Light-weight Security Architecture for IEEE 802.15.4 Body Area Networks

K. T. Meena Abarna
Assistant Professor, Department of Computer Science & Engineering, Faculty of Engineering & Technology, Annamalai University

K. Venkatachalapathy
Associate Professor, Department of Computer Science & Engineering, Faculty of Engineering & Technology, Annamalai University

ABSTRACT
In IEEE 802.15.4 Body Area Networks (BAN), security solution is required for data confidentiality, authentication and integrity at low cost. But the existing solutions for WBAN either provide any one of the security features or provide all the features with high cost. In this paper, we propose to develop light-weight security architecture for IEEE 802.15.4 BAN. It consists of local sensors situated on various parts of the body which forms various clusters. The local sensor collects data from different parts of the body and transmits the data to their respective cluster head. A wireless local gateway (WLG) is deployed within the patient's home and a hospital gateway (HG) is set in the hospital. The cluster head transmits the data securely to the WLG. At WLG, a new message is created by aggregating all messages from various clusters of a patient. A secret key is generated using Elliptic Curve Cryptography (ECC) for encryption and the encrypted message with message authentication code (MAC) is transmitted to the HG. At the destination, the doctor first authenticates the MAC and then decrypts the data with the secret key and monitors the patient's health condition. Thus the data cannot be read by any other person, providing a secured transmission at low cost.

Keywords
IEEE 802.15.4, Wireless Body Area Networks, MAC, WLG

1. INTRODUCTION

1.1 IEEE 802.15.4 Networks
The rapid growing popularity of the wireless communication has led to the need for a new standard having the low complexity, low power consumption etc for wireless sensor networks inevitable. IEEE 802.15.4 standard for the low-rate wireless personal area network (LR-WPAN) is having low complexity, ultra low power consumption, and low data rate wireless connectivity in the fixed, inexpensive, portable, and moving devices which has no devices to operate [1]. It is formed by the WPAN working group that specifies the physical layer and the medium access control (MAC) layer protocol for the low-rate (LR-WPANs) [2].LR-WPAN uses two kinds of devices defined by the IEEE 802.15.4 standard. They are the full function device (FFD) and the reduced function devices (RFD).The full function devices (FFD) are those in which all IEEE 802.15.4 functions and features specified by the standard are present. The reduced function devices (RFD) have only limited functionality to lower the cost and complexity of the network. The FFD can act as PAN coordinator whereas RFD can communicate only with the FFD. The IEEE 802.15.4 MAC has features like low-duty cycle operation and self organization for WPANs. Hence this standard is more attractive for providing multimedia services over the networked sensors [3]. Industrial control, environmental and health monitoring, home automation, entertainment and toys, security, location, asset tracking, emergency and disaster response are some of the applications of IEEE 802.15.4 devices [4].

The biomedical sensors which are distributed over the human body for mobile healthcare applications form the Wireless Body Area Networks (WBANs). A WBAN has several nodes implanted in or worn on the human body which collects information. The wireless channel is used by the sensor nodes for communication among themselves. The collected biomedical information is transmitted to the controller node [5].A Body Area Network (BAN) uses IEEE 802.15.4/Zigbee technology to detect and predict the human physiological states of wakefulness, fatigue and stress [6].IEEE 802.15.4 suits the WBANs due to it low power communication, and low data rate [7]. The WBANs consider IEEE 802.15.4MAC protocol as a standard for wireless communication. Some of the applications of WBANs are elderly care, health care of patients with specific chronic diseases such as COPD, and post-surgery monitoring etc [9].

1.2 Attacks in WBANS
The development of WBANs is hindered by various security threats due to the vulnerable nature of wireless channel. Some of the major attacks in WBANs are as follows:

a. **Eavesdropping:** The features of wireless channels in WBANs are open. Hence the radio communication between the nodes in the WBANs can be intercepted by the attackers freely and easily. This allows the attackers to eavesdrop packets from node to node. It also helps the attackers to obtain sensitive and valuable information. [5]
b. **Data Modification:** The eavesdropped information are partly or fully removed or replaced by the attackers. The modified information is send back to the original receiver to achieve some illegal purpose.
c. **Impersonation Attack:** The attacker eavesdrop the legal BAN Network Controller (BNC's) or the BAN nodes (BN's) private identity information. He uses the legal identity information to cheat BN's or BNC. [17]
d. **Replaying:** A part of the valid information can be eavesdropped by the attacker and is send back to the original receiver after some time to achieve the same purpose in different case.

e. **Denial of Service:** When the traffic is beyond the capacity of the systems, the Denial of Service (DoS) attack occurs. The effect of both intentional act of malicious and compromised nodes and unintentional excessive peak network utilization is associated with it. A DoS attack can be easily initiated by the attackers using the infected BNs, when the authenticated BNs are compromised. [18]

1.3 Security Requirements in WBANS

In general, the characteristics of an application are needed to build robust security mechanism, which defend the system from possible security threats. The fundamental security requirements in WBAN are described below, [10].

1. Data Confidentiality
To protect the data from a disclosure, the system require data confidentiality. In WBAN, sensitive information such as patient's health status is transferred by the BN's. During communication, there is a possibility of overhearing and eavesdropping the sensitive information by the adversary. Since, the adversary can utilize the acquired data for many illegal purposes; the result of eavesdropping can be severe to the patient. Encrypting the data with a secret key and sharing the secret key through a secure channel is one of the ways to acquire confidentiality.

2. Data Authentication
Applications including both medical and non-medical application necessitates data authentication. Each BN and BNC has to verify whether the data is transmitted by the trusted sensor or by the adversary. Because, the adversary can deceives the sensor node to accept the false data. Symmetric technique can be used in a WBAN to achieve data authentication. This technique shares the secret key to compute Message Authentication Code (MAC) for all data.

3. Data Integrity
Data integrity is necessary as an adversary can alter the data that is transmitted over an insecure channel. Absence of data integrity technique paves a way to the adversary to modify the information before it reaches the BNC. Data integrity is attained through data authentication protocols, which ensures that the received data is not changed by the adversary.

4. Data Freshness
The data freshness technique is essential to assure data confidentiality and integrity. The adversary may confound the BNC by taking data during transmission and retransmit them later. Data freshness guarantees the newness of data. In our words, it checks the arrangement of data frames. Strong freshness and weak freshness are the two types of data freshness. Weak freshness guarantees partial data frames ordering but does not guarantee delay whereas the strong freshness guarantees data frames ordering as well as delay. The low duty cycle BNs like Blood pressure (BP) makes use of Weak freshness. Conversely, strong freshness is used in situation when a beacon is transmitted by the BNC. In simple, it is needed during synchronization.

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

6. Availability
It guarantees that the patient's information is accessible to the doctor. This accessibility can be destroyed by the adversary by disabling an ECG mode. This may lead to critical situation such as loss of life. During the loss of availability, a technique is required to maintain the operation of the BNs and switch the operation to another BN [19]

In addition to the basic security requirements like confidentiality, integrity protection and authentication certain other goals should be met. It includes:

Efficiency: An important aspect of a BSN's design is energy-efficiency due to the limited capabilities of sensors. Severe loads are imposed on the sensors of a BSN in terms of energy due to the cryptographic and protocol requirements of secure communication. The continuous monitoring requirements of a BSN can be hindered by the frequent energy depletion even though the sensors are rechargeable. Hence energy-efficient secure communication is needed for BSN. There is a limited memory available at each sensor of the BSN. Hence the secure communication schemes for BSNs should be space-efficient with respect to the number of key it need to store.

Support for different types of secure communication: The two types of communication possible with BSN are unicast and group communication. Hence these two types of communications should be ensured confidentiality, integrity and authentication by the security mechanism for BSN

Usability: The security solutions **for** BSN have to be useable. The usable security solutions are defined which are activated on employment in plug-n-play manner with minimal initialization procedures [14].

1.4 Proposed Solution

An effective security solution for body area networks requires data confidentiality, authentication and integrity at lower cost which also provides defense against node capture attacks. But the existing solutions for WBAN either provide any one of the security features or provide all the features with high cost.

In this proposal, we propose security architecture for body sensor networks. Our proposed architecture consists of local sensors situated on various parts of the body, which forms different clusters. Each cluster has a cluster head. The local sensor collects data from different parts of the body and transmits the data to their respective cluster head. Each cluster head communicates with a wireless local gateway (WLG) which can be deployed within the patient's premises or home. The WLG communicates with the remote hospital gateway (HG). The collected data from the WLG is transmitted to the corresponding destination from the HG. The destination refers to the nurse or doctor authorized to monitor the patient's health condition. We assume the existence of a certificate authority (CA) server situated in the hospital.

The local sensor collects data from the patient's body. The collected data includes physiological values like temperature, heart beat etc. The collected data is given to the cluster head in the form <patient ID, Cluster ID, and data>. The WLG maintains a table which contains <Pid, CHid, Ksec>, where

Ksec is the shared secret key of each cluster and WLG, Pid is the patient id and CHid is the cluster id. The WLG broadcasts the table to the respective CHs.

Each CH aggregates data from the local sensors and generates the message containing cluster ID, patient id and aggregated data. This message is encrypted by Ksec at the CH and sent to the WLG.

At the WLG, the message is decrypted using the same key Ksec, to ensure the security of the data. Then a new message is created by aggregating all messages from various clusters of a patient. For each patient, a new string is generated in the format (date, time, Pid, aggregate data) and a public key Pu_k is created from the string using ECC. The string is then stored in the CA. The WLG then encrypts the aggregated data and Pid using Pu_k and a MAC has been created for this, using the shared key between WLG and HG. The MAC value is transmitted to the HG.

At the HG, the MAC value compared with the already calculated MAC value. In case of a match, the message is forwarded to the destination.

At the destination, whenever the data is required by the authorized person, a request is sent to the CA along with Pid, date and time. The CA then generates the corresponding private key Pr_k for the same string using which the message is finally decrypted by the authorized person.

2. RELATED WORK

Jingwei Liu and Kyung Sup Kwak [5] proposed a feasible hybrid security mechanism to meet the security requirements of WBANs with strict resource constrains. They also discussed the security issues of WBANs. They also analyzed the main security risks in the recent advances of WBANs. It helped WBANs against attacks when compared to other networks without resource constraints and the security requirement of WBANs. They proposed a hybrid security structure for the available cryptographic algorithm. A primitive to develop efficient and secure WBAN systems are provided by the proposed security mechanism.

Chiu C.Tan et al [11] have developed IBE-Lite, a lightweight identity-based encryption suitable for sensors in a BSN. They presented protocols based on IBE-Lite. It balanced security and privacy with accessibility. The commercially available sensors were used for performance evaluation experiments.

Masahiro Kuroda et al [12] have proposed a secure body area network (SBAN).It can be commercially employed with reduced computational burden on a real sensor. These sensors have limited RAM/ROM sizes and CPU/RF power consumption under a light-weight battery. The vital data ordering among the sensors in the S-BAN are provided by the proposed S-BAN. It also provides low networking with zero administration security by automatic private key generation. The power-efficient media access control (MAC) is designed and implemented with resource-constraint security in sensors.

Y. M. Huang et al [13] have presented a healthcare monitoring architecture coupled with wearable sensor systems and an environmental sensor network. It is used for monitoring elderly or chronic patients in their residence. The wearable sensor system consists of various medical sensors built into a fabric belt. The sensors collect a timely set of physiological health indicators transmitted via low energy wireless communication to mobile computing devices. The proposed network architecture implements three application scenarios. The use of ad hoc mode for the group-based data collection and data transmission promotes the outpatient healthcare services as only one medical staff is assigned to a set of patients. They also performed the adaptive security issues for the data transmission based on different wireless capabilities. They also presented a monitoring application prototype for capturing sensor data from wireless sensor nodes.

Krishna K. Venkatasubramanian and Sandeep K.S. Gupta [14] have presented Physiological Value based Security (PVS).It is a usable and efficient way of securing inter-sensor communication schemes for BSNs. In PVS scheme, the key used to secure a particular message is distributed along with the message itself. It is hided using physiological values. It eliminates the need for explicit key distribution. It also reduces the number of keys required at each node to meet all its secure communication requirements.

S.S.Mohanavalli and Sheila Anand [15] proposed a novel architecture to ensure continuous, unobtrusive and remote patient monitoring. It takes into account the inherent hardware constraints of the sensors. The proposed architecture enabled senior ciziten, patients with chronic ailments and patients requiring post operative care to be monitored from their homes. They have also discussed the security threats and challenges inherent to wireless communication of sensor data. They have also proposed a security mechanism to ensure data confidentiality, integrity and authentication.

3. PROPOSED LIGHT-WEIGHT SECURITY ARCHITECTURE

3.1 Cluster Formation

Initially the local sensors are situated on various parts of the body. These local sensors form different clusters. Each cluster has a cluster head. The local sensor collects data from different parts of the body and transmits the data to their respective cluster head. The cluster head collects data from other nodes in the cluster, undergoes data fusion and is forwarded to the wireless local gateway (WLG).

If these local sensors are not organized into clusters, each movement of the sensor nodes causes all the sensors to reach the WLG along with the observed data. Network congestion can be caused due to this and it provides the base station with redundant data. In order to reach the WLG each node spends too much of energy.

When the cluster head collects overall data and transmits it to the WLG, the energy spent is reduced.

The following three steps include the cluster formation phase:

Step 1: *Broadcast request*- Each cluster head broadcasts a REQ which consists of its ID and other control information.

Step 2: *Selection of Cluster*- The subset of non CH nodes in the network receives the RREQ. If at least one RREQ is received by the non-CH, it decides to join the cluster of the CH.

Step 3: *Transmitting reply*- Each local sensor collects data from the patient's body. The collected data includes physiological values like temperature, heart beat etc. The collected data is sent to the cluster head in the form <patient ID, Cluster ID, and data>. [14]

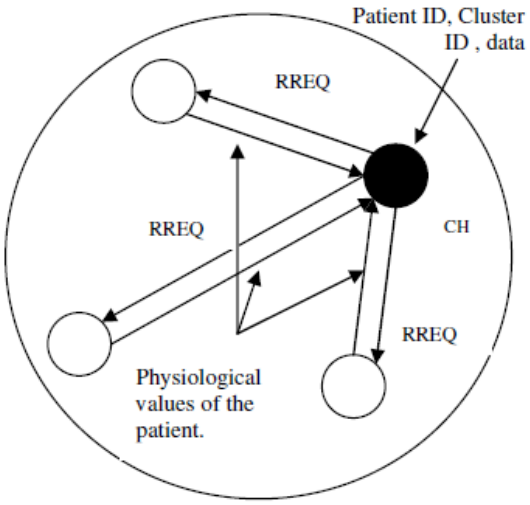

Figure 1: Cluster Formation

3.2 Communication Using Wireless Local Gateway (WLG)

- A patient is fitted with many local sensors in the body forming a cluster. The cluster head, which is the major sensor node, collects the information from the local sensors.
- Each cluster head transmits the collected data through a WLG and this is deployed within the patient's premises or home. The WLG maintains a table of the form <Pid, CHid, Ksec> where Ksec is the secret key shared between each cluster and WLG. The WLG broadcasts this table to the respective CHs.
- The collected data contains the patient ID (Pid), cluster ID (CHid) and the sensed information. The collected data from all the patients are transmitted to the wireless local gateway (WLG) using wireless communication.
- Each patient can be identified using the unique Pid. Pid is related to the patient's data so that the origin of data can be identified.
- The energy, resource requirements and wireless range of the used sensors, only needs to be sufficient for transmission within the confines of the home. Single hop transmission is ample for transmitting from WLG and lesser power is consumed for wireless transmission.
- The hospital is also set with a remote hospital gateway (HG). Then it reaches the destination which is referred as the nurse or doctor authorized to monitor the patient's health condition.
- As this transmission is confined within the house, the security attacks would be considerably less than the internal/external attacks possible during direct transmission in the public domain.

The standard communication channels like Internet, Virtual private network or dedicated line is used to transmit medical data of the patients between WLG and HG. The advantage in this is that the patients can be at home and carry on their routine work. Hospitalization charges, charges for nurses and trained aides can be saved efficiently.

The medical experts can be alerted in emergency situations due to monitoring data of such patients. The data can be collected at more frequent intervals by increasing the sampling frequency of the sensors. The frequency can be varied at WLG by medical professionals via HG during abnormality in essential conditions. The values of the essential parameters are monitored by WLG and HG can alert the care givers. [15]

For example in this figure 1, we set up a home with four patients to be monitored. Each patient has four local sensors in the body. The cluster heads of all the four patients transmits the collected information to the WLG. It carries the patient ID, CH id and the secret key. The WLG then transmits this data to the HG. This information is given to the doctor so that they can identify the patient and provide treatment accordingly.

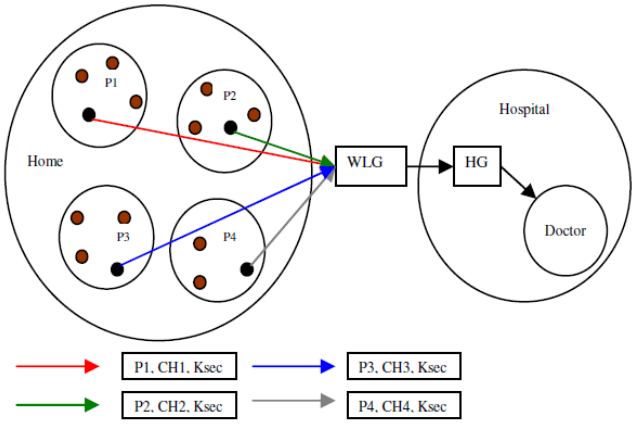

Figure 2: Communication through the Architecture

3.3 Encryption and Decryption of Message

The encryption which is used here allows a public key to be generated from an arbitrary string. Corresponding discrete private key is generated later, on demand. This encryption is based on Elliptic curve cryptography (ECC) [16], a public key primitive suitable for BSN.

Each CH aggregates data from the local sensors and generates the message containing cluster ID, patient id and aggregated data. This message is encrypted by Ksec at the CH and sent to the WLG.

At WLG, the message is decrypted using the same key Ksec in order to ensure the security of data. For each patient, each day a new string is created which has a format <date, time, Pid, aggregated data>. The public key Pu_k is generated from the string using ECC (to be explained in section 3.3.1). The String is stored in a offline certificate authority (CA).

The WLG then encrypts the aggregated data (to be explained in section 3.3.2) and Pid using Pu_k and a MAC has been created for this, using the shared key between WLG and HG. The MAC value is transmitted to the HG.

At the HG, the MAC value compared with the already calculated MAC value. In case of a match, the message is forwarded to the destination.

The patient instructs the certificate authority (CA) to release the keys to any doctor. Then the CA will derive the corresponding secret key by using the same string. Only the doctor is allowed to decrypt the messages (to be explained in section 3.3.3) which are encrypted by the sensors, using the same string.

3.3.1 Generation of Public key using ECC

At WLG, a master secret key is created over an elliptic curve C. We take the base point of C as L and r as the order of L. The patient generates m secret keys $K_1, K_2, \ldots K_m$ in order to generate the master secret key.

$$K = K_1, K_2, \ldots K_m$$

The m public keys are then generated to make up the master public key

$$Pu_k = Pu_1, Pu_2, \ldots Pu_m$$

where $Pu_i = KiL$

Finally the patient selects a collision resistant one way hash function Hi.

Then the patient generates a secret key corresponding to a public key generated by a string S.

$$\text{It executes} \quad K_{sec} = \sum_{i=1}^{m} Hi(S)Ki$$

3.3.2 Encryption

Encryption is done in order to encrypt the message using a public key which is derived from the string S. The ciphertext R can be determined by encrypt (d, S). Pu_k is the public key, and Ee is ECC encryption.

1. Determine S using agreed upon syntax.
2. Pu_k is generated, where

$$\mathrm{Pu_k} = \sum_{i=1}^{m} Hi(S).Pui$$

3. Execute Ee (d, Pu_k) to obtain R

At the destination, whenever the data is required by the authorized person, a request is sent to the CA along with Pid, date and time. The CA then generates the corresponding private key Pr_k for the same string using which the message is finally decrypted by the authorized person.

3.3.3 Decryption

The doctor executes Decrypt (R, Pu_k) to obtain the original message d which was encrypted using a secret key derived from S. Ed is ECC decryption

1. Doctor requests data from CA to obtain private key.
2. CA runs keygen (S) to derive Ks.
3. Decryption is done at the destination by executing Ed (R,Ks). [11]

4. OVERALL ALGORITHM

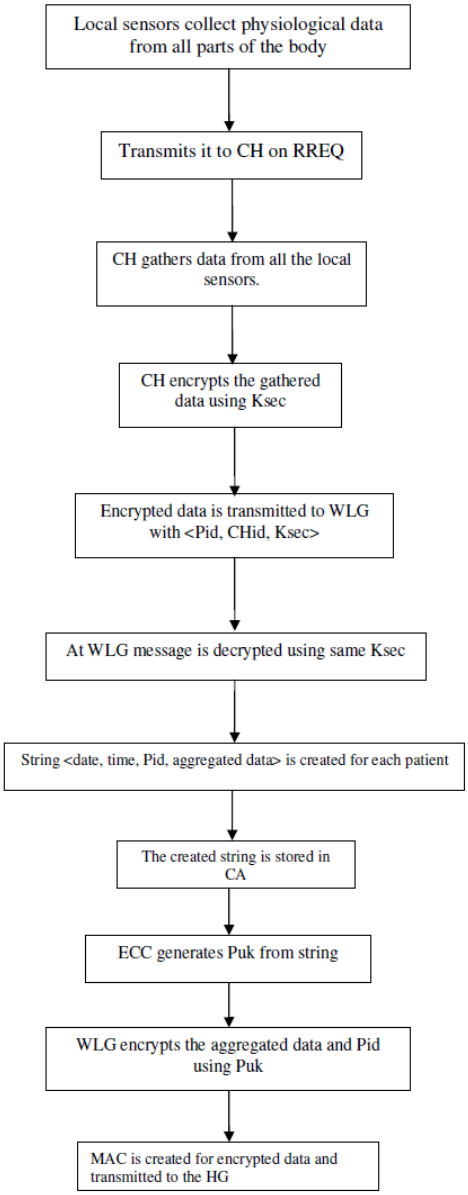

Figure 3: Flow chart of overall algorithm

5. SIMULATION RESULTS

5.1 Simulation Setup

The performance of the proposed Lightweight Security Architecture (LSA) is evaluated using NS2 [17] simulation. A network which is shown is figure 4 is deployed in an area of 50 X 50 m is considered. The IEEE 802.15.4 MAC layer is used for a reliable and single hop communication among the devices, providing access to the physical channel for all types of transmissions and appropriate security mechanisms. The IEEE 802.15.4 specification supports two PHY options based on direct sequence spread spectrum (DSSS), which allows the use of low-cost digital IC realizations. The PHY adopts the same basic frame structure for low-duty-cycle low-power operation, except that the two PHYs adopt different frequency bands: low-band

(868/915 MHz) and high band (2.4 GHz). The PHY layer uses a common frame structure, containing a 32-bit preamble, a frame length.

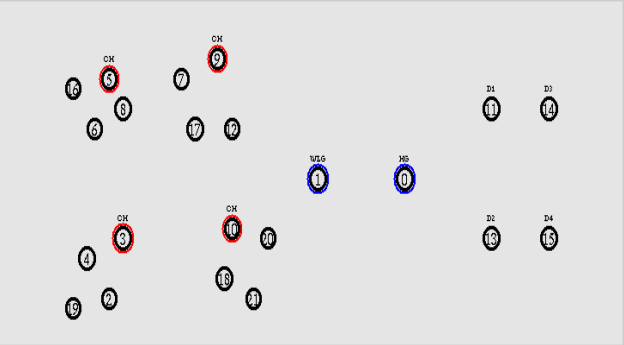

Figure 4: Network Topology

The simulated traffic is exponential with UDP source and sink. Table 1 summarizes the simulation parameters used

Table 1. Simulation Parameters

No. of Nodes	22
Area Size	50 X 50
Mac	IEEE 802.15.4
Simulation Time	25 sec
Transmission Range	25m
Routing Protocol	LSA
Traffic Source	Exponential
Packet Size	250 to 1000 bytes
Number of keys	50 to 250

5.2. Performance Metrics

The performance of LSA is compared with the normal architecture (NoLSA) without applying the security scheme. The performance is evaluated mainly, according to the following metrics.

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 and the total number of packets transmitted.

Packet Drop: It is the number of packets dropped during the data transmission.

The simulation results are presented in the next section.

5.3 Results

A. Based on Keys

In the first experiment we vary the number of keys as 50,100,150,200,250.

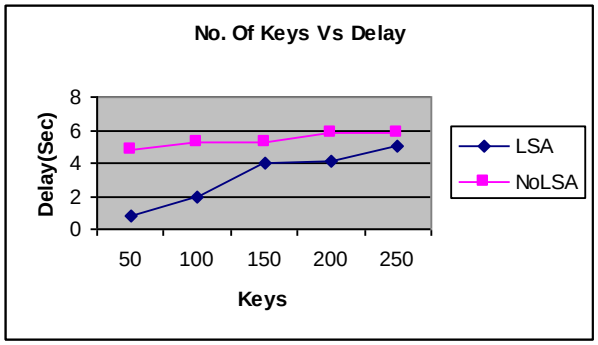

Figure 5: No. Of Keys Vs Delay

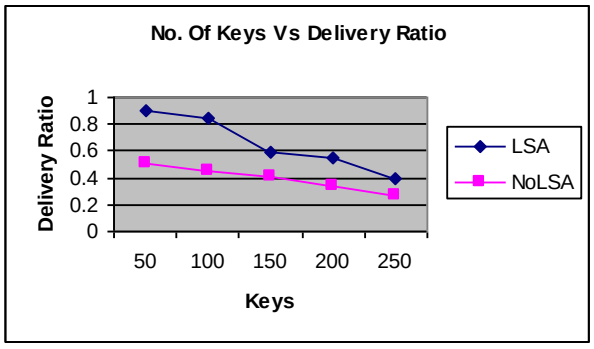

Figure 6: No. Of Keys Vs Delivery Ratio

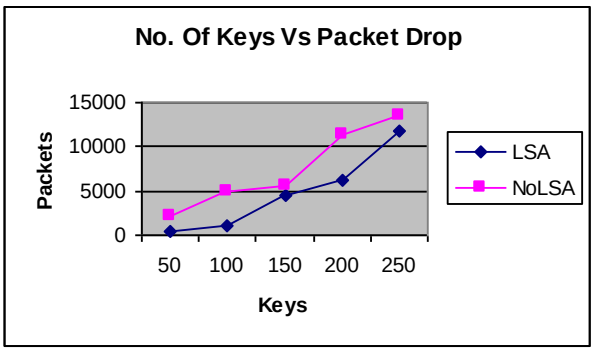

Figure 7: No. Of Keys Vs Packet Drop

From Figure 4, we can see that the average end-to-end delay of our proposed LSA protocol is less than the existing normal scheme.

From Figure 5, we can see that the delivery ratio of our proposed LSA protocol is higher than the existing normal scheme.

From Figure 6, we can see that the packet drop of our proposed LSA protocol is less than the existing normal scheme.

B. Based on Packet Size

In out second experiment we vary the packet size as 250, 500, 750, 1000 bytes.

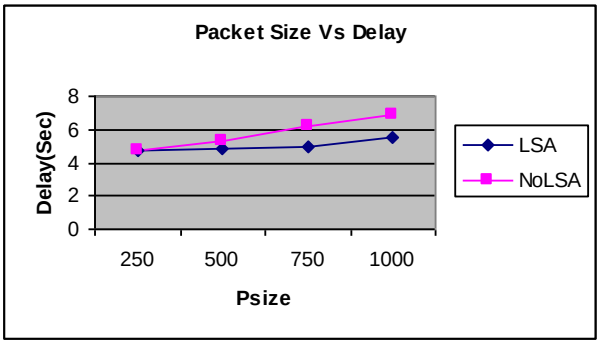

Figure 8: Packet Size Vs Delay

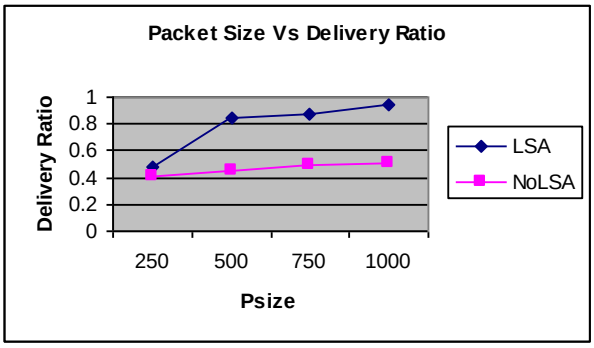

Figure 9: Packet Size Vs Delivery Ratio

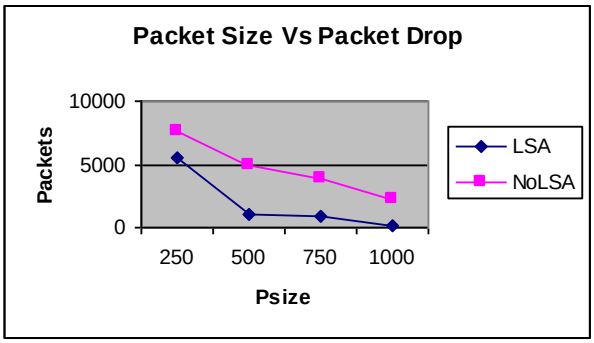

Figure 10: Packet Size Vs Packet Drop

From Figure 7, we can see that the average end-to-end delay of our proposed LSA protocol is less than the existing normal scheme.

From Figure 8, we can see that the delivery ratio of our proposed LSA protocol is higher than the existing normal scheme.

From Figure 9, we can see that the packet drop of our proposed LSA protocol is less than the existing normal scheme.

6. CONCLUSION

In this paper, we have developed light-weight security architecture for IEEE 802.15.4 wireless body area networks (WBAN). It consists of local sensors situated on various parts of the body which forms clusters. A wireless local gateway (WLG) is deployed within the patient's home and a hospital gateway (HG) is set in the hospital. The local sensors collect physiological data like temperature, heart beat etc. from different parts of the body and transmit it to their respective cluster heads. Each CH aggregates data from all the local sensors and generates the message containing cluster ID, patient id and aggregated data. This message is encrypted by the shared secret key at the CH and sent to the WLG. The WLG maintains a table with Patient ID, CH ID and the secret key. Each patient can be identified using the unique Patient ID. Patient ID is related to the patient's data so that the origin of data can be identified. At WLG, a new message is created by aggregating all messages from various clusters of a patient. A string containing date, time, patient ID, and aggregated data is generated using ECC which is encrypted and a MAC is created. This string is stored in CA. This MAC is transmitted to the HG. If the MAC is same as already calculated MAC, the message is forwarded. CA derives the corresponding private key using string whenever it receives a request from the doctor. The doctor decrypts the data using the private key and monitors the patient's health condition. Thus the data cannot be read by any other person, providing a secured transmission at low cost.

7. REFERENCES

[1] Eui-Jik Kim, Meejoung Kim, Sung-KwanYoum, Seokhoon Choi, Chul-Hee Kang, "Priority-based service differentiation scheme for IEEE 802.15.4 sensor networks", International Journal For Electronics and Communications,pp.69-81,2007.

[2] Deze Zeng, Song Guo, Victor Leung, and JiankunHu, "The Exploration of Network Coding in IEEE 802.15.4 Networks", International Journal of Digital Multimedia Broadcastring,pp.1-9,2011.

[3] 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"pp.2568-2581,2008.

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

[5] Jingwei Liu, Kyung Sup Kwak, "Hybrid Security Mechanisms for Wireless Body Area Networks", pp.98-103,2010.

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

[7] Sana Ullah, Bin Shen, S.M. Riazul Islam, Pervez Khan, Shahnaz Saleem and Kyung Sup Kwak, "A Study of MAC Protocols for WBANs", pp.128-145,2010.

[8] Young-Sun Seo, Dae-Young Kim, Jinsung Cho, Ben Lee, "OCDP : A WBAN MAC Protocol for Contention-based Medical and CE applications",

[9] Majid Nabi,Twan Basten, Marc Geilen, Milos Blagojevic, Teun Hendriks, "A Robust Protocol Stack for Multi-hop Wireless Body Area Networks with Transmit Power Adaptation",sept,2010.

[10] 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, Vol 3, No 3, Sept 2009.

[11] Chiu C. Tan, Haodong Wang, Sheng Zhong, and Qun Li, "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks", IEEE Transactions On Information Technology In Biomedicine, Vol.13, NO. 6, pp. 926-932, Nov.2009.

[12] Masahiro Kuroda, Shuye Qiu, and Osamu Tochikubo, "Low-power Secure Body Area Network for Vital Sensors toward IEEE802.15.6", 31st Annual International Conference of the IEEE EMBS, pp.2442-2445, Sept 2009.

[13] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks" , IEEE Journal On Selected Areas In Communications, Vol. 27, NO. 4, pp.400-411, May 2009.

[14] Krishna K. Venkatasubramanian and Sandeep K.S. Gupta, "Physiological Value Based Efficient Usable Security Solutions for Body Sensor Networks", pp.1-77.

[15] S.S.Mohanavalli and Sheila Anand, "Security Architecture For At-Home Medical Care Using Body Sensor Network", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.1,pp.60-69, March 2011

[16] Mugino Saeki "Elliptic Curve Cryptosystems" 1997.

[17] Neha Sharma and Er.Meenakshi Bansal, "Preventing Impersonate Attacks Using Digital Certificates in WBAN", International Journal of Advanced Engineering Sciences and Technologies, Vol-9, pp- 31-35, 2011

[18] T.V.P. Sundararajan and A. Shanmugam, "A Novel Intrusion Detection System for Wireless Body Area Network in Health Care Monitoring", Journal of Computer Science, pp- 1355-1361, 2010

[19] Shahnaz Saleem , Sana Ullah and Kyung Sup Kwak, "A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks", Sensors, vol- 11,pp- 1383-1395, 2011

8. AUTHORS FROFILE

K. T. Meena Abarna received her Bachelor's degree in Computer Science & Engineering from Annamalai University, Tamilnadu, India in 2006 and her Master's degree in Computer Science & Engineering from Annamalai University, Tamilnadu, India in 2008. She is currently working as an Assistant Professor in the Department of Computer Science & Engineering, Faculty of Engineering & Technology, Annamalai University. She is having 4 years and 9 Months experience in teaching. She has published 3 research papers in International and National conferences . Her field of interest includes Computer networks. She is a life member in CSI.

Dr. K. Venkatachalapathy received his B.Sc. degree in Physics from Madras University, Tamilnadu in 1987 and he received his Master's degree in Computer Applications from Pondicherry University in 1990. He completed his Ph.D in Computer Science & Engineering from Annamalai University, Tamilnadu, India in 2008. He is currently working as an Associate Professor in the Department of Computer Science & Engineering, Faculty of Engineering & Technology, Annamalai University. He is having 18 years of experience in teaching. He has published more than 20 research papers in international conferences and journals. His field of interest includes Image Processing and Computer networks. He is currently guiding 6 research scholars towards Ph.D. He is a life member in various professional bodies like ISTE, CSI. Etc.,