2012 International Conference on Intelligent Information and Networks (ICIIN 2012)
IPCSIT vol. 23 (2012) © (2012) IACSIT Press, Singapore

Mutual Authentication Protocol for WSN on Medication Safety

Hsuan-Hsun Wu[+], Chih-Hung Huang,Yu-Jung Huang

Department of Electronic Engineering
I-Shou University, Kaohsiung, Taiwan, R.O.C.

Abstract. Due to the convenience of Wireless Sensor Networks (WSN), we intend to build a Medication Safety WSN system. Nowadays, medication administration can be quiet complex encompasses information of inpatients, drugs and data storages. Therefore, potential medication errors may exist often caused by false human judgment or lack of human resource (e.g. outnumbered nurses), and threats may occur because of the vulnerability of wireless communication. In this paper we propose a mutual authentication protocol for WSN on medication safety to fit the IT infrastructure of hospitals. The performance of the protocol is verified and simulated using Verilog hardware description language.

Keywords: wireless sensor networks, mutual authentication protocol, WSN security, medication error

1. Introduction

In Wireless Sensor Network (WSN), the sensor nodes are distributed in the environment to collect information according to detection of an event; data is sent to the user or base-station, which allows the user to have further analysis and processing. By applying the characteristics of wireless sensor networks can reduce human resource costs and errors [1] on each particular site data collection of information. In exchanging information for wireless sensor network via wireless transmission, the data protection of transmission must be disposed; otherwise data interception and tampering on transmission can happen easily, which will also cause the base-station to receive false message, and further result in unexpected damage. For example: the sensor network may be deployed in a medical monitoring system, if it is vulnerable to attacks, the messages or personal information that are transmitting in progress can be tampered or stolen, which may consequence in the danger of personal privacy and safety, thus, the security of data transmission for wireless sensor the network is a important issue to be discussed. In order to achieve application of secure authentication, usually involves encryption technology to protect data privacy and integrity, where a security system of wireless sensor network can be established by mutual authentication protocol, which can effectively ensure the security of communication between the transmitter and receiver. In this paper, we intend to utilize the cover coding between the sensor nodes to realize wireless sensor network mutual authentication protocol and achieve security requirements.

2. Background Review

Wireless sensor networks send messages through a wireless communication media, where often the attacker is able to conduct a connection through an anonymous message transmission, making it vulnerable to attacks. Hence, in order to prevent the possibilities of security breaching, many of these issues are considered and the implementation on the performance of special symmetry cryptography have been proposed continuously, for example, Hight [2], DESXL [3], Present [4] and so on. In the application of wireless network, both side of the party must have a public key to manage protocol and create a pair of keys between sensor nodes, there are currently many researches that explore this area of topic [5-6]. One

[+] Corresponding author.
E-mail address: isu9902017m@isu.edu.tw.

commonly seen is enable the network of sensor node to have a secure operation for basic conditions, the encryption keys between nodes accomplishes communication security.

Despite many studies on security issues of recent wireless sensor network have been published, the current research report shows that user identity verification in wireless sensor network has not been addressed adequately. For example, the use of different keys to manage protocol for supporting a specific function of sensor network are often been referred [7]. Recently, Wong et al [8] proposed a dynamic user authentication scheme for wireless sensor network, which includes registration, login and user authentication. Tseng et al [9] also proposed a revised protocol to improve the defects on the work of Wong et al; the solution includes registration, login, user authentication and password change. However, the protocol of Tseng et al does not have mutual authentication mechanism between the user and sensor nodes, nor between the sensor gate and sensor node, hence exists the threat of attack.

3. Security Methodology

For the purpose of ensuring safe data transmission and access, we have improved the original one-way hash function of Tseng et al who proposed mutual authentication protocol, and then a KeyGen() algorithm is created to encrypt the transmitting data with reference to the authentication mechanism given by Tseng et al, thus leading to a new mutual authentication mechanism of WSN.

According to definition, when wireless transmission of data is in progress, if the node receives the correct access information Msg_A and password PW, the command message will then be permitted, we assume Msg_A and PW is 32 bit message data, and its expression are:

$$Msg_A = a_0 a_1 a_2 \dots a_{31} \quad (1)$$

$$PW = P_0 P_1 P_2 \dots P_{31} \quad (2)$$

The random number will be set to 16 bit for Rt and Rm, and substitute Msg_A into KeyGen () algorithm to obtain the key Keyx, the expression is:

$$R_t = d_{t1} d_{t2} d_{t3} d_{t4} (Base\ 10) \quad (3)$$

$$R_m = d_{m1} d_{m2} d_{m3} d_{m4} (Base\ 10) \quad (4)$$

$$Msg_A - KeyGen(R_t, R_m) = a_{d_{t1}} a_{d_{t2}} a_{d_{t3}} a_{d_{t4}} \parallel a_{d_{t1}+16} a_{d_{t2}+16} a_{d_{t3}+16} a_{d_{t4}+16} \parallel a_{d_{m1}} a_{d_{m2}} a_{d_{m3}} a_{d_{m4}} \parallel a_{d_{m1}+16} a_{d_{m2}+16} a_{d_{m3}+16} a_{d_{m4}+16} = d_{v1} d_{v2} d_{v3} d_{v4} (Base\ 10) \quad (5)$$

$$PW - KeyGen(d_{v1} d_{v2} d_{v3} d_{v4}, R_t) = Key_x \quad (6)$$

Calculation from encryption function KeyGen () obtains Keyx, then execute XOR on the transmitting data Msgx will generate CCMsgx which accomplishes an encryption. Afterwards, the encryption only requires Keyx and execute XOR once again to decode, the expression is:

$$CCMsg_x = Key_x \oplus Msg_A \quad (7)$$

$$Msg_A = CCMsg_x \oplus Key_x \quad (8)$$

4. MS-WSN Protocol

In this section, we propose a Medication Safety WSN protocol (MS-WSN) which provides a solution to improve medication safety based on WSN technology. Safe drug procedure: A nurse is given the prescription of a particular inpatient and the tag of the inpatient is read through a PDA- which acts as a reader. Then the PDA updates inpatient's identification, UrKey to Hospital Info System (HIS) hence the registration phase. Afterwards, PDA and pharmacy receives random number to proceed login phase. At last, the authentication phase, the nurse sends message via PDA to unit dose to verify validity and message continues back to the PDA and finally, authentication calculation with the inpatient to complete authentication phase. This system is designed to adapt the IT infrastructure of modern hospital.

The three phases of the protocol are shown in figure 1 and details are as follows:

The first section is registration

Step 1 PDA will self-generate and save random number RM and UrKey, utilizing KeyGen() algorithm and ID to compute x.

Step 2 PDA sends x then demand (HIS) to generate random number RN and password PW.

Step 3 After HIS receives demand from PDA, begins to generate and save random number RN, TS and password PW, ID and PW employs KeyGen() to compute P, then P$\oplus$PW produce CCPWx, and then use CRC-16to produce PWGK.

Step 4 After PDA and pharmacy receives PWGK, TS and RN from HIS, proceed decode and save PWGK, and ends the registration phase.

The second section access message phase

Step 1 Pharmacy receives random number RN and Msg that is to be sent and password PW, then employs KeyGen() algorithm and CRC-16 to generate MUK.

Step 2 Pharmacy sends MUK, x* and t_1 to PDA through unit dose.

Step 3 After PDA receive information from pharmacy, simultaneously records time t_2 and examine (t_2 - t_1)>ΔT. If it is in the legitimate time range, begins to produce MGK, and verifies if the MUK and x* from user matches with saved data, when valid save MGK and T_1.

Step 4 PDA sends MGK, x*, t_1 and t_3 to inpatient.

Step 5 After inpatient receives information from PDA, simultaneously records time t_4 and examine (t_4 - t_3)>ΔT. If it is in the legitimate time range, begins to produce MSK, and verifies if the MGK and x* from user matches with saved data, when valid save MSK and T_1.

Step 6 After PDA receive MSK, x*, t_1 and t_5 from inpatient, access message phase is completed.

The third section authentication phase

Step 1 After PDA receives information from inpatient, simultaneously record time to examine (t_6– t_5)>ΔT, and verifies if t_1 from user exist on the list of saved data, when one of the two requirements fails will end the authentication phase. Afterwards, examine if MGK and x matches with MSK and x*.

Step 2 Unit dose receives MGK*, t_1, x* and t_7 from PDA.

Step 3 After Unit dose receives information, simultaneously record time to examine (t_8– t_7)>ΔT, and verifies if t_1 from user exist on the list of saved data, when one of the two requirements fails will end the authentication phase. Afterwards, examine if MSK and x matches with MGK and x*.

Step 4 Unit dose sends MSK*, t_1, x* and t_9 to inpatient.

Step 5 After inpatient receives information, simultaneous record the time t_{10} to examine (t_{10}– t_9)>ΔT, and verifies if t_1 from user exist on the list of saved data, when one of the two requirements fails will end the authentication phase. If it is in the legitimate time range, begins to decode and verifies if MSK* and x* from sensor node matches with saved data MUK and x, then decode x* to generate UrKey*, then verify if it matches, once valid end authentication phase.

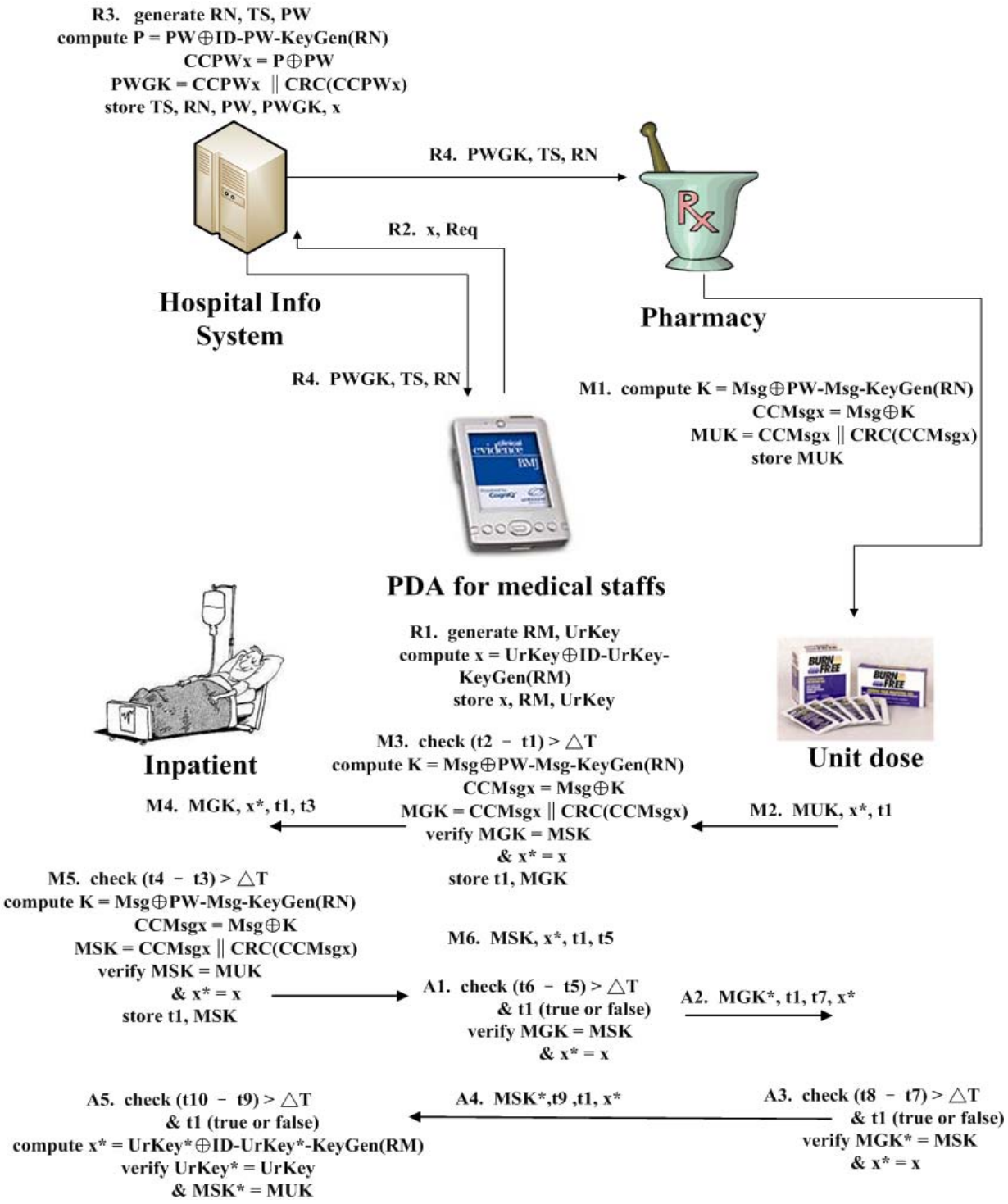

Figure 1 Medication Safety WSN protocol

5. Design and Implementation

A system structure is provided by utilizing Altera Quartus II software, the hardware frame is as shown in figure 6. First of all, R_{TX} and R_{MX} is send to 4_to_2Choose module to do optional XOR operation, then set 2 Inputs from 4_to_2 Choose module, and choose Msg_A or PW from 2_to_1 Choose module for KeyGen() algorithm computation, and last, set output to internal Register1 or Register2 for temporary store from 1_to_2 Choose module, then Register1 and Register2set to feedback or output. Output "Control" set by "Choose module" is applied by the state machine for signal control.

Figure 7 shows KeyGen() algorithm simulation results. In this simulation, "RTN_do" and "RMN_do" has been used as a control signal for random number generating, when control signal is high begin

generating random number, we set access message Msg_A=12345678, password PW=ABCDEF01; for random numbers generate R_T=6C00, R_M=CF03 when "RTN_do" and "RMN_do" turns high. The computation results are two key data string Key_M=3333, Key_L=33DD; here $(Msg_A)_M$, $(Msg_A)_L$ proceed XOR operation and encryption, $CCMsg_M$=2107, $CCMsg_L$=65A5.

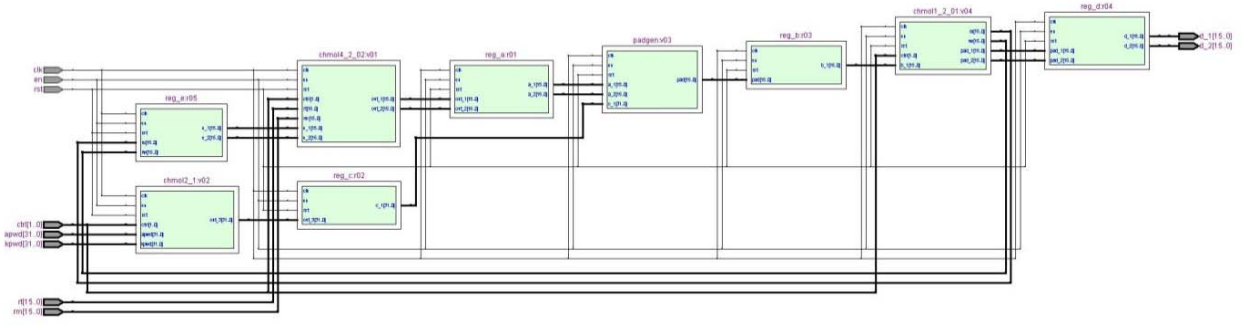

Figure 2 System framework of WSN

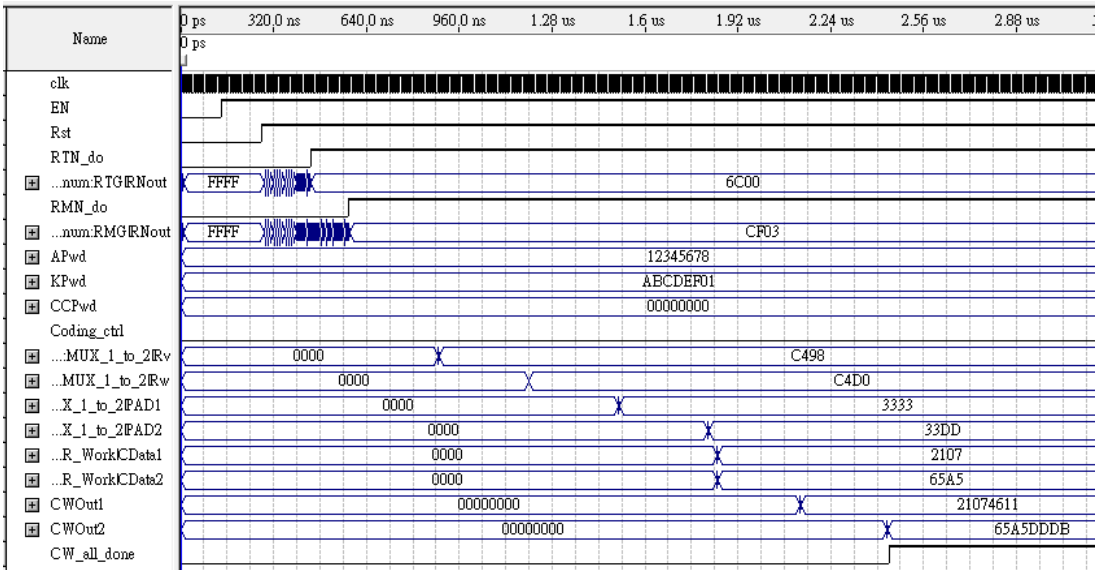

Figure 3 KeyGen() algorithm simulation results

6. Conclusion

In this paper WSN mutual authentication framework has been provided, KeyGen() algorithm was applied in mutual authentication framework to enhance the security of hiding original information. The design application on WSN system is proposed to realize authentication relation between sensor nodes on wireless sensor network and its application in medication safety has also been verified. The system performance is also realized through Verilog hardware description language to accomplish the framework design of each related module and system for medication purpose electronic devices.

7. Acknowledgement

This work was supported in part by the National Science Council, Taiwan, under Grants NSC 100-2221-E-214 -052 – and NSC 99-2221-E-214 -068 -.

8. References

[1] DJP Williams, "Medication errors", Consultant clinical pharmacologist, Department of Clinical Pharmacology, Aberdeen Royal Infirmary, Foresterhill, Aberdeen, Scotland, UK, 2007.

[2] Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.-S, Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., and Chee, S., "HIGHT: A New Block Cipher Suitable for Low-Resource Device," In: Goubin, L., Matsui, M.(eds.)

CHES 2006. LNCS, Vol. 4249, Springer, Heidelberg, pp. 46-59, 2006.

[3] G. Leander et al. “New Lightweight DES Variants,” Proc. Fast Software Ecryption 2007, LNCS 4593, Springer-Verlag, pp. 196-210, 2007.

[4] A. Bogdanov et al., “PRESENT”: An Ultra-Lightweight Block Cipher,” Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES07), LNCS 4727, Springer, pp. 450-466, 2007.

[5] Suat Ozdemir, and Yang Xia, “Secure data aggregation in wireless sensor networks: A comprehensive overview Computer Networks,” Vol. 53, No. 12, pp. 26-32, 2008.

[6] Xuan Hung Le; Sungyoung Lee; Phan Truc; La The Vinh; Khattak, A.M. ;Manhyung Han; Dang Viet Hung; Hassan, M.M.; Kim, M.; Kyo-Ho Koo; Young-Koo Lee; Eui-Nam Huh, Consumer Communications and Networking Conference (CCNC), 7th IEEE, 2010.

[7] Yun Zhou, Yuguang Fang, and Yanchao Zhang, “Securing wireless sensor networks : a survey,” volume 10 of Communications Surveys and Tutorials, pp. 6-28, IEEE, 2008.

[8] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” In Proc. of the IEEE International Conference on Sensor Networks, Ubiqutous, and Trustworthy Computing(SUTC’06), pp. 244-251, Jun. 2006.

[9] H.R. Tseng, R.H. Jan, and W. Yang, “An improved dynamic user authentication scheme for wireless sensor networks,” In Proc. of the IEEE Global Communications Conference (GLOBECOM’07), pp. 986-999, Nov. 2007.