# Reinforcement Learning Based Clock Synchronization in WBAN

**Pallvi, Sunil Kumar Gupta and Rajeev Kumar Bedi**
Department of Computer Science and Engineering, Beant College of Engineering and Technology,
Gurdaspur, Punjab, India
E-Mail: pallvimahz88@gmail.com, skgbcetgsp@gmail.com.com, rajeevbedi@rediffmail.com

*Abstract* **- Wireless Body Area Network (WBAN) is an application of wireless sensor network (WSN). WBAN therefore forms a comprehensive collection of devices that are not only capable of providing continuous information about the health status of a person but also offers helpful details about the activities and environment of the person. In this paper, we have evaluated TDMA based MAC protocol performance through several metrics and TDMA approach is used to avoid packet collision which leads to higher packet loss rate. Reinforcement Based Clock synchronization is the solution of problem like packet collision. After clocks of WBAN sensor nodes are synchronized, data can be transferred between sensor nodes and sink efficiently and rapidly. Reinforcement learning iteratively optimizes the clock synchronization technique. Experimental results indicate that the proposed algorithm is more efficient than existing techniques.**
*Keywords:* **Wireless body Area Network, Throughput, TDMA, MAC protocol**

## I. INTRODUCTION

### A. Wireless Body Area Network (WBAN)

WLAN stands for Wireless Local Area Network whereas WBAN stands for Wireless Body Area Network. There are various thesis and research topics in WBAN. First of all, know the basic concept of WBAN.
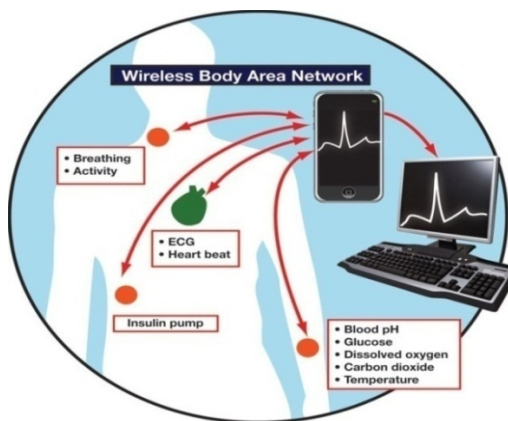


Fig. 1 Wireless Body Area Network [2]

Wireless Body Area Network (WBAN) is an application of wireless sensor network (WSN). WBAN therefore forms a comprehensive collection of devices that are not only capable of providing continuous information about the

health status of a person but also offers helpful details about the activities and environment of the person. It therefore contributes greatly towards gaining a complete understanding of an individual's health and would also enable suitable and appropriate action in case of emergencies. Further the network as a whole is always-on and this permits real-time continuous monitoring. Therefore information obtained from WBAN is more detailed when compared to traditional monitoring methods and hence provides a better insight. WBANs are unique not only in their inherent features, but are also distinctive in terms of the challenges they pose for deployment, operation, maintenance and security. Although WBAN throws open several interesting applications that benefit diverse groups of the society, the heterogeneous nature of the WBAN participant devices gives rise to major challenges that needs to be addressed in the design and practical implementation of WBAN in each of the applications.When WBAN is used as health purpose, the collected data has healthiness information. This information must be safe and not being accessed by unauthorized entities. Non reliable or insecure communication may highly affect health assistance of patient, so the communication must be reliable in wireless body area network (WBAN) [7]. Reliable and Secure communication is also necessary for another application of WBAN.

## II. REINFORCEMENT LEARNING

Reinforcement learning is widely used in wireless body area network. Reinforcement learning is the learning technique of artificial intelligence in which system determines the situations itself and adapts the environment conditions to achieve the desired goal without any supervision. In this technique system learn itself which signal is correct by comparing the current value with the previous values. This algorithm used reinforcement technique by tuning the forgetting factor itself no human interference is required in this.

The algorithm formed by combination of the reinforcement technique and RLS algorithm is known as the reinforcement learning based recursive least square algorithm. In this algorithm no external agent told how to achieve desired signal and which action has to take, system has to learn it by itself how to maximize the signal in the desired direction, to place deep null in the direction of interference, to achieve better convergence speed. This algorithm used

reinforcement technique by tuning the forgetting factor itself no human interference is required in this. System has to decide which signal is better based on his current status and previous status.

RLS algorithm have ability to track fast moving signal because of fast convergence speed but have less stable signal. Therefore, beam formation is not better than LMS algorithm. To solve this problem RLS algorithm is combining with one learning technique known as reinforcement learning technique. By using reinforcement technique speed of convergence and stability in signal both achieve as compare to the RLS algorithm and LMS algorithm. Also this algorithm provides better beam formation than other two algorithms. This Proposed RLS is called as Reinforcement learning based RLS (RRLS) algorithm.

### III. RELATED WORK

WBAN is a very active research field and many studies have addressed this issue using a variety of protocols, relaying mechanisms and topology selection. It has also been shown that persons suffering from cardiovascular diseases, asthma (Chu *et. al.,* 2006), diabetes (Zhao *et. al.,* 2005) can be monitored using wearable health systems. Ng *et. al.,* (2004) proposed UbiMon, composed of wearable and implantable sensors using an ad hoc network. The UbiMon architecture consists of body sensor nodes, a Local Processing Unit (LPU), a Central Sever (CS) and a Work Station (WS). This helps the monitored person to receive immediate professional advice / care based on the continuously monitored data. A general architecture of a RHM system (Chris Otto *et. al.,* 2006) is explained. For instance, a representation of remote monitoring patient architecture suggested for 5G infrastructure by Oleshchuk V & Fensli R (2010). A notable feature of RHM systems is that they generate huge volume of data that needs to be stored at the medical server. In addition, a patient may generally have many healthcare providers including, primary care providers, therapists, specialists etc. (Wu *et. al.,* 2012). Cloud computing has become a promising solution as it could increase the efficiency of data storage and management.

A RHM architecture that uses cloud storage (Mukerjee *et. al.,* 2014) Security is a crucial part of WSN architecture as it is vulnerable to a number of security threats which has variable impact on the network depending on its application (Durresi *et. al.,* 2004). (Gelbestein 2011) refers to the quality of correctness and is achieved by preventing deliberate or accidental but unauthorized modifications, insertions or deletion of data. Wenbo He *et. al.,* (2008) have proposed WSN nodes sense the same parameter and hence integrity can be validated by comparing data from different aggregation trees. On the other hand, each node in WBAN senses a specific physiological parameter and therefore this scheme would not be suitable for WBANs. Vimal Kumar & Sanjay Madria (2010) has proposed a privacy and integrity

preserving algorithm for WSN. Their work is based on Recursive Secret Sharing (RSS). Chen *et. al.,* (2012) have proposed a method that allows the BS to recover all sensing data from the aggregated data sent by other sensor nodes in the network.

Wadhwa *et. al.,* (2013) in their work has proposed a method that assures the integrity of the message. The authors have appended the current date and time to the data and have computed the hash of the same. Sun *et. al.,* (2013) have proposed a watermarking scheme that does not require additional memory to store the watermark. In their scheme, hash of the sensor data is used as the watermark content. Zu *et. al.,* (2013) have suggested an aggregation scheme for WSN which also addresses the problem of preserving data integrity. Park & Shin (2004) have proposed a lightweight key management scheme for WSN.

Their method is cluster-based and each group choses a group head (GH).To control the security of the Group each GH acts as a key server (KS). For the purpose of keying and intergroup communication all KS belonging to the same network form an internal network among themselves. Wang *et. al.,* (2006) in their work for assisted living using WBAN have suggested using a USB stick to store the ring of encryption keys that are generated in prior. Wood *et. al.,* (2006) have used secret keys that have been preloaded in the end-to-end communicating devices for an assisted living and residential monitoring system.

In the literature review, some of the latest and standard paper are discussed in which, it is found that in [1] there is a problem with data lost, in [2] it need some security features, in [3] it discussed a  protocol for data aggregation, in [4] it discussed the various security techniques related to data, in [5] it discussed the repudiation threat is defined so as to recover it data integrity is maintained, in[6] it discussed the various security techniques to share the data securely over the network, in[7] it discussed a remote monitoring patient architecture for 5G infrastructure  in [8] it need to be discussed different reliability requirements, in [9] It should be include the design of a stochastic slot allocation scheme, in [10] the delay of signal should be discussed, and overall many performance metrics are not discussed.

### IV. METHODOLOGY

To achieve the Objectives for minimizing the packet loss, improving the througput and packet delivery ratio using reinforcement learning based clock synchronization for proposed work the following strategies will be adopted

*1. Initial Phase*

Sink broadcasts its location through short information packet. Sensor nodes store position of sink.Every sensor transfers short data packet to sink which holds node ID, its residual energy and location. Sink broadcasts information to all sensors

### 2. Selection of Forwarder Node

Minimum cost function is used to choice optimal information forwarder. Cost function confirms new forwarder in each round

Cost Function (i) = distance (i) / Residual Energy

### 3. Scheduling

Forwarder node assigns TDMA schedule to its children node. Children nodes transfer their information in allocated time slot. TDMA scheduling saves energy of sensor nodes.
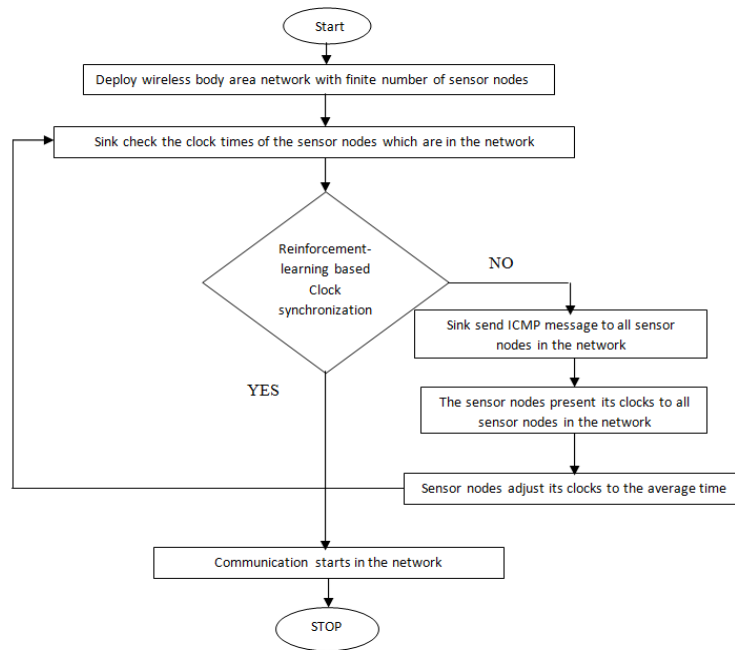


Fig. 2 Flowchart of Methodology

### V. SIMULATION RESULTS AND ANALYSIS

We have showed a general set of experimentations using MATLAB R2013a. It calculates the comparison between the SIMPLE Protocol and PROPOSED protocol. The description of performance evaluation metrics are as follow.

#### A. Network Life Time

It is the amount of time until the first node in the network runs out of energy and mathematically can be represented as:

$$network\ lifetime = minT_k$$

Where $T_k = \dfrac{intial\ energy}{energy\ consumption\ per\ unit\ time}$

As Network life time ought to be higher which implies proposed algorithm is indicating the superior results when compared to access methods as the Network life time is higher in each case.

Network lifetime denotes total network time taken till the latest node die. Figures 3-6 shows that proposed protocol has higher stability period. This is estimated, due to suitable variety of novel forwarder in all rounds. Therefore, in all round of each node obtain approximately identical energy as well as each and every node die almost at the same time. Therefore, these nodes expire initially. Proposed protocol

attains 22% additional stability period as well as 0.4% lengthier network lifetime.
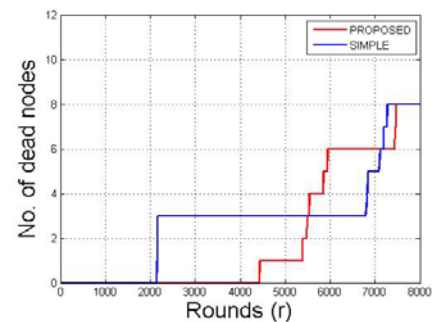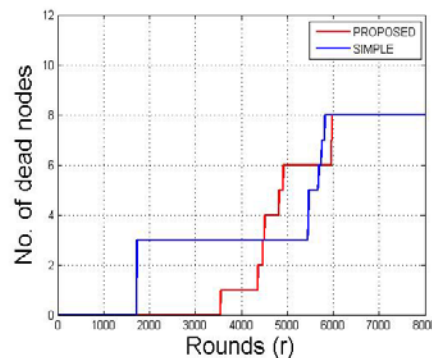


Fig. 3 Network lifetime at EO = 0.3
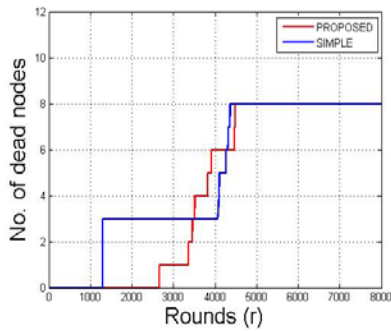


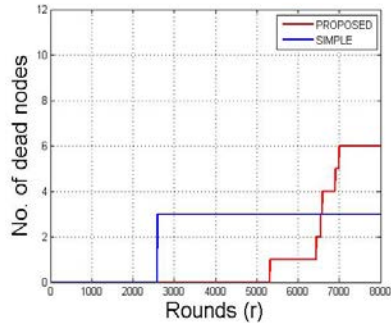Fig. 4 Network lifetime at EO = 0.4

Fig. 5 Network lifetime at EO = 0.5


Fig. 6 Network lifetime at EO = 0.6


Fig. 8 Throughput at EO = 0.4


Fig. 9 Throughput at EO = 0.5


Fig. 10 Throughput at EO = 0.6

While comparing the EXISTING protocol with PROPOSED protocol we have concluded 22% mean improvement has been noticed in respect of EO(initial energy) values at 0.3, 0.4, 0.5, 0.6.

*B. Throughput*

Throughput is defined as; the ratio of the total data reaches a receiver from the sender. The time it takes by the receiver to receive the last message is called as throughput. Throughput is expressed as bytes or bits per second (bytes/sec or bits/sec). Throughput (bits/sec) is represented mathematically as

$$Throughput = \frac{Number\ of\ delivered\ packet\ \times\ Packet\ size\ \times\ 8}{Total\ duration\ of\ simulation}$$

Numbers of active nodes notify the no of packets send to the sink. Extra active nodes send extra packets to sink which results rises in throughput of network. PROPOSED protocol attains high throughput in comparison with EXISTING, as presented in figures 7-10.
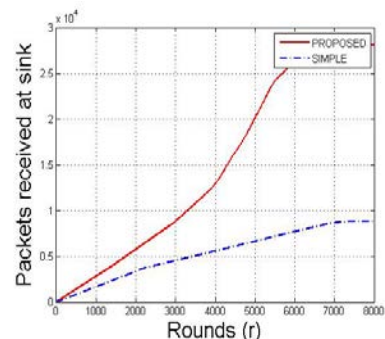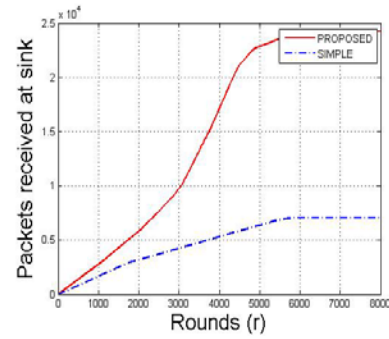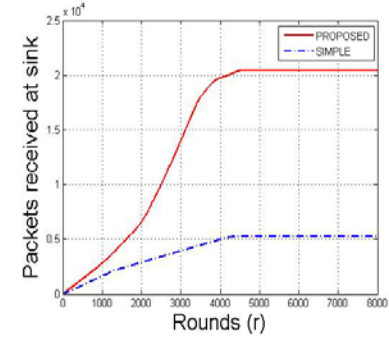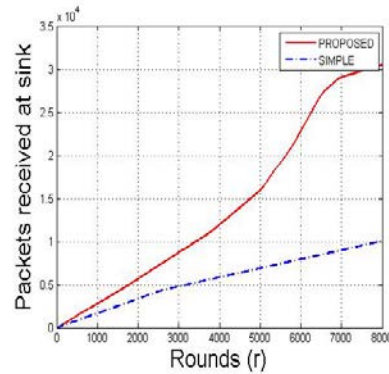

Fig. 7 Throughput at E.O = 0.3

The stability period of EXISTING protocol is smaller than PROPOSED protocol in which no of packets sent to sink diminished. Therefore, PROPOSED protocol realizes great throughput due to extensive stability period. On contrary, throughput of EXISTING protocol diminished.

While comparing the EXISTING protocol with PROPOSED protocol we have concluded higher improvement has been noticed in respect of EO (initial energy) values at 0.3, 0.4, 0.5, 0.6.

*C. Residual Energy*

The proposed model use MAC topology, each extreme node transfers its information to sink over a forwarder node. Forwarder node is chosen by cost function. Choice of suitable forwarder in each round donates to save energy. To transfer packets to sink, MAC topology takes a different forwarder node in each round, this constrains over loading of particular node. The average energy used up by network in every round is shown in figures 11-14.
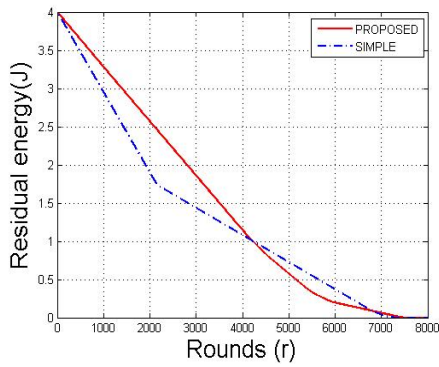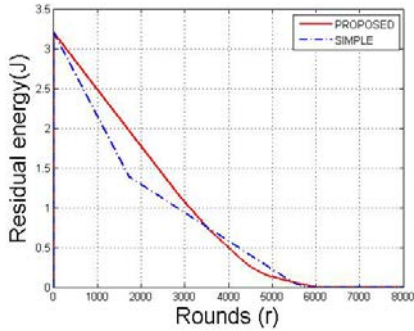
Fig. 11 Remaining energy at EO = 0.3


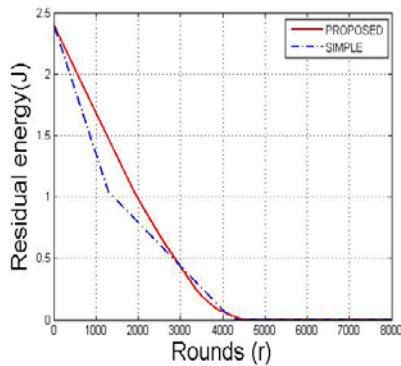Fig. 12 Remaining energy at EO = 0.4


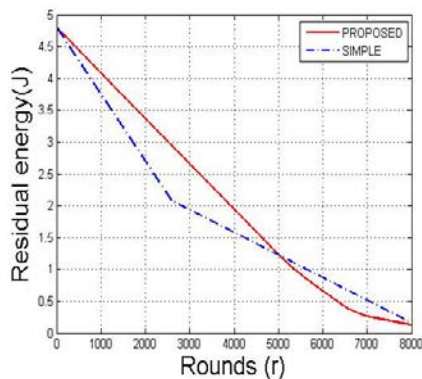Fig. 13 Remaining energy at EO = 0.5


Fig. 14 Remaining energy at EO = 0.6

Simulation results show that EXISTING protocol, some nodes get exhausted early due to larger amount of traffic. On the other hand, in proposed protocol it uses lowest energy till 20% of replication time. It means, in stability period, more nodes have sufficient energy and they transmit more data packet to sink.

While comparing the EXISTING protocol with PROPOSED protocol we have concluded 20% mean improvement has been noticed in respect of EO (initial energy) values at 0.3, 0.4, 0.5, 0.6.

### D. Path Loss

Path loss is a utility of frequency and distance [12]. It is designed from its distance to sink with constant frequency. Proposed topology decreases path loss as presented in figures 15-18. It is due to the fact that MAC transmission decreases distance. On the other hand, once 2000 rounds, path loss of EXISTING protocol reduced as certain nodes of EXISTING topology die. Smallest number of active nodes has smallest collective path loss.
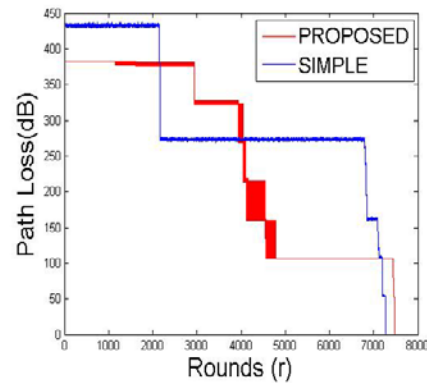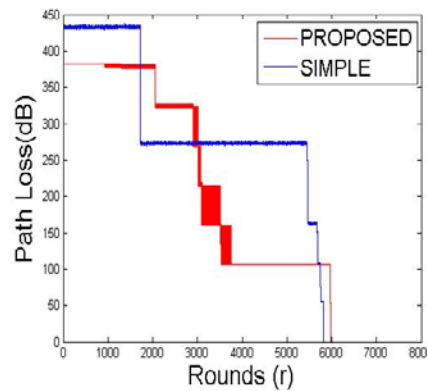

Fig. 15 Network path loss at EO = 0.3


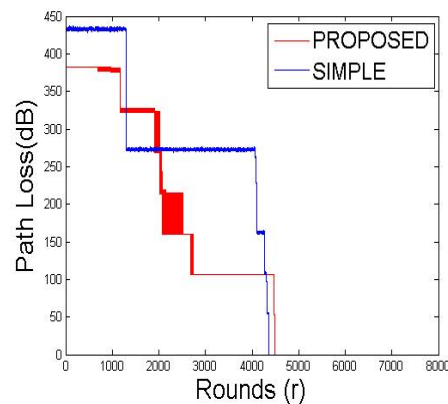Fig. 16 Network path loss at EO = 0.4


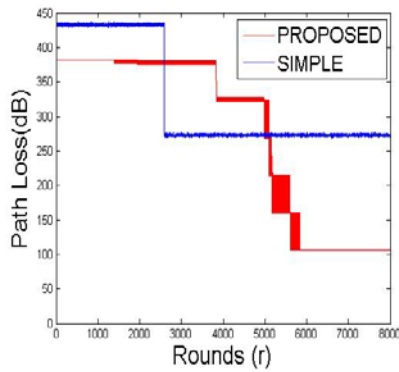Fig. 17 Network path loss at EO = 0.5

Fig. 18 Network path loss at EO = 0.6

As proposed protocol has extended stability period and extra active nodes have to extra increasing path loss [12, 13]. While comparing the EXISTING protocol with PROPOSED protocol we have concluded 11 % mean improvement has been noticed in respect of EO(initial energy) values at 0.3, 0.4, 0.5, 0.6.

## VI. CONCLUSION AND FUTURE SCOPE

In this report, we have proposed a novel protocol for WBANs. The proposed technique has modified TDMA based MAC protocol to reduce the required number of sensors required to successfully monitor the environment of body are network. The proposed technique has been designed and implemented in the MATLAB 2013a with the help of wireless communication toolbox. It has been observed that the proposed technique has significantly reduced the required number of servers. Extensive experiments reveal that the proposed protocol outperforms existing one in terms of residual energy, throughput, network lifetime and path loss. The technique of Reinforcement Learning automatically depicts the situation that how to perform in artificial intelligence. In this report, we have not considered the use of any security attacks on WBANs. Therefore, in near future we will modify proposed technique to handle security attacks.

## REFERENCES

[1] S. Mukherjee, K. Dolui and S. K. Datta, "Patient health management system using e-health monitoring architecture", *in Advance Computing Conference (IACC), IEEE,* pp. 400-405, 2014.

[2] X. Sun, J. Su, B. Wang and Q. Liu, "Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks", *International Journal of Security and Its Applications,* Vol. 7, No. 4, 2013.

[3] L. Zhu, Zhen Yang, Meng Li and Dan Liu, "An Efficient Data Aggregation Protocol Concentrated on Data Integrity in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks,* vol. 2013.

[4] N. Wadhwa, S. Z. Hussain and Rizvi SAM, "A Combined Method for Confidentiality, Integrity, Availability and Authentication (CMCIAA)", *Proceedings of the World Congress on Engineering, WCE,* Vol. 2, 2013, London, U. K.

[5] Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin and Hung-Min Sun 2012, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems,* Vol. 23, No. 4.

[6] Ruoyu Wu, Gail-JoonAhn and Hongxin Hu 2012, "Secure Sharing of Electronic Health Records in Clouds," *8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing,* Collaboratecom 2012 Pittsburgh, PA, United States.

[7] Ed Gelbestein 2011, "Data Integrity-Information Security's Poor Relation", *ISACA Journal,* Vol. 6.

[8] Vladimir Oleshchuk and Rune Fensli, "Remote Patient Monitoring Within a Future 5G Infrastructure," *Wireless Personal Communication, Springer Science,* 2010.

[9] Wenbo He, X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher, "iPDA: An Integrity-Protecting Private Data Aggregation Scheme for Wireless Sensor Networks", *IEEE MILCOM,* pp. 1-7, 2008.

[10] H. T. Chu, "A Ubiquitous Warning System for Asthma-Inducement", *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing,* Taichung, pp. 186-191, 2006.

[11] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selvao, Y. Wu, L. Fang, Z. He, S. Lin and J. Stankovic, "ALARM-NET:Wireless Sensor Networks for Assisted Living and Residential Monitoring", Technical Report CS-2006-13, Department of Computer Science, University of Virginia, 2006.

[12] Y. J. Zhao, "A MEMS Viscometric Glucose Moni-toring Device", *Proc. of the 13th IEEE International Conference on Solid-State Sensors, Actuators and Microsystems,* Pittsburgh, pp. 1816-1819, 2005.

[13] J. W. P. Ng, B. P. L. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou and G. Z. Yang, "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)", In Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp"04), Nottingham, U. K., 2004.

[14] T. Park and K. G. Shin, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks", *in ACM Transaction*, 2004.

[15] Arjan Durresi, VamsiParuchuri, RajgopalKannan and Iyengar, "A Lightweight Protocol for Data Integrity in Sensor Networks", *IEEE, ISSNIP,* SS 2004.