Research Journal of Medical Sciences 1 (4): 191-194, 2007
ISSN: 1815-9346

Ubiquitous Healthcare over the World Wide Web

[1]Kuo-Ching Liu and [2]Hui-Feng Huang
[1]School of Medical Laboratory Science and Biotechnology,
China Medical University, Taichung 404, Taiwan, R.O.C.
[2]Department of Information Management,
National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.

Abstract: Ubiquitous Healthcare is essential not only for providing efficient medical care but also in saving medical expenses. Currently, sensor networks are widely used for applications such as environmental monitoring, airport safety, healthcare, etc. In healthcare situations, sensor nodes can be deployed to remotely monitor and assist disabled patients. Also a concern is the protection of privacy with electronic communication of patient data. However, the sensor networks are easily compromised if an attacker sends forged or modified messages. If a medical unit receives false messages and all efforts of the working staff are implemented under false pretenses, the loss of resources and manpower would be great. Therefore, the receiver (medical unit) has to authenticate messages transmitted from the sensor nodes (monitored patients) over the wireless sensor network. To provide the quality and security of the growing healthcare, it is necessary to reduce the computation load for both parties of the medical unit and the monitored patient. In this study, we will present a new security and privacy of authentication so that ubiquitous healthcare is possible through the sensor network.

Key words: Healthcare, medical, security, privacy, authentication, sensor network

INTRODUCTION

Due to the development of low-cost wireless sensor network technology which allows the biologists to remotely supervise and control life cycles of plants and animals, it is possible to apply similar technology to human lifestyle (Akyildiz *et al*., 2002; Sara *et al*., 2005; Shaojun and Xu, 2002; Velasco *et al*., 2003). With modern advance these techniques now gradually become possible by way of the development of the biosensor (Sara *et al*., 2005; Shaojun and Xu, 2002; Velasco *et al*., 2003). The fusion of these technologies makes remote patient care possible. Therefore, the inevitable prerequisite for high quality and ubiquitous healthcare is becoming more and more important. A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon (patient) or very close to it (Akyildiz *et al*., 2002; Sara *et al*., 2005; Shaojun and Xu, 2002; Velasco *et al*., 2003). These tiny sensor nodes consist of sending, data processing and communication components (Akyildiz *et al*., 2002; Chang *et al*., 2005). They use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrains or disaster relief operations. Therefore, the sensor networks are expected to lead to a wide range of applications. Some of the application areas are health care, military activities, environmental monitoring and home securities.

Consider the overwhelming task of health care for a densely populated city or even a remote community of people who live a long distance from a well equipped hospital. The wireless sensor networks open new possibilities for ubiquitous healthcare. For instance, medical staff could use the wireless sensor network to receive health records or emergency information from suburbia or a disaster area. Thus, medical staff could more accurately and immediately deliver high quality and efficient care for the monitored patient. In addition, the security and privacy protection of medical information for the patient is a very important concern in the electronic transactions (Liu *et al*., 2001; Meyer *et al*., 1998; Safran and Goldberg, 2000; Yang *et al*., 2006). Due to the property of sensor devices, the sensor networks may easily be compromised by attackers who send forged or modified messages. The sensor networks are easy targets and misleading or unverified messages can begin a wild

Corresponding Author: Hui-Feng Huang, Department of Information Management, National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.

goose chase. For example, if a medical unit (or observation unit) receives a forged message and all efforts of the working staff are implemented under false pretenses, the loss of resources and manpower would be wasteful and frustrating. To prevent information and communication systems from illegal delivery and modification, message authentication needs to be examined through certificated mechanisms. Therefore, when a monitored patient requests to use a medical service, he needs to be authenticated first before receiving the service from the medical unit (or physician). Similarly, the monitored patient also has to verify the identity of the medical unit (or physician). For example, if the patient does not verify the identity of the medical unit, an attacker can forge the identity of the physician to obtain confidential patient information. To provide quality and security in growing healthcare services, it is necessary to reduce the computation load for both parties of the medical unit and the sensor node (monitored patient). However, most previous schemes proposed for the security of distributed sensor networks have used asymmetric cryptography such as Diffie-Hellman key agreement or RSA signatures schemes (Rivest *et al*., 1978; Diffe and Hellman, 1976). These traditional message authenticated encryption schemes require a great of computation time. They are often not suitable for sensor networks due to limited computation, energy resources of sensor nodes and network dynamics, etc (Akyildiz *et al*., 2002; Chan *et al*., 2003; Chang *et al*., 2005; Liu *et al*., 2001; Liu and Ning, 2003).

In this study, we will present a new security and privacy protection protocol for healthcare which could significantly reduce time overhead by avoiding modular exponentiation and inverse computations. This authenticated encryption protocol allows the verifier to recover and verify the message simultaneously. Our scheme could provide low-computation costs for both the receiver and monitored sensor node, especially for the monitored sensor node. Therefore, the receiver (physician or medical unit) can provide more efficient and safer healthcare services to a monitored patient. In addition, both the receiver (physician or medical unit) and the monitored sensor (patient) only keep their private information in storage. It is adoptable for the sensor nodes that are limited in power, computational capacities and memory. Hence, the proposed protocol could possibly provide security and privacy protection of the patient for ubiquitous healthcare in the 21st century over sensor networks.

The proposed scheme: In this study, we will develop a low-computation authenticated encryption procedure for security and privacy protection of ubiquitous healthcare over sensor networks. Assume that two communication parties are the monitored sensor and the receiver. In some application areas, the monitored sensor could be those sensors deployed to monitor patients, biology experiments, etc.; and the receiver could be a physician, healthcare provider, biologist, environmentalist, etc. (Akyildiz *et al*., 2002; Sara *et al*., 2005; Shaojun and Xu, 2002; Velasco *et al*., 2003).We now explain the proposed method. The receiver or the physician selects a secret key x and computes $k_i = f(I_i \oplus x)$ for each monitored sensor i, where I_i is the identity number of the monitored sensor i, f( ) is a one-way hash function and⊕ signifies the XOR operation. Then, the receiver distributes the private information K_i to each monitored sensor (patient) i during the initialization phase. When the monitored sensor (patient) i wants to deliver a message (signal) m to the receiver (physician), the procedure of our authenticated encryption processes for the receiver (physician) and any monitored sensor (patient) i are described as follows.

Step 1: Monitored sensor (patient) i → receiver (physician) side:

The monitored sensor I randomly selects an integer $a_i$and computes $z = (a_1 + k_i) \oplus (a_1 + m)$ and $s = f(k_i \| (m \oplus a_1))$, then sends a_1,z, s and the identity number I_i to the receiver, where‖ signifies the connection.

Step 2: Authentication and message recovery: After receiving a_1,z, s and I_i from the monitored sensor i, the receiver computes $K_i = f(I_i \oplus x)$ and recovers m by computing $m = (z \oplus (a_i \oplus k_i)$, where x is a secret key of the receiver (physician). To make sure the message (signal) m was sent from the monitored sensor i, the receiver checks if $k(k_i \| (m \oplus a_i))$. If it is satisfied, the receiver (physician) confirms that the message m was really sent by the monitored sensor (patient) i. In this situation, the receiver could make a decision about the monitored sensor (patient) I. On the other hand, the receiver computes $t = f(k_i \| \alpha_i \| m)$ and send *t* to the monitored sensor (patient) i.

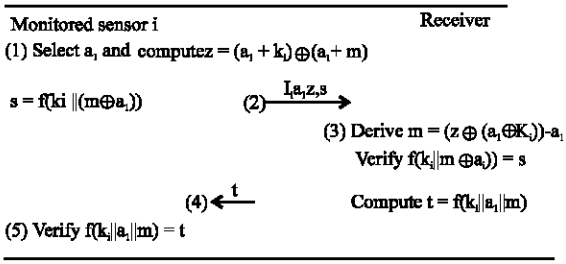

Fig. 1: The proposed scheme

Step 3: After receiving *t*, the monitored sensor *i* computes $f(k_i||a_i||m)$ and checks if $f(k_i||a_i||m)$ holds. If it holds, the monitored sensor i authenticates the receiver (physician). In this protocol, the integer a_i is used one time. It could preserve the replay attack. The above processes are briefly illustrated in Fig. 1.

DISCUSSION

In this study, are going to explore the securities and the performances of our protocol.

Security analysis: The security of the presented scheme is based on the one-way hash function f ( ) and the XOR operation. In the proposed method, $k_i = f(I_i \oplus x)$ is the private information of the monitored sensor (patient)i and I_i is the identity number of the monitored sensor (patient) i. With the secret key $k_i = f(I_i \oplus x)$, it does not help for the monitored sensor i to obtain the receiver's (physician) secret key *x* because it is protected by the one-way hash function f(). Without the receiver's secret key x, no one can easily obtain another secret key K_j of the monitored sensor (patient) j, where $k_i = f(I_i \oplus x)$. Moreover, the presented scheme can withstand the following three attacks.

Replay attack: In our protocol, the integer$_{\bullet}$ is used one time. Then, an adversary cannot send the information a_i, z and s to the receiver (physician) again. Without knowing K_i, the adversary cannot easily derive other z′and s′by computing $z' = (a_i + k_i) \oplus (a_1 + m)$ and $s' = f(k_i||(m \oplus a'_1))$ for some selected number a'_1 and message m. Therefore, the proposed scheme can withstand the replay attack.

Masquerade attack: With a_i, $z = (a_1, k_i) \oplus (a_1 = m)$, $s = f(k_i||(m \oplus a_1))$ and $t = f(k_i||a_1||m)$ is steps 1 and 2, it is very hard for the adversary to derive k_i and message m from z, s and t. Since they are protected under the one-way hash function f( ). Hence, the adversary is unable to masquerade as the monitored sensor (patient) i or the receiver (physician). Therefore, the proposed scheme can withstand the masquerade attack.

Guessing attack: Supposing that an adversary obtains the information a_i, $z = (a_1, z) = (a_1 = k_i) \oplus (a_1 + m)$, $s = f(k_i||(m \oplus a_1))$ and $t = f(k_i||a_1||m)$ and from steps 1 and 2. To implement the secret guessing attack, an adversary must first guess the secret information k'_i to be k_i and m′ to be m, before he can try to compute $z' = (a1 = k'_i) \oplus (a_1 + m')$, $s' = f(k'_i||(m' \oplus a_1))$ and $t' = f(k'_i||a_1||m')$. If $z = z'$, $s = s'$ and, $t = t'$ then the adversary can guess the correct secret information k_i and m. In this situation, he could retrieve the correct message m. However, he would have to do an exhaustive search for guessing the secret information k_i and m. Hence, our scheme can also withstand the secret guessing attack.

Table 1: Computations of the proposed scheme

	The receiver	The monitored sensor
Exponentiation	0	0
One-way hash function	3	2
Exclusive or (XOR)	3	2

Performances: With regards to efficiency, the details of our protocol are described as follows. Note that the time for computing addition and subtraction are ignored, since it is much smaller than multiplication computation and hash function. As shown in Table 1, no modular exponentiation or inverse computations are required for the receiver (physician) or the monitored sensor (patient) to perform. Only three hash functions and three exclusive operations (XOR) are performed by the receiver; alternately, the monitored sensor performs two hash functions and two exclusive operations. It is obvious that the proposed scheme can provide low-computation costs for both the receiver and sensor nodes, especially for a monitored sensor. Because the proposed scheme can provide a fast authenticated encryption algorithm, the receiver (physician or biologist) can provide more efficient and safer healthcare to the monitored sensors (patients or biology). In addition, each monitored sensor i only keeps the private information K_i in its memory. The receiver just stores the secret key x in its storage space. Then, the receiver (physician) can avoid the requirement of maintaining a secure database for those monitored sensor secret keys. It is very suitable for the sensor nodes that are limited in power, computational capacities and memory.

CONCLUSION

Wireless sensor network applied to the monitoring of physical environments have recently emerged as important infrastructure. In this study, we have proposed a new efficient authenticated encryption protocol for the security and privacy of healthcare over sensor networks. Only three hash functions and three exclusive operations are performed by the receiver (physician or medical unit); and just two hash functions and two exclusive operations for the monitored sensor (patient). It can provide low-computation costs for both the receiver and a monitored sensor node, especially for the monitored sensor. Our scheme is reasonably suitable to apply sensor networks to the ubiquitous healthcare in which security and privacy of patient information can be protected.

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasuramaniam and E. Cayirci, 2002. A survey on sensor networks, IEEE. Commun. Mag., 40: 102-114.

Chan, H., A. Perrig and D. Song, 2003. Random key pre-distribution schemes for sensor networks, IEEE. Symposium on Security and Privacy, pp: 197-213.

Chang, W.P., J.C. Sung and Y.Y. Hee, 2005. A novel key pre-distribution scheme with LU matrix for secure wireless sensor networks, Computational Intelligence and Security-International Conference on Computational Intelligence and Security (CIS 2005), Springer-Verlag, Germany, LNAI. 3801, Part I, pp: 494-499.

Liu, C.T., A.G. Long, Y.C. Li, K.C. Tsai and H.S. Kuo, 2001. Sharing patient care records over the Word Wide Web, Int. J. Med. Informatics, 61: 189-205.

Liu, D.and P. Ning, 2003. Establishing pairwise keys in distributed sensor networks', Proc. 10th ACM. Conf. Comput. Commun. Security, pp: 52-61.

Meyer, F.D., P.A. Lundgres, G.D. Moor and T. Fiers, 1998. Determination of user requirements for secure communication of electronic medical record information, Int. J. Med. Informatics, 49: 125-130.

Rivest, R.L., A. Shamir and L.M. Adleman, 1978. A method for obtaining digital signatures and public key cryptosystems, Commun., ACM., 21: 120-126.

Safran, C. and H. Goldberg, 2000. Electronic patient records and the impact of the Internet, Int. J. Med. Informatics, 60: 77-83.

Sara, R.M., A.M. Lopez de, M.P. Marco and B. Damia, 2005. Biosensors for environmental monitoring: A global perspective, Talanta, 65: 291-297.

Shaojun, D. and C. Xu, 2002. New aspects in biosensors, Rev. Molecular Biotechnol., 82: 303-323.

Velasco, G., V.G. Maria N. and M. Toby, 2003. Biosensor Technology addressing agricultural problems, Biosys. Eng., 84: 1-12.

Diffe Whitfield and M. Hellman, 1976. New directions in cryptology, IEEE. Trans. Infom. Theory, 22: 644-654.

Yang, C.M., H.C. Lin, P. Chang and W.S. Jian, 2006. Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA, Computer Methods and Programs in Biomed., 82: 277-282.