International Journal of Applied Information Systems (IJAIS) ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12 - No. 20, March 2019 - www.ijais.org

Wearable Networks: Requirements, Technologies, and Research Trends

Ernest Ofosu Addo
Dept. of Info. Eng and Math. Sciences
University of Siena
Siena, Italy

Benjamin Kommey
Dept. of Computer Eng.
KNUST
Kumasi, Ghana

Andrew Selasi Agbemenu
Dept. of Computer Eng.
KNUST
Kumasi, Ghana

ABSTRACT

Wearable networks are ubiquitous and they form the backbone of today's fast-growing smart wearable industry. The wireless nature of these networks coupled with smaller but sophisticated nodes offer the possibility of a wide array of innovative and advanced applications. This paper gives an overview of the concepts of wearable networks and their characteristics. Requirements for optimal application of these networks for various systems are also presented. Key enabling technologies for implementing wearable networks are discussed and compared.

General Terms:

Wearable Networks, Protocols

Keywords

WBANs, Energy Efficiency, QoS, Coexistence

1. INTRODUCTION

Smart computing is incessantly undergoing a miniaturization and performance revolution making devices much more smaller, wearable and easily integrated into daily life. It has been projected that each individual is likely to own an average of six connected devices by 2020 [1]. This rapid growth introduces challenges in terms of handling of large amounts of generated data and device power needs. Since these connected gadgets are essentially nodes on wearable networks, these challenges are translated into network requirements and characteristics. Furthermore, the complex and diverse nature of modern devices in these networks adds application-specific quality-of-service (QoS) and reliability needs; all of which the networks must satisfy.
The contribution of this work is to provide a quick but detailed overview of the world of wearable networks, its promising prospects and current research works being undertaken in the area.
Beyond this introduction, this paper is organized into four main parts. Section 2 presents an overview of the concept of wearable networks and details requirements to be considered for their build and optimal operation. Significant emphasis is placed on the body area subfamily of networks. Possible implementation technologies and their enabling properties are presented in Section 3. Section 4 discusses open research areas and ongoing trends in this field and Section 5 draws conclusion remarks.

2. REQUIREMENTS OF WEARABLE NETWORKS

A wearable network (WN) constitutes different devices which are interconnected to achieve in-body, on-body, body-to-body, and off-body communications. For off-body and body-body communications, either the transmitter or the receiver terminal is on a host's body and the other terminal is not. Both terminals are affixed on the same body in on-body networks whereas, with in-body, one of the terminals is imbedded in the host.
WN devices are grouped into three different types. These are sensor nodes, coordinators, and actuator nodes. A sensor node collects data on stimuli, processes them if needful, and wirelessly relays the information. An actuator node acts on the information gathered by the sensor, and the coordinator controls the other nodes within the network. An on-body or wireless body area networks (WBAN), has some sensor and actuator nodes for stimuli interaction; and coordinators for connecting the WBAN to other networks using off-body communications. The generic architecture of WNs is shown in Figure 1.
Wireless communication technologies have provided interconnectivity in WNs with reasonable independence of space and time. However, the need for effective and regulated flow of information demands that these networks operate under certain constraints. Such constraints present unique requirements whose enforcements are typically application-dependent. These factors include bandwidth, power consumption, security, transmission latency, reliability, and quality-of-service (QoS).

2.1 Bandwidth

Bandwidth requirements vary significantly as a result of the significant heterogeneity of WN applications. Data rates range from a few kbps for low rate sensors to several Mbps for multimedia data stream systems. For example, technical staff using interactive multimedia for design documents would need larger bandwidth, while low data rates will suffice for delivery workers. In some cases, data transmission can also occur in bursts. However, this transmission scheme may considered energy inefficient depending on the application.

2.2 Energy Efficiency

Often very restricted in WNs especially WBANs, power available in nodes is regarded as a very challenging requirement. Power in a WN is mainly expended in sensing, wireless communication and processing of data. Of these three energy sinks, wireless communication is frequently the most power consuming. Most WBAN devices use batteries as their primary power sources, and per existing technologies, the capacities of batteries are strongly correlated to the weight and form-factor of nodes. Consequently, batteries are to be kept small translating to reduced expected energy consumption of nodes. Thus, network factors that also affect battery life such as traffic patterns and the transmit/receive duty cycle, must be carefully chosen and keenly monitored. This is particularly important for in-body network applications where implant nodes such as leadless pacemakers are expected to operate while maintaining an extended battery life without intervention. Employing power-efficient medium access control (MAC) protocols is a proven way to reduce transmission energy [5]. It is also vital that the network topology is optimized and the application layer also adopts more convenient schemes for sampling and transmitting data as was demonstrated in [4].

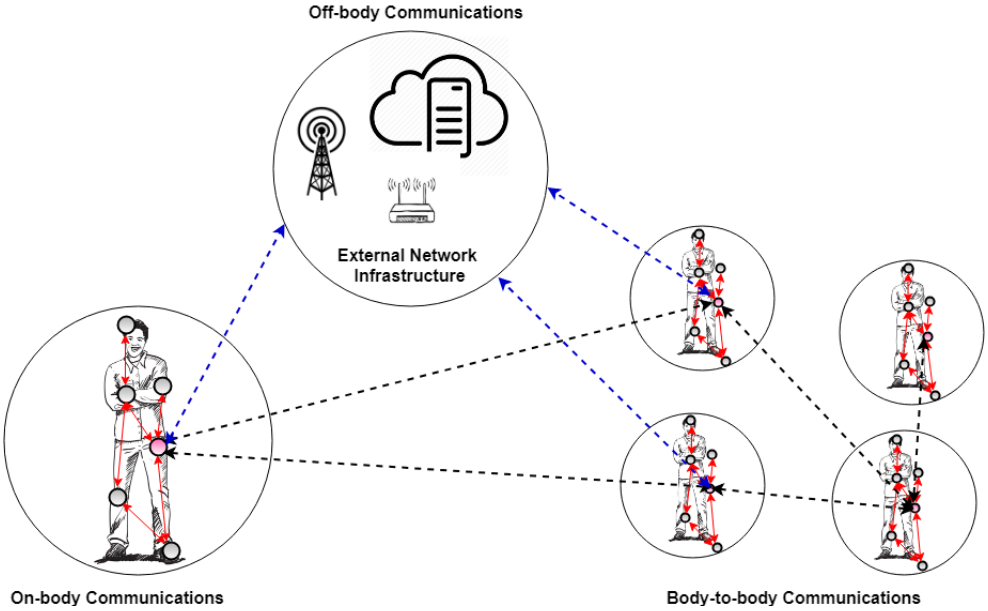

Fig. 1. Generic architecture of WNs

2.3 Privacy and Security

In WNs, it is strongly desired that privacy of data in a WBAN and over off-body networks is rigorously upheld. This is particularly important for wireless media, which are inherently less secure. Therefore, data must be encrypted at all times to protect the user's privacy. Introducing security and privacy protection schemes into networks are computationally expensive and as a result, increases the energy costs. These protective mechanisms should, therefore, be as energy efficient and lightweight as possible[8]. Overly secure systems can also be detrimental in some critical network applications.
In WBANs, security of data is measured against four yardsticks: data confidentiality, authenticity, integrity, and freshness [8]. The data confidentiality metric deals with the assurance that transmitted data can only be accessed by authorized individuals and is strictly private. With data authenticity, efforts are made to ensure that the data being received is sent by the claimed sender. Similar to authenticity but with focus on data, data integrity assesses the tamper-free nature of the received information. Freshness guarantees that information received is recent and not a replay of older data, which is a common cyber attack strategy.

2.4 Reliability and QoS

WBANs are widely used in time-critical medical/non-medical applications. Real time and guaranteed data delivery is very essential for these operations. This can be achieved with high transmission reliability and low latency. These requirements generally rely on how well the lower network layers are designed [5]. Optimum network efficiency and reliability are achieved if MAC protocols are designed application-specific. Reliability can be provided in terms of the acceptable transmission loss ratio (TLR) which inversely depends on data rates. Lower rate networks handle high TLR fairly well whiles lower TLRs are more suitable for higher bandwidth applications. The requirement can also be quantified with other QoS metrics like delay jitter and delay profile. Delays and packet loss rates can be reduced by using suitable channel access, packet re-transmission, and enhanced scheduling schemes.

3. WEARABLE NETWORK TECHNOLOGIES

In recent years, various technologies have been used in WN research works as well as commercial systems. These technologies are often categorized based on their location in the wireless network ecosystem shown in Figure 2. This classification indicates the type of wireless specification that the technology is and defines its appropriate use regarding off-body, body-to-body, on-body, or in-body communications. Nonetheless, there are existing research works and commercial products that have used both body-to-body and off-body technologies to achieve on-body communications. A WBAN technology operates close to the host body and has limited communication ranges typically 1-2m. WBANs are useful for in-body and on-body node interconnection and communications. WPANs are networks in the immediate environment around a user. Communication on WPANs can reach up to a 10m range for high bandwidth applications and several dozen meters for low bandwidth applications [8]. WLANs have ranges reaching hundreds of meters and communication in WANs can be achieved using satellite links. WMANs and WANs will not be discussed in this work.

3.1 WLAN technologies

3.1.1 WiFi. WiFi is a radio technology based on the IEEE 802.11 standard which defines the PHY and MAC layers. In infrastructure mode, compatible devices can connect directly to the Internet via an access point (AP). WiFi generally operates on the 2.4 GHz and 5 GHz ISM (Industrial, Scientific, and Medical) radio bands and when running on suitable hardware at close range, speeds that vary from 11 Mbps to 1 Gbps can be achieved depending on the version of the WiFi.
The 802.11 MAC layer protocol supports two modes. These are the Distributed Coordination Function (DCF) and Point Coordination Function (PCF) modes [3]. In DCF mode, the carrier-sense multiple access with collision avoidance (CSMA/CA) scheme is employed for channel access hence no central device controls communication. In PCF mode, which is not used in practice[10], the AP monitors each node and oversees the process of communication. Though a WLAN technology, WiFi is

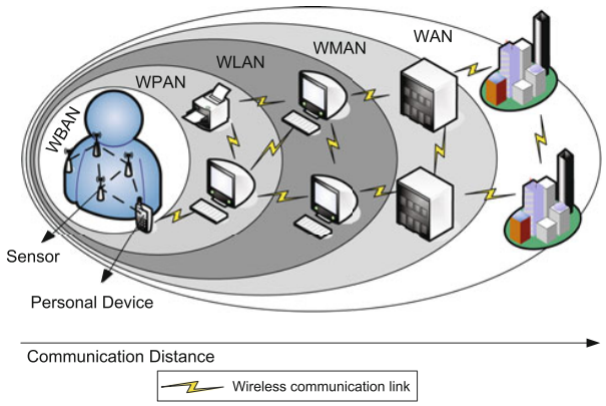

Fig. 2. The ecosystem of wireless networks

used in some WNs for on-body communications where nodes need to stream huge bandwidth traffic with minimum possible lag. However, this feature comes at high power costs. Wi-Fi Protected Access protocols: WPA, WPA2, and WPA3 are options for securing WiFi based WNs.

3.2 WPAN technologies

3.2.1 Bluetooth: Classic and Low Energy. The 802.15.1 standard forms the foundation of the Bluetooth technology. Bluetooth operates on the 2.4 GHz ISM band and has about a 10-50m communication range. Bluetooth employs a master/slave network architecture where each master node can control a maximum of 7 active and 255 inactive (or parked) slave devices. Bluetooth networks are known as piconets and by using a bridge slave, multiple piconets can be interconnected to form a scatternet[3] as shown in Figure 3.

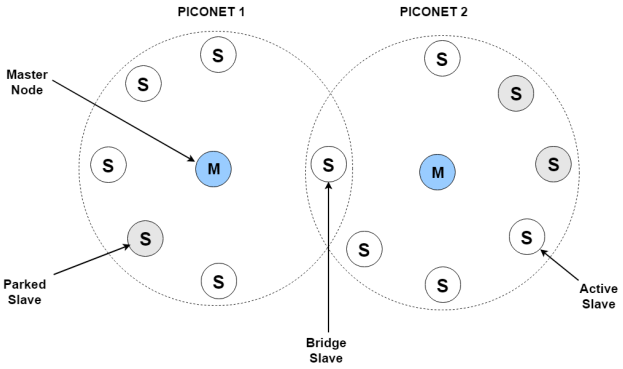

Fig. 3. Two Bluetooth piconets connected to form a scatternet

The 802.15.1 MAC layer protocol uses a time division multiplexing (TDM) scheme known as time division duplex for polling. In this scheme, a master polls each slave node in one time slot to inquire if it has data to transmit. The slave sends data to the master in the next slot, if there is any to send. Polling is done periodically to keep slaves synchronized even if there is no data to be exchanged. Slaves cannot communicate directly with each other. Information must be relayed through the master node in a cluster fashion. Through the basic rate, each piconet supports a reliable 64 kbps master-slave communication in each direction.
As part of the Bluetooth 4.0 standard released in 2010, the Bluetooth Low Energy (BLE) came as a low power alternative to Classic Bluetooth. BLE has a less complex stack and works well with short-range communications. By using about half the number of frequency channels as its predecessor, BLE achieves device synchronization and discovery in less time. This makes BLE a candidate for time-critical and resource-limited networks. Bluetooth Low Energy also provides highly reliable data transfer providing up to 1 Mbps data rate and a power-efficient idle mode [5]. Bluetooth Classic uses algorithms based on the SAFER+ block cipher to implement confidentiality, authentication, and shared secret key derivation. BLE utilizes a Counter Mode CBC-MAC based encryption algorithm.

3.2.2 ZigBee. The IEEE 802.15.4 standard defines lower layer characteristics for the operation of power-efficient low-rate WPANs which achieves a typical 10-100m radio range. It serves as the basis for ZigBee which extends the standard by building the higher layers.
The PHY layer supports three ISM bands: 868 MHz for Europe (1 channel), 915 MHz for North America (30 channels), and 2.4 GHz for other jurisdictions worldwide (16 channels). Nodes in an 802.15.4 based network are categorized as either full function devices (FFDs) or reduced function devices (FFDs). FFDs supports all of 802.15.4's characteristics and can communicate with all devices in the network. They are also capable of extending networks thus each netwok must at least have an FFD. RFDs, on the other hand, are low-power, low complexity devices that can only communicate with an FFD. Star and peer-to-peer are the two network topologies natively supported by 802.15.4. The MAC layer protocol operates in either the non-beacon or

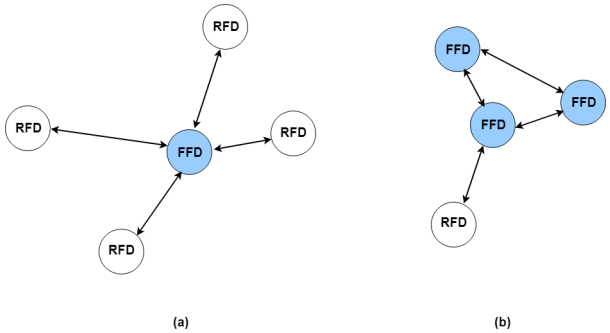

Fig. 4. Native topologies in 802.15.4 (a) Star (b) Peer-to-Peer

beacon modes. In the non-beacon mode, nodes access a channel by simply using un-slotted CSMA/CA. In the beacon mode, an FFD controls data transmission by using periodic beacons for synchronization. The beacon mode uses a super frame (Figure 5) which is divided into a time-slotted active period and an inactive period where devices sleep. Active periods have three parts:

—Beacon
—Contention Access Period (CAP)
—Contention Free Period (CFP)

At the start of an active period, the coordinator sends beacon frames with the period duration information. Following the beacon is the CAP where nodes transmit data using slotted CSMA/CA. CFP, which has 7 Guaranteed Time Slots (GTSs), begins after CAP ends. CFP uses the GTSs to accommodate time critical data.
ZigBee adds mesh networking to the underlying radio by splitting FFDs into coordinators and routers. ZigBee coordinators are responsible for initializing, maintaining and stores information about the network. With the star topology, the coordinator acts as the central node and routers are used as end devices. In meshes and trees, routers to extend networks. Routers route data using Ad hoc On-Demand Distance Vector Routing (AODV).
ZigBee uses a 128-bit AES algorithm for security. The algorithm

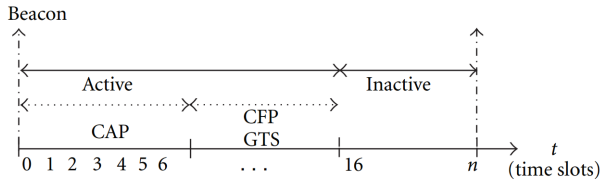

Fig. 5. 802.15.4 MAC protocol beacon mode frame structure

includes methods for key generation and transport, and frame protection.

3.3 WBAN technologies

WBAN is widely used as an efficient paradigm for e-health applications where tiny nodes are used to collect body health indicators. Initially, WBANs had been thought of as a trivial extension of wireless sensor networks (WSNs). However, there are major differences between WSNs and WBANs. Firstly, WBANs have stricter size and energy limitations. In WBANs, node transmitter power is much limited due to health hazard concerns and this reduces radio range. Furthermore, unlike WSN, data in WBANs hold very personal information which makes security and reliability issues very crucial [7]. Finally, WBANs typically use fewer heterogeneous and non-redundant nodes with different demands and properties whereas WSNs mostly use many homogenous nodes which perform similar functions. Consequently, WBANs impose more stringent constraints making existing WSNs protocols ill-suited for WBANs.
Bluetooth has been adopted in the implementation of some WBAN applications [11]. However, the small size networks, (higher) bandwidth and power requirements; and single-hop communication of the 802.15.1 standard makes Bluetooth an inefficient choice. BLE was introduced to meet the needs of WBANs applications. With BLE, lower power expenditure is achieved using low duty cycle operation. Nonetheless, this energy-saving strategy is inappropriate for certain WBAN applications such as health monitoring which depend heavily on frequent data reporting.
ZigBee offers larger coverage area and lower power consumption compared to Bluetooth. However, Zigbee's lower data rate results in increased delays due to extended channel fading [7]. This is unsuitable for time critical applications.Therefore, Zigbee fails to offer sufficient QoS for every WBAN application.

3.3.1 The IEEE 802.15.6 WBAN standard. Given the limitations of Bluetooth and Zigbee, the IEEE 802.15.6 standard has been recently developed to dedicated WBAN technology. 802.15.6 was designed to provide a low-power, short-range, and highly reliable in-body or on-body communications. The standard uses different frequency bands defined by different PHY layers. These are the

—Human Body Communication (HBC) band :10-50 MHz

—Narrowband (NB): 0.4, 0.8, 0.9, 2.3, and 2.4 GHz

—Ultra Wideband (UWB): 3.10-11.20 GHz

However, not all the bands are suited for every WBAN application. For instance, HBC is incapable of supporting voice or video applications and UWB operation falls out of the unlicensed ISM bands and can only be used by authorized persons or institutions.

3.3.2 MAC layer protocols for WBAN. Various MAC protocols have been proposed for WBAN in order to address the rigorous communication requirements discussed above. Since WBANs and WPANs are similar in many respects, many of these protocols adopt the 802.15.4's superframe structure. Nonetheless as aforesaid, 802.15.4 doesn't fair well in WBAN's high QoS and time-critical communication requirements [9]. Discussed below are proposed WBAN-specific protocols that do not adopt this structure[12]. Emphasis is placed on how energy inefficiencies resulting from idle listening, collision, control overhead, and overhearing are tackled.

Battery-Aware TDMA Protocol
This protocol is designed to maximize the network lifespan. Variables such as queuing characteristics and battery properties are considered in the design. The problem of idle listening is addressed by using a cyclic wakeup mechanism. Each node is assigned a dedicated GTSs wherein data is transmitted when the coordinator's beacon is received. This ensures timely packet delivery and reliability. End nodes remain in sleep mode for an inactive period of time to save energy. this protocol, however lacks a mechanism defined for emergency data.

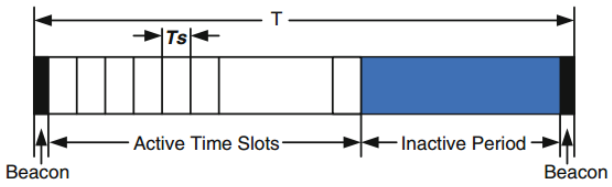

Fig. 6. Battery-Aware TDMA Protocol frame structure

Priority-Guaranteed MAC Protocol
Here, the active period is subdivided into 5 parts to handle various traffic types. Control Channels AC1 and AC2 are used for randomized ALOHA-based uplink control of critical health applications and consumer electronics applications respectively. Additional slots: TSRP and TSRB, are reserved for periodic and burst data respectively. Nodes are synced by a beacon and they transmit data in GTSs. The protocol's primary drawbacks are frame complexity and intolerance to emergency data traffic.

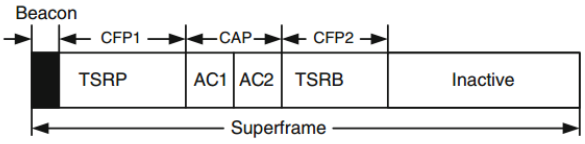

Fig. 7. Frame structure of the Priority-Guaranteed MAC Protocol

Energy-Efficient Medium Access Protocol (EMAP)
EMAP centrally controls periodic sleep and wakeup mechanisms in order to maximize energy efficiency. A star topology with a central coordinator is assumed to control with up to a maximum of 8 slave nodes. EMAP has 3 operational parts: link establishment, alarm process and wakeup scheduling. When a node requests to join the cluster, link establishment is triggered. Each successfully linked device is then given with a different sleep time to avoid overhearing and idle listening. The alarm process is initiated to facilitate communication of emergency data. The Wakeup Fallback Time (WFT) mechanism is used to ensure reliable communication. The drawbacks of EMAP are highly complex implementation, lack of on-demand data mechanism, limited node number and slow per node link establishment process.

A Power-Efficient MAC Protocol for WBANs
This protocol uses two wakeup mechanisms to improve transmission reliability required by varied traffic types. Traffic-based wakeup handles normal traffic whiles the wakeup radio mechanism manages emergency/on-demand traffic. A new superframe structure is defined which is divided into beacon, Configurable CAP (CCAP) which uses slotted ALOHA for short data bursts, and CFP for collision free communication. An application-dependent traffic-based wakeup table is maintained by the coordinator for control. Energy losses due to idle listening and overhearing is eliminated.

Energy-Efficient Low Duty Cycle (ELDC) MAC Protocol
ELDC efficiently utilizes TDMA to maximize network life and accommodate large data streaming. A master node is tasked with network synchronization and coordination. The multi-slotted frame is divided into node-dedicated and reserved time slots. Reserved time slots facilitate emergency/on-demand traffic communication. Guard bands are inserted between successive slots to prevent packets transmission collisions due to clock drifts.

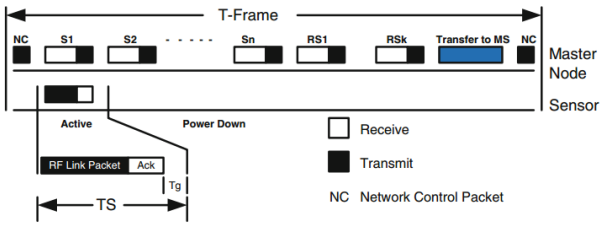

Fig. 8. ELDC MAC Protocol frame structure

BodyMAC
BodyMAC improves energy efficiency by using TDMA-defined uplink and downlink subframes. The protocol achieves improved control packet transmission and network stability using 3 efficient and flexible bandwidth management procedures to support different data streaming. These are the Periodic Bandwidth, Burst Bandwidth and Adjust Bandwidth procedures. The downlink manages on-demand traffic while a beacon syncs nodes. The uplink subframe is divided into a CSMA/CA-based CAP and CFP. In CAP, nodes send requests to the coordinator for GTSs. Nodes are assigned GTSs for energy efficient collision-free communication in CFP.

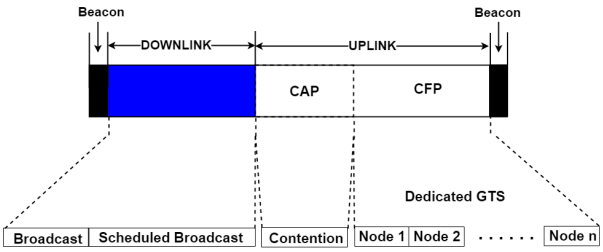

Fig. 9. ELDC MAC Protocol frame structure

Heartbeat-Driven MAC Protocol (H-MAC)
H-MAC employs the heartbeat rhythm for synchronization instead of periodic coordinator control messages. Each node gathers the rhythm information from sensory data for syncing. This reduces overall energy consumption and controls idle listening and overhearing. The protocol adopts the star network topology where a coordinator calculates the sync frame cycle. H-MAC assigns GTSs to sensor nodes for collision-free data communication. A limit to this protocol is the fact that not all sensors can access the heartbeat rhythm. Thus, nodes cannot by synced with the system. Attempts to integrate such sensors with other nodes to access the rhythm increases complexity.

Medical Medium Access Control (MedMAC) protocol
MedMAC improves power efficiency and channel access by utilizing the TDMA approach to assign variable length and application-dependent GTSs to end nodes. An optimal contention period is utilized for initializing network and managing low data streaming and emergency traffic. Coordinator and nodes syncing is achieved by timestamp scavenging with the Adaptive Guard Band Algorithm (AGBA). Synchronization using AGBA and unique GTS assignment eliminates packet collision. AGBA defines guard band sizes by using the Drift Adjustment Factor (DAF).

3.3.3 Network layer protocols for WBANs. Specialized routing strategies have been proposed to meet WBAN unique needs. These protocols are generally grouped into Cluster-based, Temperature-aware, QoS-aware, and Postural-Movement-based routing protocols.

Cluster-based routing protocols
In these protocols, nodes are sectioned into clusters with each cluster selecting one node act as cluster head using different methods. Data from all nodes in a cluster are routed through cluster heads to the central station (sink). This reduces direct interaction between nodes and the sink. Examples of these protocols are AnyBody and Hybrid Indirect Transmission (HIT) [8].

Temperature-aware routing protocols
For wireless transmission in, on or around the human body, important issues such as radiation energy absorption (quantified by Specific Absorption Rate (SAR)) and heating effects are considered. Limiting of radio transmission power or the use of thermal-aware traffic control algorithms are used to reduce tissue heating. Proposed temperature-aware routing protocols include Least Temperature Rise (LTR), Adaptive Least Temperature Rise (ALTR), Thermal-Aware Routing Algorithm (TARA), and Least Total Route Temperature (LTRT) [2, 8].

QoS-aware routing protocols
These protocols utilize different modules for different QoS metrics. Examples of protocols are Routing Service Framework, Data-Centric Multi-Objectives QoS-Aware Routing (DMQoS),QoS-Aware Peering Routing for Reliability-Sensitive Data (QPRR), and Reinforcement Learning based Routing Protocol with QoS Support (RL-QRP). [2]. These protocols have high design complexities due to effective module coordination requirements.

Postural-Movement-based routing protocols
These protocols are aimed at solving the problem of link disconnection caused by body postures and movements. The protocols choose lowest cost routes to forward the packets from the sensor devices to the sink. The cost function is updated periodically. On-Body Store and Flood Routing (OBSFR), DTN Routing with Dynamic Postural Partitioning, Probabilistic Routing with Postural Link Cost (PRPLC), and Opportunistic Routing protocols are examples [2].

3.3.4 Cross layer protocols for WBANs. Cross-layer design is a high-interest but less-researched area where effort is made to

Table 1. A comparison of key enabling technologies for wearable networks

Parameter	WiFi (802.11 a/b/g/n)	Bluetooth (802.15.1)	BLE (802.15.1)	ZigBee (802.15.4)	802.15.6
Operational Modes	Infrastructure Ad-hoc	Ad-hoc	Ad-hoc	Ad-hoc	Ad-hoc
PHY Layers	NB	NB	NB	NB	HBC, NB, UWB
Frequency Bands (GHz)	2.4 5.0	2.4	2.4	0.868	0.01-0.05
				0.915	0.4, 0.8, 0.9, 2.3, 2.4
				2.4	3.10-11.20
Communication Range	Up to 250m	100m	$<$100m	Up to 75m	Up to 10m
Maximum Data Rate	Up to 1 Gbps	Up to 3 Mbps	Up to 1 Mbps	20 Kbps (0.868 GHz)	10 Kbps - 10 Mbps
				40 Kbps (0.915 GHz)	
				250 Kbps (2.4 GHz)	
Power Consumption	(˜800 mW)	Medium (˜100 mW)	Low (˜10 mW)	Low (˜60 mW)	Ultralow (˜1 mW for 1 m range)
Network Topology	Infrastructure-based	Piconet, Scatternet	Piconet, Scatternet	Star, Tree, Mesh	Inter-WBAN: non-standardized
					Intra-WBAN: 1 or 2 hop star
Topology Size	˜2000 nodes for structured BSS	Up to 8 nodes per Piconet	Up to 8 nodes per Piconet	Up to 65536 nodes per network	Up to 256 nodes per body
					Up to 10 WBANs per $6m^3$
Target BAN Architectures	Off-Body	On-Body	On-Body	Body-to-Body	In-Body
				Off-Body	On-Body

improve the overall efficiency of a network by combining multiple layers of the protocol stack. An alternative approach is entirely abandoning the stratified structure and implementing the needed functionality in separate interactive and dynamic modules. Cross layer protocols for WBANs include Cascading Information Retrieval by Controlling Access with Dynamic Slot Assignment (CICADA), Timezone Coordinated Sleeping Scheduling (TICOSS), and Wireless Autonomous Spanning Tree Protocol (WASP) [2, 8].

3.4 Coexistence and Interoperability in WNs

Nearly all discussed WN related technologies operate in the same frequency bands. This gives rise to phenomena such as adjacent channel interference and other significant interruptions. The issue of coexistence of these technologies is thus a paramount concern for today's hybrid technology applications. Coexistence strategies, both collaborative and non-collaborative, exist to mitigate this problem. These approaches often require information sharing, hence interoperability is very essential. The 802.15.6 standard proposes non-collaborative strategies such as channel hopping, beacon shifting, and superframe interleaving. CSMA/CA is often considered as inherently collaborative scheme since nodes sense the channel before transmitting to avert collision and interference[1]. The performance of coexistence schemes depends on applications requirements such as mean packet reception ratio, latency, and energy efficiency. Therefore, the optimal scheme can be selected based on binding constraints.

3.5 Other Notable Wearable Network Technologies

In addition to the discussed standardized wearable network technologies(summarized in Table 1), other proprietary ones have been developed and tailor-made for some commercial application. These technologies include ANT, Sensium, RuBee, Zarlink, Z-Wave, Wavenis, BodyLAN, EnOcean and ONE-NET, and Dash-7.
ANT, the most popular amongst this group, is an ultra low power multicast WSN technology designed and proprieted by ANT Wireless. It operates in 2.4 GHz ISM band and has a maximum communication range of 100m [6]. Designed for efficiency, ease of use, and scalability, ANT can easily adopt peer-to-peer, tree, star, and fixed mesh topologies. ANT provides adaptive and flexible isochronous network operation, reliable data communications, and immunity to cross-talk. The ANT protocol stack is extremely compact, requiring minimal hardware resources and considerably cheap to implement. ANT is a popular choice for sporting wearable applications.

4. RESEARCH TRENDS

There are a great deal of research works ongoing in the field of wearable networks towards the enhancement of their architectures and enabling technologies. For WBANs, movements of the human body and shadowing hamper the propagation of electromagnetic waves between nodes. Due to the degenerating effects of frequent time-varying and multipath fading on radio links, the development of accurate and efficient channel, path-loss and mobility characterization models has been subject of active investigation for many researchers.
Additionally, there is focus on developing more MAC protocols that address WBAN specific requirements. In this area, researchers are seeking to further reduce energy dissipation due to overhearing and idle listening by using adaptive duty cycles and blended traditional (random access and scheduled access) protocol methods and properties.
Stronger mechanisms aimed at reinforcing privacy and security in wearable networks also being explored. One of the high-interest security architecture component is the generation and management of keys for safeguarding data authenticity and integrity. A promising new frontier in key management is the use of biometrics where authentication is effected using a person's behavioural or physiological features. Some algorithms which are able generate secure encryption keys using the heartbeat rhythm of a system actor have been developed[8].
Software defined multiple-standard cognitive radio and cross layer optimized solutions are widely considered as the future of wearable networks.

5. CONCLUSION

This paper has detailed requirements and characteristics of wearable networks and the various technologies available for implementation. The field of wearable networks is a very broad and fast growing one with a nearly endless stream of applications. Ongoing research in the area is very open and promising with cross-layer networking and software defined multiple-standard cognitive radio solutions being the major focus. However, for effective realization of wireless body area network applications with multi-standard nodes, the issues of coexistence and interoperability needs to be critically investigated.

6. REFERENCES

[1] Muhammad Mahtab Alam, Dhafer Ben Arbia, and Elyes Ben Hamida. Research trends in multi-standard device-to-device communication in wearable wireless networks. 04 2015.

[2] Javed Bangash, Hanan Abdullah, Mohammad Hossein Anisi, and Abdul Khan. A survey of routing protocols in wireless body sensor networks. *Sensors (Basel, Switzerland)*, 14:1322–57, 01 2014.

[3] Maria Calle and Joseph Kabara. Mac protocols used by wireless sensor networks and a general method of performance evaluation. *International Journal of Distributed Sensor Networks*, 2012, 01 2012.

[4] William R. Deiter, Srabosti Datta, and Wong Key Kai. Power reduction by varying sampling rate. In *IEEE International Symposium on Low Power Electronics and Design, San Diego, CA, USA*, 2015.

[5] Mohammad Ghamari, Balazs Janko, Robert Simon Sherratt, William S. Harwin, Robert Piechockic, and Cinna Soltanpur. A survey on wireless body area networks for ehealthcare systems in residential environments. In *Sensors*, 2016.

[6] Chin Harrison. Ant message protocol and usage. *Dynastream Innovations Inc.*, 5(1):1–134, 2014.

[7] Thaier Hayajneh, Ghada Almashaqbeh, Sana Ullah, and Athanasios Vasilakos. A survey of wireless technologies coexistence in wban: Analysis and open research issues. *Wireless Networks*, 20:2165–2199, 11 2014.

[8] Benot Latre, Bart Braem, Ingrid Moerman, Chris Blondiam, and Piet Demeester. A survey on wireless body area networks. *Wireless Networks*, 17(1):1–18, 2011.

[9] A. Rahim, N. Javaid, M. Aslam, Z. Rahman, U. Qasim, and Z. A. Khan. A comprehensive survey of mac protocols for wireless body area networks. In *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, pages 434–439, Nov 2012.

[10] Andrew S. Tanenbaum and David J. Wetherall. *Computer Networks*. Prentice Hall Press, Upper Saddle River, NJ, USA, 5th edition, 2010.

[11] A. C. W. Wong, M. Dawkins, G. Devita, N. Kasparidis, A. Katsiamis, O. King, F. Lauria, J. Schiff, and A. J. Burdett. A 1 v 5 ma multimode ieee 802.15.6/bluetooth low-energy wban transceiver for biotelemetry applications. *IEEE Journal of Solid-State Circuits*, 48(1):186–198, Jan 2013.

[12] Feng Xia and Azizur Rahim. *MAC Protocols for Cyber-Physical Systems*. 06 2015.