IJCTA, 8(5), 2015, pp. 2127-2135
© International Science Press

PBSCHCMA: A Priority Based Secure Clustering Health Care Monitoring Algorithm for Body Area Networks

V. Sethupathi* and E. George Dharma Prakash Raj**

Abstract: The Wireless Body Area Network (WBAN) has arisen as a new upcoming technology for e-healthcare that allows the medical data of a patient's significant body parameters to be collected by using wearable sensors and transmit using tiny-range wireless communication techniques. It improves the quality of healthcare, and has found a wide range of applications from health monitoring and computer assisted rehabilitation to emergency medical response systems. But WBAN makes it inevitable suffer from many kinds of attacks unable the safeguard medical data with privacy in transmission and storage. In this paper, we propose a new algorithm PBSCHCMA by using Elliptic Curve Cryptography (ECC), to safeguard the medical data during transmission. Experimentation and Analysis shows better results to PBSCHCMA compared to other algorithm.

Index Terms: Wireless Body Area Network;Elliptic Curve Cryptography; Message Authentication Code; Clustering; Security; Health Care; Sensor; Network.

1. INTRODUCTION

People are having busy schedule in their everyday life. They don't have enough time to monitor their health periodically. This struggle can be overcome by WBAN. WBAN uses sensor networks. These sensors can be implanted into a human body. Using this, the particular person health can be monitored periodically. This regular medical information can be collected from sensor and can be transmitted to the medical server. This WBAN approach is used in hospitals. If any abnormalities happen for the person, proper action can be taken to come out from abnormalities.

There are three components (i) WBAN, (ii) An external network, (iii) Back-end-server. The WBAN contains several sensor. These sensors are connected using radio interface. Sensors collect information and it is sent to Medical Hub. External network provides a connection between Medical Hub and back-end server. The back-end server receives data from external network and collects, store, process and manages it.

WBAN has to the following security requirements [1]

- Confidentiality: To protect the sensed data and exchanging of information between sensors nodes, it is important to maintain the secrecy of messages.
- Integrity and Authentication: Integrity and authentication is very important to enable sensor nodes to detect, modified and injected packets.
- Availability: the deployment of sensor network, keeping the network available for its future use is essential. The attacks like denial-of-service (DoS) that aim at bringing down the network itself may have serious consequences to the health and wellbeing of people.
- Data freshness: It is necessary to detect replayed packets.

* Research Scholar,

** Assistant Professor, School of Computer Science, Engineering and Applications, Bharathidasan University, Trichy.

To overcome the security requirements we propose a Priority Based Secure Clustering Health Care Monitoring Algorithm for Body Area Networks algorithm that provides authentication and integrity using symmetric key cryptography and Hash based Message Authentication Code (HMAC). Elliptic curve cryptography is used to generate the secret key.

Elliptical Curve Cryptography (ECC) [2] is a public key encryption technique based on elliptic curve theory that can be used to create more efficient, smaller and faster cryptographic keys. The technology can be used in concomitant with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC algorithm can yield a level of security with a 164-bit key that other systems need a 1,024-bit key [3] to achieve. Because ECC helps to establish equivalent security with lower battery resource usage and computing power, it is becoming widely used for mobile applications.

Hash-based Message Authentication Code (HMAC) is an exact construction for calculating a message authentication code (MAC) involves a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the integrity and the authenticity of a message.

This paper proposes a Security Algorithm called as “PBSCHCMA: A Priority Based Secured Clustering Health Care Monitoring Algorithm” based on Elliptic Curve Cryptography (ECC) and Hash based Message Authentication Code (HMAC) to safeguard patient’s medical information in a WBAN Environment.

The organization of the paper is as follows. The related work is presented in Section II. The proposed work is given in Section III. Experimentation and Analysis are presented in Section IV and finally Conclusion is given in Section V.

2. RELATED WORK

Medical models for wearable and implantable Human Healthcare Monitoring sensors has been made recently. These devices are used to monitor human body over a long periods of time [4, 5]. Most of the work concerns have biocompatibility, power-efficiency, and reliability. Therefore, safeguarding the security is important in the communication among these devices [6, 7].With respect to BAN variety of security algorithm has been proposed by different authors. Theoretically, Traditional Public Key Cryptosystem (TPKC) can be only used for authentication purpose in WBAN. TPKC contains ElGamal algorithm and RSA algorithm. The concept of ECC was first introduced by Ounasser [8] and Koblitz [9] separately. Compared with TPKC, ECC could provide good performance because of smaller key size at similar security level.

Jingwei Liu and Kyung Sup Kwak [10] proposed a feasible hybrid security mechanism to meet the security requirements of WBANs with stringent resource constrains. They also discussed the security issues of WBANs and also evaluated the main security risks in the recent advances of WBANs. It helped WBANs against attacks when compared to other networks without resource constraints and the security requirement of WBANs. They proposed a hybrid security structure for the existing cryptographic algorithm. A unique to develop secure and efficient WBAN systems are existing in the proposed security mechanism.

Chiu C.Tan et al. [11] has developed IBE-Lite, a lightweight identity-based encryption technique. It is suitable for sensors in a BSN. They proposed a protocols based on IBE-Lite. It has to be balance the security and privacy with accessibility. In performance evaluation experiments existing sensors were used. Masahiro Kuroda et al. [12] have proposed a secure body area network. It can be commercially employed with reduced computational problem on a real sensor. These sensors have limited RAM/ROM sizes and CPU/RF power consumption under a light-weight battery. The vital data ordering among the sensors in the S-BAN are provided by the proposed S-BAN. It also provides low networking with zero administration security with private key generation. The efficient media access control (MAC) is developed and implemented with resource-constraint security in sensors.

Y. M. Huang et al. [13] have proposed a healthcare monitoring coupled with wearable sensor systems and an environmental sensor network. It has used for monitoring chronic patients in their own place. The wearable sensor system consists of various medical sensors. The proposed network architecture implements three application scenarios. The use of ad hoc mode for the group-based data collection and data transmission promotes the outpatient healthcare services as only one medical staff is assigned to a set of patients. They also performed the adaptive security issues for the data transmission based on different wireless capabilities. They also presented a prototype for monitoring application and capturing sensor data from wireless sensor nodes.

Cluster Head can be selected by using several technique. In [14] CH has chosen on the basis of node ID. In [15] a cluster-based protocol can use the randomized rotation of local CHs to distribute evenly in the energy load among the sensors. In [16] optimal CH selection is done by multi-objective particle swarm optimization. The above mentioned approaches cannot consider security of the techniques that are used for cluster formation. In WBANs, the above mentioned techniques are very expensive and complex due to limited resources of the nodes in WBANs. The author has proposed a secure cluster formation scheme. It is based on MicroTesla protocol. This protocol uses pre-deployment and public-key cryptography which is expensive in WBANs. The scheme proposed in this paper presents a cluster-based secure approach to choose an optimal CH on the basis of residual energy and distance of nodes present in WBANs.

3. PROPOSED WORK

The proposed work is Priority based Clustering Security Authentication Mechanism which provides security in WBAN. The proposed architecture is given in Figure 1. This architecture contains implanted sensors in Human body which sensor form a cluster. The cluster contains one cluster head. Each sensor is used to collect individual medical data continuously with the help of sensing nodes into the human body through wireless channel. The collected information is sent through cluster head to Local Body Area Network Gateway (LBANG), where Elliptic Curve Cryptography key generation algorithm and Hash based Message Authentication Code (HMAC) are used, then it is sent to Centralized Data Center (CDC). Authentication is checked in CDC. If it is an authenticated message, then update the information in CDC, otherwise the message is discarded. CDC transmits the information Priority based Health Care System (PHCS). In PHCS after verifying authentication the encrypted data will be updated in CDC, decryption takes place using shared key of ECC. The PHCS consist of Emergency Unit (EU), physician, Telemedicine Server (TS) and Primary Care Unit (PCU) and it monitors the patient and takes necessary action based on the sensing value condition.

The Patient health condition is monitored based on the three priorities Normal, Average, and Abnormal respectively. In the proposed PBSCHCMA, the physician has to monitor the patient and take necessary action

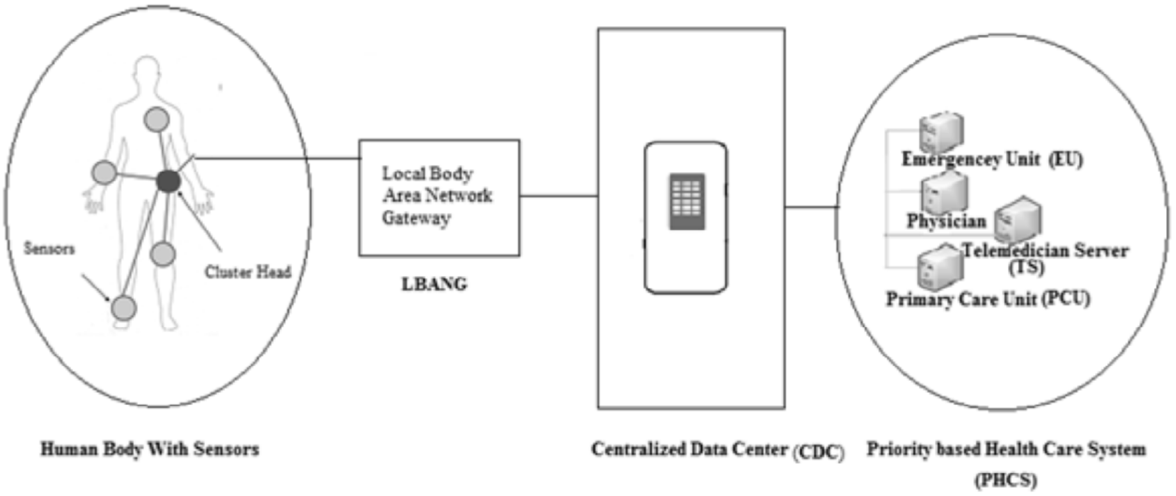

Figure 1: Priority Based Clustering Security Authentication Mechanism

based on the sensing value condition as follows. If Condition 1: Normal, the Physician takes No action. If Condition 2: Average, then the Physician sends the medical prescription to the patient before that relevant information updated in Telemedicine Server. If Condition 3: Abnormal, the Physician sends patient's medical data to the Emergency unit and Primary care unit will take the necessary action to handle the critical situation.

The PBSCHCMA Algorithm is given below

```
Step 1:   Data collecting from all sensors from the body ($d1$, $d2$,…., $dn$)
Step 2:   The aggregate data (D) send to LBANG through Cluster Head.
Step 3:   In LBAN apply Encryption based on ECC generated secret key using Symmetric cryptography
          E (D)
Step 4:   After Encryption to apply MAC [(E (D)]
Step 5:   MAC [E (D)] transmit to CDC
Step 6:   CDC check
          If (MAC = key)
          go to Step 8
          else
          continue
Step 7:   Discard the data and go to step 13.
Step 8:   Store the information in CDC.
Step 9:   Updated data Transmit D [E (D)] to PHCS
Step 10:  Decryption of D [E (D)] = D
Step 11:  Priority check
              i.   If Normal go to Step 10
             ii.   If Average go to Step 11
            iii.   If Abnormal go to Step 12
Step 10:  No action, update the data to server
Step 11:  Issue the medical prescription
Step 12:  Send Emergency Care Unit and PrimaryUnit.
Step 13:  Stop.
```

3.1. Cluster formation

The local sensors are placed in different parts of the human body and it acts as a cluster. Clustering is a combination of physical network nodes into a small number of logical assemblies and keeping them whiles the network operation. The logical assemblies are named as clusters. For the initial formation of clusters, each and every node performs a cluster formation protocol. If each cluster needs a head, nodes in each cluster should perform a head election protocol. Hereafter, we call the head as cluster head. Since a cluster head plays a vital role such as gathering sensed data from every nodes and transmits the gathered data to the Local Body Area Gateway, and it maintains a table like <CH_{id}, P_{id}>. Each patient information can be identify using the unique P_{id}. P_{id} is related to the patients data so that the source of the data can be identified

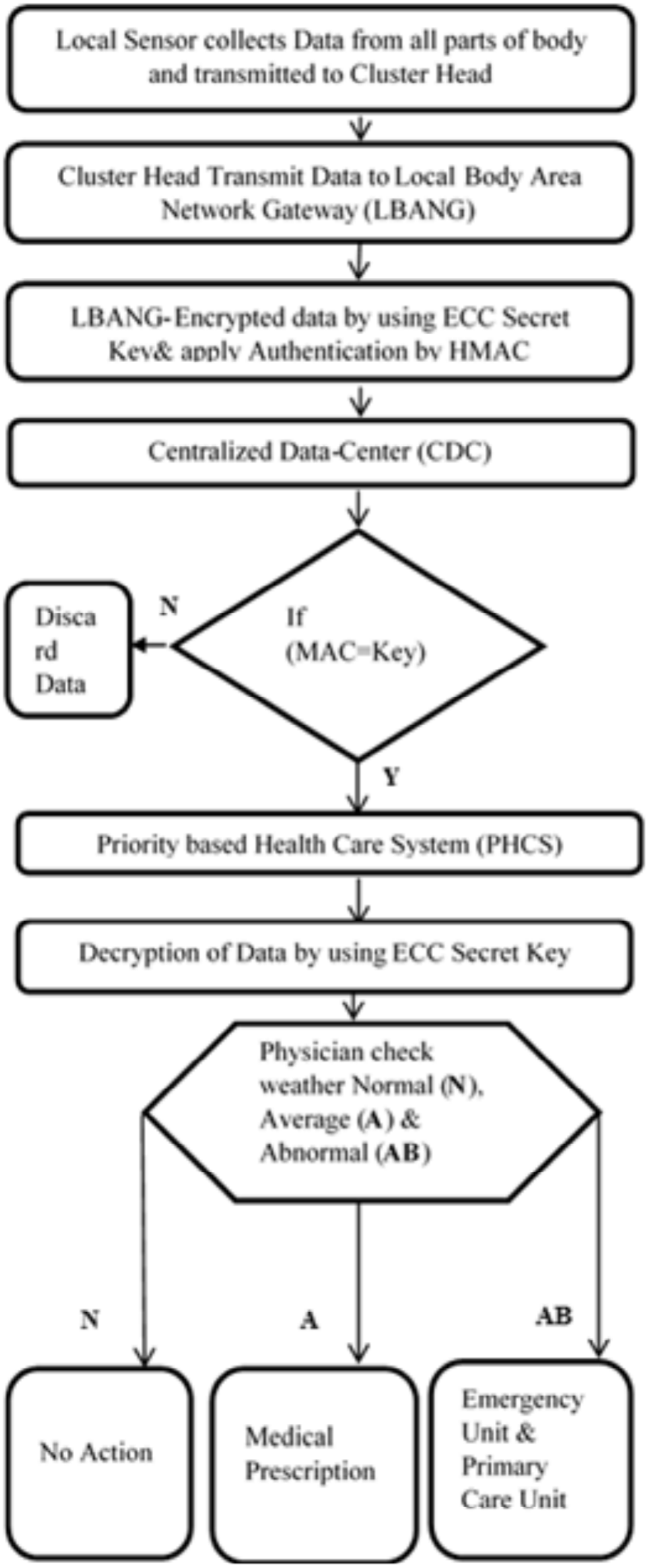
Local Sensor collects Data from all parts of body and transmitted to Cluster Head
Cluster Head Transmit Data to Local Body Area Network Gateway (LBANG)
LBANG-Encrypted data by using ECC Secret Key& apply Authentication by HMAC
Centralized Data-Center (CDC)
If (MAC=Key)
N
Discard Data
Y
Priority based Health Care System (PHCS)
Decryption of Data by using ECC Secret Key
Physician check weather Normal (N), Average (A) & Abnormal (AB)
N
A
AB
No Action
Medical Prescription
Emergency Unit & Primary Care Unit

Figure 2: Workflow of the Algorithm

The PBSCHCMA Algorithm Workflow is given below as a Flow Diagram in Figure-2.

3.2. Generation of public key using ECC

In LBANG a master secret key is generated using elliptic curve C. We take the base point of C as L r as the order of L. The generates 'n' secret keys $k1$, $k2,\ldots,$ kn in order to generate the master secret key.

$$K = k1,\ k2 \ldots kn$$

The 'n' public keys are then generated to make up the master public key

$$Puk = Pu1,\ Pu2 \ldots Pun$$

3.3. Encryption using ECC

In Local Body Area Gateway key encryption has been take place. Encryption has been done by using Elliptic curve cryptography with the help of symmetric key encryption technique. Using this technique encrypted key has been shared by both sender and receiver.

$$\text{Encryption} = E\ (\text{Key} \,\|\, \text{Data})$$

3.4. Message Authentication

Hash-based Message Authentication Code (HMAC) is an exact construction for calculating a message authentication code (MAC) involves a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the integrity and the authenticity of a message. Any cryptographic hash function, such as SHA-1, and it may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-SHA1 consequently. The strength of the cryptographic is depends upon HMAC underlying the hash function, the size of its hash output length in bits, the size and quality of the cryptographic key.

$$\text{MAC} = \text{H}\ (\text{key} \,\|\, \text{message} \,\|\, \text{key})$$

3.5. Decryption using ECC

Decryption takes place in Priority based Health Care System by using the ECC generated secret key. After decryption of message we will get an original data.

$$\text{Decryption} = \text{D}\ (\text{E}\ (\text{Key} \,\|\, \text{Message}))$$

4. EXPERIMENTATION AND ANALYSIS

The performance of the proposed work is evaluated using NS-2 [17].The Simulation Parameters are given in Table 1.

Table 1
Simulation Parameters

No. of Node	*10*
Area Size	500 × 500
Mac	IEEE 802.15.6
Simulation Time	25 sec
Transmission Range	25m
No. of Keys	50, 100, 150, 200, 250
Traffic Source	Exponential
Packet Size	250-1000 bytes

The Performance of the proposed Priority Based Secure Clustering Health Care Monitoring Algorithm (PBSCHCMA) is compared with A Secure Priority Based Health Care Monitoring Algorithm (SPBHCMA) [18] and Light Weight Security Architecture (LSA) [19], using the following metrics.

1. End to End Delay: The difference between the time at which the sender generated the packet and the time at which the receiver received the packet.

   From figure 3 it is evident that the proposed PBSCHCMA algorithm performs well in measuring the delay when compared with the exiting algorithms. This result is achieved since the clustering and HMAC technique is used in PBSCHCMA.

2. Packet Delivery Ratio (PDR): The calculation of Packet Delivery Ratio is based on received packet over sent packet in the channel.

   From figure 4 it is evident that the proposed PBSCHCMA algorithm performs well in measuring the Packet Delivery Ratio when compared with the exiting algorithms.This result is achieved since the clustering and HMAC technique is used in PBSCHCMA.

3. Throughput: The amount of successful delivery of data over a channel in a unit time and it is represented in bps.

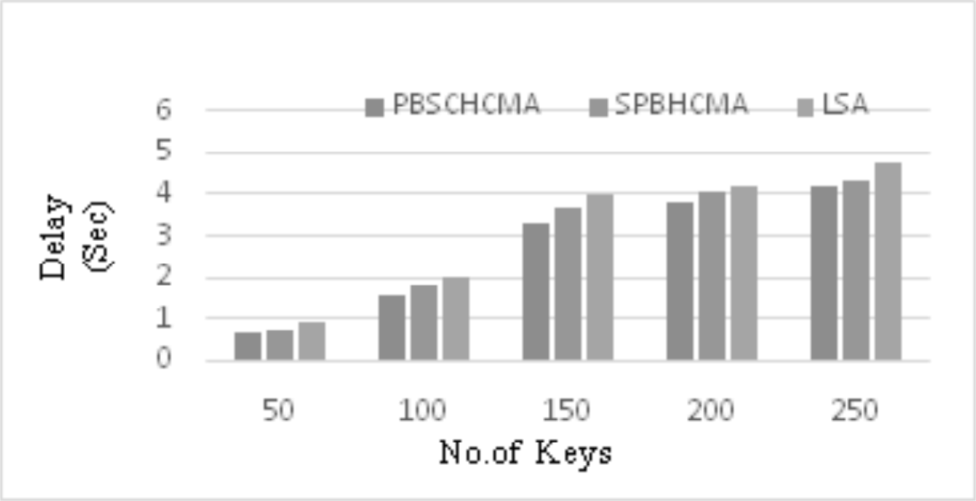

Figure 3: No. of Keys vs. End to End Delay

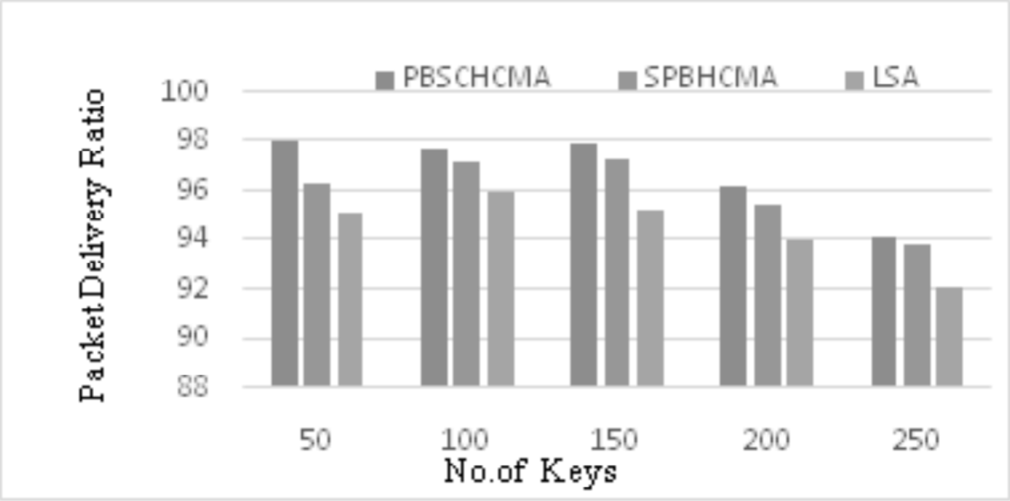

Figure 4: No. of Keys vs. Packet Delivery Ratio

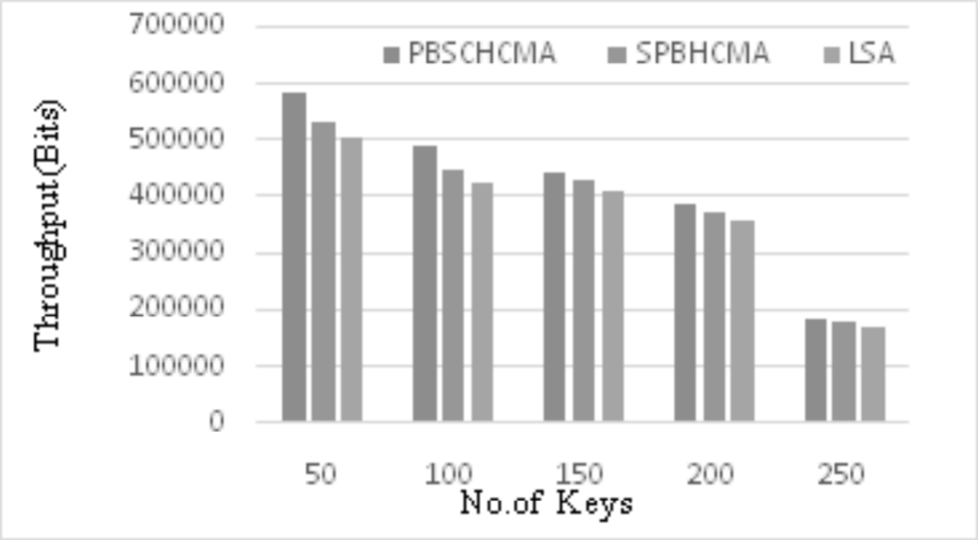

Figure 5: No. of Keys vs. Throughput

From figure 3 it is also evident that the proposed PBSCHCMA algorithm performs well in measuring the throughput when compared with the exiting algorithms.This result is achieved since the clustering and HMAC technique is used in PBSCHCMA.

Generally, manyQoS parameters are used to measure the performance of algorithms. In our proposed work, delay, throughput and Packet Delivery Ratio are considered for measuring the security level. This algorithm reduce the delay and increase the throughput and packet delivery ratio with minimum no of key length compare with SPBHCMA and LSA.

5. CONCLUSION

In this paper, the PBSCHCMA: A Priority Based Secured Clustering Health Care Monitoring Algorithm" based on Elliptic Curve Cryptography (ECC) and Hash based Message Authentication Code (HMAC) to safeguard patient's medical information is proposed. This Algorithm used the symmetric cipher algorithms to encrypt or decrypt medical data and then use ECC to handle the key's distribution, update and revocation. In the future work, the issues related to the proposed PBSCHCMA will be strengthened and will be proposed as an Enhanced Algorithm.

References

[1] TassosDimitriou, KrontirisIoannis, "Security Issues in Biomedical Wireless Sensor Network", Applied Sciences on Biomedical and Communication Technologies, 2008.

[2] Miller, V. S., "Use of elliptic curves in cryptography. In: Advances in cryptology", proceedings of CRYPTO'85, 417–26, 1986.

[3] Jinfang Jiang, Guangjie Han, Chuan Zhu, Yuhui Dong, Na Zhang, "Secure Localization in Wireless SensorNetworks: A Survey". Journal of Communications, Vol. 6(6), September 2011.

[4] Media Aminianand Hamid Reza Naji, "A Hospital Healthcare Monitoring System Using Wireless Sensor Networks", in Aminian and Naji, J Health Med Inform, 2013.

[5] A Darwish, AE Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring", Sensors. Vol. 11, pp. 5561–5595, 2011.

[6] P Kumar, HJ Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey", Sensors. Vol. 12 (1), pp. 55–91, 2012.

[7] G Selimis, L Huang, F Massé, I Tsekoura, M Ashouei, F Catthoor, J Huisken, JStuyt, G Dolmans, J Penders, H De Groot, "A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design", J. Med. Syst. 35, pp. 289–1298,2011.

[8] OunasserAbid, JaouadEttanfouhi and Omar Khadir, "New Digital Signature Protocol Based On Elliptic Curves", International Journal on Cryptography and Information Security (IJCIS), Vol. 2 (4), December, 2012.

[9] Koblitz, N., "Elliptic curve cryptosystem," Math. Comput. Vol., 48, pp. 203–209, 1987.

[10] Jingwei Liu, Kyung Sup Kwak, "Hybrid Security Mechanisms for Wireless Body Area Networks", Second International Conference on Ubiquitous and Future Networks (ICUFN), pp. 98-103, 2010.

[11] Chiu C. Tan, Haodong Wang, Sheng Zhong, and QunLi,"IBE-Lite: "A Lightweight Identity-Based Cryptography for Body Sensor Networks", IEEE Transactions On Information Technology In Biomedicine, Vol. 13(6), pp. 926-932, Nov. 2009.

[12] Masahiro Kuroda, ShuyeQiu, and Osamu Tochikubo, "Low-power Secure Body Area Network for Vital Sensors toward IEEE802.15.6", 31st Annual International Conference of the IEEE EMBS, pp. 2442-2445, Sept 2009.

[13] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J.H. Park, "Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks", IEEE Journal On Selected Areas In Communications, Vol. 27(4), pp. 400-411, May 2009.

[14] Amit Kumar, DhirendraSrivastav and SuchismitaChinara, "Simulator for Energy Efficient Clustering in Mobile Ad Hoc Networks", David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 191–198, 2012.

[15] WR Heinzelman, A Chandrakasan, H Balakrishnan, "An application –specific protocol architecture for wireless microsensor networks", IEEE Trans. Wireless Commun. Vol. 1(4), pp. 660–670, 2002.

[16] H Ali, W Shahzad, FA Khan, "Energy-efficient clustering in mobile ad hoc networks using multi-objective particle swarm optimization", Appl. Soft Comput. Vol. 12 (7), pp. 1913–1928 2012.

[17] NingGu, Young Jiang, Jun Zhang, Hai-taoZheng, "An implementation of WBAN module Based on NS-2", IEEE Computer society International conference on Computer science and Application, 2013.

[18] V.Sethupathi, E. George Dharma Prakash Raj, "SPBHCMA: A Secure Priority Based Health Care Monitoring Algorithm for Body Area Networks", International Journal of Applied Engineering Research (IJAER), Vol. 10 (82), pp. 168-172, 2015.

[19] K.T. MeenaAbarna and K.Venkatachalapathy, "Light-weight Security Architecture for IEEE 802.15.4 Body Area Networks", In International Journal of ComputerApplications Vol. 47 (22), pp. 0975–8887June 2012.