ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

Efficient Reconfiguration and Secure Communication for Wireless Body Area Network

[1]Abhay Kshirsagar, [2]Dr. Amol Deshmukh
[1]Research Scholar, [2]Professor,
Electronics Engineering Department, G.H. Raisoni College of Engineering, Nagpur [1, 2]
abhayksagar@gmail.com, aydeshmukh@gmail.com

***Abstract* – Wireless Body Area Network (WBAN) or Body Area Networks (BAN) is a wireless connection of wearable computing devices (examples like sensors and actuators). These devices are embedded inside the body, implanted or mounted on body surface that are like wearable technology. WBAN are used in many promising applications such as health monitoring, sports, home/health care, multimedia, medicine and etc. There are many challenges for WBAN like security, sensor validation, data management, reconfiguration etc. Our proposed system provides a secure communication based on reconfigurable and scalable WBAN. Reconfiguration of sensor nodes is more useful in the sensor network, which helps to improve the performance of the network, for that we provide a novel algorithm named "*Reconfiguration Algorithm (RA)*" and for secure communication, we introduce a new secure hashing algorithm named "*Modified HMAC-SHA3-384*". This algorithm presents the combination of modified HMAC (Hash Message Authentication Code) and SHA3 – 384 (Secure Hash Algorithm 3 – 384 bits) hashing technique. Our experimental results show higher performance than existing system with specific parameters like key generation time and entropy.**

I*ndex Terms* – Body Area Network (BAN), HMAC, SHA3-384, Wearable Technology.

I. INTRODUCTION

Wireless Body Area Network (WBAN) is an independent connection of computing devices such as sensors and actuators. These devices are situated inside the body, or human may carry in their hands, clothes pockets and also in bags. WBANs support more innovative medical applications which include several areas that include smart health care, Ambient Assisted Living (AAL), Bio-Feedback, emergency response, Rehabilitation and therapy. WBAN provide several applications that promises for improving the quality of life and satisfies the requirements of people based on allowing various technologies like,

- Bluetooth
- Bluetooth Low Energy (BLE)
- Zigbee and 802.15.4
- IEEE 802.11
- IEEE 802.15.6

Some of the requirements of WBAN are Reliability, Latency, Security and Power consumption [1]. Wireless Sensor Network (WSN) is different from Wireless Body Area Network (WBAN) based on protocol suiting the networks. Some of the differences between WBAN and WSN are as Density and Deployment, Mobility, Latency, Data Rate. There are many advantages using these WBAN which are Flexibility, Cost-Effective, Effectiveness. For health care based applications, we use sensor like Electrocardiography (ECG),

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

Electroencephalography (EEG), Electromyography (EMG), Motion Sensors, Accelerator (or) Gyroscope, Blood Pressure sensor. The communication in WBAN architecture has divided into three types they are 1) Intra-BAN Communication 2) Inter-BAN Communication and 3) Beyond-BAN Communication [2]. WBAN are also used in Non-Medical applications such as 1) Real Time Streaming for capturing a video clip by camera in smart phones, 2) Entertainment Applications such as gaming applications and social networking, 3)Emotion Detection which describes the induction of physical manifestations all over the human body that leads to measuring the signal production using bio-sensors, 4) Secure Authentication refers to utilizing the behavioural and physiological biometrics like Finger prints, facial prints, Iris Recognition and etc [3].

Fig 1 describes the WBAN architecture that specifies the body sensors on a human body which wirelessly transmits the data to patient's personal device. This device transmits signals to the internet through access points for storing the data in a hospital medical server. These databases are accessed by the patient's corresponding doctors or physicians in a remote control.

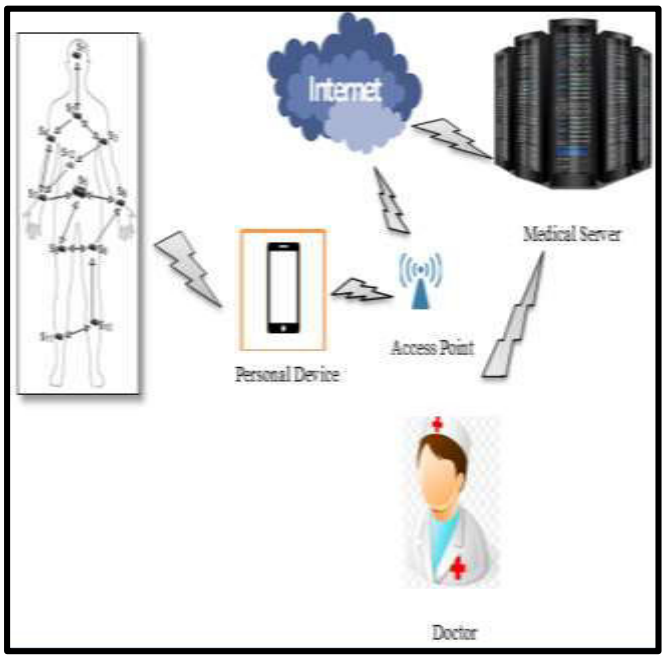

Fig 1 Architecture of Wireless Body Area Network (WBAN)

Though there are much applications developed in the WBAN and it faces many challenges in real time application. Some of the challenges faced by WBAN are scalability, Node tasks, reconfigurability, security, power supply, Node replacement etc. Many researchers and applications have focused on the WBAN architecture that arise the problem on reconfiguration of medical sensors and providing secure communication between patients and doctors or physicians. Security has two crucial features on WBAN architecture such as 1) security leads to protect the data from unauthorized access when it is transferred, processed, collected and safe storage on the medical server. 2) This also suggests the authority for controlling and gathering the access of one's personal information [5]. Our proposed work focus on providing the scalable and reconfigurable network for the real time application and also focus on providing heavy security for data accessing. We also provide the access policy for accessing the data in medical server.

In our proposed work, we allow various sensors like EMG, ECG, Gyroscope, Motion sensor etc. on the human body for monitoring their activities. The information collected from sensors is moved to the personal smart device which is used by the patient. Here we use controller that allows monitoring of sensors and its information such as sensing information, transmission timing, distance, sensor energy. If any changes identified then our proposed reconfiguration algorithm takes over. This procedure allows replacing the fault sensor with idle sensor node which has higher energy. Sensor information is transmitted to internet with the help of access point and it is stored in the hospital medical server. In server storage, the data is classified according to the patient diseases based on our proposed Disease based Clustering (DC) algorithm. Security is considered for avoiding unauthorised access on the medical server. We propose a new algorithm named Modified HMAC with SHA3-384 algorithm that focus on providing secure key for every user. This algorithm is a combination of modified HMAC and SHA3-384 algorithm. We also allow access policy for accessing of data by either physician or the doctor. Our contribution of the work is as follows:

- Proposed a novel modified HMAC-SHA3-384 algorithm for secure data storage
- Proposed a Disease based Clustering algorithm is introduced for classifying the data
- Proposed a Reconfiguration Algorithm (RA) that allows detecting the failure of sensor nodes during data transmission.

Paper Organization:

Our paper is organized as follows: Section 2 describes the literature survey of the Wireless Body Area Network. Section 3 describes the problem definition of WBAN. Our proposed system is described in section 4 that includes our proposed security algorithm, Disease Clustering Algorithm (DC) and Reconfigurable Algorithm (RA). Section 5 describes comparison of performance metrics, Section 6 describes the conclusion and references of our journals are listed in Section 7.

II. LITERATURE SURVEY

In paper [6], authors Mohammad Ghamari, et al presented the information about comparison of existing low-power communication technologies which potentially support increasing advanced development and deployment of WBAN system. This development focuses on remote monitoring of ill patients in residential environment. Here some of the energy efficient and reliable wireless communication protocols are focused and it considers the challenges and requirements of WBAN systems.

Researcher like Min Chen [7] proposed a novel hybrid WBAN architecture which is a rich media health care service via data networking and also various solutions like 1) integrating WBAN with LTE (Long Term Evolution) for high user mobility 2) Named Data Networking Technology for distributing contents 3) Adaptive streaming for dynamic bandwidth. This system has several advantages like Effective QoS support, efficient content delivery from cloud, Flexible and personalized interaction, high user mobility.

Authors like Ghada Almashaqbeh, et al proposed a health monitoring system using cloud WBAN [8]. This focuses on 1) Data Classification and aggregation for avoidance of clogging with unused traffic in the network. 2) An assignment policy is used for distributing WBANs with the user on available frequency in order to manage the interference. 3) For increase the

communication speed, a delay-aware routing metric is focused and finally 4) delay aware routing protocol is focused on the local cloud. Here security is not focused because any unauthorised person can access the sensitive data in the cloud environment.

Researchers in paper [9], proposed a secure cloud environment that focused mainly for mobile emergency medical care system. Patient's information is sensitive and private so that chaotic maps based authentication and key agreement mechanism are introduced based on the concept of Diffie-Hellman key exchange. Using this system, a patient's health information is only accessible for only authorized doctors and medical caregivers. This system supports a real-time analysis with continuous remote monitoring on WBAN-oriented health items.

Researcher such as Shahnaz Saleem, Sana Ullah and Kyung Sup Kwak proposed a surveyed a security framework for IEEE 802.15.4 in WBAN. This gives information like security vulnerabilities and major attacks on the network. Some of the attacks types on the CAP (Contention Access Period) and CFP (Contention Free Period) that are addressed here and the security requirements for the smart DoS attacks in WBAN at physical, MAC, network and transport layers are highlighted [10].

In paper [11], author proposed a new network model for the WBAN. This allows a traffic sensitive WBAN and here the performance is carried out in terms of end-to-end delay. Also a non-preemptive queue model is allowed in this model for effective data transmission. Data traffic is classified on three levels such as Normal, On-Demand, Emergency. Here classification of data traffic is based on TDMA scheduling.

Researchers like Debiao He et al have addressed the problproblems of integrity in the WBAN in the cloud environment. An Efficient Certificate Less Public Auditing (CLPA) scheme is proposed that shows security against two adversaries such as 1) Replacement of user's public keys and 2) Accessing of Master Keys. This system presents a security analysis of the proposed system for demonstrating the provable secure network in a random oracle model. Here the security model is the fundamental process of proving the cryptographic scheme and only it defines the target of the security [12].

Authors in paper [13] presented a framework for health care monitoring. This allows a distributed and energy-saving mobile health platform named mHealthMon. Here mobile users access the sensor data through cloud infrastructure based peer-to-peer (P2P) overlay network. This environment also presents the energy enhancement and faster in mobile health monitoring application. The basic idea of this environment is to satisfy the quality of service requirements based on modelling the sub-systems.

Researchers like Farrukh Aslam Khan et al [14], proposed a framework named "A secure cloud-based mobile healthcare framework using wireless body area network (WBAN)". This framework works on two procedures such as 1) Security for inter-sensor communication based on multi-biometric using key generation scheme in WBAN 2) medical records of patients are securely stored in hospital community in order to preserve the privacy of the data in the cloud environment.

In paper [15], cryptography based data access control is proposed in order to secure the health records of every patients. This system allows many services like secure transmission, tracking of patients and transmitting to the service providers etc. Here every patient data is encrypted before it is transmitted to cloud environment and it also provides efficient access

control for the health records named as "Revocable Multi Authority Attribute Set Based Encryption". This mechanism provides a centric access to all the authorized persons.

Authors in paper [16], proposed the effective managing system for Wireless Sensor Network (WSN). A WSN Management system is used for network management system was developed and is a user convenient way for monitoring and controlling the sensor network operations like collecting and analysing the information of each sensor nodes. This information are analysed for the system configuration and it facilitates the convenient management of sensors.

Authors Gert Schley et al presented a tolerant routing for fault on networks in the hierarchical units. This allows the various UP/Down routing locally in online on each unit while deadlock freedom is globally ensured on the network. Here a reconfigurability is enabled that focus on modified Dijkstra algorithm that uses a deadlock-free baseline routing, and it is used when a fault affects the network [17]. Cryptographic hash functions are widely used in the network that has been used in the secure transmission of the network.

In paper [18], author presented a new security based on the modification on HMAC algorithm due to compromising of HMAC algorithms on security. This considers the specific data attacks on the network such as birthday attack and exhaustive key search attack.

All above researchers are providing best environment in the WBAN but some papers lacks in security and privacy. Many researches have proposed privacy but failed in storage of data and takes more time for encrypting.

III. PROBLEM DEFINITION

Reconfiguration is more important for the sensor networks and its types this allows the various applications in terms of enhancing the network lifetime, scalability of the networks based on the distance capability of the sensor nodes. The main approach of reconfiguration is to manage and maintain the components and connections at the run time of the network.

Another issue in WBAN is the security and access of data. This can be solved by multiple cryptographic algorithms for the network that provides effective communication among the data with specific keys. HMAC (Hash Message Authentication Code) is the specially used hashing algorithm on securely access of the data. Here modified HMAC-MD5 algorithm [18] is used for providing higher security in the data transmission. MD5 is thoroughly compromised in multiple ways that can easily retrieve the original information on the network. It provides more collision when compared with other algorithm it takes more time for working that specifies slower working in data transmission. These are problems which are faced by existing process and it lacks in performance.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

IV. PROPOSED WORK

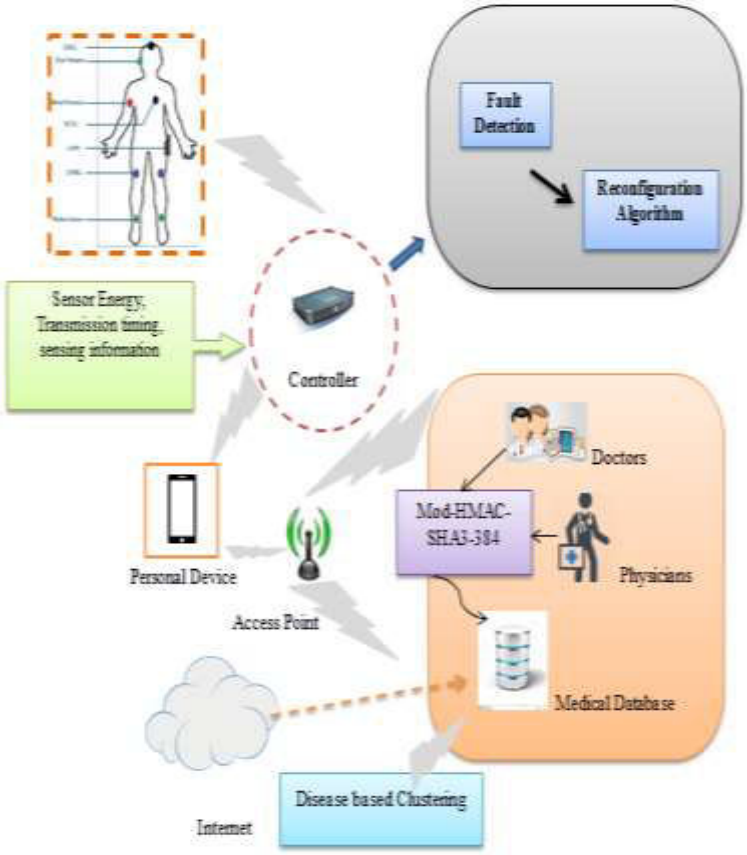

Fig 2 Proposed Architecture for WBAN

4.1. Overview Of Our Proposed Work:

Our proposed work focuses on providing the Wireless Body Area Network (WBAN) that must be scalable and reconfigurable with the secure communication. Our proposed system has advance features by providing the secure communication and improving the reconfiguration process on the environment. Initially we retrieve sensor information from human body. This information (such as sensor energy, transmission timing and sensing information) is transferred to controller and here we monitor any faults in the information if any fault occurs, we use a **Reconfiguration Algorithm (RA),** it changes the alternate node with higher energy. Then for classifying the information on server we prefer **Disease based Clustering** that clusters the information obtained from human body based on their diseases. We store the data securely and securely retrieved by the proposed algorithm named **Modified HMAC-SHA3-384**. Only the specific doctors and physicians can access the data based on the access policy. Figure 2 describes the architecture of our proposed system.

4.2. Sensors:

Sensors are motivated to oft-cited application on the medical areas. This ability to the medical telemetry with the wearable wireless sensors will have a profound impact on many clinical practices. Here medical emergency, triage and intensive care, all can benefit from continuous

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

vital sign monitoring (Notification arises when patient deterioration). Here IEEE 802.15.4 category is the largest standard for lower data rate WBANs. This category is mainly developed for low data rate monitor and control applications and this allows only low-power consumption for the extended life. IEEE 802.15.4 based sensor is the best choice for monitoring the single patient monitoring or personal use.

In our proposed work, we use many sensors that are as follows: ECG, EEG, Accelerometer, EMG, Body temperature sensor, positioning, pressure sensor, Glucose sensor, insulin injection and Toxins, implants, hearing and visions. These sensors are always uni-functional devices, works faster when there is a small range of distance. The human body information that is collected from sensor nodes is transmitted to the controller. Fig 3 describes the several sensors fit on the human body.

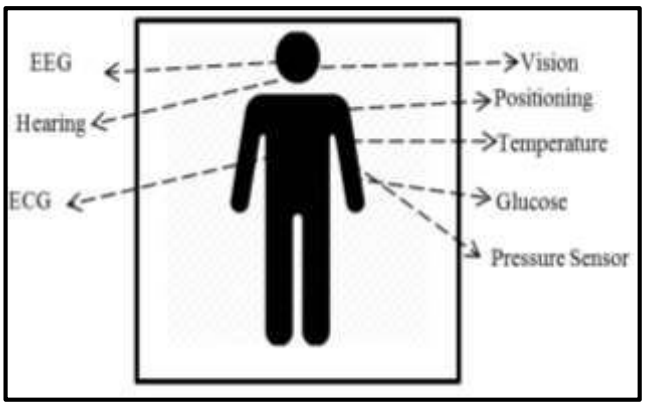

Fig 3 Body Sensors

4.3. Reconfigurable Algorithm (RA)

In our proposed method we focus on reconfiguration on the network when there is an alteration on the data transmission. After collecting the information from sensor nodes, the controller monitors the data such as sensing information, transmission timing of data, sensor energy. When this information is slightly changed during the data transmission, a fault is detected then our proposed reconfiguration algorithm takes over. Our Reconfigurable Algorithm is that defines the procedure for making correct data transmission without any difficulties on the network.

When any fault is detected on the sensor node then the current node is replaced by another sensor which has higher energy. A constraint among others is that it must be idle. The following figure 4 describes the working procedure of our proposed algorithm. The codes that are: N_E describes the energy of the sensor node, N_{TT} describes the transmission timing of sensor nodes and N_{SI} is the sensing information of the sensor node. N_I is the number of nodes participated on the WBAN. CT is the controller; FT is the fault occurrence on the information. MP is the smart phone and Re-CFG is the reconfiguration procedure for replacing the nodes with higher energy that must be idle and figure describes the work flow of the Reconfiguration Algorithm.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

==========

Pseudo Code: 1 Reconfiguration Algorithm

==========

Inputs: N_E, N_{TT}, N_{SI}, $N_i = \{ N_1 , N_2 , N_3 , \ldots \}$

Output: Eliminating FT

START

Step 1: N_E, N_{TT}, N_{SI} *of* $N_i \rightarrow CT$

Step 2: if $CT \rightarrow FT$

Goto Re-CFG N_i

Else

$CT \rightarrow MP$

Step 3: End if

Re-CFG of N_i***:***

Step 1: Eliminate N_i

Step 2: search new N_i

Step 3: if $N_i \rightarrow \{N_E \rightarrow (high)$ && $N_E \rightarrow (Idle)\}$

Replace new N_i

End -if

END

4.4. Disease based Clustering:

After reconfiguring the network, the information is transmitted to the personal device of the user. Then it is forwarded to the access point. Finally the sensor information is transmitted to the hospital medical server through the internet. The data are stored in server must be classified for future access. When there is any critical stage of a patient is noted. Emergency signal is sent by the medical server via internet to the corresponding doctor or physician. The corresponding doctor or physician transmits the precautions information to their personal device and they continue treatment process according to the patient health.

Disease based Clustering is the clustering algorithm for classifying the patients based on their disease. Health care monitoring is a common monitoring of human beings who are ill. Based on the corresponding disease of human, information from sensors is classified. Our proposed system allows some diseases like Heart attacks, Brain Tumour, Mentally ill, genetic disorders, liver disorders, intestinal diseases etc. Every disease have different stages like normal and critical stages, we store the information as normal and critical for every diseases. The following pseudo code explains the disease based clustering algorithm.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

==========

Pseudo code 2: Disease based Clustering (DC)

==========

Inputs: N_E , N_{TT} , N_{SI} , N_i = { N_1 , N_2 , N_3 , … }, N_E , N_{TT} , N_{SI} , C_i = { C_1 , C_2 , C_3 , … }, D_i = { D_1 , D_2 , D_3 , … }, SC_i = { SC_1 , SC_2 }
Output: Cluster information
START

Step 1: N_E , N_{TT} , N_{SI} of N_i → HS

Step 2: HS allocates C_i

Step 3: C_i → SC_1 or SC_2

Step 4: if (N_{SI} of N_i) → SC_2

ESG → D_i from HS

D_i → N_i

Else

N_i → SC_1

End if

END

==========

In above algorithm D_1 , D_2 , D_3 , … are the doctors or physician, N_1 , N_2 , N_3 , … are the patients who are in the health monitoring, C_1 , C_2 , C_3 , … are the clusters of the specific disease where SC_1 is the normal stage, SC_2 is the critical stage, N_E describes the energy of the sensor nodes, N_{TT} describes the transmission timing of sensor nodes, N_{SI} is the sensing information of the sensor nodes, HS is the hospital medical server and ESG is the emergency medical signal. When N_I sends information to HS, HS allocates the C_i according to the patient disease. If any critical information form N_I is detected, HS sends ESG to the D_I, else it stores information to the HS. The following figure 7 describes the diagrammatic representation of the Disease based clustering algorithm.

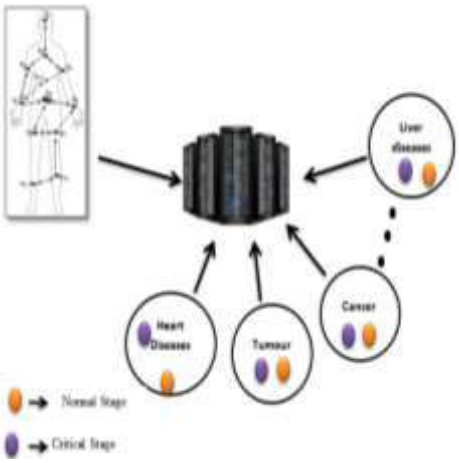

Fig 4 Disease based Clustering

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

4.5. Secure Communication:

Our proposed work mainly focuses on providing secure communication of data in the network. This allows transferring of information from sensor node to the medical server. Our communication work focused on two points 1) secure data communication is based on new hashing technique named "Modified HMAC-SHA3-384" algorithm and 2) A access policy is used which describes the information accessing of authorized person such as doctors and other physicians. Here doctor is a person who gives medical reports for the patients and physician is a person who is allowed to see the medical reports of the patient. This is because any research students or any other physicians cannot have access rights to view the specific patient's medical records. Based on having the secret key and access rights, the doctors and authorized physician are allowed to give treatment to the patients. Here Modified HMAC-SHA3-384 is the combination of Modified HMAC and SHA3-384 hashing techniques.

SHA3-384 is the sponge function (which is a Keccak family). Here a data is absorbed and their result id squeezed out. During absorption, the message blocks are XORed into subset of phase and they are transferred. In Squeezing phase, the output blocks are read from the same subset which is altered with state transformation. In SHA3-384, the size of the part read and written is specified by (r) read and part which is not touched by input and output is specified by capacity (c) which determines the security. The Keccak function is defined in SHA3 is follows:

Keccak[c] (M, n) = Sponge [keccak-p [1600, 24], pas10*1, 1600-c] (M,n).

Hash function as,

SHA3-384 (M) =Keccak [768] (M ‖ 01, 384)

Where M is the message, n is the output length and capacity (c) is the double of the digest length (768) i.e. c= 2n. the two bits [01] which appended to the message used for distinguishing the messages for SHA3 hash functions from messages.

Finally secret key K is generated. Then it is followed by the modified HMAC function [18].

HMAC is defined as the known cryptography system that uses MAC (message authentication code) function. This modified HMAC uses the hash function operating on an input string and key. If the key has length which is longer than b bits i.e., 384 bits, we will use hash function h to hash the key K to a b bit long string K^+ or will pad zeros if the key is shorter than 384 bits. Flowchart of the proposed hashing algorithm is described in figure 5 and pseudo code of the hashing algorithm is as mentioned below:

==========

Pseudo code 3: Modified HMAC-SHA3-384

==========

Inputs: *M, bits b = 768, C1= 00110110, C2= 01011100*

START

Step 1: message M

Step 2: compute K

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

Step 3: Compute Hash (K)

Step 4: if length (K) < b

Pad 0 to K

Else

$K \rightarrow K^{+}$

Step 5: $[K^{+}$ *(+) ipad with [C1] by b/8 times]* $\rightarrow S$

Step 6: (Append M and S) $\rightarrow Z$

Step 7: Hash (Z) $\rightarrow Z_1$

Step 8: $[K^{+}$ *(+) ipad with [C2] by b/8 times]* $\rightarrow S_0$

Step 6: Attach (Z_1 *and* S_0) $\rightarrow Z_2$

Step 7: Hash (Z_2) $\rightarrow$ *HMAC*

END

==========

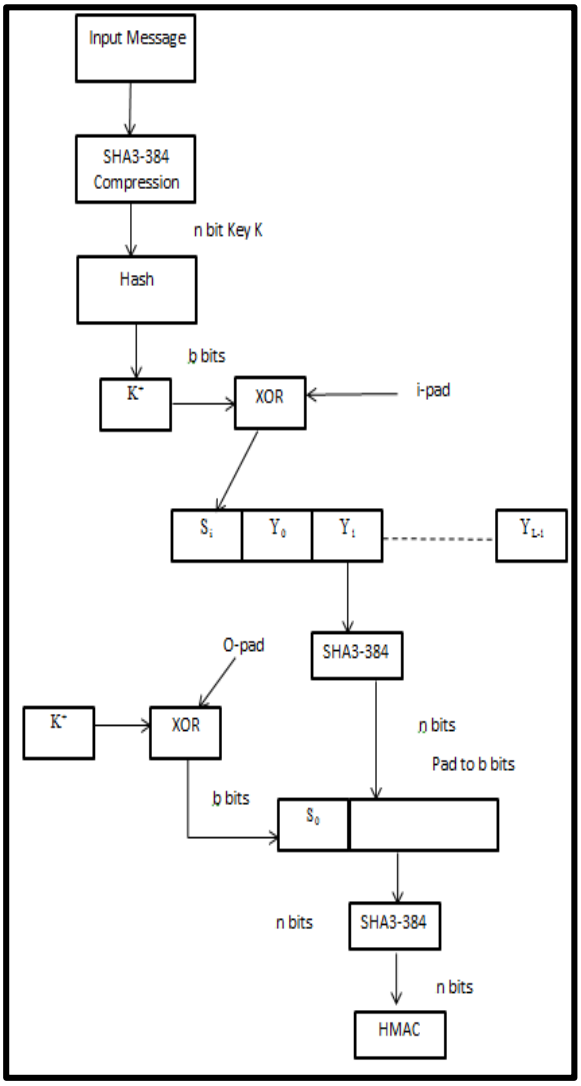

Fig 5 Modified HMAC-SHA3-384

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

The above algorithm describes the working of the modified HMAC-SHA3-384. M is the message that is needed to be encoded and b is the final length of the bits and C1 and C2 are the capacities of the output length which is used on the HMAC. Finally we get the encrypted output and key. These keys are transmitted to corresponding doctors and authorized physician for accessing the information. Our proposed system specifies the roles such as 1) Doctor and 2) Physicians. Doctor can access both personal information and medical reports of the patient. But the physician can access only the medical records of the corresponding patient. This will provide higher security of the patient information.

V. PERFORMANCE ANALYSIS

Our proposed system is evaluated with performance metrics and it is compared with other existing system. We focused on the reconfiguration of the sensor nodes and secure communication is provided in the environment. This section involves,

- Simulation Environment
- Performance Metrics
- Comparative Analysis

5.1 Simulation Environment

This paper concept is implemented by the open source software Network Simulator-2 (NS-2). Languages used are TCL and AWK script. NS2 began as a REAL network simulator in 1989 and has evolved substantially in a small year. Currently NS development support is based on DARPA with SAMAN and through NSF with CONSER, both in collaboration with other researchers including ACIRI. NS2 has always included substantial contributions wireless code from the UCB Daedalus and CMU Monarch projects and Sun Microsystems. This open source software is installed in Ubuntu 12.04 Operating System. Based on our Health monitoring application in WBAN, we design our network with required simulation parameters

Table 1: Simulation Parameters

Parameters	**Values / Ranges**
Network Simulator	NS2
Simulation Time	100s
Simulation Area	1000m X 1000m
Number of Nodes	20
MAC Protocol	IEEE 802.15.4
Packet Size	1024 bytes
Data Type	CBR
Initial Energy of node	300J
Mobility Model	Two-ray Ground

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

Here we use 20 nodes for WBAN and there are 5 users in the system. Each user has 3-5 sensor nodes in their body. To monitor the energy consumed, initial energy of node is set. Energy consumption will vary with respect to the simulation time. Here we use random way point model, because user can move a small distance in their home environment. Performance of the network is evaluated and analysed by considering certain metrics. These are discussed in the next section.

5.2 Performance Metrics:

Performance metrics are evaluated and analysed to prove enhancement through the proposed work. This section considers the different metrics that are taken into account for further improving the performance. We have considered some parameters which are as follows:

- Key Generation
- Simulation time
- Encryption time
- Detection rate
- Throughput

Key Generation

It is the process of generating keys in cryptography where a key is used to encrypt and decrypt whatever data is being communicated. This is an important factor that is used to evaluate the performance.

Entropy

Entropy is the randomness collected by an operating system or application for use in cryptography. Higher entropy in the system provides higher security. This randomness is often collected from hardware sources, either pre-existing ones such as mouse movements or specially provided by randomness generators.

Simulation Timing

The simulation timing describes the computational complexity and security of the encryption algorithm based on its input size of bits.

***Detection Rate*:**

This detection rate defines the number of affected nodes in the network which are identified successfully to avoid performance degradation in the network. This can be identified based on the infected node and time period duration.

Throughput:

Throughput can be defined as the number of packets that are successfully delivered with respect to the time taken by the node.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

5.3 Comparative Analysis

Table 2: Comparison of existing system and proposed system

Techniques	**Existing System**	**Proposed System**
[18], HMAC-MD6	Higher security but simulation timing is high	Higher security with reduced timing
Scalability [15]	Performances Reduces when key are higher	Increases when the key are higher

This section comprises of the comparison of our proposed work and existing work based on the performance metrics that are discussed in the above section. Evaluation parameters are examined against the previously implemented metrics. The same is put in tabular form above which clearly describes the enhancement over key parameters. The above table 2 describes the techniques used in existing system and proposed system with its merits and demerits. For better understanding of the enhancement in the proposed work, these parameters are plotted which clearly suggests the overall effectiveness of the proposed work.

5.3.1 Entropy:

Here we describe the comparison of entropy in the existing system [14] and proposed system. The results are shown with graphical representation in figure 6. The length of keys of [14] is 320 bits and proposed keys are about 384 bits. Table 3 specifies the comparison results of proposed scheme and existing schemes.

Table 3: Results of Entropy

Values	**Existing System [14]**	**Proposed System**
5	0.986	0.987
10	0.985	0.989
15	1	1
20	0.980	0.991
25	0.987	0.997

5.3.2 Key Generation:

Here we describe the comparison of key generation in the existing system [15] and proposed system. The results are shown with graphical representation in figure 7 and values are shown in table 4. The key generation time is calculated by,

$$\text{Key generation} = \frac{key\ size}{attributes}$$

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

Table 4: Results of Key Generation

Values	Existing System [15]	Proposed System
2	0.06	0.04
4	0.05	0.05
6	0.1	0.06
8	0.17	0.1
10	0.18	0.14

5.3.3 Detection rate:

The comparison of detection rate in the existing system and proposed system [19] is graphically shown in figure 8 and table 5 shows the values of detection rate. The detection rate is calculated by,

$$\text{Detection Rate} = \frac{Number\ \ of\ infected\ \ Nodes}{Time\ \ period}$$

Table 5: Results of Detection Rate

Values	Existing System [19]	Proposed System
1	0.01	0.04
2	0.02	0.08
3	0.04	0.13
4	0.05	0.16

5.3.4 Simulation Timing:

Here a comparison of simulation timing in the existing system and proposed system [18] is represented graphically as shown in figure 9 and table 6 shows the simulation timing values. The simulation timing is calculated by,

$$\text{Simulation timing} = \frac{Input\ \ size}{Number\ \ of\ rounds}$$

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

Table 6: Results of simulation timing

Values	Existing System [18]	Proposed System
10	60	30
20	80	50
30	135	100
40	150	120
50	200	170
60	245	200
70	270	230

5.3.5 Throughput:

Throughput is measured in bits per second (bps) corresponding to the time taken. The expected performance of the proposed system is shown with this throughput parameter. Finally throughput of the network is obtained in figure 10 and table 7 shows the results of throughput obtained.

$$\text{Throughput} = \frac{\text{Number of packets send}}{time}$$

Table 7: Results of Throughput

Values	Throughput on Proposed System
10	3
20	4
30	5
40	6
50	7
60	8

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

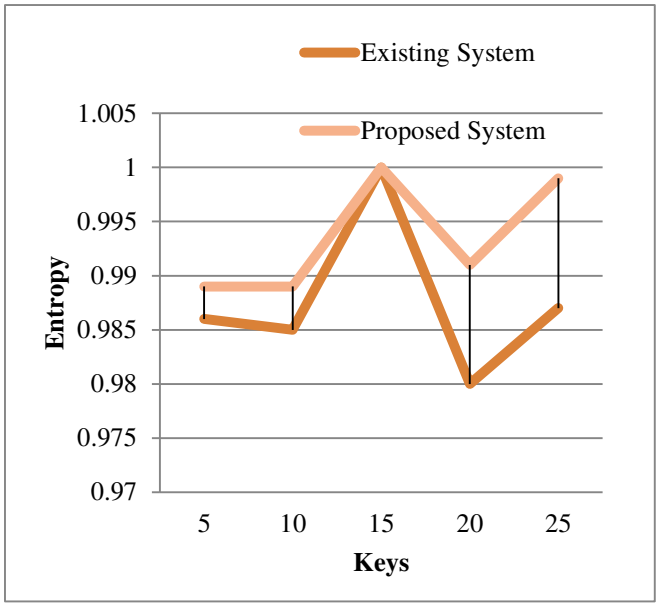

Fig 6 Graphical representation of Entropy comparison
On existing [14] and proposed system

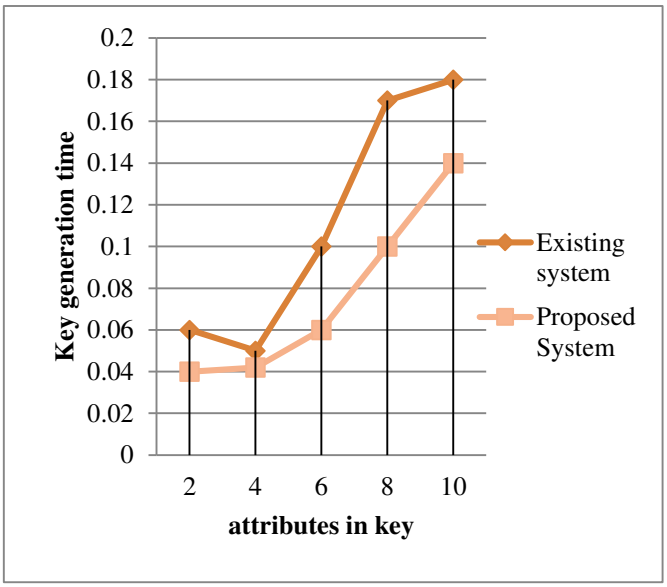

Fig 7 Graphical representation of key generation time comparison
On existing [15] and proposed system

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

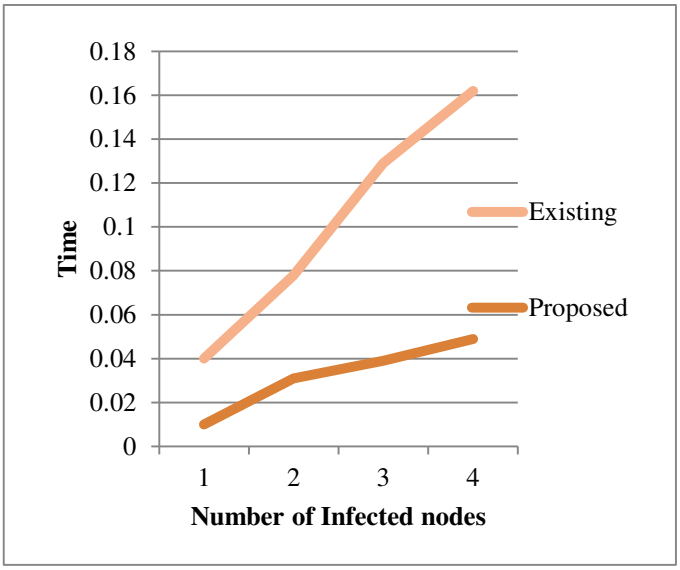

Fig 8 Graphical representation of detection rate comparison
On existing [19] and proposed system

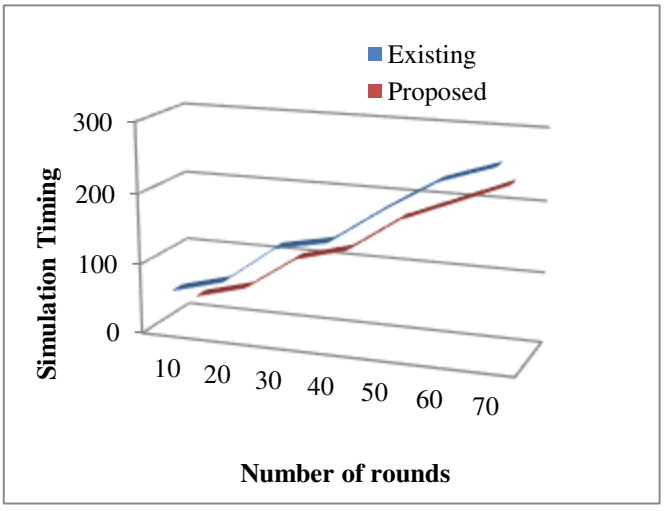

Fig 9 Graphical representation of simulation timing comparison
On existing [18] and proposed system

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.3, March 2017

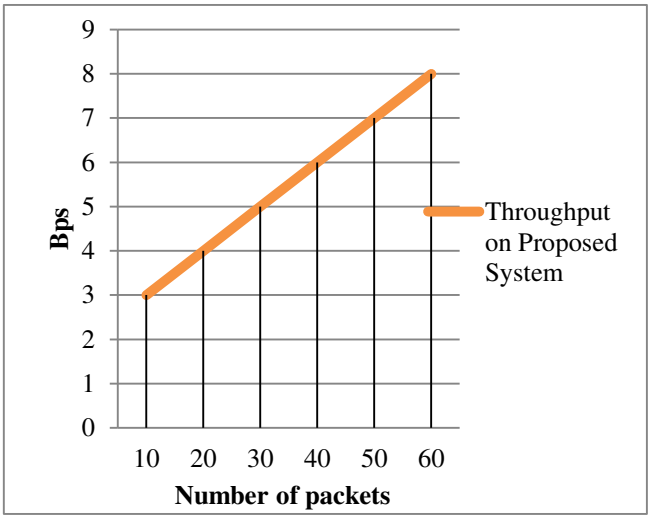

Fig 10 Graphical representation of throughput on our proposed system

VI. CONCLUSION AND FUTURE WORK

Wireless Body Area Network (WBAN) is an emerging technology with the base on Wireless Sensor Network (WSN). This technology promises the wide improvement in terms of reliability of monitoring the human health in given environment. Several sensors and actuators are implanted on the human body. This in turn faces many problems and challenges in terms of secure communication, reconfiguration, capacity, accessing the data and etc. To solve these problems we proposed a new system that enhances the problems faced on secure communication, reconfiguration. Our modified HMAC-SHA3-384 provides best results when compared with the existing system and produced effective results in the simulation environment.

Our reconfiguration algorithm avoids the degradation of network performance based on identifying the faults in the initial stage and it helps to identify the power of every sensor and allocates the replacement node when any faults occur. Our proposed system works effectively that are showed visually in the form of graphical representation such as detection rate, key generation, simulation timing, and entropy. Throughput is used for measuring the overall performance which shows the effective performance of our proposed system in graphical manner.

VII. FUTURE WORK

Our future plan is to focus on the classification of data in the hospital server based on some classification algorithm and clustering algorithm used in the data mining techniques with the reduction of effective time complexity and acquiring higher accuracy.

REFERENCES:

[1] Rim Negraa, Imen Jemilia, Abdelfettah Belghith, Wireless Body Area Networks: Applications and technologies", The Second International Workshop on Recent Advances on Machine-to-Machine Communications, ISO/IEEE 11073: International Organization for Standardization/ Institute of Electrical and Electronics Engineers 11073: Personal Health Data (PHD) Standards, 1274 – 1281, 2016.

[2] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, Victor C. M. Leung, "Body Area Networks: A Survey", Springer Science+Business Media journals, 171-193, 2010.

[3] Samaneh Movassaghi, Student Member, IEEE, Mehran Abolhasan, Senior Member, IEEE,Justin Lipman, Member, IEEE, David Smith, Member, IEEE, and Abbas Jamalipour, Fellow, IEEE, "Wireless Body Area Networks: A Survey", 2013 IEEE COMMUNICATIONS SURVEYS & TUTORIALs articles, 2013.

[4] Deena M. Barakah, Muhammad Ammad-uddin, "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture", 2012 IEEE Third International Conference on Intelligent Systems Modelling and Simulation978-0-7695-4668-1/12, DOI 10.1109/ISMS.2012.108, 2012.

[5] Samaher Al-Janabi, Ibrahim Al-Shourbaji , Mohammad Shojafar, Shahaboddin Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications", Elsevier Magazine, http://dx.doi.org/10.1016/j.eij.2016.11.001, 2016.

[6] Mohammad Ghamari, Balazs Janko , R. Simon Sherratt, William Harwin , Robert Piechockic 3 and Cinna Soltanpur, "A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments", sensor magazines, doi:10.3390/s16060831, 831, 1-33, 2016.

[7] Min Chen, "NDNC-BAN: Supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks", Elsevier Magazine, http://dx.doi.org/10.1016/j.ins.2014.06.023, 2014 .

[8] Ghada Almashaqbeh , Thaier Hayajneh, Athanasios V, Vasilakos , Bassam J, Mohd, "QoS-Aware Health Monitoring System Using Cloud-Based WBANs, article from Springer Science and Business Media New York 2014, DOI 10.1007/s10916-014-0121-2, 38:121, 2014.

[9] Chun-Ta Li, Cheng-Chi Lee, Chi-YaoWeng, "A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical Care System", article from Springer Science and Business Media New York 2016, 1-15, 2016.

[10] Shahnaz Saleem, Sana Ullah and Kyung Sup Kwak, "A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks", Sensors article, 1383-1395; doi:10.3390/s110201383, 1384-1395, 2011.

[11] Köksal Gündoğdu & Ali Çalhan, " An Implementation of Wireless Body Area Networks for Improving Priority Data Transmission Delay", Springer Science and Business Media New York article, DOI 10.1007/s10916-016-0443-3, 40-75, 2016

[12] Debiao He, Sherali Zeadally, Senior Member, IEEE, and Libing Wu, Senior Member, IEEE, "Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks", IEEE SYSTEMS JOURNAL, 1932-8184, 10.1109/JSYST.2015.2428620, 1-10, 2015.

[13] Jong Hoon Ahnn and Miodrag Potkonjak, "Toward Energy-Efficient and Distributed Mobile Health Monitoring Using Parallel Offloading", 35th Annual International Conference of the IEEE EMBS, 978-1-4577-0216-7/13/, 7257-7261, 2013.

[14] Farrukh Aslam Khan, Aftab Ali, Haider Abbas, Nur Al Hasan Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks", The 2nd International Workshop on Communications and Sensor Networks (ComSense-2014), 1877-0509, doi: 10.1016/j.procs.2014.07.058, 511-517, 2014

[15] Dr. Ragesh G. K, Dr. K. Baskaran, "Cryptographically Enforced Data Access Control in Personal Health Record Systems", Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, Elsevier journal, 473-480, 2016.

[16] Yi-Wei Ma, Jiann-Liang Chen, Yueh-Min Huang and Mei-Yu Lee, "An Efficient Management System for Wireless Sensor Networks", Sensors articles, doi:10.3390/s101211400, 11400-11413, 2010.

[17] Gert Schley, Ibrahim Ahmed, Muhammad Afzal, Martin Radetzki, "Reconfigurable fault tolerant routing for networks-on-chip with logical hierarchy", Elsevier journal, 2016.

[18] Syeda Iffat Naqvi, Adeel Akram, "Pseudo-random Key Generation for Secure HMAC-MDS", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference, 978-1-61284-486-2/111$26.00, 2011.

[19] Honggang Wang, Zhaoyang Zhang, Xiaodong Lin, and Hua Fang, "Socialized WBANs in Mobile Sensing Environments", IEEE Network magazines, 0890-8044/14/$25.00, 2014.