

# A STUDY ON SECURITY ISSUES IN HEALTHCARE APPLICATIONS USING MEDICAL WIRELESS SENSOR NETWORK AND IOT

E. Sowmiya\*, L. Malathi, A. Thamarai selvi

Dept. of Computer Science and Engineering, Vivekanandha college of Engineering for Women, Elayampalayam, Tiruchengode-637205, Tamilnadu, INDIA

## ABSTRACT

**Aim:** Now a day's, due to the change in the human food habits, environmental changes, and the industrial consequences the cause of the chronic disease was increasing rapidly. People want to check and monitor their health data regularly. It is a big annoyance and sometimes not possible to check their health condition by spending their time in hospitals. Similarly, the doctors also need to take care of their In-Patients (IP) and Out-Patients (OP) data. In order to reduce these, many healthcare smart devices were found and used by the people. The integration of these smart devices leads to Internet of Things (IoT). Already some secure IoT- based solutions were suggested by the researchers where the smart devices hold by the patients will deliver the patient health condition to the remote doctor securely by using the Internet. This study analyzes that system in terms of integration and security analysis. **Result:** The performance parameters like rate of malicious node detection and number of successful packets transfer were analyzed. Here IoT application is used to fields and it is very success full. Finally, the security loopholes of the existing system and proposed solution for that security threat were presented.

Published on: 2<sup>nd</sup> -December-2016

### KEY WORDS

Healthcare, MWSN, Security, Authentication, DoS attacks, Internet of things, chronic disease, RFID

\* Email: [eswaramoorthysowmiya@gmail.com](mailto:eswaramoorthysowmiya@gmail.com); Tel.: +91 9486088962

## INTRODUCTION

In the present era, the IoT (Internet of things) plays an important role in almost add fields importantly Home automation, Agriculture, Environmental monitoring and especially in medical fields. For example, IoT has lively capabilities to connect D2M (Device-to-Machine), O2O (Object-to-Object), P2D (Patient-to-Doctor), P2M (Patient-to-Machine), D2M (Doctor-to-Machine), S2M (Sensor-to-Mobile), M2H (Mobile-to-Human), T2R (Tag-to-Reader). This astutely connects humans, machines, smart devices, and dynamic systems and other devices to reduce the human workload [12].

In the area of healthcare is not only used in medical alliance and hospital, but also reachable by persons who are not actually present in the hospital. This is possible by the in-home patient monitoring system which gives good results with more efficiency in terms of healthcare. This in-home patient monitoring system has a high demand for age population and the ripened people. As the age population is more prone to chronic diseases and is in need of an effective in-home health monitoring system, recently, a Wireless Body Area Network (WBAN) with wearable medical sensors was developed [11]

**IoT in Healthcare:** Prevailing works in communication technologies have motivated the development of telemedicine to a great amount. Telemedicine reimbursement not only helps the customers who are able to receive health care more efficiently but also benefits the doctors to refashion their efforts to take care of more patients. To a great amount of computer- based monitoring has become an economical stipulation requiring deployment on a vast scale in various intensive care units around the world. **Figure-1** shows the patient monitoring. The system design shows that the sensors of two types one is wearable and another one is an in-planted sensor using any of this sensor the data about the patient is sensed and send it to the patient's mobile phone through Bluetooth from there it will send to the database from there it will send to the web server. The doctor can view the updates of patients detail by a web server. And else the doctor will suggest the treatments by observing the regular updates of patients through mobile or other devices.



Fig. 1: The System design

Without using PC and to support the patient monitoring in outdoor environment GPS enabled mobile phone is used in the proposed system. Security is the major issue when storing Personal Health Records (PHR) because PHR contains responsive data and they have to be securely stored and accessed [12]. If it is not possible to obtain the authentic and correct data by the medical experts, it leads to wrong and ineffective treatment and it turns to fatal predicament [13].

**Security Threats in Health care applications:** Security violates in healthcare applications of sensory networks is a major concern. It is also worth to mention that since healthcare applications of sensory networks are almost similar to WSN application environment, most of the security issues. Some of them are Malicious Node in Routing, Data modification, Impersonation attack, Eavesdropping, and Replaying.

## PROBLEM DEFINITION

Up to now, we have talked about different methods and techniques used in health Monitoring system all the above discussion is about the data transferring using different techniques such as ZigBee, cloud storage etc., in this only few authors, discussed the securities and authentication. Each and every node has to cross more levels to reach the destination. In between it needs to cross different access points, base station; gateways etc., in that time there will be a chance of occurring the attacks by the hacker. Because in healthcare system the data are very sensitive even one wrong information can lead to the tedious end. There are different types of Denial of services are there to attack the data. The most of the attacks are occurs while routing. In that, they discussed about different attacks such as black hole and selective forwarding Even though it has a solution with the minimum of 86% accuracy of detecting the malicious node .It also has some drawbacks while distributing the sequence number to access point and there is no trustworthiness in the routing algorithm. In the existing work, they provide the security up to the central data storage. To overcome this drawbacks the solution were found in the proposed system.

## PROPOSED SYSTEM

In the existing work some drawbacks has been raised to overcome those drawbacks the former solution has been found by changing the pre-deployment and routing phase algorithms, in the existing it focused up to the central storage. In this proposed work the security and authentication is provided up to the other end receiver (Doctor) which means providing security and authentication from the Patient to doctor (P 2 D).In this the different modules has been discussed in detail.

## MODULES

Our project, Health care application using medical wireless sensor network and IoT is made up of four modules. They are:

- Pre-deployment
- Clustering
- Secure Routing
- Secure access by doctors

## MODULE DESCRIPTION

### Pre-deployment

In this module, during this module every access point (AP) should be in-range with its base station (BS) which make easy for the distribution of exclusive random numbers from the BS to APs. Where the final use of the exclusive node ID as an initial seed to create a final seed. After the creation of numbers, the base station distributes them using unicast messages. That message distributed only to the access points to its own hardware devices. That avoids the malicious node which takes place in the beginning.

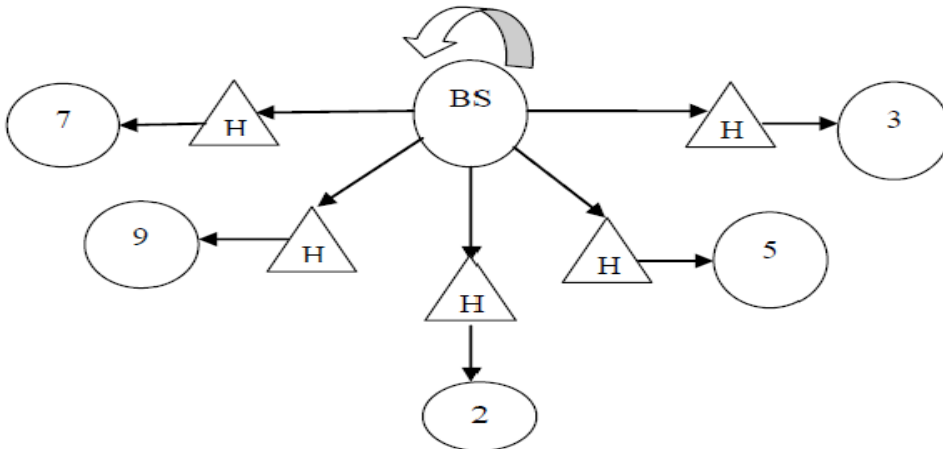


Fig. 1: The Pre-deployment unique code transmissions to its own hardware device

### Clustering

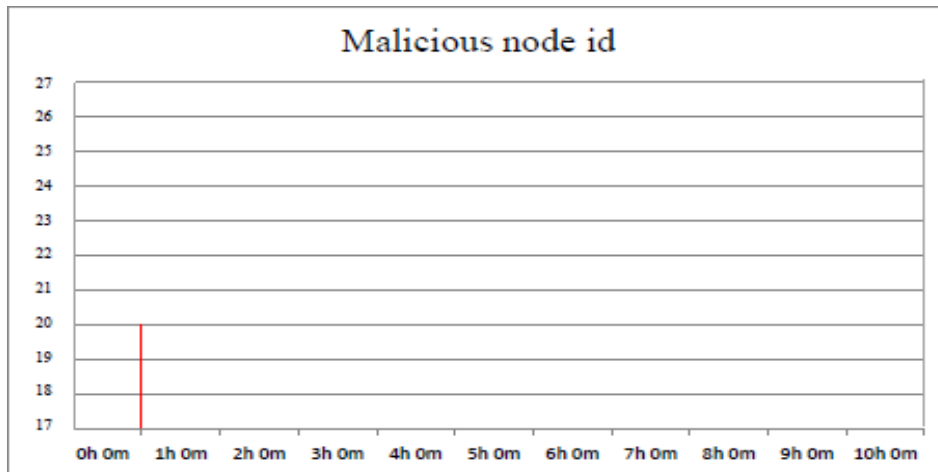
This module It is not feasible for all nodes to transmit data independently to the nearest access point (AP). This is because packet collisions and battery exhaustion leads to data loss. One solution involves the sensor nodes to electing the cluster head (CH) among themselves by using a weight computation procedure after the unbeaten election of the cluster head the nodes transmit their data to the cluster head. Then it aggregates the encrypted data and transmits it to the nearest access point. This access point in turn routes the data to the base station using a customized version of mesh routing this prevents the data transmission from collision, traffic and data loss.

### Secure Routing

Routing is very important in any type of data transmission and most of the attacks occur during the routing phase. To avoid this, the trust worthy between each node should be included before the route reply and route request has been confirmed. If trustworthy is added to each node then the data transmission will be on trusted way so there is no chance of passing the information through the malicious node thereby the attack can avoid. If any un-trusted node has been identified in between the transmission it automatically select the another trusted node for the data transmission this helps to avoid the malicious act in the routing phase.

### Secure Access by Doctors

In the medical health care monitoring system the security and authentication is very important because it carries very sensitive data about the patient. That much security and authentication should be provided to the data which is going to be accessed by the doctor from the central storage. Only the authorized doctor should access the patient data from the central storage by using the password or by using other cryptography techniques.



Graph-1 Node 15 turns to malicious node in time 1000s

## LITERATURE SURVEY

### Introduction

In this work, the detailed study of the recent health care monitoring system has been studied and analyzed for the remote data delivery and security of the data in HMS. Some papers based on different technologies has been discussed their transmission of data and methods and others focused on the security and authentication of the remote data. From the different sensors which are placed in the patient body. In this different mechanisms has been analyzed briefly in the below sections.

### Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT

In this they proposed the solution for black hole and selective forwarding attack in PMS (Patient monitoring system) by introducing the pre-deployment and routing algorithm which is to find the malicious node in data transmission. This algorithm shows high accuracy compared to its existing work. Even though it gives high accuracy it has some draw backs in the pre-deployment and in routing phase because routing is important to transmit the data and attacks also frequently occur in the routing phase, so it needs more security in routing [1].

### Secure authentication for remote patient monitoring with wireless Medical sensor networks

In this work the protocol is based on the Rabin authentication algorithm, which is modified in this paper to improve its signature signing process, making it suitable for delay-sensitive medical sensor network applications. To advance the competence of the Rabin algorithm, they implemented the algorithm with different hardware settings and encoding of an FPGA to appraise its design and presentation. It is considered an individual security of data called of RSA. However, Rabin's system was faster and lighter than RSA. This gives it an estimable candidate for our distant patient monitoring system with medical sensor network. Compared to earlier hardware platforms, FPGA implementation provides better features, including hustle, lower cost, faster growth time and elasticity [2].

### Raspberry Pi Based patient health status observing method using internet of things

In this a temperature, respiration, patient's body actions and heartbeat analysis are monitoring using Raspberry Pi. These sensory signals send to the Raspberry Pi via amplifier circuit and to the signal conditioning unit (SCU), because its signal levels are low (gain), so amplifier circuit is used to boost up the signal and transmit the signals to the Raspberry Pi. The Raspberry pi is a Linux -based operating system it will work as a small PC processor system. The patient's body temperature, body movements, respiration and heart rate is measured using own sensors and it can be monitored on the monitor screen of a computer using Raspberry Pi and it can be monitor through anywhere in the world using internet source [3].

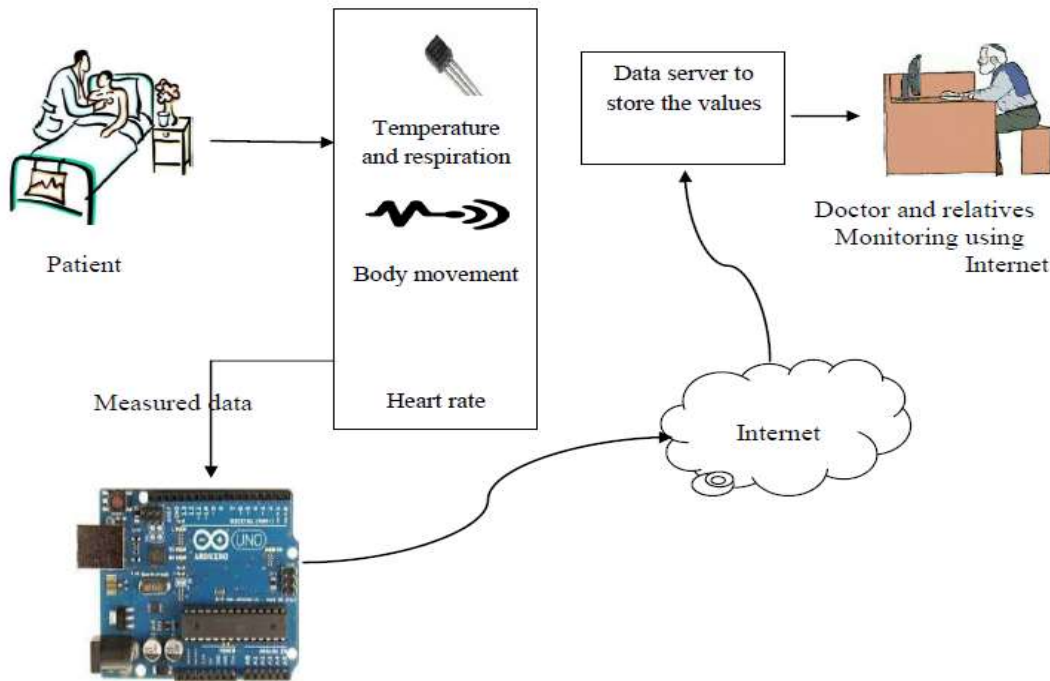


Fig.4. Architecture of Healthcare using Raspberry Pi

#### Secured smart healthcare monitoring system based on IoT

This project has PIC18F46K22 microcontroller used as a entry to converse the various sensors such as warmth sensor and pulse sensor which was placed in the human body .The microcontroller act as bridge to transfer the collected information and stored in the PIC18F46K22 by using the WiFi that data will transfer to the particular doctors web page from there the doctor can view the patients update regularly. And it also has additional feature such as alerting technique. When the sensor observes any emergency values beyond the normal level the buzzer alerts will be sent to the doctor and patients care taker. Even though it has some advantages it also has drawbacks because it only focused on in-patient monitoring system [4].

#### A healthcare monitoring system using wireless sensor network with GSM

This paper presents a monitoring system to monitor the physiological parameters such as BP, ECG, Body Heat and Respiration etc., the manager node has to attach to the body of patients for collecting a signal from wireless sensors. The wireless sensors send this signal message to base station or control room of physician. The wireless sensors from wireless body sensor network. The node of each WSN collected of healthcare sensors and RF trans-receiver it will send data back to end server. Sensors can be chosen in the range of WSNs, while RF trans-receiver is implemented as a manager which manages WSN other than forwarding the data. The sensory data of each patient are stored in the back-end of the server with each has its own ID. The data analysis, database inquiry, data manning and the system managing are the process in a web page of a server. The system can detect an abnormal condition of the patient and send it through the SMS or e-mail to the physician [5].



### Real time wireless health monitoring application using mobile Devices

This real time monitoring system uses the mobile phone as a device to display the updates to the doctor it uses the LabVIEW technique. The same process is used in this by sensing the data from the human body using the sensor and transmits its psychological information using the WiFi and to display its update by using the LabVIEW technique. In this it used the alerting system such as buzzer and email to the doctor and patients relatives who cared for the patient. This also focused only on the in-patient monitoring system [6].

### Patient monitoring system using MSP430 microcontroller

It is a tough job for the doctor and medical staff to monitor each patient for 24 hours. In this paper, it introduces a system in which it collects physiological signals of patient transfer this signals to a personal computer using Ethernet controller. So hear patient can be analyzed by the doctor or other paramedical team from central observation centre or from their PC. And also this bodily signal displayed on LCD screen [7].

### Security and privacy issues in wireless sensor networks for healthcare applications

There is a possibility of serious communal conflict due to the fright on such devices may be used for monitoring and tracking individuals by government agencies or other private organizations. In this paper, the discussion is about the issues and analyze in detail. The problems and their possible measures. All communications over wireless networks and internet are essential to be encrypted to protect the data from the attack. Some countries have added this type of section in their active legal acts or enacted new laws. Another important gauge is to create awareness in general public. It will be extremely beneficial if people are educated regarding security and privacy issues and there is an implication from now on. It is mentioned by authors in that common people do not understand the technology and therefore may not be in a position to make balanced judgments concerning the extent to which it will have a negative impact on their own values of privacy. Therefore educating a common people will greatly help in this regard [8].

### Wireless health care monitoring

Doctor need to monitor the patient's health condition regularly but it is tedious job to take care of regular update of both in-patient and out-patient. To make it easy the different sensors are placed in the patient's body by using the GSM module the sensed data was transmitted using the GSM. Now-a-days the use of GSM in different fields becomes very familiar. Based on that technique in healthcare monitoring system GSM plays a vital role by using that the data will be transmitted to the webpage and doctor can retrieve the stored information anywhere and suggest the treatment at any time [9].

### Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN

In this, the protected routing protocol is based on observing of different nodes and trust mechanism. The eminence value is made up of packet forwarding rate and node's lingering energy. So this exposure and routing device is worldwide because it can take account of both the safety and lifespan of a network. In this, they discussed different techniques such as watchdog, Trust Mechanism to identify unruly nodes in wireless ad hoc networks [10].

This proposal can be applied in WSN and it was the earliest trust mechanism which is the foundation of many defense methods. In their approach, each sensor node has its own watchdog that checks and records the behaviors by its one-hop neighbors. The watchdog system of each node provisions the routing table which is about the act good or bad of the neighbor nodes. In proposed work the OPNET simulation is to appraise the custom of our trust monitor model and routing system. In our simulation, 100 sensor nodes and 10 monitor nodes are erratically dispersed over a 100 m × 100 m area. We only do the imitation of the local network. A monitor node controls 10 common nodes in each region. Firstly, the nodes will be numbered to meet the design needs of the software.

## ANALYSIS

This section presents the comparison of different methods used and compared its advantage and disadvantages of on patient health monitoring system which we reviewed detail and based on this the solution will be found in the finest scheme of the patient health care monitoring system.

**Table:1. Comparative Analysis of Health Care Applications**

PAPER No.	METHODS USED	ADVANTAGE	DISADVANTAGE
1	- Cryptographic hashes -pre-deployment -Routing phase	- It shrink the further possibility of different attacks because it has different time intervals	-In pre-deployment there is no chance to find the malicious attack before the distribution of unique code. -Needs trust worthiness
2	-Rabin algorithm	-Rabin signature generation drastically reduced the delays	- Rabin scheme is only focused on the in-patient monitoring system and its performance was measured using with and without parallel execution. It doesn't have any standard execution.
3	-Raspberry Pi, putty Software, putty Software, apache server	-It reduces patient's money and time. -Using this technology development, patient's record their health status in Their own mobile phone and then store the data. -it will automatically send alert message to doctors and relatives mail.	-Only few Parameters have been measured.
4	-PIC microcontroller, ESP8266 Wi-Fi module, AES128	-It is capable with low power utilization capability, easy setup, high routine and time to time response.	-It won't connect all the sensed data easily through WiFi
5	-RF trans-receiver , GSM modem	- Decrease the power utilization	-Security issues are very high
6	-ZigBee, LabView	-Low cost, low power, easy functioning, trustworthy, and high sanctuary.	-Few parameters has been measured
7	-Ethernet controller	-Patient can be analyzed by doctors from central observation centre.	-For hospitalized patients
8	-WBAN, Privacy and security	-Improves the security by encrypting the data adequately	- All infrastructure over wireless networks and internet are required to be encrypted to protect the user's time alone.
9	-GSM, ZigBee.	-Low cost for monitoring	-Need more sensors -Vulnerable Security threats -Investment Cost is high
10	-Secure routing protocol, monitor node	-Improves the finding of malicious node in beneficial way	-Need to improve the trustworthy

**Table: 2. Performance Evaluation**

Technology and algorithm	Accuracy of remote data delivery	Malicious node detection rate
- Cryptographic hashes -pre-deployment -Routing phase[1]	86%	93%

-Rabin algorithm[2]	88%	92.5%
-Raspberry Pi, putty Software, putty Software, apache server [3]	92%	-
-PIC microcontroller, ESP8266 Wi-Fi module, AES128 [4]	90%	-
-RF trans-receiver, GSM modem [5]	93%	-
-ZigBee, LabView [6]	92.5%	88%
-Ethernet controller [7]	91%	-
-WBAN, Privacy and security [8]	89%	90%
-GSM, ZigBee [9]	90%	-
-Secure routing protocol, monitor node [10]	89%	93%

## CONCLUSION

The Importance of the automated health care application and the existing available health care applications are discussed in this article. Then the security threads imposed on those applications and their performances are compared for remote data delivering from patient to doctor database by using Sensor ,Bluetooth, Mobile phones ,Cloud storage etc., All this is to reduce the human workload .This type of techniques is used in different fields for regular monitoring and secure data delivery. In the Healthcare it plays the major role and it is very useful for the patients to manage their health conditions frequently with help of doctors being in the home. In future security and privacy issues while transmitting the remote data delivery can be protected using a cryptographic technique.

## CONFLICT OF INTEREST

The authors declare no conflict of interests.

## ACKNOWLEDGEMENT

None

## FINANCIAL DISCLOSURE

None

## REFERENCES

- [1] Avijit Mathur, Thomas Newe and Muzaffar Rao.[2016] Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT , Published on 19 January 2016 Received- 17 December 2015, Accepted- 14 January 2016, Academic Editor- Rongxing LuSensors 2016, 16:118, doi:10.3390/s16010118
- [2] Thayer Hayajneh, Bassam J Mohd, Muhammad Imran, Ghada Almashaqbeh, Athanasios V.[2016] Vasilakos Secure Authentication for Remote Patient Monitoring withWireless Medical Sensor Networks” Published: 24 March 2016, Sensors 16, 424: doi:10.3390/s16040424
- [3] R Kumar, M Pallikonda Rajasekaran. Raspberry Pi Based Patient Health Status Observing Method Using Internet of Things” *International Conference on Current Research in Engineering Science and Technology (ICCREST-2016)* E-ISSN :2348 – 8549.
- [4] BK Bhoomika, Muralidhara K N. Secured Smart Healthcare Monitoring System Based on IoT’ *IJRITCC*, ISSN:-2321-8169 3(7):4958 – 4961.
- [5] L Sunil Rahane, S Ramesh Pawase, A Healthcare Monitoring System Using Wireless Sensor Network with GSM’ *IJAREEIE*, An ISO 3297:- 2007 Certified Organization 4(7)-July 2015 ISSN: 2320 – 3765:ISSN (Online)-2278 – 8875.
- [6] Ali Abou-ElNour ,Asma Ismael, Aisha Rashid, Amna Abdullah.[2015] Real Time Wireless Health Monitoring Application Using Mobile Devices’ *IJCNC- 7(3)* DOI - 10.5121/ijcnc.2015.7302.
- [7] Pradip S. Bhendwade, Ms. Sarika M. Patil,” Patient monitoring system using MSP430 microcontroller”, *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)* 4(1), January 2015,ISSN: 2278 – 909X All Rights Reserved © 2015 IJARECE
- [8] Kyungsup Kwak,Moshaddique Al Ameen ,’Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications’ Received- 18 December 2009 ,Accepted- 16 February 2010 Published online- 12 March 2010: *J Med Syst* (2012) 36:93–101 DOI 10.1007/s10916-010-9449-4
- [9] Bazila Banu A, Kavitha KC.[2014] Wireless Health Care Monitoring’ *IJRSET*, 3(SPL.3) ISSN (Online) :- 2319 – 8753 ;ISSN (Print) :- 2347 – 6710.
- [10] Hongshuai Wang ,Yu Hu, ‘ Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust



Mechanism in WSN' WSN; 2014; 6; 237-248 Published Online November 2014 in SciRes.

- [11] M Li, W Lou. Data Security and Privacy in Wireless Body Area networks", IEEE Wireless Comm., Feb. 2010, pp. 51-58.
- [12] Luan Ibraimi, Muhammad Asim, Milan Petko Vic.[2010] Secure Management of Personal Health Records by Applying Attribute-Based Encryption, *IEEE* 2010.
- [13] N Jaisankar, R Saravanan, KD [2010]'A novel security approach for detecting black hole attack in manet';GaoI, F.L., Thankachan, N, Eds- Springer:- Berlin: Germany:.
- [14] An Internet of Things. Last access Mar. 14, 2015. Available on: <http://postscapes.com/internet-of-things-examples/>.
- [15] Wassnaa AL-mawee. [2012]Privacy and Security Issues in IoT Healthcare Applications for the Disabled users. A Survey" Western Michigan University Scholar Works at WMU Master's Theses, Graduate College2-2012
- [16] P Thangaraj, K Geetha.[2015] FGT2- ABR: Fuzzy Game Theory Trust Associativity Based Routing to Mitigate Network Attacks in Pervasive Health Monitoring Systems, *Journal Of Pure And Applied Microbiology*, 9:161-168.
- [17] S Brand.[ 1994] What happens after they are built, in *How Buildings Learn*, London, U.K.: Penguin.