J Med Syst (2013) 37:9958
DOI 10.1007/s10916-013-9958-z

ORIGINAL PAPER

Security Analysis and Improvement of a Privacy Authentication Scheme for Telecare Medical Information Systems

Fan Wu · Lili Xu

Received: 26 March 2013 / Accepted: 18 June 2013 / Published online: 2 July 2013

Abstract Nowadays, patients can gain many kinds of medical service on line via Telecare Medical Information Systems(TMIS) due to the fast development of computer technology. So security of communication through network between the users and the server is very significant. Authentication plays an important part to protect information from being attacked by malicious attackers. Recently, Jiang et al. proposed a privacy enhanced scheme for TMIS using smart cards and claimed their scheme was better than Chen et al.'s. However, we have showed that Jiang et al.'s scheme has the weakness of ID uselessness and is vulnerable to off-line password guessing attack and user impersonation attack if an attacker compromises the legal user's smart card. Also, it can't resist DoS attack in two cases: after a successful impersonation attack and wrong password input in Password change phase. Then we propose an improved mutual authentication scheme used for a telecare medical information system. Remote monitoring, checking patients' past medical history record and medical consultant can be applied in the system where information transmits via Internet. Finally, our analysis indicates that the suggested scheme overcomes the disadvantages of Jiang et al.'s scheme and is practical for TMIS.

F. Wu (✉)
Department of Computer Science and Engineering,
Xiamen Institute of Technology, Huaqiao University,
Xiamen 361021, China
e-mail: conjurer1981@gmail.com

L. Xu
School of Information Science and Technology,
Xiamen University, Xiamen 361005, China

Keywords Mutual authentication · Anonymity · Smart card · Telecare medical information system

Introduction

With the rapid development of computer network technology, the TMIS provide a way for relating patients, doctors and a medical server. By building TMIS, hospitals try to cut down medical and time expenses and meanwhile make the quality of medical service better. Many patients can be diagnosed at home via TMIS. The medical server owns patients' private medical information such as names, telephone numbers, past medical history and so on. Patients can send instant data of their body to the server via the Internet and doctors can give some advice according to the accumulated patients' health data. For some patients who have chronic illnesses, it may save them a lot of time on the way between his own house and the hospital.

Based on the development background, we take part in an initial research on a telecare medical information system for the residents which may be inconvenient to go to hospital. The old or disabled people who have chronic illnesses can get advice from doctors in time and not to go to hospital usually. Also, people may consult the doctors about recent symptoms. Doctors can monitor patients' physiological data and make corresponding decisions for them. The users should be authenticated and the messages between communication entities should be protected. In order to keep privacy, an authentication scheme should be built in the TMIS to enable the service available for legal users, either patients or doctors. So user authentication becomes important for remote systems. Our contribution

is the proposed new secure authentication scheme for this system.

To enhance the security, schemes based on smart cards and passwords have appeared. They belong to two-factor authentication schemes. However, information in the smart card can be extracted[9, 11]. So a successful authentication scheme based on the smart card should still be secure even if the information in the card is stolen.

Recently, many two-factor authentication schemes for TMIS have been raised and unfortunately some of them have been criticized quickly. In 2012, Wu et al. [15] proposed one remote user authentication scheme for telecare medical service. He et al. [5] pointed out Wu et al.'s scheme [15] was vulnerable to impersonation attacks and insider attacks and proposed a new scheme for TMIS. But Wei et al. [13] showed that schemes in [5, 15] were not secure due to no two-factor authentication and proposed an improved scheme to overcome the problem. Soon after that Zhu [17] pointed that scheme in [13] was vulnerable to off-line password guessing attack and proposed a new scheme according to RSA. However, none of the schemes in[5, 13, 15, 17] protects the user's identity secretly. That is to say, the identity of the user in the above schemes are in plaintext over the network.

In 2004, Das et al. [4] proposed a dynamic ID-based authentication scheme to conceal user's identity in transmission. A lot of ID-based schemes have been proposed. However, many of them have been attacked [3, 8, 12, 14]. In 2012, Chen et al. [2] showed that Khan et al.'s scheme [8] did not have the character of anonymity and presented a new dynamic ID-based authentication scheme with smart cards for TMIS. Then Cao et al. [1], Xie et al. [16], Lin [10] and Jiang et al. [7] all demonstrated that Chen et al.'s scheme [2] had weaknesses such as off-line password guessing attack, tracking attack, lack of privacy protection and so on. They also proposed their own scheme respectively. Unfortunately, we find that Jiang et al.'s scheme [7] has useless ID and it is vulnerable to off-line password guessing attack ,user impersonation attack and DoS attack. And we propose an improved authentication scheme for TMIS which can protect the user's privacy.

The rest of the paper is organized as follows. In next section we give some notations and definitions throughout this paper. In Section "Review of Jiang et al.'s scheme" we briefly review their scheme. Then the Section "Security analysis of Jiang et al.'s scheme" shows its disadvantages. In Section "System environment and the improved scheme" and Section "Security analysis and comparison", we propose the framework of the project and an improved authentication scheme. Then we analyze our scheme's security and performance. And in the last Section some conclusions are drawn.

Notations and definitions

In this Section, we list the notations used throughout the paper. They are defined in Table 1. Also, we describe some premises in order to analyze the schemes. They are listed as definitions after Table 1:

Definition 1 A user's password can be collected in a finite set, which can be guessed in polynomial time.

Definition 2 The secret number x in S is a strong key, which can not be guessed in polynomial time.

Definition 3 The hash function $h(.)$ and symmetric key cryptosystem are secure(e.g.SHA-1 and AES).

Definition 4 The attacker A can control over the communication channel between the user and the remote server. And A may either (1) get a user's password, or (2) obtain the smart card and extract secret parameters in it, (3) but not the both above.

Review of Jiang et al.'s scheme

In this Section, we briefly review Jiang' et al.'s scheme [7]. It contains five phases: Registration phase, Login phase, Authentication phase, Password change phase and Lost smart card revocation phase.

Table 1 Notations in the paper

U_i	a user
ID_i	the identity of U_i
PW_i	the password of U_i
S	the remote server for the system
A	the attacker
$\Rightarrow$	a secure channel
$\rightarrow$	an insecure channel
x	S's secret key
T_i	the timestamp generated by U_i
T_s	the timestamp generated by S
N	registration times of U_i
sk	the session key generated between the user and server
$E_{key}(M)$	Encryption of a message M using key
$D_{key}(M)$	Decryption of a message M using key
$h(.)$	a secure one-way hash function
$\oplus$	the bitwise XOR operation
$\|\|$	concatenation

Registration phase

The user registers or re-registers with the remote server. A person who wants to become a new legal user U_i must do the following steps through a secure channel:

(1) $U_i \Rightarrow S : ID_i, RPW_i$.
U_i selects an identity ID_i, a password PW_i and produces a random number r_i. Then he computes $RPW_i = h(r_i||PW_i)$ and sends the message $R = \{ID_i, RPW_i\}$ to the server S.

(2) $S \Rightarrow U_i : card$.
After receiving R, S verifies whether ID_i is valid, and rejects it if it is invalid. Then S checks the account record. If U_i is a new user, S adds $(ID_i, N = 0)$ into the database. Otherwise, S sets $N = N + 1$, chooses a random number b and computes

$$J_i = h(x||ID_i||N)$$

$$L_i = J_i \oplus RPW_i$$

$$AID_i = E_x(ID_i||b)$$

Finally, S stores $(L_i, AID_i, h(.), E_{key}(.), D_{key}(.))$ into a smart card and sends it to U_i.

(3) $U_i \Rightarrow card : r_i$.
U_i stores r_i into the smart card.

Login phase

To login the system, U_i inserts his smart card into the device. Then he inputs ID_i and PW_i.

(1) The smart card retrieves r_i, L_i and AID_i in itself, and computes

$$RPW_i = h(r_i||PW_i)$$

$$J_i = L_i \oplus RPW_i$$

$$C_1 = h(T_i||J_i)$$

(2) $U_i \rightarrow S : m = \{AID_i, T_i, C_1\}$.
U_i sends the login message $m = \{AID_i, T_i, C_1\}$ to S.

Authentication phase

Upon receiving the message m, S follows steps below:

(1) $S \rightarrow U_i : m' = \{C_2\}$.
S checks the validity of the user's timestamp T_i. If it is invalid, S rejects this request. Otherwise, S uses x to decrypt AID_i, obtains ID_i and b and calculates $J_i = h(x||ID_i||N)$. Then S compares whether C_1 is equal to $h(T_i||J_i)$. If it does not hold, S rejects the request. Otherwise, S selects another random number b', computes

$$AID_i' = E_x(ID_i||b')$$

$$C_2 = E_{J_i}(AID_i'||C_1||T_s)$$

and sends $m' = \{C_2\}$ to U_i. At last S can compute $sk = h(J_i||T_i||T_s)$.

(2) After receiving m', the smart card decrypts C_2 to get AID_i', C_1' and T_s, checks the validity of T_s and stops this session if T_s is invalid. Then the card checks the equation $C_1' = C_1$. If $C_1' \neq C_1$, U_i terminates the session. Otherwise, S is authenticated. U_i calculates the session key $sk = h(J_i||T_i||T_s)$. The smart card replaces AID_i with AID_i', which will be used in the user's next login phase.

Password change phase

If U_i wants to change his password, he inserts the smart card and inputs the old password PW_i and the new password PW_i^{new}. Then the card computes

$$RPW_i = h(r_i||PW_i)$$
$$RPW_i^{new} = h\left(r_i||PW_i^{new}\right)$$
$$L_i^{new} = L_i \oplus RPW_i \oplus RPW_i^{new}$$

and replaces L_i with L_i^{new}.

Lost smart card revocation phase

To revoke the lost smart card and request a new one, U_i can re-register with S through the secure channel as the registration phase. S verifies U_i's secret information such as date of birth known to U_i. After validating, S issues a new smart card to U_i.

Security analysis of Jiang et al.'s scheme

Jiang et al. claimed their scheme achieved many security characters. However, in their scheme the user's identity is useless and the scheme is vulnerable to off-line password guessing attack ,user impersonation attack and DoS attack.

ID uselessness

Let's see the login phase of Jiang et al.'s scheme. U_i inputs ID_i and PW_i, but the card does not use ID_i at all. The login message m employs AID_i as the user's identity on the communication channel, which is directly read from the smart card. ID_i is useless in the login phase. The user can input any string as an identity.

Off-line password guessing attack

If the attacker A steals U_i's smart card temporarily, he can extract (L_i, AID_i', r_i) from the card and then return it to U_i. A gets the login and authentication message of U_i: $m = \{AID_i, T_i, C_1\}$ and $m' = \{E_{J_i}(AID_i'||C_1||T_s)\}$. Then A guesses the password as PW_i^*, computes $RPW^* = h(r_i||PW^*)$, $J_i^* = L_i \oplus RPW_i$ and $C_1^* = h(T_i||J_i)$. He can use J_i to get C_1 from decryption of m'. If $C_1^* = C_1$, the password PW^* is correct. Otherwise, A can try the next candidate password. Since T_i, C_1, L_i, r_i are all known to A, A only need to repeat guessing the password until PW_i^* is correct. Because J_i does not vary in different sessions, A can use many Login & Authentication messages between U_i and S to guess the password. Once A has guessed the correct password, J_i, T_s can be obtained and the session key sk can be computed easily.

User impersonation attack

After the above off-line guessing attack, A gets the right password and then he can pass himself off as a legal user. Due to the disadvantage of ID uselessness, A can input a random string for the identity to start a session and impersonate a legal user successfully.

DoS attack

There are two cases of DoS attack:

(1) Once A logins successfully, he can get the next AID_i and make the legal U_i under DoS attack right away. In other words, U_i does not owns the next login information AID_i. So he can not login unless he re-registers again.
(2) In fact, due to the lack of checking password mechanism, Password change phase can always be successful. User might input a wrong old password by mistake and this will lead to a failed login next time. So without verification, changing one's password is insecure. Obviously, there is no password-checking mechanism for Password change phase in Jiang et al.'s scheme. So the scheme is also under this attack. And we find that schemes proposed in[5, 7, 10, 13, 14, 16] are all vulnerable to this attack, too.

System environment and the improved scheme

We first show the structure of system environment and its application. After that, we will present our authentication scheme.

Structure of system environment

First, some medical devices should be placed in residents' houses or a service center in community. For example, cameras, microphones, transducers for collecting temperature and signals of pulse, blood pressure and so on are needed in the terminal. The collected information should be transmitted via the communication channel. In Fig. 1, if the patient requests a medical help, he should login with his smart card at the beginning. Then the user uses devices to collect body data and sends the information to the server. The doctor should also have identity checked first. According to the patient's video, audio body information and history data, the doctor can communicate with the patient and give some advice to the patient for concrete symptoms. At the end of the diagnosis, the doctor verifies the service the patient requested before and the patient pays the bill. Moreover, a patient can access his own health history data, too.

All users of this system must register on the server first and the server issues a smart card to the user. These data flows are via a secure channel. Then the legal user uses his own smart card with devices like personal computers and notebooks to login in. Of course the messages from Login phase to the end of the session are in insecure channel.

Our proposed scheme also has five phases: Registration phase, Login phase, Authentication phase, Password change phase and Lost smart card revocation phase. In Fig. 2, we show the Registration, Login and Authentication phase. The details are as follows:

Registration phase

U_i can register or re-register at the remote server S and perform the following steps through a secure channel:

(1) $U_i \Rightarrow S : ID_i, RPW_i$.
U_i chooses his identity ID_i, a password PW_i and generates a random number r_i. Then he calculates $RPW_i = h(r_i||PW_i)$ and sends the message $R = \{ID_i, RPW_i\}$ to S.
(2) $S \Rightarrow U_i : card$.
Upon receiving R, S checks if ID_i is valid. If it is invalid, S rejects it. Then S checks the account records in database. If U_i is a new user, S adds $(ID_i, N = 0)$ into the database. Otherwise, S sets $N = N + 1$ and stores it. Then S calculates

$$J_i = h(x||ID_i||N)$$
$$L_i = J_i \oplus RPW_i$$
$$e_i = h(x) \oplus h(RPW_i||ID_i)$$

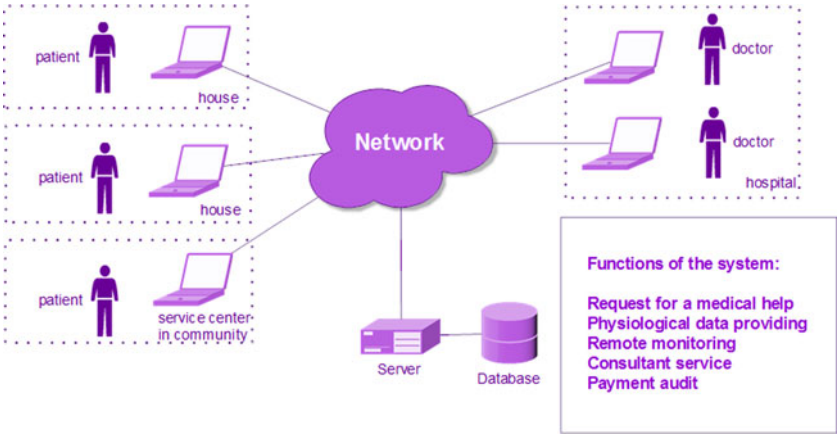

Fig. 1 Simple frame of our system

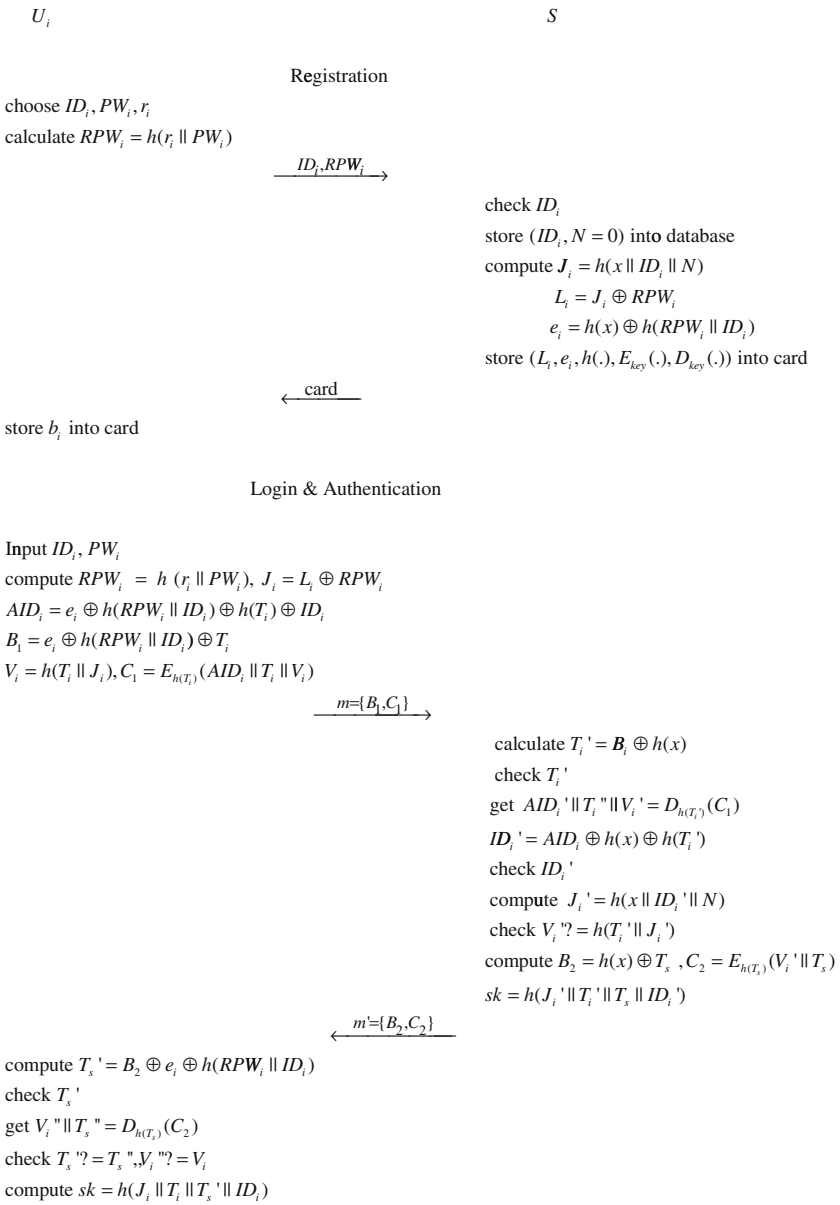

Fig. 2 Registration, Login & Authentication phases of our scheme

Finally, S stores $(L_i, e_i, h(.), E_{key}(.), D_{key}(.))$ into a smart card and issues it to U_i.

(3) $U_i \Rightarrow card : r_i$.
U_i stores r_i into the smart card.

Login phase

When U_i wants to login the system, he inserts his smart card into the card reader and inputs ID_i with PW_i. The messages between U_i and S transmit via an insecure channel.

(1) The smart card retrieves r_i, L_i and e_i, and computes

$$RPW_i = h(r_i||PW_i)$$
$$J_i = L_i \oplus RPW_i$$
$$AID_i = e_i \oplus h(RPW_i||ID_i) \oplus h(T_i) \oplus ID_i$$
$$B_1 = e_i \oplus h(RPW_i||ID_i) \oplus T_i$$
$$V_i = h(T_i||J_i)$$
$$C_1 = E_{h(T_i)}(AID_i||T_i||V_i)$$

(2) $U_i \rightarrow S : m = \{B_1, C_1\}$
U_i sends the login message $m = \{B_1, C_1\}$ to S.

Authentication phase

Upon receiving the message m, S does the steps as follows:

(1) $S \rightarrow U_i : m' = \{B_2, C_2\}$.
S computes $T_i' = B_1 \oplus h(x)$, and checks the validity of the user's timestamp T_i'. If it is invalid, S terminates this request. Otherwise, S decrypts C_1 with $h(T_i')$, gets AID_i', T_i'', V_i', and checks if the equation $T_i' = T_i''$ is true. If it does not hold, S rejects the request. Otherwise, S calculates $ID_i' = AID_i' \oplus h(x) \oplus h(T_i')$ and checks whether ID_i' is in the account table. If it is true, S obtains N, computes $J_i' = h(x||ID_i'||N)$ and compares whether V_i' is equal to $h(T_i'||J_i')$. If it does not hold, S rejects the request. Otherwise, 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 $m' = \{B_2, C_2\}$ to U_i.

(2) When U_i receives 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 it passes, U_i should decrypt C_2 with $h(T_s')$ and gets V_i'' and T_s''. U_i checks the equations $T_s' = T_s''$ and $V_i'' = V_i$ and ends the session if either of them is not correct. Otherwise, U_i calculates the session key $sk = h(J_i||T_i||T_s'||ID_i)$.

Password change phase

If U_i wants to change his password, he inserts the smart card and inputs his identity ID_i, the old password PW_i and the new password PW_i^{new}.

(1) It's as same as the Login phase.
(2) It's as same as the first step of Authentication phase. But S need not to compute sk.
(3) After receiving m', the smart card gets T_s' as in Authentication phase, decrypts C_2 with $h(T_s')$ and checks $T_s' = T_s''$ and $V_i'' = V_i$. If either of them is not right, U_i terminates the session. Otherwise, the smart card computes

$$RPW_i^{new} = h\left(r_i||PW_i^{new}\right)$$
$$L_i^{new} = L_i \oplus RPW_i \oplus RPW_i^{new}$$
$$e_i^{new} = e_i \oplus h(RPW_i||ID_i) \oplus h\left(RPW_i^{new}||ID_i\right)$$

and replaces L_i, e_i with L_i^{new}, e_i^{new} respectively.

Lost smart card revocation phase

If U_i has lost his smart card, he can re-register at S through the secure channel as the registration phase. S verifies U_i, makes $N = N+1$ and stores (ID_i, N) into the account table. At last, S issues a new smart card to U_i.

Security analysis and comparison

In this Section, we analyze our scheme. Clearly it can resist general attacks and has common security features. Then we compare it with Jiang et al.'s scheme. The details are as follows:

ID usefulness

In the login and authentication phase, ID_i is used to compute session parameter AID_i and the session key sk. So the user's identity is useful in the scheme.

On-line password guessing attack

On-line password guessing attack denotes that an attacker A can guess a legal user's password on line successfully. To overcome this attack, we can limit the login times of the same identity in a short time. If A tries more times than the upper bound, S can reject the request and do some extra secure steps such as freezing the card.

Off-line password guesssing attack

If A eavesdrops all the messages in the communication channel and steals U_i's smart card, A can get L_i, e_i, r_i, B_1, C_1 and C_2. Because x is unknown to A, A can't guess PW_i via any of above parameters. For example, A guesses a password PW^* to compute $J_i = L_i \oplus h(r_i||PW^*)$, but J_i is protected in V_i and V_i is encrypted by $h(T_i)$. So A has to get T_i to check J_i. If A wants to get T_i, he has only one way, which is to calculate $T_i = B_1 \oplus h(x)$. Unfortunately A can't get x and fails to guess correct PW_i.

Privileged insider attack

The manager of the medical server may impersonate the user if he knows the legal user's password. There is no password table in S in our scheme. And every PW_i is protected by a random number r_i and hash function in the registration, login and password change phase. Therefore our scheme can resist privileged insider attacks.

Stolen-verifier attack

There is no verification table such as hashed passwords or any information containing PW_i. The server S authenticates the user's session by its secret number x and uses no number relating to PW_i. So our scheme is secure against stolen-verifier attack.

Replay attack

Suppose A replays the eavesdropped messages, such as m which is sent to S, he will not succeed. Each message can be checked by the timestamp. So a replayed message can be easily detected and dropped.

Man-in-middle attack

Assume that A intercepts the messages between U_i and S, and replaces part or the whole message with his own faked information to impersonate the user or the server. However, it's impossible for A to fabricate legal messages due to lack of x. The faked message can not pass either side's verification. In other words, the fact A can't produce false session information denotes that our scheme withstands User impersonation attack, Server impersonation attack and Modification attack which are referred in Jiang et al.'s scheme.

Mutual authentication

It's important for the TMIS to let the user and the remote server verify the identity of each other. In fact, once the scheme can withstand user & server impersonation attack, it satisfies the character of mutual authentication. According to the analysis of Man-in-middle attack, we can see this point. Furthermore, in our scheme, the session key formed at the last of Authentication phase is denoted as $h(J_i||T_i||T_s||ID_i)$. Only the server and the user know the elements of the key and can build it without any difficulty. Because the two timestamps are not directly transmitted in the channel, the session key including them means both sides confirm each other. So our scheme satisfies this feature.

DoS attack

Compared to the analysis of DoS attack to Jiang et al.'s scheme, our scheme avoids the two cases. That is to say, weaknesses including off-line password guessing attack and no password-checking do not happen in it. First, our scheme does not employ the method that S gives the next login identity to U_i and it can resist off-line password guessing attack. Thus the first case of DoS attack in Jiang et al. does not exist. Second, in our scheme, U_i must input ID_i and the old PW_i, which are to be authenticated by S. The old password does not pass the verification means legal user's wrong input by mistake or a malicious attacker's trial. Only after the proper authentication, L_i and e_i can be changed correctly. Also, it's certain that the password change phase can be transferred via insecure channel. So our scheme can resist DoS attack.

User anonymity and untraceability

It's obvious that any third party can't know the real identity of U_i, because ID_i is concealed in AID_i and AID_i is encrypted by $h(T_i)$. And T_i is protected in B_1 by $h(x)$, so the attacker A faces the problem to get T_i. Furthermore, AID_i varies in each session because AID_i is generated by the timestamp T_i. It's difficult for A to tell apart U_i from others in communication channel. So our scheme satisfies user anonymity and untraceability.

Known-key security

The session key is produced as $sk = h(J_i||T_i||T_s||ID_i)$ and the two timestamps T_i, T_s can not be same in different sessions. Keys in different sessions are independent of each other. Due to the secure hash function, A can not get the plaintext $J_i||T_i||T_s||ID_i$. So if the attacker A knows some session keys, other session keys will not be affected.

Freely password chosen and update

According to our scheme, the user can randomly choose his password according to his hobbies in registration phase and

Table 2 Security comparison

Characters	Jiang et al.'s	Ours
against On-line password guessing attack	Yes	Yes
against Off-line password guessing attack	No	Yes
against Privileged insider attack	Yes	Yes
against Stolen-verifier attack	Yes	Yes
against Replay attack	Yes	Yes
against User impersonation attack	No	Yes
against Server impersonation attack	Yes	Yes
against Modification attack	Yes	Yes
against DoS attack	No	Yes
Mutual Authentication	Yes	Yes
User anonymity and untraceability	Yes	Yes
ID usefulness	No	Yes
Known-key security	Yes	Yes
Freely password chosen and update	Yes	Yes

change it without restriction when required. So this feature can be satisfied.

Comparisons

Here Table 2 lists security comparisons and Table 3 shows performance comparisons.

From Table 2, it's easy to know our scheme is secure while Jiang et al.'s scheme is under off-line password guessing attacks, user impersonation attacks and DoS attacks.

We use the time cost of hash function and symmetric encryption/decryption in [6], and compare our scheme with Jiang et al.'s in Table 3. T_H denotes the computation time of the hash function, e.g., SHA-1, which costs about 0.5ms. And T_S denotes the computation time of symmetric encryption/ decryption, e.g., AES, which costs about 8.7ms. Other operations, such as XOR and concatenation, cost too little time, so we omits them.

From Table 3, in our scheme the total computation time of registration phase is $4T_H \approx 2$ ms, which is lower than Jiang et al.'s scheme. In Login and Authentication phase, the computation of our scheme costs $11T_H + 4T_S \approx 40.3$ ms totally, while Jiang et al.'s scheme costs $6T_H + 4T_S \approx 37.8$ ms. The time cost of our scheme is 2.5 ms, or 6.6 % more than Jiang et al.'s. But more specifically, the time cost in Server side is less than Jiang et al.'s, with only 19.9 ms in our scheme, reduced by 36.7 %. In other words, our scheme needs more time in user side. It's good for easing the Server's stress. Password change phase in our scheme costs a lot more time because it employs steps in Login phase and part of Authentication phase. However, we should notice that the probability of using password change phase is far less than Login and Authentication. The card revocation phase in two schemes costs the same time as the registration phase respectively, so we omit it. The most important thing is, our scheme is secure and on the contrary, Jiang et al.'s scheme is vulnerable to three different attacks. From the above analysis, we can see that our scheme is better.

Conclusion

In this paper, we show that Jiang et al.'s scheme has some disadvantages including ID uselessness and under off-line password guessing attack, user impersonation attack and DoS attack. In order to overcome those defects, we propose a new scheme for our telecare medical information system research. With analysis we can see that our scheme can resist general attacks and overcome the drawback of Jiang et al.'s scheme. The scheme can protect the messages transmitting through the insecure channel between the user and

Table 3 Performance comparison

Phase		Jiang et al.'s	Ours
Registration	User	$T_H \approx 0.5ms$	$T_H \approx 0.5ms$
	Server	$T_H + T_S \approx 9.2ms$	$3T_H \approx 1.5ms$
	Total	$2T_H + T_S \approx 9.7ms$	$4T_H \approx 2ms$
Login& Authentication	User	$3T_H + T_S \approx 10.2ms$	$6T_H + 2T_S \approx 20.4ms$
	Server	$3T_H + 3T_S \approx 27.6ms$	$5T_H + 2T_S \approx 19.9ms$
	Total	$6T_H + 4T_S \approx 37.8ms$	$11T_H + 4T_S \approx 40.3ms$
Password change	User	$2T_H \approx 1ms$	$5T_H + 2T_S \approx 19.9ms$
	Server	0	$4T_H + 2T_S \approx 19.4ms$
	Total	$2T_H \approx 1ms$	$9T_H + 4T_s \approx 39.3ms$
security		no	yes

According to[6], $T_S \approx 8.7ms$, $T_H \approx 0.5ms$

the server obviously. There's no doubt that our scheme is suitable for using in the TMIS.

Acknowledgments The authors would like to thank the anonymous referees for their invaluable comments.

Conflict of Interests The authors declare that they have no conflict of interest.

References

1. Cao, T., and Zhai, J., Improved dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.*, 2013. doi:1007/s10916-012-9912-5.
2. Chen, H. M., Lo, J. W., Yeh, C. K., An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 36(6):3907–3915, 2012.
3. Das, M. L., Two-factor user authentication in wireless sensor networks. *IEEE Trans. Wirel. Commun.* 8(3):1086–1090, 2009.
4. Das, M. L., Saxena, A., Gulati, V. P., A dynamic id-based remote user authentication scheme. *IEEE Trans. Consum. Electron.* 50(2):629–631, 2004.
5. He, D., Chen, J., Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989–1995, 2012.
6. Hsieh, W. B., and Leu, J. S., Anonymous authentication protocol based on elliptic curve diffie–hellman for wireless access networks. *Wirel. Commun. Mob. Comput.*, 2012. doi:10.1002/wcm.2252.
7. Jiang, Q., Ma, J., Ma, Z., Li, G., A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.*, 2013. doi:10.1007/s10916-012-9897-0.
8. Khan, M. K., Kim, S. K., Alghathbar, K., Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme. *Comput. Commun.* 34(3):305–309, 2011.
9. Kocher, P., Jaffe, J., Jun, B., Differential power analysis. In: *Advances in Cryptology(CRYPTO99).* pp. 388–397. Springer, 1999.
10. Lin, H. Y., On the security of a dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.*, 2013. doi:10.1007/s10916-013-9929-4.
11. Messerges, T. S., Dabbish, E. A., Sloan, R. H., Examining smartcard security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002.
12. Wang, Y., Liu, J., Xiao, F., Dan, J., A more efficient and secure dynamic id-based remote user authentication scheme. *Comput. Commun.* 32(4):583–585, 2009.
13. Wei, J., Hu, X., Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3597–3604, 2012.
14. Wen, F., and Li, X., An improved dynamic id-based remote user authentication with key agreement scheme. *Comput. Electr. Eng.* 38(2):381–387, 2011.
15. Wu, Z. Y., Lee, Y. C., Lai, F., Lee, H. C., Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012.
16. Xie, Q., Zhang, J., Dong, N., Robust anonymous authentication scheme for telecare medical information systems. *J. Med. Syst.*, 2013. doi:10.1007/s10916-012-9911-6.
17. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.