J. Appl. Environ. Biol. Sci., 4(7S)210-216, 2014

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

Secure Key Establishment and Cluster Head Selection for Body Area Networks Based on Signcryption

Noor Ul Amin, Jawaid Iqbal, Arifa Rasheed Abbasi, Nizamuddin, Asfandyar-Khan

Department of Information Technology, Hazara University, Mansehra, Pakistan

Received: September 1, 2014
Accepted: November 13, 2014

ABSTRACT

Body Area Network (BAN) has been using in medical for monitoring of human body. To store and transmit health data confidentially in resource constrained BANs, it needs lightweight cryptographic and key management schemes. The paper suggests a secure hybrid key establishment scheme for BANs based on Signcryption and symmetric cryptography. The session key and cluster head selection is performed in a single step. The proposed scheme would significantly reduce the computation cost as well as traffic overhead.

KEYWORDS: Body Area Networks, Elliptic Curve, Key Management, Clustering

1 INTRODUCTION

BAN is a specialized and new emerging area of Wireless Sensor Networks (WSNs) reshaping the healthcare industry. The nodes in these types of networks are special purpose because of the sensitivity of human body. It consists of small and low cost nodes known as biosensors which can be implanted in human body to monitor different activities like body heat, sudden reaction, blood pressure, ECG and SpO2.

The key role of a sensor node in BANs is to collect, process and perform necessary computation on the data gathered from the human body. These sensors communicate with a node rich in resource i.e. memory, computational power called base station. The sensors communicate the updated information to the base station from time to time. In other word the base station controls all the sensors in the body as well as communication with the external network. The external network constitute of a medical server which stores the patient's data and generates reports for the professionals/physicians based on the information received from the BAN's base station.

As BAN is wireless network and is always on security risk due to its open air communication [10]. Apart from security problem, resource limitation is another problem and should be addressed while designing new scheme. The attacker can target the BAN if found successful he may not only be able to temper with the sensitive information but also may take over the system. In order to protect the sensor data there is not only a need for the secure and lightweight cryptosystem but also a need for secure, energy and memory efficient key agreement protocol. Traditional security solutions are not directly applicable to these networks due to their constrained nature there by providing copious avenues for researchers. The focus of this paper is to design a key agreement protocol with high security strength, computationally less expensive, low communication cost and energy efficient. This scheme uses Signcryption for key establishment and symmetric cryptography for session data transmission in BANs.

2 RELATED WORK

This section presents review of different key management schemes for sensor networks.

In scheme [1] proposed hybrid technique based on DHECC and RSA for key agreement provide rekeying feature to ensure backward and forward secrecy which is efficient in term of scalability, resilience and storage efficiency via particular routing algorithm in key agreement process but its increased computation cost is the main problem and not feasible for BANs environment.

*** Corresponding Author:** Noor Ul Amin, Department of Information Technology, Hazara University, Mansehra, Pakistan.

In scheme [2] review of BAN technology and wireless medical monitoring scheme discuss WBAN architecture, required hardware for WBAN, diseases that are being monitored through this technology and WBAN traffic. At the end they highlight some issues related to WBAN, like infrastructure, security, privacy, reliability and social issues.

In scheme [3] a hybrid model for key agreement in BAN is introduced using symmetric cipher and RSA. RSA is expensive and not appropriate for the constrained natured environment like BAN.

In proposed hybrid scheme [4] ECC and AES is implemented for key agreement and secure exchange of data which has still a loop hole of communication and computation cost.

Weighted Low Energy Adaptive Clustering Hierarchy Aggregation (W-LEACH) algorithm [5] is a modified form of LEACH, in which author proposed data aggregation algorithm that handles uniform and non-uniform Wireless sensor network for increasing the network lifetime rather than for BAN.

3 Proposed Scheme

The topological structure of the proposed network consist of bio sensors, base station and centralized sever as is shown in figure.1.

We assume that the bio sensor have limited resources while base station has high.

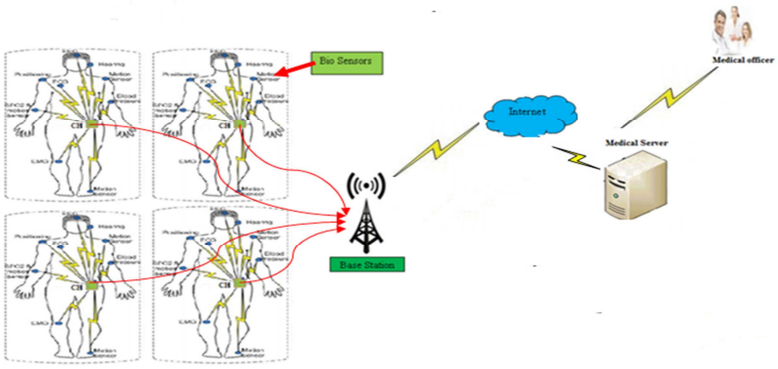

Figure 1. Proposed scheme structure for BANs

Our proposed protocol has the following phases.

- System Initialization Phase
- Session Key Establishment and Cluster HeadSelection Phase
- Secure Session Data Forwarding
- Cluster Head Rotation Phase
- Rekeying Phase

Following are the notations in Table 1 are public parameters used.

Table1. Public parameters

Notation	Description
q	A large prime number ($q \geq 2^{160}$)
E	An Elliptic Curve over prime field Fq of order q
G	Point Elliptic Curve E of order ($n \geq 2^{160}$)
E_k/D_k	Encryption / Decryption with key k
h / h_k	Hash / Keyed Hash Function
M-EXP	Modular Exponentiation
ECPM	Elliptic Curve Point Multiplication

3.1 System Initialization

Base station BS is preloaded with his private and public keys $\mathrm{Pr_{BS}}$, $\mathrm{Pu_{BS}}$ respectively. Before bio sensor deployment on patient body each sensor $\mathrm{S_i}$ is preloaded with its private key$\mathrm{Pr_{si}}$, public key $\mathrm{Pu_{si}}$ and corresponding base station public key $\mathrm{Pu_{BS}}$.

Each deployed sensor $\mathrm{S_i}$ public key $\mathrm{Pu_{si}}$ is also forwarded to base station BS as well.

3.2 Session Key Establishment and Cluster Head Selection

In this phase secure session key is established between each bio sensor and corresponding base station using Signcryption [6] coupled with cluster head selection on the base of energy level.
To accomplish the above task following steps are performed:

Bio Sensor

1. Each bio sensor $\mathrm{S_i}$on patient P_i generates a random number r_{si} where $\mathrm{i} \in \{1,2,3, \ldots \mathrm{n}-1\}$
2. Each bio sensor $\mathrm{S_i}$ on patient $P_i$has energy level EL_{S_i}
3. Signcryption$(r_{si},\ EL_{S_i},\ n, \mathrm{Pr_{si}},\ \mathrm{Pu_{BS}}, h, h_k,\ E_k)$
   a. Select an integer $k \in \{1,2,3 \ldots \ldots \ldots . n-1\}$ randomly
   b. Compute $k.\mathrm{Pu_{BS}}\ mod\ n$
   c. Compute $(K_1\ , K_2)$ $=h(k\mathrm{Pu_{BS}})$
   d. Compute$r = h_{K_2}(\mathrm{r_{si}}||EL_{S_i})$
   e. Compute$c = E_{K_1}(\mathrm{r_{si}}||EL_{S_i})$
   f. Computes$s = \left(\frac{k}{(r+Pr_{BS})}\right) modn$
   Send Signcrypted text (c, r, s) to base station BS

Base Station

1. Base station Unsigncrypt the Signcrypted text (c, r, s)received from each sensor $\mathrm{S_i}$
2. Unsigncryption$(c, r, s, n, \mathrm{Pr_{BS}},\ \mathrm{Pu_{BS}}, \mathrm{Pu_{si}}, \mathrm{h}, \mathrm{h_k}, D_k)$
   a. Compute $u = s\mathrm{Pr_{BS}} modn$
   b. Compute $(K_1, K_2) = \mathrm{h}(u(\mathrm{Pu_{si}} + rG))$
   c. Compute $\mathrm{r_{si}}||EL_{S_i} = D_{K_1}(c)$
   d. Check $h_{K_2}(\mathrm{r_{si}}||EL_{S_i}) = r$, if satisfied accept the random number $\mathrm{r_{si}}$ and energy level EL_{S_i}otherwise reject
3. Base station compute session key $\mathrm{k_{P_i}}$ for patient $\mathrm{p_i}$by selecting two $\mathrm{r_{si}}$from those bio sensor $\mathrm{S_i}$installed on same patientpi as:
$$\mathrm{k_{P_i}} = \mathrm{r_{si}} \oplus \mathrm{r_{s\,i+1}}$$
4. Base station select cluster head for data forwarding form bio sensor to installed on patient $\mathrm{p_i}$ as:
5. Cluster head selection
   Select one bio sensor as cluster head $\mathrm{CH_{Si}}$having maximum energy form those bio sensor installed on same patient$\mathrm{p_i}$ by comparing there energy levels (EL_{S_1}, EL_{S_2} $\ldots . EL_{S_t}$), the remaining bio sensor become member of that cluster. Where $\mathrm{ID_{CH_{Si}}}$is address of Cluster head $\mathrm{CH_{Si}}$, and $\mathrm{ID_{si}}$is address of cluster member $\mathrm{CM_{Si}}$.
6. Encrypt session key and cluster head address to each bio sensor using symmetric cipher and $\mathrm{r_{si}}$encryption key as:
   a. $\mathrm{C} = \mathrm{E_{r_{si}}}(\mathrm{k_{pi}}||\mathrm{CH_{Si}}||\mathrm{ID_{csi}})$
   Send encrypted text C to bio sensor.

Bio Sensor

1. Each bio sensor $\mathrm{S_i}$ received and decrypts the encrypted text (C) by using symmetric cipher and key $\mathrm{r_{si}}$ as:

a. $k_{pi}||CH_{Si}||ID_{csi} = D_{r_{si}}(C)$
b. Cluster memberCM_{Si}send join request to cluster headCH_{Si}.

3.3 Secure Session Data Forwarding
Bio sensor sensed patient information (vital sign) encrypt with session key k_{pi} using symmetric cipher. The encrypted data is forward to cluster head and further forwarded to base station.

3.4 Cluster Head Rotation
In this phase cluster head is rotated, when the cluster head energy level reached to a threshold value.

Bio Sensor
Each sensor sends energy level in encrypted form to base station.
a. $c = E_{k_{pi}}(EL_{S_i})$
b. Send encrypted text C to base station.

Base Station
Reselect cluster head with maximum energy as:
a. Compute $EL_{S_i} = D_{k_{pi}}(c)$
b. Select one bio sensor as cluster head CH_{Si}having maximum energy form those bio sensor installed on same patientp_i by comparing their energy levels(EL_{S_1}, EL_{S_2} .... EL_{S_t}), the remaining biosensor become member of that cluster. Where $ID_{CH_{Si}}$is address of Cluster head CH_{Si}, and $ID_{si}$is address of cluster member CM_{Si}.
c. Compute $C = E_{r_{si}}(CH_{Si}||ID_{csi})$
d. Send encrypted text C to bio sensor

Bio Sensor
Each bio sensor $S_i$received and decrypts the encrypted text (C) by using symmetric cipher and keyr_{si} as:
a. $CH_{Si}||ID_{csi} = D_{r_{si}}(C)$
b. Cluster member CM_{Si}send join request to cluster head CH_{Si}.

3.5 Rekeying
To ensure forward secrecy in case of node leave, backward secrecy in case new node join and key freshness after a threshold amount of timeΔt Rekeying is performed as:

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}
3. Signcryption$(r_{si}', n, Pr_{si}, Pu_{BS}, h, h_k, E_k)$
   a. Select an integer $k \in \{1,2,3 \ldots \ldots \ldots . n-1\}$ randomly
   b. Compute $k.Pu_{BS}\ mod\ n$
   c. Compute $(K_1, K_2) = h(kPu_{BS})$
   d. Compute$r = h_{K_2}(r_{si}')$
   e. Compute$c = E_{K_1}(r_{si}')$
   f. Compute $s = \left(\frac{k}{(r+Pr_{BS})}\right) mod\ n$
   Send Signcrypted text (c, r, s) to base station BS

Base Station
4. Base station Unsigncrypt the Signcrypted text (c, r, s)received from each sensor S_i
5. Unsigncryption$(c, r, s, n, Pr_{BS}, Pu_{BS}, Pu_{si}, h, h_k, D_k)$
   a. Compute $u = sPr_{BS}\ mod\ n$

   b. Compute $(K_1, K_2) = \mathrm{h}(u(\mathrm{Pu_{si}} + rG))$
   c. Compute $r_{si}{}' = D_{K_1}(c)$
   d. Check $h_{K_2}(r_{si}{}') = r$, if satisfied accept the random number$r_{si}{}'$otherwise reject
6. Base station compute session key $\mathrm{k_{P_i}}$ for patient$\mathrm{p_i}$by selecting two $r_{si}{}'$from those bio sensor $\mathrm{S_i}$ installed on same patientpi as:
   a. $\mathrm{k_{P_i}} = r_{si}{}' \oplus r_{si}{}'$+1
7. Base station select cluster head for data forwarding form bio sensor to base station installed on patient$\mathrm{p_i}$as:
8. Encrypt session key to each bio sensor using symmetric cipher and $r_{si}{}'$encryption key as:
   a. $\mathrm{C} = \mathrm{E}_{r_{si}{}'}(\mathrm{k_{pi}}')$
   b. Send encrypted text C to bio sensor

Bio Sensor

1. Each bio sensor $\mathrm{S_i}$received and decrypts the encrypted text $(C)$by using symmetric cipher and key$r_{si}{}'$ as:
   a. $\mathrm{k_{pi}}' = D_{r_{si}{}'}(\mathrm{C})$

4 Security Analysis

Our scheme fulfilled following BANs requirements for secure key agreement [9].

4.1 Confidentiality

In order to achieve confidential session key exchange, we use Signcryption based on ECC and symmetric encryption Blowfish with sufficient parameters which ensure confidentiality of information exchange during session key and lead to confidential session key exchange.

4.2 Integrity

In session key establishment, from bio sensor to base station integrity is achieved by Signcryption routine and from base station to bio sensor by hash function.

4.3 Authentication

Signcryption ensure authenticity, therefore in session key establishment authenticity of information received from each sensor at base station is achieved. Authenticity of information received at sensor is achieved by ID and hash function.

4.4 Data Freshness

It ensures that received data are not replayed and should be fresh and created newly. In a structure, where session key strategies are employed, data freshness plays a significant role.

4.5 Node Capture

In case of node capturing base station has the capability to sense it and establish new session key for secure session data forwarding using rekeying. Our scheme provides admirable resilience beside node capture attack via forward secrecy.

4.6 Scalability

Our proposed protocol for BANs has the ability to maintain considerable increase in size of network after deployment.

4.7 Backward and Forward Secrecy

To ensure forward secrecy [7, 8] in case of node leave, backward secrecy in case new node join and key freshness after a specific interval of time rekeying is performed which ensure forward as well as backward secrecy.

5 Performance Analysis

In this section a comprehensive analysis of the proposed secure key establishment and cluster head selection protocol in term of performance is given:

5.1 Memory Requirement Analysis for Key Storage

We presume that base station is resource-rich and bio sensors are resource constrained so it required light weight security technique to consume less memory.

NIST recommended secure key size for ECC is 160 bits and blowfish cipher 32-448 bits.Key size of blowfish cipher from32 to 448, RSA $\geq 2^{1024}$ and ECC $\geq 2^{160}$. Figure 2 indicates memory requirement analysis of our proposed scheme with other schemes.

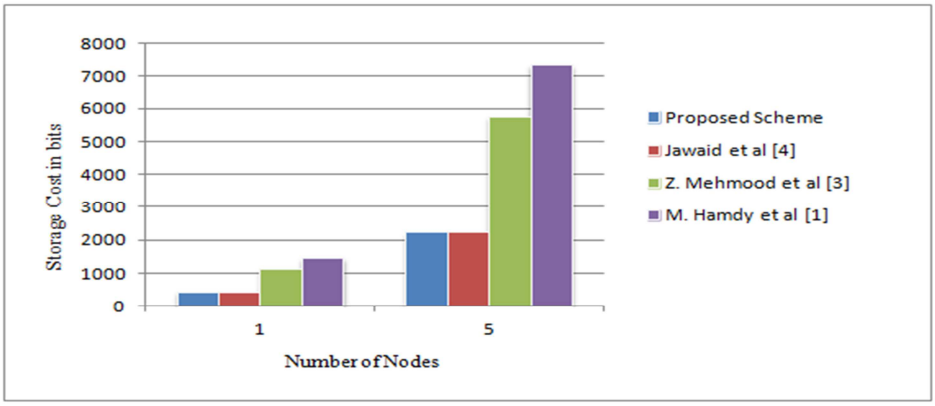

Figure 2. Memory requirement for key storage

5.2 Computation Cost Analysis

In our proposed secure key establishment technique, the expensive operations are ECPM and M-Exp. figure 3shows the processing cost analysis of our scheme with existing schemes.

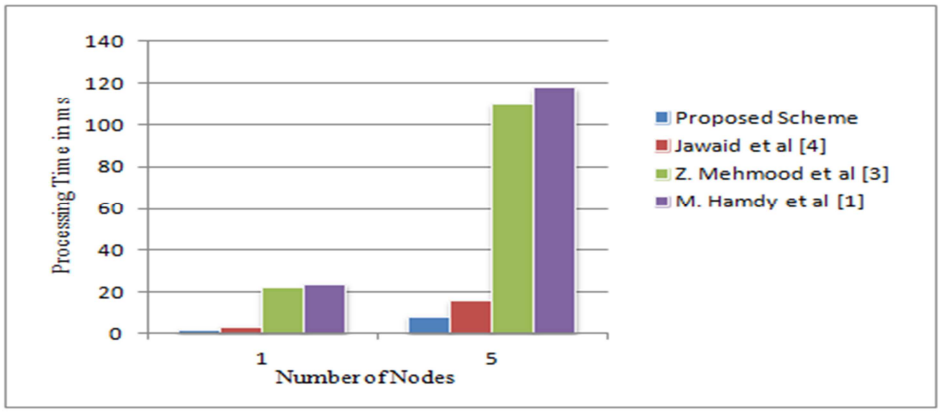

Figure 3. Computation cost of key establishment

5.3 Communication Overhead Analysis

As in BANs speed of link usage is a main issue so we need smart cryptosystem for less communication cost. Figure 4shows the communication overhead analysis of proposed key establishment and existing schemes.

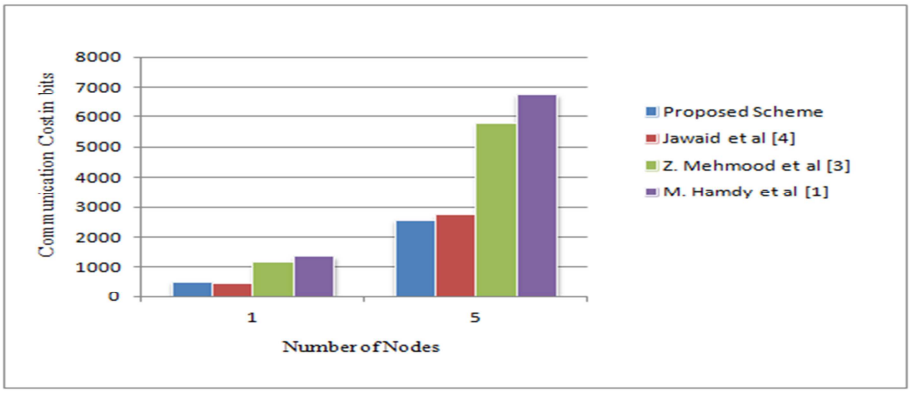

Figure 4. Communication overhead of key establishment

6 CONCLUSION

Signcryption based on elliptic curve cryptography (ECC) in BANs is the unique feature of this paper. Life of the network is increased by cluster rotation among the sensors. Forward and backward secrecy is maintained by rekeying. The proposed scheme is favorable due to significant reduction in computation cost as well as communication overhead for BANs over other existing schemes while fulfilling essential security parameters.

REFERENCES

[1] Eldefrawy, M. H., Khan, M. K., and Alghathbar, K. "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography", In International Conference onAnti-Counterfeiting Security and Identification in Communication (ASID), (2010) 1-6

[2] Ahmad, J., and Zafar, F, "Review of body area network technology & wireless medical monitoring", International Journal of Information, 2(2), (2012)

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

[4] Iqbal, J., Nizamuddin, Amin, N., and Umar, A. I. "Authenticated Key Agreement And Cluster Head Selection For Wireless Body Area Networks" In 2nd National Conference on Information Assurance (NCIA), (2013), 113-117

[5] Abdulsalam, H. M., &Kamel, L. K. "W-LEACH: Weighted Low Energy Adaptive Clustering Hierarchy aggregation algorithm for data streams in wireless sensor networks", In IEEE International Conference on Data Mining Workshops (ICDMW), (2010), (pp. 1-8)

[6] Zheng, Y.and Imai, H. "How to construct efficient signcryption schemes on elliptic curves", Information Processing Letters, 68(5), (1998), 227-233.

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

[8] Ch, S. A., Nizamuddinand Sher, M. "Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem", In Information Systems, Technology and Management, (2012), 135-142

[9] Amin, N.,Asad, M., Nizamuddin and Chaudhry, S. A. "An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem", 9thIEEE International Conference on Networking, Sensing and Control (ICNSC), (2012), 118-121

[10] Khan, M., Ahmad, A., & Park, G. "Computer Network Protocols Convergence Under Secure and Non Secure Environment", VAWKUM Transaction on Computer Sciences, 1(2), 2013