International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Trust Based Distributed Group Key Management Technique for Securing Multithreaded WBAN

Sanchari Saha, Dinesh K Anvekar

Abstract**:** ***Wireless body area networks (WBANs) are having immense application areas such as medical, battlefield, entertainment, sports, gaming and many more. Transmitting information through WBAN in a secured way has gained interest of many researchers. In this paper, we have extended the security to multithreaded environment where multiple WBANs operate together. We have proposed an optimal key selection method based on trust value for securing multithreaded wireless body area network. We have adopted prioritized routing approach where first priority is given to emergency data, next to on-demand data and last to periodic data transfer between sink node and root node. In our security proposal advanced encryption standard (AES) is combined with group key management to enforce data security. We have estimated the best optimized performance in presence of design parameters such as network topology, energy levels, source rates, received power and node count. We have implemented the security model for a fixed deployment strategy and done test runs to prove that this security solution achieves notable improvement in network throughput, packet delivery delay, packet drop ratio, detection ratio, energy consumption and network lifetime.***

Index Terms**:** ***MWBAN, Cluster-head, Priority, Group key, Security, Energy efficiency.***

I. INTRODUCTION

Increase in average lifespan demands a healthcare system which will support continuous ubiquitous monitoring of a human health. This system requires an advanced wireless data transmission technology with on-body or in-body sensors as major component. These sensor nodes can be implanted inside or mounted on a human body for sensing physical stimulations and convert them into digital readings. Wireless body area networks (WBANs) fulfil this demand by providing remote health monitoring in a ubiquitous manner. WBAN applications can be either medical or non-medical [1]. Non-medical applications include sports, battlefield, virtual gaming, lifestyle and entertainment etc. [2]. Further, medical applications are classified as in-body and on-body medical application [3]. In the medical field, a WBAN consists of need based various medical sensors as ECG sensor, EEG sensor, temperature sensor etc., and a coordinator which either can be a personal digital assistant (PDA) or a smart phone. The main purpose of these devices is to collect, store and process sensed physiological data and facilitate ubiquitous healthcare service. Due to specific operational requirements such as high reliability and security, wider mobility, small size, limited power, high data rate and quality of service, ability to handle heterogeneous traffic, WBANs require special protocols designed to meet the requirements [4]. Even though WBAN is a special type of WSN, there are notable differences between these two networks which are summarized in Table I [5].

Revised Manuscript Received on 30 May 2019.
* Correspondence Author

Sanchari Saha*, Department of Information Science & Engineering, MVJ College of Engineering, Bangalore, India.
Dinesh K Anvekar, Department of R&D and Product Innovation Cell, Vijaya Vittala Institute of Technology, Bangalore, India.

Criteria	Wireless Sensor Network	Wireless Body Area Network
Location	In the environment	On the human body
Node count	More nodes	Less nodes
Accuracy level	Less accuracy	More accuracy
Power	High power	Low power
Security need	Lower security	Higher security
Replacement	More flexible to replace	Less flexible to replace

Table I. WSN & WBAN comparison

One of the major challenges faced by WBAN is resource constraint. Various routing protocols are designed to tackle the resource constraint challenge. WBAN routing protocols are designed based on various categories such as communication route type from source to sink within the network, network structure, communication initiator etc.

In [6] trusted nodes are found by enquiring its direct neighbor and credit check with its indirect neighbor. This technique requires complex MAC scheduling that effects energy consumption and incurs high network load. In [7] to isolate misbehaving nodes packet forwarding ratio of neighboring nodes are aggregated. But this scheme suffers from route maintenance & high routing overhead. To evaluate trust of its neighbor by observing packet forwarding ratio different method is proposed in [8] but as this equally shares network traffic load among trusted nodes, reduces network lifetime.

One more scheme is proposed in [9] where periodically a beacon message is broadcasted with node-ID, energy and location information.

Trust of every neighbor is calculated with reputation request and reputation response message and final summary of these messages. Even though it is a lightweight solution yet imposes extra overhead and consumes extra energy for request and response broadcast.

In WBAN, data transmission between sink node and base station is more prone to several types of security attacks [10] [11] [12] [13] [14]. These attacks can be restricted with strong cryptographic primitives but as WBAN is resource constrained, cannot perform high computations. Therefore, security of WBAN data within limited resources remains a concern for the research group [10] [12]. In [15] one security approach is proposed which used Elliptic Curve Cryptography (ECC) for key distribution and data sharing. ECC is capable to resolve much of the security requirements within a resource constrained environment. But implementation of ECC gives rise to a new problem of replay attack and mutual authentication. All these problems we have tried to solve through our proposed work.

In this paper, our proposed network model is divided into three tiers called tier-1, tier-2 and tier-3 and all the following five major components are distributed across these three tiers [16] [18].

Body Sensors (BS): WBAN body sensors are small in size and are highly resource constrained. Each BS is equipped with communication devices for extra body communication. It resides in tier-1.

Cluster Head (CH): The proposed network model is divided into multiple groups referred to as clusters. For every cluster there is one designated cluster head (CH) responsible for periodic update of group key for sensors in its own cluster. It resides in tier-1.

Personal Server (PS): This is generally stationary and is usually placed at the border of peer clusters and sometime at cross networks of the clusters. The personal server can be either a personal digital assistance (PDA) or a smart phone. Under normal operation, the medical server can make a rough estimation of ΔTj, the time period for a WBAN sensor to pass by two personal servers in the cluster j, based on the statistics of traffic and density of personal servers. It resides in tier-1.

Central mediator: The most important part of WBAN is Central mediator or base station which needs to be positioned in such a way so that WBAN can be connected to other systems for emergency communication. It resides in tier-2.

Medical Server (MS): This server ensures authenticity by registering all members in the system. It can be highly trusted and is designed to be free from attack. It resides in tier-3.

Three tier architecture of our proposed network model is shown in Fig. 1.

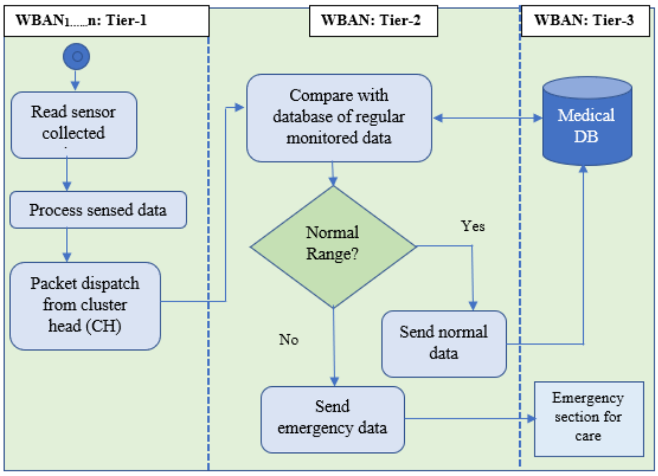

Fig. 1 Three tier architecture of MWBAN

With the above network model, in this paper, we have explored the possibility of a better group key management algorithm applicable for secured routing of information through multiple WBANs working in parallel (multithreaded WBAN environment).

In the following, Section-II gives details on cluster head selection. Then, a priority based routing approach is explained in section III. Section-IV discusses cryptographic key management technique. Section V explains the security claims achieved by the proposed solution. Section VI presents simulation parameters and implementation results. Finally, concluding remarks are presented in section VII.

II. CLUSTER HEAD SELECTION

In individual WBAN, each node works in a cooperative manner to form clusters and each cluster has a designated cluster head (CH) along with some cluster members in its transmission range. The cluster head is selected based on several parameters such as energy consumption, delay in transmission, distance from the sink node, trust value, packet forwarding ratio etc. [17]. Once a cluster member joins a cluster, the cluster member and the cluster head exchange cluster-head-HELLO-packet and cluster-member-HELLO-packet to maintain connection with each other. To determine link interference in WBAN, the following mechanism is used: For an interval, each node periodically exchanges the list of single-hop neighbors with its immediate neighbor node through prefixed count of HELLO messages. Each node is supposed to keep this received HELLO message record to determine link interference. If the count of received HELLO messages from neighbor node is equal to the expected count, then it is assumed that no interference is there over the link. Under this situation, if a node drops any data packet, it can be due to some abnormality in the node and not due to any link interference problem. But, for a particular interval if the expected count of HELLO messages is not received by a node from its neighbor, it indicates that there is a link interference problem between these two nodes. In our proposed scheme, along with neighbor lists, nodes also exchange information about link status of each of the neighbor nodes.

By using the information about the HELLO messages, the probability of successful data transmission from one node to another node can be computed based on the quality of link layer between two nodes. The probability of packet forwarding is calculated by using the equation:

$$P_{PF} = \frac{\sum Hello_R\left(t_{i-1}, t_i\right)}{\sum Hello_E\left(t_{i-1}, t_i\right)} \qquad (1)$$

where, $Hello_R$ is the total count of received HELLO packets and $Hello_E$ is the total count of expected HELLO packets for a particular time interval $\left(t_{i-1}, t_i\right)$. Delay in packet forwarding is calculated using the equation:

$$Delay_i = \left(\frac{E_i - E_{res}}{E_i} + Rand(0,1) + P_{PF}\right) * Rate_{Data} \qquad (2)$$

where, E_i is the initial energy, E_{res} is the residual energy, Rand (0,1) is a random number, P_{PF} is the probability of packet forwarding between two nodes calculated by using Equation (1). Randomized back-off delay assures that a cluster head having higher residual energy tends to become a cluster head [18].

Advantage of Clustering:

In cluster based MWBAN model, all the nodes with respect to individual WBAN are grouped into clusters wherein the cluster head is responsible for transmitting the aggregated data of its own cluster to other cluster heads or the base station as shown in Fig. 2. In this model, data flows from a lower to a higher cluster layer. Therefore, even though it hops from one node to another, as the hopping is layer based, this approach covers a larger distance and transmits data faster to the base station. Comparatively cluster based WBAN model has less delay time than multi-hop model [19].

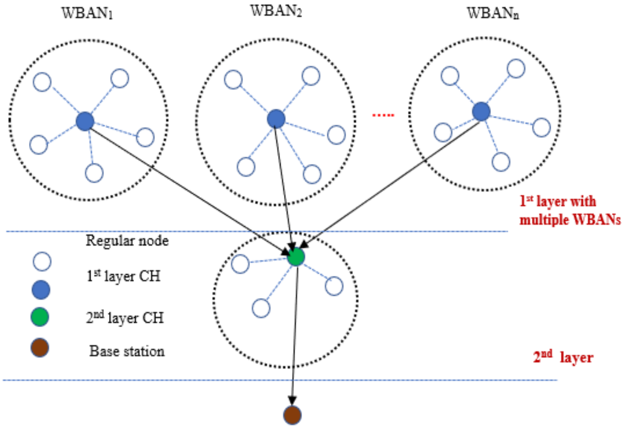

Fig. 2 Clustering approach in MWBAN

III. PRIORITY BASED ROUTING

To provide QoS in MWBAN communication, the routing mechanism classifies the traffic from each WBAN based on priority, latency, packet loss and throughput. The variegated WBAN traffic needs a power efficient mechanism to ensure reliable delivery. In our proposed work the entire MWBAN traffic is classified as normal, on-demand and emergency traffic, as shown in Fig. 3.

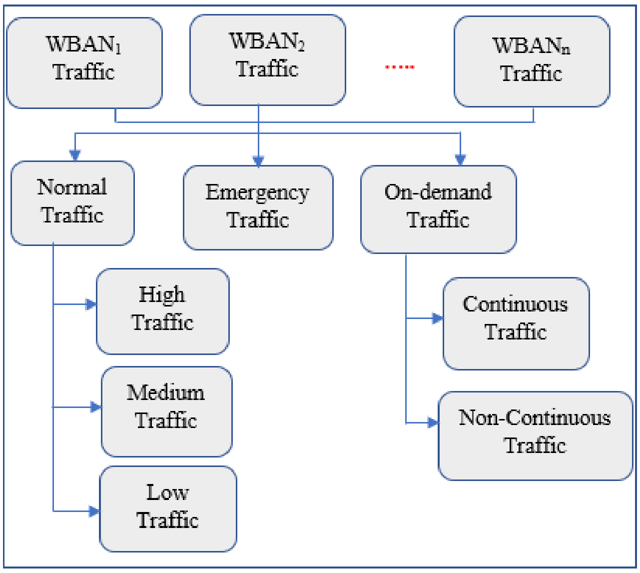

Fig. 3 MWBAN traffic classification

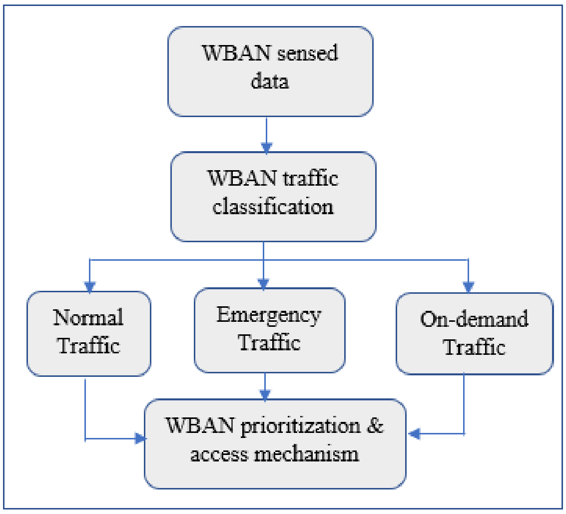

Fig. 4 Processing of each WBAN data based on priority

The normal traffic is again classified as low, medium and high traffic, and on-demand traffic is further classified as continuous and non-continuous traffic.

Normal traffic

Normal traffic is generated based on normal operation between sensor node and the WBAN coordinator as per the defined pattern and is usually transmitted at regular intervals without any critical time condition.

Even though there is a requirement to follow the deadline precisely, a reasonable amount of packet loss is acceptable. Normal traffic carries routine healthcare data such as the video streaming of an old person's motion data or any multimedia packet. This normal traffic is forwarded to medical database, and only if there is some notable deviation from the regularly received data value, the required medical care is provided.

On-demand traffic

Whenever any immediate information is needed by the doctor or by the WBAN coordinator for diagnosing sensed data, on-demand traffic is generated. This type of traffic contains regularly monitored physiological values. On-demand traffic is classified as continuous traffic which is usually required during surgical cases, and non-continuous traffic which is required for casual information. For on-demand traffic also precise deadline requirement needs to be met but in contrast to normal traffic, packet loss in continuous on-demand traffic is not tolerable.

Emergency traffic

Emergency traffic is initiated whenever any node needs to send critical data urgently. This type of traffic is generated beside the scheduled transmission traffic. Emergency traffic contains critical data values that exceed the normal range threshold. This type of traffic needs to be initiated anytime, and hence is unpredictable. Also, the delivery time for emergency traffic should be very short, and packet loss is intolerable.

Based on the priority of these three classes of data traffic, the sensed data is processed by WBAN prioritization and access mechanism as shown in Fig. 4. The priority is calculated by using the equation:

$$\Pr iority_i = \frac{Traffic\_Class_i}{Rate_{Data} * PacketSize_i} \qquad (3)$$

where, $Priority_i$ denotes the priority of the traffic, $Traffic\_Class_i$ denotes the traffic class, i.e. normal, on-demand, emergency, $Rate_{Data}$ denotes the data generation rate, and $PacketSize_i$ denotes the packet size in bytes.

Priority of any packet is mainly calculated based on its traffic class and rate at which data is generated by the node.

Based on calculated priority, the packets are classified as Critical, Moderate, and Regular. The packets with emergency traffic class and highest data generation rate are treated as critical packets and assigned the priority value of 1 (highest priority). The implication of this is that packets with emergency traffic class contain critical data values that exceed the normal range threshold and should be sent reliably for medical care without much delay. The packets that are generated from a node with highest data generation rate should be sent immediately to avoid node overflow and packet loss. Packets with normal traffic class and low data generation rate are designated as regular packets and assigned the priority value of 3 (lowest priority). The implication of this is that packets with normal traffic class contain routine data that has normal range values and hence need not be sent urgently. The packets that are generated from a node with low data generation rate take more time to overflow, and therefore, the chance of packet loss is very low. The data packets with on-demand traffic class and medium data generation rate are designated as moderate packets and assigned the priority value of 2 (medium priority). Because of this, the packets with on-demand continuous traffic class contain routine data that may be required for surgical cases and therefore should be sent as early as possible to the request originator. The packets generated from a node with medium data generation rate take considerably less time than the lowest priority packets to overflow. It is the responsibility of forwarding nodes to allocate transmission slots in the contention-free period (CFP) for the sensor nodes depending on assigned priority values. Critical packets with highest priority are allocated transmission slots superseding the other type of packets. Once slot requirement for all critical packets is met, the next slot is assigned to moderate packets with mid-priority. Lastly, the remaining slots are allocated to the regular packets with lowest priority.

IV. CRYPTOGRAPHIC KEY MANAGEMENT

In our proposed security solution bilinear pairing is used as the main cryptographic base . Linear mapped relation between two cyclic groups is used here [20].

Following pairing parameters are used for bilinear mapping :

p: prime number
G1: p order additive cyclic groups
GT: p order multiplicative cyclic groups
g1: generator of G1
gT: generator of GT

Following three properties are satisfied by the bilinear map, ˆe: G1 × GT → GT:

(i) Polynomial computation which depicts that, ˆe is computed in polynomial time.
(ii) Bilinearity which depicts that, if P1, P2∈G1 and a, b∈ Y* q then, ˆe (aP1, bP2) = ˆe (P1, P2) ab
(iii) Non-degeneracy which depicts that ˆe (g1, g1) = gT

Any WBAN group with such bilinear map is called bilinear group. Following two problems can be defined for such WBAN bilinear group :

(1)*Elliptic curve discrete logarithm problem :*

On an elliptic curve when point P is order of q and point Q is present on the same curve, Elliptic curve discrete logarithm problem is to find the integer a, $0 \leq a \leq q-1$, in such a way that Q = aP.

(2)*Computational Diffie-Hellman problem :*

With two unknowns a, b $\in Y^* q$, the Computational Diffie-Hellman problem is to compute abP∈G. with P, aP, bP∈G.

(3)q-Strong Diffie--Hellman problem:

When there is unknown v∈ $Y^* q$ with q+1 tuple (g1, vg1, . . ., vqg1), then q-Strong Diffie--Hellman problem is to generate SDH tuple (x, (1/ (v + x)) g1).

Phases of our proposed group key management approach are system initialization, distributed key updation, identity revocation and message signatures with verification.

Proposed algorithm for optimal key selection based on trust value is presented below:

```
Start
Step 1: Initialize network node $N_K$,  k= 1,2,3…...n
Step 2: if
            $N_K$ is in active state then send message to all network
            nodes
            end if
Step 3: Form cluster and designate cluster head ($CH_j$) ,
              where, j=1,2….n
Step 4: if
            CH1 is selected
            then , CH1 = Trust (T1 )
Step 5: Nk transmits trust request to Nneighbor
Step 6: if
            T ($N_{neighbour}$ ) >= Threshold, Emax
            select optimal key based on trust value
Step 7: Calculate Key K as Trust (Tn )ϵ threshold limit
             satisfied
Step 8: Select $K_{optimal}$ = Tn ∀ Trust value
Step 9: $CH_{final}$ = $T_{final}$
            Repeat until breakpoint
Stop
```

A. System initialization

Table II. Notations

Symbol	Notation
v	Master secret key of MS (Medical Server)
w	Master public key of MS (Medical Server)
groupj	jth group
CHj	The cluster head of groupj or clusterj
BSi	ith body sensor
ΔTj	The time period that a sensor data can pass by two cluster members in the clusterj under normal situation.
Timestamp t’ j	t^{th} time stamp in groupj.
F1()	A hash function as $\{0,1\}^* \rightarrow G$
F2( )	A hash function - SHA-1
< zj, Xj >	The group key of Body Sensor BSi
$PK^n{}_{CH_j}$	The public key tuples of CHj with $n \in [1,4]$
||	Message concatenation operation for appending multiple messages together

(i) Chosen basic elliptic curve parameters by medical server are p, G1, GT, g1, gT, ˆe.

(ii) Two one-way functions selected by medical server are F1 and F2.

F1: {0, 1} ∗ → G1 maps strings of certain length to elements of group G1 and F2 as,

F2: {0, 1} ∗ → Yp maps strings of certain length to the integers of group Yp.

(iii) Symmetric encryption function selected by medical server is SEα where α is AES symmetric key.

(iv) v is used as random number with the relation: $v \xleftarrow{R} Y_q^*$ which is private key and calculates $w \leftarrow vg1$ as the public key.

(v) Strong Diffie--Hellman pair <z, X > is computed by medical server for body sensors and Cluster Heads respectively, where $z \xleftarrow{R} Y_p^*$ and $X \leftarrow (1/(v + z))\, g1$.

BS_i (Body Sensor) uses < z_i, Xi > as private key for assigning signature. Once the Strong Diffie--Hellman pair < z_j, Xj > is computed by the medical server, the cluster head CH_j considers z_j as private key and creates tuples < $PK^0{}_{CHj}$, $PK^1{}_{CHj}$, $PK^2{}_{CHj}$, $PK^3{}_{CHj}$ >

$$PK^0{}_{CHj} \leftarrow z_j\, g1 \tag{4}$$

$$PK^1{}_{CHj} \leftarrow X_j \tag{5}$$

$$PK^2{}_{CHj} \leftarrow z_j X_j \tag{6}$$

$$PK^3{}_{CHj} \leftarrow z_j\, (g1 - z_j\, X_j) = v\, PK^2{}_{CHj} \tag{7}$$

B. Distributed key updation

Time domain for groupj is split into time stamps by ΔTj. Let us assume $TimeStamp^t{}_j$ denote t-th time slot in groupj. In $TimeStamp^t{}_j$, BSi requests group key either for the current time slot or requests next one from CHj through personal server PS. The distributed key updation is carried out using below mentioned steps:

(i) BSi chooses random number RN1 so that $rn_1 \xleftarrow{R} Y_p^*$ and computes $\alpha \leftarrow rn_1 PK^2{}_{CH_j}$ which is symmetric encryption key, $\beta \leftarrow rn_1 PK^1{}_{CH_j}$ which is partial symmetric encryption key and $\theta \leftarrow rn_1 X_i$ which is key updation parameters. We assume that BSi finds out a group key for the time-stamp $TimeStamp_j^{t'}\,(t' \leftarrow t)$ or $TimeStamp_j^{t'}\,(t' \leftarrow t+1)$ and calculates update request $RQ \leftarrow \beta \,||\, Time_{stamp} \,||\, SE_\alpha(Z_i, \theta, t')$. For saving request from damage, BSi uses rn_1 as private key and calculates signature $Sign \leftarrow rn_1 F_1(\mathrm{Re}\, q)$ using short signature process.

(ii) BSi can send request message CHj as $RQ \,||\, Sign$ once signature is computed. Once the timestamp expires, CHj may drop key update request from BSi.

After that it will verify message signature.

If, $\hat{e}(\theta, F1(RQ)) = \hat{e}\left(PK^1{}_{CH_j}, Sign\right)$ is true, then symmetric key α is computed as,

$\alpha \leftarrow z_j \beta = rn_1 PK^2{}_{CH_j}$ and using this symmetric key, message can be decrypted to retrieve zi, θ and t’. If t’ is equal to t or (t+1), then following equation holds:

$$\hat{e}(\theta, w + z_i g1) = \hat{e}(\beta, w + z_j g1) \tag{8}$$

If this equation is verified as true, then CHj computes update key as:

$$\rho \leftarrow \frac{1}{\left(z_j + F_2\left(t'\right)\right)\left(z_i - z_j\right)}\left(\beta - \theta\right)$$

$$= \frac{1}{\left(z_j + F_2\left(t'\right)\right)\left(z_i - z_j\right)} rn_1\left(PK^1{}_{CH_j} - X_i\right) \tag{9}$$

$$= \frac{rn_1}{\left(z_j + F_2\left(t'\right)\right)\left(v + z_i\right)} PK^1{}_{CH_j} \tag{10}$$

(iii) CH$_j$ sends ρ to BS$_i$ and maintains service record <z$_{i,}$ t'>, i.e. BS holding key z$_i$, updates the group key which is valid for Time$_{stamp}$$^{t'}$$_j$ from CH $_{j.}$

After renewed key μ is obtained, BS$_i$ generates private key:

$$X_i^{j,t'} \leftarrow \frac{1}{rn_1}\rho = \frac{1}{\left(z_j + F_2\left(t'\right)\right)\left(v + z_i\right)} PK^1{}_{CH_j} \tag{11}$$

and does equation verification as:

$$\hat{e}\left(X_i^{j,t'}, PK^0{}_{CH_j} + F_2\left(t'\right)g1\right) = \hat{e}\left(X_i, PK^1{}_{CH_j}\right) \tag{12}$$

If the verification is cleared, then the BS$_i$ will maintain <z$_{i,}$ $_{Xi}$$^{j,t'}$ > as private key of signature for TimeStamp$^{t'}$$_{j.}$

C. Message signature with verification

Public key P1 and P2 should be updated for group$_{j,}$ with the development of time slots.

For the current time stamp TimeStamp^t$_j$, p1 and p2 are calculated as:

$$P_1 \leftarrow PK^2{}_{CH_j} + F_2\left(t\right)PK^1{}_{CH_j} = \left(z_j + F_2\left(t\right)\right)PK^1{}_{CH_j} \tag{13}$$

$$P_2 \leftarrow PK^3{}_{CH_j} + F_2\left(t\right)\left(g1 - PK^2{}_{CH_j}\right) = vP_1 \tag{14}$$

Any BS$_i$ with a valid group key (z$_i$,X$_i$$^{j,t'}$) is able to sign a message as follows:

- BS$_i$ selects a random number

$rn_2 \xleftarrow{R} Y_q$ and finds

$$A \leftarrow F_1\left(rn_2 \,||\, Msg\right) \in G_1 \tag{15}$$

and $B \leftarrow F_1\left(rn_2 g1 \,||\, Msg\right)$ (16)

- BS$_i$ selects a random number $\lambda \xleftarrow{R} Y_q$ and computes,

$$T_1 = \lambda A \tag{17}$$

$T_2 = \lambda B + X_i^{j,t}$ and $\delta \leftarrow \lambda z_i$ (18)

- BS$_i$ selects random number $rn_\lambda rn_z rn_\delta \xleftarrow{R} Y_p$ and computes:

$$RN_1 \leftarrow rn_\lambda A,$$

$$RN_2 \leftarrow \hat{e}\left(T_2, P_1\right)^{rn_z} \hat{e}\left(B, P_2\right)^{-rn_\alpha} \hat{e}\left(B, P_1\right)^{-rn_\delta},$$

$$RN_3 \leftarrow rn_z T_1 - rn_\delta A,$$

$$C \leftarrow F_2\left(Msg \,||\, rn_2 \,||\, T_1 \,||\, T_2 \,||\, RN_1 \,||\, RN_2 \,||\, RN_3\right),$$

$$s_\lambda \leftarrow rn_\lambda + c_\lambda,\ s_z \leftarrow rn_z + cz_i,\ s_\delta \leftarrow rn_\delta + c\delta \tag{19}$$

- Output message signature is computed as follows:

$$\sigma \leftarrow \left(rn_2, T_1, T_2, c, s_\lambda, s_z, s_\delta\right) \tag{20}$$

'Msg' is used to denote while receiving the message and the signature $\sigma = \left(rn_2, T_1, T_2, c, s_\lambda, s_z, s_\delta\right)$. Other nodes in CH$_j$ can authenticate message as follows:

- Compute,

$$A \leftarrow F_1\left(rn_2 \,||\, Msg\right) \tag{21}$$

and $B \leftarrow F_1\left(rn_2 g1 \,||\, Msg\right)$. (22)

on group G1.

- Compute,

$$RN_1 \leftarrow s_\lambda A - cT_1 \tag{23}$$

$$RN_2 \leftarrow \hat{e}\left(T_2, P_1\right)^{s_z} \hat{e}\left(B, P_2\right)^{-s_\lambda} \hat{e}\left(B, P_1\right)^{-s_\delta} \times\left(\hat{e}\left(T_2, P_2\right)\Big/\hat{e}\left(PK^1{}_{CH_j}, PK^1{}_{CH_j}\right)\right)^c \tag{24}$$

$$RN_3 \leftarrow s_z T_1 - s_\delta A \tag{25}$$

- Accept the message if,

$$C = F_2\left(Msg \,||\, rn_2 \,||\, T_1 \,||\, T_2 \,||\, RN_1 \,||\, RN_2 \,||\, RN_3\right) \tag{26}$$

The relation can be justified as:

$$RN_1 = \left(rn_\lambda + c\lambda\right)A - c\lambda A = rn_\lambda A = RN_1 \tag{27}$$

$$RN_2 = \hat{e}\left(T_2, P_1\right)^{rn_z + cz_i} \hat{e}\left(B, P_2\right)^{-rn_\lambda - c\lambda} \hat{e}\left(B, P_1\right)^{-rn_\delta - c\delta}$$

$$(\hat{e}\left(T_2, P_2\right)/\hat{e}(PK^1{}_{CH_i}, PK^1{}_{CH_i}))^c$$

$$= RN_2\hat{e}\left(\lambda B + X_i^{j,t}, P_1\right)^{cz_i} \hat{e}\left(B, vP_1\right)^{-c\lambda} \hat{e}\left(B, P_1\right)^{-c\lambda z_i}$$

$$(\hat{e}\left(\lambda B + X_i^{j,t}, vP_1\right)/\hat{e}(PK^1{}_{CH_j}, PK^1{}_{CH_j}))^c$$

$$= RN_2\hat{e}\left(X_i^{j,t}, P_1\right)^{cz_i} \hat{e}\left(X_i^{j,t}, vP_1\right)^c \Big/\hat{e}(PK^1{}_{CH_j}, PK^1{}_{CH_j})^c$$

$$= RN_2\hat{e}(\frac{1}{z_j + F_2(t))(v + z_i)} PK^1{}_{CH_j},$$

$$(z_j + F_2(t))PK^1{}_{CH_j})^{c(z_i + v)} \Big/\hat{e}(PK^1{}_{CH_j}, PK^1{}_{CH_j})^c$$

$$= RN_2 \tag{28}$$

$$RN_3 = (rn_z + cz_i)T_1 - rn_\delta + c\lambda z_i)A$$

$$= rn_z T_1 - rn_\delta A$$

$$= RN_3 \tag{29}$$

D. Identity revocation

Once BS_i is revoked, the medical server informs all the cluster heads regarding key pair (z_i, X_i). After receiving this information cluster head immediately stops giving service to users having key z_i. In TimeStamp^t_j, cluster head performs database search. In this search operation, if service record $< z_i, t' >$ is found where, t' = t or (t +1) then CHj will compute key of BSi in TimeStamp^t_j as :

$$\tilde{X}_i^{j,t'} \leftarrow \frac{1}{(z_j + F_2(t'))(z_j - z_i)}(PK^1{}_{CH_j} - X_i)$$

$$= \frac{1}{(z_j + F_2(t'))(v + z_i)} PK^1{}_{CH_j}$$

$$= X_i^{j,t'} \tag{30}$$

Later, CHj will add $\tilde{X}_i^{j,t'}$ in group revocation list (RL) and using inter-WBAN communication, will broadcast to all the body sensors in the group_j. If revocation list is not empty, then all the members of group_j needs to check for revocation before they can verify message signature:

$$\sigma = \left(rn_2, T_1, T_2, c, s_\lambda, s_z, s_\delta\right) \tag{31}$$

For every component $\tilde{X}_i^{j,t'}$ in revocation list, following relation is verified:

$$\hat{e}(T_2 - \tilde{X}_i^{j,t'}, A) = \hat{e}(T_1, B) \tag{32}$$

If this relation holds, it means that the message arrived from certain revoked body sensor which has the key $\tilde{X}_i^{j,t'}$ and hence, the message needs to be discarded.

V. SECURITY CLAIM

Our proposed trust based distributed group key management (TPDGKM) technique satisfies following security claims:

Claim 1: Body sensors cannot forge an identity and acquire a legitimate group key from a cluster head.

Proof: Proposed key updation procedure ensures that the requesting body sensor has Strong Diffie—Hellman tuple. If body sensor requests for authentication information from cluster head where the requesting message signature Req||Sign is correctly verified, then body sensor is having a rn_1 as random number and $\alpha \leftarrow rn_1 PK^1{}_{CH_j}$.

Again, if following equation is satisfied

$$\hat{e}(\eta, w + z_i g1) = \hat{e}(\alpha, w + z_j g1) \tag{33}$$

$$\eta = (rn_1 / v + z_i))g1 \tag{34}$$

Then surely, body sensor possesses Strong Diffie—Hellman tuple $(z_i, (1/v + z_i))g1)$, and therefore from q-Strong Diffie--Hellman problem, body sensors cannot forge a SDH tuple from a cluster head and hence the claim is proved.

Claim 2: No cluster head can acquire the body sensor group key when distributed key updation is in process.

Proof: If body sensor requests for an updated authentication information from the cluster head then body sensor must provide the linear encryption computation as:

$\eta \leftarrow rn_1 X_i$. It can be observed that , rn_1 is the main factor to block leakage of body sensor group key. For cluster head with $\alpha \leftarrow rn_1 PK^1{}_{CH_j}$ and $PK^1{}_{CH_j}$ solving is an elliptic curve discrete logarithm problem.

Without rn_1, cluster head cannot get group key of body sensor which is Xi. Hence, it is also not possible to obtain the group key $X_i^{j,t'}$ used for that group. Therefore, group key of body sensors remains private.

Claim 3: Body sensors having valid group key only can do successful message signature.

Proof: Message authentication is satisfied only if the equation: $RN_2 = RN_2$ is true. It means that,

$$\hat{e}\left(X_i^{j,t}, P_1\right)^{cz_i} \hat{e}\left(X_i^{j,t}, vP_1\right)^c = \hat{e}(PK^1{}_{CH_j}, PK^1{}_{CH_j})^c \tag{35}$$

and $$X_i^{j,t'} = \frac{1}{(z_j + F_2(t'))(v + z_i)} PK^1{}_{CH_j} \tag{36}$$

These two above equations imply that the source of a verified message must have a valid group key. Depending on these above three claims and corresponding proofs it can be assured that our proposed trust based prioritized distributed group key management (TPDGKM) technique satisfies all the important security requirements for data transfer.

VI. IMPLEMENTATION RESULT

Simulation Tool: NS-2
Programming languages: TCL and C++

Platform: Linux (ubuntu or fedora or redhat)

Table III. Simulation parameter

Parameter	**Value**
Simulator	NS-2.34
Topology	Random
Number of nodes	50
Bandwidth	2.4Ghz
Propagation Model	Two Ray Ground
Physical Model	Wireless
Antenna model	Omni Antenna
Queue Size	50
Traffic type	CBR, UDP
Mobility Model	Random Way Point
Routing Algorithm	TBPRGKM

Packet size	512
Mac protocol	802.11 standard
Simulation Time	200Sec
Initial energy	100
Number of attackers	5,10,15,20,25

Result of our overall proposed scheme TPDGKM and existing ECC_HOMOMORPHISM scheme is compared which is highlighted using following comparison graphs:

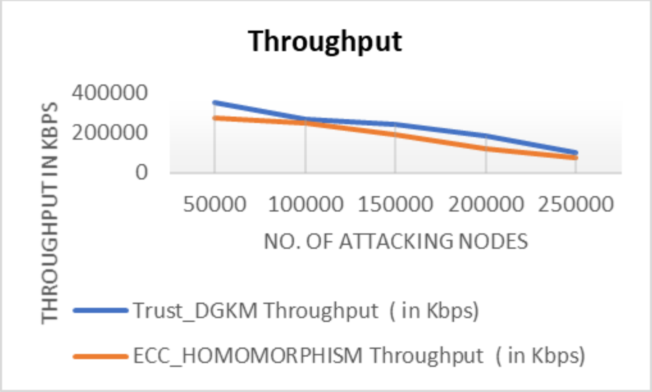

Fig 5. Throughput Comparison

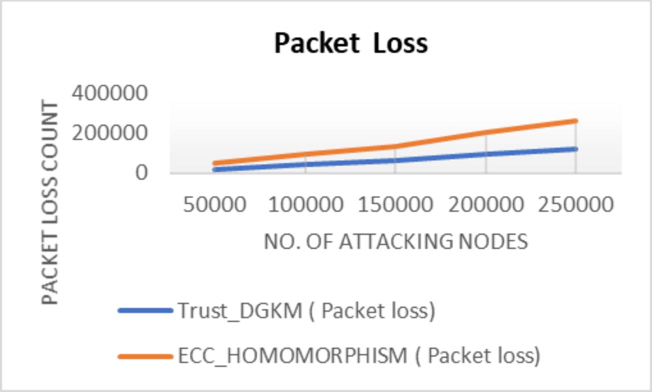

Fig 6. Packet loss Comparison

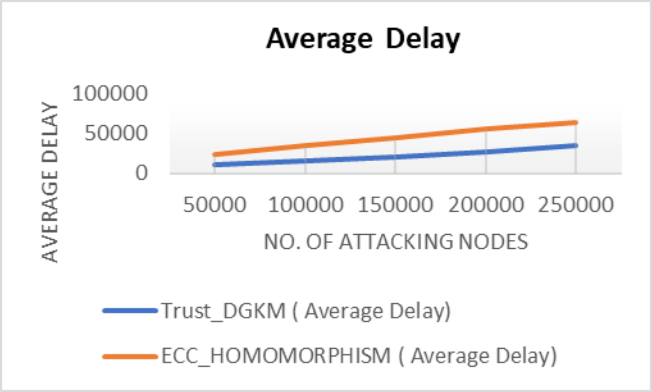

Fig 7. Average Delay Comparison

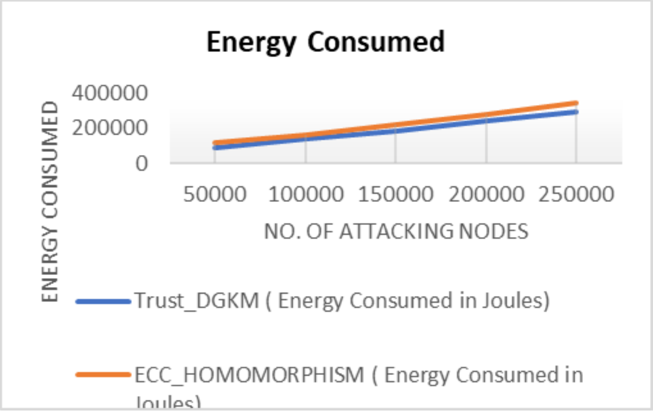

Fig 8. Energy Consumed Comparison

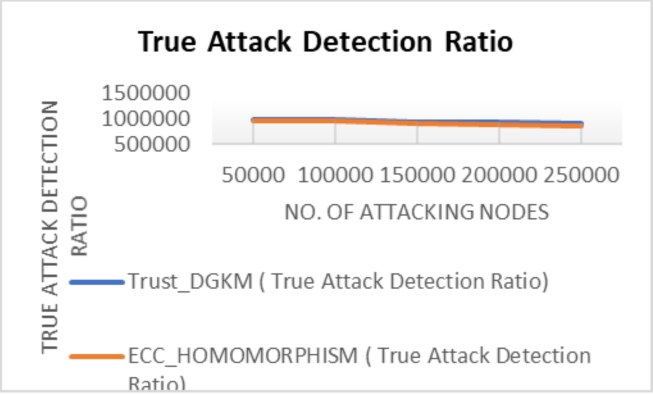

Fig 9. True Attack Detection Ratio Comparison

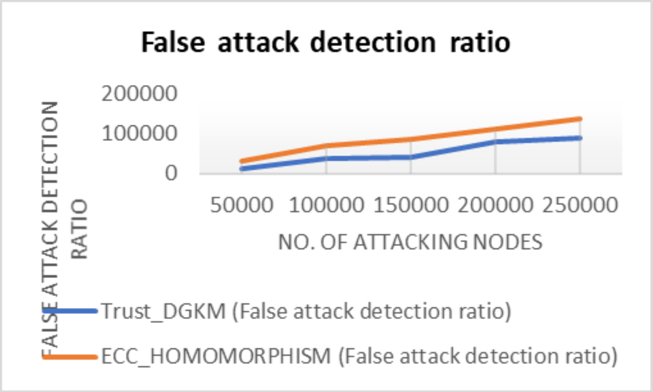

Fig 10. False Attack Detection Ratio Comparison

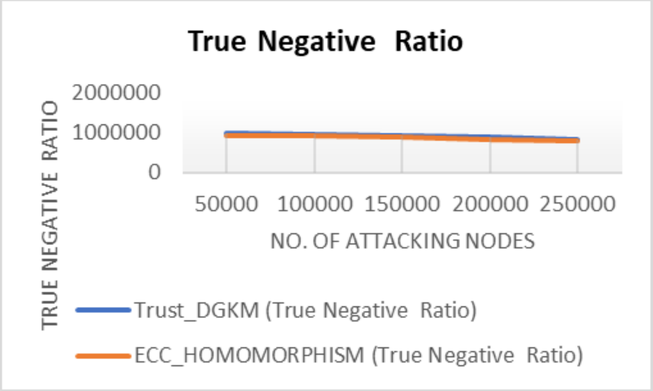

Fig 11. True Negative Ratio Comparison

VII. CONCLUSION

In our proposed security solution, the network is first initialized by creating complete nodes through which data transmission is about to be proceeded. Based on the nodes that are active, the cluster head is selected on basis of the trust value. The optimal key selection based on the trust value is the novelty which we employ in our proposed approach. Final cluster head (CH) selection depends on the trust value i.e., those which satisfies the threshold values will be finalized. With optimized combination of AES and distributed group key management data is securely transmitted between the nodes and hence ensures data integrity. With reduced amount of packet loss and less delay time, our proposed method is capable in achieving better multithreaded WBAN performance.

REFERENCES

1. Md. Taslim Arefin, Mohammad Hanif Ali, A. K. M. Fazlul Haque, " Wireless Body Area Network: An Overview and Various Applications", Journal of Computer and Communications, Vol.5, pp. 53-64, 2017.
2. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., & Kwak, K. S, "A comprehensive survey of wireless body area networks", Journal of medical systems, Vol. 36, no. 3, pp. 1065-1094, 2012.
3. Tobon, D. P., Falk, T. H., & Maier, M., "Context awareness in WBANs: a survey on medical and non-medical applications", Wireless Communications, IEEE, Vol. 20, no. 4, pp. 30-37, 2013.
4. Hadda Ben Elhadj , Jocelyne Elias , Lamia Chaari , Lotfi Kamoun, "A Priority based Cross Layer Routing Protocol for healthcare applications", pp 1570-8705, Elsevier, 2015.
5. Ms. Sanchari Saha, Dr. Dinesh K Anvekar, "Protocol Design Issues in Implementing Security for Wireless Body Area Network" , International Journal of Engineering and Technical Research, Vol. 2, no. 12,ISSN: 2321-0869, Dec.2014.
6. Rezgui, A., & Eltoweissy, M., "TARP: A trust-aware routing protocol for sensor-actuator networks", IEEE internatonal conference on mobile adhoc and sensor systems, 2007.
7. Channa, M. I., & Ahmed, K. M., "A reliable routing scheme for post-disaster ad hoc communication networks", Journal of Communications,Vol.6, no.7, pp. 549–557, 2011.
8. Marchang, N., & Datta, R. , "Light-weight trust-based routing protocol for mobile ad hoc networks", IET Information Security, Vol.6, no.2, 2010.
9. Zahariadis, T., Trakadas, P., Leligou, H. C., Maniatis, S., & Karkazis, P. "A novel trust-aware geographical routing scheme for wireless sensor networks", Wireless Personal Communications, Vol.69, no.2, pp. 805–826, 2013.
10. Meng Zhang, Anand Raghunathan, Niraj K. Jha., "Trustworthiness of medical devices and body area networks", Proceedings of the IEEE , Vol. 102, no. 8, 2014.
11. YataoYang, Shuang Zhang, Jhuming Yang, Jia Li and Zichen Li., "Targeted fully homomorphic encryption based on a double decryption algorithms for polynomials", Tsinghua science and technology, Vol. 19, 2014.
12. Samaneh Movassaghi, Mahyr Shirvanimoghaddam, Mehran Abolhasan, David Smith, "An energy efficient network coding approach for wireless body area networks", 38th Annual IEEE Conference on Local Computer Networks, 2013.
13. Tsung-Chih Hsiao, Yu-Ting Liao, Jen-Yan Hunag, Tzer-Shyong Chen, Gwo-Boa Horng, " An authentication scheme to healthcare security under wireless sensor networks", Springer, Vol. 36, no. 6, pp. 3649–3664, 2012.
14. Anurag Singh Tomar, CD Jaidhar, S Tapaswi, "Secure Session Key Generation Technique for group communication", International journal of information and electronics engineering, Vol.2, no. 5, pp. 831-834, 2012.
15. K. Malhotra, S. Gardner, R Patz, "Implementation of elliptic-curve cryptography on mobile healthcare devices", IEEE International Conference on Networking, Sensing and Control, 2007.
16. Ms. Sanchari Saha, Dr. Dinesh K Anvekar, "A Poly_hop Message Routing Approach through Node and Data Classification for Optimizing Energy Consumption and Enhanced Reliability in WBAN", IEEE International Conference on SMARTTECH ,Aug.2017.
17. Aftab Ali, Farrukh Aslam Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications", EURASIP Journal on Wireless Communications and Networking, 2013.
18. Ms. Sanchari Saha, Dr. Dinesh K Anvekar , "An Energy Efficient Cluster-head Formation and Medium Access Technique in Multi-hop WBAN", ICTACT Journal on Communication Technology, Vol. 09, no. 03, Sep.2018.
19. Mohammed Joda Usman et al "Recent Advances on Energy Efficient Cluster Based Routing Protocols of Wireless Sensor Networks for Healthcare Systems", International Journal of Computer Science Issues, Vol. 11, no. 3, pp.1694-0814, May 2014.
20. Qi Jiang et al, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth", ACM digital library, Journal of Medical Systems, Vol. 40 , no. 11, pp. 1-10,Nov. 2016.

AUTHORS PROFILE

Ms. Sanchari Saha holds a Master's degree from CMRIT (VTU), Bangalore, and Bachelor of Engineering degree from NIT, Agartala. Currently, she is working as an Assistant Professor in MVJCE, Bangalore, and pursuing research work towards her PhD degree. She has published a textbook titled "Object Oriented Modeling & Design pattern" and total 24 & counting more papers in reputed national & international journals and conferences. She has received gold medal from VTU for securing 1st rank during her Master's degree. She is a member of Indian Society for Technical Education.

Dr. Dinesh Anvekar is currently working as Director for Research & Product innovation, VVIT, Bangalore. He obtained his Bachelor degree from University of Visvesvaraya college of Engineering. He received his Master's and PhD degrees from Indian Institute of Science. He received best Ph. D Thesis Award from Indian Institute of Science. He has completed two Nokia sponsored projects in Indian Institute of Science during 1997-1998. He has filed 100 patents and 15 US patents issued for work done in IBM Solutions Research Center during 1998-99, Bell Labs during 1993-94, and Lotus Interworks during 2000-04, and for Nokia Research Center, Finland. He has authored a book and over 55 technical papers.