International Journal of Control and Automation
Vol. 9, No. 9 (2016), pp.129-138
http//dx.doi.org/10.14257/ijca.2016.9.9.13

Security Remarks on Secure Authentication Scheme for Remote Health Monitoring System using WBAN

Sung Woon Lee[1] and Hyunsung Kim [2,3]

[1] *Dept. of Information Security, Tongmyong University*
Busan 608-711, Korea
[2](Corresponding Author) *Dept. of Cyber Security, Kyungil University*
Kyungsan, Kyungbuk 712-701, Korea
kim@kiu.ac.kr
[3]*Dept. of Mathematical Sciences, Chancellor College, University of Malawi*
P.O.Box 280, Zomba, Malawi

Abstract

To provide secure authentication for wireless body area networks (*WBANs*), *recently Mtonga proposed a scheme based on identity-based cryptography, bilinear pairing and non-interactive identity-based key agreement scheme. He argued that his scheme provides authenticated key agreement, privacy preservation and authenticity, integrity and freshness of transmitted health messages. Unfortunately, this paper provides security remarks on Mtonga's scheme focused on lack of integrity provision, lack of untraceability and masquerading attack feasibility. They are very important aspects in a system's required security and privacy features. Furthermore, this paper provides simple directions of the counterpart's solutions on them.*

Keywords*: Wireless body area network, information security, authentication, bilinear pairing, non-interactive identity-based key agreement*

1. Introduction

Recent technology advances in integration and miniaturization of physical sensors have enabled a new generation of wireless body area networks (WBANs) [1-3]. One of the most important uses of WBANs is ubiquitous healthcare application to monitor patient remotely [4-10]. Sensor node can be placed on the human body to collect patient's health information (PHI) that is called medical body area network (MBANs) [4-5]. Remote monitoring based on MBANs allows an individual's PHI to be collected and sent to the remote healthcare center, where physician can be able to review the data remotely. Even if various benefits could be provided for the patient, remote monitoring system leaves patient's PHI highly vulnerable [11-13]. Thereby, the most important challenge in remote monitoring system is how to ensure the patient privacy during and after transmission of PHI to avoid the threat from attackers.

Many researchers have been proposed mechanisms to provide privacy and security in remote health monitoring systems over WBAN [14-18].Huang *et al*. in [14] proposed an identity-based authentication and context privacy preservation scheme in wireless health monitoring system does not achieve anonymity of patient and is furthermore weak against password guessing attack. Laymouni *et al.* proposed a privacy protection protocol for remote monitoring system, which uses both of symmetric cryptosystem and asymmetric cryptosystem, especially RSA algorithm [15]. Jian *et al.* proposed a location privacy routing protocol (LPR) to achieve path diversity [16]. By combining LPR with fake packet injection, the location privacy of the receiver can be protected, and subsequently, the contextual

ISSN: 2005-4297 IJCA

privacy is achieved. Similar to [16], Lin *et al*. in [17] deal with the contextual privacy also from protecting the receiver's location privacy. They proposed a strong anti-wiretapping privacy protection system which used the identity-based cryptography (IBC) to encrypt data based on Diffie-Hellman problem, verify the information sent by the patient through the digital signature, and applied the broadcast mechanism for the global network eavesdropping to achieve the objective of protecting patient privacy. Recently, Mtonga proposed secure authentication scheme for remote health monitoring system using WBAN [18]. Mtonga's work was focused on to providing security and privacy during the transmission of messages outside of the WBAN, which is based on IBC and aimed to be secured against eavesdropping attack, identity and tracing attack, impersonation attack, replay attack, data modification attack, denial of service attack and physical tampering attack.

There are two purposes of this paper: one is to show security weaknesses in Mtonga's authentication scheme and the other is to provide research direction in brief to solve the problems in Mtonga's scheme. First of all, this paper shows three weaknesses Mtonga's authentication scheme focused on lack of integrity provision, lack of untraceability and masquerading attack feasibility. Then, this paper will also provide future research directions in brief to give a proper direction of the research.

The rest of this paper is organized as follows. In Section 2, network configuration is provided for the understanding of the environment over WBAN. Mtonga's secure authentication scheme for remote health monitoring system using WBAN is reviewed in Section 3. In Section 4, we provide security remarks on Mtonga's scheme. Section 5 concludes the paper with the direction of future works.

2. Network Configuration

The network environment for Mtonga's scheme has three main parties as shown in Figure 1, which is a bit more revised for the better understanding on the environment ; patient with WBAN, health monitoring center (HMC) with electronic health record (EHR) and physician [18].

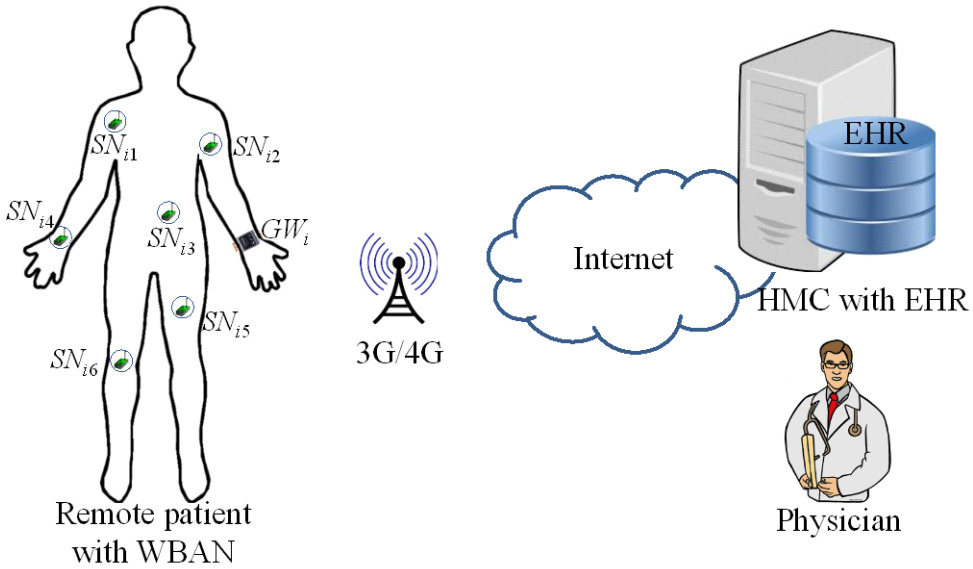

Figure 1. Remote Health Monitoring System Configuration

WBAN is defined by IEE 802.15 as a communication standard optimized for low power devices and operation on, in or around the human body. WBAN has many applications such as health monitoring, sports and fitness monitoring and so on. They have unique requirements in terms o bandwidth, latency, power usage and signal distance. Thereby, health monitoring system over WBAN also satisfies those requirements. A WBAN consists of multiple sensor nodes, which has functionalities of sensing, processing and communicating. In remote health monitoring system, WBAN enables pervasive, long-term, and real-time health management for patient. Main roles of each participant are as follows

- Patient : Patient's network is consisted with two parts, WBAN part and personal server part with smart phone or smart watch. WBAN nodes are either attached to or implanted into the patient's body and have communication capability. Personal server has more memory, processing and communication capabilities than the WBAN nodes. It collects vital signs from WBAN nodes after filtering redundant data from the nodes. It works as an end point of patient in the communication viewpoint.
- EHR (or HMC) : EHR keeps electronic medical records of registered patients and provides various services to patients, medical personnel and informal caregivers. EHR needs to have responsibility of authentication of patients and patients, accept health monitoring session uploads from patients and physicians, format and insert session data into corresponding medical records and forwards new instructions to patients.
- Physician : Physician can access his enrolled patients data from EHR, examine it to ensure patients health condition and provide proper treatment based on the collected PHI information directly to the patient if the examination of patient's data is imminent danger or indirectly vis EHR if it is not in urgent situation.

3. Mtonga's Secure Authentication Scheme for Remote Health Monitoring System using WBAN

This section reviews Mtonga's secure authentication scheme for remote health monitoring system using WBAN [18]. Mtonga's authentication scheme is consisted with six phases: system initialization, registration, physician selection, PHI transfer to EHR, patients authentication and PHI receiving and storing by EHR and PHI request and recovery by physician.

3.1. System Initialization

This phase is run by HMC. Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of prime order q. Let P be a generator of $G_1$and $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$be a pairing satisfying the properties as above. HMC chooses a random number $s \in Z_q^*$ as the master secret key and computes the corresponding public key $P_{pub}=sP$. It chooses two hash functions $H_1(\,):\{0, 1\}^* \rightarrow G_1^*$ and $H_2(\,):\{0, 1\}^* \rightarrow Z_q^*$. It computes the public key $Q_{EHR}=H_1(id_{EHR})$ and corresponding private key $d_{EHR}=sH_1(id_{EHR})$for EHR. The key pair {,} is sent to EHR via a secure channel. HMC publishes { G_1, G_2, $\hat{e}$, q, P, P_{pub}, $H_1(\,)$, $H_2(\,)$ } as public parameters.

3.2. Registration

All registrations are carried out by HMC via a secure channel. It is assumed that all remote health monitoring communications among patient, EHR and physician are carried over an insecure channel. To register, patient PT_i submits his/her real identity id_{PTi} to HMC. After receiving the identity, HMC processes the following

(1) Validates the received identity id_{PTi}.
(2) Computes PT_i's private key $d_{PTi}=sH_1(id_{PTi})$.

(3) Sends d_{PTi} to PT_i through a secure channel.

When physician D_l registers to HMC with id_{Dl}, HMC works as follows

(1) Validates the received identity id_{Dl}.
(2) Computes D_l's private key $d_{Dl}=sH_1(id_{Dll})$.
(3) AddsD_l into the list of registered doctors.
(4) Sends d_{Dl} to D_l through a secure channel.

3.3. Physician Selection

To allow patients selection of a physician of their choice, HMC publishes a list of certified physician on its portal. Once patient chooses physician of his/her choice, with help of HMC a contract is established between the patient and selected physician, in which the patient grants rights to the physician to monitor his/her body sensors remotely. With the protection of the contract, the patient and the physician can communicate securely. The steps that PT_i follows to successfully establish a contract with D_l are as follows

(1) To initialize the process, PT_i chooses a pseudo identity pid_{PTi}, of his/her choice and forms a message $M=T||id_{PTi}||id_{HMC}||id_{Dl}||t||pid_{PTi}$, encrypts it as $C_{req}=E(SK_{PTi\text{-}HMC}, M)$ and sends { id_{PTi}, id_{HMC}, T, C_{req} } to HMC via a secure channel. Here $SK_{PTi\text{-}HMC}=\hat{e}(d_{PTi}, H_1(id_{HMC}))$, T is the time stamp and t is the period the patient wants to be monitored. Here t can also be considered as the expiry date of the contract, hence allowing for revocation of service subscription by HMC.
(2) After receiving { id_{PTi}, id_{HMC}, T, C_{req} }, HMC first uses id_{PTi} to compute $SK_{HMC\text{-}PTi}=\hat{e}(d_{HMC}, H_1(id_{PTi}))$, decrypts C_{req} to recover M and checks its freshness, authenticity and integrity. Further, HMC checks validity of id_{PTi} and id_{Dl}. If they are valid, HMC establishes a contract between id_{PTi} and id_{Dl}, in which PT_i grants D_l rights to monitor his/her body sensors. Finally, HMC adds t to $pid_{PTi}=pid_{PTi}||t$ and computes contract key as $K_{PTi}=sH_1(pid_{PTi}||t)$.
(3) HMC forms $M'=pid_{PTi}||id_{Dl}||id_{HMC}||T||K_{PTi}$, encrypts it as $C_{resp}=E(SK_{HMC\text{-}PTi}, M')$ and sends { id_{HMC}, pid_{PTi}, T, C_{resp} } to PT_i.
(4) At the same time, HMC forms $M''=id_{HMC}||id_{Dl}||T||t||pid_{PTi}$, encrypts it as $C_{agree}=E(SK_{HMC\text{-}Dl}, M'')$ and sends { id_{HMC}, id_{Dl}, T, C_{agree} } to D_l.
(5) Upon receipt of { id_{HMC}, id_{Dl}, T, C_{agree} }, PT_i decrypts C_{resp} to recover the message M' and checks its freshness, authenticity and integrity. If they hold, PT_i stores K_{PTi} to use later.

After receiving { id_{HMC}, id_{Dl}, T, C_{agree} }, D_l decrypts C_{agree} to recover the message M'' and checks its freshness, authenticity and integrity. If they hold, D_l stores pid_{PTi} on his/her patient list.

3.4. PHI Transfer to EHR

To send PHI to EHR, PT_i carries out the following steps

(1) Takes his pseudo identity pid_{PTi} and the corresponding contract key K_{PTi}.
(2) Computes a session key by using the contract key as $SK_{PTi\text{-}Dl}=\hat{e}(K_{PTi}, H_1(id_{Dl}))$.
(3) Computes $R=T_{PTi}\cdot SK_{PTi\text{-}Dl}$, where T_{PTi} is current time stamp.
(4) Performs IBC-encryption as $C_1=E(SK_{PTi\text{-}Dl}, M||T_{PTi}||R||pid_{PTi})$, where M is PHI and computes the signature$\sigma_{PTi}=H_2(C_1)\cdot K_{PTi}$ on C_1.
(5) Sends { T_{PTi}, pid_{PTi}, C_1, σ_{PTi}, id_{Dl} } to EHR.

3.5. Patients Authentication and PHI Receiving and Storing by EHR

When EHR receives the message { T_{PT_i}, pid_{PT_i}, C_1, σ_{PT_i}, id_{D_l} } from PT_i, it carries out the following authentication steps

(1) Checks if T_{PT_i} satisfies $T_{PT_i\text{-}last}$-$T_{PT_i} \leq \Delta T$, where $T_{PT_i\text{-}last}$ is last time of message receipt by EHR and is fixed time interval between successive PHI collections. If successful, it proceeds to examine the expiry date included in pid_{PT_i} to verify the service expiration time.

(2) Using public parameters and received values, EHR checks the validity of the signature by computing $\hat{e}(\sigma_{PT_i}, P)=\hat{e}(H_2(C_1)\cdot H_1(pid_{PT_i}), P_{pub})$. Once the computation satisfies, EHR accepts the message as authentic and stores the necessary message components. EHR can either notify the respective D_l of the received PHI or may wait for a message request from D_l.

3.6. PHI Request and Recovery by Physician

To access a patient's PHI, D_l sends a request to EHR by following the steps

(1) Carries out IBC-encryption as $C_2=E(Q_{EHR}, T_{D_l}||id_{D_l}||pid_{PT_i})$ and computes the signature $\sigma_{P_l}=H_2(C_2)\cdot d_{D_l}$.

(2) Sends { T_{D_l}, C_2, σ_{D_l}, id_{D_l}, pid_{PT_i} } to EHR as request for a patient's PHI.

Once EHR receives the message { T_{D_l}, C_2, σ_{D_l}, id_{D_l}, pid_{PT_i} } from D_l, it carries out the following steps

(1) Validates the timestamp T_{D_l} by checking if the in equality T'-$T_{D_l} \leq \Delta T$ holds, where T' is the time of arrival of the request.

(2) Decrypts as $\{T_{D_l}||id_{D_l}||pid_{PT_i}\}=D(d_{EHR},C_2)$.

(3) Using id_{D_l} and public parameters, EHR validates the received signature by computing $\hat{e}(\sigma_{D_l}, P)=\hat{e}(H_2(C_2)\cdot H_1(id_{D_l}), P_{pub})$.

(4) Forwards the message { pid_{PT_i}, C_1, id_{D_l} } to D_l.

To recover M, D_l carries out the following steps

(1) Computes $SK_{D_l\text{-}PT_i}=\hat{e}(d_{D_l}, H_1(pid_{PT_i}))$, where physician could precompute $SK_{D_l\text{-}PT_i}$ by using his patient list.

(2) Performs decryption onC_1 as, $\{M||T_{PT_i}||R||pid_{PT_i}\}=D(SK_{D_l\text{-}PT_i},C_1)$.

(3) To check freshness of M, the physician makes use of R, P, R_{pub} and T_{PT_i} to compute the pairing $\hat{e}(R, P)=\hat{e}(H_1(pid_{PT_i}), P_{pub})^{T_{PT_i}}$.

If the pairing holds, the physician believes that the received PHI if fresh ad can now analyze M so as to give necessary and timely medical advice to PT_i. By checking T_{PT_i}, D_l is able to tell when the information was sent by PT_i. This can help him/her to estimate a patient's health condition sine the time the data was collected by biomedical devices. To send medical advice M_{advice} to PT_i in response to the received PHI, D_l carries out the following steps

(1) Compute $auth=H_2(SK_{D_l\text{-}PT_i}||pid_{PT_i}||id_{D_l})$.

(2) Encrypts M_{advice} using $SK_{D_l\text{-}PT_i}$ as $C_3=E(SK_{D_l\text{-}PT_i}, M_{advice}||T_{D_l}'||auth)$.

(3) Sends { T_{D_l}', $auth$, C_3 } to PT_i.

Upon receiving { T_{D_l}', $auth$, C_3 }, PT_i proceeds as follows

(1) Validates timestamp to overcome replay attacks.

(2) Computes verification code $veri=H_2(SK_{PT_i\text{-}D_l}||pid_{PT_i}||id_{D_l})$ and checks if $veri=auth$ holds. If the equation holds, PT_i believes that the message is from legitimate D_l and that he/she has established a secure channel.

(3) Decrypts C_3 using $SK_{PT_i\text{-}D_l}$ as $\{M_{advice}||T_{D_l}'||auth\}=E(SK_{PT_i\text{-}D_l}, C_3)$ and act upon the medical advice.

4. Security Weaknesses and Remarks on Mtonga's Scheme

This section provides cryptanalyses and simple solutions on Mtonga's secure authentication scheme for remote health monitoring system using WBAN in [18], which has lack of security and design considerations. It does not provide integrity of message and untraceabilility on patient's point of view and is weak against masquerading attack.

4.1. Lack of Integrity Provision

Integrity deals with methods that ensure the contents of a message have not been tampered with and altered. Integrity checking is one of important components for the information security provision [19]. In physician selection phase, Mtonga argued that the phase provides integrity of message but actually it does not. PT_i sends { id_{PTi}, id_{HMC}, T, C_{req} } to HMC. After that, HMC sends { id_{HMC}, pid_{PTi}, T, C_{resp} } to PT_i and { id_{HMC}, id_{Dl}, T, C_{agree} } to D_l, respectively. Upon receipt of the message, it is argued that PT_i and D_l could decrypt the encrypted message and check its freshness, authenticity and integrity. However, there is no way to check integrity of the message by D_l and PT_i because it does not provide any integrity check method on the message.

The most common approach to provide integrity is to use oneway hash function that combines all the bytes in the message with a secret key and produces message authentication code (MAC) that is impossible to reverse. So, it is recommendable to add MAC in each message to use the hash function $H_2()$ by computing $MAC_i=H_2()$with both inputs of message and related secret keys. Thereby, the format of messages for D_l and PT_i should be changed from { id_{HMC}, pid_{PTi}, T, C_{resp} } and { id_{HMC}, id_{Dl}, T, C_{agree} } to { id_{HMC}, pid_{PTi}, T, C_{resp}, MAC_1 } and { id_{HMC}, id_{Dl}, T, C_{agree}, MAC_2 }, respectively, which are computed as $MAC_1=H_2(C_{resp})\cdot K_{PTi}$ to PT_i and $MAC_2=H_2(C_{agree})\cdot d_{EHR}$ to D_l. After that, the counterpart could check the integrity of the message as the same way from the patients authentication and PHI receiving and storing by EHR phase based on bilinear pairing operation. Otherwise, the hash function could use input with both of the message and the related secret key.

4.2. Lack of Untraceability

If a message transmission is untraceable, it should not be possible to determine where it came from or who did it. This implies a level of anonymity, in that you cannot name the entity which carried out the transaction. However, it may be possible to trace a transaction back to a certain identity without being able to name that identity. If system uses some suitable security mechanism, any entity could communicate with an entity in the system in a manner that is traceable in that they can be certain that it's the entity who sent the message, but it is anonymous because they do not know who the entity actually are [20]. Mtonga's scheme uses pseudonym to provide anonymity on each patient. In one sense a pseudonym provides anonymity as no one can uniquely identify an entity's real identity. But in another sense, having a known pseudonym is the opposite of anonymity as any entity have a name that uniquely identifies the entity within the group of all other pseudonyms. Mtonga's scheme uses pid_{PTi} for t, which is the period the patient wants to be monitored. Thereby, pid_{PTi} is not changed in the period of t at the PHI transfer to EHR phase and the patients authentication, PHI receiving and storing by EHR phase, which have a known pseudonym to attacker during t.

The most common approach to provide untraceability is to combine the use of pseudonym and random number different in each message. So, it is recommendable to use random numbers to make adversaries not to distinguish continuous sessions with the same pid_{PTi} in Mtonga's scheme.

4.3. Masquerading Attack Feasibility

Masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If n authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack [21]. Masquerade attack can be perpetrated normally using stolen passwords and logons, by locating gaps in programs, or finding a way around the authentication process. The attack can be triggered either by someone within the system environment or by an outsider if the system is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they have managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they have gained the highest access authority to a system. Personal attacks, although less common, can also be harmful. By finding a way around the authentication process, Mtonga's scheme is feasible against masquerading attack. For the attack, attacker just chooses a random number x, multiplies it to pid_{PT_i} and replaces $x \cdot pid_{PT_i}$ with any previous message's pid_{PT_i} within the time period of $T_{PT_i\text{-}last}$-$T_{PT_i} \leq \Delta T$. In the patient authentication, PHI receiving and storing by EHR phase, EHR checks the validity of the signature by computing $\hat{e}(\sigma_{PT_i}, P)=\hat{e}(H_2(C_1) \cdot H_1(pid_{PT_i}), P_{pub})$. Once the computation satisfies, EHR accepts the message as authentic and stores the necessary message components, which means that there is no way EHR checks the changes from attacker. Thereby, Mtonga's scheme is weak against masquerading attack.

It is not easy to cope from masquerading attack to an authentication scheme, which needs to design carefully. However, Mtonga's scheme just uses basic operation over bilinear pairing, which could be easily modifiable and make easily indistinguishable of original one from the faked one. Thereby, it needs to add some more information of patient's related secret to cope from the attack.

5. Conclusion

This paper has shown the security weaknesses in recent secure authentication scheme for remote health monitoring system using WBAN proposed by Mtonga, which does not provide integrity of message and untraceabilility on patient's point of view and is weak against masquerading attack. Furthermore, we provided solution directions on each weakness. This paper's remarks could be very helpful and useful to enhance the security and the privacy of remote health monitoring system based on WBANs, which are very critical part for the commercialization of the system.

For the future work, it is desirable to devise an uniform framework for the security and privacy for WBANs, which has basic subfunctions of authentication, confidentiality, integrity, access control, nonrepudiation, and privacy. However, the framework should consider various applications requirements. Thereby, it needs to be simplified at the very beginning and needs to be expanded by adding the required aspects from various entities on remote health monitoring system over WBAN.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575) and also was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2011-0008890).

References

[1] S. Shin, S. W. Lee and H. Kim, "Authentication Protocol for Healthcare Services over Wireless Body Area Networks", International Journal of Computer and Communication Engineering, vol. 5, no. 1, **(2016)**, pp. 50-60.
[2] H. Kim and S. W. Lee, "Authenticated Key Agreement Scheme with Forward Secrecy for Wireless Sensor Networks", International Journal of Control and Automation, vol. 8, no. 11, **(2015)**, pp. 279-288.
[3] I. F. Akyildiz, T. Melodia and K. R. Chowdhury, "A survey on wireless multimedia sensor networks", Computer Networks, vol. 41, no. 4, **(2007)**, pp. 921-940.
[4] H. Kim and S. W. Lee, "Freshness Preserving Secure Data Gathering Protocol over Wireless Sensor Networks", International Journal of Control Automation, vol. 8, no. 6, **(2015)**, pp. 411-420.
[5] R. Shahriyar, M. F. Bari, G. Kundu, S. I. Ahamed and M. M. Akbar, "Intelligent Mobile Health Monitoring System (IMHMS)", International Journal of Control and Automation, vol. 2, no. 3, **(2009)**, pp. 13-27.
[6] H. Kim, "Freshness-Preserving Non-Interactive Hierarchical Key Agreement Protocol over WHMS", Sensors, vol. 14, **(2014)**, pp. 23742-23757.
[7] D. Suresh and P. Alli, "An Overview of Research Issues in the Modern Healthcare Monitoring System Design using Wireless Body Area Network", American Journal of Applied Sciences, vol. 9, no. 1, **(2012)**, pp. 54-59.
[8] J. T. Kim, U. G. Kang, Y. H. Lee and B. M. Lee, "Security of Personal Bio Data in Mobile Health Applications for the Elderly", International Journal of Security and Its Applications,vol. 9, no. 10, **(2015)**, pp. 59-70.
[9] T. Jin and W. Yjing, "The Research of Secure Transport Protocol based on Node's Clock Characteristics for Body Area Networks", International Journal of Security and Its Applications, vol. 8, no. 5, **(2014)**, pp. 457-470.
[10] X. Wu, "A Lightweight Trust-based Access Control Model in Cloud-Assisted Wireless Body Area Networks", International Journal of Security and Its Applications, vol. 8, no. 5, **(2014)**, pp. 131-138.
[11] J. Welch, F. Guilak and S. D. Baker, "A wireless ECG smart sensor for broad application in life threatening event detection", Proc. on Engineering in Medicine and Biology Society 2004, **(2004)** pp. 3447-3449.
[12] P. Kumar and H. J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Network: A Survey", Sensors, vol. 12, no. 1, **(2012)**, pp. 55-91.
[13] S. S. Javadi and M. A. Razzaque, "Security and Privacy in Wireless Body Area Networks for Health Card Applications", Wireless Networks and Security, **(2013)** pp. 167-186.
[14] Q. Huang, X. Yang and S. Li, "Identity authentication and context privacy preservation in wireless health monitoring system", International Journal of Computer Network and Information Security, vol. 3, no. 4, **(2011)**, pp. 53-60.
[15] M. Laymouni, K. Veslype and M. T. Sandikkaya, "Privacy-Preserving Telemonitoring for eHealth", Lecture Notes in Computer Science, vol. 5645, **(2009)**, pp. 95-110.
[16] Y. Jian, S. Chen, Z. Zhang and L. Zhang, "Protecting receiver location privacy in wireless sensor networks", Proc. of INFOCOM 2007, **(2007)**, pp. 1955-1963.
[17] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "SAGE: a strong privacy preserving scheme against global eavesdropping for ehealth system", IEEE Journal of Selected Areas of Communications, vol. 27, no. 4, **(2009)**, pp. 365-378.
[18] K. Mtonga, "Secure Authentication Scheme for Remote Health Monitoring System using WBAN", M. S. Thesis, Kyungil University, **(2013)**.
[19] Message integrity, http://encyclopedia2.thefreedictionary.com/message integrity.
[20] Untraceable, http://security.stackexchange.com/questions/74031/relationship-between-anonymity-and-untraceability.
[21] Masquerade attack, https://www.techopedia.com/definition/4020/masquerade-attack.

Authors

SungWoon Lee, He is a professor at the Department of Information Security, Tongmyong University, Korea. He received the B.S. and M.S. degrees in Computer Science from Chonnam National University, Korea in 1994 and 1996, respectively, and the Ph.D. degree in Computer Engineering from Kyungpook National University, Korea, in 2005. He was with the Korea Information System as a researcher, Korea, from 1996 to 2000. His research interests include cryptography, network security, and security protocol.

Hyunsung Kim, He is a full professor at the Department of Cyber Security, Kyungil University, Korea from 2012. Furthermore, he is a visiting professor at the Department of Mathematical Sciences, Chancellor College, University of Malawi, Malawi from 2015. He received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.