J Med Syst (2015) 39: 65
DOI 10.1007/s10916-015-0229-z

MOBILE SYSTEMS

Robust and Efficient Biometrics Based Password Authentication Scheme for Telecare Medicine Information Systems Using Extended Chaotic Maps

Yanrong Lu · Lixiang Li · Haipeng Peng · Dong Xie · Yixian Yang

Received: 3 November 2014 / Accepted: 11 February 2015 / Published online: 22 April 2015

Abstract The Telecare Medicine Information Systems (TMISs) provide an efficient communicating platform supporting the patients access health-care delivery services via internet or mobile networks. Authentication becomes an essential need when a remote patient logins into the telecare server. Recently, many extended chaotic maps based authentication schemes using smart cards for TMISs have been proposed. Li et al. proposed a secure smart cards based authentication scheme for TMISs using extended chaotic maps based on Lee's and Jiang et al.'s scheme. In this study, we show that Li et al.'s scheme has still some weaknesses such as violation the session key security, vulnerability to user impersonation attack and lack of local verification. To conquer these flaws, we propose a chaotic maps and smart cards based password authentication scheme by applying biometrics technique and hash function operations. Through the informal and formal security analyses, we demonstrate that our scheme is resilient possible known attacks including the attacks found in Li et al.'s scheme. As compared with the previous authentication schemes, the proposed scheme is more secure and efficient and hence more practical for telemedical environments.

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

Y. Lu · L. Li · H. Peng · D. Xie · Y. Yang
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Y. Lu · L. Li (✉) · H. Peng · D. Xie · Y. Yang
National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: li_lixiang2006@163.com

Keywords Authentication · Chebyshev chaotic maps · Smart cards · Telecare medicine information systems

Introduction

With the fast development of information and communication technologies, the demand of low-cost handheld telecommunication systems and customized patient physiological monitoring devices are continuously rising. Meanwhile, more and more people demand for the health promotion and medical services are on the increasing due to the continued population ageing [1]. As a consequence, the above phenomena lead to a gaining popularity for telecare services applications. Telecare is regarded as a time and expense saving substitute compared with traditional medical service. The Telecare Medicine Information Systems (TMISs) build a bridge between patients at home and doctors at a clinical center or home healthcare (HHC) agency [2]. In such system, the patients only need to stay at home, they can still access a convenient and prompt treatment from the medical center over internet or mobile networks [2, 3]. However, one of the most concerned problem of TMISs is the open communication channel between patients and doctors may lead to provide an opportunity for an adversary to gain the privacy of patients. Security of the private data becomes crucial because nobody is willing to reveal his own sensitive information to light. Therefore, how to safeguard information privacy in TMISs during transmission via the insecure network becomes a significant concern.

Authentication mechanisms become an essential need for TMISs when a remote patient tries to access the resources of telecare server. Several authenticated key agreement schemes [4, 11] have been proposed for TMISs. In 2010,

Wu et al. [12] proposed a low computation password based authentication scheme. However, He et al. [13] pointed out that Wu et al.'s scheme was vulnerable to the insider and impersonation attacks. In order to overcome these weaknesses, He et al. proposed an improved scheme. Unfortunately, Wei et al. [14] demonstrated that both of Wu et al.'s scheme and He et al.'s scheme suffered from the off-line password guessing attack. To solve the limitations in the scheme of Wu et al. and He et al., Wei et al. also developed an improved scheme. Later, Zhu [15] showed that Wei et al.'s scheme was insecure against the off-line password guessing attack and also designed an improved authentication scheme. Nevertheless, the high computation overhead caused by modular exponential operations leads to decrease those works for practical applications.

With the rapid development of chaos theory related to cryptography [16, 18], more and more authentication schemes based on chaos theory have been studied widely since it has better performance than traditional cryptography [19]. In 2007, Xiao et al. [20] developed the first chaotic maps based authenticated key agreement protocol using random numbers. After that, Tseng et al. [21] also proposed a user anonymity-preserving chaotic maps-based authentication and key agreement scheme. Unfortunately, Niu et al. [22] found that Tseng et al.'s scheme failed to provide user anonymity. Consequently, Niu et al. also presented an improved scheme to overcome the weakness. However, Xue et al. [23] pointed out that Niu et al.'s scheme was vulnerable to the man-in-the-middle attack. Recently, Guo et al. [24] proposed a chaotic maps-based password authenticated key agreement using smart cards. Unfortunately, both Hao et al. [25] and Lin [26] pointed out that Guo et al.'s scheme could not guarantee user anonymity. To remedy the identified deficiencies, Hao et al. and Lin presented their modified version of Guo et al.'s scheme, respectively. Nevertheless, Jiang et al. [27] and Lee [28] respectively showed that Hao et al.'s scheme did not achieve fairness in session key establishment and suffer from stolen smart card attack. They then developed their improved scheme to conquer the flaws of Hao et al.'s scheme. Unfortunately, Li et al. [29] demonstrated that both Lee's and Jiang et al.'s schemes could not withstand the service misuse attack for non-registered users and provide user identity during authentication phase. While addressing the limitations of Lee's and Jiang et al.'s schemes, Li et al. present a slight modification on Lee's scheme to prevent the shortcomings.

In this paper, we find that Li et al.'s scheme has still some weaknesses such as violation the session key security, vulnerability to user impersonation attack and lack of local verification. To conquer these flaws, we propose a chaotic maps and smart cards based password authentication scheme by applying biometrics technique [30] and hash function operations. Through the informal and formal security analyses, we demonstrate that our scheme is resilient possible known attacks including the attacks found in Li et al.'s scheme. As compared with the previous authentication schemes, the proposed scheme is more secure and efficient and hence more practical for telemedical environments.

The remainder of this paper is organized as follows. Section "Preliminaries" introduces some preliminaries about hash functions and Chebyshev chaotic maps. The review and security analysis of Li et al.'s scheme are shown in Section "Review of Li et al.'s scheme" and Section "Security analysis of Li et al.'s scheme", respectively. Section "Proposed authentication scheme" and "Security analysis" show our proposed scheme and analyze its security. Section "Functionality and performance analysis comparison" depicts the performance and security features comparisons among the proposed scheme and other related ones. Section "Conclusion" is a brief conclusion.

Preliminaries

In this section, we briefly introduce the one-way hash function [31] and Chebyshev chaotic maps [32, 34].

Definition 1 A secure one-way hash function $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$, which takes an input as an arbitrary length binary string $x \in \{0, 1\}^*$ and outputs a binary string $h(x) \in \{0, 1\}^n$. The probability of $\mathcal{A}$ in finding collision is defined as $Adv^{\mathcal{A}}_{HASH}(t_1) = Pr[\mathcal{A}((x, x'), x \neq x') : h(x) = h(x')]$.

Definition 2 Let n be an integer, x is a real number from the set $[-1, 1]$, the Chebyshev polynomial of degree n is defined as $T_n(x) = cos(n \cdot cos^{-1}(x))$.

Definition 3 Given two elements $x, y \in Z^*_p$, the Chaotic Maps Discrete Logarithm Problem (CMDLP) is to find the integer r, such that $y = T_r(x)$. The probability of $\mathcal{A}$ can solve the CMDLP is defined as $Adv^{\mathcal{A}}_{CMDLP}(t_2) = Pr[\mathcal{A}(x, y) = r : r \in Z^*_p, y = T_r(x) mod p]$.

Definition 4 Given three parameters x, $T_r(x)$ and $T_s(x)$, the Chaotic Maps Diffie-Hellman Problem (CMDHP) is to compute $T_{rs}(x)$ such that $T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$.

Review of Li et al.'s scheme

In this section, we will review Li et al.'s extended chaotic maps based password authentication scheme for TMISs. Their scheme is composed of three phases, which are registration, authentication and password change. For convenience, some notations used in this paper are described in Table 1.

Table 1 Notations

$U,\ S$	User and sever
$ID,\ PW$	Identity and password of an entity U
$H(\cdot)$	Biohash function
$h_1(\cdot),\ h_2(\cdot)$	Hash function $h_1 : \{0,1\}^* \rightarrow \{0,1\}^l$, hash function $h_2 : [-1,1] \rightarrow \{0,1\}^l$.
$k_u,\ k_s$	Secret key selected by U and S, respectively
$\oplus,\ \|\|$	Exclusive-or operation and concatenation operation

Registration

(1) U generates a random number b, selects a password PW and sends $\{ID, h_1(ID||h(PW||b))\}$ to S.
(2) S selects a random number r, computes $IM_1 = IM_3 = h(k_s) \oplus r$, $IM_2 = IM_4 = h_1(k_s||r) \oplus ID$, $D_1 = h_1(ID||k_s) \oplus h_1(ID||h_1(PW||b))$. Then, S stores $\{IM_1,\ IM_2,\ IM_3,\ IM_4,\ D_1,\ h_1(\cdot),\ h_2(\cdot)\}$ into U's smart card and issues it to U. Moreover, S keeps a status table which is composed of three fields, i.e., U's identity, latest random number and LB, where LB presents whether U logins into S or not.
(3) U computes $D_2 = h_1(ID||PW) \oplus b$ and stores D_2 into smart card. Now, the smart card contains $\{IM_1, IM_2, IM_3, IM_4, D_1, D_2, h_1(\cdot), h_2(\cdot)\}$.

Authentication

There are two types of authentication processes. Case 1 is satisfied when the latest random number kept by U and S are identical. Case 2 is satisfied when the latest random number kept by U and S are different. We mainly consider case 1 since our cryptanalysis aims at it.

(1) U inserts his smart card into a card reader and enters his identity ID and password PW. Then the smart card generates a random number u and computes $b = h(ID||PW) \oplus D_2$, $K = D_1 \oplus h_1(ID||h(PW||b)) = h_1(ID||k_s)$, $T_u(K)$ and $X_1 = h_1(K||IM_1||IM_2||T_u(K)||T_1)$, where T_1 is the current timestamp. At last, U sends the login request $M_1 = \{IM_1,\ IM_2,\ T_u(K), X_1,\ T_1\}$ to S.
(2) After receiving the message from U, S verifies if $T_2 - T_1 \leq \Delta\ T$ holds or not, where T_2 is the timestamp. If it is so, S computes $r' = IM_1 \oplus h(k_s)$ and $ID' = IM_2 \oplus h_1(k_s||r')$ and checks if $(ID',\ r')$ equals maintained $(ID,\ r)$. If it is found, S computes $K' = h_1(ID'||k_s)$ and checks if $h(K'||IM_1||IM_2||T_u(K)||T_1) \stackrel{?}{=} X_1$. If it holds, S generates two random numbers r_{new} and v and computes $IM_1^* = h_1(k_s) \oplus r_{new}$, $IM_2^* = h_1(k_s||r_{new}) \oplus ID'$, $T_v(K')$, $sk = h_2(T_u(K), T_v(K'), T_v(T_u(K)))$, $Y_1 = IM_1^* \oplus h_1(sk||T_1)$, $Y_2 = IM_2^* \oplus h_1(sk||T_2)$, $Y_3 = h_1(sk||IM_1^*||IM_2^*||T_v(K')||T_2)$ and sends $\{Y_1,\ Y_2,\ Y_3,\ T_v(K'),\ T_2\}$ to U.
(3) On receiving the message from S, U verifies if $T'' - T_2 \leq \Delta\ T$ holds or not. If it holds, U computes $sk' = h_2(T_u(K),\ T_v(K'),\ T_u(T_v(K')))$, $IM_{1new}^* = Y_1 \oplus h_1(sk'||T_1)$, $IM_{2new}^* = Y_2 \oplus h_1(sk'||T_2)$ and checks if computed $h_1(sk'||IM_{1new}^* ||IM_{2new}^* ||T_v(K')||T_2) \stackrel{?}{=} Y_3$. If equivalent, U replaces $\{IM_1, IM_2,\ IM_3,\ IM_4\}$ with $\{IM_{1new}^*,\ IM_{2new}^*,\ IM_1, IM_2\}$. Then, U computes $M_3 = X_2 = h_1(IM_{1new}^* ||IM_{2new}^*||T_u(T_v(K'))||sk'||T_3)$ and sends $\{M_3, T_3\}$ to S.
(4) After receiving the response message from U, S verifies if $T_4 - T_3 \leq \Delta T$ holds or not. If it holds, S checks if computed $h_1(IM_{1new}^*||IM_{2new}^*||T_v(T_u(K))||sk||T_3) \stackrel{?}{=} X_2$. If it is identical, S updates r with r_{new} in its status table.

Password change

U inserts the smart card into the card reader and keys identity ID, original password PW and a new password PW^{new}. Then, the smart card computes $b = D_2 \oplus h_1(ID||PW)$, $D_1' = D_1 \oplus h_1(ID||h(PW||b)) \oplus h_1(ID||h(PW^{new}||b))$, $D_2' = h_1(ID||PW^{new}) \oplus b$ and updates the smart card's memory $D_1,\ D_2$ by $D_1',\ D_2'$.

Security analysis of Li et al.'s scheme

Li et al. claimed that their scheme could resist the session key attack. However, we demonstrate that their scheme is not really secure against the session key attack. Furthermore, we find that their scheme is also unable to protect against user impersonation attack and provide local verification. Now, Let's see the details of these problems.

Violation the session key security

Let $\mathcal{A}$ be an active adversary [35] who steals the smart card of U. Then, $\mathcal{A}$ can extract [36] the secret information $\{IM_1,\ IM_2,\ IM_3,\ IM_4,\ D_1,\ D_2\ h_1(\cdot),\ h_2(\cdot)\}$ and hence he can easily obtain the session key between U and S. The session key proceeds as follows:

(1) $\mathcal{A}$ steals the information $\{ID,\ r\}$ stored in the sever and compromises the server's long-term key [37] k_s' to compute $K = h_1(ID||k_s)$. $\mathcal{A}$ then intercepts the login message $\{IM_1,\ IM_2,\ T_u(K),\ X_1,\ T_1\}$.
(2) Using the approach [38], $\mathcal{A}$ computes $u' = \frac{arcos(T_u(K))+2k\pi}{arcos(x)}$, $v' = \frac{arcos(T_v(K))+2k\pi}{arcos(x)}$, $\forall k \in Z$ to satisfy the equation $T_u(K) = T_{u'}(k)$, $T_v(K) = T_{v'}(K)$.

Then, $\mathcal{A}$ can compute $T_{u'}(T_{v'}(K)) = T_{u'}(T_v(K)) = T_v(T_{u'}(K)) = T_v(T_u(K)) = T_{vu}(K)$. Therefore, $\mathcal{A}$ can get the session key $sk = h_2(T_u(K), T_v(K), T_{vu}(K))$

User impersonation attack

As described in the subsection, $\mathcal{A}$ can also impersonate as a legal user to cheat S when he knows the value of K. The details are described as follows:

(1) $\mathcal{A}$ generates a random number u' and computes $X_1 = h_1(K||IM_1||IM_2||T_{u'}(K)||T_1')$, where T_1' is the current timestamp. Then, $\mathcal{A}$ sends $\{IM_1, IM_2, T_{u'}(K), X_1, T_1'\}$ to S.
(2) When receiving the message from $\mathcal{A}$ who pretends to be U, the messages can successfully pass S's verification and S performs the following scheme normally. Finally, S sends the authenticated message $\{Y_1, Y_2, Y_3, T_v(K), T_2\}$ to $\mathcal{A}$, where v and T_2 are the random number and the current timestamp on sever side, respectively.
(3) Upon $\mathcal{A}$ receiving the authenticated message, he checks if $T_3 - T_2 \leq \triangle T$, where T_3 is the current timestamp. If it holds, $\mathcal{A}$ computes $sk = h_2(T_{u'}, T_v(K), T_{u'v}(K))$, derives the values of IM_{1new}^*, IM_{2new}^* by using sk, computes $X_2 = h_1(IM_{1new}^*||IM_{2new}^*||T_u(T_v(K))||sk||T_4)$ and sends the message $\{X_2, T_4\}$ to S, where T_4 is the current timestamp.
(4) When receiving the message from $\mathcal{A}$, S continues to proceed the scheme without detected. Finally, $\mathcal{A}$ and S "successfully" agree on a session key sk. But unfortunately S mistakenly believes that he is communicating with the legitimate true U.

Lack of local verification

In the login and authentication phases of Li et al.'s scheme, U inputs and directly sends the login message to S. Note that the smart terminal of U does not verify the entered information correctly or not. Therefore, even if U mistakenly keys the wrong information or $\mathcal{A}$ sends an forged message, S will accept and still continue as original scheme. This will result in an unnecessary waste of communication and computational costs.

Proposed authentication scheme

In this section, we will propose a biometrics based password authentication scheme for TMISs using extended chaotic maps. In the proposed scheme, we employ biometrics to conceal password. We adopt Biohashing to protect biometrics of patients, which can resolve high false rejection and hence decrease denial of service access probability [39]. And biohashing is very efficient and lightweight as compared to modular exponentiation and elliptic curve point multiplication [40]. Our scheme consists of three phases: registration, login and authentication and password updating.

Registration

(1) U inputs his biometrics characteristic BIO, selects an identity ID and a password PW. Then U computes $PWD = h_1(PW||H(BIO))$ and submits $\{ID, PWD\}$ to S through a secure channel.
(2) S computes $K = h_1(ID||PWD)$, $IM_1 = K \oplus h_1(k_s)$, where k_s is S's secret key. S then issues a smart card containing $\{IM_1\}$ to U.
(3) U selects a secret key k_u and computes $f = h_1(ID||k_u) \oplus PWD$. U then stores f into smart card. Thus, it is noted that the smart card of U contains the information $\{IM_1, f, h_1(\cdot), h_2(\cdot), H(\cdot)\}$.

Login and Authentication

(1) U first inserts the smart card into a device reader and enters his identity ID, password PW, secret key k_u and also imprints biometric BIO at the sensor. U then checks whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO)) \stackrel{?}{=} f$. If it holds, U computes $K = h_1(ID||h_1(PW||H(BIO)))$, then generates a random number u and computes $R_1 = K \oplus ID$, $R_2 = ID \oplus T_u(K)$, $R_3 = h_1(ID||T_u(K))$. Finally, U sends the message $\{R_1, R_2, R_3\}$ to S.
(2) Upon receiving the message from U, S uses his key k_s to derive K by computing $K' = IM_1 \oplus h(k_s)$, he then computes $ID = R_1 \oplus K$, $T_u(K) = ID \oplus R_2$ and checks $h(ID||T_u(K)) \stackrel{?}{=} R_3$. If it is correct, S then generates a random number v and computes $IM_2 = T_v(K) \oplus ID$, $Auth_s = h_1(K||T_v(K)||sk)$, $T_{uv}(K))$, $sk = h_2(T_u(K), T_v(K)$. Finally, S sends the message $\{Auth_s, IM_2\}$ to U.
(3) After receiving the message from S, U derives $T_v(K)$ by computing $IM_2 \oplus ID$ and computes $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ to verify whether $Auth_s' = h_1(K||T_v(K)||sk)$ is equal to the received $Auth_s$. If it holds, U successfully authenticates S and computes $Auth_u = h_1(sk||T_v(K)||K)$ and then sends the message $\{Auth_u\}$ to S.
(4) Once receiving the message from U, S validates whether $h_1(sk||T_v(k)||K) \stackrel{?}{=} Auth_u$. If it is true, S

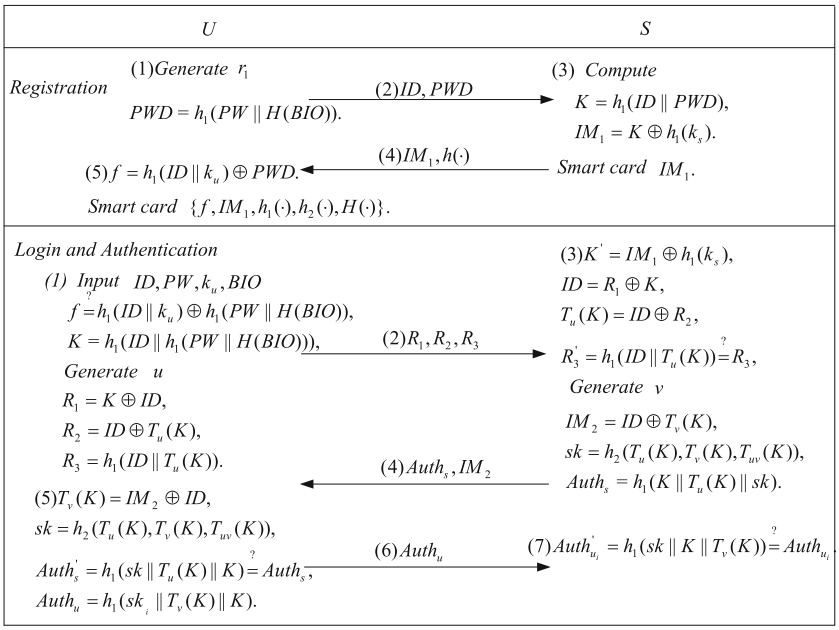

Fig. 1 Our proposed scheme

successfully authenticates U; otherwise, S aborts this request. Finally, U and S have a common session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$.

Password change

If U wants to change password, U inserts his smart card into the card reader and keys in ID, PW, k_u and BIO. Then, the smart card checks $h_1(ID||k_u) \oplus h_1(PW||H(BIO)) \stackrel{?}{=} f$. If it holds, U submits a new password PW^{new} and a new secret key k_u^{new}, the smart card then computes f^{new} and then replaces f with f^{new} (Fig 1).

Security analysis

In this section, we first adopt Burrows-Abadi-Needham (BAN) logic [41] to prove that a session key between U and S can be correctly generated within authentication process. Then, we conduct a security analysis of the proposed scheme through both the informal and formal.

Verifying authentication scheme with BAN logic

BAN logic [41] is a set of rules for defining and analyzing information exchange schemes. It helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both. It has been highly successful in analyzing the security of authentication schemes [42]. In this subsection, we prove that a session key between communicating parties can be correctly generated within authentication process using BAN logic. First, we introduce some notations and logical postulates of BAN logic that we will used in our scheme (Table 2).

(1) BAN logical postulates

a. Message-meaning rule: $\frac{A|\equiv A \stackrel{K}{\leftrightarrow} B,\ A \triangleleft \{X\}_K}{A|\equiv |B \sim X}$: if A believes that the key K is shared by A and B, and sees X encrypted with K, then A believes that B once said X.
b. Nonce-verification rule: $\frac{A|\equiv \#X,\ A|\equiv B|\sim X}{A|\equiv B|\equiv X}$: if A believes that X could have been uttered only recently and that B once said X, then A believes that B believes X.
c. The belief rule: $\frac{A|\equiv X,\ A|\equiv Y}{A|\equiv (X,\ Y)}$: if A believes X and Y, then A believes $(X,\ Y)$.
d. Fresh conjuncatenation rule: $\frac{A|\equiv \#X}{A|\equiv \#(X,\ Y)}$: if A believes freshness of X, B believes freshness of $(X,\ Y)$.
e. Jurisdiction rule: $\frac{A|\equiv B \Rightarrow X,\ A|\equiv B|\equiv X}{A|\equiv X}$: if A believes that B has jurisdiction over X and A trusts B on the truth of X, then A believes X.

Table 2 BAN logic notations

$A\| \equiv X$	A believes a statement X
$U \stackrel{K}{\leftrightarrow} S$	Share a key K between user and sever
$\#X$	X is fresh
$A \triangleleft X$	A sees X
$A\| \sim X$	A said X
$\{X,\ Y\}_K$	X and Y are encrypted with the key K.
$(X,\ Y)_K$	X and Y are hashed with the key K.
$< X >_K$	X is xored with the key K

(2) Idealized scheme

$U : < ID >_{U \overset{K}{\longleftrightarrow} S}, < ID >_{\{U \overset{K}{\longleftrightarrow} S\}_u}, (ID)_{\{U \overset{K}{\longleftrightarrow} S\}_u}$,

$(U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_v)_{U \overset{K}{\longleftrightarrow} S}$

$S : (U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_u)_{U \overset{K}{\longleftrightarrow} S}, < ID >_{\{U \overset{K}{\longleftrightarrow} S\}_v}$

(3) Establishment of security goals

$g_1. U| \equiv S| \equiv U \overset{sk}{\longleftrightarrow} S$

$g_2. U| \equiv U \overset{sk}{\longleftrightarrow} S$

$g_3. S| \equiv U| \equiv U \overset{sk}{\longleftrightarrow} S$

$g_4. S| \equiv U \overset{sk}{\longleftrightarrow} S$

(4) Initiative premises

$p_1. U| \equiv \#u$

$p_2. S| \equiv \#v$

$p_3. U| \equiv U \overset{K}{\longleftrightarrow} S$

$p_4. S| \equiv U \overset{K}{\longleftrightarrow} S$

$p_5. U| \equiv S \Rightarrow (U \overset{sk}{\longleftrightarrow} S)$

$p_6. S| \equiv U \Rightarrow (U \overset{sk}{\longleftrightarrow} S)$

(5) Scheme analysis

a_1. Since p_3 and $U \triangleleft (U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_u)_{U \overset{K}{\longleftrightarrow} S}$, we apply the message-meaning rule to obtain: $U| \equiv S| \sim (U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_u)$.

a_2.Since p_1 and a_1, we apply the fresh conjuncatenation rule and nonce-verification rule to obtain: $U| \equiv S| \equiv (U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_u)$.

g_1. Since a_2 and p_3, we apply the belief rule to obtain : $U| \equiv S| \equiv U \overset{sk}{\longleftrightarrow} S$.

g_2. Since p_5 and g_1, we apply the jurisdiction rule to obtain: $U| \equiv U \overset{sk}{\longleftrightarrow} S$.

a_3. Since p_4 and $S \triangleleft (U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_v)_{U \overset{K}{\longleftrightarrow} S}$, we apply the message-meaning rule to obtain: $S| \equiv U| \sim (U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_v)$.

a_4. Since p_2 and a_3, we apply the fresh conjuncatenation rule and nonce-verification rule to obtain: $S| \equiv U| \equiv (U \overset{sk}{\longleftrightarrow} S, \{U \overset{K}{\longleftrightarrow} S\}_v)$.

g_3. Since a_4 and p_4, we apply the belief rule to obtain: $S| \equiv U| \equiv U \overset{sk}{\longleftrightarrow} S$.

g_4. Since g_3 and p_6, we apply the jurisdiction rule to obtain: $S| \equiv U \overset{sk}{\longleftrightarrow} S$.

As a result, analyzing the security of our scheme with BAN logic, we can now be sure that the proposed scheme is truly capable of achieving the goals.

Informal security analysis

In this subsection, we analyze the security of the proposed scheme to withstand various known attacks including the aforementioned attacks found in Li et al.'s scheme. The following attacks are based on the assumptions that a malicious adversary $\mathcal{A}$ has totally control over the communication channel connecting U and S in login and authentication phases. So $\mathcal{A}$ can intercept, insert, delete, or modify any message transmitted via public channel [43].

User is anonymous

Our scheme can preserve the identity anonymity since ID cannot be derived from R_1 without the knowledge of K. Additionally, K cannot be derived from IM_1 without the server's private key k_s. Also, ID cannot be derived from R_3, owing to the one-way property of the hash function. Therefore, the proposed scheme provides user anonymity.

Insider attack

In the registration of our scheme, U sends $\{ID, h_1(PW||H(BIO))\}$ to S. The privileged insider $\mathcal{A}$ of S cannot get the password PW since it is protected by user's biometrics and the secure hash function. Therefore, our scheme can withstand the insider attack.

Perfect forward secrecy

In the proposed scheme, the session key $sk = H(T_u(K), T_v(K), T_{uv}(K))$ is related with the value K and two random numbers u and v. The value K is hidden by sever's secret key k_s and is computed by user's password PW and biometrics BIO, anyone except U does not know. The two numbers were chosen by U and S, respectively. If $\mathcal{A}$ wants to compute u and v from $T_u(K)$ and $T_v(K)$, he will face the CMDLP. Therefore, our scheme can provide perfect forward secrecy.

Mutual authentication

In the authentication phase of our scheme, U and S can authenticate each other by checking the correctness of $Auth_s$ and $Auth_u$ separately. If $\mathcal{A}$ wants to forge the message, he will face the CMDLP and the CMDHP. Both the validity of $Auth_u$ and $Auth_s$ are confirmed by U and S, respectively. Therefore, mutual authentication between U and S is achieved.

Table 3 Algorithm $EXP_{HASH,\ CMDLP}^{BECMPATMISs,\mathcal{A}}$

1. Eavesdrop login message $\{R_1,\ R_2,\ R_3\}$
2. Call the Reveal oracle 1. Let $(ID',\ T_u'(K)) \leftarrow$ Reveal 1 (R_3)
3. Call the Reveal oracle 2. Let $(\check{u}) \leftarrow$Reveal 2 $(T_u'(K))$
4. Eavesdrop authentication message $\{IM_3,\ Auth_s\}$
5. Call the Reveal oracle 1. Let $(K^*,\ T_u^*(K),\ sk^*) \leftarrow$ Reveal 1 $(Auth_s)$
6. Call the Reveal oracle 2. Let $(\tilde{u}) \leftarrow$ Reveal 2 $(T_u^*(K))$
7. **if** $(\check{u} = \tilde{u})$ **then**
8. Call the Reveal oracle 1. Let $(\dot{ID}, \dot{PWD}) \leftarrow$ Reveal 1 (K^*)
9. **if** $(ID' = \dot{ID})$ **then**
10. Call the Reveal oracle 1. Let $(\hat{PW}, H(\hat{BIO})) \leftarrow$ Reveal 1 $(\dot{PWD})$
11. Accept the derived $\hat{PW}$ and sk^*, as the correct PW of U
12. and the session key sk between U and S, respectively
12. **return** 1 (Success)
16.**else**
17. **return** 0 (Failure)
18. **end if**
19. **else**
20. **return** 0 (Failure)
21. **end if**

Stolen smart card attack

Suppose $\mathcal{A}$ can extract all the information from the smart card by the side channel attack [36]. $\mathcal{A}$ may attempt to retrieve the password from the stolen information, but the password is protected by the elements ID, BIO and k_u that $\mathcal{A}$ does not know. Therefore, our scheme is secure against the stolen smart card attack.

Off-line password guessing attack

$\mathcal{A}$ intercepts the communication between U and S, obtains all messages (R_1, R_2, R_3, $Auth_s$, IM_3, $Auth_u$) and plans to launch an off-line password guessing attack. As we know, all messages are related with U's password and these messages are all "encrypted" by K which is hidden by sever's secret key k_s and is computed by user's password PW and biometric BIO, anyone except U does not know. Thus, $\mathcal{A}$ cannot verify whether his guessed password is right or not. This means our scheme can resist the off-line password guessing attack.

Impersonation attack

$\mathcal{A}$ cannot impersonate the user and the server through the intercepted messages. Since $\mathcal{A}$ has to generate a fresh message if he wants to impersonate the user or the server. Without the user's personal details ID, PW, BIO and k_u, $\mathcal{A}$ cannot generate the legal login message $\{R_1,\ R_2,\ R_3\}$, where $R_1 = K \oplus ID$, $R_2 = ID \oplus T_u(K)$, $R_3 = h_1(ID||T_u(K))$ and $K = h_1(ID||h_1(PW||H(BIO)))$, u is a random number generated by U. Without the server's secret key k_s, $\mathcal{A}$ cannot generate the authentication message $\{Auth_s,\ IM_2\}$ either. Therefore, our scheme can resist the impersonation attack.

Session key security

Suppose $\mathcal{A}$ eavesdrops all the messages $\{R_1, R_2, R_3, Auth_s, IM_2, Auth_u\}$ transmitted in public channel, steals the smart card and extracts [36] the information $\{f, IM_1, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ from it. Then, our scheme can provide session key security as follows: U and S compute a unique session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ in each execution of the scheme. To compute $T_u(K)$/ $T_v(K)$ from R_2/ IM_2, the user's identity ID is needed. In order to retrieve ID from R_1, $\mathcal{A}$ needs to know PW and $H(BIO)$. Since only U can imprint biometrics BIO at the sensor, no adversary can achieve the user's identity ID and PW. On the other hand, anyone except U and S has to compute$T_{uv}(K)$ from $T_u(K)$ and $T_v(K)$ if he wants to get the session key, then he will face to solve the CMDHP. Therefore, the

Table 4 Functionality comparison

Items/Schemes	Ours	[24]	[26]	[27]	[28]	[29]	[32]	[33]	[34]
Provide user anonymity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Provide mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Provide perfect forward secrecy	Yes	-	-	Yes	-	Yes	Yes	Yes	-
Provide Session key security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resist insider attack	Yes	No	Yes	-	-	No	No	Yes	-
Resist impersonation attack	Yes	-	-	Partial	-	No	-	-	-
Resist off-line password guessing attack	Yes	-	-	Yes	Yes	Yes	Yes	-	Yes
No time synchronization	Yes	No	No	No	No	No	Yes	Yes	Yes

proposed authentication scheme can provide session key security.

Formal security analysis of the proposed scheme

In this subsection, we provide the formal security analysis of our scheme and show that our scheme is secure.

Theorem 1 *Under the Definition 3, our scheme is secure against an adversary $\mathcal{A}$ deriving the password PW of a legal user U and the session key sk between U and S if the hash function $h_1(\cdot)$ closely behaves like a random oracle.*

Proof The formal security proof of our scheme is similar to that as in [44, 45]. Using the following oracles to construct $\mathcal{A}$ who will have the ability to derive the user's PW and the session key sk between U and S.

Reveal 1: This random oracle will unconditionally output the input x from the given hash value $y = h_1(x)$.

Reveal 2: This random oracle will unconditionally output r from the given values $y = T_r(x)$ and x.

$\mathcal{A}$ runs the experimental algorithm showed in Table 3, $EXP^{BECMPATMISs,\mathcal{A}}_{HASH,\,CMDLP}$ for our biometric and extended chaotic maps based password authentication scheme for TMISs, say BECMPATMISs.

Define the success probability for $EXP^{BECMPATMISs,\mathcal{A}}_{HASH,CMDLP}$ is $Succ^{BECMPATMISs,\mathcal{A}}_{HASH,CMDLP} = |2Pr[EXP^{BECMPATMISs,\mathcal{A}}_{HASH,CMDLP} = 1] - 1|$ and the advantage function for this experiment then becomes $Adv^{BECMPATMISs,\mathcal{A}}_{HASH,CMDLP}(t, q_{R_1}, q_{R_2}) = max_{\mathcal{A}} Succ^{BECMPATMISs}_{HASH,CMDLP}$, where the maximum is taken over all $\mathcal{A}$ with execution time t and the number of queries q_{R_1}, q_{R_2} made to the Reveal 1 and Reveal 2 oracles, respectively. Consider the experiment showed in Table 3 for $\mathcal{A}$. If $\mathcal{A}$ has the ability to solve the hash function and the CMDLP provided in Definition 1 and Definition 3, then he can directly derive user's PW, and the session key sk between U and S. In this case, $\mathcal{A}$ will discover the complete connections between U and S. However, it is a computationally infeasible problem to invert the input from a given hash value and outputs r from given values $T_r(x)$, i.e., $Adv^{\mathcal{A}}_{HASH}(t_1) \leq \epsilon_1$, $Adv^{\mathcal{A}}_{CMDLP}(t_2) \leq \epsilon_2, \forall \epsilon_1 > 0,\ \epsilon_2 > 0$. Hence, we have $Adv^{BECMPATMISs,\mathcal{A}}_{HASH,\,CMDLP}(t,\ q_{R_1},\ q_{R_2}) \leq \epsilon$, as it is dependent on $Adv^{\mathcal{A}}_{HASH}(t_1)$, $Adv^{\mathcal{A}}_{CMDLP}(t_2)$. Therefore, our scheme is probably secure against $\mathcal{A}$ deriving PW and sk. □

Functionality and performance analysis comparison

In this section, we evaluate the functionality and performance analyses of the proposed scheme and make a comparison with other related schemes [24, 26–29, 32–34]. We list the functionality comparisons between the proposed scheme and other schemes in [24, 26–29, 32–34] are given. Table 4 shows that our scheme is more secure and robust than other related schemes and achieves more functionality features. In the performance comparison, define T_{CCM}, T_E and T_H be the time for performing a Chebyshev chaotic map operation, a symmetric encryption/decryption operation and a hash function, where $T_{CCM} \approx 70T_E \approx 175T_H$ [23]. From Fig. 2, we can see that our scheme takes much less computation to accomplish the mutual authentication and key agreement than the previous chaotic maps based authentication schemes for TMISs.

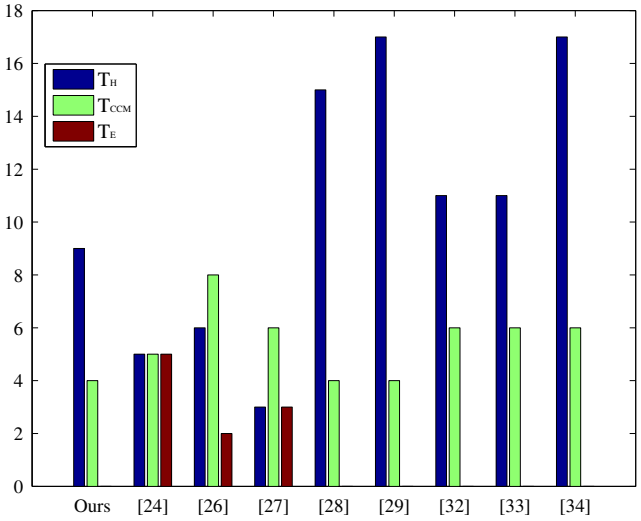

Fig. 2 Performance comparison

Conclusion

In this paper, we analyzed the security weaknesses of one of the most recent chaotic maps and smart cards based authentication schemes for TMISs proposed by Li et al.. Li et al. claimed that their authentication scheme was secure against various known attacks with mutual authentication and key agreement. However, we found that Li et al.'s authentication scheme could not secure against user impersonation attack while failing to provide local verification and the session key security. We further proposed a secure biometric based authentication scheme for TMISs using extended chaotic maps to conquer the security flaws of Li et al.'s scheme. Our proposed scheme is immune to user impersonation attack while providing the session key security and local verification which Li et al.'s scheme fails to satisfy. Meanwhile, our scheme can withstand the trace, off-line

password guessing and stolen smart card attacks. In addition, our scheme achieves the mutual authentication and perfect forward secrecy. We present a cryptanalysis of our scheme through both informal and formal security analyses. Besides, our scheme has the lowest computational cost among other related schemes. Considering the security and efficiency provided by our scheme, we conclude that our scheme is more appropriate for telemedical applications in comparison with other related schemes.

Acknowledgements The authors would like to thank all the anonymous reviewers for their helpful advice. This paper is supported by the National Natural Science Foundation of China (Grant No. 61121061), the Beijing Natural Science Foundation (Grant No. 4142016), and the Asia Foresight Program under NSFC Grant (Grant No. 61411146001).

References

1. Hsu, C.L., Lee, M.R., Su, C.H., The role of privacy protection in healthcare information systems adoption. *J. Med. Syst.* 37(5):1–12, 2013.
2. Lambrinoudakis, C., and Gritzalis, S., Managing medical and insurance information through a smart-card-based information system. *J. Med. Syst.* 24(4):213–234, 2000.
3. 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.
4. Maitra, T., and Giri, D., An efficient biometric and password-based remote user authentication using smart card for telecare medical information systems in multi-server environment. *J. Med. Syst.* 38(12):1–19, 2014.
5. Das, A.K., and Goswami, A., An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *J. Med. Syst.* 38(6):27, 2014.
6. Kim, K.W., and Lee, J.D., On the security of two remote user authentication schemes for telecare medical information systems. *J. Med. Syst.* 38(5):1–11, 2014.
7. Alomair, B., and Poovendran, R., Efficient Authentication for Mobile and Pervasive Computing. *IEEE Trans. Mobile. Comput.* 13(3):469–481, 2014.
8. Sui, Y., Zou, X.K., Du, E.Y., Li, F., Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method. *IEEE Trans on Comput* 63(4):902–916, 2014.
9. Lu, Y.R., Li, L.X., Peng, H.P., Yang, X., Yang, Y.X.: A lightweight ID based authentication and key agreement protocol for multi-server architecture. *Int. J. Distrib. Sens. N.* vol. 2015, Article ID 635890, 9 p, 2015. doi:10.1155/2015/635890.
10. Lu, Y.R., Li, L.X., Yang, Y.X.: Robust and efficient authentication scheme for session initiation protocol. *Math. Probl. Eng.* vol. 2015, Article ID 894549, 9 p, 2015. doi:10.1155/2015/894549.
11. Lu, Y.R., Li, L.X., Peng, H.P., Yang, Y.X.: An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. *J. Med. Syst.* 39(3): 1–8, 2015.
12. 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.
13. He, D.B., Chen, J.H., Zhang, R., A More Secure Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 36(3):1989–1995, 2012.
14. Wei, J., Hu, X., Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3597–3604, 2012.
15. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.
16. Özkaynak, F., and Yavuz, S., Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* 74(3):551–557, 2013.
17. Hussain, I., Shah, T., Gondal, M., Mahmood, H., An efficient approach for the construction of LFT S-boxes using chaotic logistic map. *Nonlinear Dyn.* 71:133–140, 2013.
18. Khan, M., Shah, T., Mahmood, H., Gondal, M., An efficient method for the construction of block cipher with multichaotic systems. *Nonlinear Dyn.* 71:489–492, 2013.
19. Gao, B., Shi, Y.F., Yang, C.L., Li, L.X., Wang, L.C., Yang, Y.X., STP-LWE: A variant of learning with error for a flexible encryption. *Math. Probl. Eng.* 341490:1–7, 2014. Article ID 2014.
20. Xiao, D., Liao, X., Wong, K., An efficient entire chaos based scheme for deniable authentication. *Chaos Soliton. Fract.* 23:1327–1331, 2005.
21. Tseng, H., Jan, R., Yang, W., A chaotic maps-based key agreement protocol that preserves user anonymity. *IEEE Int. Conf. Commun.* 1–6, 2009. ICC09.
22. Niu, Y., and Wang, X., An anonymous key agreement protocol based on chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* 16(4):1986–1992, 2011.
23. Xue, K., and Hong, P., Security improvement on an anonymous key agreement protocol based on chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* 17:2969–2977, 2012.
24. Guo, C., and Chang, C.C., Chaotic maps-based passwordauthenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer. Simul.* 18(6):1433–1440, 2013.
25. Hao, X., Wang, J., Yang, Q., Yan, X., Li, P., A chaotic map-based authentication scheme for telecare medicine information systems. *J. Med. Syst.* 37(2):9919, 2013.
26. Lin, H.Y.: Improved chaotic maps-based password-authenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer, Simul.* doi:10.1016/j.cnsns.2014.05.027, 2014.
27. Jiang, Q., Ma, J., Lu, X., Tian, Y., Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *J. Med. Syst.* 38(2):12, 2014.
28. Lee, T.F., An eEfficient chaotic map-based authentication and key agreement scheme using smart cards for telecare medicine information systems. *J. Med. Syst.* 37(6):9985, 2013.
29. Li, C.T., Cheng, C.L., Chi, Y.W., A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems, *J. Med. Syst.* 38(9):1–11, 2014.
30. Gao, B., Li, L.X., Peng, H.P., Kurths, J., Zhang, W.G., Yang, Y.X., Principle for performing attractor transits with single control in Boolean networks. *Phys. Rev. E* 88,062706, 2013.
31. Stallings, W., *Cryptography and Network Security: Principles and Practices*. 3rd edn. Englewood Cliffs: Prentice Hall, 2003.
32. Li, C.T., Lee, C.C., Weng, C.Y., An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. *Nonlinear Dyn.* 74:1133–1143, 2013.
33. Lee, C.C., Lou, D.C., Li, C.T., An extended chaotic maps-based protocol with key agreement for multiserver environments. *Nonlinear Dyn.* 76(1):853–866, 2014.
34. Lee, C.C., and Hsu, C.W., A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. *Nonlinear Dyn.* 71:201–211, 2013.
35. Zhao, D.W., Peng, H.P., Li, L.X., Yang, Y.X., A secret sharing scheme with a short share realizing the (t, n) threshold and

the adversary structure. *Comput. Math. Appl.* 64(4):611–615, 2012.
36. Messerges, T.S., Dabbish, E.A., Sloan, R.H., Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002.
37. Hölbl, M., Welzer, T., Brumen, B., An improved two-party identity-based authenticated key agreement protocol using pairings, *J. Cmput. Syst.* 78:142–150, 2012.
38. Bergamo, P., Arco, P., Santis, A., Kocarev, L., Security of public key cryptosystems based on Chebyshev polynomials. *IEEE. Trans. Circ. Syst. I* 52:1382–1393, 2005.
39. Lumini, A., and Nanni, L., An improved biohashing for human authentication. *Pattern Recognition* 40(3):1057–1065, 2007.
40. Das, A.K., and Goswami, A., An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *J. Med. Syst.* 38(6):27, 2014.
41. Burrow, M., Abadi, M., Needham, R., A logic of authentication. *ACM Trans. Compu. Syst.* 8:18–36, 1990.
42. Zhao, D.W., Peng, H.P., Li, L.X., Yang, Y.X., A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Pers. Commun.* 78:247–269, 2013. doi:10.1007/s11277-014-1750-y.
43. Lamport, L., Password authentication with insecure communication. *Commun. ACM* 24(11):770–772, 1981.
44. Odelu, V., Das, A.K., Goswami, A., A secure effective key management scheme for dynamic access control in a large leaf class hierarchy. *Inform. Sciences* 269(10):270–285, 2014.
45. Das, A.K., and Bruhadeshwar, B., An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. *J. Med. Syst.* 37:9969, 2013.