J Med Syst (2014) 38:26
DOI 10.1007/s10916-014-0026-0

MOBILE SYSTEMS

An Improved Anonymous Authentication Scheme for Telecare Medical Information Systems

Fengtong Wen · Dianli Guo

Received: 22 October 2013 / Accepted: 5 March 2014 / Published online: 30 April 2014

Abstract Telecare medical information system (TMIS) constructs an efficient and convenient connection between patients and the medical server. The patients can enjoy medical services through public networks, and hence the protection of patients' privacy is very significant. Very recently, Wu et al. identified Jiang et al.'s authentication scheme had some security drawbacks and proposed an enhanced authentication scheme for TMIS. However, we analyze Wu et al.'s scheme and show that their scheme suffers from server spoofing attack, off-line password guessing attack, impersonation attack. Moreover, Wu et al.'s scheme fails to preserve the claimed patient anonymity and its password change phase is unfriendly and inefficient. Thereby, we present a novel anonymous authentication scheme for telecare medical information systems to eliminate the aforementioned faults. Besides, We demonstrate the completeness of the proposed scheme through the BAN logic. Furthermore, the security of our proposed scheme is proven through Bellare and Rogaways model. Compared with the related existing schemes, our scheme is more secure.

Keywords Telecare medical information systems · Smart card · Authentication · Anonymity · BR-Model · BAN logic

Introduction

With the rapid development of information and communication technology, the telecare medical information systems are increasingly applied to enable or support healthcare delivery services. Patients can conveniently access health information and medical services through public networks at home. Considering the patients' privacy and security issues, a viable authentication mechanism will thus be in demand to verify the authenticity of all participants and to tackle the illegal access. Generally, smart cards and passwords are used to design remote identity-based authentication schemes [1–6].

In 2012, Wu et al. [7] proposed an authentication scheme with a pre-computation approach for TMIS. Later, He et al. [8] showed that Wu et al.'s scheme was insecure to against impersonation attack, insider attack, and then proposed an improved scheme to enhance the security. However, Wei et al. [9] stated that both of the mentioned authentication schemes were vulnerable to off-line password guessing attack once the patient's smart card was compromised. To rectify this flaw, Wei et al. presented a modified authentication scheme for TMIS. Unfortunately, soon after that Zhu [10] demonstrated that Wei et al.'s scheme was still susceptible to off-line password guessing attack and proposed a RSA based scheme. Nevertheless, in the above schemes, the identities of patients are transmitted in plaintext over the insecure network which may result in ID-theft attack and impersonation attack.

In order to negate this risk, dozens of dynamic ID-based authentication schemes for TMIS have been proposed [11–14, 17]. In 2012, Chen et al. [11] pointed out that Khan et al.'s scheme [12] had some security drawbacks and proposed a new dynamic ID-based scheme for TMIS. Later on, Jiang et al. [13] observed that Chen et al.'s scheme failed to provide patient anonymity and untraceability. Furthermore, they proposed an authentication scheme accomplishing patient privacy protection. Unluckily, Wu et al. [14] and Kumari et al. [17] demonstrated that Jiang et al.'s

This article is part of the Topical Collection on *Mobile Systems*

F. Wen (✉) · D. Guo
School of Mathematical Sciences, University of Jinan,
Jinan 250022, China
e-mail: wftwq@163.com

scheme fell short to resist a range of attacks such as off-line password guessing attack, impersonation attack, DoS attack and so on. They also proposed their own schemes to overcome these identified weaknesses, respectively. Here, we examine Wu et al.'s authentication scheme and identify its security pitfalls in this paper. And then, we propose a modified authentication scheme for TMIS which can achieve patient anonymity and untraceability.

The rest of this paper is organized as follows. In the next section, we present the preliminaries that will be used throughout the paper. In Section "Security model", we review the security model and definition for authenticated key exchange protocols. we briefly review Wu et al.'s scheme in section "Review of Wu et al.'s scheme". Subsequently, we show its weaknesses in Section "Security pitfalls in Wu et al.'s scheme". Then, we proceed with proposing our new scheme in Section "The improved scheme", together with analyzing its security in Section "Security analysis of the proposed scheme". In Section "Performance and functionality analysis", we compare the performance of our new scheme with the previous schemes. Section "Conclusion" concludes the paper.

Preliminaries

Symmetric-Key Encryption A symmetric encryption scheme can provide privacy. It consists of three algorithms: the key generation algorithm KG'', the encryption algorithm E and the decryption algorithm D.

For privacy, we consider the notion of indistinguishability under adaptive chosen plaintext attack (IND-CPA). Let $b \leftarrow \{0, 1\}$ denote a random bit. The adversary $\mathcal{A}$ has access to a left-or-right (LR) oracle which returns $E_K(M_b)$ upon receiving a pair of messages (M_0, M_1) from the adversary. Finally, the adversary outputs $b' \in \{0, 1\}$ as her guess of the value of b. We define the advantage of $\mathcal{A}$ as

$$\mathbf{Adv}_{\mathcal{A}}^{ind-cpa}(k) = |\Pr[b = b'] - 1/2|. \quad (1)$$

We say a symmetric-key encryption scheme is secure against adaptive chosen plaintext attacks if for any polynomial time adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{ind-cpa}(k)$ is negligible in k.

Decisional Diffie-Hellman (DDH) Assumption. Let g denote a generator of a cyclic group G with prime order q. Let g^x denote the modular exponentiation operation in G for any $x \in Z_q$. The DDH assumption [15] says for any polynomial time algorithm $\mathcal{D}$,

$$\mathbf{Adv}_{\mathcal{D}}^{ddh}(k) = \Pr[\mathcal{D}(g, g^a, g^b, g^{ab}) = 1]$$

$$-\Pr[\mathcal{D}(g, g^a, g^b, g^r) = 1] \quad (2)$$

is negligible in k where a, b, r are randomly selected from Z_q. That is, given the tuple (g, g^a, g^b), g^{ab} is computationally indistinguishable from a random element g^r of G.

Security model

The first formal security model for authenticated key exchange protocols is due to Bellare and Rogaway [16], which is usually referred to as the BR93-Model. In the following section, we review the BR93-Model and then prove that our scheme meets the requirements of BR93-Model.

The security model and concepts

We denote the client oracle which plays the role A to interact with B in the ith session by $\Pi^i_{A,B}$, and denote the server oracle which plays the role B to interact with A in the jth session by $\Pi^j_{B,A}$.

Let P be the proposed authentication protocol. In this protocol, there are two partner oracles $\Pi^i_{A,B}$ and $\Pi^j_{B,A}$, and a probabilistic polynomial time adversary $\mathcal{A}$ who can control the entire network and obtain the transmitted data in the past processes. In each protocol execution, or session, the adversary activates an instance either by an external request or by an incoming message. In addition, the adversary $\mathcal{A}$ can make the following oracle queries:

Execute query: This query models all kinds of passive attacks, where a passive adversary can eavesdrop all transmitted data between the client oracle $\Pi^i_{A,B}$ and the server oracle $\Pi^j_{B,A}$ in the running protocol.

Send query: This query models active attacks where an adversary sends a message m to an oracle $\Pi^i_{A,B}$ (or $\Pi^j_{B,A}$). The oracle executes the protocol based on the received message m and sends the response back to the adversary. An adversary can also initiate a session by setting $m = \lambda$(empty string).

Leak query: This query models the leakage of one of the two authentication factors owned by a user. When the adversary makes the query, the client oracle will respond one of two factors to the adversary. We will consider the following cases: 1) the leakage of the password; 2) the leakage of the data stored in the smart card.

Reveal query: This query allows the adversary to learn the session key generated by an oracle $\Pi^i_{A,B}$(or $\Pi^i_{B,A}$). Such a query is only valid when the oracle currently holds a session key.

Test query: An adversary can only make this query once to a test oracle. Upon receiving this query, a random coin

b is tossed. If $b = 1$, the real session key held by the test oracle is returned to the adversary; otherwise, a random key is selected from the session key space and returned to the adversary.

At the end of the game, the adversary outputs a bit b' as her guess for b. The adversary's advantage in winning the game is defined as

$$\mathbf{Adv}_{\mathcal{A}}(k) = |\Pr[b' = b] - 1/2|.$$

Review of Wu et al.'s scheme

Wu et al.'s authentication scheme consists of five phases, i.e., registration phase, login phase, authentication phase, password change phase and lost smart card revocation phase. The detailed steps of login phase and authentication phase are further illustrated in Fig. 1. For clarity, notations used in Wu et al.'s scheme are listed in Table 1.

Registration phase

Step 1. A patient U_i chooses his identity ID_i, password PW_i and a random number r_i. Then he/she computes $RPW_i = h(r_i \| PW_i)$ and transmits $\{ID_i, RPW_i\}$ to the medical server S via a secure channel.

Step 2. After receiving U_i's registration request, S verifies the validity of ID_i. If the verification fails, S rejects it. On the contrary, S maintains an account table for the registration patient, which records the identity ID_i and the registration time N in the format (ID_i, N) (if it is U_i's first registration, S sets $N = 0$; otherwise, S sets $N = N + 1$).

Step 3. S computes $J_i = h(x \| ID_i \| N)$, $L_i = J_i \oplus RPW_i$, $e_i = h(x) \oplus h(RPW_i \| ID_i)$. Afterwards, S writes $\{L_i, e_i, h(\cdot), E_{key}(\cdot), D_{key}(\cdot)\}$ into a smart card and issues it to U_i.

Step 4. U_i enters r_i into his/her smart card.

Login phase

Step 1. U_i inserts his/her smart card into the device and keys ID_i, PW_i. Subsequently, the smart card calculates $RPW_i = h(r_i \| PW_i)$, $J_i = L_i \oplus RPW_i$, $AID_i = e_i \oplus h(RPW_i \| ID_i) \oplus h(T_i) \oplus ID_i = h(x) \oplus h(T_i) \oplus ID_i$, $B_1 = e_i \oplus h(RPW_i \| ID_i) \oplus T_i = h(x) \oplus T_i$, $V_i = h(T_i \| J_i)$ and $C_1 = E_{h(T_i)}(AID_i \| T_i \| V_i)$, where T_i is the current timestamp.

Step 2. The smart card sends the login request message $m = \{B_1, C_1\}$ to S.

Authentication phase

Step 1. Upon receiving m, S computes $T_i' = B_1 \oplus h(x)$ and checks the validity of the timestamp T_i'. If it is invalid, S aborts the login request; otherwise, S decrypts C_1 using $h(T_i')$ to obtain AID_i', T_i'', V_i', and then verifies T_i' with the decrypted T_i''. If $T_i' \neq T_i''$, S terminates this session. Otherwise, S computes $ID_i' = AID_i' \oplus h(x) \oplus h(T_i')$ and checks whether ID_i' is in the account table. If it is true, S retrieves N, calculates $J_i' = h(x \| ID_i' \| N)$ and compares whether the decrypted V_i' equals to the computed $h(T_i' \| J_i')$. If they are equal, the login request is accepted and U_i is authentic; otherwise, the procedure is terminated immediately. After the verification of U_i, S computes $B_2 = h(x) \oplus T_s$, $C_2 = E_{h(T_s)}(V_i' \| T_s)$, $sk = h(J_i' \| T_i' \| T_s \| ID_i')$ and sends the reply mutual authentication message $m' = \{B_2, C_2\}$ to U_i.

Step 2. After receiving the response message m', the smart card computes $T_s' = B_2 \oplus e_i \oplus h(RPW_i \| ID_i)$ and checks the validity of T_s'. If the verification holds, U_i decrypts C_2 using $h(T_s')$ to get V_i'' and T_s''. Subsequently, U_i verifies $T_s' ? = T_s''$ and $V_i ? = V_i''$. If either or both are false, the authentication fails; else, U_i confirms that S is authentic and computes the session key $sk = h(J_i \| T_i \| T_s' \| ID_i)$.

Password change phase

When U_i wants to change his/her password, he/she inserts the smart card into a terminal and inputs identity ID_i, old password PW_i, new password PW_i^{new}.

Step 1. U_i sends the password change request $m = \{B_1, C_1\}$ to S. Afterwards, S and U_i perform the mutual authentication to verify the validity of each other as depicted in the authentication phase.

Step 2. If the mutual authentication fails, the smart card rejects U_i's password change request directly. If the mutual authentication is completed successfully, the smart card computes $RPW_i^{new} = h(r_i \| PW_i^{new})$, $L_i^{new} = L_i \oplus RPW_i \oplus RPW_i^{new}$, $e_i^{new} = e_i \oplus h(RPW_i \| ID_i) \oplus h(RPW_i^{new} \| ID_i)$.

Step 3. The smart card replaces L_i, e_i with L_i^{new}, e_i^{new}, respectively.

Lost smart card revocation phase

If the smart card of U_i is lost, he/she could re-register at S through the secure channel as registration phase. After

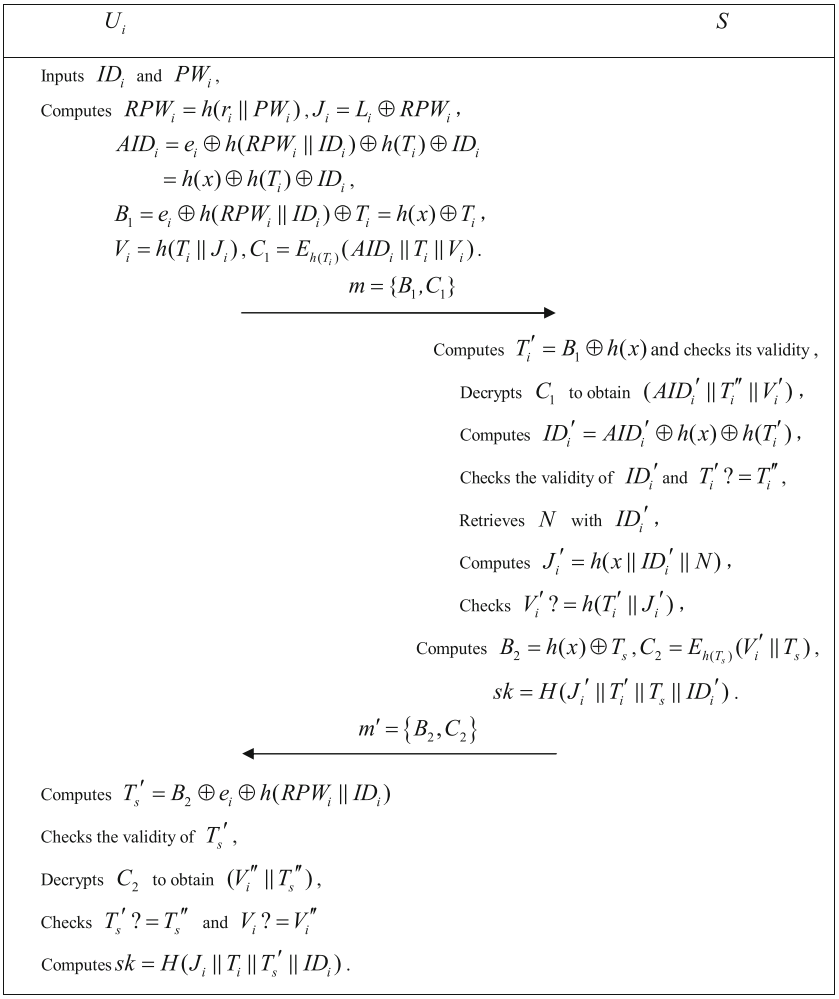

Fig. 1 Login phase and authentication phase

the verification of the identity ID_i, S retrieves N from the account table and sets $N = N + 1$, then stores the new entry (ID_i, N) in to account table. Finally, S issues a new smart card which contains security parameters to U_i.

Security pitfalls in Wu et al.'s scheme

In this section, we demonstrate that Wu et al.'s scheme is susceptible to various attacks, such as server spoofing attack, off-line password guessing attack and impersonation attack. Furthermore, their scheme cannot provide the claimed patient anonymity and the password change phase is unfriendly and inefficient. The details of these flaws are described as follows.

Failure of protecting patient anonymity

In Wu et al.'s scheme security analysis, the authors claimed that the adversary could not decrypt C_1 without T_i to retrieve AID_i which contained ID_i, and there-by, their scheme satisfied patient anonymity and untraceability. However, we find it is not true due to the following analysis.

Any legal but malicious patient $\mathcal{A}$ of the server can get the secret value $h(x)$ by computing $h(x) = e_{\mathcal{A}} \oplus h(RPW_{\mathcal{A}} \| ID_{\mathcal{A}})$. Consider that $\mathcal{A}$ has recorded U_i's previous login request message $m = \{B_1, C_1\}$. Then, with the computed secret number $h(x)$, he/she can easily compute $T_i = B_1 \oplus h(x)$. After getting the timestamp, the attacker $\mathcal{A}$ can further decrypt C_1 using $h(T_i)$ to obtain AID_i and calculates $ID_i = AID_i \oplus h(x) \oplus h(T_i)$.

Server spoofing attack

As explained above, with the computed secret value $h(x)$, the malicious patient $\mathcal{A}$ can masquerade as S to fool any legitimate patient by performing the following steps:

Step 1. Intercepts the login request message $m = \{B_1, C_1\}$ of U_i and computes $T_i = B_1 \oplus h(x)$.

Table 1 Notations

Notation	Meaning
U_i	A user(patient)
S	The remote server of the system
ID_i	The identity of U_i
PW_i	The password of U_i
x	The master secret key of S
T	Timestamp
N	Registration times of U_i
sk	The session key shared among U_i and S
$E_{key}(M)$	Encryption of a message M using key
$D_{key}(M)$	Decryption of a message M using key
$h(\cdot)$	A one-way hash function
$\oplus$	Exclusive-OR operation
$\|$	String concatenation operation
$F(\cdot)$	A pseudo-random function.

Then $\mathcal{A}$ can decrypt $C_1 = E_{h(T_i)}(AID_i \| T_i \| V_i)$ to get V_i with $h(T_i)$.

Step 2. Computes $B_2^* = h(x) \oplus T_s^*$, $C_2^* = E_{h(T_s^*)}(V_i \| T_s^*)$, where T_s^* is the current timestamp. Then, sends the forged reply message $m'^* = \{B_2^*, C_2^*\}$ to U_i.

It is easy to see that the response message m'^* can pass the verification due to $\mathcal{A}$ forges m'^* with the valid timestamp and the correct secret information V_i which is decrypted from C_1.

Off-line password guessing attack

Password as an easy-to-remember credential drawing from a small space is easily hacked from off-line password guessing attack. In case a legal remote patient U_i's smart card is somehow obtained (e.g. stolen or picked up) by the malicious patient $\mathcal{A}$, and the stored secret values $\{L_i, e_i, r_i\}$ can be extracted by side-channel attacks [18, 19]. Then $\mathcal{A}$ avails of the compromised $h(x)$, ID_i to launch off-line password guessing attack.

Step 1. Computes $e_i^* = h(x) \oplus h(h(r_i \| PW_i^*) \| ID_i)$ where PW_i^* is a guessed password from the password space $\mathcal{D}$.

Step 2. Verifies whether e_i^* equals to e_i to ensure the correctness of PW_i^*.

Step 3. Repeats the Steps 1 and 2 by replacing another guessed password PW_i^* until U_i's password PW_i is found.

Using the guessing password PW_i, the adversary can proceed impersonation attack easily.

The improved scheme

In this section, we present a new authentication scheme with privacy preservation for TMIS which can resist a range of attacks such as off-line password guessing attack, server spoofing attack and impersonation attack, even if the smart card is compromised. Our scheme also consists of five phases, i.e., registration phase, login phase, authentication phase, password change phase and lost smart card revocation phase. In Fig. 2, we will further depict the login phase and authentication phase.

In order to initialize this scheme, S chooses a multiplication group $G = Z_p$ and a element $g \in G$ with order q, where p and q are two large prime numbers such that $p = 2q + 1$. Then S selects the master secret key $x \in Z_q$ and computes the public key $g^x \ mod \ p$.

Registration phase

Step 1. A patient U_i chooses his/her identity ID_i, password PW_i and generates a random number r_i. Then he/she computes $RPW_i = h(r_i \| PW_i)$ and sends $\{ID_i, RPW_i\}$ to the medical server S over a secure communication channel.

Step 2. Upon receiving $\{ID_i, RPW_i\}$, S verifies the legitimacy of ID_i. If it is valid, S maintains an account table (ID_i, N) for the registration patient, where N is the registration time (N=0, if it is U_i's first registration; otherwise, $N = N + 1$). Then, S computes security parameters $J_i = h(x \| ID_i \| N)$, $L_i = J_i \oplus RPW_i$ and $K_i = h(ID_i \| RPW_i)$.

Step 3. S personalizes the smart card with $\{L_i, K_i, g, g^x \ mod \ p, p, q, h(\cdot), E_{key}(\cdot), D_{key}(\cdot)\}$ and issues it to U_i via a secure channel.

Step 4. U_i inserts r_i into the received smart card.

Login phase

Step 1. U_i inserts the smart card into a card reader and inputs his/her identity ID_i and password PW_i. Then, the smart card computes $RPW_i = h(r_i \| PW_i)$, $K_i' = h(ID_i \| RPW_i)$ and verifies whether $K_i' = K_i$ or not. If $K_i' = K_i$, proceeds to Step 2; otherwise, the login phase is terminated immediately.

Step 2. The smart card computes $J_i = L_i \oplus RPW_i$, then chooses a random number a and computes $A_i = g^{J_i a} \ mod \ p$, $B_i = (g^x \ mod \ p)^{J_i a} \ mod \ p$, $C_i = E_{B_i}(ID_i, T_i, g^a \ mod \ p)$, where T_i is the current time.

Step 3. The smart card sends the login request message $\{A_i, C_i\}$ to S.

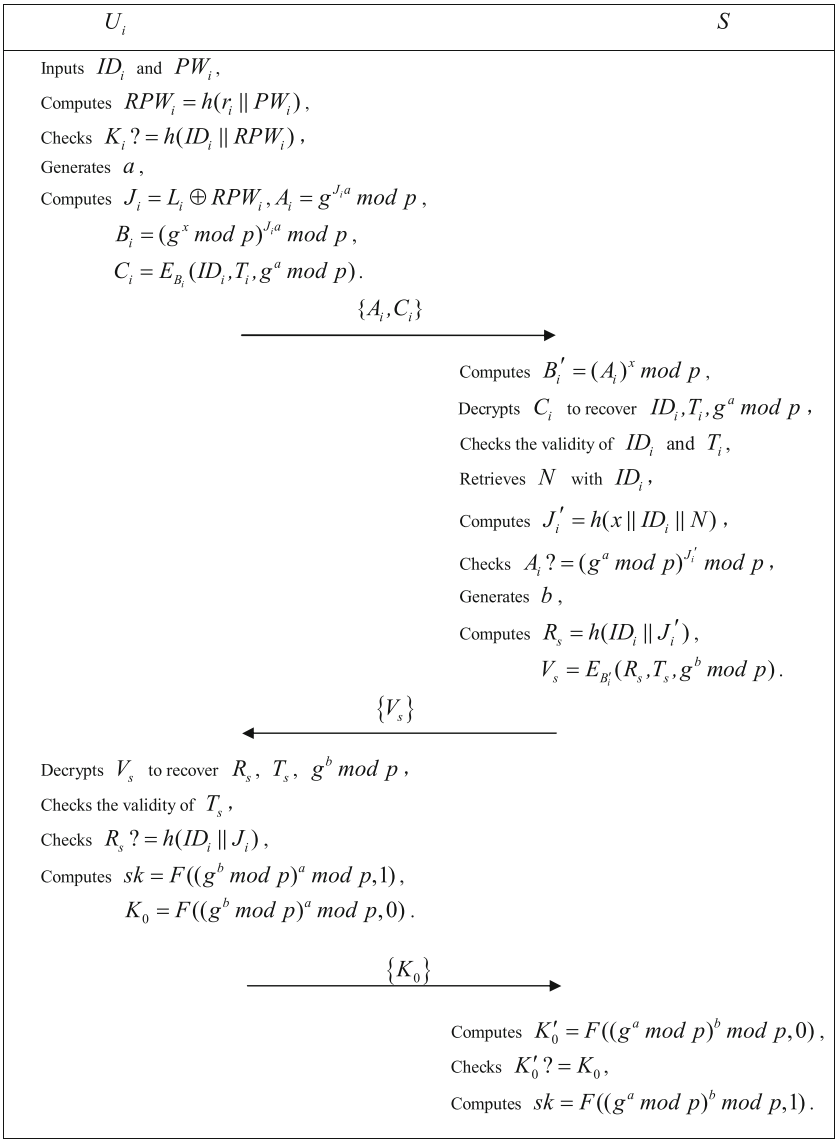

Fig. 2 Login phase and authentication phase

Authentication phase

Step 1. On receiving $\{A_i, C_i\}$ from U_i, S computes $B_i' = (A_i)^x \bmod p$ and decrypts C_i using B_i' to recover ID_i, T_i, $g^a \bmod p$. Subsequently, S checks the validity of ID_i and T_i. If either or both are invalid, the login request is rejected.

Step 2. S retrieves N from the account table with ID_i and computes $J_i' = h(x \| ID_i \| N)$, $A_i' = (g^a \bmod p)^{J_i'} \bmod p$. Then S compares the computed A_i' with the received A_i. If they are equal, the legitimacy of U_i is ensured; on the contrary, S terminates this session immediately.

Step 3. S acquires the timestamp T_s and generates a random number b, then computes $R_s = h(ID_i \| J_i')$, $V_s = E_{B_i'}(R_s, T_s, g^b \bmod p)$. Afterwards, S sends the mutual authentication message $\{V_s\}$ to U_i.

Step 4. Upon receiving the reply message $\{V_s\}$ at T_s', U_i decrypts V_s to recover the values R_s, T_s, $g^b \bmod p$ with B_i. Then U_i checks the validity of T_s. If $T_s' - T_s \geq \Delta T$, U_i terminates this session; otherwise, proceeds to Step 5.

Step 5. U_i computes $h(ID_i \| J_i)$ and compares it with the decrypted R_s. If they are equal, the server S is authenticated by U_i; otherwise, this session is terminated. Finally, U_i computes $K_0 = F(g^{ab}, 0)$ and set the session key as $sk = F(g^{ab}, 1)$ shared with S, where F denotes a pseudo-random function. U_i sends the K_0 to the server.

Step 6. The server computes $K_0' = F(g^{ab}, 0)$ and verifies whether $K_0 = K_0'$ or not. If it is true, the server accepts the user and computes the session key $F(g^{ab}, 1)$ shared with U_i.

Password change phase

This phase is invoked whenever U_i wants to change his/her password PW_i with a new password PW_i^{new}.

Step 1. U_i inserts his/her smart card into a card reader and keys in ID_i, PW_i and requests to change the password.

Step 2. The smart card computes $RPW_i = h(r_i \| PW_i)$, $K_i' = h(ID_i \| RPW_i)$ and checks whether $K_i' ?= K_i$. If the equation holds, proceeds to Step 3; otherwise, this phase is terminated.

Step 3. U_i inputs a new password PW_i^{new} twice for correctness of PW_i^{new}. Note that if the input passwords are not consistent, the smart card will ask him/her to key in a new password twice again. If the input passwords are consistent, the smart card computes $RPW_i^{new} = h(r_i \| PW_i^{new})$, $L_i = L_i \oplus RPW_i \oplus RPW_i^{new}$ and $K_i^{new} = h(ID_i \| RPW_i^{new})$. Then the smart card replaces L_i, K_i with L_i^{new}, K_i^{new}, respectively.

Lost smart card revocation phase

If U_i's smart card is lost or stolen, he/she could re-register at S through the secure channel as registration phase. After the verification of the identity ID_i, S retrieves the entry (ID_i, N) from the account table and sets $N = N + 1$, then stores the new (ID_i, N) in its database. Afterwards, S computes the security parameters of the patient and issues a new smart card to him/her as depicted in the registration phase.

Security analysis of the proposed scheme

Security analysis based on BR93 model

Below we prove that the proposed authentication and key agreement scheme is secure in the security model presented in Section 1.

Theorem 1 *If the symmetric-key encryption scheme is secure against adaptively chosen plaintext attack, and the function F is a secure pseudo-random function, then the proposed authentication and key agreement scheme is secure under the DDH assumption.*

Proof Let $\mathcal{B}$ be an adversary against proposed authentication protocol. We separate the proof into two cases, based on the factor that is leaked to the adversary. □

Case 1. The password is leaked. (1.1) We first consider the situation that the test query is made to an instance belonging to a user. Below we define a sequence of games with Game 0 being the original security game defined in Section 1.

Game 1. This game is the same as the original game, except that before the adversary begins, a random value $m \leftarrow \{1, 2, ..., l_u\}$ is chosen where l_u denotes the maximum number of user instances that would be activated in the game. If the Test query is not made to the m-th instance, then the simulation halts and a random bit b' is returned.

Game 2. This game is the same as Game 1, except that if the adversary successfully forges a valid response V_s with respect to U_i before or in the test session, then the simulation halts and a random b' is returned.

Game 3. This game differs from the previous one in the following way: a random value $\gamma = g^r$ is chosen and the value g^{ab} used in the protocol is replaced with γ.

Game 4. In this game, we replace $F(g^r, \cdot)$ with a truly random function $RF(\cdot)$.

In the analysis below, we use σ_i to denote the event that $b' = b$, and τ_i to denote the advantage of the adversary, in Game i.

Analysis of Games 1: Let E denote the event that the m-th session is the test session. We have

$$\begin{aligned}\Pr[\sigma_1] &= \Pr[\sigma_1|E]\Pr[E] + \Pr[\sigma_1|\overline{E}]\Pr[\overline{E}] \\ &= \Pr[\sigma_1|E]\Pr[E] + 1/2(1 - \Pr[E]) \\ &= (\Pr[\sigma_1|E] - 1/2)\Pr[E] + 1/2 \\ &= 1/l_u(\Pr[\sigma_0] - 1/2) + 1/2\end{aligned}$$

Hence,

$$\tau_1 = \Pr[\sigma_1] - 1/2 = \tau_0/l_u.$$

Analysis of Game 2: Since the symmetric encryption scheme E is ind-cpa secure, the difference between Game 1 and Game 2 is bounded by

$$\tau_1 \leq \tau_2 + \mathbf{Adv}_E^{ind-cpa}(k).$$

Analysis of Game 3: If $\mathcal{B}$ can distinguish Game 2 from Game 3, then we can construct adversary $\mathcal{D}$ which can break the DDH assumption. Let $\alpha = g^x, \beta = g^y, \gamma$ be the DDH problem $\mathcal{D}$ aims to solve. When m-th session is activated, $\mathcal{D}$ uses its inputs (α, β, γ) instead of the values g^a, g^b, g^{ab} in the test session. Notice that since the adversary cannot forge a valid response V_s in Game 2, $\mathcal{D}$ can successfully plant the DDH problem into the test session. $\mathcal{D}$ outputs 1 if $\mathcal{B}$ wins, and 0 otherwise. Then we

have,

$$\begin{aligned}&\mathbf{Adv}_{\mathcal{D}}^{ddh}\\&= \Pr[\mathcal{D} \rightarrow 1|\gamma = g^{xy}] - \Pr[\mathcal{D} \rightarrow 1|\gamma = g^{r}]\\&= \Pr[\mathcal{B}\ wins|\gamma = g^{xy}] - \Pr[\mathcal{B}\ wins|\gamma = g^{r}]\\&= \Pr[\sigma_2] - \Pr[\sigma_3]\end{aligned}$$

and

$$\tau_2 \leq \tau_3 + \mathbf{Adv}^{ddh}(k).$$

Analysis of Game 4: since the function F is a secure pseudo-random function, the difference between Game 2 and Game 3 is also negligible, and we have

$$\tau_3 \leq \tau_4 + \mathbf{Adv}_{F}^{prf}(k).$$

In Game 4, we can see that the key returned to the test query is random no matter $b = 0$ or $b = 1$, so $\Pr[\sigma_4] = \frac{1}{2}$ and $\tau_4 = 0$.

Combining the above results, we can conclude:

$$\tau_0 \leq l_u(Adv^{ddh}(k) + \mathbf{Adv}_{F}^{prf}(k) + \mathbf{Adv}_{E}^{ind-cpa}(k)).$$

(1.2) We then consider that the test query is made to an instance of S.

Game 1. is the same as in the case (1.1). That is we guess that the test query will be made to the m-th instance of the server S (assume that there are at most l_s server instances). Let U_i denote the user involved in the test session.

Game 2. This game is the same as Game 1, except that if the adversary successfully forges a valid login request C_i with respect to U_i before or in the test session, then the simulation halts and a random b' is returned.

Game 3. and Game 4. are the same as in case (1.1).

Analysis of Game 2: Since the symmetric encryption scheme E is ind-cpa secure, the difference between Game 1 and Game 2 is bounded by

$$\tau_1 \leq \tau_2 + \mathbf{Adv}_{E}^{ind-cpa}(k).$$

Game 3 and Game 4 are the same as in the case (1.1), and therefore, we have

$$\tau_0 \leq l_s(\mathbf{Adv}_{E}^{ind-cpa}(k) + \mathbf{Adv}^{ddh}(k) + \mathbf{Adv}_{F}^{prf}(k)).$$

Case 2. The smart card data is leaked. (2.1) The test query is made to an instance belonging to a user. The proof is the same as in (1.1) and is omitted here.

(2.2) The test query is made to an instance belonging to the server.The proof is the same as in (1.1) and is omitted here. Therefore, we have

$$\tau_0 \leq l_s(\mathbf{Adv}_{E}^{ind-cpa}(k) + \mathbf{Adv}^{ddh}(k) + \mathbf{Adv}_{F}^{prf}(k)).$$

where l_s denotes the number of send queries made by $\mathcal{B}$ in the game.

Discussion on the other possible attacks

In the following, we analyze our proposed scheme and show that it can preserve user privacy and is secure to against various threats.

Patient's privacy protection

It is very essential for a secure authentication scheme for TMIS to provide patient privacy. In the proposed scheme, the patient's identity is hidden in $C_i = E_{B_i}(ID_i, T_i, g^a\ mod\ p)$. If the adversary wants to retrieve the patient's identity ID_i from C_i, he/she has to compute $B_i = (g^x\ mod\ p)^{J_i a}\ mod\ p$ from $A_i = g^{J_i a}\ mod\ p$ and $g^x\ mod\ p$, then he/she will face with the Computational Diffie-Hellman problem. Furthermore, the login request message $\{A_i, C_i\}$ varies in each session run due to the randomness of a and T_i. Therefore, it is impossible for the adversary to identify and trace the patient who is involved in the authentication session. In other words, the proposed scheme achieves patient anonymity and untraceability.

Off-line password guessing attack

Suppose that an adversary has obtained the secret parameters $\{L_i, K_i\}$ stored in the smart card of another legitimate patient U_i [18, 19], then he/she tries to get U_i's password from $K_i = h(ID_i \| RPW_i) = h(ID_i \| h(r_i \| PW_i))$ by launching off-line password guessing attack. However, the attacker has to guess both ID_i and PW_i at the same time. As pointed in [21], the probability of crack a veritable password (or identity) comprised by n characters is approximately $\frac{1}{2^{6n}}$. In the proposed scheme, the probability of crack the correct ID_i comprised by m characters and PW_i, which incorporated in K_i simultaneous is approximately $\frac{1}{2^{6(n+m)}}$. Since there can be a huge number of users in the system, it is infeasible for an adversary to do an exhaustive search for all the possible (ID, password) pairs. However, we remark that if the user ID space is small, then offline password guessing attack would become feasible if the smart card of a user is stolen and compromised by the attacker. On the other hand, since the attacker didn't know the secret key x, he/she could not obtain U_i's password from the message $L_i = J_i \oplus RPW_i = J_i \oplus h(r_i \| PW_i) = h(x \| ID_i \| N) \oplus h(r_i \| PW_i)$.

Replay attack

The replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. The proposed scheme is capable of detecting and resisting the replay attack since the random nonce and timestamp is contained in each session run. If an

Table 2 Comparisons of functionality

	Jiang et al.'s	Wu et al.'s	Ours
Prevention of impersonation attack	No	No	Yes
Prevention of off-line password guessing attack	No	No	Yes
Prevention of server spoofing attack	Yes	No	Yes
Prevention of replay attack	Yes	Yes	Yes
Preserving patient privacy	No	No	Yes
Freely change password	No	No	Yes
Known key security	Yes	Yes	Yes
Perfect forward secrecy	Yes	Yes	Yes

adversary eavesdrops and replays any authentication message exchanged between U_i and S, the replayed message can be easily detected and dropped.

Authentication proof based on BAN-logic

BAN logic [20] is a logic of belief which focuses on the beliefs of the legitimate principals involved in the protocol. It has been highly successful in analyzing the security of authentication schemes. In this section, we demonstrate that the proposed scheme is working correctly by achieving the authentication goals using BAN logic. The notations used in BAN logic analysis are defined as follows:

- $P \mid\equiv X$: The principal P believes a statement X or P would be entitled to believe X.
- $\sharp(X)$: The formula X is fresh.
- $P \Rightarrow X$: The principal P has jurisdiction over the statement X.
- $P \lhd X$: The principal P sees the statement X.
- $P \mid\sim X$: The principal P once said the statement X.
- (X, Y): The formula X or Y is one part of the formula (X, Y).
- $\{X\}_Y$: The formula X is encrypted under the key Y.
- $P \overset{K}{\longleftrightarrow} Q$: The principal P and Q use the shared key K to communicate. Here, K will never be discovered by any principal except for P and Q.
- sk: The session key used in the current session.

Some main logical postulates of BAN logic are described as follows:

- The message-meaning rule: $\frac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$.
- The freshness-conjuncatenation rule: $\frac{P \mid\equiv \sharp(X)}{P \mid\equiv \sharp(X,Y)}$.
- The nonce-verification rule: $\frac{P \mid\equiv \sharp(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$.
- The jurisdiction rule: $\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$.

According to the analytic procedures of BAN logic, we list the verification goals of the proposed scheme as follows:

Goal.1: $U_i \mid\equiv (U_i \overset{sk}{\longleftrightarrow} S)$
Goal.1: $S \mid\equiv (U_i \overset{sk}{\longleftrightarrow} S)$

Next, the proposed scheme is arranged from the generic type to the idealized form in the following:

Message 1: $U_i \rightarrow S$: $\{ID_i, T_i, g^a \ mod \ p\}_{B_i}$
Message 2: $S \rightarrow U_i$: $\{R_s, T_s, g^b \ mod \ p\}_{B_i}$

We make the following assumptions about the initial state of the scheme to further analyze the proposed scheme:

A.1: $U_i \mid\equiv \sharp(g^a \ mod \ p)$
A.2: $S \mid\equiv \sharp(g^b \ mod \ p)$
A.3: $U_i \mid\equiv (U_i \overset{B_i}{\longleftrightarrow} S)$
A.4: $S \mid\equiv (U_i \overset{B_i}{\longleftrightarrow} S)$
A.5: $U_i \mid\equiv S \Rightarrow g^b \ mod \ p$
A.6: $S \mid\equiv U_i \Rightarrow g^a \ mod \ p$

Based on the above-mentioned assumptions and rules of BAN logic, we analyze the idealized form of the proposed scheme and the main procedures of proof as follows:

According to the message 1, we obtain:

$$S \lhd \{g^a \ mod \ p\}_{B_i}.$$

According to the assumption A.4 and the message meaning rule, we obtain:

$$S \mid\equiv U_i \mid\sim g^a \ mod \ p.$$

Table 3 Performance comparisons

		Jiang et al.'s	Wu et al.'s	Ours
Computation cost	U_i	$3T_h+T_s$	$6T_h+2T_s$	$3T_h+T_m+4T_e+2T_s$
	S	$3T_h+3T_s$	$5T_h+2T_s$	$2T_h+4T_e+2T_s+T_F$
Communication cost		4	4	5

According to freshness-conjuncatenation rule and the nonce verification rule, we obtain:

$S \mid\equiv U_i \mid\equiv g^a \ mod \ p.$

According to the assumption A.6 and the jurisdiction rule, we obtain:

$S \mid\equiv g^a \ mod \ p.$

According to $sk = F(g^{ab}, 1)$, we obtain:

$S \mid\equiv (U_i \overset{sk}{\longleftrightarrow} S)$(**Goal 2**).

According to the message 2, we obtain:

$U_i \triangleleft \{g^b \ mod \ p\}_{B_i}.$

According to the assumption A.3 and the message-meaning rule, we obtain:

$U_i \mid\equiv S \mid\sim g^b \ mod \ p.$

According to freshness-conjuncatenation rule and the nonce-verification rule, we obtain:

$U_i \mid\equiv S \mid\equiv g^b \ mod \ p.$

According to the assumption A.5 and the jurisdiction rule, we obtain:

$U_i \mid\equiv g^b \ mod \ p.$

According to $sk = F(g^{ab}, 1)$, we obtain:

$U_i \mid\equiv (U_i \overset{sk}{\longleftrightarrow} S)$(**Goal 1**).

Performance and functionality analysis

In this section, we will evaluate the performance and functionality of the modified scheme and make comparisons with two related schemes: Jiang et al.'s scheme [13] and Wu et al.'s scheme [14]. The comparison based on the key security among these schemes is given in Table 2, while we compare their efficiency in terms of computation and communication cost in Table 3. Let T_h, T_s, T_F, T_m and T_e be the time for performing an one-way hash function, a symmetric encryption/decryption, a pseudo-random function, a modular multiplication and a modular exponentiation, respectively.

It is visible from Table 2 that the proposed scheme provides better security than the other two related schemes. Jiang et al.'s scheme only satisfies four criterion listed in Table 2. Wu et al.'s scheme does not satisfy five of the eight criterion. While the proposed scheme can achieve all requirements listed in Table 2. Note that, the proposed scheme offers the patient anonymity and untraceability which are the most important features of an authentication scheme for TMIS.

From Table 3, we can see that the total computation cost in the login phase and authentication phase of Jiang et al.'s scheme, Wu et al.'s scheme, the proposed scheme are $6T_h + 4T_s$, $11T_h + 4T_s$, $5T_h + T_m + 8T_e + 4T_s + T_F$. Compared with the other two related schemes, our scheme needs more computational cost and communication cost. Nevertheless, our scheme can thwart many security threats identified in these schemes and provide more additional security features.

Conclusion

In this article, we have demonstrated that the recently proposed Wu et al.'s authentication scheme for TMIS could not achieve patient privacy and is susceptible to server spoofing attack, off-line password guessing attack, impersonation attack. Besides, the password change phase of Wu et al.'s scheme is unfriendly and inefficient since the patient has to communicate with the medical server to update his/her password. In order to rectify these security flaws, we proposed a new smart card based authentication scheme with privacy protection for TMIS. According to the performance and functionality analysis, we show that the proposed scheme is robust for the telecare medical information systems.

Acknowledgments The authors are grateful to the editor and anonymous reviewers for their valuable suggestions, which improved the paper. This work is supported by Natural Science Foundation of Shandong Province(No.ZR2013FM009).

References

1. Das, M.L. Two-factor user authentication in wireless sensor networks. *IEEE Trans. Wirel. Commun.* 8(3):1086–1090, 2009
2. Hwang, M.S., and Li, L.H., A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* 46(1):28–30, 2000
3. Lee, N.Y., and Chiu, Y.C., Improved remote authentication scheme with smart card. *Comput. Stand. Interfac.* 27(2):177-180, 2005
4. Wen, F.T., Susilo, W., and Yang, G.M., A robust smart card-based anonymous user authentication protocol for wireless communications. *Secur. Comm. Netw.*, doi:10.1002/sec.816, 2013
5. Wen, F.T., Susilo, W, and Yang, G.M., A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless Pers. Commun.* 73(3):993–1004, 2013
6. Yang, G., Wong, D.S., Wang, H., and Deng, X., Two-factor mutual authentication based on smart cards and passwords. *J. Comput. Syst. Sci.* 74(7):1160–1172, 2008
7. Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., and Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012
8. He, D.B., Chen, J.H., and Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989–1995, 2012

9. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3597–3604, 2012
10. Zhu, Z., An effcient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012
11. Chen, H.M., Lo, J.W., and Yeh, C.K., An effcient and secure dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 36(6):3907–3915, 2012
12. Khan, M.K., Kim, S.K., and Alghathbar, K., Cryptanalysis and security enhancement of a more effcient & secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 34(3):305–309, 2011
13. Jiang, Q., Ma, J.F., Ma, Z., and Li, G.S., A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.* 2013. doi:10.1007/s10916-012-9897-0
14. Wu, F., and Xu, L.L., Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. *J. Med. Syst.* doi:10.1007/s10916-013-9958-z, 2013
15. D. Boneh, The Decision Diffe-Hellman Problem. In Proc. Third Algorithmic Number Theory Symposium, Springer press,1998, pp.48-63
16. Mihir, B., and Phillip, R., *Entity authentication and key distribution. Proceedings on Advances in Cryptology (CRYPTO'93)*: Springer press, 22–26, 1993
17. Kumari, S., Khan, M.K., and Kumar, R., Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems. *J. Med. Syst.* doi:10.1007/s10916-013-9952-5, 2013
18. Kocher, P., Jaffe, J., and Jun, B., *Differential power analysis. Proceedings of Advances in Cryptology*: Santa Barbara, CA, USA., 388–397, 1999
19. Messerges, T.S., Dabbish, E.A., and Sloan, E.A., Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002
20. Burrows, M., Abadi, M., and Needham, R., A logic of authentication. *ACM Trans. Comput. Syst.* 8(1):18–36, 1990
21. Chang, Y.F., Yu, S.H., and Shiao, D.R., An uniqueness and anonymity-preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37:9902, 2013