J. Appl. Environ. Biol. Sci., 6(5S)64-72, 2016

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

Public Verifiable Signcryption and Cluster Head Selection for Body Sensor Networks

Jawaid Iqbal[1], Noor Ul Amin[1], Arif Iqbal Umar[1], Nizamuddin[2]

[1]Department of Information Technology, Hazara University Mansehra Pakistan
[2]Iqra National University Peshawar Pakistan

Received: February 3, 2016
Accepted: April 12, 2016

ABSTRACT

Signcryption is the logical combination of the signature and encryption which provides sender authentication and confidentiality. Authenticity of a sender can only be proved after unsigncrypting the signcrypted message. A judge or third party can only prove the authenticity of sender after infringing the confidentiality. The advantage of public verifiable signcryption is that a third party or judge can prove authenticity of a sender without infringing the confidentiality or getting the private key of the receiver. Third party just needs the signcrypted message and some other parameters. In this work we have proposed a public verifiable signcryption based scheme which satify the necessary security parameters along with public verifiability. Cluster head selection is performed by rotating the cluster head on the basis of the energy level. This scheme is efficient for the resource constrained environment of Body Sensor Networks.

KEYWORDS: Hyper Elliptic Curve Cryptography; Signcryption, AES; Clustering; Public Verifiability.

1. INTRODUCTION

Body Sensor Networks (BSNs) are special type of WSN in which tiny biosensors deployed inside/outside of a human body to monitor vital signs like EEG, ECG, EMG, blood pressure, body temperature for early finding of the different diseases of human body along with reducing the healthcare costs.

BSNs deal with sensitive physiological information which need of strong secure cryptographic functions (i.e. encryption, authentication, integrity , public verifiability etc) to protect patient information against malicious attacks data can only be accessed by the legal users and securely transferred and stored in medical server. Strong security requires extensive resources which is not optimal for BSNs so light weight cryptographic solutions are required. Secure key management and distribution along with efficient cluster head selection and rotation is required to minimize the cost and increase BSN life time.

These two separate algorithms of data encryption and digital signatures are joint into a single operation called

signcryption by Y. Zheng [1].

HECC is suitable cryptosystem for resource constraint environment of BSNs as compared to other cryptographic techniques, due to shorter parameters of HECC which provide equal security as compared to other public key infrastructure algorithms. HECC used 2^{80} bits key, ECC 2^{160} bits and RSA 2^{1024} bits in our proposed scheme selection of efficient CH will improve the overall performance of BSNs.

$$\mathbb{C}: y^2 + h(x)y = f(x) \quad (1)$$
$$2y + h(x) = 0 \quad (2)$$
$$h(x)'y - f(x)' = 0 \quad (3)$$

The order of the Jacobian $\#\mathrm{J_c(Fq)}$

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

2. **Related Work**. A BSNs is used to collect sensitive data from bodies used for multiple purposes. An in depth literature review exposed contributions and limitations of the schemes discussed in this section.

In scheme [2] energy saving routing architecture with a uniform clustering algorithm for WBSNS is used. In which authors mainly focus to balance the traffic load between clusters along to reduce information transmission distance to cluster head but the selection method of cluster head in proposed model is not

* **Corresponding Author:** Jawaid Iqbal, Department of Information Technology, Hazara University Mansehra Pakistan. jawaid5825@gmail.com

suitable for BSN because centralized approach consume more energy. In scheme[3] a new approach LAEEBA (Link-aware and Energy Efficient scheme for Body Sensor Networks) is used which used single-hop as well as multi-hop communication channel for data transmission to increase the network life time. The limitation of the proposed scheme is that only two selected node communicate with sink and failure of two nodes can down the entire network. In scheme [4] a novel algorithm for energy saving SECA is established to overcome the energy consumption problems in WSN. SECA is used to obtained uniform cluster algorithm to computes efficient routing for data transmission from sensors to sink node. The main flaw of the scheme is lack of data security. In scheme [5] a new clustering algorithm is proposed to enhance the network life time of WSN. In proposed scheme randomly Cluster Head (CH) is selected which is suitable for data transmission to a long distance. Randomly selection of CH is suitable for increasing the overall efficiency of the network. The main drawback of the scheme is traffic balance overhead and quality of services. In scheme [6] proposed a new data dissemination protocol for wireless body to body communication in BSN which is basically consist of two approaches one is distributed and second is cluster based approach. Exceed from the predefine standard range of WBSNs which is limitation of the scheme. In scheme [7] proposed new routing algorithm which have capability to support mobility and selection of CH on the basis of residual energy plus its distance from base station. The biosensor node with slightest cost function value is selected as forwarder. It is only suitable for single body one tier architecture scheme which shortcoming of the proposed scheme. In scheme [8] IEEE 802.15.6 standard is defined which is specially design both for medical and non-medical applications**.** It consists on three levels between sensor nodes and BS. No security, authentication level and encryption levels. Security services concentrate on key generation, key distribution along with message authentication. Diffie–Hellman key technique is used for the generation and distribution of keys, MAC for message authentication and AES for ciphering of data. In scheme[9] efficient key management technique is proposed using public key infrastructure RSA and DHECC for WSN which is not suitable for resource constraint environment of BSN due to high cost . In scheme [10] a novel hybrid technique is proposed for secure patient information from source node (biosensor nodes) to target position (medical server) using RSA and symmetric cipher which is inefficient for BSN due to long key size.

3. **Proposed Scheme**. The proposed network model consist of body sensor, base station and medical sever as is shown in figure.1. We assume that the body sensor nodes have limited resources while base station has high.

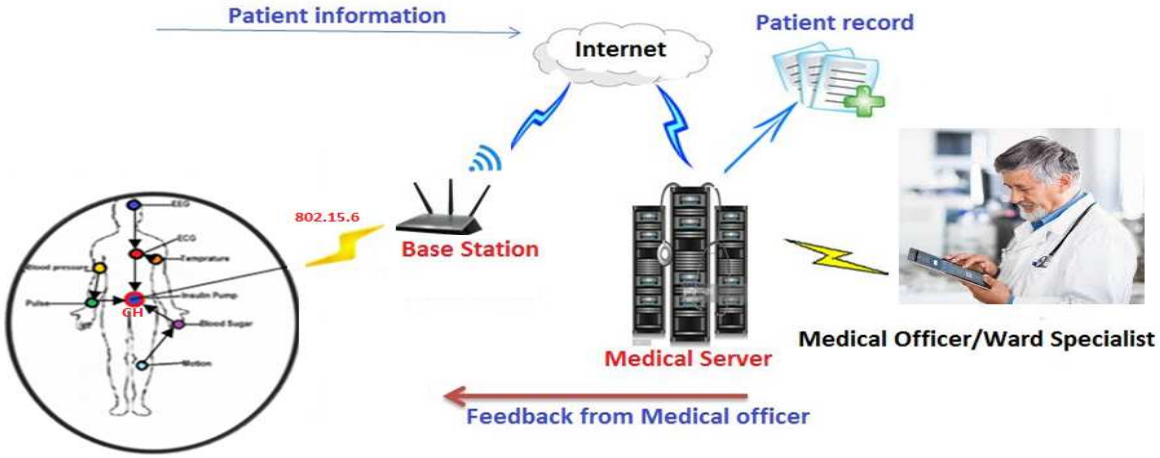

Figure 1. Network Model of Proposed Scheme

Our proposed scheme has the following phases.

- Initialization Phase
- Secret Session Key Establishment Phase
- Public Verifiability Phase
- Cluster Head Selection Phase
- Secure Data Tranmission Phase
- Cluster Head Rotation Phase
- Key updating Phase

P ublic parameters are shown in Table 1.

Table1. Notation Guide

Notation	Description
S_i	Body sensor/Biosensor node i
$\mathbb{C}$	Hyper Elliptic Curve
D	A divisor of large prime order n in $J_c(Fq)$, $n \geq 2^{80}$
φ	A function which map a divisor to integer value
EL_{S_i}	Energy level of sensor node i
Pu_{BS},	Public key of base station
Pr_{BS}	Private key of base station
Pu_{si},	Public key of biosensor node
Pr_{si}	Private key of biosensor node
k_{pi}	Secret session key
E_k/D_k	Encryption / Decryption with key k
h / h_k	Hash / Keyed Hash Function
m/c	Message/Cipher text
M-EXP	Modular Exponentiation
ECPM	Elliptic Curve Point Multiplication
$\perp$	Reject

3.1. **Initialization Phase**. Initially private and public keys of BS (Pr_{BS}, Pu_{BS}) are preloaded on BS, private key Pr_{si}, public key Pu_{si} of biosensor node along with Pu_{BS} are preloaded on sensor node and then sensor nodes are deployed in body of the patient to continuously monitor vital sign of human body. All deployed S_i public key (Pu_{si}) is also forwarded to BS as well.

3.2. **Secret Session Key Establishment Phase.**

In this section secret session key is established among each body sensor and related BS using Signcryption[11]. To achieve the above task algorithm (1) is performed:

Bio Sensor

1. Each bio sensor S_i on patient P_i generates a random number r_{si} where $i \in \{1,2,3, \ldots n-1\}$
2. Each bio sensor S_i on patient P_i has energy level EL_{S_i}

ALGORITHM 1: Signcryption$(d, r_{si}, EL_{S_i}, Pu_{BS}, Pr_{si}, Pu_{si})$

a. Select an integer $d \in \{1, 2, \ldots n-1\}$
b. Computes $K_1 = d.D$
c. Computes $K_2 = D.\ Pu_{BS}$
d. Computes $r = h(K_1 || r_{si} || EL_{S_i})$
e. Computes $c = E_{k2}(r_{si} || EL_{S_i})$
f. Computes $s = \left(\frac{d}{(r + Pr_{si})}\right) mod\ n$
g. Computes $z = r.D$
h. Forwarded signcrypted text (c, z, s) to BS

Base Station

BS Unsigncrypt the Signcrypted text (c, z, s)received from each biosensor S_i using algorithm(2)

ALGORITHM 2: Unsigncryption $(Pu_{BS}, Pu_{si}, Pr_{BS}, c, z, s)$

a. Computes (K_1, K_2)
b. $K_1 = s(Pr_{BS} + z)$
c. $K_2 = s(Pu_{si}(Pr_{BS} + z))$
d. Computes $(r_{si} || EL_{S_i}) = D_{K_2}(c)$
e. Check $r.D = z$ if satisfied accept the random number r_{si} and energy level EL_{S_i}otherwise reject
f. BS computes round session key k_{P_i} for patient p_i by selecting two r_{si} from those bio sensor S_i installed on same patient p_i as: $k_{P_i} = r_{si} \oplus r_{s\,i+1}$

ALGORITHM 3: P-Verify

Public Verifiability

a. Computes $(K_1) = h(\varphi(s(Pr_{BS}+z)))$
b. Computes $r = h(K_1||r_{si}||EL_{S_i})$
c. Computes $z = r.D$
d. If satisfied the signcrypted text is legitimate, otherwise not

The proposed scheme is public verifiable where third party can easily verify the signcrypted message without knowing the sender or receiver private keys whenever any dispute occurs.

Judge Verification

In public verifiable signcryption schemes a third party or judge can verify authenticity of sender without breaching the confidentiality and without knowing the receiver private key, the judge just needs the signcrypted text and some additional parameters

Third party wants BS to provide (c, $Pu_{BS,}$ s, z) and subsequent steps to adjust the BS claim.

Cluster Head Selection Phase

To enhance the life time of BSNs along with decresing the transmission cost base station select cluster head for data forwarding to base station and then medical server using algorithm(4) and Cluster Head Selection process shown in figure.2

Base station

ALGORITHM 4: Cluster Head Selection

a. Computing the highest energy level sensor node from all deployed senor nodes on patient body (EL_{S_1}, EL_{S_2} ….EL_{S_t})
b. Select cluster head CH_{Si} having maximum energy
c. Remaining sensor nodes become cluster members of that cluster
d. Where $ID_{CH_{Si}}$ is address of Cluster head CH_{Si}
e. ID_{si} is address of cluster member CM_{Si}
f. Symmetric encryption using AES algorithm
g. $c = E_{r_{si}}(k_{pi}||CH_{Si}||ID_{csi})$
h. Transmit encrypted text c to bio sensor Si

Bio Sensor

ALGORITHM 5: Decryption encoded message (c)

1. All deployed biosensor nodes S_i get the encoded message (c)
2. Then decrypts (c) using AES algorithms and key r_{si} as:
   a. $k_{pi}||CH_{Si}||ID_{csi} = D_{r_{si}}(c)$
   b. All cluster member CM_{Si} transmit join request messages to CH_{Si}

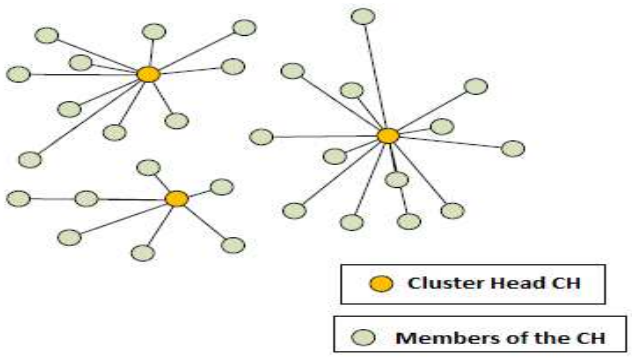

Figure 2. Cluster Head and Members of CH

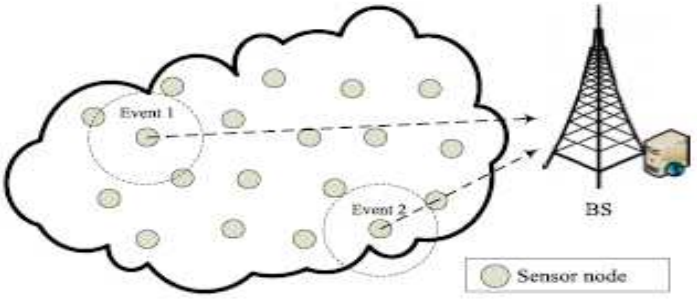

Figure 3. Direct communication protocol inWSN

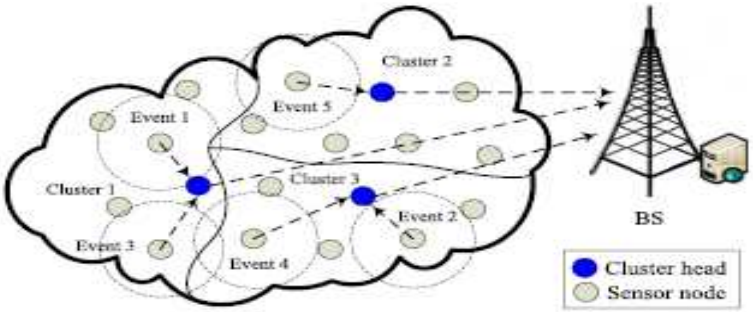

Figure 4. Cluster base routing protocol in WSN

3.3. **Secure Data Transmission Phase**

Secure transmission of patient biological data using wireless channel from source node to target node is very essential in BSN to protect patient information from different attacks.

Biosensor

ALGORITHM 6: Secure Data Transmission

For each biosensor node $S_i \in P_i$

a. Sense patient data M_{ri}
b. Computes $D_i = \text{HASH}(M_{ri})$
c. Computes $c_{ri} = E_{r_{si}}(M_{ri}, D_i)$
d. Transmit c_{ri} to BS

End for

Base station

ALGORITHM 7: Decryption (c_{ri})

for each body sensor encrypted data $c_{ri} \in P_i$

a. $(M_{ri}, D_i) = D_{r_{si}}$ (c_{ri})
b. Computes $D_i' = \text{HASH}(M_{ri})$
c. Accept if $D_i' = D_i$ Save data to patient P_i record otherwise $\perp$

End for

3.4. **Cluster Head Rotation Phase**

To increase the life time of BSNs cluster head is rotated,when the CH energy level reached to a threshold value. The node have maximum energy is Reselect CH uing algorithm(8).

Biosensor

ALGORITHM 8: Cluster Head Rotation Phase

a. All body sensor nodes transmit energy level in encrypted form to BS
b. $c = E_{r_{si}}(EL_{S_i})$
c. Forwarded cipher text c to BS

Base Station

ALGORITHM 9: Decrption (c)

a. Computes $EL_{S_i} = \mathrm{D}_{\mathrm{r_{si}}}(c)$
b. Select one node as a cluster head $\mathrm{CH_{Si}}$ having highest energy (EL_{S_1}, EL_{S_2} ….EL_{S_t})
c. The remaining sensor nodes become member of that cluster
d. Where $\mathrm{ID_{CH_{Si}}}$ is address of Cluster head $\mathrm{CH_{Si}}$
e. $\mathrm{ID_{si}}$ is address of cluster member $\mathrm{CM_{Si}}$
f. Symmetric encryption using AES algorithm
g. $c = \mathrm{E_{r_{si}}}(\mathrm{CH_{Si}} \,||\mathrm{ID_{csi}})$
h. Transmit encrypted text c to bio sensor Si

Bio Sensor

*ALGORITHM 10***:** Decrypt (c)

a. $(\mathrm{CH_{Si}} \,||\mathrm{ID_{csi}}) = \mathrm{D_{r_{si}}(c)}$
b. Then cluster member $\mathrm{CM_{Si}}$ forwarding join request messages to $\mathrm{CH_{Si}}$

End

3.5. **Key Updating Phase**

Key updating is required after each session to protect patient information from modification/illegal usage. forward secrecy and backward secrecy is ensure using key updating algorithm(11).

Bio Sensor

Each sensor nodes $\mathrm{S_i}$ on patient P_i generates a random number r_{si}' where $\mathrm{i} \in \{1,2,3, \ldots \mathrm{n}-1\}$

ALGORITHM 11: Signcryption$(\mathrm{d}, r_{si}', \mathrm{Pu_{BS}}, \mathrm{Pr_{si}}, \mathrm{Pu_{si}})$

i. Select an integer $d \in \{1, 2, \ldots n-1\}$
j. Computes $K_1 = \mathrm{d.D}$
k. Computes $K_2 = \mathrm{D.\ Pu_{BS}}$
l. Computes $r = h(K_1 || r_{si}')$
m. Computes $c = E_{k2}(r_{si}')$
n. Computes $s = \left(\frac{d}{(r+\mathrm{Pr_{si}})}\right) mod\ n$
o. Computes $z = r.D$
p. Forwarded signcrypted text $(\mathrm{c, z, s})$ to BS

Base Station

BS unsigncrypt the signcrypted text (c, z, s)received from each biosensor $\mathrm{S_i}$ using algorithm(12)

*ALGORITHM 12***:** Unsigncryption $(\mathrm{Pu_{BS}}, \mathrm{Pu_{si}}, \mathrm{Pr_{BS}}, \mathrm{c, z, s})$

a. Computes (K_1, K_2)
b. $K_1 = s(\mathrm{Pr_{BS}} + z)$
c. $K_2 = s(\mathrm{Pu_{si}}(\mathrm{Pr_{BS}} + z))$
d. Computes $(r_{si}') = D_{K_2}(c)$
e. Check $r.D = z$ if satisfied accept the random number $\mathrm{r_{si}}$ otherwise $\perp$
f. BS computes round session key $\mathrm{k_{pi}}'$ for patient $\mathrm{p_i}$
g. Selecting two r_{si}' from those bio sensor $\mathrm{S_i}$ installed on same patient $\mathrm{p_i}$ as:
h. $\mathrm{k_{pi}}' = r_{si}' \oplus r_{si}'_{+1}$

4. **Objective of Proposed Scheme.** To fill the research gaps identified in the relevant literature we establish efficient key agreement and cluster head selection and rotation technique along with public verifiability with low routing overhead, less energy and computation cost to increase network life time.

   Our proposed efficient key agreement and cluster head selection and rotation routing protocol based on HECC make BSNs communication more efficient which consume less energy for data transmission and optimally bandwidth utilization of the BSN.

   We reduce space problem in our proposed scheme using HECC for key agreement as compare to other schemes and achieved efficiency with significant reduction in computational and communication cost.

5. **Security Analysis**. Our proposed scheme satisfied following BANs security requirements for secure session data transmission and key agreement [12].

5.1. **Confidentiality.** The security of patient vital sign is very essential in resource constraint environment of BSNs. In our proposed scheme symmetric cipher AES is used to ensure confidentiality of patient information and HECC is used for confidential distribution of secret key during each session.

5.2. **Integrity.** In our scheme Integrity is used to check either the data is original or modified. In our proposed sachem HEC signcryption routine and one way Hash function is used to ensure data integrity.

5.3. **Authentication.** In BSNs patients data are transmitted using wireless channel which are easily vulnerable to the attacker. Authentication process is needed to prove the validity of data/node. In session key establishment phase authenticity is ensure using HEC signcryption Three are two types of authentication which are discussed below:

5.4. **Node authentication**. In node authentication check the identity of the sensor node either it is valid or not. If sensor node is legitimate so it will join the networks otherwise blacklisted and isolated from the networks.

5.5. **Data authentication**.In data authentication receiver verify that the data was sent really by the claimed user are not. If it is valid so it will be store on medical data base and use for further analysis otherwise discard. Authentication is used to avoid impersonation attacks.

5.6. **Data Freshness.** Data freshness is the important property of cryptography to ensure that received patient information are not replayed and created newly. Data freshness play important role in BSNs where session key technique used for secure session data transmission.

5.7. **Node Capture.** In our scheme when attacker hack/get session key, BS has the capability to sense it and create new session key .in ou proposed key updating phase forward secrecy ensure node capturing properties.

5.8. **Scalability.** In proposed scheme has the aptitude to control significant increase/decrease in size of network after biosensor nodes deployment in our proposed initialization phase[13].

5.9.**Backward and Forward Secrecy.** Our scheme ensure backward and forward secrecy [14][15] using key updating phase.

Table 2. Security Properties in Communication Protocols

Protocol	Bluetooth	Zigbee	TG6
Confidentiality	Yes	Yes	Yes
Integrity	No	No	Yes
Non Repudiation	No	No	No
Authentication	Yes	Yes	Yes
Authorization	No	No	No

6. **Cost Analysis.** In our proposed cost analysis section we discuss memory requirement for keys storage, processing cost of CPU and communication delay in detail.

6.1. **Space Analysis for storing Keys.** NIST recommended secure key size for different cryptosystem is shown in the given table. In our proposed scheme we used HECC with shorter key size $2^{80}$and AES with 128 bits for security purposes. Figure (5) indicates memory requirement analysis of our proposed scheme with other schemes.

Table 3. NIST Recommended Key Size

Symmetric Cryptosystem	RSA and Diffie-Hellman	Elliptic Curve	Hyper Elliptic Curve
80	1024	160	80
112	2048	224	112
128	3072	256	128
192	7680	384	192
256	15360	512	256

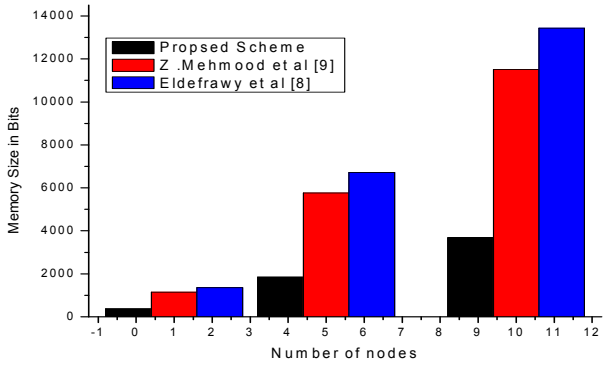

Figure 5. Space requirement for key storage

6.2. **Processing Cost Analysis.** In our proposed scheme used HECC instead other expensive public key infrastructure (RSA, Diffie-Hellman) which sufficiently decreased the processing cost shown in figure(6).

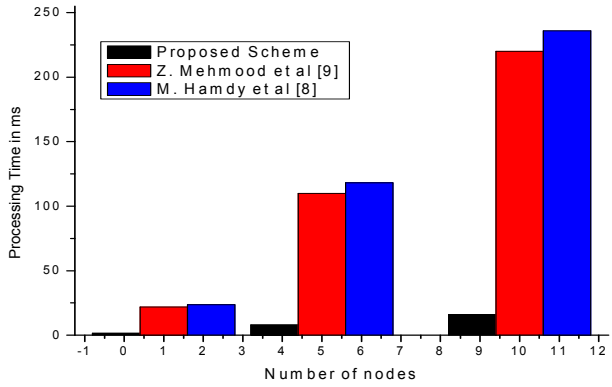

Figure 6. Processing Cost for Computation

6.3. **Communication Delay Analysis.**In proposed scheme bandwidth is efficiently utilized because we used light weighted cryptosystem (HECC). Figure (7) indicate communication delay analysis of proposed scheme and existing schemes.

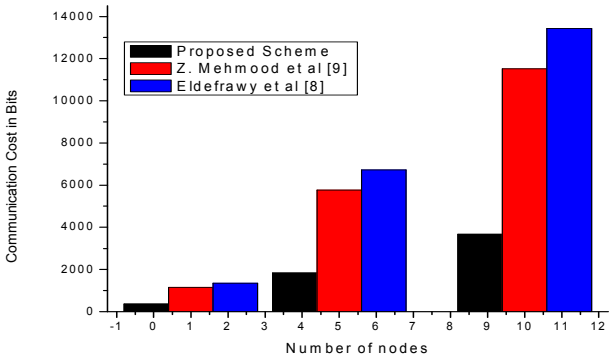

Figure 7. Communication Delay Analysis

7. **Conclusion**. The proposed scheme is public verifiable where third party can easily verify the signcrypted message without knowing the sender or receiver private keys whenever any dispute occurs. The energy level of the sensors are leveled by rotating the cluster head. The efficiency and security of this scheme proves it feasible for the resource constraint environment of body sensor networks.

REFERENCES

[1] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)," in *Advances in Cryptology—CRYPTO'97*, 1997, pp. 165–179.

[2] J.-Y. Chang and P.-H. Ju, "An energy-saving routing architecture with a uniform clustering algorithm for wireless body sensor networks," *Futur. Gener. Comput. Syst.*, vol. 35, pp. 128–140, 2014.

[3] S. Ahmed, N. Javaid, M. Akbar, A. Iqbal, Z. A. Khan, and U. Qasim, "LAEEBA: Link aware and energy efficient scheme for body area networks," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 435–440, 2014.

[4] J. Chang and P. Ju, "An efficient cluster-based power saving scheme for wireless sensor networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 172, pp. 1–10, 2012.

[5] S. Babaie, A. K. Zadeh, and M. G. Amiri, "The new clustering algorithm with cluster members bounds for energy dissipation avoidance in wireless sensor network," *2010 Int. Conf. Comput. Des. Appl. ICCDA 2010*, vol. 2, no. Iccda, pp. 3–7, 2010.

[6] D. Ben Arbia, M. M. Alam, R. Attia, and E. Ben Hamida, "Data Dissemination Strategies for Emerging Wireless Body-to-Body Networks based Internet of Humans," *11th IEEE WiMob Conf. Second Int. Work. Emergenc y Networks Public Prot. Disaster Reli. EN4PPDR*, pp. 1–8, 2015.

[7] N. Javaid, A. Ahmad, Q. Nadeem, M. Imran, and N. Haider, "IM-SIMPLE: IMproved stable increased-throughput multi-hop link efficient routing protocol for Wireless Body Area Networks," *Comput. Human Behav.*, vol. 51, pp. 1003–1011, 2014.

[8] X. Cai, F. Fan, X. F. Li, B. Q. Pei, H. J. Niu, and Y. B. Fan, "6th European Conference of the International Federation for Medical and Biological Engineering," *IFMBE Proc.*, vol. 45, pp. 162–165, 2015.

[9] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography," *Anti-Counterfeiting Secur. Identif. Commun. (ASID), 2010 Int. Conf.*, pp. 1–6, 2010.

[10] Z. Mehmood, Nizamuddin, S. Ashraf Ch., W. Nasar, and A. Ghani, "An efficient key agreement with rekeying for secured body sensor networks," *2012 2nd Int. Conf. Digit. Inf. Process. Commun. ICDIPC 2012*, pp. 164–167, 2012.

[11] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Inf. Process. Lett.*, vol. 68, no. 5, pp. 227–233, Dec. 1998.

[12] N. Amin and M. Asad, "An Authenticated Key Agreement with Rekeying for Secured Body Sensor Networks Based on Hybrid Cryptosystem," pp. 118–121, 2012.

[13] J. Iqbal, N. U. Amin, and A. I. Umar, "Authenticated key agreement and cluster head selection for Wireless Body Area Networks," *2nd Natl. Conf. Inf. Assur.*, pp. 113–117, 2013.

[14] Nizamuddin, S. A. Ch., and N. Amin, "Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem," in *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, 2011, pp. 244–247.

[15] S. Ashraf Ch, Nizamuddin, and M. Sher, "Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem," *Commun. Comput. Inf. Sci.*, vol. 285 CCIS, pp. 135–142, 2012.