SMCRP : A SECURE MULTICAST CERTIFICATELESS ROUTING PROTOCOL FOR NETWORK SECURITY IN WBAN

Sujatha Rajkumar[1], Ramakrishnan. M[2]

Abstract

In Wireless Body Area Networks (WBAN), key factors are important issue to be considered for confidential data transmission that includes data security and privacy in emergency medical response systems. Comparing to Sensor Ad hoc Networks (MANET), security is a major concern in WBAN. Hence in this research, a Secure Multicast Certificateless Routing Protocol (SMCRP) for withstanding attacks in body area networks. It consists of three phases. First, the secure cluster topology is constructed in the body sensor networks based on path reliability and trust recommendation of sensor nodes. Second, the signcryption and unsigncryption phases are performed together to verify the authenticity of sensor nodes. Third, the secure multicast group management is performed to avoid replay attacks and to keep network connectivity. Last the packet format of proposed protocol ensures high confidentiality between the sensor nodes located in body area networks. Based on the extensive theoretical and practical simulation results, the proposed protocol achieves better performance interms of computational cost, time, delay, packet drop, delivery ratio, end to end delay.

Keywords : SMCRP, Certificateless signcryption and unsigncryption, delay, cluster topology, multicast group management, path reliability and trust recommendation of sensor nodes.

I. Introduction

The concept of WBAN is discovered by Zimmerman which is otherwise defined as Wireless Personal Area Network (WPAN) [1]. WBAN is the network that permits the combination of smart, small scale, minimum power, aggressive/discreet sensor nodes which monitors body activities and neighboring environment. Every intelligent node in the network has potential to forward the information to the base station after processing to obtain the diagnosis and prescription [3]. The application of WBANs is concerned with medical field and it also upholds consumer electronics applications concurrently [2].

The features of WBAN are listed below [3]:

- It is a miniature wireless network for communicating within 3 m gap · The speed at which the data is transmitted varies from 10 Kbps to 10 Mbps
- The star topology is the fundamental arrangement considered in WBANs and BAN Nodes (BNs) communicate with BAN Network Controller (BNC) alone

[1]Research Scholar, Karpagam University, Coimbatore.(Working as Assistant Professor, S.F.R College for Women, Sivakasi)

[2]Professor, Department of Computer Science, Periyar University, Salem.

- BNs possess restricted power, calculation and communication capabilities · Energy efficient security mechanism is required with reduced overhead and also the requirement such as data integrity, authentication and encryption should be fulfilled
- The network surrounds the body closely for implanting its communication system.
- BAN mainly detects, collects and transmits the biomedical information

In general, BAN applications deal with sensitive patient medical information but it has significant security, privacy and safety implications which may prevent the wide adoption of this technology. It has great privacy concerns in the public towards interoperable medical devices (IMDs) [4]; however, data security in BANs has not drawn enough attention, although the lack of it would lead to fatal consequences [5], [6]. Node authentication is the fundamental step towards a BAN's initial trust establishment and subsequent secure communications. Since IMDs transmit critical health monitor reports to and receive commands from the CU, if an attacker successfully pretends to be a legitimate sensor node or CU and joins the BAN, it can either report wrong patient health status information or inject false commands which may put the patient's safety at risk. In current practices, IMDs are not designed with enough security considerations. Over the years, a number of remote hacking incidents of individual IMDs [7], [8] are reported, which exploited unprotected wireless channels. In BANs, the situation is even worse if attackers can spoof multiple medical devices simultaneously. Thus, an effective node authentication mechanism is the key to BAN's security and patient safety.

Certificateless Signcryption ensures more confidentiality and data integrity. It avoids key escrow problem in identity based cryptography technique. In our proposed we achieve less computational cost, computational time because of integration of secure multicast and certificateless verification.

II. Related Work

Mohammed Mana et.al [9] presented a secure and efficient key exchange for wireless body area network to solve the problem of security and privacy in WBAN. The main of this key exchange was to generate and distribute securely and efficiently the session keys between sensor nodes and the base station to secure end to end transmission. The secure communication links were established between the nodes themselves using biometric data. The problem of this key exchange was lack of security and privacy.

Yuling Liu et.al [10] proposed an effective hashing method for image authentication. The log-polar coordinate transform and invariant centroid algorithm can be applied for geometric correction. Theoretical analysis demonstrated that the proposed feature is robust to the some geometrical attacks, such as translation, scaling, rotation, etc. This algorithm cannot only tolerate the perceptually similar manipulations, such as JPEG compression, low-pass filtering, median filtering, Gaussian noise, etc., but also can distinguish two visually distinct images.

Aftab ali and Aslam Khan [11] proposed and evaluated an energy-efficient key management scheme for WBANs. It was taken into account available resources of a node

during the whole life cycle of key management. This scheme was a cluster-based hybrid security framework that supported both intra-WBAN and inter-WBAN communications. By using multiple clusters, energy-efficiency was ensured. The cluster formation process itself is secured by using electrocardiogram (EKG)-based key agreement scheme. The ptechnique is hybrid because we use both preloading of keys and physiological value-based generated keys. A highly dynamic and random EKG values of the human body was used for pairwise key generation and refreshment.

Lu Shi eta.al [12] proposed a lightweight body area network authentication scheme that does not depend on prior-trust among the nodes and can be efficiently realized on commercial off-the-shelf low-end sensor devices. This was achieved by exploiting physical layer characteristics unique to a BAN and an off-body channel. This finding was that the latter is more unpredictable over time, especially under various body motion scenarios. This unique channel characteristic naturally was originated from the multi-path environment surrounding a BAN, and cannot be easily forged by attackers. Including this, the clustering analysis was also adopted to differentiate the signals from an attacker and a legitimate node.

Chunqiang Hu et.al [13] developed the Fuzzy Attribute-Based Signcryption that makes a proper tradeoff between security and elasticity. Fuzzy Attribute-based encryption was leveraged to enable data encryption, access control, and digital signature for a patient's medical information in a BAN. It also combines digital signatures and encryption, and provides confidentiality, authenticity, unforgeability, and collusion resistance. It allows a patient to specify a set of attributes and a physician is expected to possess in order to access a certain piece of sensitive information. It also allows a physician to access the data if the intersection between the physician's credentials and the required ones exceeds a pre-determined threshold.

Siva Sangari and Manickam [14] proposed a low cost and high quality electro cardiography and diagnostic system for healthcare applications. A major issue was how to preserve security and privacy of patient's medical healthcare information over wireless communication. The energy consumption and data security are still major challenges in healthcare applications. The scheme was based on light weight security algorithm. Skipjack is the secret key encryption algorithm which provides the secure communication between sensor node and sensor node. This algorithm protects the patient data against eavesdropping attack.

Ming Li et.al [15] proposed group device pairing (GDP), a user-aided multi-party authenticated key agreement protocol. Devices authenticated themselves to each other under the aid of a human user who performs visual verifications. This pairing supports fast batch deployment, addition and revocation of sensor devices, does not rely on any additional hardware device, and is mostly based on symmetric key cryptography. It also sets up an authenticated BAN group with much fewer human interactions than establishing authenticated individual shared keys between the nodes one at a time using traditional device pairing techniques. In GDP, each device authenticates itself to every other device in the group as a legitimate member, which can be verified visually by a human.

Lin Yao et.al [16] introduced an ECG (electrocardiogram) signal-based key establishment protocol to secure the communication between every sensor and the control unit before the physiological data are transferred to external networks for remote analysis or diagnosis. The uniqueness of ECG signal guarantees that our protocol can provide long, random, distinctive and temporal variant keys. Biometric Encryption technique is applied to achieve the mutual authentication and derive a non-linkable session key between every sensor and the control unit. The correctness of the proposed key establishment protocol was formally verified.

Sarah Irum et.al [17] proposed technique that was based on preloaded keys as well as keys automatically generated from biometrics of the human body. The biometric-based calculations are of linear time complexity to cater the strict resource constraints and security requirements of WBANs. The proposed security mechanism provides an efficient solution for the security of both intra- WBAN and inter-WBAN communications. The proposed inter-WBAN communication was purely based on preloading of keys. The minimum number of keys was used for preloading in the sensor's memory due to its small storage capability. This technique was efficient in terms of memory utilization and also in terms of security because the combination of auto key generation and preloading of keys strengthens the security of the technique.

Zhaoyang Zhang et.al [18] presented a novel key agreement scheme that allows neighboring nodes in BANs to share a common key generated by electrocardiogram (ECG) signals. The improved Jules Sudan (IJS) algorithm was introduced to set up the key agreement for the message authentication. The proposed ECG-IJS key agreement can secure data communications over BANs in a plug-n-play manner without any key distribution overheads. The ECG-IJS scheme shared a key in energy-efficient manner for BANs and a novel hash-based authentication approach was used to measure ECG signals at both sender's and receiver's sites. In this approach, ECG signals were used as biometric to generate keys in data encryption and hash-based message authentication.

Jingwei Liu et.al [19] presented a pair of efficient and light-weight authentication protocols to enable remote WBAN users to anonymously enjoy healthcare service. These authentication protocols were rooted with a novel certificate less signature (CLS) scheme, which is computational, efficient, and provably secure against existential forgery on adaptively chosen message attack in the random oracle model. These designs ensured that application or service providers have no privilege to disclose the real identities of users. Even the network manager, which serves as private key generator in the authentication protocols, was prevented from impersonating legitimate users.

Lu Shi et.al [20] proposed a lightweight body area network authentication scheme that does not depend on prior-trust among nodes and can be efficiently realized on commercial off-the-shelf low-end sensors. A unique physical layer characteristic was exploited naturally arising from the multi-path environment and the distinct received signal strength (RSS) variation behaviors among on-body channels and between on-body and off-body communication channels. Based on distinct RSS

variations, clustering analysis was adopted in BAN to differentiate the signals from an attacker and a legitimate node. It also make use of multi-hop on-body channel characteristics to enhance the robustness of the authentication mechanism.

Daojing He et.al [21] proposed a lightweight and confidential data discovery and dissemination protocol. It used low-complexity symmetric cryptographic techniques for maintaining confidentiality. The encryption key was changed on a per-packet basis to prevent the intermediate nodes from forging the keys, ensuring authenticity of the broadcast data items. This solution conformed with the resource limitations of a WBAN. This dissemination protocol also presented the design, implementation, and evaluation of a secure, lightweight, confidential, and denial-of-service-resistant data discovery. Based on multiple one-way key hash chains, this protocol provided instantaneous authentication.

Osman Salem et.al [22] proposed a lightweight anomaly detection approach for medical WSNs, where faulty measurements and injected malicious data could threat the life of the monitored patient. This approach was based on wavelet decomposition, non-seasonal Holt–Winters, the Hampel filter, and boxplot. It allowed achieving spatial and temporal analysis, without prior knowledge of fault signatures. It was suitable for online detection and isolation for faulty or maliciously injected measurements with low computational complexity and storage requirement.

Our aim is to arrive at a multicast protocol which strikes a balance between defending against attacks and more energy consumption of nodes.

III. Overview Of Optimized Multicast Routing Scheme

In this research, a certificateless secure protocol is proposed for WBAN. It consists of set of body area networks connected to the sub server. This server communicates the biometric information calculated by the sensor node to the main server through the online mode. Once the information is established, all sensor nodes will determine the main server based on the sensor node id. The main server will then create a single secret key for each node. When a sensor node wants to join a network in the region, it forwards a Hash based MAC (HMAC) protected message to the main server via the sub server. The main server verifies the HMAC and calculates a data key and a main key for the sensor node and sends it to sub server. The sub server encrypts data key with main key and sends it to the sensor node that initiates the joining procedure. After all the sensor nodes receive key information from main server, the cluster server schedules re-generating period to restore the main key.

Secure Cluster WBAN Construction based on Reliable Paths:

Cluster is formed based on reliable neighbor nodes using trust vector value. It is derived from how much of packet information is successfully carried via neighbor nodes from source node to destination node. The packet integrity should be maintained through the entire route. Each node has routing table which contains packet information, packet id, cluster member id, node to node connectivity, neighbor coverage range, link quality etc.

Based on high and medium trust vector value, the node is considered as a cluster head otherwise cluster member.

Trust Vector T_B^A is given by,

$$\frac{\textit{Outcoming delivered packets from node B - Packets sent from node B to A}}{\textit{Incoming received packets from node B - Packets sentfrom node A to B}} \quad (1)$$

After calculating trust vector value, each node chooses one node that has highest trust value, it is called trust authenticator. Then the trust authenticator becomes cluster head and the chooser is considered as cluster member node. If the chosen sensor node is already a member of another cluster region, a sensor node of high trust value is selected. In this way, the cluster region is formed.

Route establishment:

Route is established between the nodes based on link stability. For transmission range T_r link stability L_{sb} between any two nodes overtime period t can be calculated by:

$$L_{sb} = \frac{T_r}{\sqrt{\left\{\left(p_1^{'} - p_2^{'}\right) + t\left(n_1\cos\theta_1 + n_2\cos\theta_2\right)\right\}^2 + \left\{\left(q_1^{'} - q_2^{'}\right) + t\left(n_1\sin\theta_1 + n_2\sin\theta_2\right)\right\}^2}}$$

L_{sb} is the link stability of individual links between any two nodes and for a path and it is same as the minimum link stability along the path. Once the stability is calculated, the route discovery process is initiated by means of flooding route request packet from source to destination. If any destination node replies with route reply within periodical time, stability rate is high otherwise it is low. Cluster head maintains the link stability status among all the cluster members to the destination. If any route having high stability rate, that route is given with first priority for packet transmission. All cluster members update route establishment status to cluster head based on link stability rate. In order to avoid link break or failure by means of malicious attackers, link stability is maintained among all cluster members and cluster head.

Certificateless Routing:

The proposed protocol consists of two parties namely sending sensor node and receiving sensor node. Three phases are present in this protocol based on elliptical curves as follows:

- Key generation
- Signcryption
- Unsigncryption

Key Generation:

In this key generation process, the encryption and authentication are essential for message transmission in the network. In the initial phase, main server generates and publishes all the public parameter of elliptic curve as well as each sensor node chooses his own private key and calculates his related public key.

In this phase, main server generates the parameter based on elliptical curve procedure.

1. p is a prime number.
2. Initialize the (a, b) two integer element and $(a, b) < p$ that satisfies $4a^3 + 27b^2 \neq 0 \bmod p$.
3. Define the elliptic curve over finite field F with order n, which satisfy equation $y^2 = x^3 + ax + b \bmod p$.

4. Set the base point G of F.

5. Find the hash function $H : \{0,1\}^* \rightarrow Z_p$

6. Publish parameters (p, G, a, b, H, n).

Generating Private key and Public key of sending sensor node by main server

Private key : $X_I \in [1,2,.....(n-1)]$ Public Key : $Y_I = X_I.G = (Y_{I1}, Y_{I2})$

Calculating the public key and private key of receiving sensor node

Private Key : $X_m \in [1,2,.....(n-1)]$ Public Key : $Y_m = X_m.G = (Y_{m1}, Y_{m2})$

Signcryption:

Signcryption is a cryptographic primitive which achieves integrity and confidentiality in a single logical step. Signature then encryption requires two steps but by signcryption only one step is sufficient for achieving confidentiality and integrity so signcryption reduces the communication as well as computation cost and increase the efficiency.

Step 1: Select the random integer $w \in [1, n-1]$

Step 2: Determine the secret key from the main server

$$K = t.Y_I = (K_1, K_2)$$

Step 3: Derive the session key for encryption as

$$k = H(x_k \parallel ID_{sn_i} \parallel y_k \parallel ID_{rn_j})$$

Step 4: Compute the cipher text $C = E_{K_1}(m)$

Step 5: Determine the master key $B = H(m, K_2)$

Step 6: Compute the digital signature

$$s = (t - B.X_I) \bmod n$$

Step 7: Send the signcrypted text $\delta = (c, B, s)$

Unsigncryption

Receiving node receives the signcrypted text and decrypt the text to extract plain text and verify the digital signature as follows:

Step 1: Computes the session key based on master key and digital signature

$$K' = s.Y_m + B.X_I.Y_m = (K_1', K_2')$$

Step 2: Recover the message from signcrypted text is

$$m' = D_{K_1'}(c)$$

Step 3: Verifies the authenticity by following condition

$$B' = H(m', K_2')$$

Physical Authentication Model:

From the proposed model, wireless devices can authenticate themselves through wireless data channel for assisting physical data transmission among devices. The physical data transformation involves the user's actions such as replication of the data output from one device to the other device, comparison of output of two devices, entering similar data into both the devices. This process does not require the user to enter long strings of digits. In general, the user has to either enter or evaluate approximately 32 binary digits.

Secure Multicast Group Formation:

In the proposed secure multicast, hop by hop encryption is adopted. Packet is multicasted with its level key. Each member node that is a logical child of the cluster head will then decrypt the message. If the member node receiving the packet is a parent of a subsequent level, the node will re-encrypt the message using its parent level key and send the message onto each of its children. The packet format is given as,

Cluster group ID + MAC ID+ Seq.No+ Message (3)

At each level the packet will be decrypted and re-encrypted with the next level's keys before being sent on. An alternative would be to have the cluster head generates a random key, *K*, and encrypt the message with this key. At each level, the parent decrypts and re-encrypts *K*, but not the entire message. This would speed propagation of the message by saving us from having to decrypt and re-encrypt the entire message at every level during packet forwarding.

F. Packet format of SMCRP

Source ID	Destination ID	Hop Count	Data Confidentiality	Integrity	FCS
2	2	1	4	4	2

Figure 1 : SMCRP Packet format

In figure 1, the proposed packet format of SMCRP is shown. Here the source and destination node ID carries 2 bytes. The third field hop count determines the number of n does connected to the particular node in the cluster. It occupies 1 byte. The data confidentiality occupies 4 bytes. Each sensor node checks integrity of the packets to destination nodes. The last filed FCS i.e. Frame Check Sequence which is for error correction and detection in the packet while transmission.

G. Description of SMCRP

The proposed scheme is to identify the authenticated route in the network. For that, secure multicast backbone is constructed to find the trustable and non trustable nodes using the link and node stability ratio estimation. In previous multicast routing schemes, either link or node stability is focused. Based on signcryption, the network achieves high network integrity.

IV. Performance Evaluation

The performance of the proposed approach is evaluated in this section. The simulation model is discussed in Section 6.1 and the simulated results are presented and described in Section 6.2.

A. Network Model

In the proposed network model, it is assumed that K+1 sensor nodes are present in the network while taking the source node is K and destination node is (K+1). The packets are received in a queuing order from the rest of K nodes. The proposed model is symmetric and synthetic model. Here the sensor node may in the transmission range or out of the range. The packets are transmitted in a fixed size and the route discovery time is deterministic. Packets are arrived to the destination according to the Markovian Arrival Process in discrete time (DBMAP/D/1/N). Here, N is the buffer size of the destination sensor node. So, the process is in the queuing condition. Mobility

nodes are randomly chosen while considering the packet loss probability which involves transition matrix is (K+1)(N+1) x (K+1)(N+1).

B. Simulation Model and Parameters

We have simulated our results using NS2.34 simulator. It is an object oriented discrete event simulator to identify the performance of proposed scheme. The Backend language of NS2.34 is C++ and front end is Tool command language (Tcl). NS2 is user friendly and easy to fabricate our own protocol. Tcl is a string-based command language. The language has only a few fundamental constructs and relatively little syntax, which makes it easy to learn. The syntax is meant to be simple. Tcl is designed to be glue that assembles software building blocks into applications. Here we made the assumption that adopted for simulation is all nodes are moving dynamically including the direction and speed of nodes. Mobility scenario is generated by using random way point model with 100 nodes in an area of 1000 m × 1000 m. Our simulation settings and parameters are summarized in table 1.

Table1. Simulation and Settings parameters of SMCRP

No. of Nodes	100
Area Size	1000 X 1000
Mac	IEEE 802.15.4
Radio Range	250m
Simulation Time	50 sec
Traffic Source	Exponential
Packet Size	512 bytes
Routing Protocol	SMCRP

D. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio :

It is the ratio of the number of packets received successfully to the total number of packets transmitted.

Communication Overhead :

The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets. It suppresses the communication between the source and destination nodes.

End-to-end delay :

It depends on the routing discovery latency, additional delays at each hop and number of hops.

Packet Drop :

It is the ratio of number of packets dropped to number of packets successfully sent.

E. Results

We compared our proposed protocol with ECG-IJS[18], CLS [19] and BANA [20]. The results are examined by using performance metrics end-to-end delay, packet delivery ratio, computational cost, computational time, packet drop rate, end to end delay and overhead.

Fig.2 shows the analysis of Energy efficiency Vs Time. From the results, our proposed protocol achieves high energy than the existing schemes namely BANA, ECG-

IJS and CLS because of secure multicast deployed in the optimized routing.

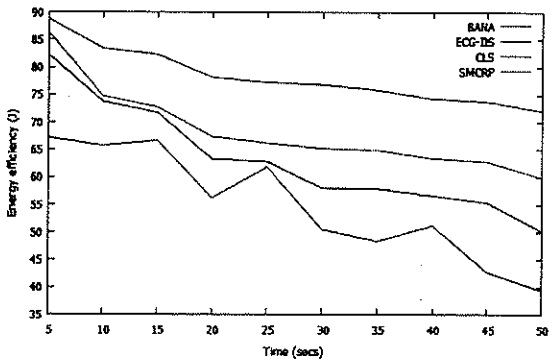

Figure 2 : Energy Efficiency Vs Time

In Fig.3, we vary the time from 20 to 200. While increasing the time, the computational time of proposed protocol SMCRP has low than ECG-IJS, CLS and BANA. This is achieved by employing the key factors used in the transmission process.

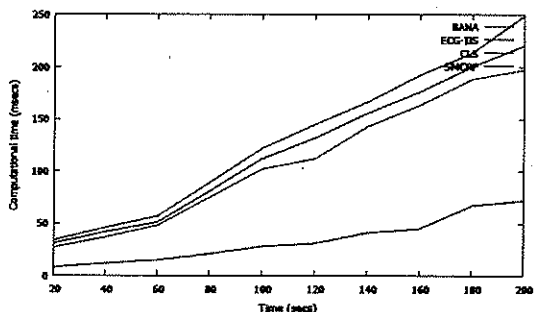

Figure 3 : Computational Time Vs Time

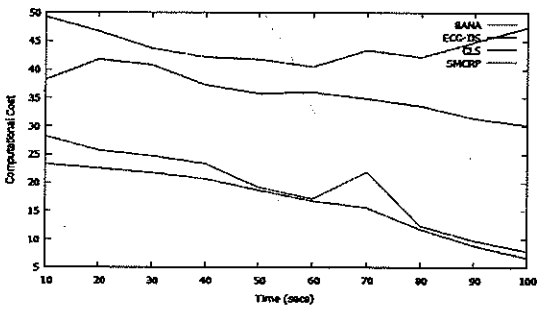

Figure 4 : Computational Cost Vs Time

In Fig. 4, time is varied from 10 to 100 msec. The computational cost of proposed protocol achieves fewer resources than ECG-IJS, CLS, BANA and RMRBDP because of high path reliability criterion.

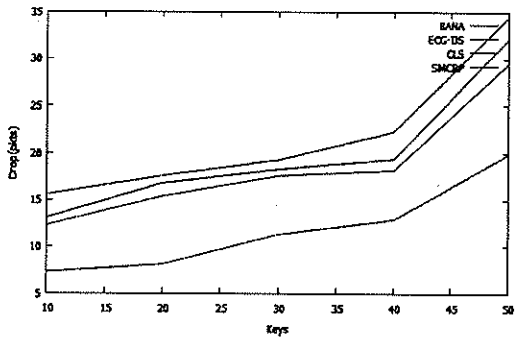

Figure 5 : Drop Vs Keys

In fig. 5, we vary keys from 10, 15,...50. The packet dropping rate of SMCRP achieves lesser than ECG-IJS, CLS, RMRBDP and BANA.

In Fig 6, key is varied as 10, 20....100. When we increase the number of keys, the delay is also getting increasing. The proposed protocol SMCRP has low end to end delay per packet than ECG-IJS, CLS, BANA and RMRBDP.

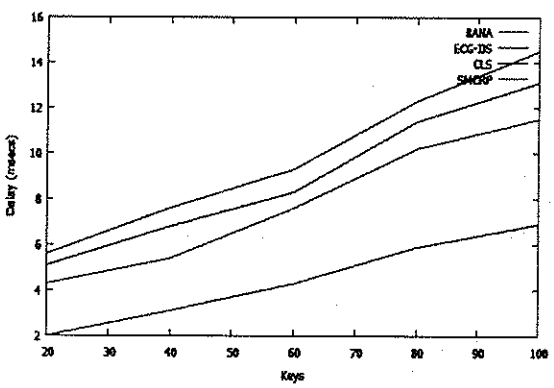

Figure 6 : End to end delay Vs Speed

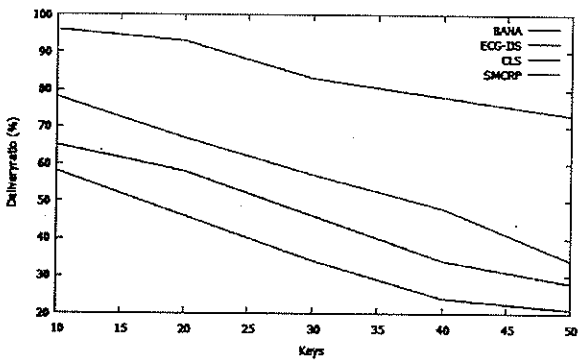

Figure 7 : Delivery Ratio Vs Keys

In Fig. 7, keys are varied as 10, 20....50. The packet delivery ratio of the proposed protocol SMCRP is high than ECG-IJS, CLS, BANA and RMRBDP. While residual energy of the path increases, the delivery rate is getting increased.

V. Conclusion And Future Work

A secure multicast certificate less routing prtocol for WBAN to achieve security challenges. The proposed protocol contains cluster topology that includes main server and sub server to verify the authenticity of biometric information. Through the propsoed signcryption and unsigncryption scheme, the data is transmitted securely and the vulnerability of inside and outside the attackers is avoided. The propsoed scheme uses symmetric master key to achieve authentication of sensor node located in BAN. The proposed protocol is simulated with NS2 to evaluate its performance. Comparing to previous scheme, it acheives better performance than existing schemes. In future, we plan to combine both elliptical curve and identity based cryptography schemes to maintain the secrecy policy of the networks. Energy model will also be integrated in future to avoid more consumption of network resources.

REFERENCES :

[1] Li, C., J. Li, B. Zhen, H.B. Li and R. Kohno, 2010. *"Hybrid unified-slot access protocol for wireless body area networks"*, Int. J. Wireless Inform. Networks, 17: 150-161. DOI: 10.1007/s10776-010-0120-2.

[2] Ullah, S., B. Shen, S.M.R. Islam, P. Khanemail and S. Saleem et al., 2009. *"A study of MAC protocols for WBANs"*, Rev. Literature Arts Am., 10: 128-145. DOI: 10.3390/s100100128.

[3] Khan, P., M.A. Hussain and K.S. Kwak, 2009. *"Medical applications of wireless body area networks"* Int. J. Digital Content Technol. Appli.

[4] *"Experts see data breach risks in medical devices on hospital networks,"* may 2011. [Online]. Available : http://www.ihealthbeat.org/articles/2011/5/12/experts-see-databreach-risks-in-medical-devices-on-hospital-networks.aspx

[5] M. Li, W. Lou, and K. Ren, *"Data security and privacy in wireless body area networks,"* IEEE Wireless Commun., vol. 17, no. 1, pp. 51– 58, february 2010.

[6] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, *"Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body,"* in Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on, oct. 2003, pp. 432–439.

[7] K. Timm, *"Medical device hacking prompts concern,"* august 2011. [Online]. Available: http://www.cyberprivacynews.com/2011/08/medicaldevice- hacking-prompts-concern/

[8] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, *"Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,"* in Security and Privacy, 2008. SP 2008. IEEE Symposium on, may 2008, pp. 129–142.

[9] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber, *"SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network),* International Journal of Advanced Science and Technology, Vol. 12, November, 2009, pp.45-60.

[10] YuLing Liu, Yong Xiao, *"A Robust Image Hashing Algorithm Resistant Against Geometrical Attacks",* Radioengineering, Vol. 22, No. 4, December 2013, pp.1072-1081.

[11] Aftab Ali and Farrukh Aslam Khan, *"Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications",* EURASIP Journal onWireless Communications and Networking, Vol.216, 2013, pp.1-19.

[12] Lu Shi, Ming Li and Shucheng Yu and Jiawei Yuan, *"BANA: Body Area Network Authentication Exploiting Channel Characteristics",* Wisec, 2012, pp.1-12.

[13] Chunqiang Hu, Nan Zhang, Hongjuan Li, Xiuzhen Cheng and Xiaofeng Liao, *"Body Area Network Security: A Fuzzy Attribute-based Signcryption Scheme",* IEEE Conference, 2012, pp.1-10.

[14] A.Siva Sangari and J.Martin Leo Manickam, *"Light Weight Security and Authentication in Wireless Body Area Network",* Indian Journal of Computer Science and Engineering, Vol. 4, No.6, Dec 2013-Jan 2014, pp.438-446.

[15] Ming li, shucheng yu, Joshua. D. Guttman, wenjing lou and Kui ren, *"Secure Ad-Hoc Trust Initialization and Key Management in Wireless Body Area Networks"* ACM Transactions on Sensor Networks,2010,pp.1-35.

[16] Lin Yao, Bing Liu, Guowei Wu, Kai Yao, and JiaWang, *"A Biometric Key Establishment Protocol for Body Area Networks",* International Journal of Distributed Sensor Networks, 2011, pp.1-11.

[17] Sarah Irum,Aftab Ali, Farrukh Aslam Khan, and Haider Abbas, *"A Hybrid Security Mechanism for Intra-WBAN and Inter-WBAN Communications",* International Journal of Distributed Sensor Networks, 2013, pp.1-12.

[18] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang, *"ECG-Cryptography and Authentication in Body Area Networks",* IEEE Transactions on Information Technology in Biomedicine, Vol. 16, No. 6, November 2012, pp.1070-1078.

[19] Jingwei Liu, Member, IEEE, Zonghua Zhang, Xiaofeng Chen, and Kyung Sup Kwak, Member, IEEE, *"Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks"*, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, 2014, pp.332-342.

[20] Lu Shi, Student Member, IEEE, Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, and Jiawei Yuan, Student Member, IEEE, *"BANA: Body Area Network Authentication Exploiting Channel Characteristics"*, IEEE Journal on Selected Areas in Communications, Vol. 31, No. 9, September 2013, pp.1803-1816.

[21] Daojing He, Member, IEEE, Sammy Chan, Member, IEEE, Yan Zhang, Senior Member, IEEE, and Haomiao Yang, Member, IEEE, *"Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks"*, IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 2, March 2014, pp.440-448.

[22] Osman Salem, Yaning Liu, Ahmed Mehaoua, and Raouf Boutaba, Fellow, IEEE, *"Online Anomaly Detection in Wireless Body Area Networks for Reliable Healthcare Monitoring"*, IEEE Journal of biomedical and health informatics, Vol. 18, No. 5,September 2014, pp.1541-1551.

AUTHOR'S BIOGRAPHY

Sujatha Rajkumar received the B.E. Degree from the Department of Electronics and Communication Engineering, Madras University, Chennai, India, in 1999. She received the Master of Engineering Degree from the Department of Applied Electronics, Anna University, Chennai in 2008. She has published five papers in international Journals. She has published six papers in International Conference and eleven papers in National Conferences. She is an active member in IETE. She is pursuing her PhD in Information and Communication Engineering under the supervision of Dr.M.Ramakrishan. Her research interests are Network Security, Certificateless Sisgncryption, Compressed Signcryption and parallel computing.

Dr. M. Ramakrishnan was born in 1967. He is currently as a Professor and Head, School of Computer Science, Madurai Kamarajar University, Madurai, India. He received Ph.D Degree in Computer Science, Anna University, Chennai, 2008, Ph.D Degree in Computer Science & Engineering, Anna University Coimbatore, Tamil Nadu, in 2011. He is a supervisor for research scholars in reputed Universities. His research interests include Parallel Computing, Image Processing, Web Services and Network Security. He has 23 years of teaching and research experience and published 20 International journals and 47 National and International conferences. He is active member of ISTE, CSI and Senior Member of IACSIT.