Secure Communication Schemes over ISO/IEEE 11073-20601 for Smart Healthcare Service

Sang Kon Kim[1] and Tae Kon Kim[2]*
[1] Dept. of Electronics and Information Engineering, Korea University
2511 Sejong-ro, Sejong City, 30019 - KOREA
[e-mail: paulka@korea.ac.kr]
[2] Dept. of Electronics and Information Engineering, Korea University
[e-mail: taekonkim@korea.ac.kr]
*Corresponding author: Tae Kon Kim

Received December 23, 2021; revised May 29, 2022; accepted June 19, 2022; published July 31, 2022

Abstract

For advanced healthcare services, a variety of agents should maintain reliable connections with the manager and communicate personal health and medical information. The ISO/IEEE 11073 standards provide convenient interoperability and the optimized exchange protocol (OEP) supports efficient communication for devices. However, the standard does not specify secure communication, and sensitive personal information is easily exposed through attacks. Malicious attacks may lead to the worst results owing to service errors, service suspension, and deliberate delays. All possible attacks on the communication are analyzed in detail, and the damage is specifically identified. In this study, novel secure communication schemes over the 20601 OEP are proposed by introducing an authentication process while maintaining compatibility with existing devices. The agent performs a secure association with the manager for mutual authentication. However, communication with mutual authentication is not completely free from attacks. Message encryption schemes are proposed for concrete security. The authentication process and secure communication schemes between the secure registered agent (SRA) and the secure registered manager (SRM) are implemented and verified. The experimental analysis shows that the complexities of the SRA and SRM are not significantly different from those of the existing agent and manager.

Keywords: ISO/IEEE 11073, personal health device, secure 20601 OEP, smart healthcare

This work was supported by the Korea University Grant.

http://doi.org/10.3837/tiis.2022.07.006 **ISSN : 1976-7277**

1. Introduction

With advances in medical science and technology, the life expectancy of humans has increased significantly, and the elderly population is rapidly increasing in several countries. Moreover, individuals of all ages are increasingly paying attention to their daily health care beyond disease management. Accordingly, a variety of health/medical care services have been developed, such as e-health or smart health. These services should be cost-effective, clinically acceptable, and convenient for both individuals and healthcare providers. Initially, services were mainly focused on monitoring individual health status in a residential environment using personal health devices (PHDs) such as weight scales, thermometers, and blood pressure monitors. In recent years, a variety of health devices are utilized for human body information, and their convenience and accuracy can reach beyond imagination. With innovations in communication technology, seamless connectivity, sufficient capacity, and minimum latency can be guaranteed regardless of time and place. In fact, healthcare services are evolving into a real-time monitoring system with appropriate supports including emergency management from various healthcare providers under all circumstances [1-2].

The ISO/IEEE 11073 personal health device (PHD) standards provide convenient interoperability of healthcare, medical, and wellness devices for health care services [3]. A personal health device (an agent) measures the body information and it is designed to have limited resources. A compute engine (a manager) with good capabilities handles the information and performs most of the tasks. 11073-104zz standards define the specifications of devices and an optimized exchange protocol (OEP 11073-20601) supports logical connections between an agent and manager at the application layer [4-5]. Several developers and manufacturers can provide compatibility and interoperability of various types of devices by utilizing the 20601 OEP under the assumption of connectivity below the transport layer. In the standard, a usage model is assumed in which an agent and its corresponding manager operate exclusively as a pair. Recently, a manager with good resources can handle a number of agents and a significant amount of health information. It plays a central role for healthcare services as a portal device in the home or office environment [6-7]. However, the 20601 OEP does not provide secure communication, and sensitive personal information, including the user's body information, is easily exposed through cyber-attacks. This can cause health care services to become temporarily or permanently disabled, and malicious attacks may lead to the worst results owing to service errors and deliberate delays. That is, attacks can delay or interfere with the communication between the agent and manager, and they can easily intercept and modify personal information for malicious use [8-9].

An ultimate health monitoring system should always supply satisfactory real-time care service at any place. People expect appropriate care services in residential areas, office environments, public places, and hospitals. In all these environments, necessary and available agents measure user's health information intermittently or periodically, and they can communicate with a manager (**Fig. 1**). For the sake of user convenience, both the agent and manager are expected to provide mobility and maintain connectivity without user intervention. The usage models of personal health care were originally based on personal area communications (PANs). Recently, body area networks (BANs) and IoT environments are expected to be considered. Healthcare services in residential areas, a network gateway into the house, might be the most efficient candidate for a manager. The high-performance manager supported by the electric wall power can communicate with the healthcare service providers (HSPs) through a wired network, and it can manage all agents through wired and wireless networks. Instead of the above fixed manager, people can assume a manager as an app installed

on a smartphone. Although it guarantees excellent mobility, it is difficult to expect a sufficient role as a manager because of the power consumption and cost associated with the transmission of large amounts of data such as an electrocardiogram (ECG) [10] and electroencephalography (EEG). In public places such as fitness centers and hospitals, the user's agents can be rarely connected to the private manager directly, and they may communicate with certain public managers. Therefore, the risk of personal health information being exposed is very high in the public environment, and it is inevitably very vulnerable to cyber-attacks.

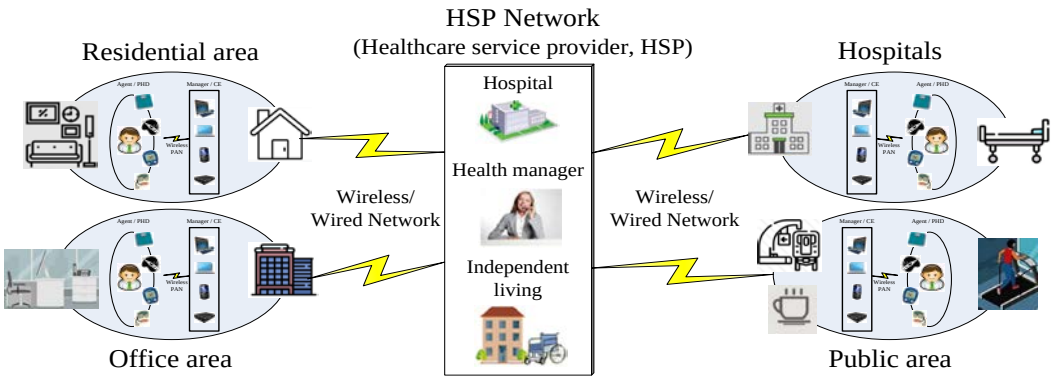


Fig. 1. Healthcare monitoring service system

In this study, novel secure communication schemes based on the 20601 OEP between a manager and an agent are proposed. By introducing an authentication process that is not defined in the standard, solid security is established. Devices with the proposed security schemes maintain full compatibility with existing agents and managers. When an agent registers with the manager for the first time, they perform initial authentication for future secure associations. Subsequently, they always proceed with a secure association to confirm mutual authentication at the start of communication. It is assured that the agent is connected with its own authenticated manager. Secure communication can support encryption techniques, and messages in cyphertext form can be used to completely block data exposure. An agent and manager pass the authentication process together and are referred to as the secure registered agent (SRA) and secure registered manager (SRM), respectively.

The authentication process and secure communication protocol between the SRA and the SRM were verified using an embedded system and a PC. Verification of compatibility between the secure devices (SRA and SRM) and the existing ones is executed. The security level against all possible attacks on the SRA and SRM was analyzed and verified in several types of environments. When only authentication is supported, the SRA and SRM transfer messages in plaintext form. However, when the encryption is supported, the implemented attacker views the captured messages as an unknown bit stream but cannot interpret it at all. The analysis showed that the increase in complexity for secure communication is not significant and acceptable to the systems currently in use.

2. Background on ISO/IEEE 11073 PHD Standards

The ISO/IEEE 11073 personal health device (PHD) working group (WG) has developed a group of standards addressing interoperability of healthcare and wellness devices. With device specifications (11073-104zz) [11-14], an optimized exchange protocol (11073-20601) defines the communication model between an agent and manager in a point-to-point (P2P) way [4-5].

However, the standard does not specify secure data communication or any protection method for attacks. In fact, it mainly focuses on plug-and-play interoperability between PHDs.

2.1 11073-20601 Optimized Exchange Protocol (OEP)

The ISO/IEEE 11073 standards aim to enable personal healthcare device communication for interoperability. The 20601 OEP provides a fundamental framework for the abstract models of personal health data and supports a logical connection between devices at the application layer. Several developers and manufacturers can provide compatibility and interoperability of various types of devices (PHDs, PMDs, wellness devices) by using these standards under the assumption of connectivity below the transport layer. For connection, USB and LAN technologies are assumed for wired communication, and Wi-fi, Bluetooth, and ZigBee are supported for wireless communication [15-16]. In other words, the usage models of personal health care are originally based on local or personal area networks (LANs or PANs). Body area networks (BANs) and IoT environments are expected to be considered in near future.

The system model of the 11073 PHD consists of a domain information model (DIM), service model, and communication model. The DIM characterizes the information of an agent as a set of objects having one or more attributes. Attributes describe measurements, elements for behavior control, and reports on the status of the agent. The service model defines data access primitives of the messages between the agent and manager, and data can be exchanged by the Get, Set, Action, and Event Report commands. For the P2P connection, the connection state machine specifically shows the dynamic system behavior of the agent and manager pair. The connection machine of a device defines the states and substates related to connection, association, and operations.

An agent collects and transmits personal health data to an associated manager. The manager receiving data from agents controls health care systems including connection management and reliable transfer. A logical connection between them should be established for communication. The 20601 OEP defines the commands, agent configuration information and data format, and provides the foundation to support different types of PHDs. When both devices are in a connected, associated and operating state, they can communicate correctly using the proper DIM and service model.

2.2 Measurement Data Transmission between Agent and Manager

Firstly, the agent transmits an association request (AssocRequest) to the manager for communication. When the system ID and configuration ID in AssocRequest from the agent are not registered yet, the manager may respond with the accepted-unknown-config parameter (AssocResponse) to accept the request. The agent sends the configuration information for the following configuration procedure. After checking the information, the manager responds with the accepted-config parameter when it can support it; otherwise, it responds with the unsupported-config parameter. When the agent receives an unsupported-config attribute from the manager, they cannot interoperate with each other. When they can communicate, the manager moves an associated operating state and it identifies configuration information such as the handle number, attribute count, ID, and value for object handles. If the agent is associated with the appropriate configuration process once, then the association procedure is simplified into two steps (① in **Fig. 2**). When both devices are in the associated and operating state, they can communicate and perform appropriate operations. For example, by using the GET service, the manager can obtain the medical device system (MDS) object of the agents. Information such as the type of agent, manufacturer and model number, system-id, config-id,

and product specification is included in the MDS object. Subsequently, managing the measurement data becomes the important role of the manager due to the limited resources of the agent.

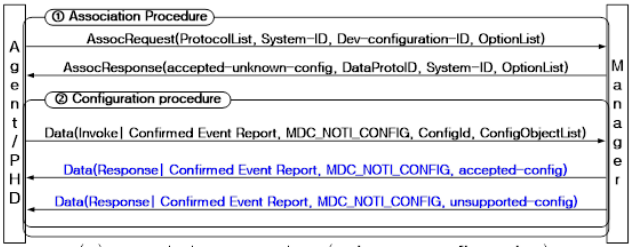


Fig. 2. Association procedure

Either the agent or manager can initiate data transmission. When the agent measures the data intermittently and stores small amounts of data temporarily, agent-initiated transfers are typically used. When the agent collects a large amount of data periodically, manager-initiated transfers are used. It can control the data flow and support data streaming services. A sequence diagram for data transmission between an agent to manager is shown in **Fig. 3**. After an agent sends measured data, it may receive any confirmed response. Under any circumstances, the agent is likely to delete the transmitted data to avoid unnecessary duplication of transmission.

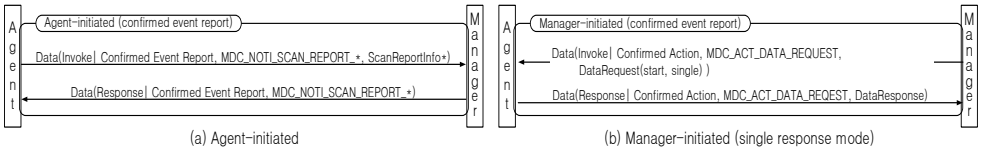


Fig. 3. Measurement data transmission

3. Analysis on Attacks

Because the 20601 OEP assumes a P2P connection in the application layer between an agent and manager, any security schemes in the lower layers are ineffective from attacks at the same application layer. Attackers based on the 20601 standards can easily detect or intercept a transmitted message that includes sensitive personal information in plaintext format. By pretending to be a manager, they can obtain almost all the information they need from agents. This can result in a significant loss of measurement data and a waste of the agent's limited resources. Disguised as an agent, they may give manipulated or false information to the manager, and they even can destroy the manager's role by sending a huge amount of dummy data. It is almost impossible for the agent and manager to detect the presence of an attacker, and they only respond to a received packet.

Attacks can be classified by various perspectives, but they are generally classified as passive or active. A typical example of a passive attack is eavesdropping, which captures transmitted information without interfering with normal communication. An active attack aims to acquire the desired information by actively intervening in communication. It includes denial of service (DoS), impersonating, replay, modification (false data injection) [8-9]. All possible types of attacks and issues are presented and analyzed in this section.

3.1 Eavesdropping

An attacker detects the transmission of data between an agent and manager without any action and views the message as a bit stream at the application layer. The attacker identifies all types of messages defined over the 20601 OEP and correctly understands the information contained in the messages. The **Fig. 4** shows an example of an eavesdrop in the process of association.

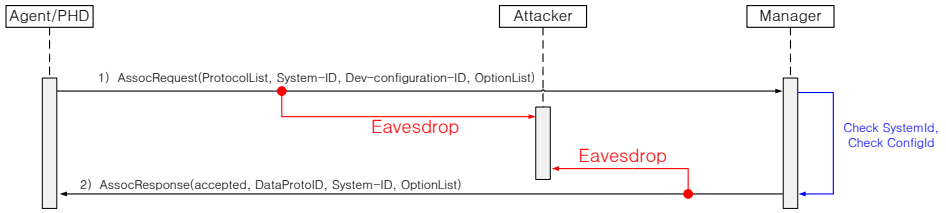


Fig. 4. Eavesdropping during association

3.2 Denial of Service (DoS)

The attack is a malicious one that makes normal communication impossible between an agent and manager with active interruptions. By sending a malicious message during the communication procedure, either the agent or manager cannot complete the entire communication successfully. This attack consumes significant battery power, computing capacity, and communication capacity, and causes delays or an inability to service. The **Fig. 5** shows an example of an attack that delays or disables the connection by sending an abort message during the association procedure.

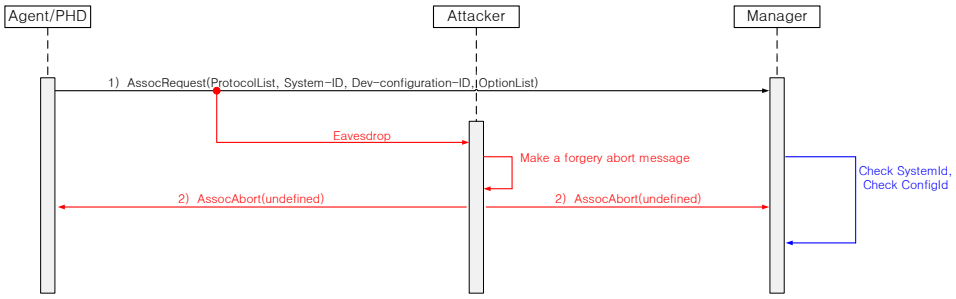


Fig. 5. Abort attack during association

3.3 Impersonating (Illegal Information Acquisition)

In this scheme, an attacker pretends to be a manager, and it illegally obtains the agent's information that can be requested. The **Fig. 6** shows that the attacker intervenes in the association process and responds faster than the manager to the agent. The agent completes the association process with the attacker and is ready to respond. This is possible because it takes time for the manager to check the transmitted message, including checking System-ID and Configuration-ID, while the attacker copies the eavesdropped message and responds immediately. Because an agent cannot establish more than one connection, the agent ignores the association response from the manager. Currently, the manager shifts to the associated state, and all of them are in the associated state. The attacker sends the MDS Get request to the agent, and the agent responds with its MDS information in the example. An attacker can unfairly obtain all information on the device.

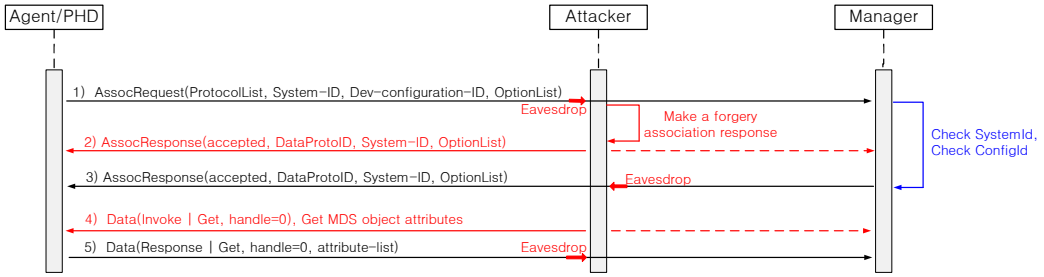


Fig. 6. Illegal information acquisition during association

3.4 Replay

An attacker captures the transmitted data between the agent and manager passively. It pretends to be an agent and repeatedly sends data to the manager (**Fig. 7**). Because data that do not include time information are repeatedly transmitted to the manager, it can cause significant disruption and errors in the service. Alternatively, fake time information can be used to induce a larger problem.

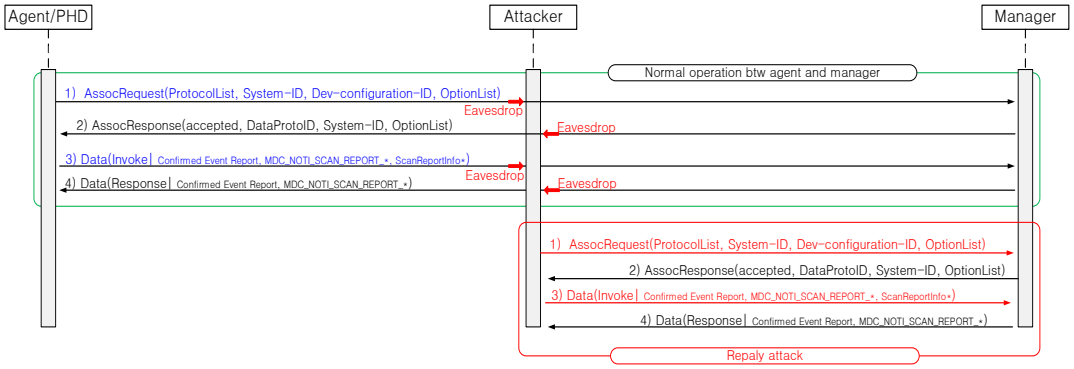


Fig. 7. Replay attack to the manager

3.5 Modification (False Data Injection)

An attacker can easily obtain the agent information, including its MDS, hence he can freely access the manager as if he were the agent. Therefore, starting with sending the association request message to the manager, all operations can be performed pretending to be an agent (**Fig. 8**). The attacker may send modified or false information to the manager, and it may even provide a large amount of dummy data. This can cause serious service errors and deliberate delays, which may lead to the worst results in health/medical care.

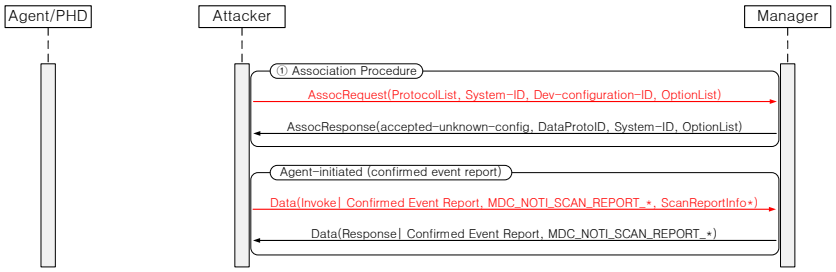


Fig. 8. False data injection to the manager

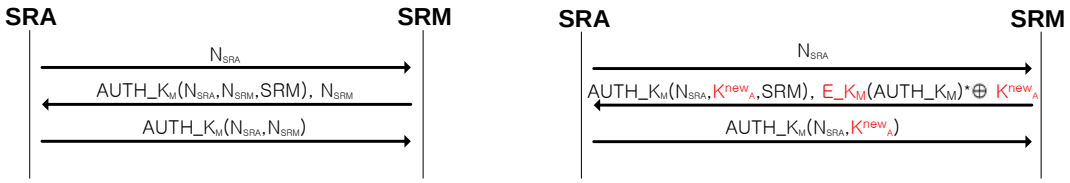
4. Proposed Security Schemes

The communication between devices easily exposes sensitive personal information and is very vulnerable to attacks. Therefore, for advanced healthcare services with various personal health devices, it is essential to apply enhanced security techniques to the 20601 OEP. The application of the added security schemes should certainly maintain compatibility with existing communication protocols.

When an agent initiates a connection by sending an association request to a manager, it is necessary to confirm that the corresponding manager is authenticated. Security can be strengthened by adding the process of verifying the shared secret information between the agent and manager. The schemes can be achieved by an authentication process, and through this process, certain information, including a master key, is shared. Even if the above feature is added, the messages over the 20601 OEP utilize the known message structures in a plaintext form, hence they cannot be completely free from attacks. Therefore, it is essential to apply encryption schemes through a key distribution for concrete security.

4.1 Authentication and Encryption

Initially, when an agent with security features registers with the secure manager, it performs an appropriate authentication process to ensure enhanced secure communication. In the **Fig. 9** (a), the authentication process applied with 2 party authentication protocol (2PAP) is presented as an example [17]. This is a type of security authentication that can be performed repeatedly when communication is started between them. The variables N_{SRA} and N_{SRM}, which are generated one-time random numbers, are used by each party to challenge the other. The one-way hash functions with the shared master key and challenges are used to confirm the mutual authenticity. The **Fig. 9** (b) shows an example of authentication using 2 party authentication and key distribution protocol (2PAKDP) [18-19]. In this case, encrypted messages are used to completely block data exposure, and the scheme enables a significant level of secure communication. In this paper, an agent and manager that supports secure communication and has passed the authentication process together are referred to as the secure registered agent (SRA) and secure registered manager (SRM), respectively.



(a) 2PAP (b) 2PAKDP

Where, K_M is a master key, AUTH_K_M is HMAC (hash-based message authentication code) with a master key, E_K_M(AUTH_K_M)* is encryption of AUTH_K_M(N_{SRA},$K^{new}{}_A$,SRM), and $K^{new}{}_A$ is a session key.

Fig. 9. Authentication examples

4.2 Secure Communication (Secure Association and Encryption)

To apply the secure communication method to the 20601 OEP by using an authentication process and to maintain compatibility with existing devices, the following conditions should be satisfied: First, the SRA must be able to request secure communication to the SRM in a mutually exclusive manner. This request must appear to the existing manager as an association request. Second, the SRM must be able to respond exclusively. For the request from the SRA,

the SRM recognizes the secure communication request and responds in such a way that only the SRA can understand. Furthermore, an existing agent understands the SRM response as a general association response from an existing manager. Third, upon receiving the SRM response, the SRA needs to respond using the existing message format for its authentication to the SRM. Finally, the SRM checks the received message and completes the secure association by providing an appropriate response to the SRA.

To address the above problems, AssocRequest, which is included in the SRA's association request and AssociateResult, which is included in the SRM's association response are described in detail. Utilizing some values reserved for future use in the messages, the SRA and SRM perform the secure association process while maintaining compatibility with existing devices. The AssocRequest contains the information:

1) protocol-version, 2) encoding-rules, 3) nomenclature-version, 4) functional-units,
5) system -type, 6) system-id, 7) dev-config-id, 8) data-req-mode-capab, 9) option-list.

The functional-units information can be used to solve the problems.

FunctionalUnits ::= BITS-32 {
fun-units-unidirectional(0), fun-units-havetestcap(1), fun-units-createtestassoc(2),
fun-units-secureauth(3), fun-units-cryptInfo(4) }.

The fun-units-secureauth(3) and fun-units-cryptInfo(4) indicate that secure authentication or encryption is supported by the SRA. Three values of AssociateResult in the SAM's association response are used.

AssociateResult ::= INT-U16 {
accepted(0), rejected-permanent(1), rejected-transient(2), accepted-unknown-config(3),
rejected-no-common-protocol(4), rejected-no-common-parameter(5),
rejected-unknown(6), rejected-unauthorized(7), rejected-unsupported-assoc-version(8),
accept-secureauth(9), accept-cryptMess(10), accepted-unknown-secureconfig(11) }.

The accept-secureauth(9) and accept-cryptMess(10) values indicate that the secure authentication or encrypted message will be supported, respectively. The SRM uses the "accepted-unknown-secureconfig(11)" value to inform the SRA that it is resuming the authentication procedure. These values are meaningful information only for the SRA and SRM, whereas they are meaningless for existing devices.

In this study, a secure association scheme using an existing association procedure is proposed (**Fig. 10**).

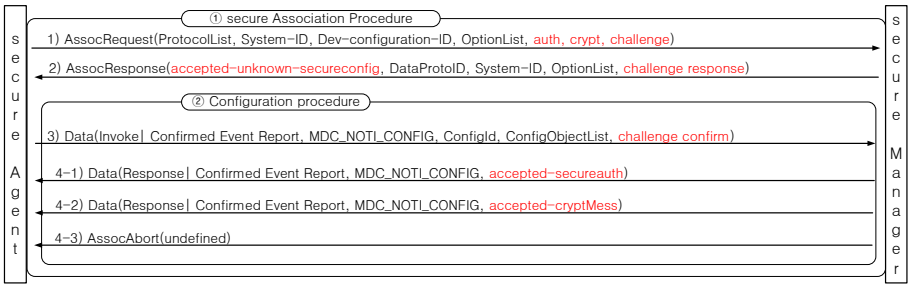


Fig. 10. Secure association

1) The SRA initiates secure association with the SRM by sending the AssocRequest message with the necessary security information. This can include information about authentication, encryption, and challenge (e.g., nonce). At this time, because an existing manager cannot recognize security information, it proceeds with the association procedure in response to an agent's request.

2) The SRM recognizes the security information included in the received message and generates the corresponding challenge response. The challenge response has different values according to the Auth and Crypt information. That is, in the case of Auth(1) & Crypt(0), the challenge response is used for mutual authentication only, and in the case of Crypt(1), it is used for both authentication and encryption. The SAM sends the AssocResponse message with "accepted-unknown-secureconfig," which makes them move on to the configuration procedure. The configuration procedure will be used for subsequent secure association.
3) The SRA checks the challenge response in the message from the SAM and generates challenge confirmation information. The Data message with the challenge confirmation is sent to the SAM. When the SRA receives the association response from an existing manager, the agent may work with it, depending on the user's decision.
4) The SRM verifies legitimate authorization by checking the message from the SRA. Depending on the MDS information and capability of the SRA, it is decided whether to use only authentication or full security, including encryption. When the encryption is used, 20601 messages in the form of encrypted ciphertext using the distributed key are utilized. Otherwise, the messages in the form of an unencrypted plaintext are used. Finally, it completes the secure association by sending the Data message to the SRA.

5. Analysis and Verification

5.1 Implementation and Verification

To verify the interoperability of the SRA and SRM to which the proposed security schemes are applied, the agent of blood pressure monitor and the manager are used [14]. Agents are typically considered to have limited resources and managers are designed to perform most of the tasks. In the consideration of price, size and limited resources, a blood pressure monitor with a pulse rate is implemented on the embedded system. The system has the 8-bit processor, 16Mhz system clock, 8KB SRAM, 64KB program memory, and 4KB EEPROM. The SRM is implemented on a PC. The two devices were connected using Bluetooth version 2.0 wireless communications [15]. The association procedure, configuration procedure, MDS object, and measurement data transmission defined in the 20601 OEP were tested and verified.

For secure communication between devices, the SRA should go through an appropriate authentication process when first registering with the manager. In this study, two types of discussed authentication processes are implemented and tested. For the use of authentication only, 2 party authentication protocol (2PAP) is implemented [17]. It is confirmed that the two devices are mutually authenticated by successfully performing a secure authentication process. For encryption, 2 party authentication and key distribution protocol (2PAKDP) encryption is implemented [18-19]. In this case, encrypted messages using the distributed key as well as the completion of secure association are verified. A method of encrypting the entire message is used, and the encryption of all types of messages is confirmed. After a successful secure association, the SRA and SRM move to a secure associated operating state. It is verified that the agent-initiated data transmission with the Data message in both plaintext and cyphertext forms is transmitted correctly.

The verification of compatibility between the secure devices (SRA and SRM) and the existing ones is executed in the following two cases: between the agent and the SRM, and between the SRA and the manager (**Fig. 11**). Devices are assumed to be in a Bluetooth environment. In the case (a), the agent initiates the communication by sending the association request. It is verified that the agent properly associates with the SRM. When the SRM receives

the request, it recognizes that the request message is from an existing agent, and it responds like the existing manager. In the case (b), the SRA sends a secure association request and the manager cannot recognizes it. It proceeds with an association procedure in response to agent's secure request. It is verified that the SRA makes an association with the existing manager.

(a) communication between EA and SRM (b) communication between SRA and EM

Fig. 11. Verification models for compatibility

5.2 Security Verification

The security level against all possible attacks on the SRA and SRM is analyzed and verified in three different types of environments: where they are in secure association, where they transfer messages in plaintext form, and where they transmit messages in cyphertext form. It is assumed that an attack is impossible when an agent with a secure function makes a secure association while registering with the corresponding secure manager for the first time.

During secure association, an attacker can eavesdrop on messages, but cannot intervene. However, by sending the abort message, an attacker incompletely stops the association process, which leads to a delay or inability of service. The implemented attacker captures the transmitted messages in the application layer and recognizes the message type, header information, and payload. It is confirmed that both the installed SRA and the SRM stop the association process in response to the attacker's abort message. After secure association, they confirm mutual authentication and move to the operating state for data transmission. When only authentication is supported, the installed attacker identifies all types of transmitted messages and correctly understands the information contained in the messages. The SRM always responds to the attacker's data transmission, and the SRA provides the device's information according to the attacker's request. On the contrary, when the encryption is supported, the attacker views the transmitted messages as a bit stream at the application layer but cannot interpret it at all. The security level against attacks in three different types of environments is summarized in **Table 1**.

Table 1. Security level against attacks

	Eavesdropping	DoS	Impersonating	Replay	Modification
Authentication Process (During Secure Association)	◐	◐	●	N/A	N/A
Authentication only (Message in plaintext)	●	●	◐	●	●
Authentication & Encryption (Message in cyphertext)	◎	◎	◎	◎	◎

Where, ◎, ◐, and ● indicate high-, middle-, and low-level security, respectively.

5.3 Complexity Analysis

In this study, complexity in the 20601 OEP and the device specification layers is analyzed. The complexity of the SRA and SRM is calculated in terms of the additional memory space and computational capacity required for secure association and encryption. When the agent of blood pressure monitor is implemented on the embedded system, the occupied memory size is about 25 KB [20]. The space for initial authentication and secure association, including hash function-based message authentication code, MD5 does not exceed a maximum of 4 KB. The space for the encryption using a stream cipher, RC4, is also limited to a maximum of 14 KB [21]. The increase in the complexity for secure communication is not significant and acceptable to the systems currently in use. In addition, the recent development of microcontrollers with hardware RC4 suitable for application in IoT environments is expected to accelerate the spread of secure communication proposed in this paper.

6. Conclusion

In the advanced healthcare service system, a variety of agents and managers constantly communicate a large amount of personal health and medical information. The ISO/IEEE 11073 device specifications and the optimized exchange protocol provide convenient interoperability for devices. However, the standard does not specify secure communication, and sensitive personal information is easily exposed to attacks. Malicious attacks may lead to the worst results, owing to service errors and delays. In this study, novel secure communication schemes over the 20601 OEP are proposed by introducing an authentication process. The proposed methods support secure and reliable communication with full compatibility. The agent and manager always confirm mutual authentication at the start of the communication. However, a secure association for authentication does not guarantee secure communication between them. Therefore, the encryption of messages is additionally proposed for higher-level security. The proposed authentication process and secure communication schemes between the SRA and the SRM were implemented and verified. The experimental analysis showed that an increase in the complexity of the SRA and SRM is acceptable.

References

[1] S. Raj and K. C. Ray, “A Personalized Point-of-Care Platform for Real-Time ECG Monitoring,” *IEEE Trans. on Consumer Electronics*, vol. 64, no. 4, pp. 452-460, November, 2018. Article(CrossRef Link)

[2] X. Wang and Z. Jin, “An Overview of Mobile Cloud Computing for Pervasive Healthcare,” *IEEE Access*, vol. 7, pp. 66774-66792, May, 2019. Article(CrossRef Link)

[3] Health Informatics-Personal Health Device Communication, ISO/IEEE 11073. [Online]. Available: http://standards.ieee.org/.

[4] Health Informatics-Personal Health Device Communication Part 20601: Application Profile-Optimized Exchange Protocol. ISO/IEEE Std. 11073-20601-2008. [Online]. Available at: http://standards.ieee.org/findstds/standard/11073-20601-2008.html.

[5] Health Informatics-Personal Health Device Communication Part 20601: Application Profile-Optimized Exchange Protocol Amendment 1. ISO/ IEEE Std. 11073-20601a-2010. [Online]. Available at: http://standards.ieee.org/findstds/standard/11073-20601a-2010.

[6] S.-K. Kim, T.-K. Kim, and H.-K. Lee, “A Novel Transmission Scheme for Compressed Health Data Using ISO/IEEE11073-20601,” *KSII Transactions on Internet and Information Systems*, vol. 11, no. 12, pp. 5855-5877, Dec., 2017. Article(CrossRef Link)

[7] Tzong-Shyan Lin, Pei-Yu Liu, and Chun-Cheng Lin, "Home Healthcare Matching Service System Using the Internet of Things," *Mob. Netw. & Appl*. vol. 24, no. 3, pp. 736-747, June 2019. Article(CrossRef Link)
[8] AKM I. Newaz, Amit K. Sikder, Leonardo Babun, and A. S. Uluagac, "HEKA: A Novel Intrusion Detection System for Attacks to Personal Medical Devices," in *Proc. of IEEE Conf. on Comm. and Net. Sec.*, June 2020. Article(CrossRef Link)
[9] Óscar J. Rubio, Jesús D. Trigo, Álvaro Alesanco, Luis Serrano, and José García, "Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility," *Journal of Biomedical Informatics*, vol. 60, pp. 270–285, 2016. Article(CrossRef Link)
[10] Health Informatics-Personal Health Device Communication Part 10406: Device Specialization-Basic Electrocardiograph. ISO/IEEE Std. 11073- 10406-2011. [Online]. Available at: http://standards.ieee.org/findstds/standard/11073-10406-2011.html.
[11] Health Informatics-Personal Health Device Communication Part 10408: Device Specialization-Thermometer. ISO/IEEE Std. 11073-10408-2010. [Online]. Available at: http://standards.ieee.org/findstds/standard/11073-10408-2010.html.
[12] Health Informatics-Personal Health Device Communication Part 10415: Device Specialization-Weighing Scale. ISO/IEEE Std. 11073-10415-2010. [Online]. Available at: http://standards.ieee.org/findstds/standard/11073-10415-2010.html.
[13] Health Informatics-Personal Health Device Communication Part 10417: Device Specialization-Glucose Meter. ISO/IEEE Std. 11073-10417-2010. [Online]. Available at: http://standards.ieee.org/findstds/standard/11073-10417-2010.html.
[14] Health Informatics-Personal Health Device Communication Part 10407: Device Specialization-Blood Pressure Monitor. ISO/IEEE Std. 11073-10407-2008. [Online]. Available at: http://standards.ieee.org/findstds/standard/11073-10407-2008.html.
[15] Bluetooth Health Device Profile Version 1.0 Revision 00. [Online]. Available: https://www.bluetooth.com/specifications/specs/health-device-profile-1-0/.
[16] ZigBee Health Care Profile Specification Version 1.0 Revision 15. [Online]. Available: https://davidhoglund.typepad.com/files/105619r00zb_zhc_ptg-zigbee_health_care_profile_1.0_public.pdf.
[17] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, "Systematic design of a family of attack-resistant authentication protocols," *IEEE JSAC special issues on secure communications*, vol. 11, no. 5, pp. 679-693, 1993. Article (CrossRef Link)
[18] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, "The KryptoKnight family of authentication and key distribution protocols," *IEEE/ACM Trans. on Netw.*, March 1995.
[19] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, "The KryptoKnight family of light-weight protocols for authentication and key distribution," *IEEE/ACM Trans. Networking*, vol. 3, no. 1, pp. 31-41, Feb. 1995. Article (CrossRef Link)
[20] S.-K. Kim and T.-K. Kim, "Improvement of Wireless Connectivity and Efficiency in E-Healthcare Service System Using a Proxy in Body Area Device," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 3, pp. 991-1013, Mar., 2020. Article (CrossRef Link)
[21] P. Jindal, and B. Singh, "A Survey on RC4 Stream Cipher," *International Journal of Computer Network and Information Security*, vol. 7, pp. 37-45, Jun. 2015. Article (CrossRef Link)

Sang-Kon Kim He received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2008. He is currently an associate professor of Electronics and Information Engineering in Korea University. His research interests include wired and wireless networks and communications, network and computer security, and e-health.

Tae-Kon Kim He received the Ph.D. degree in electrical engineering from the Pennsylvania State University, University Park, PA, in 2001. From 2001 to 2002, he was with Technology & Research Labs, Intel Corporation, Chandler, AZ. From 2003 to 2004, he was with Digital Media R&D center, Samsung Electronics, Suwon, Korea. Since 2005, he has been with Korea University, Korea, where he is an associate professor of Electronics and Information Engineering. His research interests include multimedia signal processing, wireless networks and communications, and e-health.