AN EFFICIENT AND SECURE SESSION KEY ESTABLISHMENT SCHEME FOR HEALTH-CARE APPLICATIONS IN WIRELESS BODY AREA NETWORKS

Gulzar Mehmood[1*], M. Zahid Khan[1], Haseeb Ur Rahman[1], and Sohail Abbas[2]

ABSTRACT

Wireless Body Area Network (WBAN) is special breed of Wireless Sensor Network (WSN). Due to the increasing interest and the tremendous advancement in miniaturization and sensor technology, WBAN has emerged as an active filed of research. WBAN has many unique applications especially in medical and health-care. This kind of network provides support in on-the-spot decision making and therapeutic treatments. However, one of the main issues with WBAN in medical applications is security and patients' information privacy. In such applications ensuring human vital sign privacy and security is very important. To address this important issue, in this paper we propose a novel secure session key establishment scheme for WBAN in health-care domain to ensure security and privacy of vital sign related to human body. In the proposed scheme, session key is established for a specific period of time in order to communicate important data related to vital signs of patients' health securely. Hence, on the basis of this reliable and secure data transmission, efficient required medical decision can be taken. As a result, on the spot health-care operation can be performed by utilizing different health-care units. The proposed scheme is dynamic in nature, i.e. if a node in the network is compromised or a new node joins the network, the process of session key establishment is re-initiated. The proposed scheme has been evaluated through extensive simulation, and the results are compared with an existing scheme. The simulation results show that our scheme is efficient and cost effective in terms of communication and computation cost, and key establishment delay, hence conserves energy and enhances security.

KEYWORDS: *WBAN (Wireless Body Area Network); Bio-sensor; RSA; ECC*

INTRODUCTION

Due to the rapid advancement in technology, the life style of people is changing tremendously. Among these technologies one new recent and important is WBAN. This specific type of Wireless Sensor Network (WSN) changes the way different activities are performed. WBAN have many significant applications such as assisted living, medical diagnosing and sport examination. Wearable technology analyses body status and ensures quality of life efficiently. This new approach is now-a-days adopted in broad range of fields. On medical side small bio-sensors (sensor designed for human activity monitoring) are attached with human body or planted with human body, which sense vital signs (important data sensed from human body) and send them to the medical server for medical analysis, where physician take advantages from these information in diagnosing different medical treatment (Cho *et al.,* 2016; Lee *et al.,* 2016), as shown in Figure 1. WBAN related to health-care is helpful in a large number of treatments. for instance: Blood Pressure (BP) monitoring, glucose level monitoring and heart rate monitoring, the collected data are then send to medical server for further analysis. Medical applications of WBAN are increasing day-by-day because these networks can easily be configured in such environment. Apart from medical applications WBAN can be configured for home assistance, smart nursing and sport analysis (Khan *et al.,* 2009).

A new vision of this era is HBC (Human Bound Communication) for future telecommunication will open new opportunities to communicate sensory data efficiently (Re et al., 2016). WBANs are different from WSN because of their distinguished requirements and the IEEE standard for WBAN is IEEE 802.15.6 (IEEE standards 2016), where specifications are identified for this low power small devices, there communication range, protocol structure, and bandwidth. The importance of WBAN are realized from a current survey which show that the US current health-care expenditures are 17.9 % of the GDP and will grow up to 20 % in the next coming years (Re *et al.,* 2016). There are many issues and challenges related to WBAN. However, security has always been the main issue related to WBAN, but due to limited resources the schemes proposed for wired network such

*1*Department of Computer Science & Information Technology, Network Systems & Security Research Group (NSSRG), University of Malakand, Chakdara, Dir (L), Khyber Pakhtunkhwa, Pakistan*
2Department of Computer Science, College of Sciences, University of Sharjah, UAE

as RSA (Rivet-Shamming-Adleman) and ECC (Elliptic Curve Cryptography) are not directly applied in WBAN (Movassaghi *et al.,* 2014). WBAN have features like mobility of nodes and the data they collected are very sensitive. So, there is need that authorized entity must access the patient personal information's.

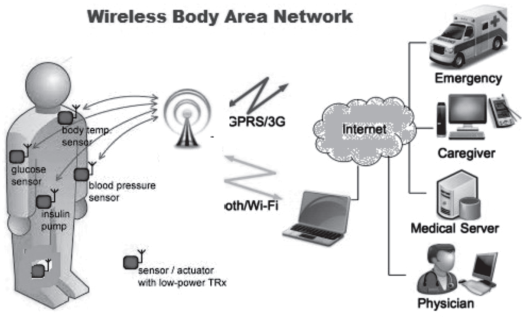


Figure 1: Architecture of Wireless Body Area Network.

In WBAN, security can be ensured at different levels i.e. hardware level and software level, and various techniques and schemes has been proposed for both levels over the time. The hardware level security is difficult and expansive, while software level security schemes are more effective, especially in health care applications (Dimitriou *et al.,* 2008). Security against different kind of issues and threats are provided to WBAN in different ways but cryptography is a very efficient way to secure information in WBAN. Most of the focus in this network is vital sign security and privacy keeping low energy consumption in mind (Zhouzhou and Wang 2016; Hu *et al.,* 2016; Zhou *et al.,* 2016). For instance, symmetric cryptography which uses same key for encryption/decryption is energy efficient but does not provide sufficient security to information related to WBAN. Asymmetric cryptography schemes are very efficient in terms of security. But the main problem with asymmetric cryptography is high computation and communication cost (Zhouzhou and Wang 2016; Hu *et al.,* 2016; Zhou *et al.,* 2016; Hu *et al.,* 2016). So most of the asymmetric schemes proposed for key management in WBAN are (Re *at al.,* 2016) expensive in term of cost i.e. more communication cost, communication overhead, and have more key establishment delay. Because RSA have key size is 1024 bits and ECC have 160 bits' key. In order to reduce energy consumption for WBAN and provide high or same level of security, in this paper a novel key management scheme has been proposed. The proposed scheme consumes less resources of WBAN, because un-wanted major operation (Asymmetric cryptography) are reduced and trust levels are created among bio-sensors involved in the operation.

The rest of the paper is organized as follows: Section 2 describe the related work, section 3 explain the proposed scheme in detail. In section 4, evaluation and results are discussed, and the paper is finally concluded in section 6 with directions for future work.

RELATED WORK

In the related work we have reviewed the most relevant and state-of-the-art solutions and schemes. In related research study some significant schemes are identified which contribute to improve the security of WBAN. However, traditional security schemes are not directly adopted for WBAN, because of limited resource. These schemes need to be used at optimum level for energy efficiency.

A bio-metric key establishment Method is also proposed in (Yao *et al.,* 2012). In this work, keys are generated from *ECG* (electrocardiogram) signal for secure communication between bio-sensors and gateway. This type of key is random, long, and unique. This method generated multiple and non-likable key for WBAN from same ECG signal. (Eldefrawy *et al.,* 2010), proposed a new scheme for secure key management in WSN with rekeying phase based on public key cryptography. The structure of the proposed scheme includes Sensor Node (SNs) and Gateway and the deployment of network is Mesh in nature. There are three steps in proposed algorithm, in first step all node and gateway are loaded with fre-session key, then in second step key agreement is perform on base of random number generated from each sensor i.e. R (Si) and then Gateway initialized a session key from all received encrypted random number i.e. G (S key) = R(S1+S2+S3+… Sn), and communicate this session key securely with all group nodes. The last step in this scheme is the steady state phase where rekeying are perform. Re-keying is performances when a node is compromised or a new node join the network. Let us consider a node Si generate a new random number r i´ and then concatenate this random number with its id and with it key which is ri and then encrypted with shared secrete key. If the node is new it authentication and validation will not be possible. Then new session will be established. Kumar *et al.,* (2011); proposed a user authentication scheme for wireless medical sensor network. In this research work two factor (smart card and password) user authentications are suggested in which a user is authentication before entering to the environment. After the process of authentication registration of user is carried out i.e. a smart card is to user by trusted entity. Smart card includes secret vale through which a user i.e. medical professional login to medical environment. Then a secure session is established between patients and the medical representative. a bio-metric base key management scheme is proposed by Razzi *et al.,* (2010); in which four type of key are used for WBAN. Which are communication key, administrative key, basic key and secret key. The proposed scheme is based on symmetric cryptography. But there is less opportunity for malicious node to access the network. The communication cost is high because each node directly communication with medical environment. Similarly, WBAN perform indoor outdoor health care monitoring securely at both side with minimum energy consumption. Ahmad *et al.,* (2015); proposed a scheme which address communication and security requirement. The author suggests data flow model between different entities involves in medical healthcare. The model is also check model checker and compare with existing scheme. Salehi *et al.,* (2016); proposed a scheme which generate 128 bit secret key for communication and improve quality of life. Apart from symmetric encryption, the alternate schemes which are based on asymmetric encryption are highly secure and suitable for dynamic environment. Many authors proposed schemes which are based on asymmetric encryption. Each addresses many advantages of these schemes. Asad *et al.,* (2012); proposed a hybrid key management scheme for WBAN, the scheme provide greater security, and suitable for dynamic environment, the proposed scheme consist of three phase, which is key pre-distribution, key establishment and rekeying. The scheme consumes greater resources of WBAN, because no clustering is used in this scheme. Majidi *et al.,* (2011); identified that symmetric key management scheme consumes less energy of WBAN, but the main problem with them is that, it is not so much secure to cope with medical application to ensure the privacy and reliability. Similarly, asymmetric key management techniques are highly secure which ensure confidentiality, but the cost require for Asymmetric scheme are high cost because of long key size of these schemes, such as RSA and ECC. So, the hybrid scheme will be most accurate choice which is proposed in this research work. Which are simulated and analyze, and conclude from the result that the hybrid scheme is energy is cost effective and also reliable to ensure the requirements of medical environment. Ertual *et al.,* (2005), adopt a new approach based on ECC algorithm. Where basically two different schemes are combined for reliably and energy better performances which is threshold cryptography and ECC, as we know that threshold cryptography is an efficient approach, which provide the facility of secure key management. The scheme creates trust among the communication environment more important for reliability and privacy and then key management is performances based on ECC. The key management message is delivering among n nodes who want are involve in message transmission. The K receives recover the original message and secure way is established between the participant nodes. Further the splitting of data/message is performing before encryption and at receiver side the splitting cipher text after encryption is perform. It is concluded from the comparison with RSA that ECC give efficient result then RSA. The main problem with the proposed work is that the process is very complex and requires more resource. But the idea is more attractive and we apply this in WBN environment for better performance. Sahana *et al.,* (2011), proposed a scheme base on RSA for securing Wireless Sensor Network. As we know that RSA Algorithm have long key size so the communication and computation cost must be high. In propose work the author suggests that the Cluster head doesn't involve in encryption/decryption. But this approach is efficient for less number of nodes. If we increase the number of nodes, then cluster head will be overloaded. Here in research work it is stated that Cluster Head (CH) perform only routing the aggregated data to the destination. A scheme for efficient anonymous authentication for wireless body area networks was developed which is based on elliptic curve key management scheme. The scheme involves three steps initialization, registration and authentication (Zhao *et al.,* 2014). The author stated that the propose scheme ensure protection against many security threads and attacks. Another access control scheme based on ECC for WBAN was developed by Chatterjee *et al.,* (2014), in the proposed scheme security against many well know attacks are ensure, such as node capture attack, denial-of-service, masquerade, stolen-verifier, replay, and man-in-the-middle attacks etc. the propose scheme having the capability to cope with dynamic environment. Also, the password is locally changed without the intervention of Base Station (BS). The proposed scheme is efficient in term of communication and computation cost. This scheme is complex and consumes maximum energy of WBAN. The ECC based schemes for secure and efficient key agreement are very effective in term of security as well as efficiency. Lee *et al.,* (2014); proposed an ECC scheme for secure session key establishment, which involves three steps, which are setup, registration, verification and finally the key exchanges. For user identification SIM card number is used, which is the number of the device places on patient body like smart phone, through which private key is generated by legal user. This approach prevents different attacks such as reply attack. Because every message has unique counter number assign to it. But there is no such information for re-configuration of the scheme in cause of some change occurs in the environment.

After all the discussion of securing WBAN especially for medical application, there is a need that the patient privacy and reliability must be preserve. In remote monitoring of certain environment, through WBAN face many non-avoidable challenges (Gurtov *et al.,* 2014). For secure authentication and Key agreement cryptographic based schemes are proposed, which provide against many kind of well know attacks as well as improve efficiency (Chaudhry *et al.,* 2015). Schemes previously proposed by different authors have significant contribution, but still there is need to address and solve key issues. Most of previous works are not energy efficient. And the security can also be improved by using CDLP (Complex Discrete Logarithmic Problem). We proposed a novel scheme for secure and efficient key agreement in WBAN. Propose scheme consume less resources of WBAN and provide sufficient security to vital sign related health-care individual.

In the next section we explain the proposed scheme in detail.

PROPOSED SCHEME

In this section, we propose a novel secure key management scheme for session key establishment for medical application in WBAN. The proposed scheme ensures the security requirements with relatively less energy consumption for WBAN. Our scheme aims to minimize the high computation cost of asymmetric cryptography, and also achieves improve level of security. We adopted complex public key cryptography in our proposed scheme for session key establishment which improve the security of WBAN. The numbers of major operations i.e. asymmetric cryptography operations involve in our scheme are reduced. So, the only major operations is between CH (Cluster Head) and Gateway. All other cryptography operations among biosensors are miner operations i.e. which are based on symmetric key cryptography as shown in Figure 2.

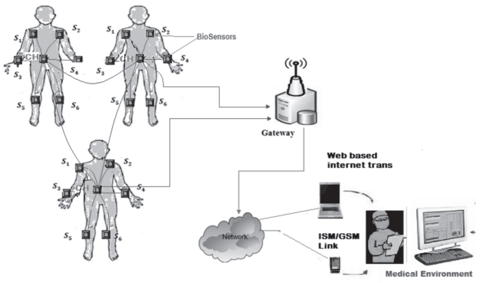


Figure 2: Topology of the Proposed Scheme.

Table 1: Proposed Scheme Notations

Notation	Description
q	A large prime number ($q \geq 2^{512}$)
b	b is a complex number of Order ($b \geq 2^{512}$)
d_{gw}	Gate way GW private key
P_{gw}	Gate way public key
d_{pi}	Patient P_i private key
P_{pi}	Patient P_i public key
r_{si}	Random number generated by sensor S_i
PS_k	Pre-session key
S_k	Session key
C_{si}	Randomly selected number by CH
r_{gw}	Random selected number by gateway
CH_1	Cluster head i
E_k	Encryption with key k
D_k	Decryption with key k
CDLP	Complex Discrete Logarithmic problem

A. Terminologies and Notations

In the proposed scheme we used the following list of notations in our scheme as given in Table 1.

B. Steps in the Proposed Scheme

Proposed schemes consist of our major steps including *key pre-loading, cluster head selection, session key establishment* and *re-keying.* In the next subsections, we will further explain these operations step by step.

B.1 Keys Pre-loading

The first step is key pre-loading where keys are pre-loaded to each sensor S_i and GW. Each S_i is preloaded with its own public and private keys as well as the public key of gateway, and. Also the GW is also pre-loaded with its own private and public keys and the public key of all sensors. Table-2 shows the keys pre-loaded to sensors and gateway.

Table 2: Keys Pre-Loading

Gate way	Sensors S_i on patient P_{pi}
d_{gw}, P_{gw}, P_{pi}	P_{gw}, d_{pi}, P_{pi}

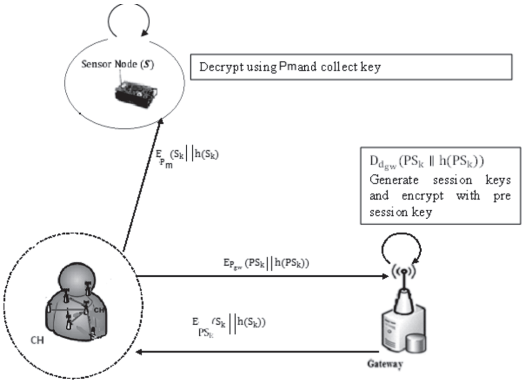
B.2. Cluster Head Selection

WBAN are made from small bio-sensors, these small devices have limited resources i.e. limited energy, and limited processing capability.

Biosensors are fixed in or with human body in such a way that they formed ultimately a cluster because all the biosensors are in the communication range. The cluster head is elected according to LEACH protocol (Asad and Chaudhry, 2012), in our proposed scheme. The CH is chosen for specific time. The patient is considering as a cluster because we want to save the energy of WBAN. This concept has significant advantages in order to save energy of the network, and is necessary for energy aware routing in WBAN.

B.3 Session Key Establishment Phase

Session Key Establishment is the important phase of our proposed scheme, where the proposed scheme algorithm and methodology are stated. The detail steps show how the session key establishments for WBAN are carried out. Following are the steps how our proposed algorithm operates. For further understanding the network specification and scenarios of the proposed scheme is highlighted in Figure 2 below.



Sensor Node (S)
Decrypt using Pmand collect key
$E_{P_m}(S_k||h(S_k)$
$D_{d_{gw}}(PS_k \parallel h(PS_k))$
Generate session keys and encrypt with pre session key
$Ep_{gw}(PS_k||h(PS_k))$
$E_{PS_k}(S_k||h(S_k))$
CH
CH
Gateway

Figure 3: Network Specification and Scenario of the Proposed Scheme

Following are algorithm steps of our proposed scheme, where different steps are given.

1 Ch → Gw Ep_{gw} $(PS_k \parallel h(PS_k))$ i.e. = PS_k = R_{ci} XOR r_{si}

2 GW Ddgw $(PS_k \parallel h(PS_k))$

3 GW→CH_i E_{PSk} $(S_k \parallel h(S_k))$ i.e. $S_k = PS_k$ XOR r_{gw}

4 CHi DPS_k $(S_k \parallel h(S_k)$

5 CH_i → S_i EP_m $(S_k \parallel h(S_k)$

6 Si Dd_m $(S_k \parallel h(S_k)$

The proposed schemes are further elaborate through scenario in the Figure 2. Which show how session key are actually established and how the communication are perform between biosensor, cluster head and the gateway. CH head generate a random number r_{ci} and consider it the pre-session key PS_k. CH then calculate hash of PS_k i.e. h (PS_k) and encrypt $PS_k \parallel$ h (PS_k) with the public key of the gateway i.e. P_{gw}. And send this payload to the Gateway. Gateway decrypts this with his own private key i.e. d_{gw}. Hash of PS_k are again calculated by GW and compare with the receive value of hash for integrity checking. If the results are same, the integrity is ensured. GW generates a random number of its own and XOR of its own generated random number with receive PS_k.

Which is the actual session key (S_k= PS_k XOR r_{gw}). GW calculate hash of the of S_k and concatenated it S_k and encrypt this information with PS_k and send back to CH. CH decrypt it with PS_k, calculated hash of S_k and compare it with received hash value for integrity checking. The session key i.e. S_k are then further send to each biosensor incorporate in WBAN. CH encrypt S_k || h (S_k) with Pm which symmetric key between all biosensor. Whenever biosensors receive the information they calculated again the hash of S_k for integrity checking. In this way session key S_k are communicated to all nodes incorporate in WBAN. The scenario of the whole scheme is given the following diagram.

B.4. Rekeying Phase

This is the last step of the proposed Session Key Establishment scheme. Which are initialized whenever a new node joins the network or when a node is died or compromise? Rekeying process is performed in same way as session key establishment process is perform, but the main difference is that the random value generated by biosensor node or GW are new and have no attaching with the old generated value. The new value generated by CH_i during rekeying phase is and then same process is carried out for new session key establishment. The following algorithm steps shows how rekeying are performed.

1 CH→GW EP_{gw} (PS_k' || h(PS_k')) i.e. = PS_k = r_{ci}' XOR r_{si}'

2 GW Dd_{gw} (PS_k' || h PS_k'))

3 GW → CHi Eps_k' (S_k' || h (S_k')) i.e. S_k = PS_k' XOR r_{gw}'

4 CH Dps_k (S_k' || h (S_k')

5 CH → Si Eps (Sk' || h (S_k')

6 S_i Ddm(Sk' || h (S_k')

The algorithm is similar process to the algorithm of session key establishment except the random value generated by CH i.e. r_{ci}' must be different from r_{ci} and also the random value generated by GW i.e. r_{gw}' must be different from r_{gw}.

EVALAUTION AND RESULTS

The proposed scheme is simulated in Opnet 14.5, because Opnet provide effective environment for wireless and mobile ad hoc network. OPNET (Optimized Network Engineering Tools) is efficient simulation software design for data network (Marghescu *et al.,* 2011). Simulation of the proposed scheme is carried out using different test case. In each test case specific numbers of nodes are selected and its parameters are specified then the required operations are performed. The experiments are performed three times, for five nodes, ten nodes and fifteen nodes simultaneously. The proposed scheme is analyzed using different parameters, and the most important parameter is energy consumption. First, we set topology of the required WBAN for simulation and then different experiments are performed and the result are taken in console text form. Then these output result are visualized using well known data analysis tool.

4.1. Network Topology and Simulation Parameters

We consider nodes on a single body as a cluster. There is trust between different nodes in a single body, because they are associated with a single person. These nodes than elected CH for themselves according to (Dawood *et al.,* 2011). And the Gateway is connected to biosensor through CH, so WBAN are three tire networks. There are certain simulation parameters which are listed in the following table.

Table 3: Simulation parameter, WBAN (IEEE 802.15.6)

SIMULATION SETUP	
Parameter	**Values**
Network Field area	(50 x50) meters
Node numbers	05~15
Cluster radius	r 50 m
Sensing radius	rs40 m
Data packet size	40 Bytes
Tx Power	0.1W
E-threshold	10pJ/bit/m2
Channel Type	Wireless
Buffer Size	256000 bits
Receiver Power Threshold	-95 dBs
Agent Trace	ON
E consume	50

4.2. Analysis of Results

In this section the simulation result are discussed in detail and comparison of the output results are perform with the existing work. The following graphs show the efficiency of our proposed scheme. There are three phases collectively form a single round of power consumption. Most power consumption is of data transmission and processing (computation) with the security provision (Das, 2009).

A. Communication Cost

We perform three test case of our scheme taking different set of nodes in order to get efficient result. The communication cost is found out for 5 nodes, 10 nodes and 15 nodes. The following Figure 4 shown comparisons between the proposed scheme and existing work. The graph shows our scheme give efficient result. And the main reason of low cost is that we reduce the number of major operations. i.e. between nodes and GW.

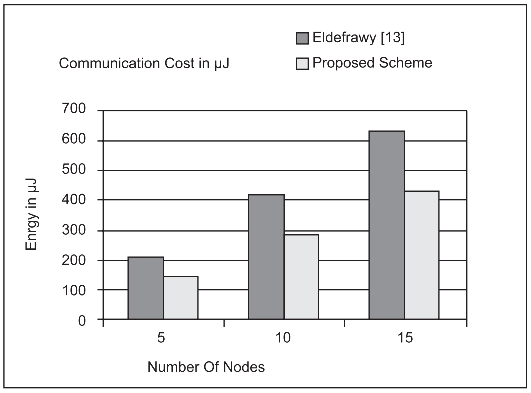


Figure 4: Communication Cost.

B. Communication Overhead

One of main issues with most of the cryptography schemes are they created significant overhead on the network. WBAN have limited bandwidth, so applying any security scheme we need to ensure that they create minimum overhead on the network. The proposed scheme ensures minimum overhead because of clustering approach and less number of nodes are involves in heavy cryptography operation. The out result in following Figure 5 show that our scheme communicate less number of bits during session key establishment.

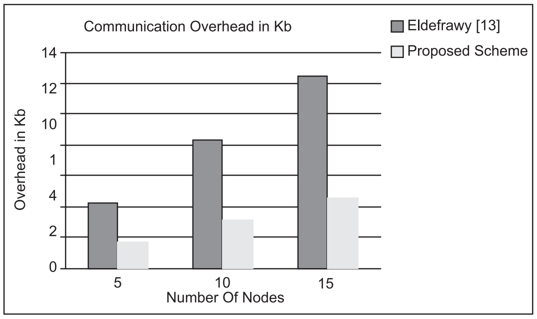


Figure 5: Communication Overhead.

C. Key Establishment Delay

The proposed scheme takes less time while performing key establishment because as we stated before the number of major operations is less in our scheme which consume more time. The results are compared with the existing scheme. More responsibility is on CH and GW which are involved in major operation i.e. pubic key operation from CH-→GW. The distance between GW and CH are taken 10 meter in our scheme. The CH are then responsible to deliver the establish session key for all node within a cluster. The communications between CH and biosensor are based on symmetric encryption, which take less time as shown in Figure 6.

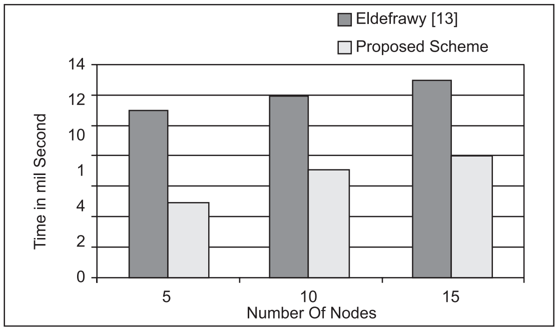


Figure 6: Key Establishment Delay.

D. Security Analysis

One of the important criteria for efficient security scheme in WBAN is how much stronger security it provides. In proposed scheme key management is based on ECC in addition with complex cryptography which increased the computation complexity of the information exchange. All nodes are pre-loading with public, private key pairs in network deployment time, to ensure that legal user can access the network. Our scheme also achieves forward secrecy, because each transmission between GW and CH generate a unique session key. So if attach know some value cannot predict further session key. A random number generate by CH i.e. r_{ci} and GW i.e. r_{gw} is unique. The integrity of the key is also check each node for the satisfaction that the secret key is not alters at any step during communication. Hash value are calculated for checking integrity of the transmitted information and this action is performed at each position to ensure that the received value are not alter by an attacker during transmission.

CONCLUSION AND FUTURE WORK

WBAN are special type of Wireless Network having many applications. In medical side it sensed vital sign of human body and sends them to the medical server. The sensed information related to human body need stronger security and privacy preservation. Security to WBAN can be provided through cryptography. Where secrete key sharing is very important. The proposed research work is a secure and authenticated key management technique for WBAN in medical environment. The proposed scheme ensures secure data transmission and with less consumption of energy of biosensors. The proposed scheme used the concept used in CDLP (Complex Discrete Logarithmic Problem) which ensure strong security. The number of major operations i.e. asymmetric operations are minimized for energy efficiency. In addition, trust is built within one cluster in WBAN because in a cluster all nodes related to one body. The communication between CH and CNs are a minor operation, which is based on symmetric cryptography. The proposed scheme ensures that unauthorized users are unable to access the secret information related to human body. Proposed scheme is also dynamic and adopt in dynamic situation where node additions are very important for energy replacement and real time monitoring of the situation. From simulation result it is concluded that the proposed scheme is more energy efficient and resilient against many type of attacks.

In future, we will develop a mathematical model using CDLP, which will ensure strong security of WBAN. We will extend this work by adding new features and requirements. More tests will be carried out using new set of parameter e.g. delay in message communication and overall Quality of Service etc.

REFRENCES

1. *Ahmad, S. S., Camtepe, S., and Jayalath, D., (2015), "Understanding data flow and security requirements in wireless Body Area Networks for healthcare", in 17th International Conference on E-health Networking, Application & Services (HealthCom), pp. 621-626.*

2. *Arshad, H., and Nikooghadam, M., (2016), "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC", Multimedia Tools and Applications, Vol. 75, No. 1, pp. 181-197.*

3. *Asad, M., and Chaudhry, S., (2012), "An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem", in Networking, Sensing and Control (ICNSC), 9th IEEE International Conference, pp. 118-121.*

4. *Chao, H.-C., Zeadally, S., and Hu, B., (2016), "Wearable computing for health care", Journal of medical systems, Vol. 40, No. 4, pp. 1-3.*

5. *Chatterjee, S., Das, A. K., and Sing, J. K., (2014), "A novel and efficient user access control scheme for wireless body area sensor networks", Journal of King Saud University-Computer and Information Sciences, Vol. 26, No. 2, pp. 181-201.*

6. *Chaudhry, S. A., Farash, M. S., Naqvi, H., Kumari, S., and Khan, M. K., (2015), "An enhanced privacy preserving remote user authentication scheme with provable security", Security and Communication Networks, Vol. 8, No. 18, pp. 3782-3795.*

7. *Das, M. L., (2009), "Two-factor user authentication in wireless sensor networks", Wireless Communications, IEEE Transactions, Vol. 8, No. 3, pp. 1086-1090.*

8. Dawood, M. S., Sadasivam, S., and Athisha, G., (2011), "Energy efficient wireless sensor networks based on QoS enhanced base station controlled dynamic clustering protocol", Energy, Vol. 13, No. 4.

9. Dimitriou, T., and Ioannis, K., (2008), "Security issues in biomedical wireless sensor networks," in Applied Sciences on Biomedical and Communication Technologies, ISABEL'08. First International Symposium, pp. 1-5: IEEE.

10. Eldefrawy, M. H., Khan, M. K., and Alghathbar, K., (2010), "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography", in Anti-Counterfeiting Security and Identification in Communication (ASID), pp. 1-6: IEEE Conference.

11. Ertaul, L., and Lu, W., (2005), "ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I)", in NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems: Springer, pp. 102-113.

12. Gurtov, P., Porambage, and Nikolaevskiy, I., (2014), "Secure lightweight protocols for medical device monitoring", in Open Innovations Association FRUCT, Proceedings of 15th Conference of IEEE, pp. 46-51.

13. Hu, C., Li, H., Huo, Y., Xiang, T., and Liao, X., (2016), "Secure and Efficient Data Communication Protocol for Wireless Body Area Networks", IEEE Transactions on Multi-Scale Computing Systems, Vol. 2, No. 2, pp. 94-107.

14. Hu, C., Li, H., Huo, Y., Xiang, T., and Liao, X., (2016), "Secure and Efficient data communication protocol for Wireless Body Area Networks", IEEE Transactions on Multi-Scale Computing Systems, Vol. 2, No. 2.

15. IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks, (2012), " IEEE Std 802.15.6-2012, pp. 1-271.

16. Khan, M. Pervez., Hussain, A., and Kwak, K.S., (2009), "Medical applications of wireless body area networks", Int. J. Digital Content Technol. And its Applications, Vol.3, No.3. pp.185-193. doi: 10.4156/jdcta.vol3.issue3.23

17. Kumar, P., Lee, S.-G., and Lee, H.-J., (2011), "A user authentication for healthcare application using wireless medical sensor networks", in High Performance Computing and Communications (HPCC), IEEE 13th International Conference, pp. 647-652.

18. Lee, J., Kim, D., Ryoo, H.-Y., and Shin, B.-S., (2016), "Sustainable Wearables: Wearable Technology for Enhancing the Quality of Human Life", Sustainability, Vol. 8, No. 5, p. 466, 2016.

19. Lee, Y. S., Alasaarela, E., and Lee, H., (2014), "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system", in Information Networking (ICOIN), IEEE International Conference, 2014, pp. 453-457.

20. Majidi, M., Mobarhan, R., Hardoroudi, A. H., and Parchinaki, A., (2011), "Energy cost analyses of key management techniques for secure patient monitoring in WSN", in Open Systems (ICOS), IEEE Conference, pp. 111-115.

21. Marghescu, C., Pantazica, M., Brodeala, A., and Svasta, P., (2011), "Simulation of a wireless sensor network using OPNET", in Design and Technology in Electronic Packaging (SIITME), IEEE 17th International Symposium, pp. 249-252.

22. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., and Jamalipour, A., (2014), "Wireless body area networks: a survey", IEEE Communications Surveys & Tutorials, Vol. 16, No. 3, Third Quarter 2014.

23. Raazi, S. M. K.-u.-R., Lee, H., Lee, S., and Lee, Y.-K., (2010), "BARI+: a biometric based distributed key management approach for wireless body area networks", Sensors, Vol. 10, No. 4, pp. 3911-3933, 2010.

24. Re, E. Del., Morosi, S., Mucchi, L., Ronga, L. S., and Jayousi, S., (2016),"Future Wireless Systems for

Human Bond Communications", Wireless Personal Communications, Vol. 88, No. 1, pp. 39-52.

25. *Sahana and Misra, I. S., (2011), "Implementation of RSA security protocol for sensor network security: Design and network lifetime analysis", in Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2nd International Conference, pp. 1-5.*

26. *Salehi, S. A., Razzaque, M. A., Tomeo-Reyes, I., Hussain, N., and Kaviani, V., (2016), "Efficient high-rate key management technique for wireless body area networks", in 22nd Asia-Pacific Conference on Communications (APCC), pp. 529-534.*

27. *Yao, L., Liu, B., Wu, G., Yao, K., and Wang, J., (2011), "A biometric key establishment protocol for body area networks", International Journal of Distributed Sensor Networks, Vol. 20, pp.1550. https://doi.org/10.1155/2011/282986.*

28. *Zhao, Z., (2014), "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem", Journal of medical systems, Vol. 38, No. 2, pp. 1-7.*

29. *Zhou, Y., Sheng, Z., Leung, V. C. M., and Servati, P., (2016), "Beacon-based opportunistic scheduling in wireless body area network", 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 4995-4998.*

30. *Zhouzhou, L., and Wang, H., (2016), "A key agreement method for wireless body area networks", IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 690-695.*