International Journal of Computer Science and Software Engineering (IJCSSE), Volume 6, Issue 4, April 2017
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 89-93

A Framework for Secure Human Healthcare Monitoring Mechanism in Wireless Body Area Networks

V. Sethupathi[1] and E. George Dharma Prakash Raj[2]

[1] Research Scholar, School of Computer Science, Engineering and Application, Bharathidasan University, Trichy, Tamilnadu, India.

[2] Assistant Professor, School of Computer Science, Engineering and Applications, Bharathidasan University, Trichy, Tamilnadu, India.

[1]gsethupathivenugopal@gmail.com, [2]georgeprakashraj@yahoo.com

ABSTRACT

Environment of next generation purely depends on various sensors and devices .Wireless Body Area Network (WBAN) is a technology that can be used in Health Care Monitoring system. Nowadays, many researchers in computer science are focusing towards Healthcare Services and there are various issues that have been raised in WBAN. WBAN is a dynamic network with many sensor nodes in and around the human body, which the doctors can used to monitor the patient's physical status. Here patient's medical data can be transmitted through wireless channel, during this transmission of data, there is opportunity for security vulnerability .In this paper, a security framework model is proposed. This framework model can be used to protect the patient's private healthcare data. This turn as a guide for providing security and privacy protection in WBAN.

Keywords: *Healthcare, Wireless Body Area Network, Security, Framework.*

1. INTRODUCTION

Rapid advancement of wireless communication technology in the area of sensor network supports several applications including medical and health care system. In WBAN, many sensor networks have been designed and the desired network can be connected to medical sensors, which is located inside and outside of human body [1, 2, 3, and 4]. WBAN is a flexible and cost consuming application with both health care professionals and patients. It has two significant advantages. The First one is it is portable and second is it is independent monitoring.

WBAN initiates the communication network, for transmitting and storing the health related data of a patient, to the remote database. With the help of the data, the decision for treatment shall be taken by external health care professionals. Now, here the major challenge is, WBAN's security [5, 6, 7 and 8]. In this paper, the vulnerability of security is studied and proposed a new security framework in WBAN.

This paper is structured as follows; Section II - discusses Security Threats in WBAN, Section III - discusses classification of security algorithms in WBAN, Section IV- discusses the framework, Section IV- Advantage of Secure Human Healthcare Monitoring framework for society and Section V- concludes the paper.

2. SECURITY THREATS IN WBAN

Security is the most important part of WBAN [9], because the information transmission through wireless media should be confidential. Various Security Threats in WBAN are:

- 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 well-being of people.
- Data freshness: It is necessary to detect replayed packets.

3. SECURITY ALGORITHMS IN WBAN

There are four security algorithms that have been proposed by this author earlier. This section gives a brief working of all the algorithm. The security threats can be cleared by

using the proposed algorithms and it is based on cryptography method. The existing method has two types 1.symmetric key based algorithm, 2.asymmetric key based algorithm. Based on the two key based algorithms, the following algorithms have been proposed. The four proposed algorithms are discussed below.

A. A Secured Priority Based Health Care Monitoring Algorithm for Body Area Network: (SPBHCMA) :

A WBAN's priority based security authentication mechanism provides security in a prioritized manner. The proposed [10] architecture in which a Wearable Medical Device (WMD) is used to collect individual's Medical data continuously with the help of sensing node inserted into human body through wireless communication channel. The collected information is transferred to Centralized Data-Center (CDC) through personalized network. Finally, this information is sent to a Priority based Health Care System (PHCS). The PHCS consist of Emergency Center (EC), Physician, Telemedicine Server (TS) and Primary Care provider (PCP).

The Proposed SPBHCMA Algorithm

Step 1: Data collecting from all parts of body (D)
Step2: Encryption based on Symmetric cryptography (AES (E (D)) ECC generated key
Step 3: After Encryption to apply MAC ((E (D))
Step 4: (MAC (E (D)) transmit to CDC
Step 5: CDC verify authentication
If Authentication success
go to Step 8
else
continue
Step 6: Discard the data
Step 7: Store (E(D)) the information in CDC
Step 8: PHCS Decryption of D [E (D)] = D
Step 9: Priority check based on the value of D
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 unit & Primary unit

In this algorithm, the sensor node in the human body collects the information individually, it is found from the experimentation that the energy requirement is high. To overcome this issue, the Secured Priority Based Health Care Monitoring Algorithm for Body Area Network is enhanced by forming the cluster.

B. A Priority Based Secure Clustering Health Care Monitoring Algorithm for Body Area Networks (PBSCHCMA):

The priority based clustering security authentication mechanism uses secure clusters which provides security. The proposed [11] algorithm works as follows: 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.

The PBSCHCMA Algorithm:

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 key using Symmetric cryptography (AES (E (D)).
Step 4: After Encryption to apply MAC [(E (D)]
Step 5: MAC [E (D)] transmit to CDC
Step 6: CDC check Authentication
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 Primary Unit.
Step 13: Stop.

If it is an authenticated message, then the information in CDC is updated, otherwise the message is discarded. CDC transmits the information with a Priority based Health Care System (PHCS). In PHCS after verifying authentication the encrypted data will be updated in CDC and 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.

Both proposed algorithms SPBHCMA and PBSCHCMA are under the In-Station Security. But the patient may be at Out-Station. So there is need to provide outstation security too. Further, the Priority Based Secure Clustering Health Care Monitoring Algorithm for Body Area Networks is enhanced with multilevel authentication by generating One Time Password.

C. A Enhanced Secure Health Care Monitoring Algorithm using One-Time Password in Wireless Body Area Networks (ESHMA):

In the proposed [12] algorithm, the server generates a Dynamic OTP (DOTP). This DOTP is encrypted with Elliptic Curve Cryptography (ECC) key and is sent to the user device. The DOTP verifies the authentication server whether the correct Authentication has been accessed after the user decrypts it. Then the user permitted to access the data otherwise denied.

The ESHMA Algorithm pseudo code for dynamic OTP generation is given below:

Step 1: ***procedure*** *One-Time Dynamic Auth (D_{OTPS})*
Step 2: Encryption (E) ← (D_{OTPS} || ECC (k));
Step 3: send (E (D_{OTPS} || ECC (k)), receiver);
Step 4: Decryption ←D (E (D_{OTPS} || ECC (k)));
Step 5: res ← Receive (D, ECC (k));
Step 6: ***if*** *res== D_{OTPS} then*
Step 7: Authentication Allowed;
Step 8: ***else***
Step 9: Authentication Denied;
Step 10: ***end if***
Step 11: OTP Update;
Step 12: ***end procedure***

During the transmission of one time password, there may be a problem in network coverage. To overcome this problem, a new technique is proposed i.e. generating one time password in offline mode.

D. A Enhanced Secure Health Care Monitoring Algorithm using Multilevel Authentication in Wireless Body Area Network (ESHCMA):

In the proposed [13], algorithm the server generates a session expired OTP (S_{OTP}). This S_{OTP} is generated on an offline mode and it is encrypted with ECC key and is sent it to the user device. The S_{OTP}, afterwards S_{OTP} verifies the authentication server whether the correct Authentication has been accessed after the user verifies it. Then the user is permitted to access the data, otherwise denied.

The ESHCMA Algorithm pseudo code for Session Expired OTP generation is given below:

Step 1: procedure Session Expired One-Time Auth (A, B)
Step 2: k ←ECC (A, B);
Step 3: OTP ← R_n ⊕ECC (k);
Step 4: Encryption (E) ← (OTP || ECC (k));
Step 5: send (E (OTP || ECC (k), receiver) ;
Step 6: Decryption ← D (E (OTP || ECC (k)))
Step 7: res ← Receive (D, k);
Step 8: ***if*** *res== S_{EOTP} then*
Step 9: Authentication Allowed;
Step 10: ***else***
Step 11: Authentication Denied;
Step 12: ***end if***
Step 13: OTP Update;
Step 14: ***end procedure***

4. SECURED FRAMEWORK FOR WBAN

The four proposed algorithms SPBHCMA, PBSCHCMA, ESDCMA and ESHMA are combined together to propose a secure framework. This section gives a diagrammatic view of the proposed framework and its explanations.

The Secured Human Health Care framework is for Wireless Body Area Network (WBAN), there are three issues [14 and 15] in WBAN which are Routing, Security, and Energy.

This paper concentrate only on security and WBAN's security can be classified into two types based on the patient station: 1.In Station-Security and 2. Out station-Security.

In- Station security denotes whether the patient is in the native place (i.e. in and around the living place, monitoring into their family doctor). When the patient is staying other than native place, then it is considered as "Out-Station".

When a patient need only an "In-Station security", A Secured Priority Based Health Care Monitoring Algorithm for Body Area Networks" (SPBHCMA) is used. When the patient need s security with energy efficiency then "A Priority Based Secure Clustering Health Care Monitoring Algorithm for Body Area Networks (PBSCHCMA)" is used.

The proposed Secure Human Healthcare Monitoring in Wireless Body Area Networks is given below

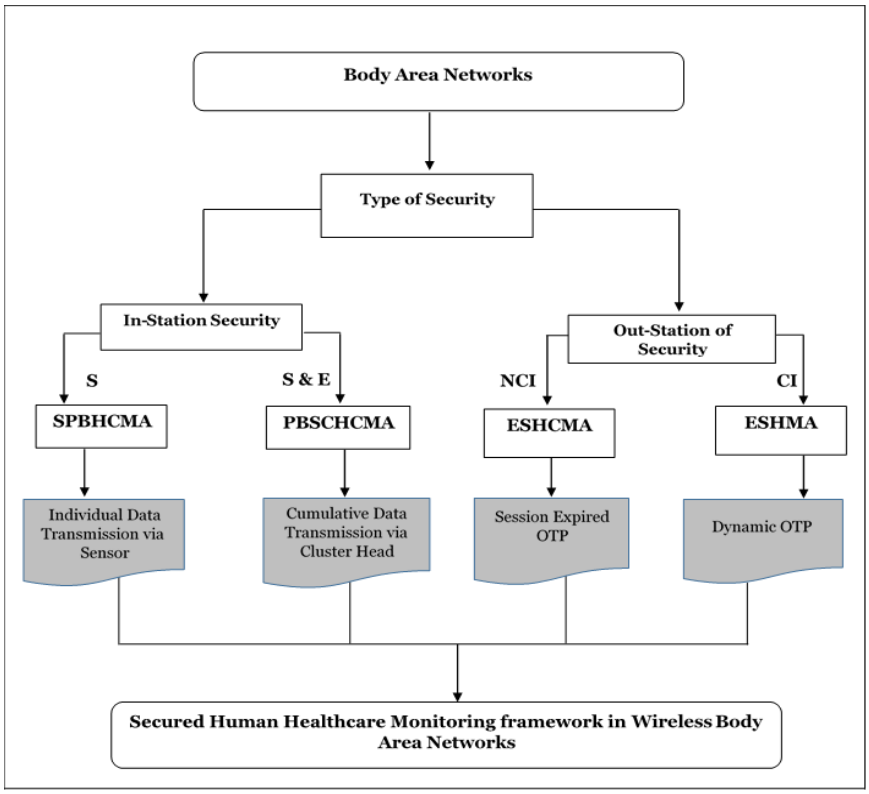

Fig. 1. Framework for Secure Human Healthcare Monitoring in Wireless Body Area Networks

In the Out-station security, there was two types of issues,

1. Coverage issue: The registered user device didn't have a network signal, while transmitting One-Time Password to the user device that situation is called as coverage issue.
2. Non-Coverage issue: The registered user device have a network signal, while transmitting One-Time Password to the user device that situation is called as Non coverage issue.

For out-station patient security, Algorithm Enhanced Secure Health Care Monitoring Algorithm using One-Time Password in Wireless Body Area Network is used for Non-Coverage Issue (NCI). If there is Coverage Issue (CI), then the algorithm Enhanced Secure Health Care Monitoring Algorithm using Multilevel Authentication in Wireless Body Area Network (ESHMA) for better transmission of OTP by using Session Expired OTP generation through offline mode.

5. CONCLUSIONS

This paper proposed a framework for securing human healthcare monitoring in wireless body area networks. The proposed framework, integrated four different algorithms to secure the human health data. Based on the patient location, the server decide the required algorithm to secure the data. The future direction of this work is to implement the framework and analyze the performance based on Quality of Service (QoS) parameters and hybrid more algorithm if needed.

REFERENCES

[1] Media Aminianand Hamid Reza Naji, "A Hospital Healthcare Monitoring System Using Wireless Sensor Networks", in Aminian and Naji, J Health Med Inform, 2013.
[2] A Darwish, AE Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring", Sensors. Vol.11, pp. 5561–5595, 2017.
[3] P Kumar, HJ Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey", Sensors. Vol.12 (1), pp. 55–91, 2016.

[4] G Selimis, L Huang, F Massé, I Tsekoura, M Ashouei, F Catthoor, J Huisken,J Stuyt, 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. 289–1298,2016.
[5] Wan, J.; Zou, C.; Ullah, S.; Lai, C.F.; Zhou, M.; Wang, X. "Cloud-enabled wireless body area networks for pervasive healthcare", IEEE Netw. 27, 56–61, 2013.
[6] Hayajneh, T.; Almashaqbeh, G.; Ullah, S.; Vasilakos, A. "A survey of wireless technologies coexistence in WBAN: Analysis and open research issues", Wirel. Netw. 20, 2165–2199, 2014.
[7] Rahimi, M.; Ren, J.; Liu, C.; Vasilakos, A.; Venkatasubramanian, N. "Mobile Cloud Computing: A Survey, State of Art and Future Directions", Mobile Netw. Appl. 19, 133–143, 2014.
[8] Almashaqbeh, G.; Hayajneh, T.; Vasilakos, A.V.; Mohd, B.J. "QoS-aware health monitoring system using cloud-based WBANs", J. Med. Syst. 38, 1–20, 2014.
[9] Tassos Dimitriou, Krontiris Ioannis, "Security Issues in Biomedical Wireless Sensor Network", Applied Sciences on Biomedical and Communication Technologies, 2008.
[10] 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 no. 82, pp. 168-172, 2015.
[11] V.Sethupathi, E. George Dharma Prakash Raj, "PBSCHCMA: A Priority Based Secure Clustering Health Care Monitoring Algorithm for Body Area Networks", International Journal of Control Theory and Applications, Vol.8 no.4, pp-17, 2015.
[12] V.Sethupathi, E. George Dharma Prakash Raj, "ESHSEA: Enhanced Secure Health Care Monitoring Algorithm using Session Expired Authentication in Wireless Body Area Network", International journal of Computer Science & Network Solutions, Volume 4.No.6, Jun.2016.
[13] V.Sethupathi, E. George Dharma Prakash Raj, "ESHMA: Enhanced Secure Health Care Monitoring Algorithm using Multifactor Authentication in Wireless Body Area Network", 4th International Conference on Advanced Computing & Communication Systems, Jan 2017.
[14] Camara, C.; Peris-Lopez, P.; Tapiador, J.E. "Security and Privacy Issues in Implantable Medical Devices", J. Biomed. Inform, 55, 272–289.2015.
[15] Mohd, B.J.; Hayajneh, T.; Vasilakos, A.V. "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues", J. Netw. Comput. Appl., 58, 73–93, 2015.

AUTHOR PROFILES:

V.Sethupathi completed his bachelor degree in computer science and engineering and master degree in computer and communication engineering in the year 2009 and 2011 respectively. He has 4 years of teaching experience at reputed engineering college, India. Currently he is doing her research in the area of Body Area Network under the guidance of Dr.E.George Dharma Prakash Raj.

Dr.E.George Dharma Prakash Raj completed his Master's Degree in Computer Science and Masters of Philosophy in Computer Science in the years 1990 and 1998. He has also completed his Doctorate in Computer Science in the year 2008. He has around twenty-four years of Academic experience and sixteen years of Research experience in the field of Computer Science. Currently he is working as an Asst.Professor in the Department of Computer Science, Engineering and Applications at Bharathidasan University, Trichy, India. He has published several papers in International Journals and Conferences related to Computer Science and has been an Editorial Board Member, Reviewer and International Programme Committee Member in many International Journals and Conferences. He has convened many National and International Conferences related to Computer Science.