Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2016, 9, 613-621
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

# Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN)

**Ahmed Alzubi, Arif Sari**

Management Information Systems, Girne American University, Kyrenia, Cyprus
Email: ahmedalzubiit@hotmail.com, arifsari@gau.edu.tr

**How to cite this paper:** Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). *Int. J. Communications, Network and System Sciences,* **9**, 613-621.
http://dx.doi.org/10.4236/ijcns.2016.912047

**Received:** August 22, 2016
**Accepted:** December 27, 2016
**Published:** December 30, 2016



## Abstract

Message integrity is found to prove the transfer information of patient in health care monitoring system on the human body in order to collect and communicate the human personal data. Wireless body area network (WBAN) applications are the fast growing technology trend but security and privacy are still largely ignored, since they are hard to achieve given the limited computation and energy resources available at sensor node level. In this paper, we propose simple hash based message authentication and integrity code algorithm for wireless sensor networks. We test the proposed algorithm in MATLAB on path loss model around the human body in two scenarios and compare the result before and after enhancement and show how sensors are connected with each other to prove the message integrity in monitoring health environment.

## Keywords

Message Integrity, WBAN Security, Health Care Monitoring System, Hash Function, Path Loss

## 1. Introduction

A wireless body area network (WBAN) is constructed in the vicinity of a human body and provides various services for both medical and non-medical services. In order to provide monitoring services for medical devices, routing algorithms for wireless sensor networks (WSN) have been considered for WBANs. WBANs are organized with heterogeneous devices having different characteristics. Thus, directly applying routing algorithms for WSNs to WBANs is inefficient. This study proposes a routing algorithm for WBANs. The proposed routing algorithm considers different communication costs for heterogeneous WBAN devices, and avoids faulty relay nodes for reliable transmission.

A Wireless Body Area Network (WBAN) consists of various electronic devices, either on, in, or around the human body, to support variety of applications, such as medical monitoring and wearable computing. It consists of a coordinator that configures and manages the network and heterogeneous devices or nodes for both medical and consumer electronics (CE) services. IEEE adopted WBAN as the next generation wireless technology for Wireless Personal Area Networks (WPANs), and a task group (referred to as IEEE 802.15.6 TG) within the 802.11.5 working group for WPAN has worked since November, 2007 [1]-[13], to standardize the WBAN technology. WBANs support flexible transmission rates of 10 Kbps to 10 Mbps as well as a very short transmission range of at least 3 m with low power. These characteristics distinguish WBANs from existing WPANs.

WBANs have been utilized as a monitoring tool for medical applications. The nodes in WBANs are tiny sensors, which have limited resources and employee routing algorithms used in wireless sensor networks (WSNs). However, the protocols support various services with different characteristics, such as medical and health care as well as CE services. Since different devices have different levels of energy and generate different size data, using a routing algorithm designed for WSNs in WBANs is inefficient. The algorithms specify low-complexity, low-cost, low power, and reliable transmission as design goals. Thus, a routing algorithm for a WBAN should support not only a variety of devices, but also satisfy these design requirements [10].

## 2. Background of the Study

The network architecture of a WBAN is similar to a WSN, where data from member nodes are forwarded to the coordinator. Thus, routing algorithms used in WSNs are also used in WBANs. The routing algorithms for WSNs are classified as either flat or hierarchical. Since the coverage area of a WBAN is small, the flat routing algorithms, which find the shortest path from the source node to the coordinator, are mainly used. In [14] [15] [16], nodes construct routing tables based on the Destination Sequenced Distance Vector (DSDV) algorithm and each node selects the shortest path as a next hop. Since WSNs consist of only tiny, resources limited devices, energy consumption is the main factor considered in data routing. In [17] [18] [19] [20] [21], routing tables are constructed based on energy cost, where each node determines a routing path by means of a probability function that depends on energy consumption of routing paths. Although the routing algorithms used in WSNs are energy efficient, they are designed for homogeneous sensor devices. A WBAN consists of heterogeneous devices with different characteristics. For example, sensor devices for medical services have similar characteristics as WSN devices. In contrast, devices for CE services require relatively high resources, event-driven data, high transmission rate, etc. Some devices require resource characteristics that lie somewhere between sensor devices and CE devices. In WBANs, serious problems occur if the device characteristics are not reflected in the routing algorithm. For example, when a large data are transmitted via tiny sensor devices, the network lifetime will rapidly decrease. Thus, the proposed of the new algo-

rithm considers not only the design goals of the efficiency sensed message but also the device characteristics.

### 2.1. The Objective of Study

The main objective of this study is solve the problem of path loss and prove the message integrity in WBAN by using use hash function, the study focused on enhancement the guarantee of send and receive information patient in medical area. Message Integrity, Even though received messages are authenticated and encrypted, an adversary can intentionally tamper with the message. In such cases the receiving node should be able to detect such data corruptions and reject the message. Data can also get corrupted due to bad physical conditions of the wireless channel. A common way to deal with message integrity is give identification with description for every sensor node; the proposed algorithm implements the following three modules: Routing Table, error Detector, and Path Selector.

### 2.2. The Research Methodology

This section reviews the research methodology that is used in this study as a way of achieving thesis objectives. In this paper several methods are employed based on different objectives as outlined below:

1. The literature review explains the use of new algorithms to get better sensed data for routing protocols in WBAN, and how to improve that the router received full sensed data from sensor nodes with a hash function algorithm to improve the energy efficiency in the network. This literature reviews and analyses the relevant information in books; theses; working papers; journal papers; conference proceedings; websites and other academic sources, which are searched by using mathematical equations and scientific program to get perfect results .

2. The structure of the new technique is that it will improve the efficiency when used as perfect solution routing protocol which is proposed in an automated way to integrity sensed data, that's by giving identification with description about the data and function for every node. Identification_key technique is designed using the short description based on protocol index.

To evaluate the proposed technique, the study depends on testing the new algorithms by implementing the following three modules: Routing Table Constructor, Error Detector, and Path Selector. When the coordinator transmits a broadcast message with identity to all the nodes to construct the routing table, each node that receives the message executes the Routing Table Constructor module to build its routing table. A node transmits data to the coordinator using the Path Selector module. The error Detector module detects whether or not this node is faulty. A node is considered faulty if it experiences congestion or when missing the identification key, a partial link problem, or a breakdown. If the node is found to be faulty, a message is sent to its neighbor nodes so that they can avoid this node during data transmission. The hash function help node to choose the nearest neighbor.

The cost field indicates the communication cost, i.e., the routing metric, for the path from this node to the coordinator. The level field indicates the level of the device and is different based on the characteristic of the node. The energy field represents the residual energy of the node and the flag field is a Boolean value representing whether or not a path contains faulty nodes. Each node records information of neighbor nodes in its routing table based on the broadcast message from the coordinator.

### 2.3. General Definition of WBAN

We can define the Wireless Body Area Network (WBAN) (Figure 1) as a group of tiny energy-efficient Wireless sensor nodes, which monitor human body biomarkers and at the same time decide the dose that the patient must be taken according to the data obtained via robot, which begins working as a replacement to nurse recently. It has been observed that WBANs proved the efficiency of different network application like computation and storage capacities, also Unlimited efficiency and scalable clearly, new technology developments coincided impacted heavily on the emergence of sensing devices meet the requirements of the patient and make him comfortable with this device that's because he can live a normal life with a small device without needing to connect to wire its mobility support. Technically WBAN application solutions today, push the researchers to do much research to prove the efficiency of this area, the newly research focus on design a new routing protocol or a new algorithm that support the efficiency of protocols.

## 3. The Proposed Method

We add a security layer to message integrity technique to prove the efficiency of message integrity in WBAN; we give the solution for the loss of messages and the change of the message through transfer between sender point and receiver point. That's mean currently the receiver device receiving data does not match with the data sent by patient sensor, this normally occurs because of the bad physical environment, type of wave

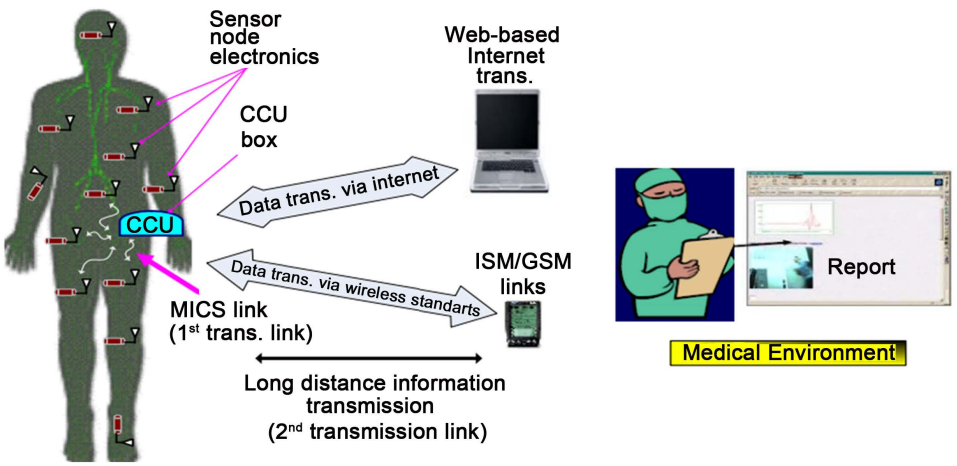


Figure 1. Wireless Body Area Network (WBAN).

transmission and the confusion. In our proposed method we use hash function based for Message Authentication, beside that using the checking factor of path loss, it's a specific method for calculating a message authentication involving a cryptographic hash function in combination with a secret key as shown in Figure 2. The cryptographic hash function calculates the length of the message, the size of its hash output length in bits, and on the size and quality of the cryptographic key.

An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. For example, sensor brain and the reader value 2.0 operate on 512-bit blocks. The size of the output of sensor brain information message length is the same as that of the underlying hash function (128 or 160 bits in the case of sensor brain or 2.0 (reading signal), respectively), although it can be truncated if desired. The proposed solution specification was motivated by the existence of attacks on more trivial mechanisms for combining a key with a hash function. In our platform the sensors on human body send the patient data to the coordinator using identification key by using the hash function with Path loss factor to give message security option, the message will be as: =H(key//message). However, this method suffers from a serious flaw with most hash functions, it is easy to append data to the message without knowing the key and obtain another valid protocol. The routing table for a node has five fields as shown in Figure 3. The id field represents identity sensor.

### 3.1. The Simulation

In the simulation part we prove the reliable and secured data transmission WBAN through proposed a new CRC scheme for data integrity in WBAN. The Previous work in this project enhances the CRC code by adding security key until we provide the requirement of data integrity, authentication and encryption patient information. In this part we give the details of the second objective by applying the first point under two

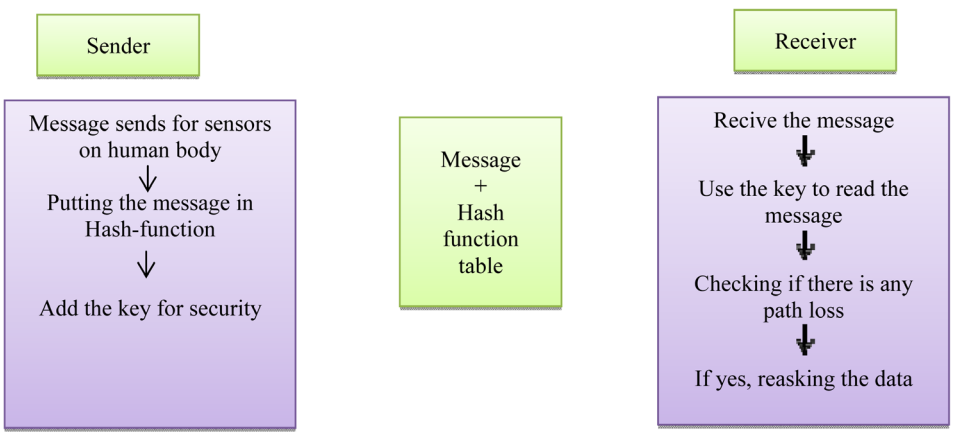


Figure 2. The main diagram of proposed method.

| identity | coast | energy | level | flag |
|---|---|---|---|---|

Figure 3. The ID field represents identity sensor.

scenarios, both of them have same environment but in the different receiver station. The features of WBAN scenarios are listed below:

1) It is a small-scale wireless network for communicating within shorter distance of 3 meters.
2) Using path loss equation to major the loss data on PC.
3) The data rate in WBAN ranges from 10 Kbps to 10 Mbps.
4) The star topology is the fundamental structure considered in WBANs.
5) Sensors possess limited power, computation and communication capabilities.
6) Energy efficient security mechanism is the main goal in the scenario.
7) The network surrounds the body closely for implanting its communication system.
8) WBAN mainly detects, collects and transmits the biomedical information.

### 3.2. The Details of First Scenario

The first scenario uses four sensors around the human body, send data through the MICS band at 400 MHz to PC in the monitoring room. The steps of running as below:

1-collecting data from sensors around the body, there are four sensors in different places (Figure 4 shows the position of the sensors),

2-sended by MICS band to PC (in this scenario there is one-receiver station),

3-checking the path loss, according the path loss factor,

4-using a hash function in checking step (putting information in a table), if the path loss rescues the data from sensors.

### 3.3. The Details of Second Scenario

The second scenario uses four sensors around the human body, send data through the MICS band at 400 MHz to PC and mobile phone in the monitoring room. The steps of running as below:

1-collect data from sensors around the body, there is four sensors in different place (Figure 5 shows the position of the sensors),

2-Send by MICS band to PC (in this scenario there is two-receiver station),

3-checking the path loss, according the path loss factor,

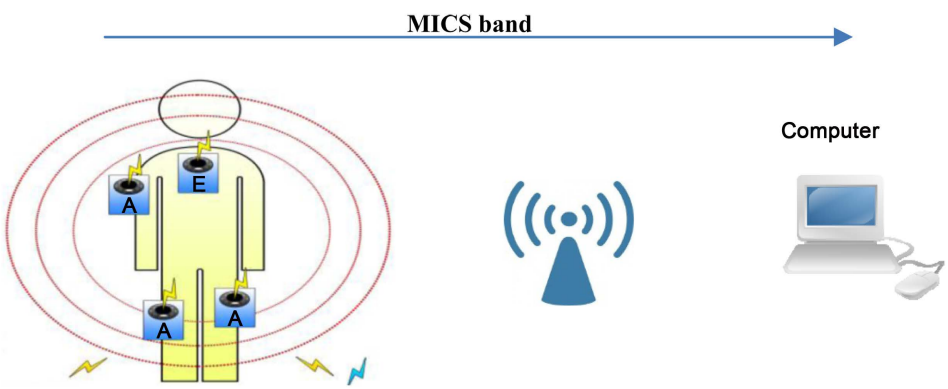


Figure 4. The first scenario.

4-using a hash function in checking step (putting information in a table), if the path loss rescues the data from sensors.

## 4. The Results and Conclusion

The result of simulation depends on the parameters of path loss in both scenarios, and the comparison between different frequencies in case before and after using the proposed method can be seen in Figure 6. In these results, we depend on the path loss equation to measure the path loss value.

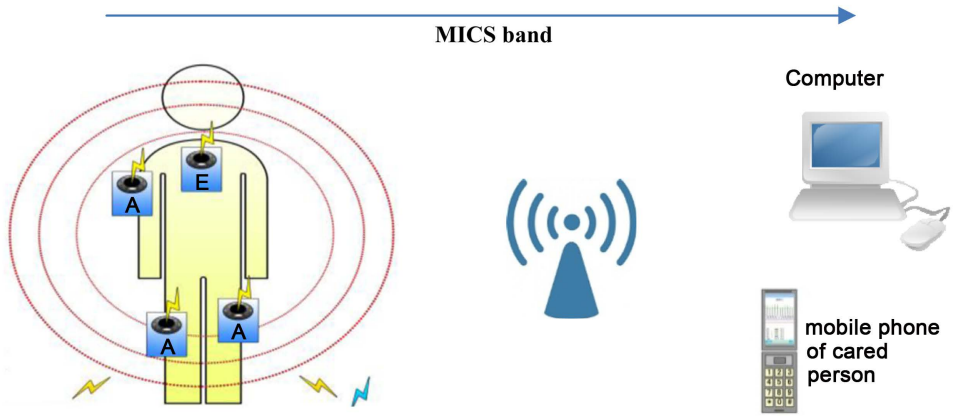


Figure 5. The second scenario.

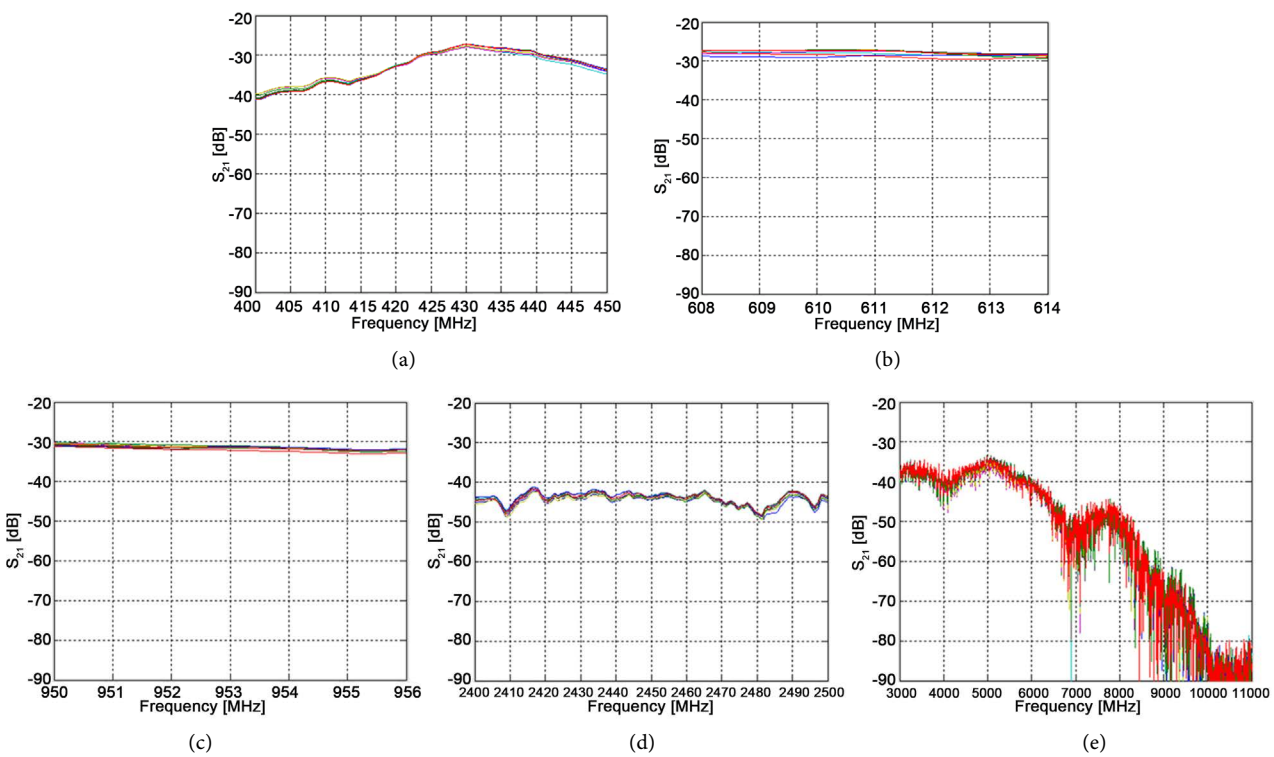


Figure 6. The result of measurment path loss parameters in different freuency bands. (a) 400 MHz; (b) 600 MHz; (c) 900 MHz; (d) 2.4 GHz; (e) UWB.

$$PL_j^p(f) = 10\log_{10}\left|H_j^p(f)\right|^2, p \in \{A-1, A-2, \cdots, J\} \quad [dB] \tag{1}$$

On the previous figures above, the $H(f)$ represents the measurement of the first and second scenario by taking into consideration of one and two receivers. The results collected are based on different frequencies (400 MHz, 600 MHz and 900 MHz) and UWB band

$$L_{path}(d) = a \cdot \log_{10} d + b + N \quad [dB] \tag{2}$$

where $L_{path}(d)$ means the path loss in dB at a distance $d$ mm. $a$ and $b$ denote parameters derived by a least square fitting to the measured average path loss over the frequency range, $l_{path_j}^p(d)$, which is given by

$$l_{path_j}^p(d) = -10 \cdot \log_{10}\left\{\frac{1}{N_F}\sum_{m=1}^{N_F} PL_j^p\left(f(m)\right)\right\} \quad [dB] \tag{3}$$

This paper presents an enhancement to CRC algorithm by using the hash function algorithm based in WBAN to prove the efficiency of sending and receiving data. We accepted the message that has the integrity according to identity table that had all information around the sensors, in addition we used security key for encrypting the patient data before sending, then decrypting the message on monitoring PC and matching between the information on the table and message that we received.

## References


[1] Li, H.-B., Takizawa, K., Zhen, B. and Kohno, R. (2007) Body Area Network and Its Standardization at IEEE 802.15.MBAN. 16t*h IST Mobile and Wireless Communications Summit*, Budapest, 2007, 1-5.

[2] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94.

[3] Kirencigil, B.Z., Yilmaz, O. and Sari, A. (2016) Unified 3-Tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. *International Journal of Scientific & Engineering Research*, **7**, 1001-1011.

[4] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 567-577. https://doi.org/10.4236/ijcns.2015.813051

[5] Rahnama, B., Sari, A. and Ghafour, M.Y. (2016) Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In: Dileep, K.G., Singh, M.K., Jayanthi, M.K., Eds., *Network Security Attacks and Countermeasures*, Information Science Reference, Hershey, PA, 270-312.

[6] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. https://doi.org/10.4236/ijcns.2015.83003

[7] Yilmaz, O., Kirencigil, B.Z. and Sari, A. (2016) VAN Based theoretical EDI Framework to Enhance Organizational Data Security for B2B Transactions and Comparison of B2B Cryptographic Application Models. *International Journal of Scientific & Engineering Research*, **7**, 1012-1020.

[8] Sari, A. (2015) Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey

of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks. In: *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, IGI Global, Hershey, PA, 66-94. https://doi.org/10.4018/978-1-4666-8345-7.ch005

[9] Li, H.-B. and Kohno, R. (2007) Introduction of SG-BAN in IEEE 802.15 with Related Discussion. *Proceedings of IEEE International Conference on Ultra-Wideband*, Singapore, 2007, 134-139. https://doi.org/10.1109/icuwb.2007.4380929

[10] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications*, *Network*, *and System Sciences*, **7**, 365-372.

[11] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 *Fifth International Conference on Computational Intelligence*, *Communication Systems and Networks*, Madrid, 2013, 334-337. https://doi.org/10.1109/cicsyn.2013.79

[12] Shah, R. and Rabaey, J. (2002) Energy Aware Routing for Low Energy Ad-Hoc Sensor Networks. *Proceedings of the IEEE Wireless Communications and Networking Conference*, Florida, USA, 2002, 350-355.

[13] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications*, **2**, 1-6.

[14] Buonadonna, P., Hill, J. and Culler, D. (2001) Active Message Communication for Tiny Networked Sensors. *Proceedings of Joint Conference of the IEEE Computer and Communication Societies*, Alaska, USA, April 2001, 1-11.

[15] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. 2013 *International Conference on Technological Advances in Electrical*, *Electronics and Computer Engineering* (*TAEECE*), 9-11 May 2013, 579, 582.

[16] Kim, D.-Y. and Cho, J. (2009) WBAN Meets WBAN: Smart Mobile Space over Wireless Body Area Networks. *Proceedings of the IEEE International Workshop on Portable Information Devices*, Anchorage, 2009, 1-5.

[17] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. *International Journal of Communications*, *Network and System Sciences*, **8**, 567-577. https://doi.org/10.4236/ijcns.2015.813051

[18] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. In: *Proceedings of the 6th International Conference on Security of Information and Networks* (*SIN*'13), ACM, New York, 454-456. https://doi.org/10.1145/2523514.2523586

[19] IEEE 802.15 WPAN Task Group 6 BAN. http://www.ieee802.org/15/pub/TG6.html

[20] Sari, A., Rahnama, B. and Caglar, E., (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence*, **2**, 11-18.

[21] Otto, C., Milenkovic, A., Sanders, C. and Jovanov, E. (2006) System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring. *Journal of Mobile Multimedia*, **1**, 307-326.