Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 462453, 5 pages
http://dx.doi.org/10.1155/2014/462453

Research Article

Privacy Protection for Personal Health Device Communication and Healthcare Building Applications

Soon Seok Kim,[1] Yong Hee Lee,[1] Jong Mo Kim,[1] Deok Seok Seo,[2] Gwang Hee Kim,[3] and Yoon Seok Shin[3]

[1] *Department of Computer Engineering, Halla University, San 66, Heungup-Li, Heungup-myon, Wonju-si, Kangwon-do 220-712, Republic of Korea*
[2] *School of Architecture, Halla University, San 66, Heungup-Li, Heungup-myon, Wonju-si, Kangwon-do 220-712, Republic of Korea*
[3] *Department of Plant and Architectural Engineering, Kyonggi University, 1154-42 Gwanggyosan-Ro, Yeongtong-gu, Suwon-si, Kyonggi-do 443-760, Republic of Korea*

Correspondence should be addressed to Deok Seok Seo; seodk@halla.ac.kr

Received 12 December 2013; Accepted 2 April 2014; Published 1 June 2014

Academic Editor: Jongsung Kim

This paper proposes a new method for protecting patient privacy when communicating with a gateway which collects bioinformation through using personal health devices, a type of biosensor for telemedicine, at home and in other buildings. As the suggested method is designed to conform with ISO/IEEE 11073-20601, which is the international standard, interoperability with various health devices was considered. We believe it will be a highly valuable resource for dealing with basic data because it suggests an additional standard for security with the Continua Health Alliance or related international groups in the future.

1. Introduction

Personal Health Device (PHD) is a term defined by IEEE to mean a health device which is normally used for measurement by a chronic patient, especially seniors, for telemedicine at home and in other buildings. There are several types such as sphygmomanometer, scales, thermometers, or glucose meters. It is a kind of "biosensor." By using these health devices, the measured bioinformation from many patients at home can be collected from smartphones, tablet PCs, or computers, also called gateways. The collected information can be transferred to an emergency medical center in a hospital in an emergency situation or to a personal health management web and is later used as a data source for emergency treatment or health management.

At the end of 2001, ISO (International Standard Organization) and IEEE jointly enacted a standard protocol, ISO/IEEE 11073-20601, in association with PHD communication at home and in buildings and, until now, have been working on revisions [1]. The "communication" in this context indicates an information exchange protocol between several PHDs and gateways.

Information transmitted from communications between individuals is personal bioinformation or medical record information, so a secure exchange of the information must be assumed. The first consideration that must be taken into account is invasion of privacy due to misuse/abuse, forgery/falsification, and hacking of personal health information by an ill-intentioned third party in a transmission process.

However, the ISO/IEEE 11073-20601 standard deals only with mutual communication protocols and frameworks and has never considered security elements until now, regardless of all sorts of security breaches.

There have been various researches into security issues in Personal Health Device communication in the past [2–5]. In 2010, Appari and Johnson [6] explained importance of protecting information in the healthcare environment, and in 2012 Kumer and Lee [7] noted that a strengthened security policy should be considered in the healthcare environment.

In 2012, Kliem et al. [8] proposed architecture for secure communication in a PHD mobile setting. In the same year, Rubio et al. [9] published a paper regarding a strong and simple security expansion for an ECG device.

According to the thesis published by Kune et al. [10], it suggested security requirement on this research and there was research whether it is satisfied or not on security requirement of ISO/IEEE 11073, or current standard protocol.

Research has mainly involved security frameworks, policies, or requirements and it has not provided any specific suggestions until now. Accordingly, this paper will propose new means of privacy protection for a patient who uses their PHD in particular out of other various security issues suggested in [10].

In Section 2 of this paper, we will introduce a communication protocol, as suggested by ISO/IEEE 110730-20601, then propose a new method for patient privacy protection in standard communication protocol suggested in Section 3, and then finally conclude the paper in Section 4.

2. ISO/IEEE 11073-20601 Communication Protocol

This standard is a protocol that defines the mutual exchange of bioinformation between a PHD and a gateway. The protocol consists of two aspects: definitions of an application layer service and protocol for data exchange between a PHD and a gateway. The protocol for data exchange is defined by commands, PHD configuration information, data formats, and whole protocols. An ASN.1 encoding regulation (also known as MDER (Medical Device Encoding Rule)) defined in the standard was used for the exchange of information between the PHD (a weight sensor) and the gateway.

According to the definition by the International Telecommunication Union (ITU), ASN.1 is a protocol defining data exchange on the network and a formal language used to exchange abstract messages between different models. It is simply a language that defines the standard and the data created with ASN.1 becoming the standard. If MDER is expressed in C language, it is as a strict type that sends basic data using a structure called ADPU. In ADPU, there are six message formats: AARQ_apdu, AARE_apdu, RLRQ_apdu, RLRE_apdu, ABRE_apdu, and PRST_apdu. According to the circumstances, communication takes place in 1 out of the 6 messages (refer to Figure 1).

In the meantime, the communication procedure is as follows (refer to Figure 2). From the PHD perspective, first, one's configuration information is sent and the gateway receives this information. The configuration information for the first connection is then saved and in case connection is attempted again, only its system ID is verified, to enable immediate communication.

As seen in Figure 2, there are two types of values. System-id is a value which notifies ID of user as a value in association with privacy protection while dev-config-id has a value which informs the PHD ID, or device. These two types of values correspond with first and second stage, or association request (AARQ_APDU) and association response (AARE_APDU) of the above communication procedure. The data format of AARQ_APDU is composed of the following (refer to Figure 3). As AARE_APDU is a response to AARQ_APDU, the option list from the PHD association information in Figure 3 is excluded and all others are the same. Right here, you can see the problem of the previous standard: two values (system-id and dev-config-id) are directly exposed to the third party. In other words, the privacy of the patient is insecure.

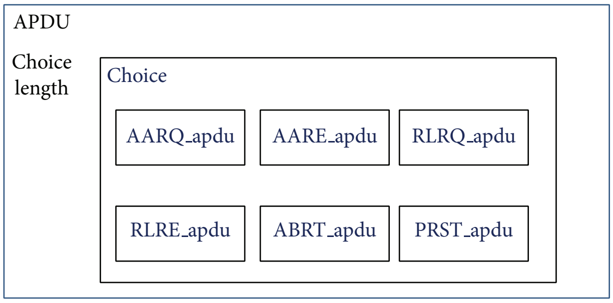

Figure 1: Types of APDU.

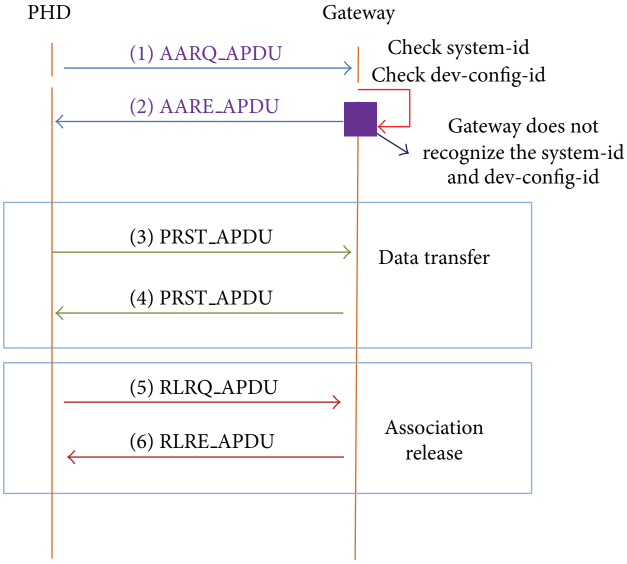

Figure 2: ISO/IEEE 11073-20601 communication procedure.

3. The Proposed Privacy Protection Method

The basic idea in suggesting a method to solve the problem in privacy protection which is referred to in Section 2 is to encrypt information by using block cipher algorithms (e.g., AES, Blowfish, etc.), which is commonly known as a field which includes patient ID. To do this, we assume that a secret key is allotted in advance of the PHD and gateway. This may already be set when the product is produced or on sale. This paper will exclude issues regarding key allocation in advance.

The suggested method is as follows (refer to Figure 4).

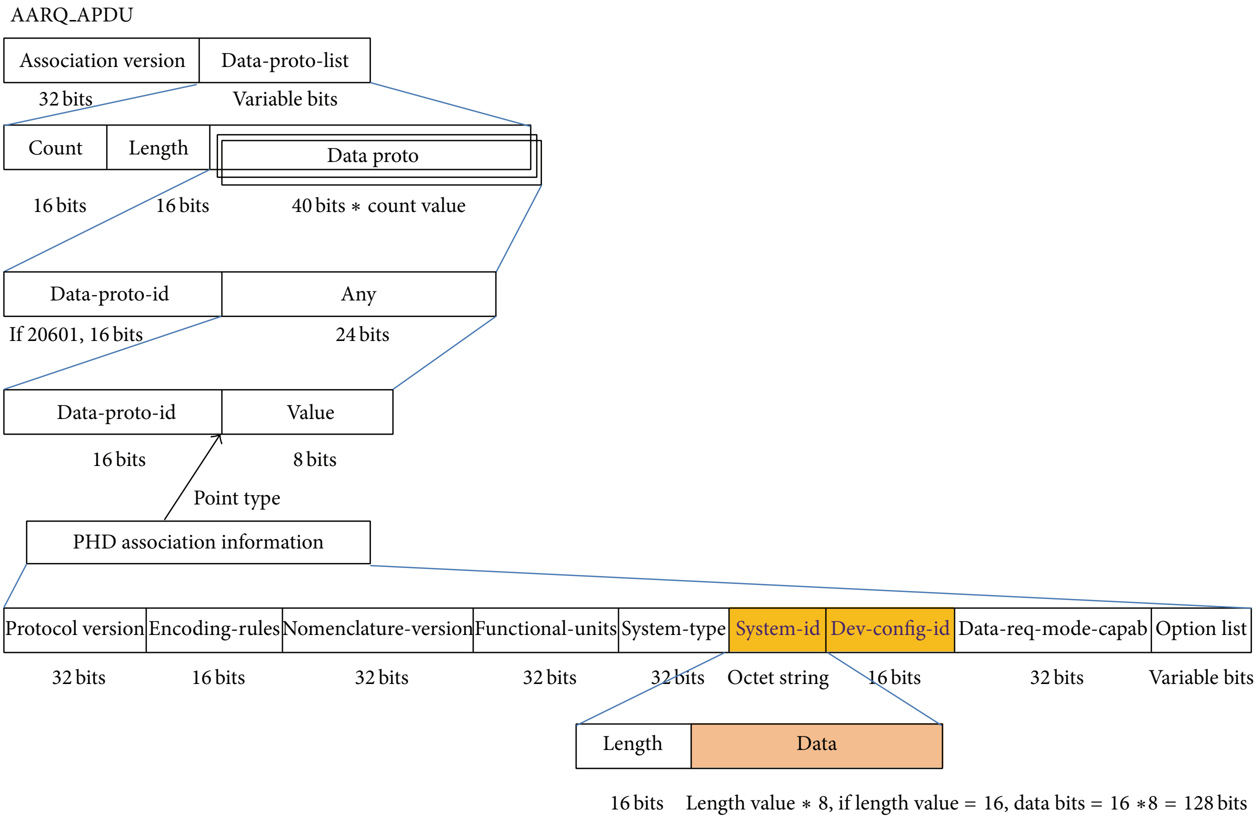

Figure 3: AARQ_APDU message data format in ISO/IEEE 11073-20601.

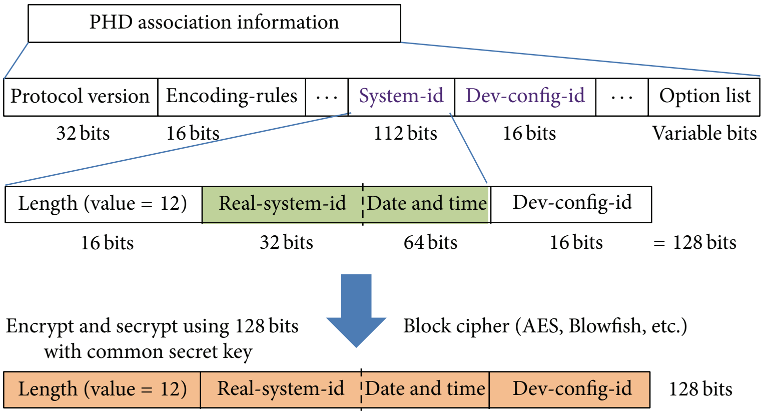

Figure 4: The proposed privacy protection method.

Step 1. When the PHD sends an AARQ_APDU message to the gateway for the first time, it configures the system-id (called real-system-id) with 32 bits along with a length value 12 fixed in PHD association information and then concatenates the date (sending time), time value (as 64 bits, it uses built-in value in PHD), and dev-config-id value. After that, it encrypts into a block cipher algorithm which is the same as AES or Blowfish by using a common secret key which the PHD and the gateway allocate in advance. Then, the following total messages will be sent to the gateway after encoding by MDER.

Step 2. The gateway decodes the AARQ_APDU message received from the PHD, decrypts the encrypted part, and confirms the real-system-id and dev-config-id. It then saves and sends the AARE_APDU message to the PHD as a response to the AARQ_APDU message.

Step 3. The procedure after Step 2 will proceed in the same way, along with existing ISO/IEEE 11073-20601, a standard communication protocol.

3.1. Discussion of Security. Since the suggested method uses a date and time value from an encrypted field, its value changes every time AARQ_APDU sends a message. Thus, it can protect against replay attack from an untrusted third party and provide security for patients who use a PHD. This applies in the same way to several patients who use the same devices or the same patient who has different devices.

The suggested method basically adopted a 128-bit block cipher. Of course, since a low-powered PHD, or biosensor, has a limitation in computation capability or memory, depending on application, it may use an encrypted algorithm which is less than 128 bits. In this case, the value should be adjusted and fixed with the gateway so that the length of the system-id field meets output size. This must be fixed because the length of the data field, which is followed by a length value, is determined when it is decoded at the gateway.

In the meantime, there is a way to encrypt the whole AARQ_APDU message which is initially sent by the PHD. In this case, considering the features of a low-powered sensor, which we mentioned previously, it may cost additional overhead, making burden when it is actually used. When all are encrypted and to ensure integrity, it may insert a message digest code or message authentication code using the cryptographic hash function on the option list in Figure 4.

In conclusion, the proposed method is simply to be able to guarantee the privacy of the patient, and moreover when using the aforementioned option list field, security services such as authentication and integrity can be further provided.

3.2. Healthcare Home and Building Design and Construction Application for Considering Privacy. Healthcare home and building design and construction include technology that can obtain health information about a subject, to be measured through a variety of sensors embedded at home and in the building, and transmits it to a health care service center via a gateway, providing the subject with a tailored healthcare service.

In most healthcare technology, the subject is aware of the existence of the sensors to measure their own health information. However, the subjects in a healthcare home or building may not know to check their own health information because of the unconstrained technology that is used to detect vital signs via the sensors built directly at home and in the building.

If the subject recognizes the existence of sensors, they may have the attention to defend the leakage of the health information, but not to know whether the subjects are defenseless against external exposure of the health information. The exposure of health information can be caused by the network between sensors and gateway. In a wireless network, health information leaks will be due to electromagnetic fields.

Therefore, although the adoption of the privacy function is optional in the PHD devices, the health care home and building design and construction technology is encouraged especially between the sensor and the gateway.

4. Concluding Remarks

So far, we have researched and suggested a new way to protect patient privacy in a PHD communication environment when telemedicine is used at home and in a building. The proposed method used ISO/IEEE 11073-20601 standard as the basic framework, which is an international standard protocol, for interoperability with existing products. We believe that our proposed method will be very useful and valuable as a basic resource by suggesting additional standards for security with the Continua Health Alliance [5] or in association with an ISO or IEEE group. In future research, we would like to propose a new protocol for user or message confirmation in order to confirm differences with existing protocols through tests and to strengthen security between the PHD and gateway.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2013R1A1A2006745). This research was financially supported by the Ministry of Education and the National Research Foundation of Korea (NRF) through the Human Resource Training Project for Regional Innovation.

References

[1] ISO/IEEE, 11073-20601: health informatics—personal health device communication, application profile optimized exchange protocol, http://www.iso.org.

[2] P. Urbauer, M. Frohner, M. Forjan, B. Pohn, S. Sauermann, and A. Mense, "A closer look on standards based personal health device communication: a resume over four years implementing telemonitoring solutions," *European Journal for Biomedical Informatics*, vol. 8, no. 3, pp. 65–70, 2012.

[3] C. A. Irmiter, *A Secure Personal Health Information Device*, American Medical Association, 2012.

[4] E. B. Sloane, "Medical device security effects of HIPAA, ARRA- and FDA-related security issues," in *Proceedings of the NIST-OCR HIPAA Conference*, May 2010.

[5] Continua Health Alliance, http://www.continuaalliance.org/.

[6] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *International Journal of Internet and Enterprise Management*, vol. 6, no. 4, pp. 279–314, 2010.

[7] P. Kumar and H. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[8] A. Kliem, M. Hovestadt, and O. Kao, "Security and communication architecture for networked medical devices in mobility-aware eHealth environments," in *Proceedings of the IEEE 1st International Conference on Mobile Services (MS '12)*, pp. 112–114, Honolulu, Hawaii, USA, June 2012.

[9] O. J. Rubio, A. Alesanco, and J. Garcia, "A robust and simple security extension for the medical standard SCP-ECG," *Journal of Biomedical Informatics*, vol. 46, no. 1, pp. 142–151, 2013.

[10] D. F. Kune, Y. Kim, K. Venkatasubramanian, I. Lee, and E. Vasserman, "Toward a safe integrated clinical environment: a communication security perspective," in *Proceedings of the ACM Workshop on Medical Communication Systems (MedCOMM '12)*, pp. 7–12, 2012.