Authentication Protocol for Healthcare Services over Wireless Body Area Networks

Seulgi Shin[1], Sung Woon Lee[2]*, Hyunsung Kim[1]

[1] The Department of Cyber Security Kyungil University, Korea.
[2] The Department of Information Security, Tongmyong University, Korea.

* Corresponding author. Tel.: +82 10-6340-0587; email: staroun@tu.ac.kr
Manuscript submitted October 2, 2014; accepted April 25, 2015.
doi: 10.17706/ijcce.2016.5.1.50-60

Abstract: Ubiquitous healthcare service is one of the major fields of research for wireless body area networks (WBANs). Ensuring complete and a good level of security for such types of WBANs, is not a trivial task. It is practically impossible to deal with all sorts of security threats with a single mechanism. This paper reviews Khan et al.'s authentication protocol for healthcare service over WBANs and shows that it does not provide forward secrecy. Furthermore, this paper proposes a remedy protocol for Khan et al.'s authentication protocol and the previous related protocols. The proposed protocol could be utilized as a basic security building block for healthcare applications based on WBANs.

Key words: Healthcare service, wireless body area network, security, authentication.

1. Introduction

Wireless sensor networks (WSNs) are an emerging technology in existing research and have the potential to make human life more comfortable. Sensor node is the smallest unit of a network that has unique features like large scale deployment, mobility, reliability, and so on. A WSN consists of a group of nodes with low cost, low power, less memory, and limited computational power that communicate wirelessly over limited frequencies at low bandwidth [1], [2]. The main goals of WSNs are to deploy a number of sensor nodes over an unattended area, and collect the environmental data and transmit it to the base station or remote location. Later, the raw data is processed online or offline for detailed analysis at the remote server according to the application requirements.

At the same time, meeting the potential of WSNs in healthcare, called as wireless body area networks (WBANs) requires addressing a multitude of technical challenges. These challenges reach above and beyond the resource limitations that all WBANs face. Specifically, unlike applications in other domains, healthcare applications impose stringent requirements on system reliability, quality of service and particularly privacy and security [3]-[6].

Ensuring complete and a good level of security for such types of WBANs, is not a trivial task. As these types of networks use wireless communications, the threats and attacks against them are more diverse and often very large in scale. It is practically impossible to deal with all sorts of security threats with a single mechanism. Instead, a combination of different security schemes for a single network could be the solution [7]. After the development of simple user authentication schemes in [8]-[12], schemes for WSNs and WBANs have also attracted to the researchers. Some works has proposed for healthcare applications using WBANs [13]-[17]. Kumar *et al*. observed that most of the schemes in [8]-[10] fall short to provide security

and also require heavy computational overhead and high communication cost and proposed a user authentication scheme named E-SAP [17]. Recently, Khan *et al.* showed that Kumar *et al.*'s scheme is weak against user impersonation attack, password guessing attack and node impersonation attack and lacks user anonymity. Furthermore, they proposed an improved user authentication protocol to solve the problems in Kumar *et al.*'s scheme [18].

This paper proposes a new user authentication protocol for healthcare services over WBANs. First of all, we will review Khan et al.'s protocol and show that it does not provide forward secrecy. After that, we will propose a new authentication protocol to solve the problem in Khan *et al.*'s protocol and the previous authentication protocols. The proposed protocol could provide anonymity and untraceability, which are very necessary properties in ubiquitous healthcare applications.

2. Review of Khan *et al.*'s Authentication Scheme

This section reviews network configuration of healthcare service based on WMSN, which is the focusing network environment in this paper. After that, we will review Khan *et al.*'s authentication scheme in [18] and show the security weakness in it.

2.1. Network Configuration of Healthcare Service Based on WMSN

There are four main parties in the WMSN, which are users, *MS* nodes, *GW* node and patients. Users are medical professionals like nurses, doctors, etc., looking for physiological data of the patient via WMSN. *MS* nodes are tiny sensors like temperature sensor, pulse oxi-meter, etc. deployed on the body of the patients. *GW* node is a powerful master node which plays the role of the registering authority and acts as an interface between the user and the *MS*-node. Patients are under vigilance of medical professionals by means of *MS* nodes for treatment (see Fig. 1).

MS nodes are tiny sensors having low processing power, limited computational capabilities, and limited energy and storage capacity [19]. *GW* node is a powerful node with sufficiently large processing power, computational capabilities, and energy and storage capacity. A patient registers himself (or herself) to *GW* node to become a valid participant of the system. Whenever a user wishes to obtain the physiological data of a patient, he (or she) transmits request message to *GW* node of the patient. Afterwards, *GW* node verifies the legitimacy of the user. Only if the verification is satisfied, directs the desired *MS* node(s) to answer to the user's request.

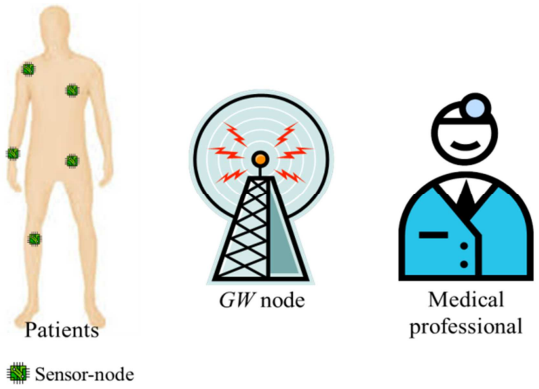

Fig. 1. Network configuration.

2.2. Khan *et al.*'s Authentication Scheme

This subsection reviews Khan *et al.*'s authentication scheme, which is consisted with five phases, user registration phase, patient registration phase, login phase, authentication phase and password change phase [18].

[User Registration Phase] The user (professional) *U* registers itself to the *GW*-node in registration center of the hospital. In the following manner:

1) User choses her/his identity ID_u and submits it to the *GW* node using a secure channel.
2) On receiving ID_u the *GW* node computes C_{ug}, K_u, and K_g as in (1), (2) and (3), respectively.

$$C_{ug} = E_K(ID_u \parallel ID_g) \tag{1}$$

$$K_u = h(K \parallel ID_u \parallel ID_g) \tag{2}$$

$$K_g = h(ID_g \parallel K) \tag{3}$$

3) *GW* node stores $\{h(.), C_{ug}\}$ into a *SC*, and provides *SC* along with values $\{K_u, K_g\}$ to *U* through the secure channel.
4) On obtaining *SC* with the information $\{h(.), C_{ug}\}$ and $\{K_u, K_g\}$, the user *U* chooses his (or her) password PW_u and computes N_u, PK_u and PK_g as in (4), (5) and (6), respectively. Finally, *U* inserts N_u, PK_u and PK_g in *SC,* so that *SC* stores $\{h(.), C_{ug}, N_u, PK_u, PK_g\}$.

$$N_u = h(ID_u \parallel PW_u \parallel K_u) \tag{4}$$

$$PK_u = K_u \oplus (ID_u \parallel PW_u) \tag{5}$$

$$PK_g = K_g \oplus (PW_u \parallel ID_u) \tag{6}$$

[Patient Registration Phase] A patient has to register itself in registration center of the hospital. Patient submits his (or her) name to the registration center. On receiving patient's name, the registration center chooses a suitable medical sensor kit (i.e., *MS* nodes and *GW* node) according to the disease of the patient and assigns medical professionals (users). Then the registration center transmits the identity ID_{pt} of the patient along with medical sensors kit information to the assigned professionals/users. Finally, a technician deploys *MS*-node on the body of the patient.

[Login Phase] A professional logs into the *GW* node in order to gain patients' medical data via WMSN. The user inserts her/his *SC* into the smart card reader and inputs ID_u and PW_u. Then the *SC* performs the following:

1) Retrieves K_u and K_g as in (7) and (8), and computes N_u* as in (9). If N_u* is the same with N_u, it continues further; otherwise stops the session.

$$K_u = PK_u \oplus (ID_u \parallel PW_u) \tag{7}$$

$$K_g = PK_g \oplus (PW_u \parallel ID_u) \tag{8}$$

$$N_u^* = h(ID_u \parallel PW_u \parallel K_u) \tag{9}$$

2) Generates a random nonce *M* and computes C_{u1} and CID_u as in (10) and (11), respectively.

$$C_{u1} = C_{ug} \oplus h(K_g) \tag{10}$$

$$CID_u = E_{K_u}(h(ID_u) \parallel M \parallel S_n \parallel C_{ug} \parallel T_u) \quad (11)$$

3) *SC* sends {CID_u, C_{u1}, T_u} as login request to the *GW* node, where, T_u is the current timestamp.

[Authentication Phase] When the login request {CID_u, C_{u1}, T_u} from *U* is received by the *GW* node, it executes the following steps

1) Acquires current timestamp T_g' and if (T_g'–T_u) ≤ ΔT. It discards the login request; otherwise proceeds further.
2) Retrieves C_{ug} as in (12) and decrypts CID_u with K_u to obtain {$h(ID_u)$', M, S_n, C_{ug}* and T_u*}. Verifies whether C_{ug}* is equivalent with C_{ug}. If it is correct, then decrypts C_{ug} with K to obtain ID_u* and ID_g.

$$C_{ug} = C_{u1} \oplus h(K_g) \quad (12)$$

3) Then computes $h(ID_u)$* and verifies whether $h(ID_u)$*, ID_g* and T_u are equivalent with $h(ID_u)$', ID_g and T_u*. If all the three equivalences hold, it believes that the login request is come from *U*; otherwise it terminates the session.
4) Acquires T_g as current timestamp, computes C_{g1} as in (13) and sends {C_{g1}, T_g} to *U*. Acquires T_{gs} as another current timestamp and computes C_{g2} and A_u as in (14) and (15), respectively. Then, the *GW* node sends {C_{g2}, A_u, T_{gs}} to the *MS* node.

$$C_{g1} = K_g \oplus (M \parallel T_g \parallel T_u) \quad (13)$$

$$C_{g2} = h(K_{gs}) \oplus (CID_u \parallel T_g \parallel M \parallel T_u) \quad (14)$$

$$A_u = h(CID_u \parallel K_{gs} \parallel T_g \parallel S_n \parallel T_{gs}) \quad (15)$$

On receiving {C_{g1}, T_g} from the *GW* node, *U* verifies the legitimacy of the *GW* node as follows:

5) Checks if (T_u'–T_g) ≤ ΔT. If so, dumps the session; otherwise continues further.
6) Obtains (M*||T_g*||T_u*) as in (16) and verifies whether M* and T_g* are equivalent with M and T_u. If they hold, then *GW* node is authenticated; otherwise terminates the login session.

$$\left(M^* \parallel T_g^* \parallel T_u^*\right) = C_{g1} \oplus K_g \quad (16)$$

After this mutual authentication, *U* and *GW* node compute $Ksess_{U\text{-}GW}$ as in (17) for the session key.

$$Ksess_{U-GW} = h(M \parallel ID_u \parallel T_g) \quad (17)$$

On receiving {C_{g2}, A_u, T_{gs}} from the *GW* node, the *MS* node performs the following operations:

7) Checks if (T_s'–T_{gs}) ≤ ΔT. If so, terminates the session; otherwise proceeds further.
8) Obtains (CID_u*|| T_g*||M*||T_u*) as in (18), computes A_u* as in (19) and compares A_u* with A_u. If the verification holds, the legitimacy of the *GW* node is successful and hence of *U*.

$$\left(CID_u^* \parallel T_g^* \parallel M^* \parallel T_u^*\right) = C_{g2} \oplus h(K_{gs}) \quad (18)$$

$$A_u^* = h(CID_u^* \parallel K_{gs} \parallel T_g^* \parallel S_n \parallel T_{gs}) \quad (19)$$

9) Acquires T_{sg} as current timestamp, computes C_{s1} as in (20), and sends $\{C_{s1}, T_{sg}\}$ to the *GW* node. Also computes C_{s2}^* as in (21), where T_s is another current timestamp of *MS* node. Then, the *MS* node sends $\{C_{s2}^*, T_s\}$ to *U*.

$$C_{s1} = h(T_g \parallel K_{gs} \parallel T_{sg}) \oplus h(CID_u \parallel S_n) \tag{20}$$

$$C_{s2}^* = h(S_n \parallel M^* \parallel T_u \parallel T_s) \tag{21}$$

On receiving $\{C_{s1}, T_{sg}\}$ from the *MS* node, the *GW* node performs the following operations:

10) Checks if $(T_g'' - T_{sg}) \leq \Delta T$, if so, terminates the session; otherwise proceeds further.
11) Obtains $(h(CID_u||S_n))^*$ as in (22), and compares it with $h(CID_u||S_n)$. The equivalence whether $(h(CID_u||S_n))^*$ is equivalent with $h(CID_u||S_n)$ verifies the legitimacy of *MS* node.

$$\left(h(CID_u \parallel S_n)\right)^* = C_{s1} \oplus h(T_g \parallel K_{gs} \parallel T_{sg}) \tag{22}$$

After this mutual authentication, *GW* node and *MS* node compute $Ksess_{GW\text{-}Sn}$ as in (23) for the session key.

$$Ksess_{GW-S_n} = h(K_{gs} \parallel T_{sg} \parallel M) \tag{23}$$

On receiving $\{C_{s2}^*, T_s\}$ from the *MS* node, *U* performs the following:

12) Checks if $(T_u'' - T_s) \leq \Delta T$. If so, dumps the session, otherwise proceeds further.
13) Computes C_{s2} as in (24) and compares it with C_{s2}^*. If C_{s2} is equal to C_{s2}^*, the authenticity of *MS* node is verified.

$$C_{s2} = h(S_n \parallel M \parallel T_u \parallel T_s) \tag{24}$$

After this mutual authentication, *U* and *MS* node compute $Ksess_{U\text{-}Sn}$ as in (25) for the session key.

$$Ksess_{U-S_n} = h(M \parallel T_s \parallel S_n) \tag{25}$$

[Password Change Phase] *U* can change his (or her) password in the following manner. For this, *U* inserts his (or her) *SC* into the terminal, inputs his (or her) ID_u and PW_u, and opts to change his (or her) password. Then the following steps are performed to update a new password:

1) *SC* retrieves K_u and K_g as in (7) and (8), and computes N_u^* as in (9). If N_u^* is equivalent to N_u, then proceeds further after asking for new password; otherwise discards the password change request.
2) *U* enters a new password $(PW_u)_{new}$.
3) *SC* computes with $(N_u)_{new}$, $(PK_u)_{new}$ and $(PK_g)_{new}$ as in (26), (27) and (28), respectively.

$$(N_u)_{new} = h(ID_u \parallel (PW_u)_{new} \parallel K_u) \tag{26}$$

$$(PK_u)_{new} = K_u \oplus (ID_u \parallel (PW_u)_{new}) \tag{27}$$

$$(PK_g)_{new} = K_g \oplus ((PW_u)_{new} \parallel ID_u) \tag{28}$$

4) *SC* replaces N_u, PK_u and PK_g with $(N_u)_{new}$, $(PK_u)_{new}$ and $(PK_g)_{new}$, respectively.

2.3. Security Analysis on Khan *et al.*'s Scheme

Khan *et al.* argued that their scheme is secure against various attacks and provides good properties. However, this section shows that Khan *et al.*'s scheme does not provide forward secrecy, which is necessary property to be supported to the key agreement scheme. We need to have an assumption that attacker could get the system's long term secret key K as usual for the forward secrecy. Also, we need another assumption that attacker also could steal and read the smart card.

For the attack, first of all, an attacker could derive ID_u' and ID_g' by decrypting C_{ug} on the smart card. After that, the attacker could derive K_g' with the long term secret key K and the identity of GW node ID_g'. Note that K_u works as a very important key for the confidentiality of communication in between. The attacker could know K_u' from the derivations by computing $h(K||ID_u'||ID_g')$ and K_{gs}' as in (29) and decrypt CID_u by using K_u to derive M' and S_n'. Then, the attacker could derive two session keys $Ksess_{U\text{-}GW}'$ and $Ksess_{U\text{-}Sn}'$ as in (30) and (31) properly. Thereby, Khan *et al.*'s scheme does not provide forward secrecy.

$$K_{gs}' = h(K \parallel ID_g') \tag{29}$$

$$Ksess_{U-GW}' = h(M' \parallel ID_u' \parallel T_g) \tag{30}$$

$$Ksess_{U-S_n} = h(M' \parallel T_s \parallel S_n') \tag{31}$$

3. Proposed Authentication Scheme

This section proposes a new user authentication protocol for healthcare services over WBANs. The proposed protocol could provide anonymity and untraceability by adopting dynamic identity depending on the session fresh random numbers. The proposed protocol is also consisted with five phases including user registration phase, patient registration phase, login phase, authentication phase and password change phase.

3.1. User Registration Phase

The user (medical professional) U registers himself (or herself) to the GW node in registration center of the hospital in the following manner:

1) User chooses her/his identity ID_u and submits it to the GW node using a secure channel.
2) On receiving ID_u, the GW node computes C_{ug}, K_u, and K_g as in (1), (2) and (3), respectively.
3) GW node stores $\{h(.), C_{ug}\}$ into a SC, and provides SC along with values $\{K_u, K_g\}$ to U through the secure channel.
4) On obtaining SC with the information $\{h(.), C_{ug}\}$ and $\{K_u, K_g\}$, the user U chooses his (or her) password PW_u and computes N_u, PK_u and PK_g as in (4), (5) and (6), respectively. Finally, U inserts N_u, PK_u and PK_g in SC, so that $SC = \{h(.), C_{ug}, N_u, PK_u, PK_g\}$.

3.2. Patient Registration Phase

A patient has to register himself (or herself) in registration center of the hospital. Patient submits his (or her) name to the registration center. On receiving the patient's name, the registration center chooses a suitable medical sensor kit (i.e., MS nodes and GW node) according to the disease of the patient and assigns medical professionals. Then, the registration center transmits the identity ID_{pt} of the patient along with medical sensors kit information to the assigned professionals/users. Finally, a technician deploys the MS node on the body of the patient.

3.3. Login Phase

A professional logs into the *GW* node in order to gain patients' medical data via a WMSN. The user inserts his (or her) *SC* into the smart card reader and inputs ID_u and PW_u. Then the *SC* performs the following processes:

1) *SC* retrieves K_u as in (7), K_g as in (8) and computes N_u* as in (9). If N_u* is equal to N_u, *SC* continues further; otherwise *SC* stops the session.
2) Generates a random nonce a and computes A as in (32), C_{u1} as in (10) and CID_u as in (11).

$$A = g^a \tag{32}$$

3) *SC* sends $\{CID_u, C_{u1}\}$ as login request to *GW* node.

3.4. Authentication Phase

When the login request $\{CID_u, C_{u1}\}$ from U is received by the *GW* node, it executes the following steps:

1) The *GW* node retrieves C_{ug} as in (12) and decrypts CID_u as $D_K(CID_u)$ to obtain $\{h(ID_u)', A, S_n^*$ and $C_{ug}^*\}$. The *GW* node verifies whether C_{ug}* is equivalent with C_{ug}. If correct, then the *GW* node decrypts C_{ug} as $D_{Ku}(C_{ug})$ to obtain ID_u* and ID_g.
2) Then the *GW* node computes $h(ID_u)$* and verifies whether $h(ID_u)$*, ID_g* are equivalent with $h(ID_u)'$, ID_g. If all equivalences hold, the *GW* node believes the login request is come from U; otherwise the *GW* node terminates the login session.
3) The *GW* node generates a random nonce b and computes B as in (33), $SK_{GW\text{-}U}$ as in (34), C_{g1} as in (35) and A_m as in (36) and sends $\{C_{g1}, A_m\}$ to U. The *GW* node computes, C_{g2} as in (37) and A_u as in (38). Then, the *GW* node sends $\{C_{g2}, A_u\}$ to the *MS* node.

$$B = g^b \tag{33}$$

$$SK_{GW-U} = A^b \tag{34}$$

$$C_{g1} = K_g \oplus (A \parallel B) \tag{35}$$

$$A_m = h(SK_{U-GW} \parallel A \parallel B) \tag{36}$$

$$C_{g2} = h(K_{gs}) \oplus (CID_u \parallel A \parallel B) \tag{37}$$

$$A_u = h(K_{gs} \parallel S_n \parallel A \parallel B) \tag{38}$$

On receiving $\{C_{g1}, A_m\}$ from the *GW* node, U verifies the legitimacy of the *GW* node as follows:

4) U obtains $(A^*||B^*)$ as in (39) and verifies A_m and checks A^* is equal with A. For A_m verification, U computes $SK_{U\text{-}GW}$ as in (40) and A_m* as in (41) and checks A_m* is equal with A_m. Only if they hold, the *GW* node is authenticated and both of U and the *GW* node share a session key $SK_{U\text{-}GW}$, which is the same with $SK_{GW\text{-}U}$ correctly; otherwise U terminates the login session.

$$(A^* \parallel B^*) = C_{g1} \oplus K_g \tag{39}$$

$$SK_{U-GW} = B^a \tag{40}$$

$$A_m^* = h(SK_{U-GW} \parallel A \parallel B^*) \quad (41)$$

On receiving $\{C_{g2}, A_u\}$ from the *GW* node, the *MS* node performs the following operations

5) The *MS* node obtains $(CID_u^*||A^*||B^*)$ as in (42), computes A_u^* as in (43) and compares A_u^* with A_u. The equivalence check between A_u^* and A_u verifies the legitimacy of the *GW* node and hence of *U*.

$$(CID_u^* \parallel A^* \parallel B^*) = C_{g2} \oplus h(K_{gs}) \quad (42)$$

$$A_u^* = h(K_{gs} \parallel S_n \parallel A^* \parallel B^*) \quad (43)$$

6) The *MS* node generates a random nonce *f* and computes *F* as in (44), $SK_{MS\text{-}GW}$ as in (45), C_{s1} as in (46) and A_{ms} as in (47) and sends $\{C_{s1}, A_{ms}\}$ to the *GW* node. Also the *MS* node computes $SK_{MS\text{-}U}$ as in (48), C_{s2} as in (49) and A_{msu} as in (50). Then, the *MS* node sends $\{C_{s2}, A_{msu}\}$ to *U*.

$$F = g^f \quad (44)$$

$$SK_{MS-GW} = B^{*f} \quad (45)$$

$$C_{s1} = h(CID_u \parallel S_n) \oplus F \quad (46)$$

$$A_{ms} = h(SK_{MS-GW} \parallel K_{gs} \parallel B^* \parallel F) \quad (47)$$

$$SK_{MS-U} = A^{*f} \quad (48)$$

$$C_{s2} = A^* \oplus F \quad (49)$$

$$A_{msu} = h(SK_{MS-U} \parallel S_n \parallel A^* \parallel F) \quad (50)$$

On receiving $\{C_{s1}, A_{ms}\}$ from the *MS* node, the *GW* node performs the following operations:

7) The *GW* node obtains *F** as in (51), $SK_{GW\text{-}MS}$ as in (52) and A_{ms}^* as in (53). The equivalence check between A_{ms}^* and A_{ms} verifies the legitimacy of the *MS* node and the session key agreement.

$$F^* = C_{s1} \oplus h(CID_u \parallel S_n^*) \quad (51)$$

$$SK_{GW-MS} = F^{*b} \quad (52)$$

$$A_{ms}^* = h(SK_{GW-MS} \parallel K_{gs} \parallel B^* \parallel F) \quad (53)$$

On receiving $\{C_{s2}, A_{msu}\}$ from the *MS* node, *U* performs the following steps

8) *U* computes *F** as in (54), $SK_{U\text{-}MS}$ as in (55) and A_{msu}^* as in (56) and compares A_{msu}^* with A_{msu}. Only if they match, *U* verifies the legitimacy of the *MS* node and the session key agreement.

$$F^* = C_{s2} \oplus A \quad (54)$$

$$SK_{U-MS} = F^* \quad (55)$$

$$A^*_{msu} = h(SK_{U-MS} \parallel S_n \parallel A \parallel F^*) \quad (56)$$

3.5. Password Change Phase

U can change his (or her) password in the following manner. For this, *U* inserts his (or her) *SC* into the terminal, inputs his (or her) ID_u and PW_u, and opts to change his (or her) password. Then the following steps are performed to update a new password

1) *SC* retrieves K_u as in (7), K_g as in (8) and computes N_u* as in (9). If N_u* is equivalent to N_u, then proceeds further after asking for new password; otherwise discards the password change request.
2) *U* enters a new password $(PW_u)_{new}$. *SC* computes $(N_u)_{new}$ as in (26), $(PK_u)_{new}$ as in (27) and $(PK_g)_{new}$ as in (28). *SC* replaces N_u, PK_u and PK_g with $(N_u)_{new}$, $(PK_u)_{new}$ and $(PK_g)_{new}$, respectively.

4. Security Analyses

This section provides security analysis of the proposed protocol. We will consider that the proposed protocol is secure under the same assumption subject to which Khan *et al.*'s protocol is attackable. The assumption is that an attacker U_a can extract the information stored inside the smart card. Also, we need to have an assumption that attacker could get the system's long term secret key *K* as usual for the forward secrecy.

4.1. Provides User Anonymity

If U_a intercepts the login request $\{CID_u, C_{u1}\}$ of *U*, U_a needs K_u to obtain $h(ID_u)$ by decrypting CID_u. But U_a neither knows K_u nor recovers $h(ID_u)$ by extracting information $\{h(.), C_{ug}, N_u, PK_u, PK_g\}$ from the lost smart card of *U*. To take out K_u from PK_u, U_a should know user's identity and password. In fact, K_u required to encrypt or decrypt CID_u is not stored directly in user's smart card and is different for each user. Therefore, U_a cannot obtain $h(ID_u)$. On the other hand, to procure identity ID_u from N_u, $PK_{\underline{u}}$ or PK_g is infeasible. It requires knowledge of keys K_u and K_g to gain ID_u out of PK_u or PK_g respectively. Moreover, one-way property of hash function does not allow the extraction of ID_u out of N_u. Therefore, U_a cannot gain the identity of a user and hence the protocol provides user anonymity.

4.2. Resists Password Guessing Attack

In order to guess *U*'s password PW_u obtained from the lost *SC* of *U*, U_a requires knowledge of ID_u and K_u. As described in the user anonymity part, U_a cannot gain the identity of a user either from the lost smart card of a user or from an intercepted login request. Besides, K_u is not available as plaintext in *U*'s *SC* and is not obtainable from PK_u without having exact values of ID_u and PW_u. Thus, the protocol resists password guessing attack.

4.3. Provides Secure Session Key between Every Entities

The proposed protocol establishes session key between every pair of participants. Session key between *U* and the *GW* node is computed as in (34), which depends on session dependent random numbers from each entity. U_a cannot compute $SK_{U\text{-}GW}$ even if the case that U_a knows *A* and *B* due to the discrete logarithm problem. Session key between the *GW* node and the *MS* node is computed as in (52) which is dynamic because of session dependent random number *b* and *f*. Session key between *U* and the *MS* node is computed as in (55) which U_a cannot compute without knowing *a* and *f*. Thus, the protocol establishes independent and secure session keys between every pair of the participants.

4.4. Provides Forward Secrecy

If we have two assumptions as the attack to Khan *et al.*'s scheme, the proposed protocol provides forward

secrecy. U_a should be able to get the messages $\{CID_u, C_{u1}\}$, $\{C_{g2}, A_u\}$, $\{C_{s1}, A_{ms}\}$ and $\{C_{s2}, A_{msu}\}$. However, there is no way U_a to know about $SK_{U\text{-}GW}$, $SK_{GW\text{-}MS}$ and $SK_{U\text{-}MS}$ due to the discrete logarithm problem. Thereby, the proposed protocol provides forward secrecy.

5. Conclusion

This paper has been proposed a new user authentication protocol for healthcare services over WBANs. First of all, we reviewed Khan *et al.*'s protocol and showed that it does not provide forward secrecy. After that, we proposed a new authentication protocol to solve the problem in Khan *et al.*'s protocol and the previous authentication protocols. The proposed protocol could provide anonymity and untraceability, which are very necessary properties in ubiquitous healthcare applications.

Acknowledgment

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

References

[1] Ko, B. J. G., Lu, C., Srivastva, M. B., Stankovic, J., Terzis, A. A., & Welsh, M. (2010). Wireless sensor network for healthcare. *Proceedings of IEEE*, *98(11)*, 1947–1960.

[2] Kumar, P., & Lee, H. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*. *12(1)*, 55-91.

[3] Caytiles, R. D., & Park, S. (2014). A study of the design of wireless medical sensor network based u-Healthcare system. *International Journal of Bio-Science and Bio-Technology*, *6(3)*, 91-96.

[4] Kim, H., Ryu, E. K., & Lee, S. W. (2013). Security considerations on cognitive radio based on body area networks for u-Healthcare. *Journal of Security Engineering*, *10(1)*, 9-20.

[5] Kim, H., & Lee, S. W. (2009). Enhanced novel access control protocol over wireless sensor networks. *IEEE Trans. on Consumer Electronics*, *55(2)*, 492-498.

[6] Mtonga, K., Yoon, E. J., & Kim, H. (2014). A pairing based authentication and key establishment scheme for remote patient monitoring systems. *Lecture Notes of the Institute for Computer Sciences*, *135*, 79-89.

[7] Haque, M., Pathan, A. K., & Hong, C. S. (2008). Securing U-healthcare sensor networks using public key based scheme. *Proceedings of 10th International Conference on Advanced Communication Technology*: *Vol. 2* (pp. 1108-1111).

[8] Kim, H., Lee, S. W., & Yoo, K. Y. (2003). ID-based password authentication scheme using smart cards and fingerprints. *Operating Systems Review* (pp. 32-41).

[9] Lee, S. W., Kim, H., & Yoo, K. Y. (2004). Improved efficient remote user authentication scheme using smartcards. *IEEE Trans. on Consumer Electronics*, *50(2)*, 565-567.

[10] Lee, S. W., Kim, H., & Yoo, K. Y. (2005). Improvement of Chien *et al*'s remote user authentication scheme using smart cards. *Computer Standards and Interfaces*, *27*, 181-183.

[11] Kim, H. (2011). Location-based authentication protocol for first cognitive radio networking standard. *Journal of Network and Computer Applications*, *34*, 1160-1167.

[12] Vallent, T. F., & Kim, H. (2013). Three factor authentication protocol based on bilinear pairing. *Lecture Notes in Electrical Engineering*, *240*, 253-260.

[13] Saleem, S., Ullah, S., & Yoo, H. S. (2009). On the security issues in wireless body area networks. *Journal of Digital Content Technology and Its Applications*, *3(3)*, 178-184.

[14] Ullah, S., & Kwak, K. (2011). Body area network for ubiquitous healthcare applications: Theory and

implementation. *Journal of Medical Systems*, *35(5)*, 1243-1244.
[15] Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., & Kwak, K. (2012). A comprehensive survey of wireless body area networks — on PHY, MAC, and network layers solutions. *Journal of Medical Systems*, *36(3)*, 1065-1094.
[16] Chung, W. Y. (2012). Multi-modal sensing M2M healthcare service in WSN. *KSII Transactions on Internet and Information Systems*, *6(4)*, 1065-1094.
[17] Kumar, P., Lee, S. G., & Lee, H. J. (2012). E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors*, *12*, 1625-1647.
[18] Khan, M. K., & Kumari, S. (2014). An improvement user authentication protocol for healthcare services via wireless medical sensor networks. *International Journal of Distributed Sensor Networks*.
[19] Mtonga, K. (2013). *Secure Authentication Scheme for Remote Health Monitoring System Using WBAN*. M. S. Thesis, Kyungil University.

Seulgi Shin is a student at the Department of Cyber Security Kyungil University, Republic of Korea from 2013. She is interested in information security protocol, wireless sensor network security, ubiquitous computing security, cloud computing security, medical healthcare security, and recent information security issues.

Sung Woon Lee 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 is a professor at the Department of Cyber Security, Kyungil University, Korea. He received his 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 2011 with the Department of Computer Engineering, Kyungil University. He had been a visiting scholar from 2009 to 2010 with the School of Computing, Dublin City University, Ireland. Currently, he is a full professor at the Department of Cyber Security, Kyungil University. His current research interests are cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.