SECURE HEALTH MONITORING IN WIRELESS SENSOR NETWORKS WITH
MOBILITY-SUPPORTING ADAPTIVE AUTHENTICATION SCHEME

SHANTALA DEVI PATIL¹ & VIJAYAKUMAR B P²
¹REVA ITM, Bangalore, Karnataka, India
²MSRIT, Bangalore, Karnataka, India

ABSTRACT

One of the major challenges of the world is the increasing old age population and those who are suffering from diseases. The old age population and the diseased want to live independently and perform tasks on their own. This creates a necessity to monitor them continuously and provide a better quality healthcare service while still they are able to live a normal life. The healthcare provided should be improved with the help of the present day technology for early detection and diagnosis of any abnormal conditions of the patient’s health. Wireless Sensor Networks (WSN) promise a low cost environment sensing and data processing capabilities in Healthcare applications. Human physiological features such as heartbeats, temperature and pulse can be monitored from a distant location through wireless sensors that can be implanted in/on the human body. Monitoring patients is one of the main tasks of Healthcare using WSN, even when the patients are on the move. Physiological data of the patient, sensed and gathered are highly sensitive, maintaining its confidentiality is highly essential. Hence, security is a vital research issue in mobile health applications. Solutions and schemes proposed in literature consider the patients to be immobile. Hence, this paper presents a secure, energy efficient and scalable security scheme called Mobility-Supporting Adaptive Authentication Scheme (MAAS). The MAAS scheme ensures that the Healthcare Provider and the Patients access and exchange patients data by authenticating themselves. Also, the scheme prevents unauthorized access to the data by providing confidentiality and integrity. Since the requirement suggests continuous uninterrupted monitoring of patients, but mobility of the patients cause interruption of links. The proposed security scheme also ensures connectivity of the links even when the patients are mobile.


INTRODUCTION

A generic Wireless Sensor Networks consists of a large number of resource constrained sensor nodes that are spatially distributed in an hostile environment and the with resource rich node called as the Base Station (BS).

The sensor nodes task is to sense physical phenomena from its immediate surroundings, process and transmit the sensed data to the other nodes or Base stations. WSNs are used in applications that are sensitive to environmental parameters that require monitoring, tracking and controlling.

One of the most promising fields for WSN is the Healthcare. Generic WSN needs to be customized to cater to the needs real time Healthcare Application with respect to deployment, support mobility of patients and also in providing reliable communication of patients data as there is a great risk of the patient privacy to be breached by the attackers (elaborated in section II).

The Healthcare WSN application is susceptible to different types of attacks and threats. The attack can be on the patient nodes: in which the attacker’s intension is to disrupt the sensors sensing the physiological data of the patients or the
healthcare provider system: in this case of attack the intention of the attacker to disrupt the link between the healthcare
providers, intermediary nodes and patient nodes.

Security being a prime concern in healthcare WSN, the core requirement is a solution that aims to subdue these
attacks and meet the security goals.

Security in Healthcare Application of WSN has attracted attention of many researchers.

In literature many security schemes are proposed but these schemes fail to address of mobility of patients.

In this paper, we propose a Mobility-Supporting Adaptive Authentication Scheme Based Secure Health
Monitoring in Wireless Sensor Networks to prevent the unauthorized access of patient’s data.

The paper is organized as follows: in section II security requirements for health monitoring applications is
discussed, we discuss about the related works in section III.

In section IV we discuss about the issues that arise due to the mobility of the patients. In section V, we propose a
security scheme called the Mobility Supporting Adaptive Authentication Scheme followed by effectiveness of the
proposed system in section VI. In section VII, we present a conclusion.

SECURITY REQUIREMENTS OF HEALTH MONITORING THROUGH WSN

For any network, three aspects of information security are Security Attacks, Security Mechanisms and Security
Services. Security attack: any action that compromises the security of information. Security mechanism: A mechanism that
is designed to detect, prevent, or recover from a security attack. Many security mechanisms are based on cryptographic
techniques. Security service: A service that enhances the security of the data processing systems and the information
transfers of organization. The services are intended to counter security attacks, and they make use of one or more security
mechanisms to provide the service.

The attacks in WSN Health Monitoring can be on the Patient Node such as the eavesdropping: Is a passive attack
where the attackers intention is to know the system, unauthorized modification: here the attacker modifies or fabricates the
information gathered by the sensors on the patient’s body and node compromising: node that has been taken over by the
attacker. Healthcare System includes Impersonation: the attacker gains access to the system and behaves as a part of
system, Denial of Service: is an attempt to make a network resource unavailable to its intended users and System.
The security requirements of the Health Monitoring using WSN include:

Patient Data Confidentiality and Integrity

The medical regulations suggest that the patient’s data be secure and private. Providing confidentiality ensures
that the patient’s medical files are protected. Integrity ensures that the patient’s files are not modified or fabricated by the
attacker.

Patient Data and WSN Authentication

Authentication refers to establishing secure communication between the patient and the healthcare provider by
verifying the identity of the healthcare staff accessing the patient’s information.

Patient Mobility and Re-Authentication

Mobility of the patients causes interruption in communication links. Also the mobility of patient’s changes the
sink to which they are attached which requires the patient to authenticate it again. This can be simplified if the sinks
secure health monitoring in wireless sensor networks with mobility-supporting adaptive authentication scheme

communicate about the moving patient and perform re-authentication.

related work

in this section we briefly review some of the security schemes.

the scheme in paper [1] proposed an energy efficient security scheme using PKC for healthcare application using WSN. the security was provided using a 2-step procedure of key handshaking scheme and derivation of decryption key by the receiver node. the advantage of this scheme, secure communication between the Base Station and Vice Versa. Disadvantage of this method was mobility of patients being monitored was not considered.

in paper [2] the scheme ensured that the patient’s data is not exposed to unauthorized access from malicious elements by providing a 2-step authentication. In the 1st step healthcare provider authenticates themselves before they access patients data and in the 2nd step the healthcare provider and the patient node establishes a secure session key for further communication. Again this method did not consider monitoring of the patients on move.

the scheme in paper [3] ensures that only the verified staff can access the vital readings of the patient without re-authentication and re-login into the system for a period of time. The scheme consists of 4 phases and these include Registration, Login, Authentication and Data Acquisition. Even though this method was able to combat the security attacks but was unable to address the mobility of the patients. Also, this method requires smart card to provide authentication.

the authentication schemes proposed in papers [4,6,13-18] also do not consider the mobility of the patients.

issues related to mobility of patients

the of the main requirement of the Healthcare Systems using WSN is continuous uninterrupted monitoring of patients, but mobility of the patients cause interruption of links. In order to support mobility of patients along with uninterrupted monitoring Patient Location Discovery method that help detect whether a patients is within the range is required. If the patient has moved from one range to another range the patient has to be re-authenticated and the link uninterrupted as shown in Figure 1.

Figure 1: A Mobile Patient Entering another Region

to detect movement of the Patient, the RSSI value is calculated for the patient implanted with the nodes. In paper [19] it has been shown that lowest acceptable RSSI value is -88dBm, after that point the connection is lost, the nodes need to connect to another sink node before this point. When the patient moves from coverage of one sink node to another only re-authentication of the patient should be carried out instead of authenticating the patient again to the sink node.

the main idea behind proposing the concept of re-authentication is that, the number of message exchanges to re-authenticate is less that authentication itself.
SYSTEM MODEL

In this Scheme, we consider a heterogeneous Wireless Sensor Network Model with Hierarchy. The main components include: 1: Body Sensor Nodes (BSN)– Responsible for collecting the physiological signals from the patient and may include sensors such as Blood Pressure Sensor, Heart Rate Sensor, Location Sensor. These sensors are implanted in/on the patient’s body. 2: Individual Coordinator Nodes (ICN)- Responsible for collection of and aggregation of all the data sensed by the sensor nodes implanted on/in the body of the patient 3: Sink Nodes (SN) – A group of ICNs together are assigned to a Sink Node, 4: Secure Base Station (SBS) 5: Healthcare Alert and Service System (HASS) as shown in figure 2.

Figure 2: A Simple Healthcare Monitoring Scenario

The sensor nodes implanted on the body of the patient senses the physiological factors and which are aggregated by the Individual Coordinator Node. These ICN forward the aggregated data to one of the sinks in the network which is then sent to the HASS through the BS. The HAAS will receive all the aggregated data from the BS and then store and interpret the data received. If the patient needs an immediate attention the system alerts the Doctors and Nurses who have authorized themselves to the HAAS.

PROPOSED MOBILITY SUPPORT ADAPTIVE AUTHENTICATION SCHEME

Assumptions

- Sink knows the public key of the BS
- BS knows the IDs and the Public Keys of the Sinks
- An ICN can be connected to a single SN at any point in time.

Data Structures Used:

- **Sink List at BS (SLB)**: a vector that stores information / Credentials about all the Sink Nodes in the BS
- **Neighbor Sink List (NSL)**: a vector that stores information / Credentials about all the Neighboring Sinks for all Sink Nodes.
- **Neighbor ICN List (NIL)**: a vector that stores information / Credentials about all the Neighboring ICN in the range of a SN.

The procedure of Mobility Support Adaptive Authentication Scheme is as follows:
Figure 3: Simple Flow Diagram of the MAAS

**Step 1:** The SN generates an HELLO message and then broadcasts it.

**Step 2:** If the HELLO message is received by the SN then go to Step 3 else if received by ICN go to Step 4.

**Step 3:** The SN that received the HELLO message checks for presence of the Sender SN in its NSL, if NSL already contains an entry of the Sender SN then the receiver simply discards the message, else it authenticates the Sender SN and updates its NSL.

**Step 4:** when an ICN receives the HELLO message from the SN, the ICN checks whether it is attached to a SN. If it is not attached to the SN, ICN authenticates itself to the SN and the SN updates its NIL, ignore the message if the ICN is already authenticated to the SN. when the node is mobile, the ICN is already authenticated by a SN previously then simply re-authenticates the ICN to the new SN else ignored.

The step wise detailed message exchange is as follows:

**Step 1:** Sink SN1 generates a M1 message and broadcasts.

M1->E PR_{SN1} [ID1 || TS1] || ID1 || TS1 || Rn

**Step 2:** If M1 message is received by the SN then go to Step 3 else if received by ICN go to Step 4.

**Step 3:** Sink SN2 upon receiving,

a: Checks the NSL_{SN2} for the presence of ID1 of SN1.

b: If the entry for SN1 is already present then M1 is discarded

c: Else,

i: Request the BS for the public key of NS1

M2->E PU_{BS} [ID1 || TS2] || ID2

Upon receiving M2, BS decrypts using its public key, then from the message extracts the ID1 and looks up into the table SLB for the public key of ID1. BS reverts back with M3.

M3-> E PU_{SN2} [ ID1 || PU S1 || TS3]

ii: upon receiving the message M3 from the BS the SN2 decrypts and extracts the public key of SN1 and with this it decrypts M1 to obtain the random number and timestamp.

iii: SN2 add this to SN1 to NSL_{SN2} revert back to the SN1 with an acknowledgement Ack1. Upon receiving SN1 verified Ack1 aand updates NSL s1 with the details of SN2
Ack1->E PU S1\|ID2 \| PU S2 \|TS4

**Step 4:** when the receiver is a ICN,

i: Say ICN1 receives M1. ICN1 derives the ID1 and the Rn from M1 and generates a key for securely communicating further with SN1.

\[ K_1 = H( ID_{ICN1} \| Rn ) \| ID_{ICN1} \]

ii: ICN1 then sends back an Ack2 to SN1, SN1 receives this acknowledgement from ID_{ICN1} and updates the CGL

Ack2->E PU SNI(PU_{ICN1}) \| TS5

If the ICN receives a message M1 that SN1 has broadcasted and is already authenticated by the sink.

**Re-Authentication Takes Place as Follows**

Say, ICN1 has moved from SN2 to SN1, and ICN1 is already authenticated with SN2

I: When ICN1 receives a message M1 from SN2, ICN1 revert back with an acknowledgement to SN2

Ack3->ID_{ICN1} \| ID_{SN1} \| TS6

II: Upon receiving the Ack3 from ICN1 the S1 will send a request for details of ICN1 to SN2 , SN2 retrieves the corresponding entry for ICN1 from NIL_{SN2} and send the credentials to SN1 and update that the ICN1 has moved to SN1. Upon receiving the credentials SN1 will update its NIL_{SN1} with the Public key and its previous history.

III: if step ii returns a success, SN1 sends an ACK to ICN1 stating that it is the new SN for further communications.

**CONCLUSIONS**

In many healthcare applications using WSN the main concern is to provide uninterrupted medical monitoring service to the patients, still allowing them to lead a normal life. While Healthcare Security protocols are designed for Static Sensor Network and cannot be extended to Dynamic Sensor Network for patient’s mobility. Also authentication of the components of the network is a major security issue.

In this paper, we propose an Mobility Supporting Adaptive Authentication Scheme (MAAS), the scheme provides efficient node authentication and node re-authentication for Mobile Nodes.

**REFERENCES**


3. Tsung-Chih Hsiao; Taichung, Taiwan; Yu-Ting Liao; Jen-Yan Huang; Tzer-Shyong Chen, "Secure


15. Chen-Guang He1, 2, Shu-Di Bao3, 1, *, and Ye Li1A NOVEL TRI-FACTOR MUTUAL AUTHENTICATION WITH BIOMETRICS FOR WIRELESS BODY SENSOR "NETWORKS IN HEALTHCARE APPLICATIONS", INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 6, NO. 3, JUNE 2013.

