Research Article

Implementation of Personal Health Device Communication Protocol Applying ISO/IEEE 11073-20601

Deok Seok Seo, Soon Seok Kim, Yong Hee Lee, and Jong Mo Kim

1 School of Architecture, Halla University San 66, Heungup-Li, Heungup-myon, Wonju-shi, Gangwon-do 220-712, Republic of Korea
2 Department of Computer Engineering, Halla University, San 66, Heungup-Li, Heungup-myon, Wonju-shi, Gangwon-do 220-712, Republic of Korea

Correspondence should be addressed to Soon Seok Kim; sskim@halla.ac.kr

Received 9 December 2013; Accepted 16 April 2014; Published 6 May 2014

Academic Editor: Jongsung Kim

Copyright © 2014 Deok Seok Seo et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In 2010, IEEE and ISO announced the exchange protocol standard (ISO/IEEE 11073-20601) [1], optimized to secure mutual compatibility between all sorts of PHDs and the gateways for collecting bioinformation from the devices and activating related services. This international standard is the first official document that has dealt with communication related to the healthcare device.

In 2010, IEEE and ISO announced the exchange protocol standard (ISO/IEEE 11073-20601), optimized to secure mutual compatibility between all sorts of PHDs and the gateways for collecting bioinformation from the devices and activating related services. This international standard is the first official document that has dealt with communication related to the healthcare device.

Most of the communication modules for external interface are currently developed by companies based on need, so it is difficult to secure compatibility with other companies’ devices, and because they are developed without a standard system, problems arise when linking them to a hospital’s information system. As communication between medical devices that support the present network is becoming important, a standardized medical information protocol for sharing and transmitting information is required.

This study uses ISO/IEEE 11073-20601 to realize a communication protocol between the weight sensor and gateway and its purpose is to implement a standard technology for mutual interoperability between medical devices and hospital systems. Moreover, advanced encryption standard (AES), which is an international standard for symmetric key encryption, has been applied to enhance security. As a result, when a cipher algorithm is applied in field of data transmission from PHD to gateway, it takes approximately 0.078 seconds longer on average compared to before.

In Section 2 of this dissertation, the recently revised ISO/IEEE 11073-20601 standard protocol is examined and Section 3 describes the actual implementation method related
to the weight sensor. Section 4 proposes the results of implementation and Section 5 draws conclusions.

2. ISO/IEEE 11073-20601 Standard [1]

This standard is a document for defining the standard format for information sent between health devices and data managers, for collecting bioinformation measured by the devices, and for the mutual exchange of information.

A sensor (such as a hemodynamometer, comprising scales, and a blood sugar device, hereafter simply referred to as PHD) collects personal bioinformation and then transmits the information to a gateway (such as a cell phone, a health device, and a personal computer) for the purpose of collection, display, and further transmission. A gateway can transmit data for the purpose of additional analysis to an healthcare service center for teleassistance and utilize information from various domains such as disease control, health and fitness, or an independent age measuring device. The communication path between a PHD and the gateway is assumed to be a logical point-to-point connection. Generally, a PHD communicates with a single gateway at a specific point when necessary. Gateways can communicate with a plurality of PHDs simultaneously using separate point-to-point connections.

Refer to the document for standard [1] for other protocols in further detail.

3. Protocol Implementation Method

In this study, as mentioned previously, a weight sensor was used to apply the ISO/IEEE 11073 standard protocol. ISO/IEEE 11073-20601 (communication protocol standard between PHD and gateway) and ISO/IEEE 11073-10415 (weight sensor communication standard) were used for the application.

The ASN.1 encoding regulation (also known as a medical device encoding rule (MDER)) defined in the standard was used for the exchange of information between the weight sensor and gateway.

According to the definition by the International Telecommunication Union (ITU), ASN.1 is a protocol defining the
data exchange on the network and is 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 becomes the standard. If MDER is expressed in C language, it is declared as a strict type that sends basic data using a structure called APDU. In APDU, 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 of the 6 messages (refer to Figure 1).

In order for communication between the weight sensor and the gateway to take place, the two devices must be mutually connected and in each status it can be divided into 10 types as shown below (refer to Figures 2 and 3). From the weight sensor perspective, first, one’s configuration information is sent and the gateway receives this information. The configuration information of the first connection is then saved and if connection is attempted again, only its ID is verified to enable immediate communication. On the other hand, Figure 4 demonstrates the communication process for the initial connection or if there is no configuration information of the weight sensor. Figure 5 demonstrates the communication process in cases where the gateway has configuration information from the weight sensor.

4. Protocol Implementation Result

In this study, the method described in Section 3 is used to apply a mutual communication protocol between the weight sensor and the gateway. The weight sensor (InBody R20 model) of the Biospace company [2] which was being sold on the market was used and the measurements from the weight sensor were received by a Pentium PC 3.0 GHz laptop for sending to the gateway (laptop Pentium PC 3.0 GHz). In order to secure accurate transmission, Visual C++ language was used in the laptop PC to create a viewer interface where features such as saving the data of the weight sensor, sending saved data, and displaying the received data were applied. Figure 6 shows the flow of the viewer program created and Figure 7 shows the weight sensor, while Figure 8 shows the viewer screen of the gateway.
Table 1: Comparison of average transfer time from PHD to gateway (unit: seconds).

| PRST_APDU | Encrypted data | Nonencrypted data | Difference |
|-----------|----------------|-------------------|------------|
| Average transmission time from PHD to gateway in 10,000 attempts | 0.026 | 0.018 | +0.008 |

For a secure transmission of PRST_APDU data from PHD to gateway, advance encryption standard (AES) protocol [3], an international standard for symmetric key encryption, was applied and used [4–6] (refer to Figure 9). As a result of this application, when the cipher algorithm was applied, in 10,000 attempts, the average implementation time was approximately 0.078 seconds longer than when it was not applied (refer to Table 1).

It was determined that applying encryption for secured transmission did not significantly influence the entire implementation time.

5. Conclusion

Until now, we have used international standard ISO/IEEE 11073-20601 to apply the communication protocol between a weight sensor and a gateway. The purpose of this dissertation is to realize a standard technology for mutual interoperability between a PHD, a health device used in households, and the hospital systems. The AES protocol, an international standard of symmetric key encryption, was applied to strengthen the security of transmission between devices, which was not available previously. As a result of this realization, when the encryption algorithm was applied, it took approximately 0.078 seconds longer on average than without.

In the future, we intend to expand the range of PHDs for application not only to the proposed weight sensor but also to ECG sensors, blood pressure devices, blood glucose device, and others.

Conflict of Interests

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

Acknowledgments

(1) 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). (2) This research was financially supported by the Ministry of Education, Science Technology (MEST) and 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] BIOSPACE CO., http://www.e-inbody.com/.
[3] AES (Advanced Encryption Standard), http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
[4] K. Jeong and S. S. Yeo, “Security analysis of block cipher LED,” Journal of Internet Technology, vol. 14, no. 2, pp. 281–287, 2013.
[5] I. Lee, S. Jeong, S. Yeo, and J. Moon, “A novel method for SQL injection attack detection based on removing SQL query attribute values,” Mathematical and Computer Modelling, vol. 55, no. 1-2, pp. 58–68, 2012.
[6] B. Vaidya, J. H. Park, S.-S. Yeo, and J. J. P. C. Rodrigues, “Robust one-time password authentication scheme using smart card for home network environment,” Computer Communications, vol. 34, no. 3, pp. 326–336, 2011.