Secured Healthcare and Patient Monitoring System using Vanet Based Wban

S. Kalaiyarasi[1] A. Joseph Selva Kumar[2]
[1]PG Student [2]Asst. Prof Dept. of IT,
[1&2]Affiliated to Anna University Chennai,
Dept. of Computer Science and Engineering
Idhaya Engineering College for Women

***Abstract* - Now a days there are thousands of diseases and lakhs of hazardous bio molecules are spread over the world, many of the human beings and other living beings in the earth gets affected by these diseases and became ill, even it causes to death. So, continuous monitoring of these patients is needed to provide proper medicines and first aids. To facilitate the continuous monitoring of patients for a long time it is not possible to get admitted in the hospital. So these patients are remotely monitored by wireless sensors even though when they are travelling. In existing system the monitoring takes place in static places such as in patients home and offices, securely. It is not possible to monitor the patient while they are travelling, or while they stay out of their monitoring area. It can monitor the patients while travelling and even they stay out of their monitoring area with the use of vehicular adhoc networks and wireless body area sensor networks.**

Index Terms-Adhocnetwork,vehicular adhoc network,wireless body area sensor network,user access control,security.

1. INTRODUCTION

A wireless ad hoc network is a decentralized wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity.

The decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on, and may improve the scalability of wireless ad hoc networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of a dynamic and adaptive routing protocol will enable ad hoc networks to be formed quickly.

1) *MAC :*MAC protocol for wireless sensor networks must consume little power, avoid collisions, be implemented with a small code size and memory requirements, be efficient for a single application, and be tolerant to changing radio frequency and networking conditions. One example of a good MAC protocol for wireless sensor networks is B-MAC. B-MAC is highly configurable and can be implemented with a small code and memory size.

2) *ROUTING:*Multi-hop routing is a critical service required for WSN. Because of this, there has been a large amount of work on this topic. Internet and MANET routing techniques do not perform well in WSN. Internet routing assumes highly reliable wired connections so packet errors are rare; this is not true in WSN. Many MANET routing solutions depend on symmetric links (i.e., if node A can reliably reach node B, then B can reach A) between neighbours; this is too often not true for WSN. These differences have necessitated the invention and deployment of new solutions.

*3) VANET:*VANET is a new technology that integrates the potentials of new generation wireless networks into vehicles. VANET aims to offer (i) continuous connectivity for mobile users while they are on the road, which enables them to link with other users through the latter's home or office based networks, and (ii)efficient wireless connection between vehicles without access to any fixed infrastructure, which enables the ITS. Consequently, VANET is also known as inter-vehicle communication (IVC).

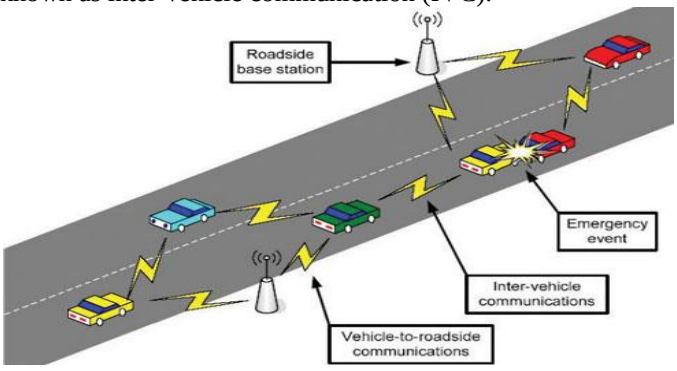


Figure 1.1 Architecture of VANET

Figure 1.1 shows that VANET devices such as on-board units are fixed in vehicles and function as the nodes to transmit and receive messages through wireless networks. These devices provide drivers and passengers with the latest information on accidents, flooding, rain, traffic jams, and any disturbances. By obtaining such

information on time, drivers can make appropriate decisions and avoid mishaps. The features of VANET are typically similar to the operation technology of a mobile adhoc network (MANET) in the sense that the self-organization, self-management, low bandwidth, and shared radio transmission conditions remain the same. However, the key operational impediment of VANET arises from the high speed and tentative mobility (in contrast to the MANET) of the mobile nodes (vehicles) along the paths. This fact indicates that the competent design of routing protocol requires improving the MANET architecture to efficiently accommodate the fast mobility of the VANET nodes.

*4) INTRODUCTION TO WBAN:*Recent advances in wireless communications and computing technologies have lent redibility in the migration of health care systems from traditional paper based to electronic system.

These chronic diseases require long-term monitoring, accurate disease management, lifestyle changes, and medication screening.Various statistics reports indicate that 133 million people or almost half of all Americans live with a chronic condition. Moreover, some large metropolitan areas contain small towns and these small towns are isolated from the central cluster. Providing long-term health care to these areas is also challenging. Recent advances in Wireless Body Area Networks (WBANs) have made it possible to deploy bio-sensors on, in, or around the patient lives at the rural area and allow to provide long-term monitoring of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels) with physical activities. However, technological solution is needed to transfer these aggregated sensed data from the patient residence to the care giver's end.

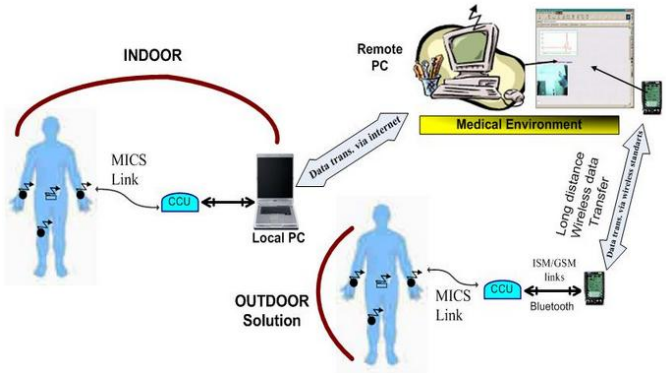


Figure 1.2 Patient monitoring using WBAN

Figure 1.2 shows WBAN sensors monitor user's heart rate and locomotive activity and periodically upload time-stamped information to the home server. The home server may integrate this information into a local database for user's inspection or it may forward the information further to a medical server. The prototype may be used for ambulatory monitoring of patients undergoing cardiac rehabilitation or for monitoring of elderly at home by informal caregivers.Remote patient monitoring provides additional benefits to both patients and medical personnel. The design principle and authentication processes of a remote health care system are more important. Timestamp based authentication protocol in remote monitoring system is introduced in this paper and a specific protocol for untrusted mobile devices is also proposed in their work.

Remote health care architecture with patient-centric access control is proposed. In order to assure the privacy of patient's personal health information (PHI), authors first defined different access privileges to data requesters according to their roles and then assigned different attribute sets to the data requesters. By using these different sets of attribute, only the qualified access requester can get access to corresponding patient's PHI and thus ensures patient-centric access policies in a remote health care architecture. A heterogeneous wireless access-based remote patient monitoring system is presented. A feasible and effective communication protocol for exchanging patient healthcare information among disconnected clinics and hospitals. By using Tele health enhance access to professional health education for rural healthcare providers. It can inform and educate rural health-care providers about changes in medicine and evidence-based practices, both of which may help them provide quality care.

2. SYSTEM WORK

In our proposed system Mobile gateway routing protocol(MGRP) is used to increase the packet delivery ratio and decrease the average hop count by exploit both inter-vehicle-based and infrastructure-based communication to route packets. Like other position-based routing protocols, MGRP assumes the presence of a GPS and a digital map so that each vehicle builds its neighbour table (including neighbouring vehicles, directions, and speeds) that would assist in routing. Furthermore, digital maps indicate the traffic load condition of roads. Figure 3.1 shows that the fixed RSUs are replaced with mobile gateways to provide connectivity in a considerably larger region. Mobile gateways are equipped with two interfaces: IEEE 802.11(IVC) and 3G interfaces (vehicle-to-infrastructure communication).

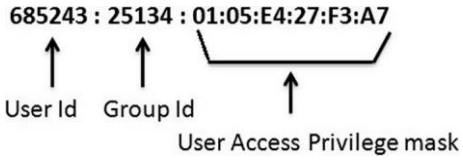


Figure 2.1 An example of a user access list.

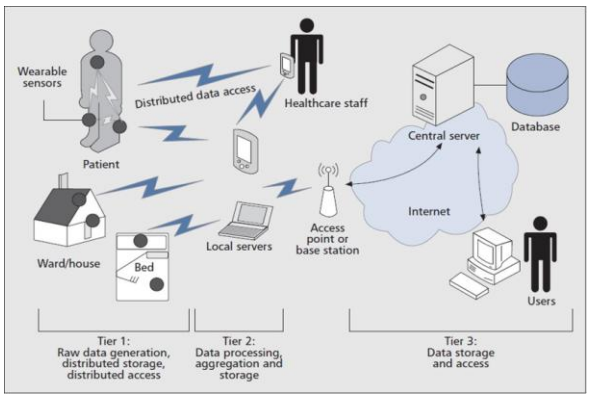


Figure 2.2 A general three-tier architecture of WBAN

3. PROBLEM STATEMENT

In an existing system the patients are monitored continuously only from static places such as their house offices etc. The access points are fixed in their living environment to monitor them continuously and send the data from the sensors attached in their body to health care monitoring systems, which are presented in their trusted hospitals. They maintain the information records, which are sent from the sensors attached in the patients' body. Different body sensors, such as accelerometer, blood pressure and oxygen saturation (SpO2) and temperature sensors frequently send the sensor data to the access point which is present in the home or office. So while travelling the patients are not able to be monitored properly, since they stay away from their environment. Also the existing system communication depends on the existing infrastructure, so if it fails the patients cannot be monitored.

In our proposed system the patients are gets monitored even though they are travelling and they stay out of the home or offices through VANET. Data communication in our proposed work relies on heterogeneous wireless environment, where WBAN (IEEE 802.15.6) is used for the body-sensor to wireless nodes present in the vehicle. IEEE 802.11p namely VANET is used for Inter Vehicular Communication (IVC) to transfer the data, it also uses road side units RSU's. In this paper we can monitor the patients while travelling and even they stay out of their monitoring area with the use of vehicular adhoc networks and wireless body sensor networks.

A typical wireless body area network kit will consist of sensors, a Processor, a transceiver and a battery. Physiological sensors, such as ECG and SpO2 sensors, blood pressure sensor, EEG sensor IEEE 802.11p, also known as Wireless Access in Vehicular Environment (WAVE), is a draft amendment to the IEEE 802.11 standard that adds applications to fast changing vehicular networks.

4. SYSTEM MODEL

1. Creating mobility nodes
2. Data transfer between nodes
3. Plotting graph for performance

4.1. CREATING MOBILITY NODES

In our model, we consider patients or users will be in travel or may be out of the coverage area where network infrastructure is not available and they need secured and long-term monitoring due to chorionic diseases or some other diseases, where the users are located at their own residence, old-home or care centre. Different nodes are developed; nodes are in mobile since the data is carried over the VANET. Data communication in our proposed work relies on heterogeneous wireless environment, where WBAN (IEEE 802.15.6) is used for the body-sensor to wireless nodes present in the vehicle. IEEE 802.11p namely VANET is used for Inter Vehicular Communication (IVC) to transfer the data, it also uses road side units RSU's. The data from the sensors are transferred to wireless nodes through WBAN IEEE.15.6, then the data reaches the destination, health centers through opportunistic routes from IEEE 802.11p.

4.2 DATA TRANSFER BETWEEN NODES

The data gets transferred from source to destination through various nodes, so there is a chance of connectivity gets loss. At that time the data should be transferred once again. For that a time stamp is fixed to get the acknowledgement from the destination, so the sender waits for an acknowledgment for the packet which is sent earlier, if is didn't receives the acknowledgement it resends the same packet in different route.

4.3 Plotting graph for performance

A performance graph is plotted to show the efficiency of the system with various parameters such as packet delivery ratio, hop count, latency of data and throughput.

According to VANET, Figure 4.3 shows the routing tables are updated to find the destination routing path. So for every periodic time interval the routing tables of every nodes in the vehicles gets updated by checking its neighbor nodes.

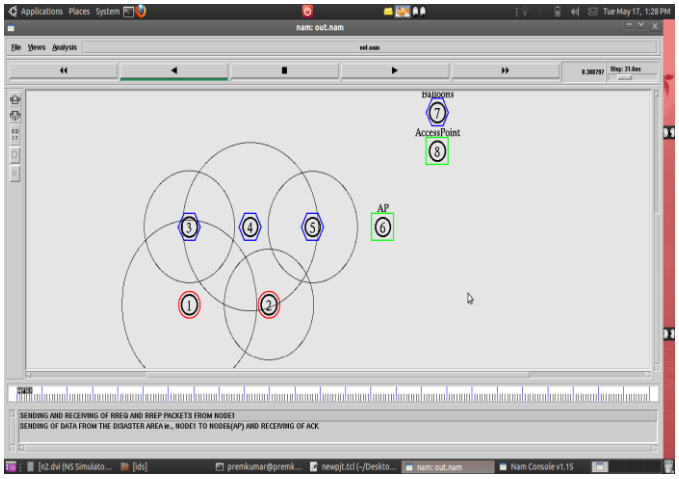


Figure 4.3 Presence of neighbour nodes

5. SYSTEM ARCHITECTURE

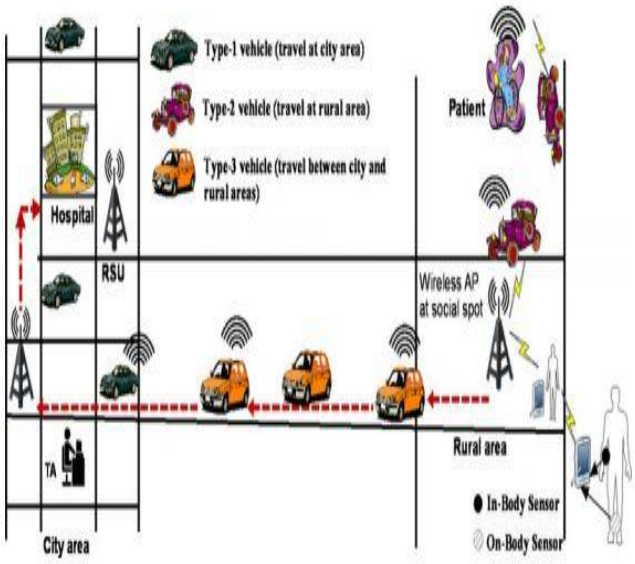


Figure 5.1 System Architecture

6.MGRP PROTOCOL

MGRP is based on the concept of mobile gateways proposed in MIBR, which utilizes buses as a mobile gateway with a fixed route. However, their connectivity is limited by their scheduling time and within the region covered by the bus routes. Unlike MIBR, it uses vehicles such as taxis as mobile gateways.TheIEEE802.11interface is used for IVC with nearby vehicles that do not have a 3G interface or vehicles that are not mobile gateways.

Figure 3.2 illustrates the basic architecture of MGRP. Upon receiving packet from the IEEE802.11interface, mobile gateways forward the packet to the base station via the3G interface .In turn; the base station forwards the packets to the gateway controller.

The gate way controller finds the position of the destination vehicle and forwards the packet to each of the mobile gateways that are closest to the destination vehicle via the base station. Upon receiving a packet from the gateway controller, mobile gateways forward the packet to the destination vehicle by using the IEEE 802.11 interface.

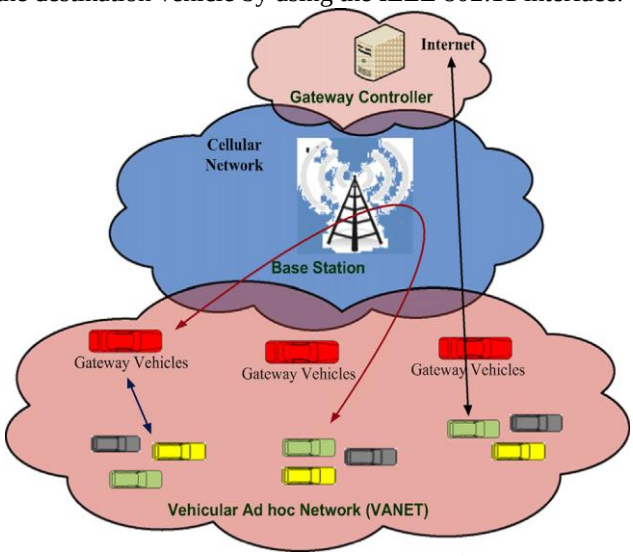


Figure 6.1 Mobile gateway architecture of MGRP

7. NOTATIONS

The notations are describe our proposed scheme given in Table 1. The public key of the base stationis K_{BS} = xG, where xG = G + G + . . . + G(x times) is called the elliptic curve scalar multiplication in an elliptic curve $E_p(a, b)$, which is the set of all points of $y^2 = x^3 + ax + b(\text{mod } p)$ such that a, b 2 Z_p = {0, 1, 2, . . ., p _ 1} are constants with $4a^3 + 27b^2$ „ 0(mod p). If nG = O, where O the point at infin-ity or zero point. Then O is called the order of the base point G in $E_p(a, b)$ (Koblitz, 1987). Here x is the private key of the base station. An example of a one-way hash function is SHA-1 (Se-cure Hash Standard, 1995), which has the above desired prop-erties (i) to (vi). However, National Institute of Standards and Technology (NIST) does not recommend SHA-1 for top secret documents. Further, in 2011, Manuel showed collision attacks on SHA-1 (Manuel, 2011). As in Das (2012, 2013) one can also use the recently proposed one-way hash function, Quark

Table 1 Notations used in the proposed scheme.

Symbol	Description
SN_i	Identifier of sensor node i
U_j	jth user
BS	Base station
PW_j	Password of user U_j
$^{G}id_j$	Group id of user U_j
APM_j	Access privilege mask of user U_j
	Private key of base station
^{K}BS	Public key of base station
$^{MK}S_i$	Master key of sensor node SN_i
$^{RM}u_j$	Random number for user U_j
K_i	Secret key of node SN_i shared with BS
H(Æ)	Secure one-way collision-resistant hash function
^{T}i	Bootstrapping time for node SN_i
AiB	Data A concatenates with data B
$E_K(M)$	Symmetric encryption using the key K
$D_K(M)$	Symmetric decryption using the key K
X fi Y:M	Entity X sends message M to entity Y

(Aumasson et al., 2010). Quark is a family of cryptographic hash functions which is designed for extremely resource-con-strained environments like sensor networks and radio-fre-quency identification (RFID) tags. Like most one-way hash functions, Quark can be used as a pseudo-random function (PRF), a message authentication code (MAC), a pseudo-ran-dom number generator (PRNG), a key derivation function, etc. Quark is shown to be a much efficient hash function than SHA-1. However, in this paper, as in Das et al. (2013) we use SHA-2 as the secure one-way hash function in order to achieve top security. We may use only 160-bits from the hash digest output of SHA-2.

7.1 DIFFERENT PHASES

This section discusses our proposed user access control scheme. Our scheme consists of the following phases: pre-deployment, post-deployment, registration, login, authentica-tion, password change and dynamic node addition. These phases are described in the following subsections.

7.1.1. PRE-DEPLOYMENT PHASE

This phase is used to preload the keying materials to all sensor nodes prior to their deployment. It is performed offline by the (key) setup server. The setup server in our scheme is the base station (the medical server). This phase is implemented offline by the base station prior to the deployment of sensor nodes on a patient's body (target field). The pre-deployment phase con-sists of the following steps:

Step P1: The base station selects a set of network parame-ters from the following: a finite field GF(p) where p is a large odd prime of at least 160 bits; an elliptic curve $E_p(a, b)$ that is the set of all points of $y^2 = x^3 + ax + b(\text{mod } p)$ such that

a, 3 b 2 $_2^Z$p = {0, 1, 2, . . ., p _ 1} are constants with 4a + 27b „ 0 (mod p); and a base point G in $E_p(a, b)$ whose p order is n, where n is at least 160 bits such that n > 4pffiffiffi. The base station first selects a random number as its own pri-vate key x 2 Z^-_n where Z^-_n ¼ f1; 2; . . . ; n _ 1g. The base sta-tion then computes its public key K_{BS} = xG.

Depending on the probable user query, the base station prepares the group-based user access privilege mask (APM) and prepares an access list consisting of the access privilege mask and the respective access group identity G_{id}. For each deployed sensor node SN_i, the base station assigns a unique identifier SN_i. The base station also assigns a unique randomly generated master key MK_{Si} for each deployed sensor node SN_i, which is only shared with the base station. The base station computes $x_iG = (x_1, y_1)$ for each sensor node SN_i where x_i is the private key for sensor node SN_i, which is known to the BS. The base station then computes the secret key $K_i = x_1$ (mod p) for each sensor node SN_i. For security, p is considered as a 160-bit number for ECC. Note that K_i is also a 160-bit number. However, to use K_i as the secret key for symmetric key encryption (for example, Advanced Encryption Standard (AES) (Advanced Encryption Standard, 2001)), we can only use 128 bits from the 160 bits of K_i.

Step P2: Once the set of network parameters are selected, the base station (BS) loads the following information into the memory of each sensor node SN_i prior to its deployment in offline: (i) a unique node identifier SN_i; (ii) the elliptic curve $E_p(a, b)$; (iii) the base point G; (iv) the secret key K_i with x_i; (v) the base station's public key K_{BS}; (vi) a secure one-way hash function H(Æ); and (vii) its own master key MK_{Si} .

7.1.2 POST-DEPLOYMENT PHASE

This phase helps the sensor nodes and the base station to establish secure connections between them. As soon as sensor nodes are deployed, their first task is to locate physical neigh-bors within their communication ranges. For secure communi-cation between sensor nodes, the nodes must establish pairwise secret keys between them. Because the major focus in this pa-per is addressing the user access control problem, we assume that nodes in a WBAN can establish secret keys by using exist-ing key establishment schemes.

For example, we can use an unconditionally secure key establishment scheme (Das AK, 2009) for pairwise key establishment between nodes in each cluster. Because our primary focus is on how authorized users belonging to different groups (doctors, nurses, medical insur-ance team, patient parties, etc.) can access the real-time data for monitoring a patient's condition from the sensors inside the WBAN, we require secure communication between the sensor nodes and the authorized users.Once deployed, each sensor node sends a message with its node identity SN_i, bootstrapping time T_i, and encrypted infor-mation containing K_i, SN_i and T_i to the base station:

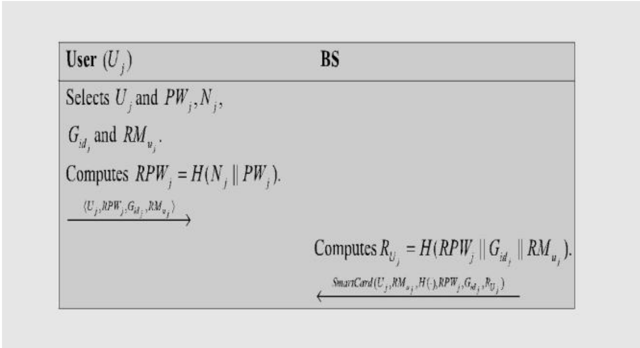
SN_i ! BS : hSN_i; T_i; E_{MKSi} ðK_i; SN_i; T_iÞi

After receiving the message from the sensor node SN_i, the BS decrypts E_{MKSi} (K_i, SN_i, T_i) with the master key MK_{Si} of SN_i, and then checks the validity of the received information K_i, SN_i, and T_i. Note that T_i is the bootstrapping time of the sen-sor node SN_i. The BS further checks if jT_i _ T^-_ij < DT_i, where T^-_i is the current system timestamp of the BS and DT_i is the ex-pected time interval for the transmission delay. If the check holds, then the BS stores $K_i$and T_i for the sensor node SN_i.

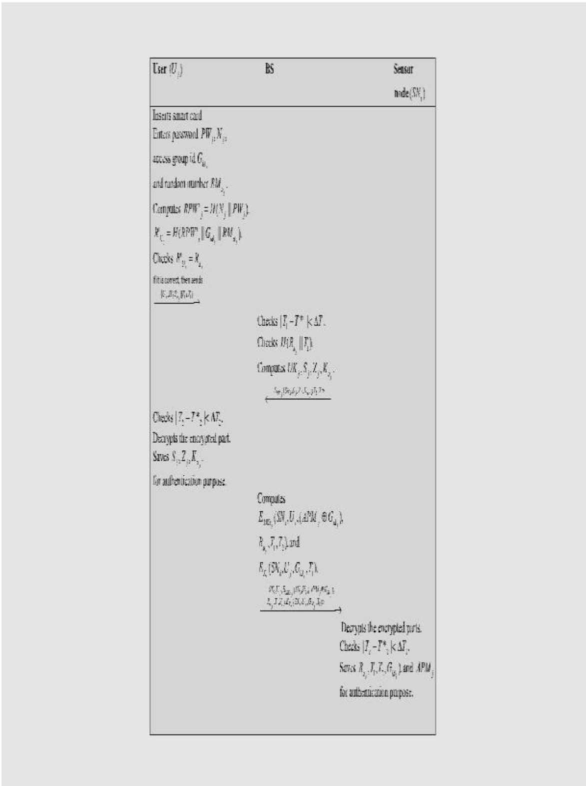
7.1.3 REGISTRATION PHASE

In the registration phase, a user U_j must register with the base station to access the real-time data from a specific sensor node in a WBAN. This phase consists of the following steps:

Step R1: The user selects his/her identity U_j, a password PW_j, his/her access group ID G_{idj} (depending on his/her access privilege), and a random number RM_{uj}. U_j generates another secret random secret value N_j that is kept secret to U_j only.



7.1.4 LOGIN PHASE



7.1.5 Authentication phase

8. CONCLUSION

It simulate that, it describes data forwarding steps from the patient end to the care giver's end i.e., hospital, where the patients' health records are monitored and maintained. That also achieves different security and privacy requirements. The fairness among all cooperative participants in our system is guaranteed by adopting proper incentive and reputation policies. These policies also improve the network performance in terms of high delivery ratio and low average delay. Through extensive security and performance analysis, it has been proven that the patients can be monitored remotely, even though they reside out of their living area while travelling. In future the patients can be monitored not only through adhoc and WBAN networks; they can be directly monitored through GPS devices. The fast blooming technology, Internet of Things can adopt our simulation to make the patients' monitoring through embedding the sensors into the patients' body, by proving the technology of monitoring the patients through the pervasive computing, ubiquitously.

REFERENCES

(1) AkyildiIF et al, (2010) The evolution to 4G cellular systems: LTE Advanced Physical Communication; 3, pp. 217–44.
(2) Alemdar.H and Ersoy. C, (2010) Wireless sensor networks for healthcare: a survey. Computer Networks 54 (15), 2688–2710.
(3) Ameen.M et al, (2012) Security and privacy issues in wireless sensor networks for healthcare applications. Journal of Medical Systems 36 (1), 93–101.
(4) Baraa RAA SharefT et al, (2013) A comparison of various vehicular adhoc routing protocols based on communication environments. In: Proceedings of the 7th international conference on ubiquitous information management and communication. Kota Kinabalu, Malaysia; pp.17– 19.
(5) BaraaT.Share et al, (2014) "Vehicular communication adhoc routing protocols: A survey" Journal of Network and Computer Applications 40, pp: 363–396.
(6) BronstedJ and KristensenLM, (2012) Specification and performance evaluation of two zone dissemination protocols for vehicular ad-hoc networks. In: Proceedings of the 39th annualsymposiumonsimulation;pp.6879.jsp?tp=&arnumber=6357181
(7) Ding Y et al, (2007) A static-node assisted adaptive routing protocol in vehicular networks. In Proceedings of the 4th ACM international workshop on vehicular adhoc networks; pp.59–68.
(8) FonsecaA and VazãoT, (2013) Applicability of positionbased routing for vanet in highways and urban environment. Journal of Network and Computer Applications 36: pp.961–73.
(9) Junhai L et al, (2009). A survey of multicast routing protocols for mobile ad-hoc networks. IEEE Communications Surveys and Tutorials ;11: pp.78–91
(10) Santanu Chatterjee et al, (2014) "A novel and efficient user access control scheme for wireless body area sensor networks" Journal of King Saud University – Computer and Information Sciences 26, pp.81–201.