Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 13 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security in mHealth Applications using Key Management Protocol

By Dhivya. S. P, Renin. A. S & Dharanika. T
SNS College of Engineering, India

Abstract - The advancement in miniature, lightweight, low-cost, and smart physiological sensor nodes should be done by the current development in sensor nodes and power efficient integrated circuits. The sensor nodes should have the capacity of sensing, processing, controlling and communication. The applications of these sensors for health monitoring includes Wireless Personal Area Networks (WPANs) or Wireless Body Sensor Networks (WBSNs).Many works have been done for developing WBSNs as flexible, reliable, secure, real-time, and power-efficient for health monitoring. In this paper, a three stage design for mobile health application is proposed for maintaining the patient data with authentication and confidentiality by using the key sharing and management mechanism. It is highly essential if the patient is having an embarrassing disease.

Keywords : authentication, confidentiality, lightweight, miniature, sensor nodes, wireless personal area network (WPAN), wireless body sensor networks (wbsn).

GJCST-E Classification : C.2.2

Security in mHealth Applications using Key Management Protocol

Dhivya. S. P [α], Renin. A. S [σ] & Dharanika. T [ρ]

Abstract - The advancement in miniature, lightweight, low-cost, and smart physiological sensor nodes should be done by the current development in sensor nodes and power efficient integrated circuits. The sensor nodes should have the capacity of sensing, processing, controlling and communication. The applications of these sensors for health monitoring includes Wireless Personal Area Networks (WPANs) or Wireless Body Sensor Networks (WBSNs).Many works have been done for developing WBSNs as flexible, reliable, secure, real-time, and power-efficient for health monitoring. In this paper, a three stage design for mobile health application is proposed for maintaining the patient data with authentication and confidentiality by using the key sharing and management mechanism. It is highly essential if the patient is having an embarrassing disease.

Keywords : authentication, confidentiality, lightweight, miniature, sensor nodes, wireless personal area network (WPAN), wireless body sensor networks (wbsn).

I. Introduction

Many applications in areas such as health monitoring, military operations, agriculture, environmental monitoring, industrial automation, and multimedia utilizes Wireless Sensor Networks(WSNs).The application of these sensors in healthcare become more fame. The wearable biomedical sensor systems design and development attains more attention not only from industry but also from academicians for health monitoring. Disease preclusion, chronic disease supervision and enlightening the health care provision are the most enthralling aids of mobile technologies. Since the usage of mobile devices increased, the mobile technology plays important role in this paper for patient data delivery. It helps the doctors, hospital proprietors and emergency service providers for the patient healthcare. Lightweight security protocol using three stage design for mhealth applications are proposed in this paper that needs low memory and computation time to minimize the energy consumption.

II. The Three Stage Design

For patient health monitoring a three stage wireless sensor nodes are introduced, that is connected with network connectors and base stations that sends data finally to the doctors and the emergency service providers. The patient data can be accessed anywhere through the internet by the doctor to realize the patient condition by checking the heart beat and blood pressure and can make sure that the patient is responding to the treatment. Continuous health monitoring can be done by wearable sensor nodes and key sharing mechanism for active and reasonable healthcare. The patient at home is fitted with body sensors for measuring heartbeat, pulse rate and blood pressure as shown in figure 1. The network connector is connected with the sensors for collecting the data from the sensors and to send the data to the base stations for immediate requirement of treatment for the patient.

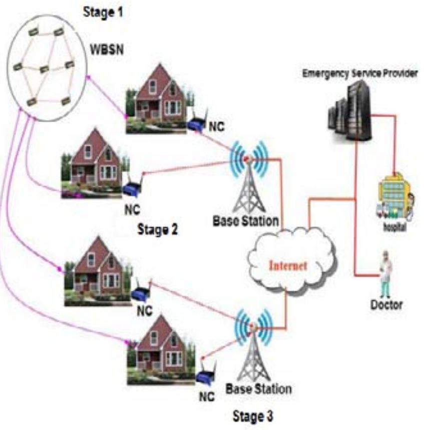

Figure 1 : The three stage network

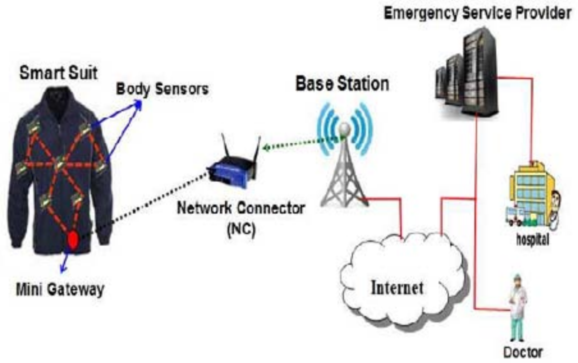

Figure 2 : Data transmission between the three stages

First Stage: Wireless Body Sensors (Wbs)

The user should wear wireless body sensors to form the WBSN. The sensors such as ECG, blood pressure monitor, accelerometer, oximeter are fitted on

Authors α σ ρ : Department of ECE, SNS College of Engineering, Coimbatore, India. E-mails : spdhivya1989@gmail.com, as.renin1802@yahoo.in, dharanika.ece@gmail.com

the patient for measuring the heartbeat, blood pressure, pulse rate, liver functioning and lungs. The gateway will analyse the data locally after collecting the sensor information and if any need for emergency, it generates alarm and transmits data to the base stations by the mini gateway present in the first stage to the second stage.

Second Stage: Network Connector (Nc)

A high computation sensor with worthy processing capacity is considered as Network Connector (NC). The second stage devices collects data by using the gateway connected in the first stage. It transmits the data to the next way in a multihop fashion. The second stage NCs should initialize, configure and synchronize the WBSN nodes. It must control, monitor and data from the body sensor nodes. It must provide secure communication through the gateway nodes.

Third Stage: Base Station (BS)

A large number of base stations are composed to form the third stage. They are very powerful with great processing speed and high battery power. They are connected with the internet for transmitting the data to the Emergency Service Provider (ESP). They may transmit data either directly through the internet or by using other base stations.

III. Nodes Classification

The entire wireless body sensor nodes are classified into three types of nodes such as sensor nodes (SN), Network Connector (NC) and Base Station (BS) and the whole network is classified with clusters using clustering algorithms and each cluster has one cluster head. The deployment of body sensors and network connector will occur randomly and the base station deployment will be done manually based on the location and communication range of the NCs. Once the SNs and NCs are deployed, they consolidate themselves to form clusters according to the location and communication range of each sensors. The network connecter acts as cluster head and controls the sensor nodes and transmits data with each other. The base station (BS) receives data from the network connector and transmits to the network manager situated remotely from the monitoring location.

Stage 1 Nodes

The first stage nodes of the network model are the group of standard sensor nodes (SN) and functions in simple, specific manner. They are usually operated independently. They sense and collect the raw data and transmit to the next hop neighbour nodes, which are finally sent to the nodes of the second stage.

Stage 2 Nodes

Some special purpose sensor nodes of limited number are deployed over the monitoring region. In every clustering group, only one network connector exists, which is the head of that cluster, receives data from the sensor nodes and transmits them to the NCs of other clusters. These nodes are more powerful in computation with longer battery life and higher memory than the sensor nodes. Each network connector of the network has a distinctive ID and is assigned based on its cluster ID. The events are tracked by the NCs using the sensors of its cluster and formulate the final report and forward them to the nodes of the third stage.

Stage 3 Nodes

The sensing and communicating nodes of high-bandwidth form the third stage of the network. They are known as the base stations of the WBSNs and multiple base stations are considered. These nodes are powerful in processing, storage, and transmission capacity and have long battery life. There is no power constraint since they are mains powered. The base stations (BSs) are connected wirelessly to the user or network manager through internet and satellite.

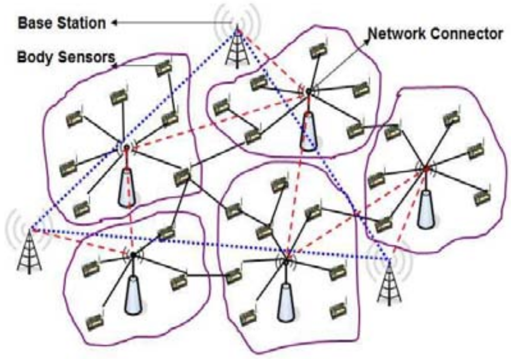

Figure 3 : Logical view of three stage design Security architecture

IV. Security Architecture

Data confidentiality and authentication algorithms are proposed in this section. Three types of keys are used for required security verifications and data confidentiality. Data confidentiality and user authentication are appropriate to all types of nodes nevertheless of its incidence in any particular stage.

a) *Key Arrangements*

The communication among SNs in every clusters are only broadcasting and routing of packets among network connectors to BSs which is only unicasting by nature. Three different types of keys for the whole network are introduced.

i. *Sensor Key*

Every sensor network has individual secret key and is common for all the sensors in the network without considering their location in any cluster. This secret key is denoted as E_{SN}. The SNs of every cluster are fixed with esteem to their cluster head (NC).

ii. *Network Connector Key*

Each cluster head (NC) has an individual secret key denoted as E_{NC}. The E_{NC} of a NC (cluster head) is common for all the NCs in the network. The network connector key E_{NC} is dissimilar from the sensor key E_{SN}. For making necessary security verification with the sensors, it stores E_{SN} and also stores its personal key E_{NC}.

iii. *Base Station Key*

Every BS of the network has individual secret key that is common for all base stations. It is denoted as $E_{BS.}$ This E_{BS} is different from E_{SN} and E_{NC}. For making security verifications every base station stores E_{BS} and E_{NC}.

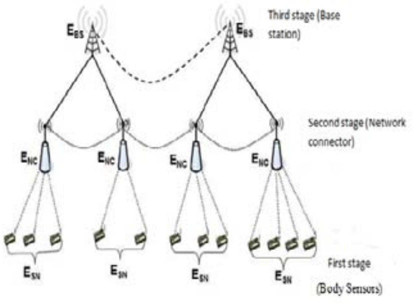
E_BS
E_BS
Third stage (Base station)
Second stage (Network connector)
E_NC
E_NC
E_NC
E_NC
E_SN
E_SN
E_SN
E_SN
First stage (Body Sensors)

Figure 4 : Key sharing architecture of the whole network

The figure 4 shows the unique secret key for each stage that is common only in that stage and maintained confidentially for other stages.

b) Data Confidentiality

A text message M, of x bits should be encrypted by the n^2 bits of E_{SN} and sent from one sensor to another. The message that is encrypted is as follows:

$$\{M\}E_{SN} = M * E_{SN} \text{ (mod p)}$$

where p is a prime number.

E_{SN} is the secret key that is known only for the sender and the receiver. But it is possible for any adversary to capture packet to intercept the cipher message and hacks the secret key. To avoid this problem, new encrypted keys are generated depending on the physical situations like time of message sent.

Consider T_i as time stamp matrix where i=1,2,3…k.

The new secret keys for sensor nodes are as follows:

$$E_1^{SN} = E_{SN} \odot T1$$
$$E_2^{SN} = E_{SN} \odot T2$$
$$E_3^{SN} = E_{SN} \odot T3$$
$$\dots$$
$$E_k^{SN} = E_{SN} \odot Tk$$

Only the sender and the receiver knows the user the user defined binary operation $\odot$. Thus the cipher text messages transmitted are,

$$C1 = M1 * E_1^{SN} \text{(mod p)}$$
$$C2 = M2 * E_2^{SN} \text{ (mod p)}$$
$$\dots$$
$$Ck = Mk * E_i^{SN} \text{ (mod p)}$$

Thus the message can be transmitted confidentially even though the adversary know the E_{SN} since only sender and receiver knows the binary operation $\odot$.

c) Authentication

Every cluster head network connectors provide individual ID for every SNs in their cluster and each BS also have individual ID. Every NCs stores their own individual ID and also the sensor nodes ID that are belong to their own clusters. Base stations stores their own individual ID and also IDs of network connectors that are connected to them.

Consider,
y: ID of the SNs/NCs/
m: The cipher message, encrypted message done by the data confidentiality technique
a, b: Unknown variables
x: Sender's secret key

The message sent from A to B is

- A → B: A(y, a, b,m) and the cryptographic function is:
- $x^2 \equiv y$ (mod n) such that
  $a - b \equiv (m + 1) * \text{(mod n)} (x/\alpha)$
  $a + b \equiv (m^2 - m + 1) * \text{(mod n)} (x\alpha)$

where, α is a random number and n is a composite number of 1,024 bits.

After receiving the packet, the B can calculate the original message as

$$a^2 - b^2 \equiv (m^3 + 1) * y \text{ (mod n)}.$$

V. Simulation Results

The figure 5 shows the transmission of message from one node to another. The authentication, key establishment and confidentiality schemes are compared with energy consumption, computation time and message bits as following in figures 6,7,8 and 9.

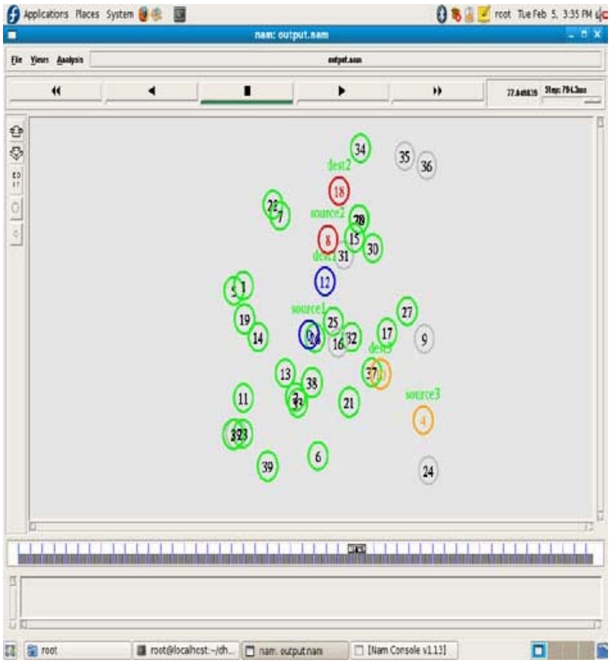

Figure 5 : Simulation result for message transmission between nodes

The figure 6 shows that the energy consumption for key establishment is higher for distinct number of nodes.

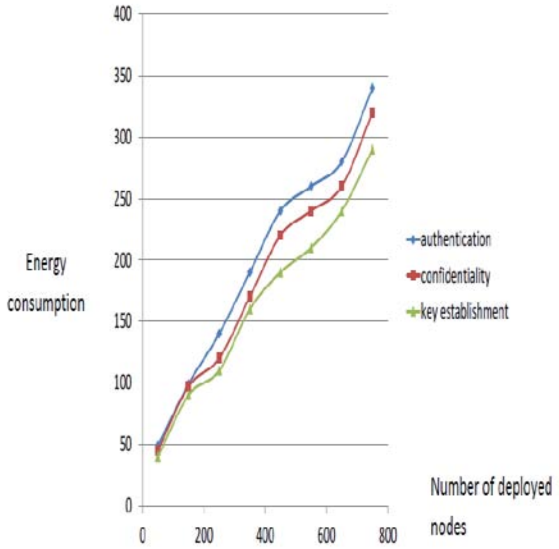

Figure 6 : Evaluation of energy consumption versus number of deployed nodes

The figure 7 shows that the energy consumption for key establishment is high for increasing computation time

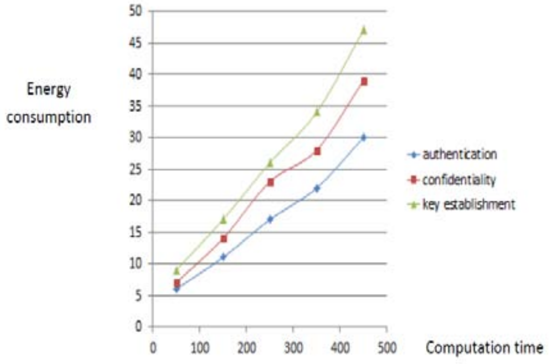

Figure 7 : Evaluation of energy consumption versus computation time

The figure 8 shows that energy consumption for key establishment is high for increasing message bits

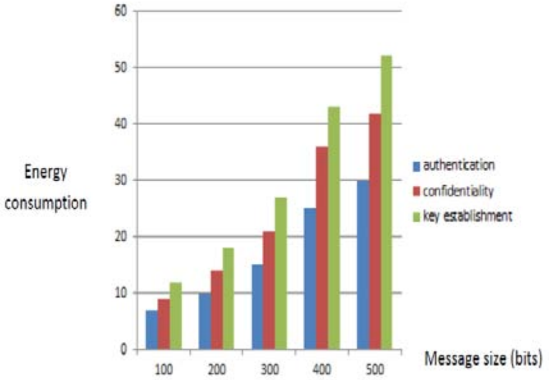

Figure 8 : Evaluation of energy consumption versus message bits

The figure 9 shows that computation time for key establishment increases with respect to the increasing message bits.

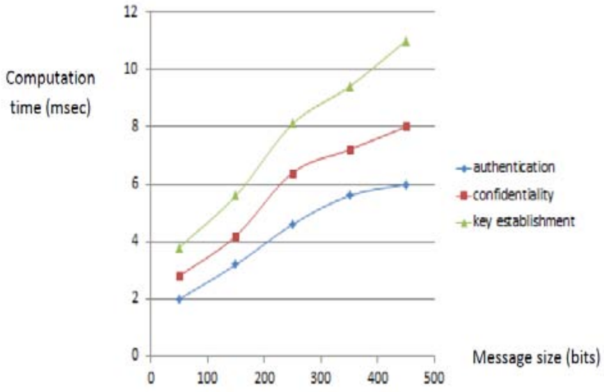

Figure 9 : Evaluation of computation time versus message bits

VI. Conclusion

Current healthcare applications include the challenges like reliability, power, portability and network interface. Some systems are hard to attach or carry because of their size and weight. They are not readily available for real life application even though they can monitor the health conditions since they use different technologies for health parameters, situation, and areas. In this paper, a three stage design is proposed for secure transmission of messages with high data confidentiality and authentication and their results are discussed. These are applicable for mobile health patient monitoring healthcare applications.

References Références Referencias

1. Kumar, P.; Lee, H.-J. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* 2012, *12*, 55–91.
2. Kumar, P.; Lee, Y.-D.; Lee, H.-J. Secure Health Monitoring Using Medical Wireless Sensor Networks. In *Proceedings of 6th International Conference on Networked Computing and Advanced Information Management*, Seoul, Korea, 16–18 August 2010; pp. 491–494.
3. Alonso, J.V.; Matencio, P.L.; Castano, F.J.G.; Hellin, H.N.; Guirao, P.J.B.; Martinez, F.J.P.; Alvarez, R.P.M.; Jimenez, D.G.; Castineira, F.G.; Fernandez, R.D. Ambient intelligence systems for personalized sport training. *Sensors* 2010, *10*, 2359–2385.
4. Wu, G.; Ren, J.; Xia, F.; Xu, Z. An adaptive fault-tolerant communication scheme for body sensor networks. *Sensors* 2010, *10*, 9590–9608.
5. Malasri, K.; Wang, L. Design and implementation of secure wireless mote-based medical sensor network. *Sensors* 2009, *9*, 6273–6297.
6. Abbasi, A.A.; Younis, M. Survey on clustering algorithms for wireless sensor networks. *Comput Commun.* 2007, *30*, 2826–2841.
7. Chakravorty, R. A Programmable Service Architecture for Mobile Medical Care. In *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW '06)*, Pisa, Italy, 13–17 March 2006.
8. Krishnan, R.; Starobinski, D. Efficient clustering algorithms for self-organizing wireless sensor networks. *Ad Hoc Netw.* 2006, *4*, 36–59.
9. Wong, K.H.M.; Zheng, Y.; Cao, J.; Wang, S. A Dynamic User Authentication Scheme for Wireless Sensor Networks. In *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan, 5–7 June 2006.

This page is intentionally left blank