Proceeding

6th International Conference on Networked Computing and Advanced Information Management

NCM2010

Seoul, Korea
August 16-18, 2010

Editors:
Franz Ko, Yunji Na

Sponsored by
The Institute of Electrical and Electronics Engineers (IEEE)
Institute of Electrical and Electronics Engineers (IEEE), Seoul Section, Korea
The International Association for Information, Culture, Human and Industry Technology (AICIT), Korea

IEEE Conference Record number: #17349
IEEE PDF Files Catalogue number: CFP1062E-ART
IEEE PDF files ISBN: 978-89-88678-26-8
IEEE Print version Catalogue number: CFP1062E-PRT
Secure Health Monitoring using Medical Wireless Sensor Networks
Pardeep Kumar, Young-Dong Lee, HoonJae Lee

IT Applications in Healthcare Information System—A Case Study of Medical Center in Taiwan
Nai-Wen Kuo

Design and Realization of Mobile Government Information Services Platform based on SMS
Fayu Wang, Hua Zhang, Guangping Xu

The study of video conference transmission security as an example on Windows Live
Chung-Hsin Liu, Wu-Fan Hsu

The safety design of the Laboratory Monitoring System
Chung-Hsin Liu, Po-Cheng Teng

The analysis on the effectiveness for the handoff of WLAN and Bluetooth
Chung-Hsin Liu, Sheng-Shiang Chang

The study for the WLAN with ZigBee Positioning System
Chung-Hsin Liu, Jian-Yun Lo

CSCW-Based supply chain performance analysis system
Yanping WANG, Bo SUN and Guannan QU

CSCW Based Customer Relationship Management System
Naiji REN, Zhiyi FANG, Hongyu SUN, Bo SUN and Yang Zhao

A System Design of the Tahe’s Forest-Fire-Prevention Management System
Xindan Gao, Nihong Wang, Jun Li

Modeling Chinese Stock Markets’ Volatility
Shu Quan Lu, Shiyu Xie, Takao Ito

The Outliers of Chinese Stock Markets
Shu Quan Lu, Takao Ito

The Earthwork Plan Application of 3D Geospatial Data
Lee Jin-nyung, Pyun Moo-uk, Lee Byung-kil, Eo Yang-dam
Secure Health Monitoring using Medical Wireless Sensor Networks

Pardeep Kumar¹, Young-Dong Lee², HoonJae Lee³
¹²Department of Ubiquitous IT, Graduate School of Design & IT
³Division of Computer and Information Engineering, Dongseo University, Busan, 617-716, South Korea
pardeepkumar@dit.dongseo.ac.kr, ydlee@dongseo.ac.kr, hjlee@dongseo.ac.kr

Abstract- In this paper, we are addressing security requirements of health monitoring using medical sensor networks and proposed a secure framework called “SHM” (Secure Health Monitoring) using wireless sensor networks. SHM provides security services such as confidentiality, authenticity and integrity to patient data at low-cost. To provide confidentiality we have used PingPong-128 stream cipher. Authenticity and data integrity is achieved by PingPong-MAC (message authentication code). We have designed a real-time prototype with ECG and triaxial accelerometer sensors on Telos-mote for evaluating the proposed secure framework and our results confirm their feasibility.

I. INTRODUCTION

In our society, the populations of aged person who have chronic diseases like diabetes, congestive heart disease and many other conditions, such as blood pressure, blood glucose levels, furthermore, children suffering from long term disease like asthma are increasing continuously. However, there is one weak link when it comes to monitoring patients health status after they have returned home. So, wireless health monitoring is possible bridge for weak link, which could be able to monitor these people continuously over a long time, then the physician can detect serious health problem as soon as possible and provide better solution to them. Therefore, the researcher’s interests are attracted towards healthcare monitoring using sensors.

Healthcare monitoring using wireless sensor networks (WSNs) are consists of discrete group of independent nodes with low cost, low power, limited computation, less memory and communicate wirelessly over limited frequency and low bandwidth. Security is the most important concern of sensor network, particularly in WSN for the healthcare monitoring. The network should be capable of keeping the collected patient’s information private [1]. Any attempt to introduce ubiquitous healthcare systems using WSN should ensure adequate protection to the confidentiality and integrity of healthcare information. At the same time, the health’s information also needs to be readily available to all authorized healthcare providers, in order to ensure the proper treatment of the patient [2]. In fact, providing security in ubiquitous healthcare application using sensor networks is not an easy task, because the deployment of WSN in healthcare application must meet increasingly stringent security and privacy requirements [3]. It might be life-threatening, or even fatal, if this healthcare monitoring data is corrupted. Furthermore, privacy protection is paramount such that only authorized users can query or monitor the networks. Thus, strict security mechanisms must always be in place to prevent malicious interactions with the healthcare systems. Such mechanisms should also be scalable, since it is expected that thousands of WSNs will be deployed within the current decade [4].

In this paper, we are addressing the security requirements surrounding health monitoring using WSN and proposed a secure health monitoring (SHM) framework using sensor network. Our SHM is providing security services such as confidentiality, authenticity and integrity at low-cost energy-efficient mechanisms.

The rest of the paper is organized as follows: In section II, discuss the related work in secure healthcare monitoring and in section III, security requirements for SHM monitoring. In section IV, discuss the design of health monitoring network model and in section V, secure health monitoring (SHM) framework using sensor. In section VI, experimental setup and evaluation of results and section VII, conclusion and future work.

II. RELATED WORK

Haque et al. [5] proposed an efficient security scheme for patient monitoring system using wireless sensors network. This scheme is composed of three main components: Patient (PT), Healthcare Service System (HSS), and Secure Base Station (SBSs). A pseudo-inverse matrix is used to derive the pair-wise shared key and a bilateral key handshake method is used to establish secure communication between HSS and BSS or PT and SBS. As SBS has prior knowledge of secret key of PTs and HSSs, so any node PT-to-BSS in network can establish the secure communication or vice versa.

Malasri et al [6] implemented a secure wireless mote-base medical sensor network for healthcare application. This mechanism has three main components: (a) A two tier scheme is used for authentication based on patient’s biometric and physiological data; (b) An ECC-based secure key exchange protocol is used to setup shared keys between sensor node and base station; and (c) symmetric encryption/decryption algorithm is used for confidentiality and integrity. Each mote is connected with small fingerprint scanner; patient’s verification is done by base station via biometric signature. In this scheme patient’s motes are using base station based public key, to secure the key exchange protocol between the patient’s mote and base-station.
Fei et al. [7] proposed software and hardware based real-time cardiac patient healthcare monitoring system known as Telecardiography Sensor Network (TSN). TSN is specially designed for U.S. healthcare community, to perform real time healthcare data collection for elder patients in large nursing homes. In TSN, patient’s ECG signals are automatically collected and processed by small ECG sensor, and transmitted wirelessly to ECG server for further analysis. TSN is composed of large amount of wireless ECG communication units; each unit is called a mobile platform. A skipjack block cipher cryptography algorithm is used to protect patient’s privacy.

III. SECURITY REQUIREMENT

The elementary requirements of secure health monitoring using WSNs are safely exchanging the patient’s health information transmitted by WSN devices, and preventing improper use of illegal devices, such as intercepting transferred data, eavesdropping patient health-status data, replaying out-of-date information. Hence, it is necessary to understand the security requirements in SHM using WSN before integrating appropriate security mechanisms. In this section, we analyze essential security requirements of SHM using sensor network as follows:

A. Data confidentiality
Health information’s are generally held under legal and ethical obligations of confidentiality. Health-status information should be confidential, except their family doctor or caregivers. Therefore, it is important to keep their health information confidential, so that an adversary cannot eavesdrop the patient’s information. This eavesdropping may cause damage to the patient since the adversary can use patient’s health data for many illegal purposes. Cryptography algorithms (encryption schemes) are possible solution to achieve patient confidentiality, to protect the patient data eavesdropping by an adversary.

B. Data authentication
Authentication services are associated to authorization; it is necessary for both medical and non-medical application. In SHM using sensor network, it is must for each body sensor and base-station to verify whether the data was sent by the trusted sensor or not. In healthcare application data authentication can be achieved by using symmetric and asymmetric techniques.

C. Data Integrity
Data integrity services guarantee that at recipient end data is not altered in transit by an adversary. Due to the broadcast nature of sensor network, the health information’s could be altered by an adversary; this is very dangerous in case of life-critical events. To confirmation of data integrity, one must have ability to identify data manipulation by illegal parties. So, proper data integrity mechanisms ensure that the received data is not altered by an adversary.

IV. HEALTH MONITORING NETWORK MODEL

Health monitoring using sensors network model is composed of: 1) body area sensor nodes (SN); 2) small number of special purpose high-capability gateway node, 3) base station (BS) that have unlimited resources as shown in Fig 1. Fig.1 illustrates, each patients has one or more wireless sensor attached to his or her body area. It is assume that there are number of gateway node throughout the hospital. Queries for health data can be made from base station, which is directly handled by professional physician or nurses. Both queries and health data travel through the gateway nodes. All the queries encrypted on end-to-end basis.

V. PROPOSED SECURE HEALTH MONITORING FRAMEWORK

A secure health monitoring framework is designed based on massage authentication code, which provides message confidentiality, authenticity and message integrity to sensor nodes. Our framework is employing on PingPong-128 stream cipher based-privacy. Stream ciphers are generally used in such applications, where data comes in huge amount of unknowable length. So we have adopted stream cipher, because they are fast in software implementation. A PingPong-128 [8] stream cipher is proposed by Hoon Jae Lee and Kevin Chen in 2007. PingPong family is based on summation generator stream cipher with addition of mutual clocked control structure. This algorithm is designed with both security and efficiency in mind to satisfy the need for lightweight algorithms. PingPong is highly secure algorithm, dedicated to hardware environment and easy to implement in software. PingPong-128 is a bit based stream cipher as shown in figure 1. This stream cipher is constructed on two mutually clocking LFSRs and a single memory bit. PingPong-128 accept key as 128-bits and 128-bits initialization vector to feed the internal states. It generates an output block of 128 pseudo-random bits from a combination of the internal states, for each iteration. PingPong-128 has 257-bits of internal state. For the detailed specification, refer to [8].
A. Definition of PingPong-MAC (PP-MAC)

To establish an end-to-end trusted and secure communication between patient and base station, a message authentication code (MAC) scheme is proposed to achieve authenticity and data integrity.

The authentication scheme is based on an internal state being transformed along with the progress of encryption process. This results from the fact that the scheme employs PingPong-128 algorithms. This feature substantially reduces the excessive program space needed by the MAC scheme. It is assuming that the underlying primitives of PingPong-128 are secure. It is possible to build a proof of the given notion of security of the MAC procedure as shown in Table I.

<table>
<thead>
<tr>
<th>TABLE I</th>
<th>PINGPONG-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let ( P_t ) as Plaintext</td>
<td></td>
</tr>
<tr>
<td>Let ( C_t ) as Ciphertext</td>
<td></td>
</tr>
<tr>
<td>Let ( k_e ) as encryption key</td>
<td></td>
</tr>
<tr>
<td>Let ( k_m ) as MAC encryption key</td>
<td></td>
</tr>
<tr>
<td>Let ( C[i] ) be denoted ( i )-th 32-bit word of ciphertext.</td>
<td></td>
</tr>
</tbody>
</table>

1. \( C_t = E_k_e(P_t) \)
2. \( \{a, b, c, d\} = k_m(128\text{-bit}) \)
3. \( IV = \{\text{destpan}||\text{addr}||\text{type}||\text{group}||\text{counter}\}*2 \)
4. \( \{a, b, c, d\} = C[i] \oplus a, b, c, d \)
5. \( \text{Output MAC(32-bit)} \)

The encrypted ciphertext \( C_t \) is splitting into 32-bit blocks, and then padding the last word with zeroes, if required. Meanwhile, the MAC encryption key \( k_m \) is fed through variables \( a, b, c, d \) and then this key is XORing with 32-bit \( C_t \) with 32-bit of \( a \), and 32-bit MAC can be obtained by XORing of all \( a, b, c, d \) outputs.

To integrate our authenticated encryption procedure into sensor network, we are adding 2 bytes of counter \( c_t \) and 4-bytes MAC into default radio stack as shown in figure 2. A 2 bytes \( c_t \) is used to achieve the semantic security and 4 byte MAC is authentication.

B. PP-MAC Analysis

Practically, if IV should be message-unique for encrypted message with the same key, then it will not give additional rooms to an attacker. Since the IV is taken from the packet header of modified radio and sent to the decryption end, the 2 bytes counter \( c_t \) gives \( 2^{16} \) variations to the IV. This security property is very necessary to guarantee that message encrypted with same key should give different ciphertext every time. The MAC length indirectly implies the computation cost which would be needed to forge the MAC in chosen ciphertext attack. Zoltak et al [9] and Karlof et al [10] suggested the MAC length, MAC=4 bytes gives a well sufficient security and easy to implement. Practically 4 bytes of MAC is sufficient to wireless sensor network.

C. Operation mode of PP-MAC

The operation of PP-MAC is as follows: A patient node simply computes a MAC on the packet with MAC key \( k_m \) and encrypted message, and then authenticated packet will be send to base station. When base station received the authenticated packet, then he/she can verify that the packet is sent by patient node or not and no information has been altered in transit. PP-MAC is an Encrypt-then-MAC stream cipher mode [9].

VI. EXPERIMENTAL SETUP AND EVALUATION

A. Experimental Setup

As shown in Fig. 2, we have used our lab developed ECG and tri-axial accelerometer sensor for secure health monitoring.

![Fig. 2. New designed ECG and accelerometer sensor board; (a) Wireless sensor node and sensor board, (b) integrated both.](image)

![Fig. 3. Experimental Setup.](image)

For the experimental setup a sensor board is integrated to a wireless sensor node which consists of an ECG and a tri-axial accelerometer sensor. In the sensor board, ECG signals from the electrodes are amplified with a gain of 300 (24.8 dB) and filtered with the cut-off frequencies of 0.05 Hz and 123 Hz. An ECG electrode has two electrodes which are integrated within the sensor belt. In addition, the sensor board also has a three-axis accelerometer sensor (MMA7260Q, Freescale) to measure acceleration signals. We have tested real time health
data with this experimental setup. As shown in Fig 3, integrated with ECG and tri-axial accelerometer sensors mote is attached to person body. Sensor mote ‘B’ serves as base-station between the patient mote and PC, receiving mote A’s wireless packets. Mote B’s is serially connected to PC via USB. The detailed specifications of TelosB [11] motes are shown in Table II.

<table>
<thead>
<tr>
<th>TABLE II</th>
</tr>
</thead>
<tbody>
<tr>
<td>TELEOSB SPECIFICATIONS</td>
</tr>
<tr>
<td>ITEMs</td>
</tr>
<tr>
<td>Processor</td>
</tr>
<tr>
<td>Internal Memory</td>
</tr>
<tr>
<td>Flash Memory</td>
</tr>
<tr>
<td>Multi-Channel Radio</td>
</tr>
<tr>
<td>Interface</td>
</tr>
<tr>
<td>Sensors</td>
</tr>
</tbody>
</table>

We have implemented SHM framework on TinyOS [12], an event-driven open source operating system specially designed for wireless sensor networks. The code is written in nesC [13] for portability reasons.

B. Implementation Evaluation

We have implemented secure health monitoring using sensor network. Our result shows the feasibility of stream cipher for secure health monitoring using sensor networks. The results are shown in Table III. Our proposed scheme is taking 1093 bytes RAM and 16,452 bytes of program space. By doing so, we achieved a secure pair wise communication between neighboring sensor nodes. We also had implemented PP-MAC in Telos rev B sensor mote. It achieves two-party authenticated communication and data integrity for transmitted packet. PP-MAC required additional 20 bytes RAM and 960 bytes of ROM.

To evaluate the execution cycles required for each component such as PingPong-128 encryption, decryption and message authentication. A MSP430 internal built-in timer (localTimer) interface is used to calculate the execution time.

<table>
<thead>
<tr>
<th>TABLE III</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPERIMENTAL RESULTS</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Without security scheme</td>
</tr>
<tr>
<td>PingPong-128 (Encryption only)</td>
</tr>
<tr>
<td>PingPong-MAC (Encrypt &amp; Auth.)</td>
</tr>
</tbody>
</table>

Time to execute cipher operations on the 4MHz TelosB sensor node marked at 18.36 ms and 19.20 ms for PingPong-128 encryption and PP-MAC, respectively.

VII. CONCLUSION AND FUTURE WORK

In this paper we have proposed secure health monitoring using sensor network. We have designed a secure health monitoring (SHM) prototype using ECG and three-axi accelerometer sensors. PingPong-128 based-security feature are embedded into SHM application. Furthermore, PingPong MAC (PP-MAC) is computed on health data that provides authenticity. PP-MAC is employing on some of already computed data underlying PingPong-128 cipher. The salient features of PingPong-128 Method are its fast key generation and fast software implementation, good primitives for security such as encryption, authentication, decryption and data integrity.

The entity verification and message authentication have been tested through the performance of authenticator encryption schemes using TelosB sensor nodes for wireless sensor networks.

Still we are working to enhance the proposed approach for making it more secure for healthcare monitoring application using sensor network.

REFERENCES

NCM2010

6th International Conference on Networked Computing and Advanced Information Management

Editors
Dr. Franz Ko, Dr. Yunji Na

Sponsored by
The Institute of Electrical and Electronics Engineers, Incorporated
Institute of Electrical and Electronics Engineers (IEEE), Seoul Section, Korea
The International Association for Information, Culture, Human and Industry Technology (AIChIT), Korea