Mobile Information Systems 7 (2011) 189–200
DOI 10.3233/MIS-2011-0117
IOS Press

Distributed authentication mechanism for secure channel establishment in ubiquitous medical sensor networks

Inshil Doh[a], Jiyoung Lim[b,*] and Kijoon Chae[a]
[a]*Department of Computer Science and Engineering, Ewha Womans University, Seoul, Korea*
[b]*Department of Computer Software, Korean Bible University, Seoul, Korea*

Abstract. In medical sensor networks, sensor nodes on a body of the patient sense the vital data and deliver them to the server system through mobile devices or gateways in the middle. However, when these linking devices do not function because of the battery outage or the system fault, the server system could not get patients' data during that period, and this situation could lead to serious problems. In this paper, to cope with this problem, we propose a distributed authentication mechanism in which substituted devices could be authenticated to deliver patients' data to the server system in the unusual situation.

Keywords: Distributed authentication, secure channel, ubiquitous, medical sensor networks, body sensor networks, security

1. Introduction

Medical sensor networks(MSNs) consist of small, intelligent devices attached on or implanted in the body, and they are capable of establishing a wireless communication link. Sensor devices provide the continuous health monitoring and the real-time feedback to the user or the medical personnel. Furthermore, the measurements can be recorded over a longer period of time, improving the quality of the measured data.

MSNs with portable devices such as smart phones enable continuous efficient monitoring and management of post-operative or chronically-ill patients. Healthcare personnel can be automatically alerted if the patient's condition deteriorates. MSNs must ensure confidentiality, integrity and availability of the physiological data, and authorization and authentication of sensors or users, as wireless sensor networks are susceptible to the passive eavesdropping, packet injection and security attacks by other devices. The authentication for devices participating in MSN is one of the most important issues for secure MSNs, because only legal device should contact MSNs.

In our paper, we propose a distributed authentication mechanism for devices in secure MSNs. Our proposal does not require the authentication server, but the server system in hospitals or healthcare centers plays the role as authenticator for devices. In distributed manner, we propose a device authentication using A3 and A8 algorithm usually adopted in mobile phones. Especially, we propose a secondary device

*Corresponding author: Jiyoung Lim, Room No. 524 Bokum, 32, 214gil Dongilro, Nowon-gu, Seoul 139-791, Korea. Tel.: +82 2 950 5444; Fax: +82 2 950 5411; E-mail: jylim@bible.ac.kr.

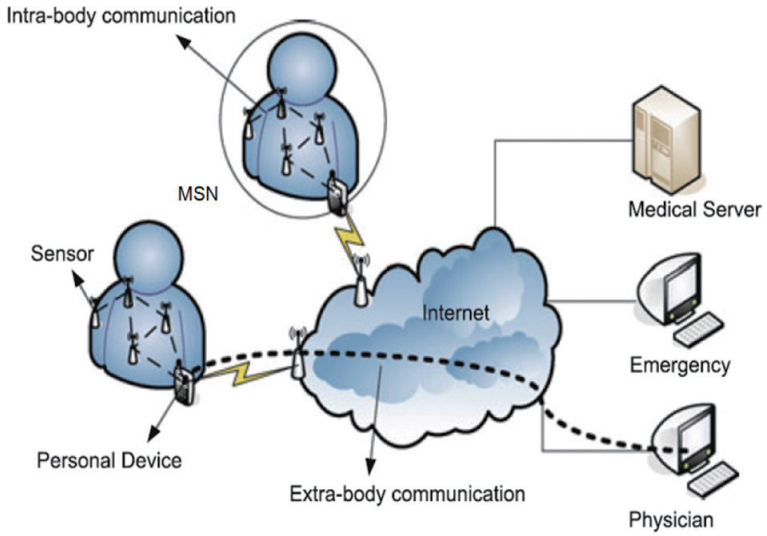

Fig. 1. Health Monitoring Architecture in a MSN [1].

authentication mechanism which enables to cope with the situation when the original device cannot relay the bio-information because of abrupt battery exhaustion or malfunction. Even in that situation, our mechanism can support the medical network securely and efficiently.

Our paper makes the following contributions:

- Proposal of a distributed secondary device authentication mechanism for devices which play the role of delivering bio-data from sensor nodes to the server system for MSNs.
- Proposal of a distributed authentication mechanism in case of malfunction of the intermediary device when the device cannot function properly with or without any notification in advance.

The rest of this paper is organized as follows. Section 2 briefly describes related works. Section 3 presents our proposed device authentication mechanism. Section 4 analyzes performance and security aspects of proposed scheme. Finally, we conclude the paper in Section 5.

2. Related work

2.1. Medical sensor networks

MSN is a network of wearable or implantable devices in the human body and it is made up of a gateway and sensor nodes. The personal device is a gateway enabling the secure data exchange between wide-area-networks and the MSN domain. In Fig. 1, a personal device plays a role of a gateway, collects bio-data from sensors via the intra-body communication, and uploads the collected data to a server and a computer of the emergence room or a physician in charge via the extra-body communication [1–3].

Medical sensor devices making up an MSN have severe restrictions on their hardware resources and radio transmission range. Sensors measure electrocardiographs (ECGs), heart beats, body temperatures and body activities. They are attached to human skin when required and send bio-data while they are attached. Transmission distance of sensors within an MSN is less than 2.5 meters and the number of sensors is normally less than 15 [4]. These sensors and devices have extremely limited resources in terms of processing capability, memory and power.

2.2. Potential attacks and security requirements

Some typical attacks [5] faced by MSNs are summarized as follows:

- Bio-information is eavesdropped: Bio-information transmitted over wireless radio frequency in MSNs may be eavesdropped. The information eavesdropping is difficult to be noticed because it is concealable.
- Bio-information is accessed by illegal entities: Unauthorized entities driven by curiosity or motivated by some cankered purposes may try to access bio-information collected in the MSN.
- Bio-information is altered: Attackers may add, delete or modify bio-information during transmission. Deletion is the most incidental attack in alteration of bio-information because it does not require decrypting the information.

Therefore, the minimum security requirements of MSNs include the followings:

1) Confidentiality: Encryption operation is the most efficient method to ensure confidentiality and to prevent bio-information to be accessed by entities without the decryption key. Attackers will not know the content of the information even if they capture it because it is encrypted. Given the limited resources of MSNs, symmetric key cryptography is found more suitable than asymmetric key cryptography for encrypting and decrypting bio-information in MSNs.
2) Authorization: Different sensors of the MSN will have distinctive privileges in accessing information collected by other sensors or devices of the same MSN. Authorization can be assigned in advance before communication.
3) Authentication: Bio-sensors or devices should recognize each other before communications to avoid accessing by unknown entity. Authentication can be implemented based on authentication keys.
4) Non-repudiation: Non-repudiation assures that an entity cannot deny transmitting or receiving a message in MSNs. Operations of digital signature and digital certificate can provide non-repudiation for the transmission process of bio-information in MSNs.
5) Integrity: There is a danger that bio-information can be modified, deleted, and replaced during transmission by a hostile entity or a device error in MSNs. Message digests or hash functions can be used to check whether some pieces of information have been altered.

2.3. Previous works

In this section, we introduce various MSN-adaptive solutions since existing security mechanisms adopted in traditional networks such as wireless sensor networks [6–8] cannot be directly used in MSNs owing to characteristics of bio-sensors. Some solution for bio-data integrity and freshness exploit biometric information [9–12] and a symmetric key [13–15] or a public key [16,17].

Biometrics is a technique commonly known as the automatic identification and verification of an individual by his or her physiological and/or behavioral characteristics [18]. In [12], an algorithm based on biometric data is described that can be employed to ensure the authenticity, confidentiality and integrity of the data transmission between the personal device and all other nodes. Algorithms that use the heartbeat to generate a key are proposed in [9–11]. In [9], they proposed the fuzzy key management with ECG. The cryptographic key intended for the entire MSN is generated at a single point and then distributed to the remaining sensors. Their scheme consumes less communication resources compared with those of the existing single-point fuzzy key methods and has the design limitation that the minimum number of bits is the length of the cryptographic key.

Another solution is authentication for message [11,19], entity (bio-sensors) [20] and secure frameworks [21,22]. Entity authentication is defined as the process whereby one party is assured of the identity of a second party involved in a protocol. In [20], their solutions provide two-tier authentication based on physiology. The key serves a dual purpose of data encryption and mutual authentication between a sensor and base station. In [21,22], they proposed the secure frameworks for authentication and data transmission.

We focus on distributed authentication methods for MSN in this paper. Distributed authentication researches in MSN are a few although they have differences with those in wireless sensor networks. In [23], they consider hand-offs between base stations due to mobility, which requests re-authentication to select only one base station among multiple base stations. They introduce the notion of tokens. Each mobile user has exactly one token including the identity and the other information. When the mobile user moves between base stations, its token goes along with the user. In [24], authors exploit the Kerberos authentication model and consider the network operator as a trusted third party that grants authentication to legitimate users and allows authentication between each communicating users. In [25], their solution is another method using public key cryptography within the Kerberos ticket framework. In [26], authors proposed, based on the tree-based group Diffie Hellman protocol, several group key agreement protocols for a dynamic communication group in a distributed fashion to join and leave the group at any time. In [27], their solution is a SIM-based subscriber authentication mechanism with detailed protocols for wireless LAN access networks. Based on this authentication mechanism, a mobile station with a GSM/GPRS SIM card can attach to WLAN access network to obtain services, without the need of presubscription to the WLAN access network.

3. Proposed distributed authentication mechanism for secure medical sensor networks

This section describes the proposed authentication mechanism. We basically adopt mobile devices including SIM (Subscriber Identity Module) or USIM (Universal Subscriber Identity Module) card. It is beneficial to use a SIM or a USIM card to save memory, because some materials such as key, A3 algorithm and A8 algorithm are pre-loaded in these cards. A3 Algorithm is used to encrypt Global System for Mobile Communications (GSM) cellular communications. In practice, A3 and A8 algorithms are generally implemented together (known as A3/A8). An A3/A8 algorithm is implemented in SIM cards and in GSM network Authentication Centers. It is used to authenticate the customer and generate a key for encrypting voice and data traffic. We especially do not require an authentication server but the server system (e.g. hospital) can take the role as an authentication server instead for authentication process.

3.1. Assumptions and terminologies

We need several assumptions for our proposal.

- Mobile devices know the IDs of sensor nodes they can communicate with.
- Pairwise keys (K_{DB}) between bio-sensors and the primary device are preloaded when the system is setup.
- Pairwise keys (K_{SD1}, $K_{SD2}\ldots$) between the server system and candidate devices are preloaded when the system is setup.
- Candidate devices which can play the role of an intermediary interconnecting between sensor nodes and the server system are registered at the initialization stage.

Table 1
Terminologies for our Device Authentication mechanism

Terminologies	Description
$\mathrm{Enc}_K(\mathrm{M})$	Encrypt message M with key K
ID_{temp}	Temporal ID for replacing real identities with artificial pseudonyms
K_{SD}	Pairwise key between server system and devices
K_{DB}	Pairwise key between device and biosensor nodes
K_i	Key i in SIM/USIM
a_1, $\mathrm{a}_2 \ldots$	Seeds for hash
N_1, $\mathrm{N}_2 \ldots$	Random numbers
RES	Response value of devices and server system
A3, A8	algorithms for authentication and key generation
primary device	the device having the responsibility of delivering bio-data from sensor nodes to server system
secondary device	the device which takes the responsibility instead when primary device cannot deliver bio-data for some period
candidate devices	candidates for secondary devices

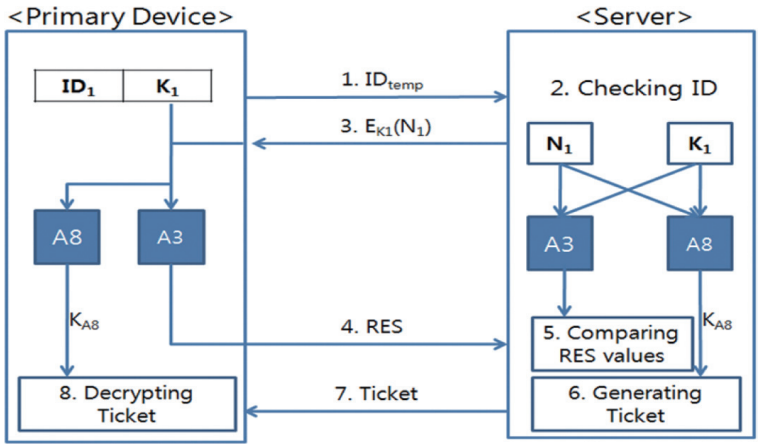

Fig. 2. User Authentication Phase in MSN.

– More than one secondary device need to be registered for the temporary channel establishment at the setup stage.
– A personal mobile phone is assumed to be the Primary device, and secondary devices could be the mobile phones of neighborhoods or home gateway in case that the patients reside at home.
– All primary and candidate devices keep the A3/A8 algorithms.

Terminologies are shown in Table 1.

3.2. Distributed authentication mechanism for primary device

In this process, user authentication is performed in the mobile phone, so that only a legal user can use the service. Figure 2 shows the simplified process of our proposed authentication mechanism based on SIM-based subscriber authentication mechanism [27].

It is necessary to authenticate the user using a mobile phone. When the system is initialized, the primary device is decided, and the server requests the primary device to start the authentication process. And the procedure is as follows:

1. The primary device sends a temporal ID (ID_{tmp}) that is preloaded in the device to assure user anonymity. Only the device and the server know the temporal IDs and outsiders do not know who is sending data.
2. When the server receives a temporal ID, it finds out the corresponding key, K_1.
3. The server generates a nonce (N_1) and encrypts it with the key (K_1) and sends it to the device.
4. The primary device decrypts data with the key, K_1 that is loaded in the SIM/USIM and obtains the nonce. Using the key, K_1 and the nonce, N_1, the device computes RES value using A3 algorithm. In addition, primary computes the A8 algorithm with the key, K_1 and the nonce, N_1. The server also computes the RES value using A3 algorithm and A8 algorithm with the key and the nonce, N_1. The primary device sends the RES to the server.
5. The server compares the RES sent from a primary device and the result computed by the A3 algorithm. It is impossible for any attacker to compute the correct RES, because s/he does not know the nonce or the key.
6. After the user authentication, the server issues tickets to legal users. A ticket includes device IDs, seeds for hash, and timestamps. The ticket is encrypted with a key generated from the A8 algorithm.

$$\text{Ticket} = \text{Enc}_{KA8}(\text{ID}_i, \text{a}_i, \text{Timestamp})$$

7. The server sends the ticket to the primary device.
8. The primary device decrypts the ticket with the key from the A8 algorithm.

Only registered users can send the data using these processes, as shown in Fig. 2.

After user authentication process is finished, patient's physiological data are sensed by bio-sensors and sent to the primary device. The data are encrypted with the pair wise key (K_{SD}) between the sensor and the device to protect data from malicious attacks.

The IDs of sensors are also sent with data to prevent sensors from sensing another person's bio-data. The form of transmitted data is

$$\text{ID}_{sensor}||\text{E}_{KSD}(\text{biodata}).$$

Once a device receives data, it checks the IDs that are transmitted from sensors first. If the sensor ID is not on the list, it considers the data as malicious or erroneous ones and discards them. After confirming the authenticity, the device decrypts data using the preloaded key (K_{SD}).

When devices receive data from several sensors, they perform data aggregation. According to the aggregation period, aggregated medical data are delivered to the server system.

3.3. Distributed authentication mechanism for secondary channel establishment

Even if the primary device is managed well, it can be discharged or missing. In some cases, they can be malfunctioning. In these abnormal cases, they cannot deliver the medical data to the server system. Unfortunately, even if the patient's condition goes bad, the server system cannot cope with this situation immediately if the medical data are not delivered by the intermediary devices. To deal with this unusual case, extra devices should be registered to play the role of the intermediary device in the abnormal situation.

We classify this situation in two cases. One is when the primary device notifies that it cannot accomplish the process sooner or later. In this case, the authentication process is relatively simple. The other case is when the primary device becomes unavailable without any notification in advance. The authentication process in this case is more complex than the former one.

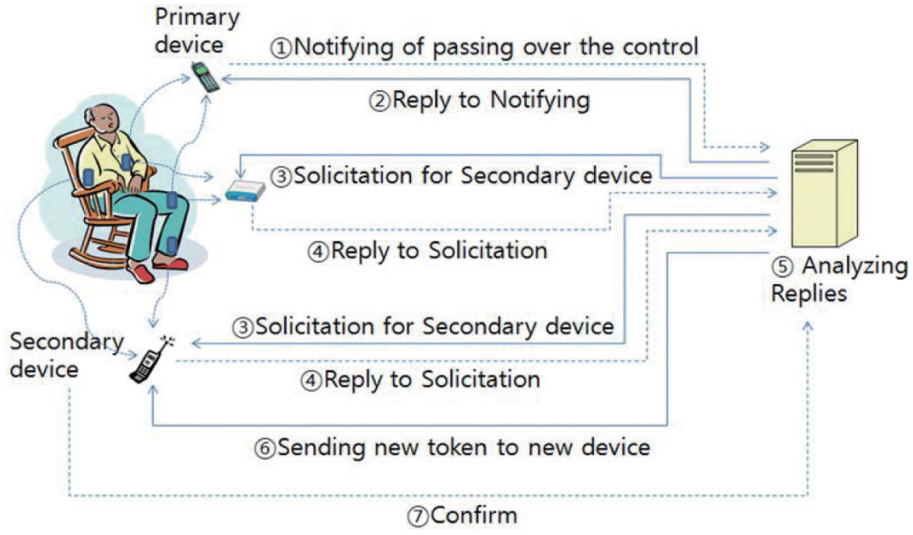

Fig. 3. Distributed Authentication mechanism for Secondary device channel establishment.

1. When the primary device notifies the abnormal situation to server system
In this case, the primary device sends a warning message to the server for the primary device to move the control to the new intermediary device. Only one intermediary keeps the control in the form of a token, which means that the only one authenticated device keeping the token can deliver the medical data to the server system. The distributed authentication process is as follows:

① Primary device informs the server that it cannot function as the intermediary for some reasons.
② Server system replies to this information.
③ Server system sends out solicitation to the candidate device to take the role of an intermediary device for certain time period.
④ Candidate device receiving this message gather the bio-data from sensor nodes for certain time interval, and reply to the solicitation from the server system.
⑤ Server system analyzes the replies and decides one candidate.
⑥ Server system generates the new token including the security information and sends it to the new intermediary.
⑦ New intermediary confirms this message.
⑧ Communication starts.

Figure 3 describes these processes.

Case 2: When the server system does not receive the medical data from the primary device without any notification from the device
In this case, the primary device may be missing, discharged or malfunctioning. Compared with Case 1, the server system needs to check if the primary device is in problem or the function can be accomplished again soon. If the server decides that the primary device cannot deliver the bio-data anymore, a secondary device needs to be chosen and to take the responsibility immediately. The server sends out Request messages to Candidate devices to be the temporary device for delivering medical data. The process is as follows:

① When server finds that the primary device is not available anymore, Server system sends out REQUEST messages to Candidate devices which have been registered at the initialization phase.
② Among the devices that have been registered as Candidates, available devices reply with REPLY message with the information that how many sensor nodes they can listen to.
③ Server system chooses one of them as secondary device based on the choice criteria.
④ Server system generates a new token for the temporary Secondary device, and sends it to the new device.
⑤ When receiving the message, the new device replies with a confirm message.
⑥ Temporary channel is established and communication starts.
⑦ Server system sends a request message to the primary device periodically for the primary device to get back to the proper function.
⑧ When Server system gets the REPLY message from the Primary device, the server sends the notification message to Secondary device to inform that the temporary transmission session is over. It generates a new token for the original device and sends it to the Primary device.
⑨ Secondary device sends the REPLY message to Server System.

Processes ⑦ $\sim$ ⑨ are common for Case 1 and Case 2 after the temporary communication channel is established. In case 1 and 2, pairwise keys between the new intermediary device and sensor nodes need to distributed again in the token before the secondary device starts working as an intermediary. The token format is as follows:

Token Format:

$$\mathbf{Enc}_{KSD2}(\mathbf{K}_{DB1}||\mathbf{K}_{DB2}||_{...}||\mathbf{K}_{DBn})||\mathbf{Enc}_{KSD2}(\mathbf{Timestamp}||\mathbf{Certificate})$$

3.4. Monitoring process of server system according to intermediary device functional ability

In our system infrastructure over MSN, intermediary devices can be active or passive according to the functional ability as the device in the middle. When the device has more functional abilities such as monitoring sensor nodes and aggregation of sensed data, it can react more actively in the case of no data from sensor nodes. For example, when the device finds out that some sensor nodes do not send bio-data for the time being, it can report this to the server system that could manage this situation, i.e., the offline operation. The intermediary device with more technical abilities can screen the traffic between the server and itself. For example, in some cases, there could be more messages from sensor nodes to server, whereas no or less messages could be generated in the other situation. By monitoring these traffic amounts, some attackers can guess the status of patients or the number of patients being taken care of. To prevent this kind of passive attack, the device can generate null messages even if there is no data from sensor nodes. When the device has advanced functional abilities, it can monitor the sensor nodes and notify the sensor nodes status to the server system. However, even when the intermediary device has these functions, it cannot cope with the situation such as malfunction or theft. Process in Case 2 is required in these unavoidable situations.

When the device does not have advanced functions, it just relays the bio-data from sensor nodes to the server system. In this case, the server system needs to monitor the behavior of the intermediary device and sensor nodes. When sensor nodes do not send the bio-data to the intermediary device, the server can catch this situation and react if required, because the server system can observe every message generated.

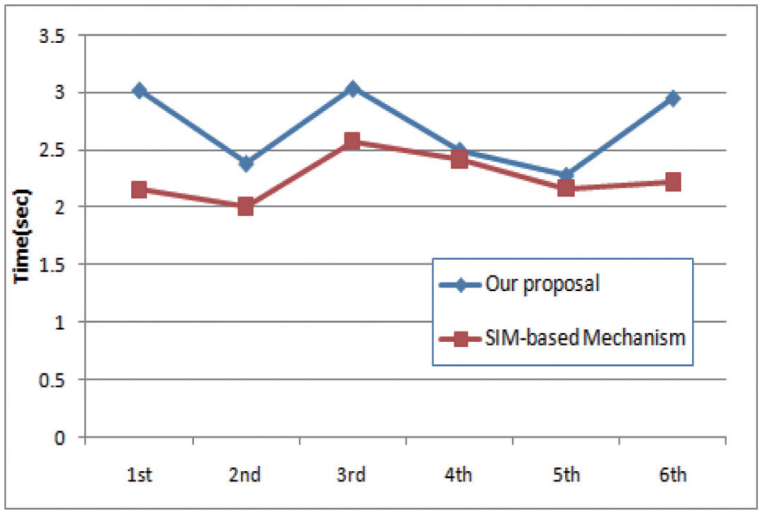

Fig. 4. Comparison of Time for user authentication between SIM-based mechanism and our Proposal.

When the server finds out that there is no data from the intermediary device, the server checks the device if it is alive, and if not, Case 2 process needs to be progressed. When the intermediary device replies to the server and the server decides that there is no problem with the device, the offline management process for the bio-sensor nodes is required.

4. Performance and security analysis

SIM-based scheme [23] and the proposed scheme perform the user authentication using the A3 algorithm. However, our proposed scheme offers the security by encrypting the ticket with a key generated from the A8 algorithm. Mobile devices use tickets and temporary IDs to support the user anonymity and the privacy in the proposed scheme. Figures 4 and 5 show the comparison of time and energy consumption of our proposal and SIM-based mechanism. Our proposal takes a little longer and consumes a bit more energy. However, it is not significant difference. In addition, we can further provide the security for IDs, seed numbers for Hash, and timestamps.

Figure 4 shows the time difference between SIM-based mechanism and our proposal. It shows that our proposal takes a bit longer than SIM-based mechanism because ours takes time for encrypting the token and checking the temporary IDs. However, the user authentication is required only when new device needs to start function at the beginning stage, and in addition to the fact, the difference is less than 1 second. On the average, it is about 0.3 second, and is ignorable.

Figure 5 shows the energy difference between SIM-based mechanism and our proposal. It also shows that the energy consumption is not significant either considering the user authentication is required only once when the device should be authenticated by the server system.

Table 2 shows that security comparison between SIM-based mechanism and our proposal. As shown in the table, both mechanisms provide user authentication. However, the replay attack is possible in the SIM-based scheme, which is, if an attacker captures encrypted data and sends them repeatedly to the server later, the server has to expend resources to decrypt the data. This kind of attack is impossible in proposed mechanism. In addition, ID is not disclosed in the mechanism, because we use temporal IDs. Man in the middle attack is also impossible in proposed mechanism.

Table 2
Security comparison between SIM-based mechanism and our proposal

Security issues	SIM-based mechanism	Our proposal
User authentication	Provided	Provided
ID anonymity	Not provided	Provided
Replay attack	Possible(Not Safe)	Impossible(Safe)
Man in the middle attack	Possible(Not Safe)	Impossible(Safe)
Transmitted data form	nonce in plaintext	encrypted nonce

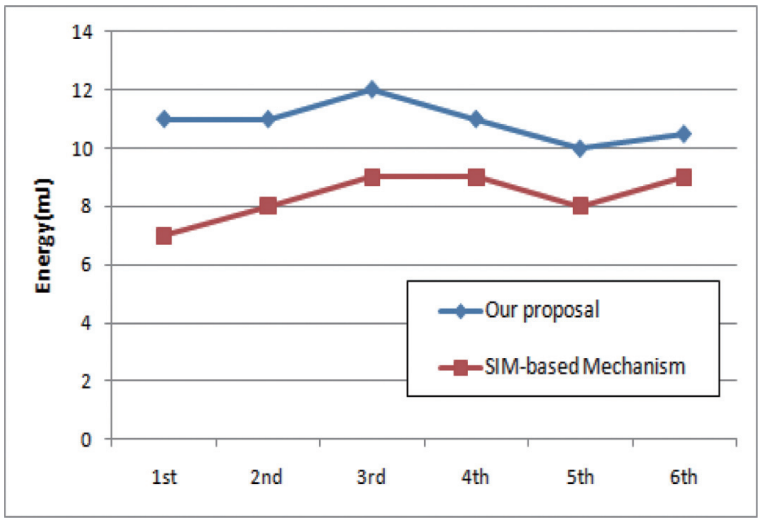

Fig. 5. Comparison of Time for user authentication between SIM-based mechanism and our Proposal.

More important contribution of our proposal is that it provides the replacement processes for the secondary device when the primary device cannot function for some reasons. However, it is difficult to prove its superiority because there is no such a mechanism. In Fig. 3, proposed mechanism requires about 6 message exchanges between the server system and the candidate devices. And the processes are safe enough to distribute symmetric keys for the new device and bio-sensor nodes because the messages are encrypted with keys between the server system and the new intermediary device.

5. Conclusion

MSN has the great importance in our ubiquitous computing environment. It will be adopted in various home and hospital environment. In this paper, we propose a distributed device authentication mechanism for MSN. It does not require the authentication server, but the server system in hospital or Health care center plays the role as the authentication server. Mobile devices or home gateways function as the intermediary devices between the server system and the bio-sensors attached on patients. They gather the bio-data from sensor nodes and deliver the data to server system. However, because the devices are usually mobile and have constraints, they can be discharged, missing, or malfunctioning. In this situation, bio-data from patients cannot be delivered to the server system, and it could cause the serious problem. We adopted candidate devices, which are deployed near the patient, and registered at the initialization stage. When the original device cannot function properly, one of the candidate devices

takes the responsibility and plays the role as the intermediary after the authentication processes. Our mechanism is efficient and safe without considerable overhead compared to other mechanisms.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MEST)(NO. R01-2009-0083-985).

References

[1] B. Latre, B. Braem, I. Moerman, C. Blondia and P. Demeester, A survey on wireless body area networks, *Journal of Wireless Networks* **17**(1) (January 2011).
[2] A.J. Jara, M.A. Zamora and A.F.G. Skarmeta, An Initial Approach to Support Mobility in Hospital Wireless Sensor Networks based on 6LoWPAN (HWSN6), *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* **1**(2/3) (2010), 107–122.
[3] A. Durresi and M. Denko, Advances in wireless networks, *Journal of Mobile Information Systems* **5**(1) (Apr 2009), 1–3.
[4] M. Kuroda Y. Tamura, R. Kohno and O. Tochikubo, *Empirical evaluation of zero-admin authentication for vital sensors in body area networks*, 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 2349–2352, 2008. EMBS 2008.
[5] G.H. Zhang, C.C.Y. Poon and Y.T. Zhang, A fast key generation method based on dynamic biometrics to secure wireless body sensor networks for p-health, 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 2034–2036, 2010.
[6] E.M. Shakshuki, X. Xing and T.R. Sheltami, Fault reconnaissance agent for sensor networks, *Journal of Mobile Information Systems* **6**(3) (Sep 2010), 229–247.
[7] W. Wu, X. Li, S. Xiang, H.B. Lim and K. Tan, Sensor relocation for emergent data acquisition in sparse mobile sensor networks, *Journal of Mobile Information Systems* **6**(2) (Sep 2010), 155–176.
[8] S. Mahfoudh and P. Minet, Maximization of energy efficiency in wireless ad hoc and sensor networks with SERENA, *Journal of Mobile Information Systems* **5**(1) (Apr 2009), 33–52.
[9] F.M. Bui and D. Hatzinakos, Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling, EURASIP Journal on Advances in Signal Processing, 2008.
[10] K. Venkatasubramanian, A. Banerjee and S.K.S. Gupta, EKG-based Key Agreement in Body Sensor Networks, The Second Workshop on Mission Critical Networks, IEEE, 2008.
[11] K.K. Venkatasubramanian and S.K.S. Gupta, Physiological value-based efficient usable security solutions for body sensor networks, *Transactions on Sensor Networks* (*TOSN*) **6**(4) (July 2010).
[12] C.C.Y. Poon, Y.T. Zhang and S. Bao, A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health, *IEEE Communications Magazine* **44**(4) (2006), 73–81.
[13] K. Malasri and L. Wang, Addressing security in medical sensor networks, Proceedings of the 1st ACM SIGMOBILE International workshop on Systems and networking support for healthcare and assisted living environments, 7–12, 2007.
[14] N. Challa, C. Hasan and S. Madhur, *Secure and Efficient Data Transmission over Body Sensor and Wireless Networks*, EURASIP Journal on Wireless Communications and Networking, 2008.
[15] M. Li, S. Yu, W. Lou and K. Ren, Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks, *Proceedings of IEEE INFOCOM* (2010), 1–9.
[16] C.C. Tan, H. Wang, S. Zhong and Q. Li, Body sensor network security: an identity-based cryptography approach, *ACM Conference on Wireless Network Security* (*WiSec*) (2008), 148–153.
[17] M.M. Haque, A.K. Pathan and C.S. Hong, *Securing U-Healthcare Sensor Networks using Public Key Based Scheme*, IEEE ICACT, 2008.
[18] M. Guennoun, M. Zandi and K. El-Khatib, *On the use of biometrics to secure wireless biosensor networks*, 3rd International conference on information and communication technologies: Fromtheory to applications (ICTTA 2008), Apr. 2008.
[19] M.R. Kanjee, K. Divi and H. Liu, *A Physiological Authentication Scheme in Secure Healthcare Sensor Networks*, 7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (SECON), pp. 1–3, 2010.
[20] S. Bao, Y. Zhang and L. Shen, *Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems*, 27th Annual International Conference of the Engineering in Medicine and Biology Society, pp. 2455–2458, 2005.

[21] A. Boonyarattaphan, Y. Bai and S. Chung, A security framework for e-Health service authentication and e-Health data transmission, 9th International Symposium on Communications and Information Technology, pp. 1213–1218, 2009.
[22] F. Al-Nayadi and J.H. Abawajy, *An Authentication Framework for e-Health Systems*, 2007 IEEE International Symposium on Signal Processing and Information Technology, pp. 616–620, 2007.
[23] S. Machiraju, H. Chen and J. Bolot, *Distributed Authentication for Low-Cost Wireless Networks*, Proceedings of the 9th workshop on Mobile computing systems and applications, pp. 55–59, 2008.
[24] H. Moustafa, J. Forestier and M. Chaari, *Distributed authentication for services commercialization in ad hoc networks*, Proceedings of the 6th International Conference on Mobile Technology, Application & Systems, 2009.
[25] M.A. Sirbu and J.C. Chuang, Distributed Authentication in Kerberos Using Public Key Cryptography, sndss, p. 134, 1997 Symposium on Network and Distributed System Security, 1997.
[26] P.P.C. Lee, J.C.S. Lui and D.K.Y. Yau, Distributed collaborative key agreement and authentication protocols for dynamic peer Groups, *IEEE/ACM Transactions on Networking* **14**(2) (Apr 2006), 263–276.
[27] Y. Tsai and C. Chang, *SIM-Based Subscriber Authentication Mechanism for Wireless Local Area Networks*, Computer Communications, pp.1744-1753, 2006.

Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995–1998, she worked in Samsung SDS of Korea to develop a marketing system. She undertook a post doctoral program at Seoul National University during 2007 and 2008. She is currently a research professor of Computer Science and Engineering at Ewha Womans University, Seoul. Her research interests include sensor network security, home network security, Wimax, wireless network security, and medical sensor networks.

Jiyoung Lim received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1994 and 1996, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2001. She worked for Computer Science and Engineering at Ewha Womans University from 2001 to 2002 and is currently an assistant professor of Computer Software at Korean Bible University, Seoul. Her research interests are in sensor network security, home network security, mobile wireless networking and medical sensor networks.

Kijoon Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D degree in Electrical and computer engineering from North Carolina State University in 1990. He is currently a professor of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include network security, sensor network, network protocol design and performance evaluation.