A Secure Privacy Data Transmission Method for Medical Internet of Things

Heping Ye, Jie Yang, Junru Zhu, Ziyang Zhang, Yakun Huang, and Fulong Chen(✉)

Department of Computer Science and Technology, Anhui Normal University, 189 Jiuhua South Road, Wuhu 241002, Anhui Province, People's Republic of China
long005@mail.ahnu.edu.cn

Abstract. With the improvement of people's living level and the rapid development of information, people put forward higher requirements for medical standard. Effective combination between traditional medical system and modern communication technologies promotes the medical level more intelligent. The medical system involves a large number of data, which contains all kinds of information. Therefore, the patient's information is facing the risk of data leakage and privacy information destruction in the transmission process. In order to effectively protect the patient's privacy information, this paper presents a secure data transmission method for privacy data of Medical Internet of Things in three aspects: the transmission model of medical data, the registration authentication and key agreement between the Gateway-node and the Server, and Multi-path transmission mechanism. The theoretical analysis shows that the transmission model could effectively ensure the security of the patient's privacy information.

Keywords: Medical Internet of Things · Privacy data · Transmission method

1 Introduction

The rapid economic development has led to the deterioration of the natural environment upon which the survival of people's health under unprecedented threat. Various non-predictability of diseases have sprung up on the patients so that the patient's illness makes it painful bring the demand for medical services growing. However limited traditional medical service resources and uncertainty treatment time urge people to begin to look for better health service to make up for the lacking of available resources. In [1], a cardiac function in real-time monitoring system that can measure heart rate and other vital signs data, then serving data to the medical center for treatment via Bluetooth communications or wireless networking technologies. Zhang mentions that obtaining data by remote sleeping monitoring could effectively help doctors diagnose disease, and adjust the pillow without affecting the premise of sleep to let patient get the timely healthcare [2].

J. Wan et al. (Eds.): Industrial IoT 2016, LNICST 173, pp. 144–154, 2016.
DOI: 10.1007/978-3-319-44350-8_15

Mni proposes that today's medical development should take a new information technology way while cleverly epitomizing the medical things meaning. He points out the key technologies in the medical field, analyzes and presents various models about medical data from generation to storage [3].

Due to the huge amount of medical data, extensive medical data sources, and various identification information which involve user privacy, once medical data loses or tampers, leakage will occur. [4,5] have presented that tags will be scanned while users are not aware of what readers do, it will easily result in the destruction of personal privacy, and it will cause the items of information suffering from attacking between Local Servers and Remote Servers. Therefore, we propose a secure privacy data transmission method for Medical Internet of Things.

2 Related Works

Facing with the large number of heterogeneous data in Medical Internet of Things, the problem is how to ensure the security of such data in the remote transmission. It has been always the focus of academic research. Ning [6] considers a variety of secure factors of Internet of Things, and composes that compromise must be existed between privacy strength and specific business needs. Namely, it needs us to custom privacy policy moderately on the basis of business needs as much as possible to protect users' privacy.

Wu introduces that the data protection methods [7] using lightweight cryptographic algorithms in most Internet of Things applications. Du [8] proposes a probabilistic key sharing scheme suitable for WSNS to share. The same communication key exists between any two nodes is p and security is not guaranteed. Song studies the secure and reliable transmission scheme SPS based on Internet of Things [9]. He presents a cooperative transmission mechanism and the rate selection algorithm based on the channel state in order to transmit data effectively and reliably. [10] Lamport first proposes safe way Hash function Encryption users.

Kothmayr proposes an end-and-end mutual authentication mechanism of Internet of Things based on DTLS protocol. The mechanism is based on the existing Public-key encryption algorithm, which is vulnerable to suffer from middle attack because of no three session process [11]. Groce [12] introduces a provably secure PAKE protocol standard model, but there is no trusted third party so as to result in non-universal about the presented protocol. In [13,14], Bi-directional authentication among nodes is presented. Peyravian mentions an authentication scheme based on Hash function [15]. Ma proposes a point-to-point authentication and secure transmission protocol [16] based on Hash functions and block cipher. A secure transmission method which is fit on the Internet of Things has been mentioned in [17]. The trusted third party is adopted while two parties are authenticating, therefore the scheme is not universal in terms of the complex web environment. In secure transmission model of Internet of Things, there is a common problem in the application, and there involves a variety of mixed-format electronic medical records and other patient data in Medical Internet of Things.

However, methods which we have discussed above cannot fit the field. When data is transferred, data attacking and data leaking leads our privacy information to be illegally obtained.

The rest of the paper is organized as follows. Section 2 describes the scheme model of the primary care. Section 3 provides our transmission protection scheme. Section 4 presents the results of our theoretical analysis. The last section concludes the paper and lays out future research directions.

3 Scheme Model in Primary Care

The Medical Internet of Things scheme is achieved in the community. Primary Care Architecture that describes the medical data sources and data transmission is presented in Fig. 1, and the slice model of medical data transmission that describes the transfer process of slicing data is showed in Fig. 2.

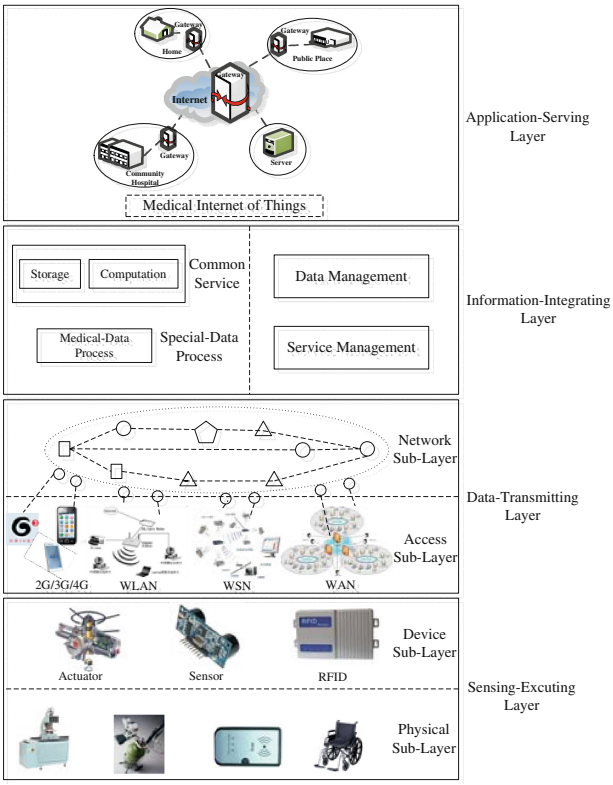

Fig. 1. Primary Care Architecture.

3.1 Primary Care Architecture

As we can see in Fig. 1, it describes an architecture of Primary Care. Data transmission integrates a variety of communication means. Sensors establish communication via Wireless self-organized network, and data in the gateway transmit through Wireless Local Area Network or mobile network.

Data from a sensor is sent toward the nearest gateway, and then the data is transmitted to the final community gateway. Connection is built between the community gateway and the database server through wireless network. In the end, the application database server provides the resolved data to users.

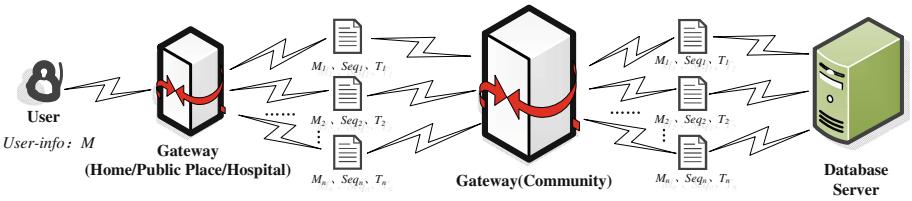

Fig. 2. Medical Data Multi-path Transmission Model.

3.2 Medical Data Multi-path Transmission Model

Medical data multi-path transmission model is painted in Fig. 2. We assume that the user's information is M, and the number of paths is n. Data is divided into n divisions when data arrives in the gateway. Each division which contains certain user information is transmitted to the database server.

4 Transmission Protection Scheme

4.1 Scheme Initialization

There needs to be an authentication with each other before the interaction between the Gateway-node and the Server. On the basis of the previous study about authentication protocol, a new Bi-directional password authentication method is showed as follows.

Gateway Node Registration

When G registers at S, G delivers the hash value of password PW_G to S, then S contrasts the hash value of password to dictionary to authenticate. Many Gateway-nodes' passwords constitute a password table. S generates a symmetric key K_{S-G}, and secretly informs G. Ultimately, both securely store K_{S-G} (Table 1).

Bi-directional Authentication Process

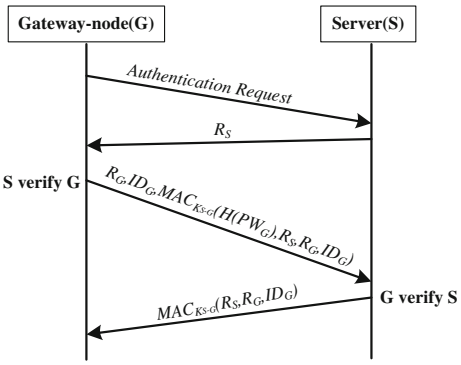

Fig. 3. Authentication Process.

Table 1. The Initial Conditions and Symbols

Number	Symbol	Definition
1	S	Server
2	G	Gateway-node
3	ID_G	Gateway-node Identification
4	PW_G	Gateway-node Password
5	$H(x)$	Strongly Non-collision Hash Function
6	R_G, R_S	Random number of Gateway-node and Server
7	K_{S-G}	Symmetric key for Gateway-node and Server
8	$MAC_{K_{S-G}}(M)$	The MAC value of M in the key K_{S-G}

4.2 Key-Agreement Mechanism

After completing Bi-directional authentication between G and S, they need to generate a shared key. Key generation and distribution process are elaborated as follows.

Step 1: A large prime number P is selected from G and S, and G is selected as a generator for the multiplicative group Z_P^*;

Step 2: G chooses a secret integer x:

$$1 \leq x \leq P - 2 \tag{1}$$

calculates $X = g^x mod\ P$, and sends X to S;

Step 3: S selects a secret integer y:

$$1 \leq y \leq P - 2 \tag{2}$$

calculates $Y = g^y mod\ P$, and sends Y to G;

Step 4: G calculates $K_G = Y^x mod\ P$, generates random number N_G, and sends $\{E_{K_G}(N_G), N_G\}$ to S;

Step 5: S calculates $K_S = X^y mod\ P, E_{K_G}(N_G)$ and generates N_S, and then sends $\{E_{K_S}(N_S), N_G, N_S\}$ to G;

Step 6: G receives and decrypts $\{E_{K_S}(N_S), N_G, N_S\}$, and then returns True to S, the two parties share the same key K_{S-G}, which is used to complete the key sharing.

4.3 Fragmented Multi-path Data Transmission

According to the mentioned above, G and S have accomplished Bi-directional authentication, and commonly share session key. To ensure the security of the data transmission process, G encrypts data by a shared key before data transmitting, and divides cipher-text into fragment to transfer. Multi-path data encryption and cipher-text transmission are described as follows.

Step 1: G uses the key K_{S-G} to encrypt the transmission data. Assuming that the data packet to be transmitted is M, the cipher-text is $C = E_{K_{S-G}}(M)$;

Step 2: C is divided into sub data packets $C_1, C_2, ..., C_n$. For every one of the sub data packets, we add a session number *seq*, sub-packet identification i and time stamp T_i to them,

$$m_i : \{C_i, s, i, T_i\}(1 \leq i \leq n); \tag{3}$$

Among them, the session number *seq* and sub packet identification i are used to be prevent replay attacking. $\{H_{K_{S-G}}(C_i, s, i, T_i)\}$ is calculated by *H(x)*, which is used to verify the message for receiver, and the message is transmitted on the each selected path.

$$S_i\{C_i, s, i, T_i, H_{K_{S-G}}(C_i, s, i, T_i)\}; \tag{4}$$

Step 3: Every packet of data received, S will authenticate the message according to the authentication code;

Step 4: When the server receives all of sub data packets which are sent from G, S will reorganize and decrypt the sub data packets to recover data packet M according to the sub-packet identification if the authentication is passed.

5 Security Analysis

5.1 Authentication

G has an authentication with S before data transmitting. If the two parties are not entirely passed the certification, S refuses to receive data in case of leaking

Table 2. Authentication security analysis

Scheme / Security condition	*Hwang*[13]	*Peyravian*[14]	*Wang*[15]	*Ma*[16]	*This paper*
Prevent DoS attacking	-	Yes	-	Yes	Yes
Prevent replay attacking	-	Yes	Yes	Yes	Yes
Prevent dictionary attacking	Yes	Yes	Yes	-	Yes
Prevent Server forging	Yes	Yes	Yes	Yes	Yes
Prevent Gateway-node forging	Yes	-	Yes	Yes	Yes
No public key mechanism	Yes	Yes	-	Yes	Yes
Hash function	Yes	Yes	Yes	Yes	Yes
MAC function	-	-	-	Yes	Yes

data to fake nodes. Even if attackers steal the password table of S, they cannot crack the password because of the unidirectional characteristic of Hash function. Therefore, it can effectively ensure the identity authentication for S and G.

As shown in Table 2 where "Yes" represents that the security condition is met, from the implementation process, the above protocol takes advantage of Hash function and MAC to become more efficient than Wang's public key algorithm. MAC function is not referred in Peyravian's research, therefore Peyravian's protocol cannot prevent Gateway forging. MA's protocol cannot prevent dictionary attacking due to the data characteristic despite of various means of attacking.

5.2 Key Agreement

In order to prevent the attacker from forging new data to result in inconsistence while the two parties are exchanging information, here, we bring three-way handshake during the session so as to ensure the correctness of the final key-agreement. In Table 3, "Yes" represents that the security condition is met.

Table 3. Key-agreement security analysis

Scheme / Security condition	*Diffie-Hellman*	*Xie*[17]	*This paper*
Prevent replay attacking	Yes	Yes	Yes
Forward security	Yes	Yes	Yes
Integrity attacking	Yes	Yes	Yes
Known key security	Yes	Yes	Yes
Prevent wiretap attacking	Yes	Yes	Yes
Prevent MITM attacking	-	Yes	Yes
Three-way handshake	-	-	Yes

6 Experimental Results

According to the security analysis, data packet will be transmitted to the Gateway Node after authenticating between Server and Gateway. Assuming that the probability of data stolen in single-path is $P(0 < P < 1)$, the probability in multi-path is $P^n(n$ presents the number of paths). Again, we assume that P is 0.7, and then the maximum number of paths is 20, simulated by Matlab as shown in Figs. 4 and 5.

Assuming that the length of the communication link from terminal node to the server is L, and k nodes will be attacked by k attackers, then we conclude that the probability of effective node is $P = 1 - k/L$.

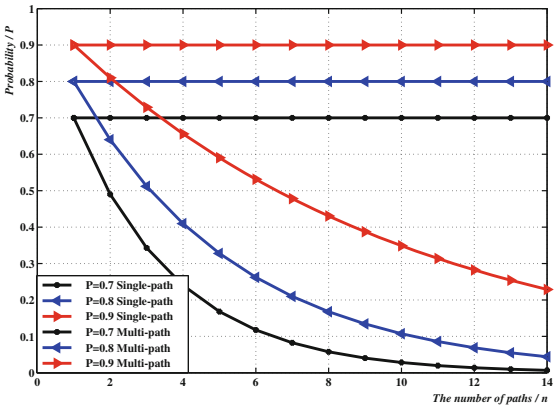

Fig. 4. Packet loss rate.

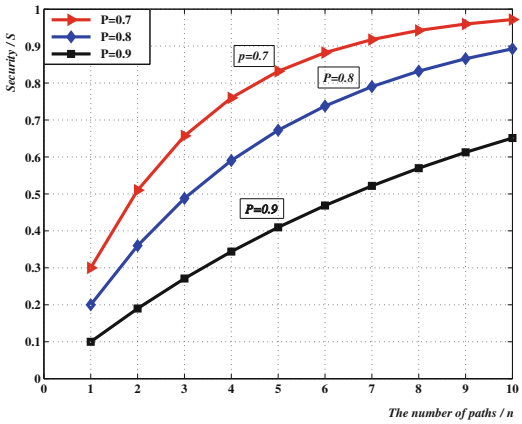

Fig. 5. Security of Communication Link.

Another assumption is that terminal node, server locates in the position 0 and $L+1$, and the reliability of security is R.

$$A(1 \leq x \leq L-k) \tag{5}$$

represents that the node in the communication link is attacked by the first attacker. A' indicates that the first node which is attacked by the x_{th} node or the former node. $P(x)$ expresses that the node which is attacked locates at the x_{th} node in the communication link. G indicates that the identity of sender is guessed correctly by the first attacker and $P(G \mid A'_G)$ expresses the probability of attacking correctly.

According to the assumption above, the probability of the first node which is attacked by attacker locates at the x_{th} node in the communication link is $P(A_x) = P^{(x-1)}(1-P)$. The probability of the first node which is attacked by attacker is in the position of first node or the latter node is

$$(1-P)\sum_{i=1}^{L-k} P^{i-1} = 1 - P^{L-k} \tag{6}$$

Therefore we can conclude the probability of $P(G \mid A'_i)$ is

$$\frac{1-P}{1-(P^{L-k})} = \frac{1-P}{1-(P^{L-P})}, \tag{7}$$

We also assume that

$$LA_x(k \leq x \leq L) \tag{8}$$

represents that the last node which is attacked locates at the node in the communication link. LA'_x indicates that the first node which is attacked by the x_{th} node or the latter node. $P_{l(x)}$ expresses that the last node which is attacked locates at the x_{th} node in the communication link. G_l indicates that the identity of receiver is guessed correctly by the last attacker and $P_l(G \mid A'_G)$ expresses the probability of attacking correctly. According to the assumption above, the probability of the last node which is attacked by attacker locates at the x_{th} node in the communication link is $P(A_x) = (1-P)P^{L-x}$. The probability of the last node which is attacked by attacker is in the position of n_{th} node or the latter node is

$$P(A_n^i) = (1-P)\sum_{j=k}^{L} P^{L-j} \tag{9}$$

So we can also conclude the probability of $P(G_l \mid A'_n)$ is

$$\frac{1-P}{1-P^{L-k+1}} = \frac{1-P}{1-P^{L\times P+1}} \tag{10}$$

To sum up from formulas (7) and (10), we can come to a decision that the reliability is

$$R = P(G \mid A'_i) \times P(G_l \mid M'_n) = \frac{(1-P)^2}{(1-P^{L\times P}) \times (1-P^{L\times P+1})} \tag{11}$$

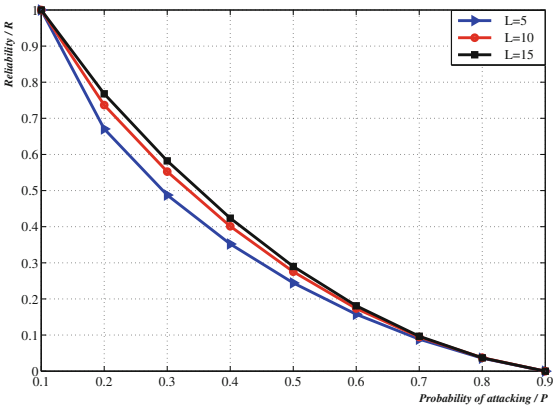

Fig. 6. The tendency of the reliability of communication link.

In order to reflect more directly the influence of the reliability about data transmitting with the impact of the length of the communication link and the probability of the node which is attacked, we have a simulation as shown in Fig. 6.

7 Conclusion

This paper takes the Medical Internet of Things as a standpoint, and aims at the security of data transmission. Then we summarize upon three aspects, authentication, communication key agreement and Multi-path security transmission. Considering of the security problems that might exist in the communication process, we improve the traditional key agreement algorithm to enhance the key negotiation security. Furthermore, we increase the multi-path transmission mechanism to become more difficult for attacker to obtain complete data without affecting Server data receiving. Finally, we analysis the security about the method inferred to the full text.

In a word, the security issue in Medical Internet of Things we discussed here is a part of the whole. And the protection of medical data storage, medical data privacy protection and other issues are also the research focus problems. The next step about our work is to explore and research for the protection of medical data storage.

Acknowledgements. The authors would like to thank our colleagues and students in Engineering Technology Research Center of Network and Information Security at Anhui Normal University, in particular, Yonglong Luo, Xuemei Qi and Yunxiang Sun. We thank National Natural Science Foundation of China under Grant No. 61572036, University Natural Science Research Project of Anhui Province under Grant No. KJ2014A084, Wuhu City Science and Technology Project under Grant No. 2014cxy04, and Anhui Normal University Postdoctoral Project under Grant No. 161-071214 for support of this research.

References

1. Gao, M., Zhang, Q., Ni, L., et al.: Cardiosentinal: a 24-hour heart care and monitoring system. J. Comput. Sci. Eng. **6**(1), 67–78 (2012)
2. Zhang, J., Chen, D., Zhao, J., et al.: RASS: a portable real-time automatic sleep scoring system. In: 2013 IEEE 34th Real-Time Systems Symposium (2012)
3. Mni, L., Zhang, Q., Tan, H.Y., et al.: Smart healthcare: from IoT to cloud computing. Scientia Sinica **43**(4), 515–528 (2013)
4. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
5. Medaglia, C.M., Serbanati, A.: An overview of privacy and security issues in the internet of things. In: Internet of Things, pp. 389–395 (2009)
6. Ning, H.S., Xu, Q.Y.: Research on global internet of things developments and its lonstruction in China. Acta Electronica sinica **38**(11), 2590–2599 (2010)
7. Wu, Z.Q., Zhou, Y.W., Ma, J.F.: A secure transmission model for internet of things. Chin. J. Comput. **34**(8), 1351–1364 (2011)
8. Du, W., Deng, J., Han, Y.S.: A pairwise key pre-distribution scheme for wireless sensor networks. In: CCS 2003 Proceedings of the 10th ACM Conference on Computer and Communications Security, vol. 8, issue: 2, pp. 42–51 (2003)
9. Song, Z., Zhang, Y., Wu, C.: A reliable transmission scheme for security and protection system based on Internet of Things. In: International Conference on Communication Technology & Application IET Digital Library (2011)
10. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24**(11), 770–772 (1981)
11. Kothmayr, T., Schmitt, C., Hu, W., et al.: A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. In: IEEE Conference on Local Computer Networks Workshops, vol. 90, issue: 1, pp. 956–963 (2012)
12. Groce, A., Katz, J.: A new framework for efficient password-based authenticated key exchange. In: Proceedings of the 17th ACM Conference on Computer and Communications Security ACM (2010)
13. Hwang, J., Yeh, T.: Improvement on Peyravian-Zunics password authentication schemes. IEICE Trans. Commun. **85**(4), 823–825 (2002)
14. Wang, B., Zhang, H., Wang, Z., et al.: A secure mutual password authentication scheme with user anonymity. Geomatics Inf. Sci. Wuhan Univ. **33**(10), 1073–1075 (2008)
15. Peyravian, M., Jeffries, C.: Secure remote user access over insecure networks. Comput. Commun. **29**(5), 660–667 (2006)
16. Ma, W.J.: Research and Application on Security Authentication Technologies in Internet of Things. Shandong University (2011)
17. Xie, W.J.: A Secure Communication Scheme based on Multipath Transportation for the Internet of Things. South China University of Technology (2013)