Three Tire Proxy Re-Encryption Secret Key (PRESK) Generation for Secure Transmission of Biosignals in Wireless Body Area Sensor Networks

M.V. Karthikeyan*, J. Martin leo Manickam
Electronics and Communication Engineering, St. Joseph's Institute of Technology, Chennai - 600119, India.
***Corresponding author: E-Mail: karthik.me09@gmail.com**

ABSTRACT

In IEEE 802.15.4 Wireless Body Area Networks (WBAN), security solution is more important to achieve data confidentiality, authentication and integrity. Here, we have proposed three tier security architecture. It consists of Bio-medical sensors each will sense any of the body parameters (Heartbeat, pulse rate, blood pressure etc.,) out of which one is considered to be Master sensor node (pacemaker), mandatorily made to sense the ECG signal. Another handheld node called the Network Controller and Coordinator (NCC) placed outside the body sends the request to the Master Sensor Node (MSN) to sense the ECG signal. In primitive systems, the sensor is placed inside the patient body itself making it energy stringent. This can be overcome by placing the NCC sensor outside the body in the form of PDA phone. On receiving the broadcast request from the NCC, the master sensor node generates a proxy re-encryption key and broadcasts it to the other biomedical sensors. The first tier of security system is established by using Proxy Re-encryption Algorithm. The sensed parameters from all the three sensors are encrypted and sent to NCC. The NCC aggregates data from all the three sensors and encrypts the data to form the second tier of security using Data Encryption Standard (DES) algorithm. Each user has a Home Access Point (HAP) attached to his/her home. The NCC transmits the data to HAP which in turn transmit it to the Hospital Gateway (HG). The third tier of security system is brought into action from HAP to the HG. Which encrypts the parameters using Ad-hoc On Demand distance Vector (AODV) routing. A doctor in remote location can examine the patient data by decrypting the parameters with a promising authentication. The simulation set up the entire sensor node structure is done using Network Simulator 2.

KEY WORDS: Proxy Re-encryption, Data Encryption standard, Ad-hoc On Demand distance Vector routing, Home Access point, Hospital gateway.

1. INTRODUCTION

A wireless Body Area Network (WBAN) is a Radio frequency based embedded technology that interconnects tiny sensors or actuators having the capabilities, of sensing Bio signal when placed in, on or around a human body. It can cover a transmission range of about 2m (meter). It had evolved from the wireless personal Area Networks (WPANs) which has a 10m radio coverage. The rapid growth in technology of embedded system and wireless technology has led to the fast growth of WBAN in many areas like astronauts' space suit, post-surgical patient, sports persons and aged persons. But due to the miniature size of the WBAN Node's, it has its own limitations like, small memory, small battery size and limited processor. The key issue is to deal with the trade-off between the cost, memory and power with that of security. To achieve the security requirements various cryptographic codes have been developed and proposed. An efficient key management cipher model is proposed with the help of existing cipher codes like Proxy Re-encryption algorithm and the Data Encryption standard (DES). Cryptographic algorithms can be differentiated into two wide categories, known as symmetric key algorithm and asymmetric algorithm (Tassos Dimitriou, 2008; Karthikeyan, 2016). Asymmetric key is Elliptical Curve Cryptography (ECC), RSA El-Gamal and others has an increase in size of the code and require large amount of processing power, memory and bandwidth which limits them for the implementation in WBAN (Shahnaz Saleem, 2009; 2011). Thus, symmetric key algorithm is chosen for our WBAN model, which has the efficient key management and low energy consumption character in it.

Attack in WBAN: Due to the wireless channel the WBAN is vulnerable to various security threats. The most common attacks are:

Data Modification: The Data transmitted over the wireless channel is obtained and modified or replaced by the attackers. This altered information is sent back to the receiver end as if no modifications are performed. These alterations are performed to misguide the treatment by doctors also the original data are achieved for some illegal purpose.

Eavesdropping: which means listening to the wireless medium secretly without the knowledge of communicating nodes. The node communication between WBANs can be easily intercepted by the attackers leading to security breach.

Replaying attacks: A portion of the transmitted information, eavesdropped by the hacker and retransmitted after sometime. The receiver end will obtain two information at one time. The real time data and other one is an old message which arise a different result in doctor's treatment that may risk patient's life.

Impersonal attack: The eavesdropper takes the legal information of either the Body Area Network coordinator or the Body Area Node Identification information. With this legal identity information the attacker pretends to be the controller or node and cheat others.

Denial of service: The denial of service (DOS) attack occurs when the system traffic is beyond its capacity. It may be due to the unintentional peak or by using the infected Body node traffic it can be maximized thus initiating a DOS attack easily.

WBAN Security Requirement: The characteristics of WBAN function are needed to build a robust security mechanism. The primary security requirements in WBAN are described below.

Data Confidentiality: To defend the patient vital signs from disclosure, the system require data confidentiality. The Body area Nodes' BN's communicate health status of patient's to the aggregator. During communication the attacker can possibly eavesdrop the information. As these vital signs of patient's are utilized for many illegal purposes, Encryption of the information with a secret key and sharing the secret key in a secure channel is one of the ways to acquire confidentiality.

Data Authentication: The Wireless Body Area Network coordinator and the node has to verify themselves that whether the data were transmitted and received between the trusted sensor and not with any adversary. As the adversary can deceive it as a BN's to accept false data. It can be used to data authenticate and distribute the secret key to compute the Message Authentication Code (MAC) for all data transmission (Sana Ullah, 2010).

Data integrity: Data integrity assures that the received data is not altered by the adversary, when transmitted over an insecure channel. Data integrity is attained by using Data authentication protocols. In absence of Data integrity, the adversary will modify the information before it reaches the Receiver end.

Data Freshness: The Data freshness technique is the backbone to assure better performance of data confidentiality and data integrity. The adversary will confound the BNC by removing the data during transmission and retransmit them later to the same receiver. The data integrity module checks the sequence and freshness of the data frames. It can be of two types: strong and weak data freshness. Strong freshness guarantees the ordered data frames and fresh data (zero delay) at the Receiver end with weak freshness partial data frames ordering and has guarantee delay. The low duty cycle BNs measures the vital signal like Blood pressure (BP), it makes use of Weak freshness. Equally, when controller transmits beacon signal it uses strong freshness and during synchronization.

Secure Management: As controller, distribute keys to nodes to achieve encryption and decryption techniques, it demands secure management. The controller adds and removes the BNs in a secure manner in the case of grouping and disassociation.

Availability: It guarantees that the patient's information is accessible to the doctor. The adversary can deactivate patient's BNs and delink the accessibility with the doctor end system. This may lead to crucial condition such as loss of life. During the absence or hiding of BN's, a procedure is required to continue the operation of the BN's and switch the operation to another BN's is availability.

Related Work: Chiu (2009), have developed a lightweight identity based encryption (IBE) suitable for WBAN, a protocol based model. It has a good trade-off between security and privacy with accessibility. Experimental results are provided with elliptical curve cryptography, (Asymmetric) giving more power consumption and making it unsuitable for WBAN. Jingwei Liu (2010), proposed a hybrid security structure for WBAN for secure communication over wireless channel. In their proposed approach, symmetric and asymmetric cryptographic algorithms are combined to obtain a security structure for a low resource constraint device. Which provides improvement in efficiency. MaSahiro Kuroda (2009), have developed a Secure Body Area Network (S – BAN) with a less computation model, by reducing the process overhead on the sensor. It automatically generates the private key with zero-administration overhead. All the data exchanged between sensors are in ordered format. Only the power and efficiency is provided and no data is provided about power consumption during data transfer and data recovery. Huang (2009), have presented three network tire security architecture for WBAN. They have combined a various security models like, the polynomial based encryption, Ad-hoc based routing, third party key agreement and public key cryptography. These above security systems provided secure approach. But a valuable implementation with proper position of the sensor system and their over power system model is not provided. Hind Chebbo (2012), have proposed a Tree Topology model which is an extension version of the star topology have restricted the number of hop in the relay nodes. This WBAN model gives a support for reliable data transfer between sensor nodes in medical application. Their Restricted Tree Topology [RTT] has an opportunistic relay, dynamic and manageable energy budget model with increased reliability, which make it a dependable model in data forwarding. But the Tree Topology doesn't work in all scenarios, as the cluster head changes depending on the resources, making it difficult to obtain the Tree Topology cluster head. Mohanavalli (2011), had proposed a model to sense data in an obstruction environment and also in remote patient monitoring. Their design gives a data confidentiality, integrity and authenticity in collection of medical signals from patients and that of forwarding to the hospitals. The complete pervasive model has been approached in this technique. Still there is a lag in the data authentication technique.

Cryptographic Models Applied To Secure Bio-Signal: The Bio-medical signal generated from the human body is a vital biological information. So the Bio-information must be communicated in secure manner, we had considered the below existing implementations and given a simulation result for supporting secure data transfer.

BBS Proxy Re-Encryption: The Proxy Re-Encryption (PRE), invented in 1998 (Mambo, 1997; Blaze, 1998), allowing a user to decrypt his own message in case of his unavailability. Proxy Re-Encryption is a public key encryption (Markus Jakobsson, 1999; Green, 2007) allowing a user Annie to “delegate” her decryption rights to another user Brown. For example, if Annie and Brown are users in an encrypted email system. Annie wants to temporarily forward message to Brown when he is out of station. In this situation she might instruct the mail server (proxy) to automatically re-encrypt her incoming mail to Brown’s key.

Proxy Re-encryption:

$$C_a \longrightarrow \boxed{\textbf{Mail Server}} \longrightarrow C_b$$

$$C_b = (g^r \cdot m, (g^{ar})^{RK})$$

$$C_{\,b} = (g^r \cdot m, (g^{ar})^{b/a})$$

$$C_{\,b} = (g^r \cdot m, g^{br})$$

C_a- Annie’s key, C_b –Bill’s Key, RK-Random Key, g-Prime Number, r-Random

To delegate the decryption rights to Brown, Annie generates a “delegation key” (or “re-encryption key). To do this she computes a piece of information with her secret key and her delegate’s public key. [Annie is the Delegator and Brown is the delegate] to generate the Re-encryption key and send it to the proxy. The proxy is considered “semi-trusted” because the content of the message during translation is not seen. Even if the malicious system administrator wants to read the Annie’s mail, the data is unavailable to any one besides Annie or Brown. Proxy uses the key to translate data from Annie’s secret key to Brown’s public key. The proposed PRL model used here is unidirectional, i.e., the proxy can re-encrypt Annie’s message to Brown, but cannot re-encrypt Brown’s message to anyone.

DES Algorithm: Security plays a very vital role in the field of data communication. There are two major cryptography namely, symmetric and Asymmetric key cryptosystems. Symmetric key cryptography use the same key for Encryption and Decryption, which can be classified as DES, AES, 3DES, IDEA and Blowfish algorithm. The Asymmetric key cryptography uses two key, one key for Encryption and a different key for decryption, that includes RSA, Digital signature and Message Digest algorithm for all these two entirely different keys are used. The Data encryption standard (Copper Smith, 1994) algorithm is a private key cryptosystems that best suits for a resource constrain system. If an Asymmetric key is selected the level of security will be high, and also the energy consumption will be high, making it unsuitable for a low resource constraint model. Based on this discussion we had adopted the DES algorithm for our model. It has a series of algorithm, block cipher and feedback. In this model it is mandatory that both sender and receiver must know about others secret key to form the Proxy Re-Encryption key. As their own secret key is pre-deployed in the sensor node itself made the DES a powerful security scheme and encryption over a trusted nodes. The second tire security model is developed using the simplified DES algorithm and applied for WBAN. That had proven for smart cards, SIM cards and miniaturized embedded systems. All support a 64 bit key size we too handled with it.

Ad - Hoc on Demand Distance Vector (AODV) Routing Protocol: The Reactive Routing Protocol establishes a route to the destination only when a demand arises. Both unicast and multicast routing is possible with Ad-Hoc on Demand distance Vector routing (Kimaya Sanzgiri, 2002). All the information to the destination node is forwarded with the help of a routing table, which contains information about recalling the destination node. Until a call arises the entire network is silent. When the network node needs a connection, it broadcast a request down the network for connection to the destination. All the nodes receives the message and forward it by creating a temporary route. When the destination node hears the message, it finds a message backward through the temporary route to the defined node. This message consists of the route information that is having the least number of hops. The destination route is updated on an on-demand basis and the link set up delay is low compared to distance vector routing and RIP. When link fails a routing error is passed back to the transmission node and the message broadcast is again repeated to find the least metric. As AODV updates the route from source to destination fresh path is updated very often which assures a guaranteed and fast delivery of data packets to the destination nodes. Thus, we have selected AODV routing protocol for communication between home access point and hospital gateway.

2. PROPOSED MODEL OF PROXY

Re-Encryption Secret Key (PRESK) Generation Model: We have proposed a three tire security architecture that consists of Bio-medical sensors, placed in and around the human Body sensor for the pervasive monitoring of patients. The data that is securely going to be transmitted from the Bio-sensor node to the NCC, is an ECG signal (Goldberger, 2000) in our security model. This is a electrical pulse generated at the Arotic notch and over the surface of the heart. A typical heart beat signal is shown in Figure 1.This data should not be compressed as it may lead to loss of information, where this is currently a method of encryption. Other Bio-signals like Blood pressure, Oxygen saturation (Spo_2), Insulin level, Motion sensor etc. can also be measured and be transmitted with ECG as this is considered as primary information.

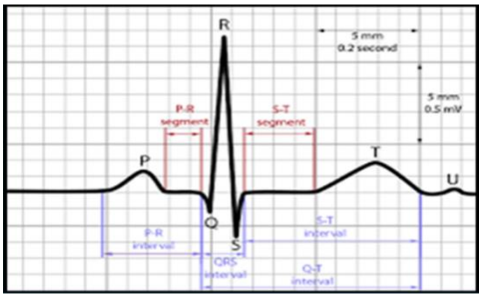

Figure.1. ECG Signal

In all the existing models, a wired communication is provided with Bio-sensors around the human body and hardware key encryption is provided, but this idea got failed as the key is compromised very easily by various attacks we moved into, a dedicated wireless communication frequency (Karthikeyan, 2010) to identify and communicate with the intended wireless Body Area sensor node. This is also weak as that frequency band will be under jamming, to disable Bio-sensors node. To solve this U.S Federation Communications Commission FCC issued the standard Industrial-science-Medical (ISM) frequency band, which is dedicated and interference free with any other frequency or a short range Infra-Red encoded signal used for sensor node identification and communication (Karthikeyan, 2010). In all this methods secret key is pre-deployed in the sensor nodes that can't be changed.

We proposed the light weight cryptographic code model. When a key is pre-deployed it can be easily under brutal force attack the secret key can be easily hacked and sensor node can be opened. So it is quite necessary to change the secret key on a session basis. For this we had borrowed the idea from the proxy Re-encryption algorithm and proposed this model, Proxy Re-Encryption Secret key (PRESK) Generation (Changu Suh, 2008; Francesca Cuomo, 2007; Yonglin Ren, 2010). In this model the MSN has a simplified proxy calculation algorithm built in it. According to the FCC directions, the MSN (pacemaker) should not initiate a session (Gollakota, 2011). This requirement is satisfied by our first idea of initiating the session request from the NCC. When the request from NCC arise to MSN, we simultaneously share the secret key of NCC with the request signal. This secret key is changed by the NCC user for each session making it unpredictable to adversary. This second idea is proposed by us in the model, with a fresh session secret key for each session. It can be easily done with the help of user friendly PDA hand held mobile unit. So that data can be protected to its maximum.

On receiving the session secret key the MSN with a portion of its secret key and NCC secret key performs the proxy re-encryption algorithm over the keys and generate the Proxy Re-Encryption Secret key (PRESK) Generation. This key is a unique, random value which is changed for each session. Further the re-encryption secret key is forwarded to other sensor nodes and to the NCC for decryption. With the new PRE Secret Key, encrypted information with the secret key is again re-encrypted with the PRES Key by the MSN.

So, even if the pre-deployed secret key is hacked decryption of the information is not possible, as it is re-encrypted by the PRES Key. The information is not tampered or altered as the session secret key is continuously changed.

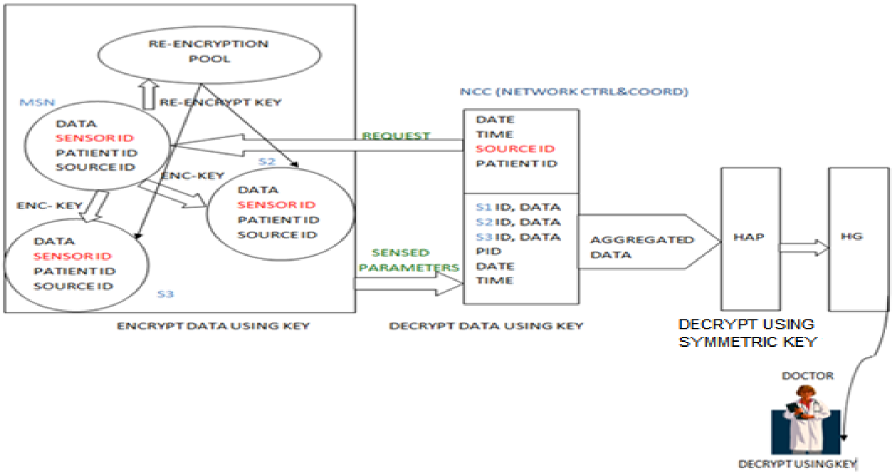

Figure.2. Block diagram of proposed (PRESK) system

The three tire security algorithm model is shown in figure.2 with short below.

- Proxy re-encryption which makes use of a Secret key for encryption and decryption. This exist between the body nodes.

- DES (Data Encryption Standard) which requires only one private key for both encryption and decryption. The NCC aggregates all data and pushes to the HAP.
- The AODV Routing Algorithm provided with the third level of security link. It exists between the Home access points (HPA) to the Hospital Gateway (HG) this is a wired multiuser traffic channel.

The three tire security architecture is shown in figure 3, shows the link and identifies the devices present at each link.

First Tier: Initially Bio-medical sensors are positioned on various parts of the Human body. Each Bio-medical sensors sense any one of the body parameter (Heartbeat, pulse rate, blood pressure etc.) out of which one is considered to be Master sensor node (MSN). All the sensor has its own secret key which is pre-deployed inside the sensor before placing inside the human body. Like this all the sensors presented here have its own secret key with the NCC. The NCC is the receiver end system knows the secret key of the sensor to decrypt the sensed patient vital information.

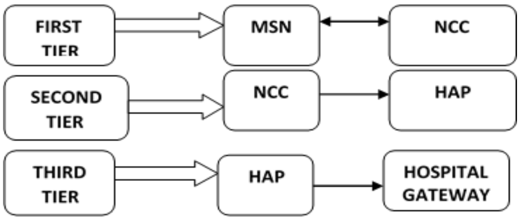

Figure.3. Three tier security architecture

The MSN has a software based proxy formation inside it The MSN knows the secret key information of NCC, with this key information the proxy Re-Encryption occurs inside the MSN and generates the proxy Re-encryption key. On receiving the request which constitutes of Date, Time, Source ID, patient ID from the NCC (external node) to sense the parameter measured by the sensor. The sensed information is encrypted, by using the secret key pre-deployed inside the sensor. The next stage is the second stage encryption, by using the proxy re-encrypted key derived by the MSN. Again the encrypted information is Re-encrypted by the Proxy Re-Encryption Key. The Proxy Re-Encrypted key is then shared to sensors (S2 & S3) and for security purpose the Re-encrypted key is stored in Re-encryption pool (internal node). This forms the first tier security system and gives two stage of key and Encryption process.

Second Tier: All the sensed parameters along with the sensor ID, patient ID & source ID (NCC) from the sensors are encrypted and sent to the NCC. The NCC decrypts the information using proxy re-encryption key and then by with its symmetric key and aggregates all the sensor information from a single patient. Here we propose the second tire of Encryption using the DES algorithm. The aggregated data from a single patient is symmetrically encrypted by the NCC and transmit it to the HAP (Home Access Point). Usually the NCC is a PDA mobile unit given to a patient collects the signals from that patient alone and forward it to the HAP. This NCC is not a resource constraint device and so can be utilized to its maximum efficiency. The information flow graph of the three tire model is given in figure.4.

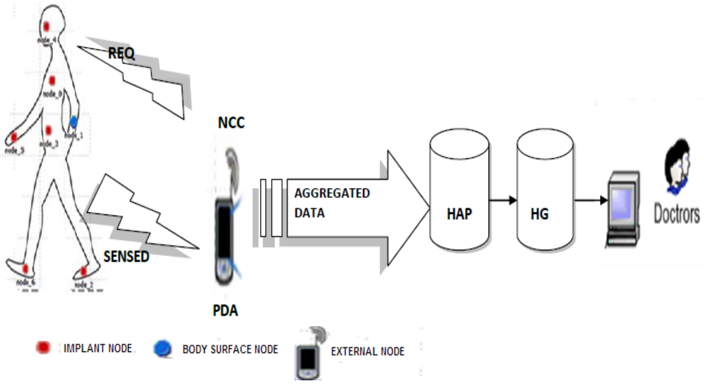

Figure.4. Flow architecture of security system

Third Tier: The HAP again encrypts the information using AODV Routing algorithm and forward the data packets by using its own security mechanism and this signal is communicated to HG (Hospital Gateway).The Doctor decrypts the parameters of the patient stored in the HG whenever required. This forms the third tier of security system.

Our main idea in this proposed model is to provide a secure data exchange between the sensor node and the NCC given to patient who form the WBAN Security model. Firstly, with the normal secret key pre-deployed in the sensor node, for the second for the more secure model, we had proposed the idea of using the Proxy Re-Encryption key method. Any third party or Adversary cannot access the information without knowing both of the sensor node and NCC secret key pre-deployed in it, where compromising both the nodes by a hacker is not possible practically.

3. SIMULATION RESULTS

The performance of the proposed Three-tier Security Architecture (TSA) is evaluated using NS2 simulation. A network which is shown is figure 5 is deployed in an area of 10 X 10 m is considered. The IEEE 802.15.4 MAC layer is reliable and single hop communication among the devices is possible. The PHY adopts basic frame structure for low-duty-cycle low-power operation as most of the medical signals are of low duty cycle, PHYs adopt frequency bands: low-band (868/915 MHz) The PHY layer uses a common frame structure, containing a 32-bit preamble, a frame length.

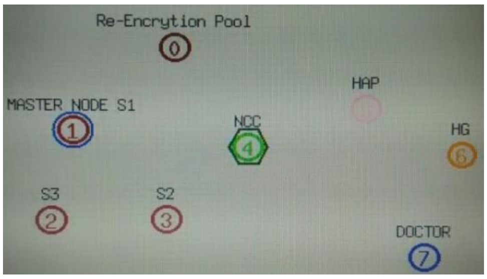

Figure.5. Network topology

Performance Matrices:

Average end-to-end Delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully to the total number of packets transmitted.

Delay: A measurement of time for a signal to reach its destination. (From Sensor node to doctor end).

Throughput: A rate of successful message delivery over the communication channel.

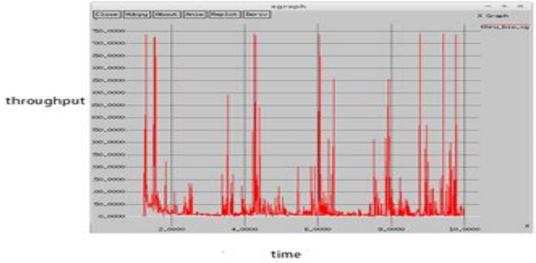

Figure.6. Time vs Throughput

Throughput = (no. of bytes*8)/(delay * 1000) (1)

From Figure.6, we observe the throughput values are maximum at even multiples of 10,000s. As the time increases, the amplitude of the throughput peaks is maximum.

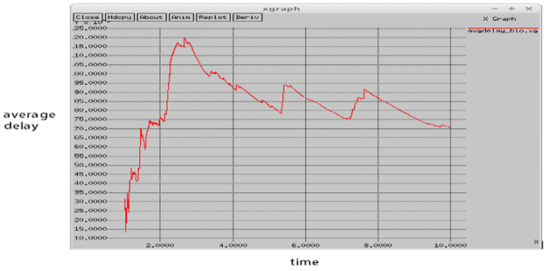

Figure.7. Time vs Average delay

AVG DELAY= (overall delay / no. of received packet) (2)

From Figure.7, we observe the average end to end delay of our proposed model increases to a maximum value and after increase in time, the average delay time of the packet delivery starts to reduce. This is considered as a good improvement, when compared to the existing models.

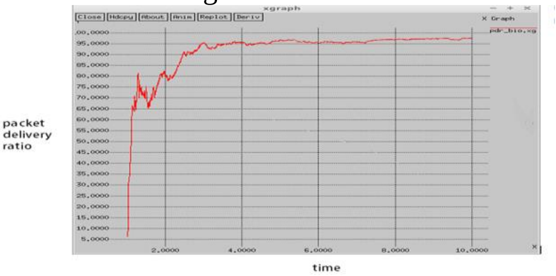

Figure.8.Time Vs packet delivery ratio

PDR={(no. of received packet)/(no. of sent packet)}* 100 (3)

From Figure.8, we can see that packet delivery ratio of our proposed model increases with time and maintains constant after 40,000 milliseconds, where obtain constant packet delivery to receiver end without any loss that is a good improvement compared to existing schemes.

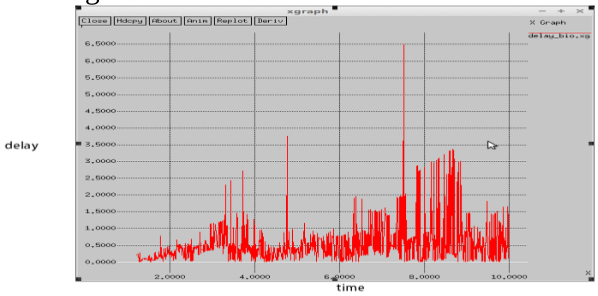

Figure.9. Time Vs Delay

DELAY = Received Time-Sent Time (4)

From Figure.9, we observe that end to end delay of our proposed model shows an increase in the delay amplitude as the time scale increases. So, in our proposed model, the transmission must be at earlier stages of time to reduce the end to end delay.

4. CONCLUSION

In this model we have proposed a three tire security model for IEEE 802.15.4 Wireless Body Area sensor Networks (WBAN). It has a wide range of sensors placed in and out, at various parts of the body with a secret key used for first level encryption and all these nodes are controlled by a Master Sensor Node. Next the MSN calculates the Proxy Re-Encryption with a portion of its own secret key and the NCC secret key. This PRE key is used and again the encrypted information is encrypted again. This Proxy Re-Encryption key is transmitted to the other sensor nodes inside the human body and stored for safety reasons. The data from all the sensors reaches the NCC where it is decrypted and aggregated. In this stage the second level of encryption occurs with the simplified DES algorithm with the HAP, with the final stage of AODV routing protocol at the HAP all the data are converted into frames and default security is added which is the third stage. It can be seen that at any point on the data transmission the original message is not seen. The only disadvantage of this model is the excess power drain for the calculation of the Proxy Re-Encryption key and for Re-encryption, which can be overcome in the future paper. By the simulation results, we have shown that the proposed scheme has reduced average delay, flat packet delivery ratio, high throughput and increase in delay with as time increases with the existing models.

REFERENCES

Blaze M, Bloomer G, and Strauss M, Divertible protocols and atomic proxy cryptography, Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Lecture Notes in Computer Science, Springer, 1403, 1998, 127–144.

Changsu Suh, Zeeshan Hameed Mir, Young-Bae Ko, Design and implementation of enhanced IEEE 802.15.4 for supporting multimedia service in Wireless Sensor Networks, The International Journal of Computer and Telecommunications Networking, 2008, 2568-2581.

Chiu Tan C, Haodong Wang, Sheng Zhong, Qun Li, IBE-Lite, A Lightweight Identity-Based Cryptography For Body Sensor Networks, IEEE Transactions on Information Technology in Biomedicine,13 (6), 2009.

Coppersmith D, The Data Encryption Standard (DES) and its strength against attack, IBM Journal of Research and Development, 38 (3), 1994, 243-250.

Francesca Cuomo, Sara Della Luna, Ugo Monaco, Tommaso Melodia, Routing in ZigBee, benefits from exploiting the IEEE 802.15.4 association tree, IEEE, 2007, 3271-3276.

Goldberger A.L, Amaral N.A.L, Glass L, Hausdorff M.J, Ivanov C.P, Mark G.R, Mietus E.J, Moody B.G, Peng K.C and Stanley H.E, PhysioBank, PhysioToolkit and PhysioNet, Components of a new research resource for complex physiologic signals, In: Circulation, 101 (23), 2000, E215-E220.

Gollakota S, Hassanich H, Ransford B and Fu K, They can hear your heartbeat, Noninvasive security for implantable medical devices, ACM SIGCOMM computer Communication Rev., 41 (4), 2011, 2-13.

Green M and Ateniese G, Identity-based proxy re-encryption, In J. Katz and M. Yung, editors, Applied Cryptography and Network Security, 5th International Conference, of Lecture Notes in Computer Science, Springer, 4521, 2007, 288–306.

Hind Chebbo, Saied Abedi, Tharaka lamahewa A, David Smith B, Dino Miniutti and Leif Hanlen, Reliable Body Area Network Using Relays, Restricted Tree Topology, International Conference on Computting, Networking and Communications (ICNC 2012), 2012.

Huang MY, Hsieh M Y, Chao CH, Hung H S and Park HJ, Pervasive, Secure Access to a Hierarchical Sensor based Health care monitoring Architecture in wireless Heterogeneous Network, IEEE Journal on selected Area in Communications, 27 (4), 2009, 400-411.

Jingwei Liu, Kyung Sup Kwak, Hybrid Security Mechanisms for Wireless Body Area Networks, ICUFN, IEEE, 2010, 98- 103.

Karthikeyan M.V, Manasa R, Nuclear Radiation Detection Using Low Cost Wireless System, Protection of Environment against Nuclear Leakage and Dump, In: Recent Advances in Space Technology Services and Climate Change (RSTSCC), 2010, 25-28.

Karthikeyan M.V, Martin Leo Manickam J, Secure IR Communication Design for Pre-Cardiac Arrest Detection in Wireless Body Area Network, International Journal on Recent and Innovation Trends in Computing and Communication, 3 (6), 2015, 3520 -3525.

Karthikeyan MV, Martin Leo Manickam J, Security Issues in Wireless Body Area Networks: In Bio-signal Input Fuzzy Security Model: A Survey, Research Journal of Pharmaceutical, Biological and Chemical Sciences, 7 (6), 2016, 1755-1773.

Kimaya sanzgiri, Briget Dahill, Brian Neil Levine, Clay Shields and Elizabeth Belding-Royer M, A Secure Routing Protocol for AdHoc Networks, IEEE Computer society, International Conference on Network Protocols, 2002.

Mambo M, Okamoto E, Proxy Cryptosystems, Delegation of the Power to Decrypt Cipher texts, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 80 (1), 1997, 54–63.

Markus Jakobsson, On quorum controlled asymmetric proxy re-encryption, In Imai H and Zheng Y, editors, Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, of Lecture Notes in Computer Science, Berlin, Germany, Springer, 1560, 1999, 112–121.

Masahiro kuroda, Qio S and Tochikubo O, Low power security body area network for vital sensors towards IEEE 802.15.6, conference proceedings of the international conference of IEEE engineering in medicine and biology society, 2009, 2442 -2445.

Mohanavalli S.S and Sheila Anand, Security Architecture for At-Home Medical Care using Body Sensor network, International Journal of Ad hoc, Sensor and Ubiquintious Computing (IJASUC), 2 (1), 2011, 60-69.

Sana Ullah, Bin Shen, Riazul Islam S.M, Pervez Khan, Shahnaz Saleem and Kyung Sup Kwak, A Study of MAC Protocols for WBANs, Sensors, 10 (1), 2010, 128-145.

Shahnaz Saleem, Sana Ullah and Kyung Sup kwak, A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks, Sensors, 11, 2011, 1385-1395.

Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo, On the Security Issues in Wireless Body Area Networks, International Journal of Digital Content Technology and its Applications, 3 (3), 2009.

Tassos Dimitriou, Krontiris Ioannis, Security issues in biomedical wireless sensor networks, IEEE Conference, Applied Science on Biomedical and Communication Technologies, ISABEL, 2008.

Yonglin Ren, Richard Werner Nelem Pazzi and Azzedine Boukerche, Monitoring Patients Via A Secure And Mobile Healthcare System, IEEE Wireless Communications, 2010, 59-65.