International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:4, No:12, 2010

Security Architecture for At-Home Medical Care Using Sensor Network

S.S.Mohanavalli, Sheila Anand

***Abstract*—**This paper proposes a novel architecture for At-Home medical care which enables senior citizens, patients with chronic ailments and patients requiring post- operative care to be remotely monitored in the comfort of their homes. This architecture is implemented using sensors and wireless networking for transmitting patient data to the hospitals, health- care centers for monitoring by medical professionals. Patients are equipped with sensors to measure their physiological parameters, like blood pressure, pulse rate etc. and a Wearable Data Acquisition Unit is used to transmit the patient sensor data. Medical professionals can be alerted to any abnormal variations in these values for diagnosis and suitable treatment. Security threats and challenges inherent to wireless communication and sensor network have been discussed and a security mechanism to ensure data confidentiality and source authentication has been proposed. Symmetric key algorithm AES has been used for encrypting the data and a patent-free, two-pass block cipher mode CCFB has been used for implementing semantic security.

***Keywords*—**data confidentiality, integrity, remote monitoring, source authentication

I. Introduction

PATIENTS who have undergone surgery and persons with chronic ailments require continuous monitoring of physiological parameters by medical professionals. This would require the patients to be either hospitalized for very long periods or visit the hospital for frequent medical care. Both options would be difficult and cumbersome for the patient as well as medical care givers.

An alternate solution would be to monitor such patients remotely either at home or at health care facilities, and medical professionals could be alerted to emergency situations to take appropriate measures such as dispatching an ambulance.

In this given scenario, patients are fitted with sensors placed non-invasively to measure the vital signs like ECG, pulse rate, blood pressure and others continuously. The sensor data is collected and transmitted to hospitals for remote monitoring by medical professionals like doctors and nurses. Sensor data is sent to the hospitals using wireless transmission, which is prone to different types of attacks such as eavesdropping, sending false values or replay of previous data. It is also essential to ensure that privacy and integrity of patient medical data is maintained. Another issue which needs to be addressed is proper authorization controls to prevent unauthorized access to patient information. In this paper, a novel architecture is proposed for monitoring patients at their homes and also certain of the key security requirements are addressed. Medical professionals can remotely monitor patients and senior citizens housed in the comfort of their homes, while at the same time satisfy the continuous care requirement.

Section 2 discusses the work related to security of medical sensor data and sensor networks. Section 3 details the proposed architecture for At-Home monitoring; Section 4 gives the features for securing the data transmission within the home premises, and simulation results. Section 5 presents conclusion and future work.

II. Related Work

Early work on sensor network security used symmetric key for securing sensitive data [13] [14]. These schemes were however more generic in nature and the unique security requirements of medical applications were not addressed. Conventional public key cryptographic systems cannot be directly applied due to constraints in sensor power and memory.

Current research focuses on sensor network for medical applications and tries to address the features specific to them. This section discusses a few of the related work, wherein, a number of medical sensors are attached to patients to measure their vital parameters. The patients are further equipped with a wearable data acquisition unit which collects the sensor data and wirelessly transmits them to remote monitoring stations at hospitals and health care facilities. The medical data is processed at the hospitals and suitably formatted and displayed for diagnosis by medical professionals. The data transmission between the sensors and wireless data acquisition units in patients can be wired or wireless. Wired transmission is achieved by integrating with wearable fabrics. CodeBlue proposed at Harvard University, one of the pioneers in medical monitoring acknowledges the importance of security for such systems but does not address the concerned issues [1]. ALARM-NET, uses AES for encryption, but does not discuss issues related to key management [2]. I-LIVING proposes a three - tier architecture, to provide data confidentiality and link level authentication using context information like authentication certificates and encryption

S.S.Mohanavalli is with Tagore Engineering College, Department of Electronics and Communication Engineering, Anna University, Chennai, India. (Phone: 91-9791071057; e-mail: ssmvalli@gmail.com).

Sheila Anand is with Rajalakshmi Engineering College, Anna University, Chennai, India. (e-mail: Sheila.anand@gmail.com).

.

keys stored in USB sticks. This requires pre-configuration of devices in the network to recognize the USB [3]. Wireless Sensor Network for Wearable Physiological Monitoring [5], discusses a wearable jacket embedded with sensors that monitor the physiological parameters. The sensed values are sent to a wearable data acquisition hardware which after processing the data sends them to the base station. This paper briefly mentions the need for data confidentiality. SNAP [4], Sensor Network for Assessment of Patients specifically addresses security issues such as data confidentiality, authentication and key exchange. The key exchange is based on ECC; the sensor data is encrypted using RC5 algorithm and HMAC is used for authentication. This work also discusses the query mechanism used for accessing the sensor data. The proposed architecture appears more relevant for continuous patient monitoring in large health care centers with many patients. The wireless sensor mote fitted on each individual patient collects the sensor data and directly transmits the data to the nearest base station. Several such base stations have to be provided to pick up signals from the patients. The query data exchange between the doctor and the patient may be routed through one or more base stations.

III. Architecture For At-Home Medical Care

The proposed architecture for At-Home medical care with remote monitoring by medical experts is given in Figure 1.

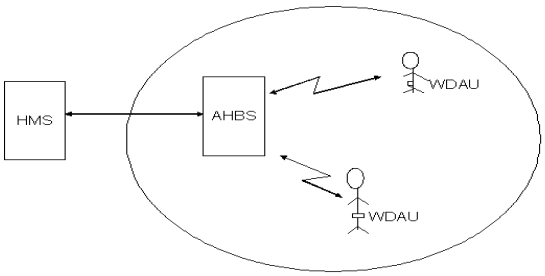

Fig. 1 At-Home Architecture

This architecture can be used to monitor one or more family members living in the same house; who require post-operative care or are suffering from chronic illness. Senior citizens can also be attached with sensors to monitor their vital signs while allowing them to carry on with their daily routine unattended.

The patients would be equipped with multiple sensors appropriately placed to measure his/her physiological parameters like ECG, blood pressure, pulse rate and others. Each patient would be fitted with a Wearable Data Acquisition Unit (WDAU) that would collect and aggregate the sensor data. The aggregated data would be transmitted wirelessly to the At-Home Base Station (AHBS). AHBS would then transmit the patient data to the Hospital Monitoring Station (HMS) for processing and follow-up by the medical care-givers. Some of the key aspects addressed in the architecture are:

(i). It is possible to monitor more than one patient within the house/home. Each patient would be provided with a WDAU and identified by a unique ID termed Patient Unique ID (PUID).

(ii). The PUID can be embedded in the WDAU and sent along with the sensor data to identify the patient. The PUID can be periodically varied for greater security.

(iii). As each WDAU needs to transmit patient data only to AHBS and not directly to HMS, the wireless range and other transmission requirements are limited to the confines of the home.

(iv). The function of WDAU includes individual patient data aggregation and wireless transmission to AHBS. As the computational requirements are limited the power consumption would also be less. Rechargeable batteries can also be used to extend the battery life.

(v). AHBS can be a simple wireless router or a conventional computer system with no constraints in power or computational capabilities.

(vi). The transmission between WDAU and AHBS has to be secure to prevent tampering of patient data.

(vii).The transmission of patient medical data between AHBS and the HMS can be done using normal communication channels. Public key and other conventional security systems can be used to provide a high level of security and privacy for patient data.

(viii). Proper authorization controls should exist for access of patient data by medical care givers.

The patients have the psychological advantage of being at home and carrying on their normal routine. At the same time the well-being of the patients can be continuously and remotely monitored by medical professionals to ensure proper medical care. There would also be tremendous cost savings such as hospitalization charges, trained assistance etc. Further, paramedics can also be specially trained to monitor such patient data and alert the medical experts in emergency situations. In cases of anomalies in vital parameters, medical professionals can also direct AHBS via HMS to increase the sampling frequency of the sensors to collect the data at more frequent intervals. AHBS can also monitor the values of the vital parameters and alert the care givers via HMS.

IV. Securing Transmission Between WDAU And AHBS

Security is a key issue and securing wireless transmission between WDAU and AHBS is addressed in this section. Certain of the common security threats include; (1) wireless transmission is inherently insecure and prone to data loss and eavesdropping; (2) patient data may be subject to unauthorized modification; (3) an attacker can inject false values in the data; (4) data packets may be captured and replayed later. Hence, it would appear that the patients are normal and stable even while the medical network is being subjected to attack. The security solution should also take into consideration the following critical aspects; (a) the patients are mobile; (b) the care givers are mobile; (c) more than one patient is being monitored; (d) more than one care giver would

need to access the data and (e) sensors can get lost either inadvertently or be physically removed by the attacker to prevent the patient from being monitored. Lastly, it is imperative to ensure privacy of the medical data.

A solution for securing the wireless transmission between WDAU and AHBS which combines data confidentiality and authentication of WDAU by AHBS is proposed. Sensors measure the values at the intended time of intervals and send them to WDAU that is attached to the patient. WDAU encrypts the data obtained from the sensors using a secret key that is shared between WDAU and AHBS. The header generated by WDAU, encrypted data and shared secret key are used to generate a Message Authentication Code (MAC). The header, encrypted data and MAC are combined into a data packet and transmitted to AHBS. The block diagram of the encryption and authentication at WDAU is given in Figure 2

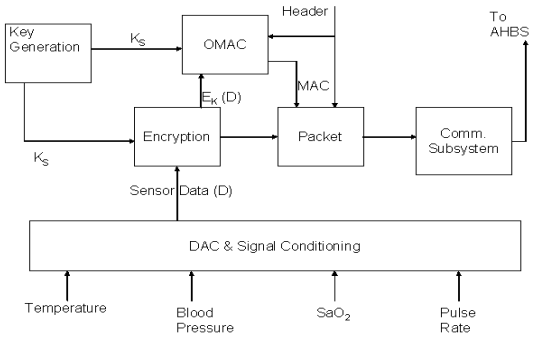

Fig. 2 Encryption/Authentication at WDAU

On receiving the packet, AHBS generates MAC using its secret key and received data. It compares the generated MAC with the received MAC and verifies that both are the same. By this, it is also able to authenticate the origin of the received data packet. Data confidentiality is ensured as the secret key is known only to WDAU and AHBS. Diffie-Hellman key exchange protocol is used to generate the secret key at WDAU and AHBS.

The block diagram of the encryption and authentication at AHBS is given in Figure 3. 128 bit AES is used for encryption. The key size should be sufficient for the At-Home scenario and to further increase the security of encryption, block cipher mode CCFB has been used [6].

On initialization, both WDAU and AHBS individually generate a 160 bit public/private key pair using Elliptic Curve Cryptography (ECC) algorithm proposed by Liu et al [15].

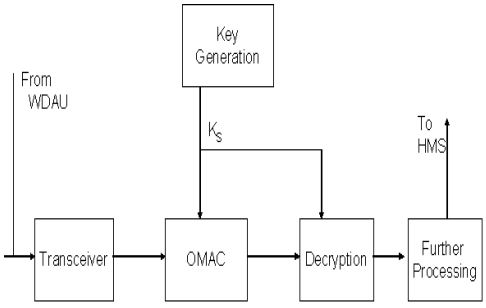

Fig. 3 Encryption /Authentication at AHBS

WDAU and AHBS exchange their public key using Diffie-Hellman key exchange protocol. The secret key KS is generated at WDAU as a function of its private key (KRM) and the public key received from AHBS (KUB). Likewise, AHBS generates the secret key KS using its private key (KRB) and WDAU public key (KUM). The secret key generated at both places would be identical. The secret key generated is verified to be the same at both AHBS and WDAU. Further, AHBS generates a session number (SN) for use in subsequent transmissions of data. The processing steps are given below

Step 1: AHBS generates a nonce n1 and a random session number SN

Step 2: SN and nonce are encrypted at AHBS using the secret key and sent to WDAU

Step 3: WDAU decrypts and obtains the nonce n1 and session number SN.

Step 4: WDAU encrypts the nonce n1 with the secret key and sends it to AHBS.

Step 5: AHBS decrypts and verifies that the secret key generated is the same.

This procedure also ensures the secure transmission of the session number. The random generation of SN prevents replay attack. The sequence of steps is summarized in Table 1.

TABLE I
SECRET KEY GENERATION AND VERIFICATION

AHBS: K_{UB}, K_{RB}
AHBS → WADU: K_{UB}
WADU : K_{UM}, K_{RM}
WADU → AHBS : K_{UM}
WADU : $K_S = f(K_{UB}, K_{RM})$
AHBS: $K_S = f(K_{UM}, K_{RB})$
AHBS → WADU: $E_K = (n_1, SN)$
WADU: $D_K (n_1, SN)$
WADU → AHBS: $E_K (n_1)$

The data encryption procedure is next explained. The sensor data is encrypted using AES algorithm which uses K_S, the secret key shared between WDAU and AHBS. The block cipher mode used here is CCFB. The Initialization Vector (IV) is a function of the nonce and the SN. MAC is generated using OMAC algorithm which takes as input the encrypted data, header and secret key KS. The generated MAC size is 128 bits.

AES with 128 bit symmetric key is used as encryption algorithm. The key length is sufficiently long to provide a reasonable amount of security that is required for the application. The block size used is 128 bit, standard fixed size for AES, with 10 rounds. So far no known successful attack has been reported on 10 round AES for 128 bit key. Since the encryption uses a publicly known algorithm, the security of the system depends only on the difficulty in getting the secret key.

Based on Shannon's work in Information theory, in order to achieve perfect security it is necessary that the key should be as long as the message to be transmitted and should be one-time pad. But it is practically infeasible to manage such long keys. Moreover in constrained situations such as that in a sensor network where nearly all resources are to be used very cautiously, the idea of a one-time pad is not a feasible solution. Instead, the focus is on increasing the computational security, by achieving semantic security, that is, the same message would generate a different cipher for every encryption. This would make it difficult for the attacker to break the cipher. CCFB block cipher mode is used to achieve semantic security and it has been specifically developed for low-end devices and small embedded systems like sensor motes and RFID tags. There are several other fast single-pass schemes but their use is deterred by patents. CCFB is a two-pass Authenticated Encryption with Associated Data (AEAD) scheme not covered by any known patents [6].

Key exchange and encryption protocol has been simulated using TinyOS 1 for MICAz motes. Four physiological parameters namely: Blood Pressure, Pulse Rate, Oxygen Saturation (SaO2) and Temperature of the patients have been used. The normal values of the parameters are given in Table 2 [5]

TABLE II
SPECIFICATION OF VITAL PARAMETERS MONITORED

Vital Parameters	**Specification**
Blood Pressure	Systolic: 60 - 200mmHg Diastolic: 50 – 110mmHg
Pulse Rate	72-90 beats per minute
Oxygen Saturation (SaO_2)	0-100%
Temperature	32°C-40°C

It is assumed that WDAU transmits sensor data every 10 seconds. The four sensor parameters have been randomly generated for continuous monitoring of five patients and the encryption / decryption process and authentication process have been verified.

V. CONCLUSION AND FUTURE WORK

In this paper, a novel architecture for continuous unobtrusive monitoring of patients at home by medical professionals is proposed. Sensors are used to measure physiological parameters at predefined intervals and sent to the hospitals for medical care and diagnosis. The work presented in this paper deals with transmission of four measured body parameters, namely, blood pressure, pulse rate, oxygen saturation and temperature. Other vital parameters like ECG, Galvanic Skin Response, and Respiratory Rate can also be measured to provide complete medical care. This work also addresses the security issues related to wireless transmission of patient data within the home environment. The open source CCFB scheme along with AES symmetric encryption and Diffie-Hellman key exchange to provide data confidentiality and source authentication has been used. This proposed architecture can be used for geriatric health care, continuous monitoring of patients who have undergone surgery, and patients with chronic ailments. It can also be adapted to monitor the health status of sports persons within a stadium or other confined enclosure.

ACKNOWLEDGMENT

S.S.Mohanavalli, thanks Dr.R.Padma (Madras Institute of Technology, Anna University, Chennai) for her valuable guidance and support.

REFERENCES

[1] V. Shnayder, B.R. Chen, K. Lorincz, T.R.F .Fulford-Jones and M. Welsh," Sensor networks for medical care", Technical Report TR-08-05, Harvard University, Apr.2005.
[2] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin and J. Stankovic," ALARM-NET: Wireless sensor network for assisted-living and health monitoring", Technical Report CS -2006-01, University of Virginia, 2006.
[3] Q. Wang, W. Shin, X. Liu, Z. Zeng, C. Oh, B. Al-Shebli, M. Caccamo, C. Gunter, E. Gunter, J. Hou, K. Karahalios and L. Sha," I-LIVING: An open system architecture for assisted living", IEEE SMC, 2006.
[4] K. Malasri, L. Wang," Addressing security in medical sensor networks", HealthNet, June 2007.
[5] P.S. Pandian, K.P. Safeer, P. Gupta, D.T. Sankunthala, B.S. Sundersheshu and V.C. Padaki," Wireless sensor network for wearable physiological monitoring", Journal of Networks, vol 3, May 2008.
[6] Stefan Lucks," Two-pass authenticated encryption faster than generic composition", Fast Software Encryption, 2005.
[7] Chiu C. Tan, H. Wang, S. Zhong and Q. Li," IBE-Lite: A lightweight identity based cryptography for body sensor networks", IEEE Transactions on Information Technology in Biomedicine, Vol 13, Nov, 2009.
[8] H. Li and J .Tan," Heartbeat- driven medium access control for body sensor networks. IEEE Transactions on Information Technology in Biomedicine, vol 14, Jan, 2010.
[9] V. Venkatasubramanian, A. Banarjee and S.K.S. Gupta," PSKA: Usable and secure key agreement scheme for Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, Vol 14, Jan 2010.
[10] Certicom Research. Standards for Efficient Cryptography (SEC) 1: Elliptic Curve Cryptography. Sept 2000.
[11] Certicom Research. Standards for Efficient Cryptography (SEC) 2: Recommended Elliptic Curve Domain Parameters. Sept 2000.
[12] Crossbow Solutions Newsletter. Motes for Mobile Communication and Tele-Medicine, 2005.
[13] A. Perrig, R. Szewczyk, J.D Tygar, V.Wen, and V.Culler, "SPINS: Security Protocols for Sensor Networks", Wireless Networks, 8 (2002), pp. 521- 534.
[14] C.Karlof, N. Sastry, D. Wagner, "TinySec : A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, November 2004, ACM Press, pp. 162-175.
[15] A. Liu, P. Kampanakis, and P. Ning, "TinyECC: Elliptic Curve Cryptography for Sensor Networks", http://discovery.csc.ncsu.edu/software/TinyECC.