks running on adjacent radio channels in industrial environments. *IEEE Transactions on Industrial Informatics* 5, 2 (2009), 157–167. DOI:10.1109/TII.2009.2018541

Elyes Ben Hamida, Guillaume Chelius, and Jean-Marie Gorce. 2009. Impact of the physical layer modeling on the accuracy and scalability of wireless network simulation. *Simulation* 85 (2009), 574–588. DOI:10.1177/0037549709106633

Azzedine Boukerche. 2005. *Handbook of Algorithms for Wireless Networking and Mobile Computing*. CRC Press.

Riccardo Cavallari, Flavia Martelli, Ramona Rosini, Chiara Buratti, and Roberto Verdone. 2014. A survey on wireless body area networks: technologies and design challenges. *IEEE Communications Surveys and Tutorials* 16, 3 (2014), 1635–1657. DOI:10.1109/SURV.2014.012214.00007

Craig A. Chin, Garth V. Crosby, Tirthankar Ghosh, and Renita Murimi. 2012. Advances and challenges of wireless body area networks for healthcare applications. In *Proceedings of the 2012 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 99–103. DOI:10.1109/ICCNC.2012.6167576

C. N. A. P. Staff. 2013. *Network Basics Companion Guide*. Cisco Press.

G. V. Crosby, T. Ghosh, R. Murimi, and C. A. Chin. 2012. Wireless body area networks for healthcare: A survey. *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)* 3, 3, 1–19.

Garth V. Crosby, Tirthankar Ghosh, Renita Murimi, and Craig A. Chin. 2012. Wireless body area networks for healthcare: A survey. *International Journal of Ad Hoc, Sensor and Ubiquitous Computing (IJASUC)* 3, 3 (2012), 1–19. DOI:10.5121/ijasuc.2012.3301

David M. Davenport, Budhaditya Deb, and Fergus J. Ross. 2009. Wireless propagation and coexistence of medical body sensor networks for ambulatory patient monitoring. In *Proceedings of the 6th International Workshop on Wearable and Implantable Body Sensor Networks*. IEEE, 41–45. DOI:10.1109/BSN.2009.8

Ruben de Francisco, Li Huang, and Guido Dolmans. 2009. Coexistence of WBAN and WLAN in medical environments. In *Proceedings of the 70th IEEE Vehicular Technology Conference Fall (VTC 2009-Fall)*. IEEE, 1–5. DOI:10.1109/VETECF.2009.5378807

Jie Dong and David Smith. 2013. Coexistence and interference mitigation for wireless body area networks: Improvements using on-body opportunistic relaying. *arXiv preprint arXiv, 1305.6992*.

Igor Dotlic. 2011. Interference performance of IEEE 802.15.6 impulse-radio ultra-wideband physical layer. In *Proceedings of the 22nd IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*. IEEE. 2148–2152. DOI:10.1109/PIMRC.2011.6139895.

Du Dakun, Hu Fengye, Wang Feng, Wang Zhijun, Du Yu, and Wang Lu. 2015. A game theoretic approach for inter-network interference mitigation in wireless body area networks. *China Communications* 12, 9 (2015), 150–161.

Stefano Galzarano, Giancarlo Fortino, and Antonio Liotta. 2012. Embedded self-healing layer for detecting and recovering sensor faults in body sensor networks. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2377–2382. DOI:10.1109/ICSMC.2012.6378098

Satish K. Garg, Sherwyn Schwartz, and Steven V. Edelman. 2004. Improved glucose excursions using an implantable real-time continuous glucose sensor in adults with type 1 diabetes. *Diabetes Care* 27, 3 (2004), 734–738.

Sai Anand Gopalan and Jong-Tae Park. 2010. Energy-efficient MAC protocols for wireless body area networks: Survey. In *Proceedings of the International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 739–744. DOI:10.1109/ICUMT.2010.5676554

Thaier Hayajneh, Ghada Almashaqbeh, Sana Ullah, and Athanasios V. Vasilakos. 2014. A survey of wireless technologies coexistence in WBAN: Analysis and open research issues. *Wireless Networks* 20, 8 (2014), 2165–2199.

Hongliang Ren and Max Q.-H. Meng. 2006. Understanding the mobility model of wireless body sensor networks. In *Proceedings of the 2006 IEEE International Conference on Information Acquisition*. IEEE, 306–310. DOI:10.1109/ICIA.2006.306015

Young-Sik Jeong, Hyun-Woo Kim, and Jong Hyuk Park. 2014. Visual scheme monitoring of sensors for fault tolerance on wireless body area networks with cloud service infrastructure. *International Journal of Distributed Sensor Networks* 2014. DOI:10.1155/2014/154180

Jamil Y. Khan and Mehmet R. Yuce. 2010. Wireless body area network (WBAN) for medical applications. *New Developments in Biomedical Engineering. INTECH* (2010), ISBN 978-953-7619-57-2, 592–627. DOI:10.5772/7598

Barbara T. Korel and Simon G. M. Koo. 2007. Addressing context awareness techniques in body sensor networks. In *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)* 2 (2007), IEEE, 798–803. DOI:10.1109/AINAW.2007.69

Ravindra V. Kshirsagar and Ashish B. Jirapure. 2011. A survey on fault detection and fault tolerance in wireless sensor networks. In *Proceedings of the International Conference on Benchmarks in Engineering Science and Technology (ICBEST (1))*. 3 (2011), *International Journal of Computer Science.* 130–138.

Benoît Latré, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester. 2011. A survey on wireless body area networks. *Wireless Networks* 17, 1 (2011), 1–18. DOI:10.1007/s11276-010-0252-4

Thien T. T. Le and Sangman Moh. 2015. Interference mitigation schemes for wireless body area sensor networks: A comparative survey. *Sensors* 15, 6 (2015), 13805–13838. DOI:10.3390/s150613805

Bin Liu, Zhisheng Yan, and Chang Wen Chen. 2011. CA-MAC: A hybrid context-aware MAC protocol for wireless body area networks. In *Proceedings of the 13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*. IEEE, 213–216. DOI:10.1109/HEALTH.2011.6026748

Hai Liu, Amiya Nayak, and Ivan Stojmenović. 2009. Fault-tolerant algorithms/protocols in wireless sensor networks. In *Guide to Wireless Sensor Networks*, Springer, London, 261–291. DOI:10.1007/978-1-84882-218-4_10

Arunanshu Mahapatro and Pabitra Mohan khilar. 2011. Online fault detection and recovery in body sensor networks. In *Proceedings of the World Congress on Information and Communication Technologies (WICT)*. IEEE, 407–412. DOI:10.1109/WICT.2011.6141280

Vikash Mainanwal, Mansi Gupta, and Shravan Kumar Upadhayay. 2015. A survey on wireless body area network: Security technology and its design methodology issue. In *Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. IEEE, 1–5. DOI:10.1109/ICIIECS.2015.7193088

Bhavneesh Malik and V. R. Singh. 2013. A survey of research in WBAN for biomedical and scientific applications. *Health and Technology* 3, 3 (2013), 227–235. DOI:10.1007/s12553-013-0056-5

Jhon. M. Maloney and John T. Santini, Jr. 2004. Implantable microchips for controlled drug delivery. In *Proceedings of the 26th IEEE Annual International Conference Engineering in Medicine and Biology Society (IEMBS'04)*. 1 (2004), 2668–2669. DOI:10.3109/10717544.2014.903579

Flavia Martelli and Roberto Verdone. 2012. Coexistence issues for wireless body area networks at 2.45 gHz. In *Proceedings of the 18th European Wireless Conference 2012, EW, VDE*. 1–6.

Sushruta Mishra, Lambodar Jena, and Aarti Pradhan. 2012. Fault tolerance in wireless sensor networks. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, 2, 10, 146–153.

Amirhossein Moravejosharieh and Jaime Lloret. 2015. A survey of IEEE 802.15.4 effective system parameters for wireless body sensor networks. *International Journal of Communication Systems* (2015). 1–24. DOI:10.1002/dac.3098

Samaneh Movassaghi, Mehran Abolhasan, and Justin Lipman. 2013. A review of routing protocols in wireless body area networks'. *Journal of Network and Computer Applications* 8, 3, (March 2013), 559–575. 10.4304/jnw.8.3

Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. 2014. Wireless body area networks: A survey. *IEEE Communications Surveys and Tutorials* 16, 3, (2014), 1658–1686. DOI:10.1109/SURV.2013.121313.00064

Georgia D. Ntouni, Athanasios S. Lioumpas, and Konstantina S. Nikita. 2014. Reliable and energy-efficient communications for wireless biomedical implant systems. *IEEE Journal of Biomedical and Health Informatics* 18, 6, (2014), 1848–1856.

Horacio Antonio Braga, Fernandes De Oliveira, Azzedine Boukerche, Eduardo Freire Nakamura, and Antonio Alfredo Ferreira Loureiro. 2009. An efficient directed localization recursion protocol for wireless sensor networks. *IEEE Transactions on Computers* 58, 5, (2009), 677–691. DOI:10.1109/TC.2008.221

Begonya Otal, Christos Verikoukis, and L. Alonso. 2009. Fuzzy-logic scheduling for highly reliable and energy-efficient medical body sensor networks. In *Proceedings of the 2009 IEEE International Conference on Communications Workshops*. IEEE, 1–5. DOI:10.1109/ICCW.2009.5208088

Chris Otto, Aleksandar Milenkovic, Corey Sanders, and Emil Jovanov. 2006. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia* 1, 4, (2006), 307–326.

Maulin Patel and Jianfeng Wang. 2010. Applications, challenges, and prospective in emerging body area networking technologies. *IEEE Wireless Communications Magazine* 17, 1, (2010), 80–88. DOI:10.1109/MWC.2010.5416354

K. M. Karthick Raghunath and N. Rengarajan. 2013. Investigation of faults, errors and failures in wireless sensor network: A systematical survey. *International Journal of Advanced Computer Research* 3, 3, (2013), 151.

Sanaz Rezvani and Seyed Ali Ghorashi. 2013. Context aware and channel-based resource allocation for wireless body area networks. *IET Wireless Sensor Systems* 3, 1 (2013), 16–25. DOI:10.1049/iet-wss.2012.0100

Nadisanka Rupasinghe and İsmail Güvenç. 2015. Reinforcement learning for licensed-assisted access of LTE in the unlicensed spectrum. In *Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1279–1284. DOI:10.1109/WCNC.2015.7127653

Tom Rutherford and A. Socio. 2012. Population ageing: Statistics. *House of Commons library (Standard not. Retrieved Jan 2, 2013, From: www. Parliament. uk/Topics/PopulationArchive* (2012)

Marwa Salayma, Wail Mardini, Yaser Khamayseh, and Muneer Bani Yasin. 2013a. Optimal beacon and superframe orders in WSNs. In *Proceedings of the 5th International Conference on Future Computational Technologies and Applications*, *Topology* 6 (2013), 49–55.

Marwa Salayma, Wail Mardini, Yaser Khamayseh, and Muneer Bani Yasin. 2013b. IEEE 802. 15.4 Performance in Various WSNs Applications. 2013. In *Proceedings of the 7th International Conference on Sensor Technologies and Applications*. 139–144.

Leo Selavo, Anthony Wood, Qing Cao, Tamim Sookoor, Hengchang Liu, Aravind Srinivasan, and Yafeng Wu. 2007. LUSTER: Wireless sensor network for environmental research. In *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems*. ACM, 103–116. DOI:10.1145/1322263.1322274

TG4. 2003. *IEEE 802.15 WPAN^{TM} Task Group 4 (TG4). Retrieved Juanuary 31, 2016 from* http://www.ieee802.org/15/pub/TG4.html.

TG4a. 2007. *IEEE 802.15 WPAN Low Rate Alternative PHY Task Group 4a (TG4a). Retrieved Juanuary 31, 2016 from* http://www.ieee802.org/15/pub/TG4a.html.

TG4j. 2012. *TG 4j Amendment Draft*. Internal Report, unpublished.

TG6. 2012. *IEEE standard for local and metropolitan area networks: Part 15.6: Wireless body area networks, 802.15.6-2012. Retrieved Juanuary 31, 2016 from* https://standards.ieee.org/findstds/standard/802.15.6-2012.html.

Wen Sun, Yu Ge, and Wai-Choong Wong. 2015. A stochastic geometry analysis of inter-user interference in IEEE 802.15. 6 body sensor networks. In *Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1912–1917. DOI:10.1109/WCNC.2015.7127760

Sana Ullah, Henry Higgins, Bart Braem, Benoit Latre, Chris Blondia, Ingrid Moerman, Shahnaz Saleem, Ziaur Rahman, and Kyung Sup Kwak. 2012. A comprehensive survey of wireless body area networks. *Journal of Medical Systems* 36, 3, (2012), 1065–1094. DOI:10.1007/s10916-010-9571-3

Xuan Wang and Lin Cai. 2011. Interference analysis of co-existing wireless body area networks. In *Proceedings of the Global Telecommunications Conference (GLOBECOM 2011)*. IEEE, 1–5. DOI:10.1109/GLOCOM.2011.6133624

Wikipedia The Free Encyclopedia. 2015. Middleware. Retrieved April 14, 2015 from http://www.ieee802.org/15/pub/TG4.html.

Guowei Wu, Jiankang Ren, Feng Xia, and Zichuan Xu. 2010. An adaptive fault-tolerant communication scheme for body sensor networks. *Sensors* 10, 11 (2010), 9590–9608. DOI:10.3390/s101109590

Mengjie Yu, Hala Mokhtar, and Madjid Merabti. 2007. Fault management in wireless sensor networks. *IEEE Wireless Communications* 14, 6 (2007), 13–19. DOI:10.1109/MWC.2007.4407222

Gang Zhou, Qiang Li, Jingyuan Li, Yafeng Wu, Shan Lin, Jian Lu, Chieh-Yih Wan, Mark D. Yarvis, and John A. Stankovic. 2011. Adaptive and radio-agnostic qos for body sensor networks. *ACM Transactions on Embedded Computing Systems (TECS)* 10, 4 (2011), 48. DOI:10.1145/2043662.2043672

Received March 2016; revised October 2016; accepted December 2016