Empirical Usage of Body Area Network and Group key in Home Health Care System

K.Suseendhra
M.Phil (CS) Research Scholar
SCSVMV University
Enathur, Kanchipuram

S.Prakasam Ph.D
Assistant Professor
Department of CSA,SCSVMV University
Enathur,Kanchipuram

ABSTRACT
Body Area Networks are the networks of wireless medical sensors, deployed on a person for enabling pervasive, individualized real time health management. As BAN deals with personal health data, securing them especially their communication over the wireless link is very crucial if there is adequate security feature for the patient in the body area sensor network then the adversaries can change the actual data which will lead to wrong diagnostics and treatment of the patient in order to provide a personalized health care system. The Body Area Network along with the group key is established for the security concern where they will provide a separate key to each of the sensors that are of deployed in the patient body when this key matches with that of the health care server system the key establishment of the network

Keywords
Sensors, group key, body area network

1. INTRODUCTION
The Body Area Network in the home health care system is used to monitor the elderly ,patients, who suffer from the chronic diseases where the sensor will send the physiological signals to the physician and in return they will send the feedback to the patient through the personal device which will provide a real time monitoring in the home health care system [3] .The security and the information access plays a vital role in home health care [8], where these can be achieved through the group key establishment among the body sensor networks these can be shared through the devices, once the data is sensed then the sensor nodes are made available [6] the main goal of the group key is to reduce the logistic constraints between the doctor and the patient

2. RELATED WORK
The work is closely related to the two distinct areas such as the body area network and group key

2.1.1 Body Area Network
The Body area network (BAN) is a wireless network of health monitoring sensors designed to deliver the personalized health care enabling the secure inter sensor communication within the BAN in a usable manner where the Body area network is deployed in the sensors to make the communication securable [1],[4] is to ensure the confidentiality and integrity by providing the key agreement where they will exchange the secrecy among the BAN by building the channel hidden from the outsiders where by creating the artificial electrical signal below the action potential by this it has no effect on the body. Securing the broadcasted data and the commands within the BAN is essential for ensuring the safety of the patient and also for preserving the privacy of the data which is established between the different sensors within the BAN another mechanism to secure the communication is to place the small electrical charge around the body and use that communication medium where they are in need off the minimal memory and the bandwidth resources are of needed this can be achieved by using the protocol known as the (SEV) secure environmental vault [14],[2] employs the sensor known for the unique patient identification where one of the nodes is employed in the body is used for the diagnostic which will have a knowledge about the sensor configuration used simply to transfer the data on the respective health system, In the wireless sensor networks each of the sensors act as the sensor node as well as the router to the system[15].A wireless body area network is a radio frequency [5]based wireless networking technology which will connects the nodes with a short range of about 2 m which will target the diverse applications such as the safeguarding of uniformed personnel athletic training, consumer electronics are some of the communication technologies.[15] employs the Ban for monitoring the physiological signals where it uses the secure socket layers which is used to avoid the jamming, and also the without the interference of the battery depletion

2.1.1.1 Group key
By using the symmetric keys between the sensor nodes are of employed in the wireless sensor networks by using three categories such as pair wise scheme, pre distribution scheme , random key method [10], the pair wise and the random schemes are of mainly used in the individual sensors that are of employed in the open environment and the pre distribution method is used for the pair of the sensors that are of deployed where they will create the trusted intermediary [7] employs the group device pairing (GDP) which is used for the secure communication in the key management protocol for the authenticated group key management in the wireless communication .A key agreement protocol is contributory and distributor in nature as it will maintain the freshness in the database[12] then the trusted third party will generate the key and then distributes it securely. The secure group key agreement can be achieved by using the protocol known as the (STR) skinny tree [9] which uses the diffie - hellman key exchange where they are of employed in the dynamic group key establishment in peer groups where this protocol will offer the key independence and perfect forward secrecy, [13] employs the wireless sensor nodes where they will share the secret key in a efficient authenticated two-party method for the improved (MAC) the method of key pool is used for the robustness where they provide a faster way of communication for the sensor nodes where only one key is used in the key pool for the life time in order to provide the reliable communication Contributory key agreement protocol is used in the peer group communication which uses the secure synchronous ring protocol(SSRP),the main property of the system is to provide the fault tolerance, and to maintain the secrecy in the group communication which will form a hierarchy towards the node leader and representative of the node where the key agreement is made between the inter and the outer ring.[11] describes about the available group key protocol known as the message broadcast protocol for the message authentication where it generates the code for the

message that ha to be generated this verification is done by using the symmetric key where it verifies the key number

3. PROPOSED ARCHITECTURE USING HOME HEALTH CARE SYSTEM FOR THE BAN & GROUP KEY

The body area network in the home health care system is a predominant in the medical application where the intelligent nodes are of deployed in the patient body which has the ability to sense, process, communicate with the different physiological signals are of also known as the (PS) that are mainly used to measure the physiological signals in the patient such as the heart beat , blood oxygen level, blood pressure where the sampling rate of these physiological signals are of recorded these sample rates are of stored in the health care server then there is unusual level of the patient is continuously monitored using the sensor nodes that are of attached where these nodes are of in minimal size and weight which will provide a integrity and calibration to the user . The actuators also play a vital role in the body area network as they inform the changes that occur in the body where the sensor will just detect the difference in the sample rate but the actuator only will be able to detect the difference that occur in which part of the body then this will be sent to the personal device .and then the physician will gives the feedback to the patient.

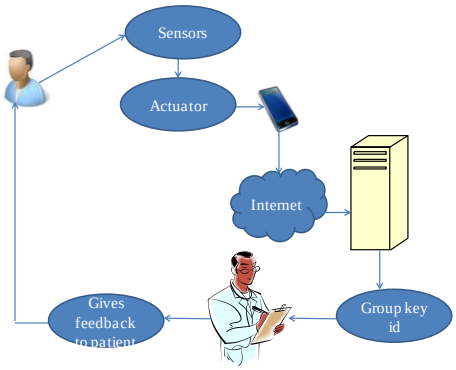

Fig 1: Architecture of home health care system using the BAN & Group key

The body sensor networks are of deployed in home health care system it will reduce the financial burden of the user as well as the cost is minimum, where it will reduce the interaction with the humans in the hospital and also provides the quick treatment to the patient .The sensor nodes in the body area network are of stationary where the patient can move anywhere this will lead the nodes to be in same direction even though many of the nodes are of deployed in the patient , if there is a small change in the movement of the patient body than the prescribed level then the sensor nodes will inform to the actuator where the Ban requires the energy for the data processing, transmitting, collecting and for the development for this the energy becomes a paramount in the nodes, the battery that are of placed in the sensor nodes are of replaceable where the energy transmission in the sensor nodes are of short range as the patient may be walking, running, or may be twisting so at that time the sensor nodes to be a static. Thus the sensor attached in the body will transmit the data for 1 to 40 times per hour where the BAN will provide a real time feedback to the users this can be made possible with the help of the specific applications in the personal device**.** The sensor nodes that are of deployed in the human body will have a contact with the neighbor nodes where the nodes will establish a key generation process to provide a group key identity to the health care server, these groupkey is classified based on the identity that is provided by the sensor nodes when they are of installed in the patient body ,the fig(1.2) represents the users of the home health care. The server will also have separate identity based on the type of the diseases they are of divided when these sensor node identity matches with that of the identity in the server then the group key identity is valid or else the key is mismatched .The nodes will inform the emergency to the other nodes in case of the critical situation where these notification is taken to the personal device which will in turn inform to the health care server

4. IMPLEMENTATION OF NEW ARCHITECTURE

The core concept behind the wireless body area network is to remove all wires that are of connected to the patient and to develop the wireless network between the sensors where these will reduce the connection with the wires and also will not reduce the comforts of the patient. The Body Area Network in the wireless technology will interconnects the tiny sensor nodes and the actuators that are implanted in the human body where these sensor nodes are of mainly deployed in the cloth or in the shoe of the patient used to monitor the patient continuously where the curvature of the body is to be considered at the time of installing the sensors in the home health care system whose function is to detect the chronic diseases that occur mainly in the aging population , the sensor nodes will senses the nodes for every 10 seconds if there is any change in the physiological signals such as heart beat, blood temperature, blood oxygen level then the sensor nodes will inform to the actuator which will in turn will send the message to the personal device about the difference in the physiological signals of the patient, then this will be sent to the wireless medium communication such as internet after that the information will pass to the health care server which is under the control of the hospital where it just shows the mobile number of the certain patient in the sever , then it will check for the group key identity that is provided for the patient at the time of the node installation, this key will be matched only when the group key identity of the server and the sensor node identity of the patient is matched or else the key is invalid. Then history of the patient details is sent to the physician form is represented in fig(4) who will in turn send the feedback to the patient, the BAN is designed to satisfy the wide range of the applications such as the health monitoring and the emergency response using the BAN the patient will experience the greater mobility and no longer to stay in the hospital where this process is considered to be the next step of the enhancement in the home health care system where it will also cope with cost of the health care system, securing of the sensor nodes will not only provide the privacy of the data but also the safety of the patient details. Sensor nodes are of mainly deployed in the health care system where any can placed anywhere in the human body where it has a contact with the neighbor nodes to establish the key generation these nodes will also have unique identification node where these will be known only to the particular node generated the sensor nodes will have a contact with the human body for every 10 seconds when they senses any frequency rate is abnormal then

it will sent the information to the other node about where there in a default in the body location where these two nodes will establishes a key generation to prevent it from the outside attack The communication of the home health care system is more flexible as the sensor nodes in the body area network will communicate with the personal device which is easy for the user of the system where there is no need of any other devices for the communication where the physician or the specialist can also contact the patient through the wireless technology as this system supports the alternative way for the communication the patients and as well as the physicians which leads to the flexible way of the communication

4.1 Networking in the Body Area Network

The application scenario of the body area network is different from the traditional sensor nodes where the sensor calibration is revisited well before the usage as the nodes can join /leave the network at any time

4.2 Temperature Routing In Body Area Network

Considering the wireless sensor nodes fig (1.3) represents the temperature monitoring in patient it will cause some heat in the tissues of the patient body this can be reduced by balancing the communication over the sensor node

4.3 Security Concern In Body Area Network

The data of the home health care system should be confidential, authenticated, as the transmission of the data is privately concerned one as it can be accessed only by the authenticated persons, as the data are encrypted this will make easy for the group key to share with the user .Furthermore the patients are in surveillance to carry the sensor nodes along with them so it will be difficult for the outside attackers to detect where the nodes are being attached in the body

4.4 Home Health Care System – Users and the Sample

To find the patient's effectiveness of health in the body area network which is based on before and after the hhealth care system during the November 2013- December 2013

Table 1 .Users of Home Health Care

Gender	Number of Respondents	Percentage
Male	60	58.4
Female	44	41.6
Total	104	100.0

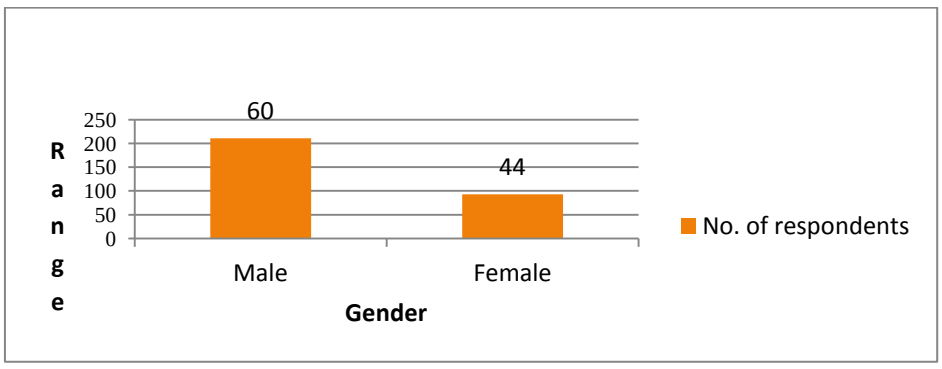

Fig 2: Users of home health care

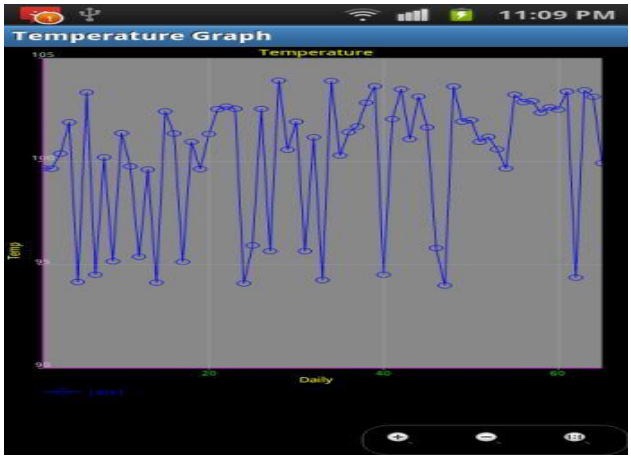

Fig 3: Body Temperature Monitoring in Patient

Table 2. Status of the patient in the health care

Date	Time	Temperature	Glucose Level	Blood pressure	Status
2013-12-01	08:00:00	102.0	80	100.0-130.0	Lowtemperature,normalblood pressure,normal glucose level
2013-11-06	08:10:00	102.0	75	10.0-140.0	Lowtemperature,highblood pressure,normal glucose level

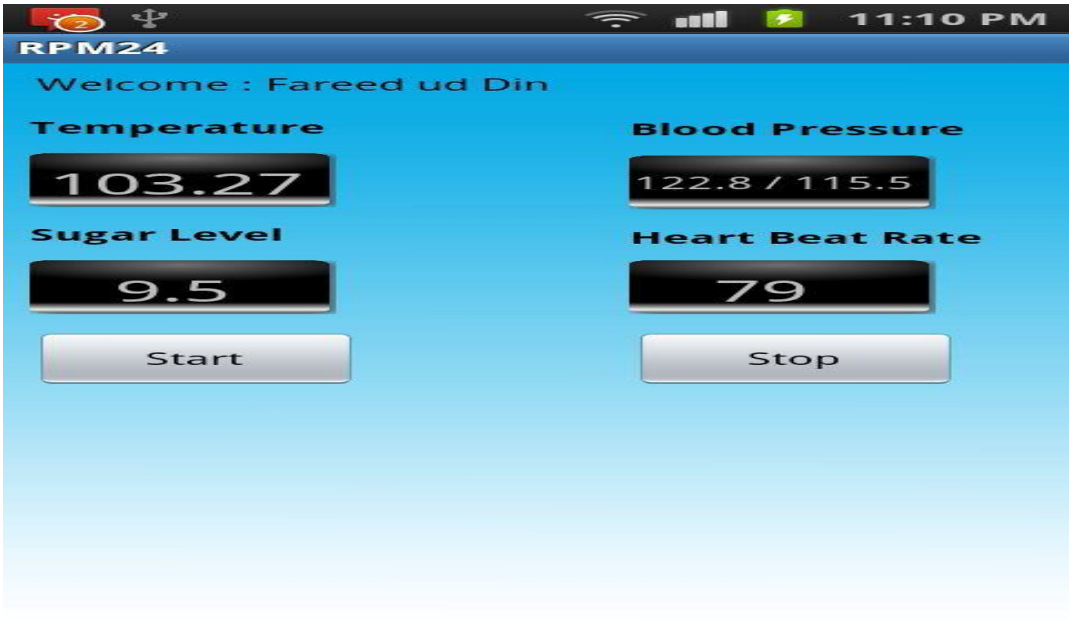

Fig 4 patient vital signal monitoring

4.5 Advantages

a) Whenever the node is deployed in the patient body it will be able to join the other nodes and also set up a route without any of the intervention
b) As the nodes are of self organizing it will able to detect the problem that occurred in the nodes
c) The entry from the outsiders is prevented by using the exclusiveness of the key where it allows only the member of the group
d) There should not be any information regarding the previous group key generation this can be solved by using the forward secrecy in the group key

The body area network will provide a real time feedback to the users using the personal device It uses a limited energy resources where they require low transmit power per node to cope up with the health issues it needs the reliable communication with limited power supply so depending on the health risk and privacy concerns all the information will not be transmitted to the hospital more sensors can be added to get more data .The command to all sensors should have secure group key the main goal of the home health care system is to reduce the logistic constraints between the doctor and the patients .

5. CONCLUSION

The wireless body area network are of mainly used in the health application as it will offer wide range of benefits to the patients by continuous monitoring them, to the medical personal , and also to the society through this it is possible to detect the diseases at the early stage , and by using the group key generation it is possible to have a multiple devices to share the key in a authenticated manner , the another feature of the home health care is the patient don't need to go to hospital by just sitting in the home it is possible for the user to know about the diseases without visiting the doctors and also having the conversation with them will lead to the wastage of the time, by using the group key technique it is possible to have reliable communication with the sensor nodes , and also it will reduce the complexity between the nodes , the sensors will integrate with the body area network in a step by step process where by having a close proximity with the nodes in the health care system so the medical information should be of stringent one in the medical field which will be able to provide a quality of the life using the home health care system in a wireless technology

6. REFERENCES

[1] K.Venkatasubramanian, (1999) " Usable and secure key agreement scheme for the body area network", member IEEE ,Ayan Banerjee, and Sandeep Kumar , S.Gupta senior member ,IEEE pp 155-165

[2] Javad Ahmad , (2004) "Review of body area network technology & wireless medical monitoring", EURASIP networking journal on wireless communication of information technology pp 1-7

[3] Kalvinder,Vallipuram Muthukkumarasamy,(2008) " Using physiological signals for the authentication in a group key agreement protocol" international of physical networking system in sensors pp 406 -407

[4] Sang –Yoon chang, Yih- Chun hu, Hans Anderson (2011)," Body Area Network security robust key establishment using the human body channel", IEEE symposium on security and privacy pp 310-315

[5] Huasong Cao and Victor Leung,(2005)" Enabling technologies for wireless body area network " IEEE journals on the information technology in medical sensors, pp 432-439

[6] Daniel Augot Raghay, Bhaskar, Valerie Issamy,(2003)" An Efficient Group Key Agreement Protocol for Ad hoc Network" IEEE engineering in medicine and bio sensors pp 73-81

[7] Ravindar Thammadi, D.jamuna ,M.Srinivasulu, Naveen Thammadi, (2006) "BAN group device coupling based protected sensor connection for key management" transaction on the medical implant sensors pp 240-245

[8] Kalvinder singh Vallipuram Muthukkumaraswamy, (2010) "Verification of key establishment protocol for the home health care system" IEEE communication magazine pp 1-6

[9] Shital Supaseri and Rajesh Ingles (2009)," Performance analysis of sponsor selection algorithms in group key agreement " IEEE ccnc volume 6 pp 819

[10] T.Falck, H.Baldus, Espina and K.Kllabunde(2003), "plug and play simplicity for wireless medical body sensors" IJERT vol 1 pp 1-16

[11] T.Balomenos (2011), "user requirements analysis and specification of health status analysis and hazard avoidance " IEEE –EMBS on medical sensors implant pp 408

[12] K.Venkatasubramanian and S.K.S Gupta (2012) "security for pervasive health monitoring of sensor applications" FIDJI on the communication on sensors pp 500-528

[13] Klabunde.k and schenk (2008) "Human centric connectivity enabled by body coupled communication" SENSORCOMM on sensor applications pp 147 -165

[14] Bao D.Poon & zhang(2011) " using the timing information of heartbeats as a entity identifier" EMBS symposium of medical sensors pp 68

[15] Wegmuller (2005) , M.S," intra body communication for bio medical sensors" ISWC on sensor networks pp 408.