J. Appl. Environ. Biol. Sci., 6(2S)151-158, 2016

© 2016, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

An Efficient Key Agreement for Wireless Body Area Networks Based on Hyper Elliptic Curves

Noor Ul Amin, Jawaid Iqbal, Arif Iqbal Umar, Nizamuddin

Department of Information Technology, Hazara University Mansehra, Pakistan

Received: January7, 2016
Accepted: March 2, 2016

ABSTRACT

. The security of Wireless Body Area Networks (WBANs) has become imperative with the rapid development of WBANs in the medical health care. This paper presents an efficient key agreement scheme based on Hyper Elliptic Curve Cryptosystem (HECC) for the secure transmission of patients' health status data to the intended medical specialist. This scheme is light weight as compare to other schemes due to the shorter parameters of HECC .The significant cost reduction along with integrity, confidentiality, authenticity and key updating can make this scheme a better choice for the resource constrained set up of WBANs.

KEYWORDS*:* WBANs; Key Agreement; HECC; Hash Function; AES

1. INTRODUCTION

The application of WBANs is rapidly evolving in the field of medical health care for urgent treatment of patients according to the type of diseases such as ECG, EEG, EMG, body glucose level, temperature, blood pressure etc. Low power and small sensors with limited processing capability are deployed on patient body which sense patients disease status and communicate the obtained information through Base Station (BS) and Medical Server (MS) to the corresponding medical specialist. As a response, medical specialist provide emergency treatment.

The security of WBANs are unavoidable for conveying the exact sensed patient data to the recipient without any amendment or reading by the unauthorized accessor of the data. Illegal access of patients personal health information is restricted by law like PRC in China [1], USA [2] and "EUD 2002/58/EC" in Europe [3]. Different security solutions provided for Wirless Sensor Network (WSN) by the researchers are not adjustable to the resource constraints setup of WBANs. Applying public key crpto systems becomes expensive for the network and symmetric crypto system suffer with key distribution problem. Hybrid solutions are acceptable but still needs improvement in cost efficiency. In [4] Koblitz coind HECC which can be a better choice in replacement of ECC for the resource constrainted environment of WBANs.

To achieve efficiency in our scheme we use HECC due its shorter key size as compare to other crypto systems, the 80 bits base field provides equivalent security as that with 180 bits ECC and RSA 1024 bits.Our efficient key agreement scheme uses HECC for resource constraint environment of WBANs.This scheme will provide security with improved cost efficiency in a hospital ward.

The rest of this paper is organized in various parts. In part (II) the literature reivew and related security schemes are critically discussed. In part (III) network model, part (IV) threat resistance model, part (V) radio model, part (VI) design requirement, part (VII) preliminaries, part (VIII) proposed scheme, part (IX) security analysis, part (X) performance analysis, and part (XI) conclusion are elaborated.

2. RELATED WORK

In proposed scheme [5], the key agreement between sensors and the base station is performed using ECC. Integrity and confidentialty of patient data maintained by Block cipher RC5. This scheme is inefficient due to its computational cost and delay. In [6], the proposed solution relies on a non-cryptographic technique BANA for the authentication of the sensors and RSS is applied for the identification of legal and illegal nodes.This non-cryptographic approach not secure as open to be frorged by creating a perfect channel. In proposed scheme [7], the hardware dependent design solution is presented for the network security and small micro-controller is introduced for saving energy. TDMA-MAC is used for the transmission of the

* **Corresponding Author:** Noor Ul Amin, Department of Information Technology, Hazara University Mansehra, Pakistan
namin@hu.edu.pk

patient physiological data. This hardware based scheme can be replaced by using efficient cryptographic technique to address the energy issue. In [8] mutual authentication technique is used for the identification of neighbor sensors and PWH. This scheme works on individual keys and pair wise keys. Pair wise key is shared with neighbor sensors and Individual with PWH. The requirement of $n\,(n-1)/2$ keys with n neighbor sensors, this polynomial key sharing leads to high computation cost, memory and communication overhead. In [9] FABSC scheme, random polynomial is selected for the distribution of private keys in key generation, source and target agreement for transmission to share keys amongst sensors using feature set exchange but if feature set of sensor is found identical with target then the attacker can easily launch the replay attack. In proposed scheme [10], a hybrid technique using ECC is used for secure key exchange. This scheme has efficiency but sensor authentication is still a problem. In [11], a hybrid scheme with flavor of authenticated and cluster head selection through rotation.AES and ECC are used in this scheme, AES for confidential transmission of data to the medical specailest and ECC for secure key exchange. In [16], a key agreement scheme is proposed with the property of rekeying using RSA and DHECC for WSN. This is a public key cryptographic scheme and not feasible for the resource constraint environment of WBANs due to high processing cost, transmission cost and storage overhead. In [17], a hybrid scheme for key management is proposed for the security of BSN which is based on public key crypto system RSA and symmetric crypto system. This scheme is inefficient for WBANs due to large key size of RSA.

Keeping in view the resources limitation of WBANs, a secure and efficient scheme is required to be proposed by reducing the cost and overhead of the other proposed schemes to become applicable in WBANs. Space using HECC instead of ECC for key agreement, a high efficiency can be achived with significant reduction in compution cost and communication overhead.

3. Network Model. The proposed WBANs architecture in Figure. 1 consists on body sensors, BS and MS. Body sensors and BS are connected in a ward of medical center for the transmission of patient physiological data to MS. Tiny disease focused sensors are deployed on patients body which sense, collect and dissiminate information wirelessly to the smart phone of medical specialist via base station for quick medical response.All sensors are directly connected to the base station. All nodes are accessable by one or two hopes and at the distance of maximum upto 10 meters. The 802.15.6 standard is adopted for the inter operationability of the WBANs. The architecture is flexible and adding or removing a node does not effect the network structure. Patients are the owners of the network and medical specialists are the users.

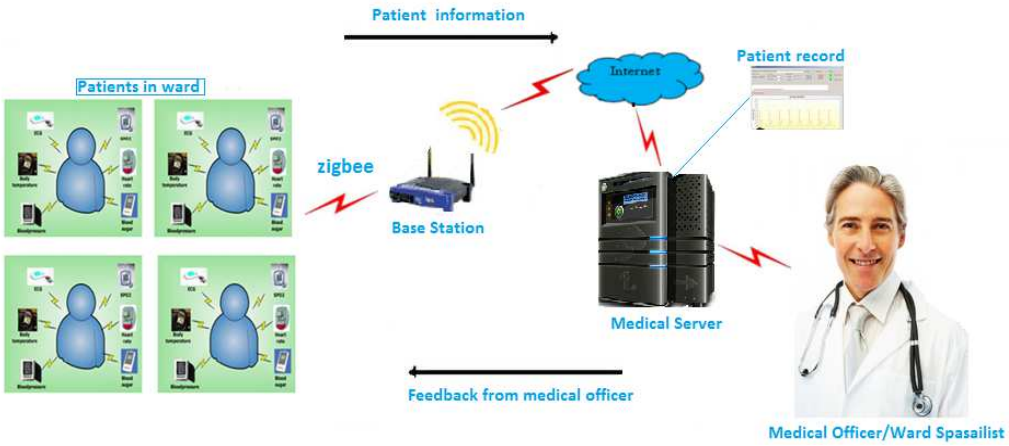

Figure 1. Design Architecture of WBANs for Patients in Medical Ward

4. Threat Resistance Model. Vulnerable wireless communication of patient status information in WBANs is threatful.The adversary can easily target the patients physiological data for misuse.This is important to make the network secure against expected threats.The model will have to address all the important security parameters of integrity, confidentiality, authenticity, scability and farward/backward secrecy. Secure hybrid approach, HECC for key agreement and AES for confidential session data transmission will be used. Keys updating is the neccssary part of this model.This can avoid the advercery from guessing the actual session key using old keys.

5. Radio Model. Here we prefer first order radio model in our scheme to measure energy consuming in transmitting patients physiological data over wireless channel in WBANs where $\boldsymbol{E_t}$ denotes transmitted energy, $\boldsymbol{l}$ denotes length of message and $\boldsymbol{d}$ denotes communication distance [12], equation(1) represents energy consumed during data transmission by the body sensors.

$$\mathrm{E_t}(l,d) = \begin{cases} l\mathrm{E_{elec}} + l\,\varepsilon_{\mathrm{fs}}\ d^2, d < d_0 \\ l\mathrm{E_{elec}} + l\,\varepsilon_{\mathrm{mp}}\ d^4, d \geq d_0 \end{cases} \qquad (1)$$

Packet length l and distance d^2 are directly proportional to power consumed by the sensors i.e. in case of short distance low power consumption and more energy consumption in case of long distance.

The following equation (2) represents the energy consumption in receiving patients data by sensor nodes where $\mathrm{E_r}(l)$ denotes energy required, l denotes length of packet and $\mathrm{E_{elec}}$ denotes energy consumption per bit.

$$\mathrm{E_r}(l) = l\mathrm{E_{elec}} \qquad (2)$$

$$E_{elec} = 50nJ/bit,\ d_0 = 100\mathrm{m}$$

The distance in our scheme $d < d_0$ so we use free space model $\varepsilon = \varepsilon_{\mathrm{fs}} = 10$ pJ/bit/m^2 . $\varepsilon_{\mathrm{fs}}$ denotes free space model amplifier energy factor.

6. Design Requirement. Timely and secure delivery of patients' physiological data to the intended recipient is the major design requirement of the health care applications which are describe below:

6.1. Body Sensor authentication. MS has the responsibility to authenticate body sensors and ensure whether the patients' data received from legal sensor or an attacker.

6.2. **Secure key agreement.** Conventional key agreement schemes are not optimal for the resource constraint WBANs due to its high cost. Light weight secure key management solutions are the design requirement of such a network composed of tiny body sensors. Secure exchange of session key for the secure communication of information is the prime concern so that to protect the patient sensitive information in the way to its destination from the adversaries. Efficient key management is a major requirement of WBANS [13].

6.3. Confidentiality of information. Confidential transmission of sensitive patients data to the targeted destination is basic design concern as its disclosure to the illegal users can put human life at risk. As per HIPAA act [2] patients' sensitive information must be protected. Patients' physiological readings sensed by the body sensors like BP, ECG, and EEG etc should only be communicated to the intended MOs for emergency feedback. For the confidential flow of information various encryption algorithms or ciphers (AES,DES, Blow fish,RC5,Skipjack) are used in the literature.

6.4. Patients Data Integrity. Patients' data integrity ensures that the data received by the MOs is not altered. To protect patients' data from modification by the adversaries various message digest algorithms (SHA-128, SHA-512,) are proposed.

6.5. Keys Updation. Updating session keys feature should be the part of our WBAN design for protecting the network from the adversaries trying to compromise session key using old keys for guessing new key.

6.6. Cost efficiency. Tiny body sensors with low power, limited processing capabilities, limited memory and short range communication require such schemes which would not only be secure but also cost efficient for resource constrained WBANs environment.

6.7. Energy Efficiency. In wireless networks transmission of data is very expensive and maximum energy is consumed in transmission as sending one bit of information consumes more than one thousand times energy than that of thirty two bit computation [14]. Minimizing data packets transmission can lead to low energy consumption.

6.8. Network Scalability. Scalability of the network becomes essential as removing, replacing or adding a sensor in the WBAN the entire frame work should not be affected and function properly.

6.9. Data Freshness. Data freshness assures that the data packets received from a body sensor is new and not replayed. The adversary may delay a data packet and replay later on which affect the freshness of data. As

fresh data is mandatory for the decision making of the MOs.

7. Preliminaries of Hyper Elliptic Curve. Hyper elliptic curves can be viewed as generalization of elliptic curves, with genus $\boldsymbol{g \geq 2}$. Let $\boldsymbol{h(x), f(x) \in Fq[x]}$, $\boldsymbol{\deg(h(x)) \leq g}$, $\boldsymbol{f(x)}$ is monic polynomial and $\boldsymbol{deg(f(x)) = 2g + 1}$. A hyper elliptic curve $\mathbb{C}$ of genus $\boldsymbol{g \geq 2}$ over the finite field $\boldsymbol{Fq}$ is set of points $\boldsymbol{(x, y) \in Fq \times Fq}$ satisfy the equation $(\boldsymbol{3})$

$$\mathbb{C}: y^2 + h(x)y = f(x) \quad (3)$$

A divisor D is a finite formal sum of points $P_i = (x_i, y_i) \in \mathbb{C}, D = \sum m_i P_i$, $P_i \in C, m_i \in Fq$. Jacobian $J_c(Fq)$is finite group and its order is $\#J_c(Fq)$

$$\left|(\sqrt{q} - 1)^{2g}\right| \leq \#J_c(Fq) \leq \left|(\sqrt{q} + 1)^{2g}\right|$$

8. Proposed Scheme. The proposed design architecture consists on four stages. Stage first include initialization , stage second key establishment, stage third secure data transmission and stage fourth session key updating stage.

Table 2 Notation Guide

Symbols	Description
S_i	Body sensor/Biosensor node i
$\mathbb{C}$	Hyper Elliptic Curve
D	A divisor of large prime order n in $J_c(Fq)$, $n \geq 2^{80}$
d_{bs}	Biosensor private key $d_{bs} \in \{1,2, \dots n-1\}$
P_{bs}	Biosensor public key $P_{bs} = d_{bs}D$
d_{ms}	Medical server private key $d_{ms} \in \{1,2, \dots n-1\}$
P_{ms}	Medical server public key $P_{ms} = d_{ms}D$
φ	A function which map a divisor to integer value
h	One way hash function
E_k/D_k	Symmetric Encryption / Decryption with key k
m/c	Message/Cipher text

8.1. Initialization Stage. In this stage, each sensor node S_i is preloaded with public key P_{bs}, private key d_{bs} and public key P_{ms} of medical server prior on the body of patients. Public key P_{ms}, Private Key d_{ms} and public keys P_{bs} of all sensor nodes are preloaded to medical server.

8.2. Key Establishment Stage. In this stage, round wise session key is generated then exchanged in secure manner among sensor nodes and medical server using HECC for onward transmission of patient data securely. Sensor node run Probalistic Encryption Algorithm 1. Encrypt (P_{ms}) to generate encrypted text for session key (k).

ALGORITHM 1: Encrypt $(\boldsymbol{P_{ms}})$

1. Select a Random integer $S_k \in \{1, 2, \dots n-1\}$
2. Computes $h_i = h(S_k \parallel ID_{si})$
3. Encode message to divisor: $S_k \parallel ID_{si} || h_i \rightarrow P_m$
4. Computes $Q = kD$
5. Computes $P_k = kP_{ms}$
6. Computes $C_m = (Q, P_m + P_k)$
7. Transmit C_m to MS

MS obtain sensor node public key from certificate authority, decrypt encrypted session key using detremiistic decryption algorithm 2 Decrypt (C_m , P_{bs}) to obtain session key (S_k) from encrypted text (C_m).

ALGORITHM 2: Decrypt $(\boldsymbol{C_m, d_{ms}})$

1. Computes $d_{ms}Q$
2. Extract $P_m + P_k$ from C_m
3. Computes $P_m = P_m + P_k - d_{ms}Q$
4. Extract message from divisor: $P_m \rightarrow S_k \parallel ID_{si} || h_i$
5. Computes $h_i{}' = h(S_k \parallel ID_{si})$

6. if $h_i{}' = h_i$ accept the session key S_k, otherwise reject

8.3. Secure Data Transmission Stage.The integrity is maintained through by taking the hash of patient sensed physical status data m_{ri} to compute ri then (m_{ri}, ri) are encrypted and cipher text c_i is obtained and forwarded to medical server. Medical server decrypts the c_i using round session key and then compare the hash of m_{ri} which is $ri'$with recieved , if matched accept otherwise discard the data packet.

LGORITHM 3: Secure Session Data Transmission

1. **Body Sensor Node**
2. **for** each body sensor node $s_i \in P_i$
   a. sense data m_{ri}
   b. Computes $ri = h(m_{ri})$
   c. Computes $c_i = \mathrm{E}_{S_k}(m_{ri}, ri)$
   d. Sends c_i to MS
3. **End for**
4. **Medical Server**
5. **for** each body sensor encrypted data $c_i \in P_i$
   a. $(m_{ri}, ri) = \mathrm{D}_{r_{Sk}}(c_i)$
   b. Computes $ri{}' = h(m_{ri})$
   c. Accept if $ri{}' = ri$ Save data to patient P_i record otherwise reject
6. **End for**

8.4. Key Updating Stage. Round wise updation of keys is the essential feature of our proposed scheme for prevention from the attack of cryptanalyst using old keys and guessing new keys. In this way forward and backward secrecy is maintained.The following algorithm 4 updating the session keys of sensors and medical server round wise . The last round data m_{ri-1} is computed by taking its hash and XOR is taken with the session key of last round. Fresh session key Sk_{ri} is computed by taking the last round data m_{ri-1} with the last round session key $Sk_{r_{i-1}}$.

ALGORITHM 4: Key Update

1. Biosensor
   a. Computes $h(m_{ri-1})$ where m_{ri-1} is last round data
   b. Computes $Sk_{ri} = Sk_{r_{i-1}} \oplus h(m_{ri-1})$
2. Medical Server
   c. Computes $h(m_{ri-1})$
   d. Computes $Sk_{ri} = Sk_{r_{i-1}} \oplus h(m_{ri-1})$

End

9. Security Analysis. The secure communication of collected patient physiological status data from body sensors to the intended recipient (medical specialist) is the key addressable issue of WBANs. Our scheme is based on computationally infeasible hard problem using Hyper Elliptic Curve Discrete Log Problem (HECDLP) [15].This scheme is protected against expected threats and fulfills all basic security parameters described below:

9.1. Confidentiality. The confidential transmission of patient physiological data from the source to target is essential, for this purpose symmetric AES algorithm is used to protect patient data from reading of illegal users. In our scheme confidential transmission of session key is performed using HECC.

9.2. Integrity. Integrity is an important property of our proposed scheme where patient data is protected from modification. Integrity is achieved using one-way hash collision resistive function.

9.3. Authenticity. Our proposed scheme ensures authenticity and only provide access to the legal users. And upon detection, illegal users can be blacklisted by the MS.

9.4. Scalability. The design architecture is scalable and a node can be added or removed as per the requirement of the network without changing the structure of the network.

9.5. Forward and Backward Secrecy. The key updating property of our scheme block the passive adversary

from guessing the session key through using old keys.

10. Performance Analysis. The parameters for the evaluation of our scheme are cost and overhead. We have analyzed our scheme with other schemes [16], [17] on the basis of these parameters. The efficiency of our proposed scheme is prominent than the other schemes.

10.1. Computational Cost Analysis. The expensive operations in [16,17] are "Elliptic Curve Point multiplication (ECPM)" and "Modular Exponentiation (M-Exp)" respectively. And in our proposed scheme the major operation is "Hyper Elliptic Curve Divisor Scalar Multiplication (HECDM)". In [16] four ECPM and two M-Exp and in [17] two M-Exp are used while in our proposed scheme two major operation HECDM is used. The analysis is shown in Fig 2.

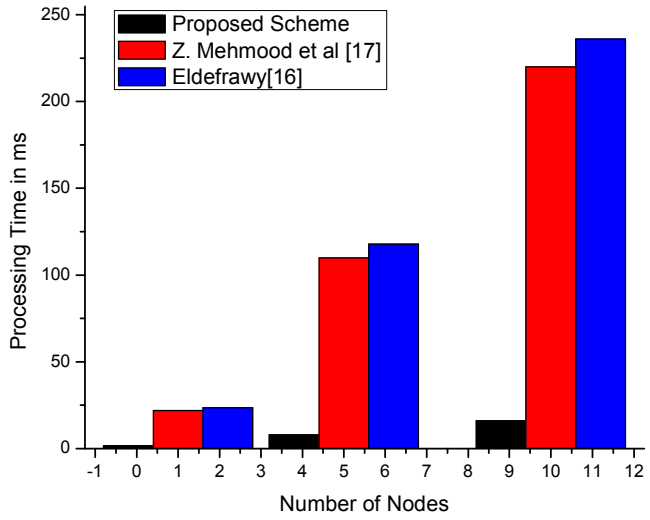

Figure 2. Computational Cost Comparison

10.2. Communication Overhead Analysis. The maximum energy is consumed on transmission of patients data which depends upon the packet size and distance between source to target. Due to use of smaller key size, our proposed scheme is efficient in communication over head as compare to other schemes. The analysis is shown in Figure.3

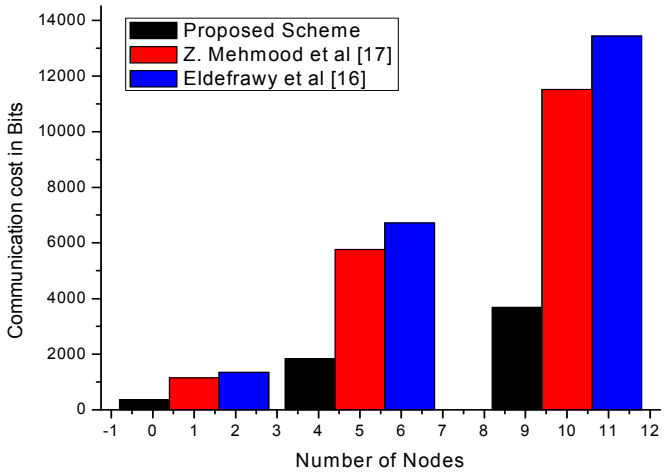

Figure 3.Communication Cost comparison

10.3. Memory Storage Cost. As the key size is smaller in our scheme using 80 bits so the number of bits to be stored are also consuming less memory as compare to [16] using 1024 bits and [17] 160 bits. The storage comparison of our proposed scheme with other schemes is shown in Figure.4

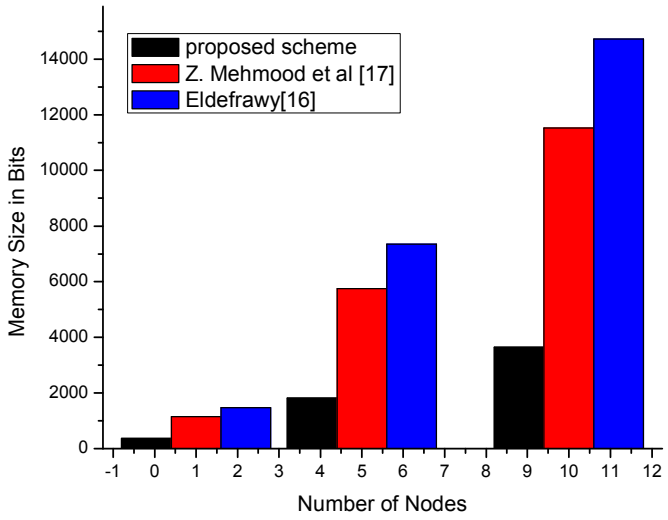

Figure 4. Storage Cost Comparison

11. Conclusion. The main focus of this paper is securing resource constraint environment of WBANs with an efficient key agreement scheme. In our proposed scheme the use of HECC with shorter key size enhanced the efficiency using smaller number of bits while acheiving the same security as that of other scheme using larger number of bits like RSA, ECC. Significant improvement in communication and storage overhead and computational cost is achieved as shown in figures (2,3,4).

12. Acknowledgments. We thank Dr. Saleem Abudullah, Mr.Abdul Waheed and our anonymous reviewers for their insightful feedback. I am very thankful to Pakistan Science Foundation (PSF) to support my research work.

REFERENCES

[1] Yang, P. L., Lin, V., & Lawson, J. (1991). Health policy reform in the People's Republic of China. *International journal of health services*, *21*(3), 481-491.

[2] Bowen, P., Johnson, A., Hash, J., Smith, C. D., & Steinberg, D. I. (2004). An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. *NIST Special Publication*, 800-66.

[3] Terry, N. P. (2003). Privacy and the health information domain: Properties, models and unintended results. *European Journal of Health Law*, *10*(3), 223-237.

[4] Koblitz, N. (1989). Hyperelliptic cryptosystems. *Journal of cryptology*, *1*(3), 139-150.

[5] Malasri, K., & Wang, L. (2009). Design and Implementation of a SecureWireless Mote-Based Medical Sensor Network. *Sensors*, *9*(8), 6273-6297.

[6] Shi, L., Li, M., Yu, S., & Yuan, J. (2013). Bana: body area network authentication exploiting channel characteristics. *Selected Areas in Communications, IEEE Journal on*, *31*(9), 1803-1816.

[7] Selimis, G., Huang, L., Massé, F., Tsekoura, I., Ashouei, M., Catthoor, F., ... & De Groot, H. (2011). A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design.*Journal of medical systems*, *35*(5), 1289-1298.

[8] He, D., Chen, C., Chan, S., Bu, J., & Zhang, P. (2013). Secure and lightweight network admission and transmission protocol for body sensor networks.*Biomedical and Health Informatics, IEEE Journal of*, *17*(3), 664-674.

[9] Hu, C., Zhang, N., Li, H., Cheng, X., & Liao, X. (2013). Body area network security: A fuzzy attribute-based signcryption scheme. *Selected Areas in Communications, IEEE Journal on*, *31*(9), 37-46.

[10] Asad, M., & Chaudhry, S. A. (2012, April). An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. In *Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on* (pp. 118-121). IEEE.

[11] Iqbal, J., ul Amin, N., & Umar, A. I. Authenticated key agreement and cluster head selection for Wireless Body Area Networks. In *2013 2nd National Conference on Information Assurance (NCIA)*.

[12] Li, I. H., Liao, I. E., & Wu, F. N. (2008, September). A traffic load-aware energy efficient protocol for wireless sensor networks. In *Proceedings of the International Conference on Mobile Technology, Applications, and Systems* (p. 5). ACM.

[13] Mišić, J., & Mišić, V. (2008). Enforcing patient privacy in healthcare WSNs through key distribution algorithms. *Security and Communication Networks*,*1*(5), 417-429.

[14] Barr, K. C., & Asanović, K. (2006). Energy-aware lossless data compression.*ACM Transactions on Computer Systems (TOCS)*, *24*(3), 250-291.

[15] Ch, S. A., Sher, M., Ghani, A., Naqvi, H., & Irshad, A. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. *Multimedia Tools and Applications*, 1-13.

[16] Eldefrawy, M. H., Khan, M. K., & Alghathbar, K. (2010, July). A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. In *Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference on* (pp. 1-6). IEEE.

[17] Mehmood, Z., Nizamuddin, N., Ch, S. A., Nasar, W., & Ghani, A. (2012, July). An efficient key agreement with rekeying for secured body sensor networks. In*Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on* (pp. 164-167). IEEE.