

# APPLICATIONS, CHALLENGES, SECURITY OF WIRELESS BODY AREA NETWORKS (WBANS) AND FUNCTIONALITY OF IEEE 802.15.4/ZIGBEE

Syed Furqan Qadri, Salman Afsar Awan, Muhammad Amjad, Masood Anwar, Suneel Shehzad  
 Department of Computer Science, University of Agriculture Faisalabad 38000, PAKISTAN  
 E-Mail: [furqangillani79@gmail.com](mailto:furqangillani79@gmail.com), [salmanafsar@hotmail.com](mailto:salmanafsar@hotmail.com), [amjadsadiq786@gmail.com](mailto:amjadsadiq786@gmail.com),  
[masoodanwargcet@gmail.com](mailto:masoodanwargcet@gmail.com), [sunny7642@hotmail.com](mailto:sunny7642@hotmail.com)

**ABSTRACT:** Development in low-power integrated circuits, ultra low-power RF (radio frequency) technology, wireless communications and micro sensors permitted the realization of Wireless Body Area Networks (WBANs). It is one of the latest approaches in medical identification, management and also key building block for future intentional networks and Internet. Wireless BAN has a capability to process and communicate data of heart beat, motion, respiration, body temperature, sound, vibration and blood pressure. Non-invasive sensors can be used to mechanically monitor physiological reading, which can be forward to nearest devices, as cell phone as a gateway. The IEEE 802.15.4 (zigbee) is designed to provide a low-power, low data rate protocol offering a high reliability. In this paper, it is presented an overview of wireless body area networks (WBANs), its applications, challenges and WBAN security concerns. It is provided a detailed investigational Parameters of IEEE 802.15.4 (Zigbee), its Operations, Functionality and comparison with OSI Model and Task Group 6 (TG6) security issues. Finally, it is fetched to light some of the design challenges and open issues that still need to be addressed to make WBANs and Zigbee truly ubiquitously for a spacious range of application.

**Keywords:** RF (Radio Frequency) technology, Wireless Body Area Networks (WBANs), IEEE 802.15.4/Zigbee, Physiological Reading, IEEE 802.15.6 Task Group 6 (TG6).

## 1. INTRODUCTION:

The rising rate of healthcare and the age population in developed countries have introduced great challenges for administration, healthcare contributor and healthcare diligence. There is huge attention in using rising wireless equipment to support remote patient scrutinize in an inconspicuous, consistent and cost effectual manner thereby providing bespoke sustainable services to patients. Wireless Body Area Networks (WBANs) is one such talented tool that has the impending to appreciably improve health care delivery, investigative monitoring, disease-tracking and related medical procedures. A critical feature of WBANs is their ability to provide highly reliable infrastructure for medical devices, especially those implanted in the human body. Wireless Body Area Network (WBAN) consists of a number of economical, trivial, minute sensors which could be situated on the body as tiny intelligent piece, included in to clothing or implanted underneath the skin or entrenched deeply in to the body tissues. Their main purpose is to enable doctors and other medicinal staff to safely supervise the health position of patients. This WBAN technology brings reasonably priced and efficient healthcare resolution to people that will advance their excellence of life [1].

Wireless BANs has applied three standard communication protocols that sponsored by the IEEE standards committee for WSN communications [2]: IEEE 802.15.1 (Bluetooth) [3], IEEE 802.15.3 (ultra wideband, UWB) [4] and IEEE 802.15.4 (Zigbee) [5], and the sketch of communication protocol of IEEE 802.15.6 has been developed for BANs security. A wireless body area network (WBAN) connects independent nodes attached to the body surface, implanted into tissues/body, or detached in the clothing for applications in home/health care, sports, entertainment, defense, insidious

computing and many other areas. WBAN does not force the patient to keep on in the hospital thereby giving much physical mobility.

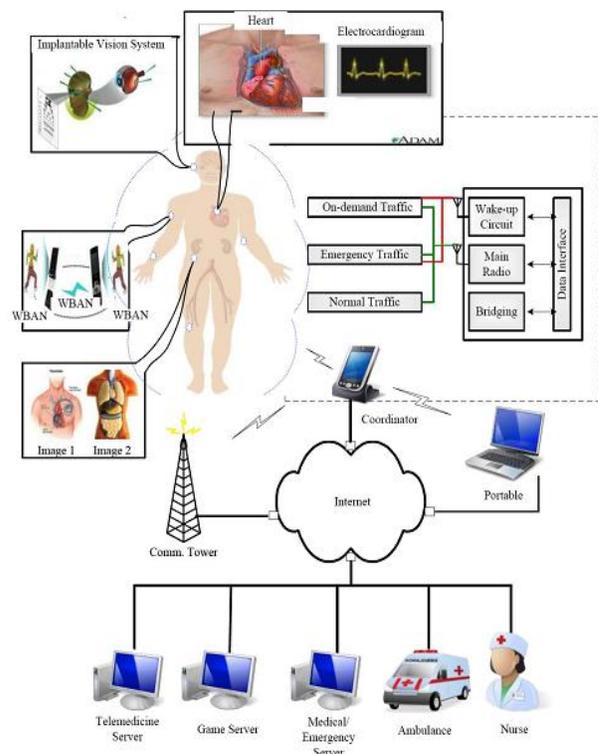


Figure 1: A WBAN infrastructure for medical and non medical applications [6]

Fig. 1 shows a WBAN infrastructure for health check and non-medical appliance. As can be seen in the figure, the

WBAN traffic is sort into On-demand, crisis, and Normal traffic [6]. On-demand traffic is start by the coordinator or doctor to obtain certain information, mostly for the purpose of diagnostic counsel. Emergency traffic is initiated by the nodes when they go above a predefined threshold and should be contain in less than one second. This type of traffic is not produce on regular intervals and is totally changeable. Usual traffic is the data traffic in a normal state with no time critical and on-demand procedures this includes inconspicuous and routine health observe of a patient and treatment of much disease such as gastrointestinal tract, neurological disorders, sarcoma detection, handicap treatment, and the most intimidating heart disease. The normal data is together and processed by the arranger. The coordinator hold a wakeup route, a main radio, and a viaduct function, all of them connected to a data interface. The wakeup circuit is used to provide somewhere to stay on-demand and urgent situation passage. The overpass task is used to establish a logical connection between different nodes working on different regularity bands. The coordinator is further connected to telemedicine, sport, and therapeutic servers for relevant commendation.

## 2. Application of WBAN:

This section covers the applications areas WBAN including E-Health care, lifestyle and sports, military applications, WBAN for animals, Preventing of Cable and Conductor (C & C) Theft and finally its applications in networks and communications.

### 2.1 E-Health Care:

BANs can make available interface for diagnostics, for remote monitor of human physiological data, for administration of drugs in hospitals and as an aid to treatment. In the future it will be possible to monitor patients constantly and give the necessary medication whether they are at home, in a sanatorium or elsewhere. Patients will no longer require to be connected to large technology in order to be monitored.

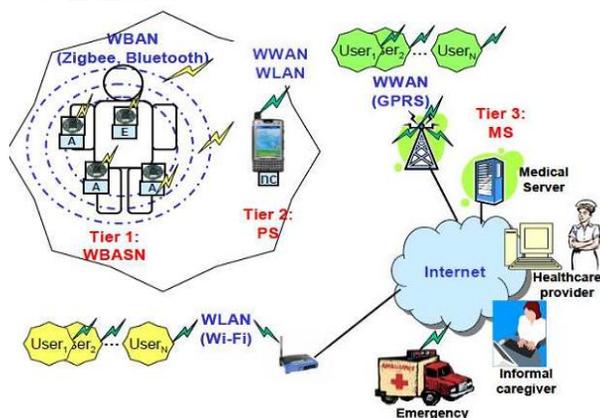


Figure 2: Basic design of E-health care system [7]

### 2.2 Lifestyle and Sports:

In [8], a Wireless BAN is utilizing to resolve the direction of the golf club and the bough of the golfer to offer real-time response to the golfer in terms of hip movement and fondle details on the golf course. The pace and the sway of the golf club can also be resolute. In accumulation, the body sensory data of a player's movement is composed to examine how to

conserve energy and make the player perform at the maximum altitude over a long era of time.

BANs facilitate new functions for wireless body-centric networks including wearable entertainment system (e.g., music entertainment), routing support in the car or while walking, museum, heart rate and performance monitoring in sports, preschooler monitoring, wireless cash card.

### 2.3 Military Applications:

The Army Research Laboratory (ARL) has accomplish experiments using auditory sensor arrays hanging below tethered aerostats to sense and confine fleeting signals from mortars, weaponry and arms fire. This unrelenting inspection can have a influential consequence on the survivability and lethality of our soldiers. Inspiring the array gives a appreciably longer range of detections under flattering MET circumstances. [9]

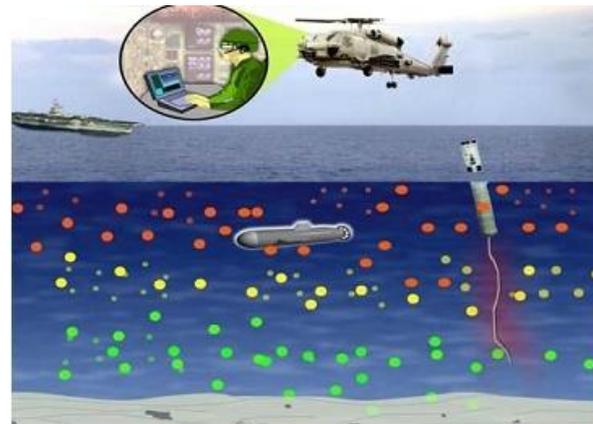


Figure 3: WBAN action in Military Operations [10]

The opportunities for using BANs in the forces are numerous. Some of the military application for BANs includes monitoring health, location, and high temperature and hydration levels. A battle dress uniform included with a BAN may become a wearable electronic network that connects devices such as life support sensors, cameras, RF and personal PDAs, health monitoring, and transports data to and from the soldier's wearable computer. The network could perform functions such as chemical recognition, detection to prevent victims from friendly fire and monitoring of a soldier's physiological condition. Calling for support, his radio sends and receives signals with an antenna blended into his uniform. As a result, BANs present new opportunities for battlefield lethality and survivability.

### 2.4 WBAN for Animals:

Wireless BANs is very beneficial device. It may be used for improving health and diagnosis of different infectious diseases in human being as well as animals. It is very important matter, if want to improve human health and control diseases first we have to improve animals health and control diseases that provide food to the human being e.g. milk, meet, eggs etc One important thing is behind this motive is that human and animals are inter depending each another. There is symbiotic relationship.

### 2.5 Preventing Cable and Conductor Theft:

These are continues reports of cable stealing, both of power cables and of telecommunication line, from many fraction of the world [11]. Wires, especially copper cables, are being stolen for the crumb value of their metal content and this has

Table 1: WBAN Challenges	
Challenges	Wireless Body Area Networks (WBAN)
Scalability	As large as human body parts (mm/cm)
Node Number	Few or more perfect sensor node essential
Node Size	invasive monitoring and they require for minimization
Event recognition	Early adverse events detection fundamental human tissue failure irrevocable
Data defense	High level wireless data transfer security necessary to protect patient's information
Contact	Implantable sensor substitute difficult and requires biodegradability
Bio Compatibility	A must for implantable and some external sensors, Likely to increase cost
Context consciousness	Very important because body composition is very sensitive to context change
Wireless tools	Low power wireless required, with signal detection more demanding

become an gradually more serious issue due to the rise in metal cost. In accumulation to cable theft, the stealing of network members of the lower-end of the tower on the T&D system is a huge risk for utilities as plain in South Africa. Business Against Crime (BAC) South Africa declare that the knock-on effects to the economy is, conventionally, ten times superior than the expenses required for replacing stolen wire. Consequently, in 2008, BAC estimated that South Africa drop in the order of \$800 million a year due to thievery of electricity, telecommunications and railway line wires [12]. skirmishing cable and network theft is a very tough problem as broadcast lines cross many kilometers of remote country through devoted walkway with no effective means of bodily security protection [13].

**2.6 Networking and communications:**

These help the integration with Internet and other networks, low operation and maintenance cost, highly secure wireless communication system to decrease the costs other resources needed to operate a WSN. Cognitive radio play important role in communications in the harsh environment. Some factors are harsh environmental condition that are, interference, highly caustic environments, high humidity levels, vibrations, dirt and dust, or other conditions that challenge its performance.

**3. Challenges of WBAN:**

Wireless BAN is a rising technology, a lot of issues still requirements to tackle, and still a lot of problems need superior solution. WBAN is in front of both moral and technical challenges like confidentiality is most significant and critical ethical issue yet to be addressed correctly [14], and main technical issue is to provide better individual Computer communication. Some technical challenges are shown bellow table as:

**4. Security in WBAN:**

Before instigate encryption, the security strategy must be concentrate on in the rest place. Furthermore, for multi-modal systems such as RFID improved invasive healthcare structure, the security matter for every modality should be deliberate disjointedly and there must be tough mechanisms against all kinds of attacks [15]. Wireless Body Area Networks (WBAN) has provided to help in real-time health monitoring of a patient and diagnose many life threats diseases. It operates in and on, or inside a human body and supports a variety of medical and non-medical applications. This paper show a survey of the security features of the WBAN system which was arranged in The IEEE 802.15.6 standard. It defines the three levels of security. Each security level has its own security properties. These areas, Level 1 it is unsecure mode of communication. In this stage there is no mechanism of checking of authentication and protection. Level 2 it is the level of IEEE in which authentication is checked only. In this level data is not encrypted. Level 3 it is the level of IEEE in which authentication and encryption are checked; it is highest level of security.

In future the ITTT level 3 will be adopted in WBAN for security and security threats.

In WBAN security is the main issue, so for this purpose frequency band selection, channel modeling, antenna design, physical protocol design, energy-efficient hardware, MAC protocol design, QoS and reliability, real time connectivity, networks, regulatory compliance, security and privacy are given importance. The main security issues are

**4.1 Data Confidentiality Integrity:**

Data confidentiality is considered to be the most important issue in WBANs. It is used to protect the data and avoid leaking out the data. Data integrity is also very important in view of life critical events of patient. It may be dangerous. When emergency data of any patient is altered, data may be lost due to bad communication environment.

**4.2 Data Authentication:**

It checks the original source code. If it ignores data authentication then data packet may suffer. It can be achieved by Message Authentication Code (MAC) (to differentiate it from Medium Access Control (MAC) that is generally computed from the shared secret key.

Table 2: Security Methods in communication protocols

Protocols	Bluetooth	Zigbee	TG6
Confidentiality	Yes	Yes	Yes
Integrity	No	No	Yes
Non repudiation	No	No	No
Authentication	Yes	Yes	Yes
Authorization	No	No	No

**4.3 Data Freshness and Secure Localization:**

In this security data is refreshed again and again. Nobody can take old data and reply old messages. There are two types of data freshness: weak freshness, which give partial data to the frames in a sequence but may some delay, and in strong freshness, data frames are sent quickly and there is no delay. In WBAN applications it is necessary to find the accurate location .of patient. In this technique tracking mechanism is applied.

**4.4 Availability and: Secure Management:**

Quick response of patient to the physician .is also necessary, so the physician suggest required medicine or other precautions. If it is slow life may be lost. One of the best ways is to switch the operation of a node that has been attacked to another node in the network. Secure management is also necessary to coordinate the provided key distribution to the nodes of the data in encryption and decryption form.

**5. IEEE 802.15.4 /Zigbee:**

Zigbee requirements of security are data authenticity, data confidentiality and replay exposure. It has 8 security levels, which include encryption and authentication also combined encryption and authentication with deferent security attribute in MAC layer. The security solution of Zigbee does not consider the two most key aspects in symmetric-key cryptography: generation and distribution. The security level of the standard is so unknown, and it relies on which security attribute is selected, the uncertainty of the key in use. The 802.15.4 standard works in three different frequency bands i.e. 16 channels in the 2.4-GHz band, 10 channels in the 915-MHz band, and 1 channel in the 868-MHz band. These channels use the shortest sequence spread spectrum. Distinctive devices are predictable to cover a 10 to 20 m range [16].

The different data, modulation and symbol rates for the related frequency bands are given in table 3 below:

IEEE 802.15.6 Task Group 6 (TG6) standard has been formed with a plan to develop a communication standard optimized for low-power devices and operations on, in, or around the human body to serve a variety of application including medical, customer, electronics or individual entertainment [17]. At current, the latest standardization of TG6 suggests that there are three security levels between nodes and hubs in the protected communication of BANs: unsecured communication, authentication but not encryption, authentication, and encryption. The security service in this plan mainly focused on the key generation,

key distribution, and message authentication, the key generation and distribution are based. TG6 support data rate ranging from 10 Kb/s to 10 Mb/s.

Table 3: Parameters of IEEE 802.15.4 (Zigbee)

Frequency Bandwidth	Physical	Symbols/second	Modulation	Bits Rate(kbps)	Symbol Duration (Ts as μs)
868.0-868.6 MHz	868 MHz DSSS	20000	BPSK	20	50
902.0-928.0 MHz	915 MHz DSSS	40000	BPSK	40	25
2.4-2.4835 GHz	2.4 GHz DSSS	62500	16-ary orth	250	16

**5.1 Zigbee Function:**

MAC layer tasks of IEEE 802.15.4 are: generate network beacons (coordinator), synchronize to network beacons, supporting MAC association and disassociation, supporting MAC encryption, employing unslotted/slotted CSMA/CA system for channel access, and handling guaranteed time slot (GTS) portion and administration. IEEE 802.15.4 expressed 4 frame structures: beacon frame, data frame, acknowledgement frame, and MAC command frame. In data transfer, three type of communication exist: from a coordinator to a device, from a device to a coordinator, and the communication between two peer devices. Data transfers are fully prohibited by the devices rather than by a coordinator. In this context a device either transfers data to the coordinator, or poll the coordinator to receive data, both according to the application-defined rate. This mechanism provides the energy protection feature of the Zigbee/IEEE 802.15.4 network, since the device can sleep when possible, rather than keeping its receiver always active [18].

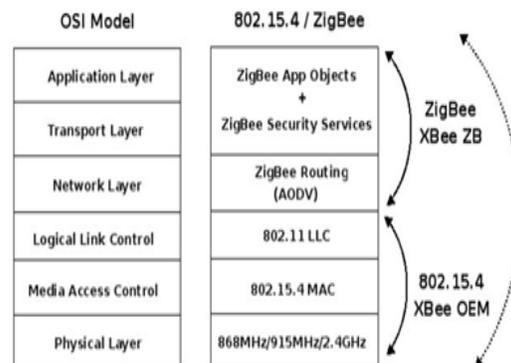


Figure 4: 802.15.4/Zigbee comparison with OSI Model [20]

**5.2 Zigbee Operations:**

Zigbee/IEEE 802.15.4 devices can work in 3 ISM bands, with data transfer rates from 20 Kbps to 250 Kbps [19]. Zigbee standards support three types of topologies star, cluster tree and mesh. Zigbee has the benefit of providing multi-hop routing in either a cluster tree topology or a mesh topology. As a consequence, BAN network coverage can be extended.

Table 4: Sensors commonly employed in BAN systems and their typical data rates [19]

Sensor	Topology	Data rate
Accelerometer/gyroscope	Star	High
Blood glucose	Star	High
Blood pressure	Star	Low
CO <sub>2</sub> gas sensor	Star	Very low
ECG sensor	Star	High
EEG sensor	Star	High
EMG sensor	Star	Very high
Pulse oximetry	Star	Low
Humidity	Star	Very low
Temperature	Star	Very low
Image/video sensor	P2P	Very high

As mention previous to 802.15.4 protocol lies over the level 2 of the OSI. This layer is called the Data Link Layer. Here the digital information units (bits) are managing and controlled to become electromagnetic impulse on the minor level, the physical one. This layer is like to others known ones such as the 802.11 (named under Wi-Fi technology) or the common Ethernet (802.3). The frequencies definite in the standard are spread among 27 different channels divided in three main bands.

**6. WBANs Problems:**

There is lot of issues in WBAN like security attacks, Energy Problem and architecture issue whose details are as:

**6.1 Security Attacks in WBAN**

In WBAN a number of key are attacked. These attacks may be in different ways, i.e., Denial of Service (DoS) attacks, privacy violation, and physical attacks. Due to restrictions on the power consumption of the sensor nodes, protection against these types of attacks is a challengeable task. In WBAN a powerful sensor can easily jam a sensor node and it can prevent collect patient’s data on regular basis. This is the major issue. These attacks on WBAN can be classified into three main types. [21]

Table 5: Attacks on WBAN

Layers	DoS attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tampering Tamper-proof, hiding Tamper-proof, hiding
Link	Collision	Error correcting code
	Unfairness	Small frames
	Exhaustion	Rate limitation
Network	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization monitoring
	Black holes	Authorization, redundancy monitoring,
Transport	Flooding	Client Puzzles
	De-synchronization	Authentication

**6.2 Energy Problem in WBAN:**

In WBAN has an energy problem. In WBAN the sensor nodes should be lightweight in computation and data storage capacity is low, it should be increase. Otherwise the power (energy) and storage capacity may be drained quickly in the system.

**6.3 Architecture issue in WBAN:**

Architecture is the most important issue of WBAN. The architecture of WBAN is divided into three main levels. The lowest level consists of sensors of intelligent sensors which can reduce function in diversely. Many non medical fields as wearable devices such as a headset, MP3 player, game controller devices are included in this level. In second level internet, Cell phone, PDA and mobile server are included. These devices of second level communicate with the external lowest level devices. In the third level all external servers are included which provide various tasks and services. For Example medical server keeps the electronic medicals records of the patients. These server record the information and provide when user demand. Managing data in network and autonomy of each node is an issue. Reducing the use of a node, the management and security insurance in this architecture is major issue.

**CONCLUSION:**

This paper provides a comprehensive overview of WBAN, its applications, challenges and security issues. WBAN can be used to distinguish identity, emergency, medical, military, remote monitoring, and collecting information. In WBAN the main challenges are its security, privacy, flexibility and accountability. WBANs are the provision of appropriate security and privacy protection of the wireless communication medium. The data traveling between the sensors nodes should be kept confidential and integrity protected. These networks when centered on the proximity of human body create a unique structure of protocol IEEE 802.15.4/Zigbee. Zigbee was developed for a communication standard optimized for low power devices and operation around the human body. WBAN is a system that provides smooth less expensive and ambulatory inspection during routine functions works in close association with wireless body area network. It also provides better and cheap substitutions for achieving good health conditions. These systems reduce the enormous costs associated to patients in hospitals as monitoring can take place in real-time even at home and over a longer period. Thus a great benefit goes to patients, physicians as well as the whole society. The goal of this review paper is not to criticize the existing WBAN rehabilitation systems, however serve as an allusion for existing success and to provide direction for future research augmentation.

**REFERENCES:**

[1] Ragesh, G. K., & Baskaran, K. (2012). An Overview of Applications , Standards and Challenges in Futuristic Wireless Body Area Networks. Journal of Computer Science, 9(1), 180-186.

- [2] E. M. Staderini, "UWB radars in medicine," *IEEE Aerospace and Electronic Systems Magazine*, vol. 17(1), pp. 13–18, 2002.
- [3] IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements part 15.1: wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)," *IEEE Std 802.15.1TM*, 2005.
- [4] IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements part 15.3: wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs) amendment 1: MAC sublayer," *IEEE Std 802.15.3b*, 2006.
- [5] IEEE Standard for Information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)," *IEEE STD 802.15.4TM*, 2006.
- [6] S. U., Khan, P., Ullah, N., Saleem, S., Higgins, H., & Kwak, K. S. A Review of Wireless Body Area Networks for Medical Applications. *Sciences-New York*, 1-7(2009).
- [7] Mana, M., Feham, M., & Bensaber, B. A. Trust Key Management Scheme for Wireless Body Area Networks. *International Journal*, 12(2), 71-79(2011)..
- [8] Arvind DK, Bates a (2008) the speckled golfer. In: Proceed-ings of Body Nets 2008. Tempe, USA.
- [9] M. V. Scanlon, C. G. Reiff, L. Solomon, "Aerostat acoustic payload for transient and helicopter detection", *Spie Defense & security Symposium*, Orlando, Florida USA, 9-13 April 2007.
- [10] Hussain, A. WSN Research Activities for Military Application. *Sensors (Peterborough, NH)*, 271-274(2009).
- [11] ICF News. (2008, January) [Online]. [http://www.icf.at/en/6050/cable\\_theft.html](http://www.icf.at/en/6050/cable_theft.html).
- [12] Engineering News. (2007, July) [Online].<http://www.engineeringnews.co.za/article/cabl-e-theft-costs-sa-billions-of-randseveryyear-2007-07-18>
- [13] C. Scott, G. Heath and J. Svoboda (2006, April) Preprint: "Vibration monitoring of power distribution poles." [Online].<http://www.inl.gov/technicalpublications/Documents/3493254.pdf>.
- [14] Kyung Sup Kwak<sup>1</sup>, M. A. Ameen<sup>1</sup>, Daehan Kwak<sup>1</sup>, Cheolhyo Lee<sup>2</sup>, Hyungsoo Lee<sup>2</sup>, A Study on Proposed IEEE 802.15 WBAN MAC Protocols vol 978-1-4244-4522-6/09/\$25.00 ©2009 IEEE
- [15] Y. Xiao, X. Shen, B. Sun, L. Cai, Security and privacy in RFID and applications in telemedicine, *IEEE Communications Magazine*, 44(4) 64-72(2006).
- [16] Ullah, N., Chowdhury, M. S., Khan, P., Ullah, S., & Kwak, K. S. (2012). Throughput and delay limits of chirp spread spectrum-based. *Library*, (May 2011), 1-15. doi:10.1002/dac.
- [17] IEEE-SA IEEE 802.15 WPANTM Task Group 6 (TG6) Body Area Networks <http://www.ieee802.org/15/pub/TG6.html> .
- [18] Zhang, G. H., Poon, C. C. Y., & Zhang, Y. T. (2011). A Review on Body Area Networks Security for Healthcare. *ISRN Communications and Networking*, 2011(1), 1-8, doi:10.5402/2011/692592.
- [19] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. M. (2010). Body Area Networks: A Survey. *Mobile Networks and Applications*, 16(2), 171-193. doi:10.1007/s11036-010-0260-8.
- [20] <http://www.sensor-networks.org/index.php?page=0823123150>.
- [21] S. Saleem, S. Ullah, and K.S. Kwak, A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks, *Sensors*, vol.11, No.2, pp. 1383-1395, 2011.