J. Appl. Environ. Biol. Sci., 6(3S)166-174, 2016

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

A Novel Key Agreement Framework for Wireless Body Area Networks Based on Hyper Elliptic Curves Signcryption

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 evolution of WBANs under the medical health care field is vital for human survival and security of patients' personnel physiological information remains appalling challenge yet to be addressed. This article presents a novel key agreement framework based on HECC signcryption best fit for inter secure communication in the resource constraint environment of WBANs. Shorter key size, low communication and storage overhead with promising efficiency and security make this scheme superior over other schemes. Similarly, avoidance of unnecessary use of cluster head in a ward decreases one hop which reduces the overall over head of the network.

KEYWORDS: Wireless Body Area Networks; Key Agreement; Hyper elliptic curve cryptosystem; Signcryption

1. INTRODUCTION

Wireless Body Area Network (WBAN) is emerging for well in time medical health care and in response medical treatment according to the nature of diseases like temperature, blood pressure heart beat, body glucose level etc. In WBAN physiological status of patients is monitored round the clock without disrupting routine life. Tiny body sensors with limited processing capabilities, limited memory and low battery power are deployed on human body for collecting health status information and communicating to the medical officers (MOs) via Base Station (BS) and Medical Server (MS) for emergency medical response. The security of WBANs is a key issue which should be addressed properly like breach of patients' personal physiological status data, altering actual data packets by the Eavesdropper (Evo), could lead to incorrect diagnosis and treatment. In many countries security of health information like USA [1], "EUD 2002/58/EC" in Europe [2], "PRC" law in China [3] is mandatory. A number of generic security solutions designed for WSNs have been tried to be implemented for WBANs which are not feasible due to WBANs resource limitations. Symmetric ciphers are fast but suffers with secure key distribution problem while asymmetric solve the secure key distribution problem but are costly. Hybrid techniques are somehow balanced but still needs cost efficiency to be best fit in WBANs resource constraint environment. The security feature of signature for authentication and encryption for achieving confidentiality were combined logically into single operation called signcryption [4]. Koblitz [5], first time introduced Hyper Elliptic Curve Cryptosystem (HECC) as alternative of Elliptic Curve Cryptosystem (ECC), feasible to achieve high security for resource constraint environment. Nizamuddin et al. [6] proposed Signcryption scheme based on HECC and reduced significant computation and communication compared to ECC based schemes.

HECC is prioritizing over other cryptographic solutions because its shorter parameters provide the same security level. HECC 80 bits base filed offer the same security with that of ECC 180 bits and 1024 bits of RSA. In our novel secure key agreement framework designed for a hospital ward, we apply HECC based signcryption for WBANs which will provide the same security level with enough lower computation, communication and storage cost and one hop reduction due to avoidance of cluster head will increase the overall performance of the network.

The rest of the paper is organized in sections. In section II "Related Work" the background and related security schemes are critically discussed. In section III "Network Model", section IV "Threat Resistance Model", section V "Radio Model", section VI "Design Requirement", section VII "Preliminaries", section

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

VIII "Proposed Scheme", section IX "Security Analysis", section X "Performance Analysis", and section XI "Conclusion "are elaborated.

2. RELATED WORK

In [7] the authors proposed ECC based setup of keys between body sensors and the gateway. Block cipher RC5 is proposed for the confidential flow and integrity of patients' physiological data. However, this approach is inefficient in computational cost and suffers from delay. A non-cryptographic solution BANA [8] for sensors authentication has been proposed where RSS is used to identify legal and illegal sensor nodes. While being non-cryptographic approach as off body attacker can easily forge in to network by creating a perfect channel. In [9] a hardware based design solution is proposed for the security of WBANs where light weight micro-controller is used to save energy. Patients' data is communicated using TDMA-MAC in system layout. This approach is evaluated on the basis of energy overhead. This hardware base solution could be expensive and the issue of energy overhead can be tackled by efficient cryptographic technique. In scheme [10] identification of neighbor sensors and PWH is performed using mutual authentication. This scheme proposes two types of keys, Individual key and pair wise key. Individual key is shared with PWH and pair wise key is shared with neighbor sensor node, however n (n-1)/2 keys are required for a body sensor with (n) neighbors. Polynomial key sharing and secret keys establishment among all sensors are costly in computation, memory and communication overhead. Selection of random Polynomial for secure private keys distribution in key generation process of [11] FABSC scheme, feature set exchange amongst all body sensors for establishing key sharing after to agree source and target transmission, if feature sets of sensor and targets are identical then can be easily targeted by the adversary launching replay attack. The authors in [12] have proposed a hybrid technique for secure key exchange using ECC is somehow cost efficient but lack of sensor authentication. Hybrid key agreement scheme [13] provides authentication and cluster head selection through rotation. This scheme is based on ECC and AES. Secret key exchange is performed using ECC and confidential data transmission to the MS, using AES. The cluster head selection and rotation leads to increased communication cost and battery power consumption as each sensor node has to reach to gateway through cluster head so one hope additional cost penalty occurs while gateway can be reached directly in a ward by each sensor node of the WBAN. In [14] the authors have proposed a solution for the security of WBAN using ECC-based signcryption and blowfish cipher. ECC-based signcryption is used for keys establishment and blowfish for confidential transmission of information.
The performance of the WBANs can be considerably improved by the design of a new key agreement frame work using HECC based signcryption.

3. NETWORK MODEL

The proposed model comprised of body sensors, gateway/base station and central medical server. WBAN architecture represented for the monitoring of physical status of the patients admitted in a hospital ward is illustrated in Figure. 1; where resource constraint sensors are deployed on the body of patients according to disease requirement. These sensors sense vital organs data of patients and route to BS via wireless infrastructure. BS collects sensors reading forward to MS for record and onward communicating to MO's smart phone for emergency medical treatment. BS and MS are rich in resources. All body sensors are in the communication range of the BS with in up to 10 meters distance and all sensors can be reached through by one or two hops, here cluster head need not to be created for the sake of cost efficiency i.e. to avoid cost consuming in receiving and transmitting of data. For interoperability of BS and sensors IEEE 802.15.6 is proposed. Upon adding or removing a sensor the network does not affect. MOs are the users of the network and the patients are the owners.

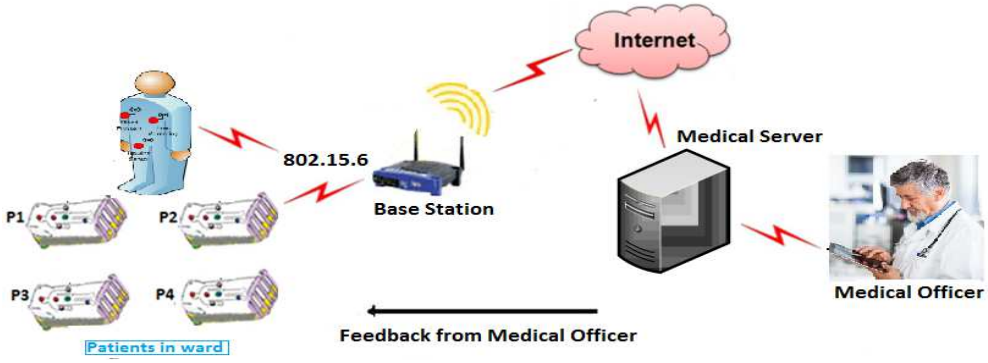

Figure 1. WBAN Architecture for Patients in a Ward of Medical Centre

4. Threat Resistance Modal. WBAN operates on vulnerable wireless channels and faces security risk. As important patients data travels through these wireless channels so its security is unavoidable. If this critical data is compromised by the attackers it can put precious human life at risk. To keep our system secure, authentication of sensors, secure key agreement, secure critical data communication, integrity of data and non-repudiation are mandatory. Low power, limited processing capability, limited memory and short communication range body sensors can't afford costly cryptographic solutions. Light weight but enough secure solution is required. Both the advantages of the symmetric and asymmetric can be cashed by using a cost effective secure hybrid technique. Keys updating can block the attacker from using old keys and guessing new keys for unwanted operation. Keys are updated round wise while three rounds are undertaken per day each of eight hours.

5. Radio Modal. First order radio model [15] is proposed in our scheme for transmitting patients' physiological data over wireless channel in WBANs. Energy consumed during data transmission by the body sensors is $\mathrm{E_t}(l,d)$.

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

Where transmitted energy E_t, length of message l, communication distance d, energy consumption per bit E_{elec} =$50nJ/bit$, $d_0 = 100\mathrm{m}$ and free space model amplifier energy factor $\varepsilon = \varepsilon_{\mathrm{fs}}$ =10 pJ/bit/m^2.

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 include body sensor authentication, secure key agreement, confidentiality of information, patients data integrity, keys update, cost and energy efficiency, network scalability and data freshness.

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

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

And there are no points which simultaneously satisfy equation (2) and the partial derivate equations (3) and (4) of equation (2)

$$2y + h(x) = 0 \qquad (3)$$
$$h(x)'y - f(x)' = 0 \qquad (4)$$

A divisor D is a finite formal sum of points $P_i = (x_i, y_i) \in \mathbb{C}, D = \sum m_i P_i$, $P_i \in C, m_i \in Fq$. A reduced divisors $D = \sum m_i P_i - (\sum m_i)\infty$ where $P_i = (x_i, y_i)$ is a point on $\mathbb{C}$ and m_i is the order of P_i is represented as a pair of polynomials$a(x), b(x)$, as $D = (a(x), b(x))$

Jacobian $\mathrm{J_c(Fq)}$is finite group such that every element in $\mathrm{J_c(Fq)}$ is an equivalence class of reduced divisor. The order of the Jacobian $\#\mathrm{J_c(Fq)}$

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

8. Proposed Scheme. The topological structure of the proposed network consists of biosensors, BS and MS as is shown in figure.1.
Our proposed framework has the following phases.

- WBAN Initialization Phase
- Session Key Establishment Phase
- Secure Session Data Transmission Phase
- Key Update Phase

Table 2 Notation Guide

Symbols	Description
S_i	Body sensor/Biosensor node i
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
k_h	Keyed hash function
E_k/D_k	Symmetric Encryption / Decryption with key k
m/c	Message/Cipher text

8.1. WBAN Initialization Phase. In this phase, each body sensor S_i is preloaded with private key d_{bs}, and MS public key P_{ms} prior to deployment on patients body. Private Key d_{ms} and public keys P_{ms} are preloaded to MS along with public keys P_{bs} of all body sensors.

8.2. Session Key Establishment Phase. In this phase, session key is generated round wise and exchanged securely between body sensors and MS using cost effective primitive signcryption for onward secure patient's data communication. Probalistic Signcryption(P_{ms}, d_{bs}, P_{bs}) algorith 1 is use to generate signcrypted text for session key (S_k).

ALGORITHM 1: Signcryption(P_{ms}, d_{bs}, P_{bs})

1. Select a Random integer $k \in \{1,2,\dots n-1\}$
2. Computes $k(P_{ms})$
3. Computes $(K_1, K_2) = h(\varphi(k(P_{ms})))$
4. Generate session key S_k
5. $c = E_{K_1}(S_k)$
6. Computes $r = kh(c||K_2)$
7. Computes $s = \left(\frac{k}{(r+d_{bs})}\right) mod\ n$
8. Transmit Signcrypted text (c, r, s) to MS

End

MS obtain biosensor public key from certificate authority. Determnsitic Unsigncryption $(P_{ms}, P_{bs}, d_{ms}, c, r, s)$ Algorithm 2 is used to obtain session key (S_k) from signcrypted text(c, r, s).

ALGORITHM 2: Unsigncryption $(P_{ms}, P_{bs}, d_{ms}, c, r, s)$

1. Computes $sd_{ms}(P_{bs} + rD)$
2. Computes $(K_1, K_2) = h((\varphi(sd_{ms}(P_{bs} + rD))$
3. Computes $r' = kh(c||K_2)$
4. Computes $(S_k) = D_{K_1}(c)$
5. Check $r = r'$, if satisfied accept the session key, otherwise reject

End

8.2.1. Proofs for Decryption

$$\mathrm{u}(\mathrm{P_{bs}} + \mathrm{rD}) = sd_{ms}(P_{bs} + rD) = \left(\frac{k}{(r + d_{bs})}\right) d_{ms}(P_{bs} + rD)$$

$$= \frac{kd_{ms}(P_{bs} + rD)}{(r + d_{bs})} = \frac{kd_{ms}P_{bs} + kd_{ms}rD}{(r + d_{bs})} = \frac{d_{bs}kP_{ms} + kd_{ms}rD}{(r + d_{bs})} = \frac{d_{bs}kP_{ms} + rkd_{ms}D}{(r + d_{bs})}$$

$$= \frac{d_{bs}kP_{ms} + rkP_{ms}}{(r + d_{bs})} = \frac{kP_{ms}(d_{bs} + r)}{(r + d_{bs})} = kP_{ms}$$

8.3. Secure Session Data Transmission Phase. The hash of patients' physiological data m_{ri} sensed by body sensors s_i is taken for computing hash value ri then the hash value ri and sensed data m_{ri} are encrypted to compute cipher text c_i for sending to medical officer via BS and MS for hurried treatment. Algorithm 3 is used for the secure transmission of patients' data.

ALGORITHM 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

End

8.4. Key Update Phase. The important feature of our solution is round wise updating of session keys to block cryptanalyst attack while getting advantage of old keys. Fresh keys guarantee forward and backward secrecy of information which significantly reduce the chance of misuse of patients' personnel data from body sensors to the decision maker MO. The proposed Algorithm 4 updates session key at the end of each round both on body sensors and MS in such a way that the hash of last data of a round m_{ri-1} is computed and then XOR of the last round secret session key $Sk_{r_{i-1}}$ and last data of a round m_{ri-1} is taken to compute fresh secret session keySk_{ri}, where three rounds are taken in twenty four hour each of eight hours. Round (Rd) starts if Rd= 11 and ends on Rd=00.

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 dissemination of patient information from body sensors to the Medical Server is of prime importance. Our proposed scheme ensures the necessary prominent security notions of confidentiality, Integrity, authenticity, Un-forgeability and non-repudiation of patient information. Security function is dependent on Hyper Elliptic Curve Discrete Log Problem (HECDLP), which is a hard problem (Computationally infeasible) [16].

Definition (HECDLP) Let D_1 *and* D_2 are devisor in the Jacobian group such that order of D_1 is n, find an

integer $k, 1 \leq k \leq n-1$ such that $D_2 = \mathrm{kD}_1$.

9.1. Confidentiality. The privacy of patient health information is crucial and it should not be eavesdrop (***Evo***). To assure privacy, proposed system confidentially exchanges the session key and communicates the session data using symmetric cipher AES. The possible attacks are demonstrated in Session key Agreement and secure data transmission and it is concluded that the proposed scheme provide confidentiality.

Case 1: An Evo can compute patient session keys (K_1, K_2) from Equation (1) if he gets d_{ms} from Equation (2), while computing d_{ms} from Equation (2) is Equivalent to solve one computationally infeasible $HCDLP$

$$(K_1, K_2) = h((\varphi(s\, d_{ms}(P_{bs} + rD)) \quad (1)$$

$$P_{ms} = d_{ms}.D \quad (2)$$

Case 2: An Evo can compute patient session keys (K_1, K_2) from Equation (3) and (4), if he gets d_{bs} from Equation (5), while computing d_{bs} from Equation (5) is Equivalent to solve one computationally infeasible $HCDLP$.

$$(K_1, K_2) = h\left(\varphi(k(P_{ms}))\right) \quad (3)$$

$$s = \left(\frac{k}{(r + d_{bs})}\right) mod\ n \quad (4)$$

$$P_{bs} = d_{bs}.D \quad (5)$$

Case 3: An Evo want to obtain patient session information m_{ri} from ciphertext c_i. AES is used as encryption algorithm so computing m_{ri} from c_i is computationally infeasible as AES is resists IND-CMA and IND-CCA.

$$c_i = \mathrm{E}_{S_k}(m_{ri}, ri) \quad (6)$$

9.2. Integrity. Proposed scheme ensures that the patient data have not been altered by ***Evo*** received at MS. In key exchange phase patient computes $\boldsymbol{r = h_k(c||K_2)}$ using one-way hash function. If ***Evo*** change the original information $\boldsymbol{c}$ as $\boldsymbol{c'}$, $\boldsymbol{r}$ is changed to $\boldsymbol{r' = h_k(c'||K_2)}$. Similarly patient encrypted information is Computes as $\boldsymbol{ri = h(m_{ri})}$. It is infeasible for an attacker to modify $\boldsymbol{c}$ as $\boldsymbol{c'}$ such that $\boldsymbol{r' = r\ and\ ri' = ri}$ due to collision resistive property of hash function.

9.3. Authenticity. Authenticity ensures the information is sent by the legitimate actual originator of data where from data flows. Medical server authenticate biosensor public key by using their certificate. And use that public key to derive session key.

9.4. Unforgeability. The ***Evo*** can not forge valid $\boldsymbol{(c, r, s)}$ without private key of the biosensor. Let an ***Evo*** attempt to forge, he must generate $\boldsymbol{s'}$ from Equation (14) for $\boldsymbol{c'}$. For computing valid signature $\boldsymbol{s'}$, he has to compute biosensor private key $\boldsymbol{P_{bs}}$ from Equation (5) which is equivalent to solve ***HECDLP***.

9.5. Non repudiation. Non repudiation warrants that both of the patients can't deny their sent information in WBANs. In case of dispute Judge/ Third party can decide that whether the message is sent by the claimed biosensor or not.

10. Performance Analysis. Biosensors have limited memory, processing capability and energy. On the basis of these parameters we analyze our scheme with existing schemes presented in the literature [7], [8], [10]. The advantage of proposed scheme is obvious from it efficiency compare to existing schemes.

10.1. Computational Cost Analysis. In established public key cryptosystem, the expensive and major operations are Modular Exponentiation (M-Exp), ECC Point multiplication (ECPM) and HEC Divisor Scalar Multiplication (HECDM). A single scalar multiplication is observed to have been consuming 469.96 ms for (ECPM) and 316.6 ms for (HECDM) on ARM @ 50MHz processor. Analysis shows that our scheme is cost efficient and best suitable for the resource constraint environment of WBANs. The result is presented in Fig 2.

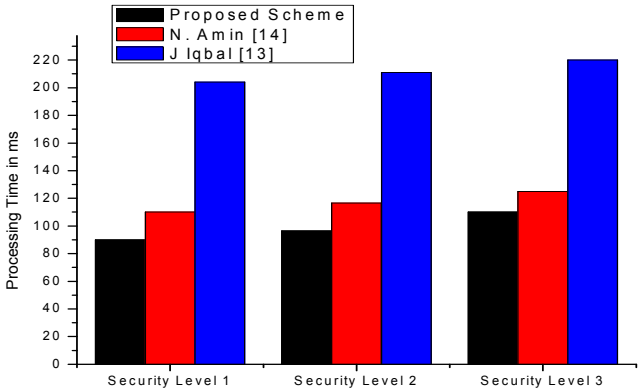

Figure 2. Computational Cost Comparison

10.2. Communication Overhead Analysis. Energy consumption of transmission is proximately 1000 time high than computation cost. The communication efficiency of our solution depends on the shorter key size and parameters of HECC. On the basis of NIST standard choice of parameters, our scheme is cost efficient in bandwidth utilization then existing schemes as shown in Figure.3.

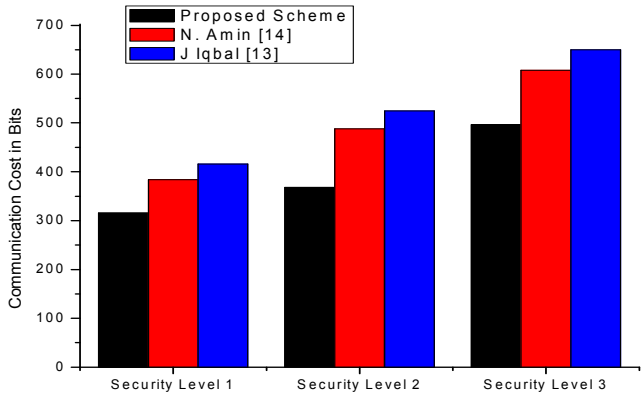

Figure 3.Communication Cost comparison

10.3. Memory Storage Cost. HECC is superior over ECC and RSA due to shorter key size as key bits length of RSA is 1024, ECC is 160 and HECC is 80. Due to significant reduction of key bits, our scheme presents the economy of storage. The storage comparison of proposed scheme and other existing schemes is presented In Figure.4

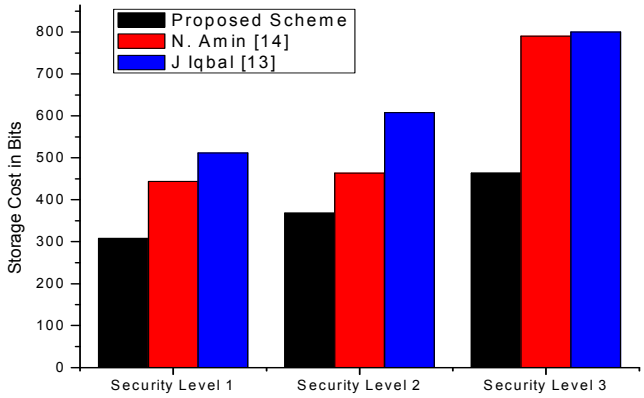

Figure 4. Storage Cost Comparison

11. Conclusion. This paper addresses the key issue of WBANs security while using HECC based signcryption which significantly out performs as compare to other cryptographic solutions. In our novel key agreement frame work HECC 80 bits base filed offer the same security level with enough lower computation, communication and storage cost. One hop reduction due to avoidance of cluster head increases overall performance of the network. The performance analysis of our proposed scheme with others depicted in graphs clearly proves the appropriateness of our framework for the resource constrained environment of WBANs.

REFERENCES

[1] 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.

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

[3] 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.

[4] Zheng, Y. (1997). Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption). In *Advances in Cryptology—CRYPTO'97* (pp. 165-179). Springer Berlin Heidelberg.

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

[6] Nizamuddin, N., Ch, S. A., & Amin, N. (2011, December). Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In*High Capacity Optical Networks and Enabling Technologies (HONET), 2011*(pp. 244-247). IEEE.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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)*.

[14] N. Amin, J. Iqbal, and A. R. Abbasi, "Secure Key Establishment and Cluster Head Selection for Body Area Networks Based on Signcryption," *J. Appl. Environ. Biol. Sci.,* vol. 4, no.7, pp 210-216, 2014.

[15] 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.

[16] 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.