Comparison and overview of Wireless sensor network systems for Medical Applications

Avijit Mathur, Thomas Newe
Optical Fibre Sensors Research Centre
Department of Electronic and Computer Engineering
University of Limerick
Limerick, Ireland

Abstract— **The need for technology to assist in medical monitoring applications is becoming more necessary in society as the number of patients in hospital and clinics continues to grow. The demand on staff to monitor every individual consistently becomes necessary. Wireless sensor networks (WSN) are now being used to facilitate this on-demand monitoring both at the patients home and in the hospital/clinic environment. This paper looks at the basic parameters necessary for a medical based WSN with particular focus on communication platforms and their security. These parameters will be compared and contrasted, and the main components necessary to form an ideal medical WSN will be highlighted.**

Keywords-sensors; WSN architecture; WSN security; wireless platform; medical WSN;

I. INTRODUCTION

A wireless sensor network (WSN) system is able to perform activities that help reduce the workload for the duty staff and provide more freedom for patients. Research into the use of WSNs for healthcare applications is ongoing in the area of technologies, methods and mechanisms. For example, normal monitoring of vitals, capsule endoscopy, monitoring of body motion for Parkinson's diseases, early warning systems predicting attacks e.g., EEG reporting symptoms of Epilepsy, ECG for measuring heart functions and pulse oxi-meter for blood saturation levels. Moreover, project CodeBlue includes systems supporting emergencies, [1], and everyday monitoring systems include HealthOS by HiNRG [2]. Others like UbiMon, monitor the patients in their natural environment as it helps analyse their physiology more accurately [3]. Tyndall research centre focuses on environment, fitness and health applications .

This paper is structured as follows. In section (ii) the general layout/architectural structure of Medical Wireless Sensor Networks (MWSN) is discussed and the necessary equipment is outlined. In section (iii) the communication protocols/standards necessary for the effective operation of MWSN are outlined and compared. The final section, (iv), discusses issues that apply to all MWSN's regardless of protocol used or topology employed, such as; energy management, routing protocols, security of data, issues and challenges. Finally, the conclusion endeavours to inform the reader of the best compromise between protocol selection, network topology and necessary security requirements.

II. ARCHITECTURE

This section provides a brief description of the system layout in the home and hospital environment settings. WSN architecture makes use of some layers of the OSI model. Three cross layers assist them: task management, mobility management and power management that are responsible for network management. They also improve the overall power efficiency by making the sensor nodes work in co-ordination [4].

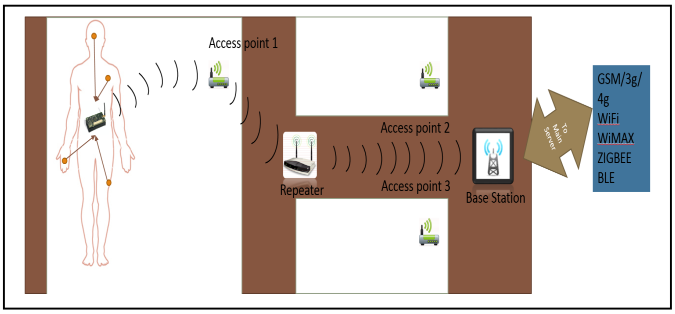

Figure 1. Home/hospital environment WSN system

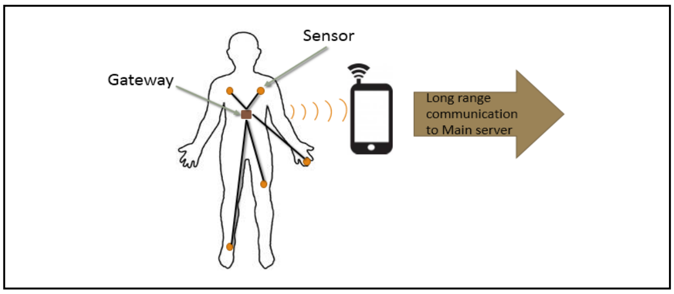

Figure 2. Work environment WSN system

Some of the key issues the architecture must address are: 1) concurrency, as there are several parallel operations like data encoding and channel monitoring. 2) Flexibility, as the system may be applied to different applications in the medical field or otherwise. 3) Synchronization, as it provides control of radio transmission timing. Finally, 4) RF and decoupling of processing speed that helps improve energy performance [5].

TABLE I. COMMUNICATION PROTOCOLS

Metric/Platform	ZIGBEE	Bluetooth Low energy (BLE)	Wi-Fi
Range	10-100 m	>60m (10m for Classic BT)	Depends on specification
Power	Low	Very Low (High for classic BT and medium for others)	High (variable for Wi-Fi Direct)
Entries	254 (>64000 per network)	2 Billion (Classic: 7)	Depends on number of IP addresses
Latency	Low	3 ms (compared to 100ms in classic BT)	Variable
Self-healing	Yes	-	Yes
Topologies	Mesh, Star and Cluster-tree	Star	Star, Point-to-Point
Data transmission rate	Up to 250Kbps	1Mbps (BT v4.0: 25Mbps)	11Mbps & 54Mbps (250 Mbps: Wi-Fi Direct)
Bandwidth	2.4GHz, 915MHz & 868 MHz	2.4 GHz only (BT + HS: 6-9 GHz)	2.4, 3.6 & 5 GHz
Transmission technique	DSSS	Adaptive FHSS (Classic BT: FHSS)	DSSS, CCK & OFDM

The sensors comprise of wearable body sensors required to monitor the vitals of the individual thereby accumulating data into the gateway or access point residing on the person's body. These access points and repeaters relay the data to the base-station which in-turn is responsible for sending it to the main server in the hospital or to a doctor's PDA/cell-phone/desktop. Fig. 1 illustrates a common in-house/hospital set-up. Here the base station is usually stationary. Fig. 2 illustrates a more mobile set-up using smartphones, which are flexible in-terms of mobility and energy consumption.

III. PROTOCOLS AND STANDARDS

There are several existing communication protocols and standards, e.g., IEEE 802.3, 802.11, 802.15 and 802.16. This section outlines 802.15.4 and 802.15.6 standards in conjunction with ZigBee, Bluetooth and Wi-Fi protocols. The features outlined suit the requirements of MWSNs.

A. IEEE 802.15.4

This standard defines physical (PHY) and MAC layers for Low rate Wireless Personal area Networks (LR-WPANs). Its advantages are low power consumption, dynamic device addressing and low latency device support. Reduction in duty cycle achieves low power consumption with the help of super-frame structures. These structures allow the sensor nodes to sleep during their period of inactivity [6].

The standard supports three schemes namely 2.4 GHz, 915 MHz and 868 MHz. Considering the 2.4 GHz scheme, some versions of 802.11 WLANs, Bluetooth and microwave ovens might cause interference due to the common frequency band ISM (2.4 GHz). According to an experiment conducted by [7], the microwave oven causes a relatively higher interference with an approximate packet error rate of 4% compared to 3% in Wi-Fi and 2% with Bluetooth or absent interfering source. Moreover this interference is increased when the distance between the source-receiver is small while vice-versa for the same distance between transmitter and receiver. Finally, the channel selection and angle between source-receiver affects the system as well.

This implies that the 2.4 GHz scheme might not be apt for communications in environments involving frequent use of this band for other purposes. While the 868 MHz scheme may not be of use in emergencies, due to its low data rate.

B. IEEE 802.15.6

Reference [8] defines a new standard for the specification of wearable WSNs. It incorporates a compulsory safety procedure and a new PHY layer i.e., Human Body Communications (HBC). The standard supports three operational PHYs. The main responsibilities of these layers are 1) radio transceiver activation/deactivation, 2) Clear channel assessment and 3) data transmission and receiving. Moreover, it defines a new MAC layer in which resource allocation is handled using CSMA/CA or slotted Aloha access procedure. This standard is a step forward in wearable wireless sensor networks as it is designed specifically for use with a wide range of data rates, less energy consumption, low range, ample number of nodes (256) per body area network and different node priorities according to the application requirements.

The standard supports three security schemes 1) unsecured communications level wherein there is no form of security i.e. authentication or encryption. 2) Authentication only, is capable of proving the authenticity of the data source and 3) authentication and encryption provides confidentiality of data in addition to its authentication [9]. Hence, it provides flexibility in security features as encryption might not be required in certain cases e.g. when two parties exchange public information (say public keys).

In [10] the performance of 802.15.6 in comparison to 802.15.4 is evaluated. This reveals that the former has a lower packet loss ratio (PLR) when the payloads are long and vice-versa when payloads are short. However, 802.15.6 incurs more delays compared to 802.15.4, but with added security features and options. Therefore, it is inferred that 802.15.6 may be apt for hospital environment, where more data is to be transmitted, while 802.15.4 is better for personal use by individual patients at home.

C. Communication Protocols

The IEEE 802.15 standard defines the necessary requirements, details and specifications for the communication protocols. Following are the important platforms for WSN implementation:

1) ZigBee: Based on the IEEE 802.15.4 standard, the ZigBee protocol defines the upper layers of the protocol stack and is optimised for systems demanding low energy

TABLE II. ROUTING PROTOCOLS ENERGY MANAGEMENT TECHNIQUES

Routing protocols	Description
Directed diffusion	Based on a publish/subscribe model; it uses caching & data processing to conserve energy [11]
SPIN (S)	If node has enough energy then protocol uses 3-way handshake security mechanism for transmission. In addition, data transmission occurs only when party is interested thus saving energy [12].
LEACH (L)	Use of cluster head rotations & single hop routing balances the energy consumption [13].
PEGASIS (P)	Absence of dynamic cluster formation avoids energy overhead. However, introduces delay for remote nodes [13].
PEGASIS Hierarchical	Reduces delay by simultaneous transmission & solves data collection problem by taking (energy * delay) quantity into consideration [14].
MECN	Low-power GPS & energy efficient relay nodes help improve energy efficiency [13].
COUGAR	Query processing is abstracted from the network layer using declarative queries implying energy saving. Data aggregation also helps save energy [11].
TEEN (T/A)	When the sensed attribute is in the range of interest, only then the nodes can transmit. Thus reducing number of transmissions, and saving energy [14].

consumption with low power and resulting low data rate. This is supported by an experiment conducted, with help of *sensing, aggregation* and *sink* tasks, using the Wireless sensor network simulator, [15]. Due to the low data rate it is difficult to implement in hospitals or clinics (multiple patients) but is ideal for personal use (single patient). A drawback of this technology is low QoS and message throughput.

2) Bluetooth Low energy (BLE): It consists of sleep periods unlike the classic bluetooth, which drops the duty cycle from 1.0% to 0.1%, [16]. A greater modulation index, compared to the radios in previous versions helps to improve the coverage area. Reference [17] proposed and implemented a prototype ECG monitoring system, which uses BLE. The results point to low power consumption, long-term monitoring and portability. However interference with other devices might be an issue as the technology operates in the 2.4GHz ISM band.

Considering the metrics defined in Table I it can be deduced that BLE and ZigBee are apt for communication between thewearable sensor nodes and the AP. This is because of their nominal data rates, low latency and low energy consumption. Moreover, adaptive frequency hop spread spectrum allows BLE to co-exist with Wi-Fi; where the latter can be used for communication between the base station and the Hospital main server.

IV. CRITICAL TOPICS

A. Energy Management

Energy management is an important aspect due to the resource constraints on WSNs. Resource constrained is addressed using the different hardware units [18], layers of the OSI stack, routing protocols, batteries and radio. Here data transmission is one of the most energy and power consuming aspect. Therefore, the communication between the BS and other components must be efficient. However, due to advancement in portable technologies it is possible to have a powerful BS while still keeping the mobility aspect of the system. Table II is an example of the techniques used for improving energy utilisation in routing protocols. Table III describes techniques used for energy management.

TABLE III. ENERGY MANAGEMENT

Categories	Management Techniques	Notes
Physical layer	Dynamic Voltage Scaling (DVS)	Dynamic adjustment of the clock speed with supply voltage, in relation to the instantaneous workload [19]
MAC layer	Collision avoidance & Reduce idle listening periods	Collision calls for retransmission, idle state consumes power
Network layer	Reduce routing table size, use real time routing protocols	Efficient clustering & data gathering techniques
Microcontroller unit	Select MCU according to the requirements of system	Factors: Transition cost, modes power, time spent in each mode [20]
Radio	Algorithms to put radio in sleep state when not required & Dynamic Modulation Scaling	Factors: Transmission power, modulation scheme, duty cycle, mode change
Batteries	Do not draw higher current than specified and relaxation effect	Discharge rate
Sensors	Use optimized hardware components. Scalable signal processing	Signal sampling & conversion, signal conditioning and ADC conversion

TABLE IV. SECURITY ATTACKS

Class	Attacks	Defence
Physical layer	Jamming	Spectrum spread, Signal strength consistency checks, SPREAD, Channel surfing, mode change, low duty cycle
	Tampering	Physical in-access, Encryption, Camouflage, Encryption (some cases)
	Sybil (affects resource allocation & Distributed storage)	Radio resource testing, random key pre-distribution, white-listing, position verification & code verification
Data Link	Exhaustion, unfairness & collision	Error correcting code, rate limitation & small frames
Network	Black Hole attack	Network monitoring, redundancy & Trust management
	Wormhole attack	Keying techniques, handshaking (detection only)
	Neglect & greed	Redundancy & probing
	Spoofing	Egress filtering, authentication, network monitoring, Received signal strength (detection only)
Transport	Flooding	Rate limitation, client puzzles & network monitoring
	De-synchronisation	Synchronisation cookies, authorization

B. *Routing protocols*

Considering monitoring in MWSNs, a routing protocol must incorporate energy management measures, reliable delivery of data and responsiveness to some extent. Possibly, the best compromise, in energy strained environments is PEGASIS (P), since reliability has higher priority than redundant transmissions in MWSNs. Moreover, considering the energy performance, the protocol outperforms LEACH (L) by approximately 100 to 300% for varied topologies and network sizes [14]. Hierarchical PEGASIS may be used as it solves some of the problems of PEGASIS like delay incurred in the single cluster connected to a sink. However, APTEEN may be more applicable when the system requires emergency mode in addition to normal monitoring.

C. *Security*

As an integral part of any system, security of WSNs is treated differently from traditional wired systems in several aspects. The platform is wireless therefore this implies that the channel is more vulnerable to attacks. Considering security mechanisms relating to traditional networks, it is not possible to apply them directly due to the lack of global ID and different network architecture [21]. Moreover, the system is also affected by interference, battery life, sensor quality and surrounding environment. Security & reliability have to be treated with utmost care thereby providing a good Quality of Service (QoS) as the system factors-in the involvement of direct human contact. Some of the basic security services that must be integrated are; 1) authentication 2) access control 3) confidentiality and 4) message integrity. Other security measures may be provided, for e.g., security at the physical layer that can be achieved by manipulating features from the frequency hopping technique, restricted time per hop and hopping sequence [22]. Most security services can be provided by the use of public key cryptography (PKC). This is more secure than symmetric key cryptography as it is generally based upon solving the discrete log problem for low powered systems. However, the energy-constrained environment makes PKC usage difficult [21]. Therefore, some of the systems use it for the distribution of session-keys.

Key management is equally important. This is because it provides security and reliability for the associated keying procedures. An implementation of key management scheme with a test-bed evaluation of a complete system can be found in [23].

Moving to the class of security attacks possible, WSNs may be targeted externally by a laptop or internally through a malicious node. The former is capable of compromising the whole network simultaneously due to its abundant resources while the latter may have capabilities equivalent to another node in the network. Table IV shows security attacks specific to WSNs by categorising them with respect to the layers of the OSI stack model [24] [25] [26] [27].

Due to the differences between traditional networks and WSNs, security protocols have been devised specifically for the latter. Table V shows MiniSec provides high security with low energy consumption thus making it suitable for MWSNs. In addition, LiSP is resistant to many security attacks and provides good security features with Intrusion Detection System (IDS), and reliable key distribution, which has been an important issue for WSNs.

D. *Issues and Challenges*

The main concern regarding WSNs for medical applications is the privacy and security of the patient data and control flow. Reference [28] describes that there is a need for role-based access control (RBAC) which is capable of defining the viewing and modifying rights of different healthcare personnel. Moreover, sensors might capture confidential data. This has led to debates on whether to allow the patient to modify the data. However, this modification can lead to QoS degradation. QoS is a major challenge as the sensors might be placed in harsh environments thereby reducing the accuracy of the data being sensed. The problem is difficult to contain as WSNs rely on low power radios. Another important aspect is the movement of the patient. This brings about the difficulty in implementation of routing. According to [33] there is a need for flexible routing infrastructure, which accounts for the fact that the nodes must dynamically allocate routes on their own because pre-programmed static routes might cause the network to fail. This is due to the motion of patient or/and sensors.

Furthermore, there is a need for a decentralized security mechanism [33], as the use of one entity for handling all the security of the network is not viable.

TABLE V. SECURITY PROTOCOLS

Protocol	Advantages	Disadvantages	Details
TinySec [29]	Flexible, Low overhead, Unauthorized packet detection	Message replay or resource consumption attacks not handled	Skipjack in Cipher-block chaining mode(CBC). Integration with OS
MiniSec [30]	Low energy consumption with high security	When large packets are sending by RF, higher energy consumption	Skipjack in Offset codebook mode (OCB). Simultaneous authentication & encryption
LiSP [31]	Reliable key distribution, robust to Denial of service (DoS) and replay attacks	Security intermediate, requires IDS for better security	Periodic shared key renewal prevents key stream re-use, no requirement of reliable broadcast at data link layer
SNEP [32]	Semantic security, weak message freshness & strong fairness, counter kept confidential	Energy consumption due to Initialisation vector (IV) table	Two party protocol between sensor node and base station
µTesla [32]	Efficient authenticated broadcast	Upper bound on maximum synchronization error must be known by each node	Keep difference between time intervals as low as possible to avoid Message authentication code (MAC) key alteration

E. Factors

Several factors contribute to efficient working of WSNs and its components. Beginning with nodes, it is important to individually secure them in addition to having network security as an attacker might be able to access the sensor nodes or the gateways physically thus initiating several classes of attacks. Moreover, reporting of failed or malfunctioning nodes is important as it assists in the organising and healing of the network.

Group key distribution techniques can help find the balance between security and power usage. This is due to the fact that individual keys for each node make the network secure but degrade the energy efficiency while a single shared key may render the network unsecure.

Furthermore, medical environment calls for higher reporting times under emergency. This feature is important and for example, can be provided with the help of Exclusive access phases period division under the super-frame defined in the MAC layer of IEEE 802.15.6, [8]. Moreover, it can be supported by routing protocols like TEEN/APTEEN as they are designed for critical applications.

F. Ideal System

As shown in Fig. 3, an ideal system would comprise of sensor nodes capable of immense battery power and compact in size. Since the sensors may be used for long-term monitoring it is important that they have long battery life and their size must be small providing greater flexibility for the patient.

A communication protocol that uses the new IEEE 802.15.6 standard fits-in well with required system parameters i.e., range, frequencies and emergency mode. However, currently Bluetooth low energy (B) satisfies the requirements for personal MWSN system with very low power consumption, apt range and low latency.

Considering routing, an ideal protocol would be energy efficient, reliable, dynamic, multi-hop, low in latency, scalable, cost efficient, secure and follow the QoS norms. Therefore, hierarchical PEGASIS fits the needs of MWSN as it is reliable, energy efficient and incurs small delay.

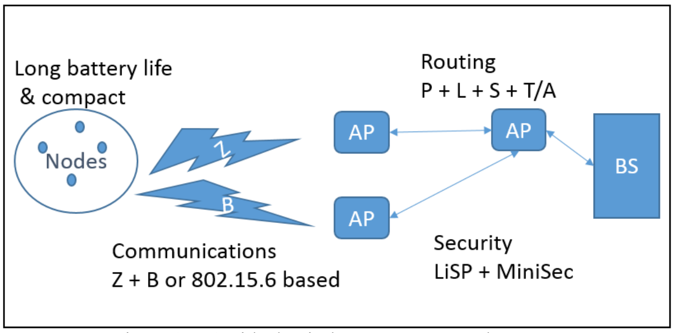

Figure 3. An ideal Wireless sensor network system

Finally, considering security, the reasons described in section IV(c) provide an insight into the construction of an efficient security protocol, which can be achieved by incorporating some features of LiSP into MiniSec. An ideal system must provide authentication, encryption, key renewals and message integrity to avoid masquerading, replay attacks, data theft and message alteration. Therefore, inclusion of a key renewal facility, design of which is out of the scope of this paper, can help achieve the desired properties of LiSP in MiniSec. Usually a combination of fast stream ciphers and a 4-Byte MAC length provides sufficient security with ease of implementation [34].

V. CONCLUSION

Existing communication protocols and standards were compared along with the description of a new standard, IEEE 802.15.6, specifically designed for wearable WSNs. Finally, an overview of different aspects of WSNs has been discussed thus outlining a possible ideal system with parameters from existing systems.

In the future, it is planned to compare different network management strategies and fuse them for the benefit of an efficient and reliable WSN system. Comparison of PKC and symmetric key cryptography with different security mechanism e.g., power and time consumption required for each cryptographic method to arrive at an efficient protocol. Furthermore, future work will look at developing an energy efficient hybrid routing protocol capable of active switching between normal and emergency mode to facilitate the critical responsiveness requirement for emergencies in medical environments.

REFERENCES

[1] Harvard, "CodeBlue: wireless sensors for medical care," 2008. [Online]. Available: http://fiji.eecs.harvard.edu/CodeBlue. [Accessed 3 January 2014].

[2] Hopkins interNetworking Research Group, "HealthOS: A platform for pervasive health applications [HOWTOS]," [Online]. Available: http://hinrg.cs.jhu.edu/joomla/projects/221-healthos-a-platform-for-pervasive-health-applications.html. [Accessed 17 January 2014].

[3] S. Stankovic, "Medical applications based on wireless sensor networks," *Transactions on internet research,* vol. IV, no. 2, pp. 19-23, 2009.

[4] A. A. A. Alkhatib and G. S. Baicher, "Wireless sensor network architecture," in *International Conference on Computer Networks and Communication Systems (CNCS 2012)*, Singapore, 2012.

[5] J. L. Hill, *System architecture for wireless sensor networks,* Berkeley: unpublished, 2003.

[6] J. A. Gutierrez, "On the use of IEEE Std. 802.15.4 to enable wireless sensor networks in building automation," in *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, Barcelona, 5-8 Sept. 2004.

[7] W. M. Healy and M. Zhou, "Impacts of 2.4-GHz ISM band interference on IEEE 802.15.4 wireless sensor network," *Instrumentation and Measurement, IEEE Transactions on,* vol. 61, no. 9, pp. 2533-2544, 2012.

[8] S. Ullah, M. Mohaisen and M. A. Alnuem, "A review of IEEE 802.15.6 MAC, PHY and security specifications," *International Journal of Distributed Sensor Networks,* vol. 2013, March 2013.

[9] K. S. Kwak, S. Ullah and N. Ullah, "An overview of IEEE 802.15.6 standard (invited paper)," in *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 3rd International Symposium on*, Rome, 7-10 Nov. 2010.

[10] F. Martelli, C. Buratti and R. Verodone, "On the performance of an IEEE 802.15.6 wireless body area network," in *Sustainable Wireless Technologies (European Wireless), 11th European* , 27-29 April 2011.

[11] N. A. Pantazis, S. A. Nikolidakis and D. D. Verfados, "Energy-efficient routing protocols in wireless sensor networks: A survey," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* vol. 15, no. 2, pp. 551-591, 2013.

[12] P. Krishnaveni and J. Sutha, "Analysis of routing protocols for wireless sensor networks," *International Journal of Emerging Technology and Advanced Engineering,* vol. 2, no. 11, pp. 401-407, November 2012.

[13] R. Cheour, F. Derbel, O. Kanoun and M. Abid, "Wireless sensor networks with power management for low energy consumption," in *Systems, Signals & Devices (SSD), 2013 10th International Multi-Conference on* , 18-21 March 2013.

[14] K. Akkaya and M. Younis, "A survey of routing protocols in wireless sensor networks," *Ad Hoc Network (Elsevier),* vol. 3, no. 3, pp. 325-349, May 2005.

[15] M. Kohvakka, M. Kuorilehto, M. Hännikäinen and T. D. Hämäläinen, "Performance analysis of ieee 802.15.4 and zigbee for large-scale wireless sensor network applications," *PE-WASUN '06: Proc. 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks,* pp. 48-57, Oct 6, 2006.

[16] J. Decuir, "Bluetooth 4.0: Low energy," 2010.

[17] B. Yu, L. Xu and Y. Li, "Bluetooth Low Energy (BLE) Based Mobile Electrocardiogram Monitoring System," in *Proceeding of the IEEE International Conference on Information and Automation*, Shenyang, 2012.

[18] M. Healy, T. Newe and E. Lewis, "Wireless Sensor Node Hardware," in *Measurement, Instrumentation, and Sensors Handbook, Second Edition, Spatial, Mechanical, Thermal, and Radiation Measurement*, CRC Press 2014, 2014, pp. 1-15.

[19] X. Lin, Y. Kwok and H. Wang, "Energy-efficient resource management techniques in wireless sensor networks," in *Guide to wireless sensor networks*, S. Misra, I. Woungang and S. C. Misra, Eds., London, Springer-Verlag, 2009, pp. 439-468.

[20] V. Raghunathan, C. Schurgers, S. Park and M. Srivastava, "Energy-aware wireless microsensor networks," *Signal processing magazine, IEEE,* vol. 19, no. 2, pp. 40-50, 2002.

[21] L. Xing and H. Michel, "Integrated modeling for wireless sensor networks reliability and security," in *Reliability and Maintainability Symposium, 2006. RAMS '06. Annual*, 23-26 Jan. 2006.

[22] H. Tahir and S. Shah, "Wireless sensor networks - a security perspective," in *Multitopic Conference, 2008. INMIC 2008. IEEE International*, 23-24 Dec. 2008.

[23] S. Möller, T. Newe and S. Lochmann, "Prototype of a secure wireless patient monitoring system for the medical community," *Sensors and Actuators A: Physical,* vol. 173, no. 1, pp. 55-65, Jan. 2012.

[24] X. Yang, T. Bin, L. Qi, Z. Jian-yi and H. Zheng-Ming, "A novel framework of defense system against DoS attacks in wireless sensor networks," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, 23-25 Sept. 2011.

[25] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*, 26-27 April 2004.

[26] V. B. Srinivas and S. Umar, "Spoofing attacks in wireless sensor networks," *International journal of Computer science Engineering and Technology,* vol. 3, no. 6, pp. 201-210, 2013.

[27] T. Newe, V. Cionca and D. Boyle, "Security for wireless sensor networks - configuration aid," in *Advances in wireless sensors and sensor networks*, Berlin, Springer-Verlag, 2010, pp. 1-24.

[28] J. Ko, C. Lu, M. Srivastava, J. Stankovic, A. Terzis and M. Welsh, "Wireless sensor networks for healthcare," *Proceedings of the IEEE,* vol. 98, no. 11, pp. 1947-1960, 2010.

[29] C. Karlof, N. Sastry and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *SenSys '04*, Baltimore, 2004.

[30] F. Ullah, M. Ahmad, M. Habib and J. Muhammad, "Analysis of security protocols for wireless sensor networks," in *Computer Research and Development (ICCRD), 2011 3rd International Conference on*, 11-13 March 2011.

[31] T. Park and K. Shin, "LiSP: A lightweight security protocol for wireless sensor networks," *ACM Trans. embedded computing systems,* vol. 3, no. 3, Aug. 2004.

[32] A. Perrig, R. Szewczyk, J. Tygar, V. Wen and D. E. Culler, "SPINS: Security protocols for sensor networks," *ACM Journal of Wireless networks,* vol. 8, no. 5, pp. 521-534, 2002.

[33] M. Welsh, D. Malan, B. Duncan, T. Fulford-Jones and S. Moulton, "Wireless sensor networks for emergency medical care," in *GE Global research conference*, Boston, 8 Mar. 2004.

[34] P. Kumar, Y.-D. Lee and H. Lee, "Secure health monitoring using medical wireless sensor networks," in *Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on*, 16-18 Aug. 2010.