Application Scheme of PKI System in Wireless Medical Data Transmission Network

Hui Wang and Chenming Gu(✉)

College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, Jiangsu, China
gcm0621@hotmail.com

Abstract. With the rapid development of Internet of Things (IoT) and medical informatization, various kinds of intelligent medical devices have emerged in the market. Intelligent medical devices are capable of monitoring the health condition of the patient through sensors and sending those information to third parties. However, if there are no management and encryption of the information to ensure accuracy, those devices will not be able to monitor health condition accurately or even cause medical accidents. Under the circumstances, a secure data transmission scheme based on Public Key Infrastructure (PKI) is proposed. This scheme controls energy efficiency by transferring the high energy consumption of asymmetric encryption calculation to third parties. This paper also estimates the data transmission energy consumption of certain kind of wireless device, which implements the scheme to ensure feasibility.

Keywords: Internet of Things · Public key infrastructure · Data security
E-health

1 Introduction

With the rapid development of computer information technology and Internet of Things (IoT), while medical information systems such as Hospital Information System (HIS), Picture Archiving and Communication Systems (PACS), Electronic Medical Record (EMR) have becoming increasingly mature. Hospitals are heading the direction of information, modernization, digitization. A wide range of intelligent medical equipment emerging under the concept of IoT. Those data will be diagnosed and stored by hospital information systems. The patients' private data and diagnostic information provided by medical institutions are sensitive information and it is critical to implement data encryption for these information during transmission. Apart from patient health data, the doctor's diagnosis became incomplete or tampered, which will cause serious consequences such as medical malpractice. Public Key Infrastructure (PKI) is the foundation and core of network security construction, which is the basic guarantee for the implementation of e-commerce security. PKI system can achieve identity authentication, secure transmission, non-repudiation and data integrity. Certification Authority (CA) is responsible for the application, production, distribution, updating, certification and management of various digital security certificates for units, individuals or equipment. A lightweight end-to-end medical data

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 387–395, 2018.
https://doi.org/10.1007/978-3-319-90802-1_34

transmission scheme is proposed in this paper to establish a secure data transmission between intelligent medical devices and servers [1–4].

2 Scheme Overview

In this chapter, we will demonstrate the network model of the scheme, then provide a macroscopic review of the protocol and the keywords used in this paper. Finally, provide a detailed description of the data transmission process.

2.1 Network Model

The network model of the scheme consists of four main components: intelligent medical devices based on mobile interactive sensors, third parties, remote servers and CA companies (Fig. 1).

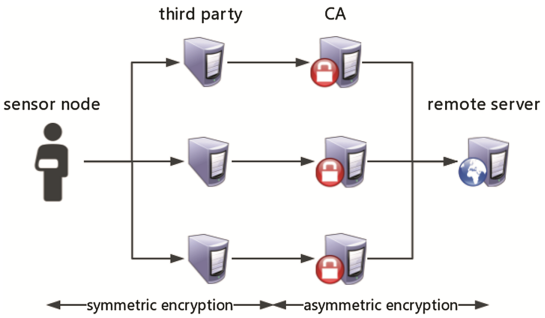

Fig. 1. The network model of the proposed scheme.

(1) Mobile interactive sensors: Through the implantation or adsorption of human body, this kind of sensor access to the patient's health data such as blood pressure, blood sugar and so on. Devices equipped with these sensors mostly adopt embedded architecture. They can perform wireless data transmission through WIFI, Bluetooth and so on [5].
(2) Third party equipment: Third parties are the key links in the scheme. A certain third party is any entity that can provide high-speed data process for the sensor nodes, such as the HIS and PACS systems of the hospital. Resource constrained sensors rely on these hardware and software for data formatting and corresponding encryption operations. Third party is denoted by TP_i [6].
(3) Certification Authority: CA mechanism ensures that third parties and remote servers communicate through certificate-based authentication, and verify the accuracy of the data by signing and verifying the data through the relevant method provided by the trusted CA authorities.

2.2 Scheme Elaboration

The proposed scheme provides a continuous message interaction process, through which the message body containing different information to complete the data encryption and transmission. Figure 2 summarizes the system message exchange process, which is divided into five phases, including 11 interactive message bodies.

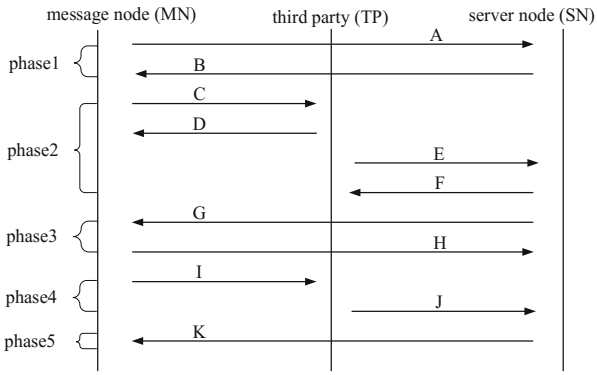

Fig. 2. Message exchange process of the data transmission

Table 1 shows the descriptions of some variables used in the scheme, they will be used mostly in the message formula.

Table 1. Notation and description of the variables in the scheme

Notation	Description
MN	Message node
SN	Server node
TP_i	Third party
CA	Certification authority
N_x	Data generated by node x
$K_{x,y}$	Symmetric key between x, y
K_x	Public key of node x
K_x^{-1}	Private key of node x
$[data]_k$	Data encrypted with key k
$SIGN_x$	Node x's digital signature
S	Credential between MN and SN

Phase 1 (initialized interaction):

Due to the limited computing power of wireless sensor nodes, MN can only perform symmetric encryption function. Node MN initiates the exchange by sending a HELLO message A to SN. This message informs SN about the security policies such as AES encryption algorithm, SHA algorithm and so on. If the server node responds, SN will

select one of the proposed security policies, SN responds with a HELLO message and generates a symmetric key for selected symmetric encryption method.

$$\text{A: } MN - hello\left(N_{MN}, SecurityPolicy\right) \tag{1}$$

$$\text{B: } SN - hello\left(N_{SN}, SecurityPolicy\right) \tag{2}$$

Phase 2 (Secure connection between nodes):

After a successful connection between the MN and the SN, this phase requires the establishment of a secure channel between TP_i and MN or SN. MN sends a message C to a TP_i device to inform its presence, this message includes a Message Authentication Code (MAC), which is encrypted by the symmetric encryption key K_{MN,TP_i} generated in phase 1, and send message D to agree to join the information exchange process. It is worth noting that in the message E, each TP_i sends public key along with certificate to the SN, meanwhile requests server certificate from SN. If the certificate provided by TP_i is certified, SN will return the certificate requested by TP_i.

$$\text{C: } \forall_i \in \{1, n\}\left[MN, N_{MN}, N_{SN}\right]_{K_{MN,TP_i}} \tag{3}$$

$$\text{D: } \forall_i \in \{1, n\}\left[TP_i - hello\left(N_{TP_i}\right)\right] \tag{4}$$

$$\text{E: } \forall_i \in \{1, n\}\left[CertRequest, Cert, N_{MN}, N_{TP_i}\right] \tag{5}$$

$$\text{F: } \forall_i \in \{1, n\}\left[Cert_{SN}, N_{TP_i}\right] \tag{6}$$

Phase 3 (Proving third party representativeness of MN to SN):

At this stage, it is necessary to prove to SN that TP_i represents a specific MN and verify the representative relationship. As response, MN will perform a hash function on each key to ensure data confidentiality and send it to the SN in message H. TP_i will send the data to the SN in the next phase and Hash value of the MN symmetric key K_{MN,TP_i}. The matching of the data proves the representation of specific MN node by perform a data comparison.

$$\text{G: } HashRequest\left(N_{SN}\right) \tag{7}$$

$$\text{H: } \left[Hash\left(K_{MN,TP_1}\right), Hash\left(K_{MN,TP_2}\right), \ldots Hash\left(K_{MN,TP_m}\right), N_{MN}\right] \tag{8}$$

Phase 4 (Encryption and transmission of critical data):

Through the first few stages of exchange, network entities have successfully established connections. At this point, MN generates medical information data S, which will be divided into m segments. Through the message I, each piece of data uses the symmetric encryption key K_{MN,TP_i} to perform symmetric encryption and sent to the specific TP_i. After received message I, TP_i will use the public key of the SN to asymmetrically encrypt the message J, and message J contains the hash value of the original

data message segment S_i, K_{MN,TP_i} along with the signature values of signing these data. SN decrypts data with its own private key after received message J, meanwhile uses verify signature method in API provided by CA to validate the accuracy of data and credential. By comparing the signature value and the original data in the message J to verify whether the data is accurate and non-repudiation. The hash value of the K_{MN,TP_i} in the message J is compared with those in message H, and if it matches, SN will recognize the data and reorganize the raw data S [7–10].

$$\text{I: } \forall_i \in \{1, m\} \left[S_i, N_{TP_i}\right]_{K_{MN,TP_i}} \tag{9}$$

$$\text{J: } \forall_i \in \{1, m\} \left[S_i, Hash\left(K_{MN,TP_i}\right), N_{MN}, N_{SN}, Sign_{TP_i}\right]_{K_{SN}} \tag{10}$$

Phase 5 (Termination phase):

SN informs the MN that the data has been received by the message K to terminate a complete data exchange process.

$$\text{K: } \left[Terminate\left(N_{MN}\right)\right]_S \tag{11}$$

3 Scheme Energy Analysis

This chapter is about energy feasibility on integrating PKI system into the data transmission. As the wireless acquisition equipment are mostly self-powered rechargeable equipment, so we must calculate the overall energy consumption.

3.1 Energy Estimation Model

In [11], the author proposed an energy consumption model for wireless sensor nodes (WSN) in data transmission. By introducing this model into the network model proposed in previous chapter, to estimate sending, receiving and listening energy consumption. The energy consumption values of Elliptic Curve Cryptography (ECC) elliptical algorithm was given [11], along with the energy consumption of ECDSA (ECC-DSA)

Table 2. Energy estimation model variables in the scheme

Message operation	Cost
Transmit 1 bit	0.72 μJ
Receive 1 bit	0.81 μJ
Listen for 1 ms	0.29 μJ
AES-128 encryption	28.11 μJ
SHA-1 128 bits MAC	23.9 μJ
ECC-160 encryption	17 mJ
ECDSA-160 signature algorithm	15 mJ

signature algorithm. In [12], the author provided the energy consumption of wireless sensor node equipped with AES encryption algorithm and SHA-1 encryption algorithm. Based on the energy calculations in these two papers. The energy estimations listed in Table 2 will serve as energy models for different data operations in the scheme.

3.2 Energy Detail Estimation

Sending energy consumption: The energy consumption of the transmission is calculated based on the length of the message of the MN and the number of third parties involved in the operation of the data. Table 3 summarizes the effect of the number of third parties on the energy consumption.

Table 3. Table of sending energy consumption using energy estimation model

Number of third parties	Size (bytes)	Energy consumption (μJ)
0	319	1831.68
2	545	3133.44
4	920	5299.34
6	1298	7464.97
8	1673	9630.56
10	2049	11796.45

Receiving energy consumption: Similar to the sending consumption, the receiving energy consumption is affected by the total length of the received message and the number of third parties. Table 4 lists the effect of the number of third parties on the receiving energy consumption.

Table 4. Table of receiving energy consumption using energy estimation model

Number of third parties	Size (bytes)	Energy consumption (μJ)
0	213	1374.4
2	258	1671.76
4	395	2553.34
6	530	3434.5
8	669	4316.67
10	803	5198.89

Listening energy consumption: The length of time that a MN is monitored is equal to the sum of the packet transmission delay (Δ), packet calculation time ($Comp$) transmission delay (T) and the reception delay (R). It is estimated that the packet transmission delay between different entities is 150 ms, and third parties and the server node have sufficient computational power and do not need to concern too much about energy efficiency. The transmission delay is calculated as follows:

$$T_{Listening} = \Delta(MN \rightarrow SN) + R(SN) + Comp(SN) + T(SN) + \Delta(SN \rightarrow MN) \quad (12)$$

Where: $\Delta(MN \rightarrow SN)$ denotes packets propagation delay from MN to SN; $R(SN)$ denotes Reception latency of SN; $Comp(SN)$ denotes Computational time of SN; $T(SN)$ denotes Transmission latency of SN; $\Delta(SN \rightarrow MN)$ denotes Packets propagation delay from SN to MN. The energy consumption monitored by the number of third-party impact is given in Table 5.

Table 5. Table of listening energy consumption using energy estimation model

Number of third parties	Listening time (ms)	Energy consumption (μJ)
0	942.27	273.12
2	2408.34	698.43
4	4215.36	1222.44
6	6023.25	1746.95
8	7830.79	2270.45
10	9637.56	2794.82

Encryption energy consumption: Encryption energy consumption is estimated by calculating the total length of the message that needs to be encrypted by the MN node, then applying the energy model to estimate the energy consumption generated by symmetric encryption and asymmetric encryption operations. It changes accordingly to the increase in the number of third parties. The asymmetric encryption algorithms adopted in China are SM series algorithms (SM2, SM3). These algorithms are improved and strengthened compared to the original ECC algorithm, but the energy consumption of this algorithm is basically similar [13] (Table 6).

Table 6. Table of encryption energy consumption using energy estimation model

Number of third parties	Size (bytes)	Energy consumption (μJ)
0	35	34000
2	132	231.56
4	264	456.87
6	388	681.45
8	517	906.53
10	640	1131.56

3.3 Scheme Energy Analysis

The scheme estimated overall sending, receiving and listening energy consumption as communication cost, and overall encryption energy consumption as computational cost, the final estimation is given in Fig. 3.

When estimating the energy consumption of communication, if there is no third party, the energy consumption on MN will be quite tremendous. Symmetric encryption and asymmetric encryption are completed in the wireless device in this case. It is technically difficult to achieve, it has certain requirements for the hardware and software conditions of the wireless devices. There must be at least one third party involved in the application to ensure that the wireless device has the highest energy efficiency. We also

find out that the energy consumption value is within reasonable range in the case where third parties are limited in number and the non-symmetric encryption operation is completed by the third party, and the feasibility of the system is verified.

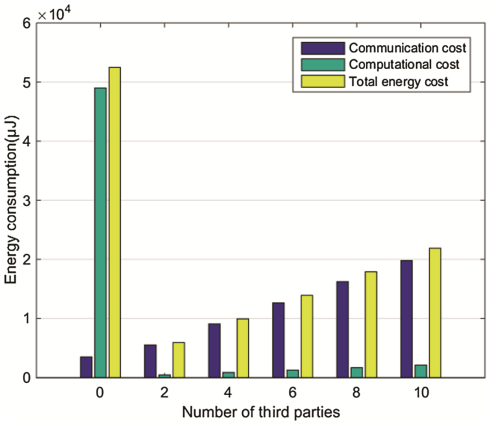

Fig. 3. Final energy consumption estimation summary

4 Conclusion and Further Work

This paper provides a feasible solution, detailed description and scheme feasibility verification of a data exchange scheme based on PKI system, with wireless intelligent medical equipment as message source. Set message nodes sending data to third party medical information system secured and unabridged as goal. Introducing PKI system into E-health applications in the context of IoT, meanwhile verified the feasibility of the system through the estimation of the energy consumption required by wireless message nodes. We have not researched on the efficiency of data transmission and the choice of data transmission channel, which will be consummated in the trailing research.

References

1. Lin, J.W.: Recent advances in PKI technologies. J. Cryptol. Res. **27**(1), 487–496 (2015)
2. Mullgan, G.: The internet of things: here now and coming soon. IEEE Internet Comput. **14**, 35–36 (2010)
3. Zen, H., Jiang, X.H., Sun, Y.F.: Research on a PKI-based IoT security model. Comput. Appl. Softw. **6**, 271–274 (2013)
4. Chowdhury, A.R., Baras, J.S.: A lightweight certificate-based source authentication protocol for group communications in hybrid wireless. In: IEEE GLOBECOM, pp. 56–59 (2008)
5. Qian, Z.H., Wang, Y.J.: Internet of things-oriented wireless sensor networks review. J. Electron. Inf. Technol. **1**, 215–227 (2013)
6. Abdmeziem, M., Tandjaoui, D.: Tailoring mikey-ticket to e-health applications in the context of internet of things. In: International Conference on Advanced Networking, Distributed Systems and Applications (Short Papers), pp. 72–74 (2013)

7. Millán, G.L., Pérez, M.G., Pérez, G.M., Skarmeta, A.F.G.: PKI-based trust management in inter-domain scenarios. Comput. Secur. **29**(2), 278–290 (2010)
8. Ning, J., Zhao, Y., Zhuang, L., Li, Y.: Design and implementation of removable storage device end-to-end encrypt system. Comput. Eng. Des. **34**(1), 1–7 (2013)
9. Braun, J., Volk, F., Classen, J.: CA trust management for the Web PKI. J. Comput. Secur. **22**(6), 913–959 (2014)
10. Delignat, L.A., Abadi, M., Birrell, A.: Web PKI: closing the gap between guidelines and practices. In: ISOC Network and Distributed System Security Symposium—NDSS (2014)
11. Meulenaer, G.D., Gosset, F., Standaert, F., Pereira, O.: On the energy cost of communication and cryptography in wireless sensor networks. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communication, pp. 580–587 (2008)
12. Kaps, J.-P., Sunar, B.: Energy comparison of AES and SHA-1 for ubiquitous computing. In: Zhou, X., Sokolsky, O., Yan, L., Jung, E.-S., Shao, Z., Mu, Y., Lee, D.C., Kim, D.Y., Jeong, Y.-S., Xu, C.-Z. (eds.) EUC 2006. LNCS, vol. 4097, pp. 372–381. Springer, Heidelberg (2006). https://doi.org/10.1007/11807964_38
13. Sun, R.Y., Cai, C.S., Zhou, Z., Zhao, Y.J., Yang, J.M.: The comparision between digital signature based on SM2 and ECDSA. Netw. Secur. **2**, 60–62 (2013)