A Privacy-Preserving Roaming Authentication Scheme for Ubiquitous Networks

You-sheng Zhou
College of Computer Science and Technology,
Chongqing University of Posts and Telecommunications, Chongqing 400065, CHINA
College of Computer Science,
Chongqing University,
Chongqing 400044, CHINA

Jun-feng Zhou
College of Computer Science and Technology,
Chongqing University of Posts and Telecommunications,
Chongqing 400065, CHINA

Feng Wang
College of Mathematical Sciences,
Dezhou University,
Dezhou 253023, CHINA

***Abstract*—A privacy-preserving roaming authentication scheme (PPRAS) for ubiquitous networks is proposed, in which a remote mobile user can obtain the service offered by a foreign agent after being authenticated. In order to protect the mobile user's privacy, the user presents an anonymous identity to the foreign agent with the assistance of his or her home agent to complete the authentication. After that, the user and the foreign agent can establish a session key using the semi-group property of Chebyshev polynomial. In this way, huge burden of key management is avoided. Furthermore, the user can update the login password and the session key between itself and the foreign agent if necessary. The correctness is proved using BAN logic, and the performance comparison against the existing schemes is given as well.**

Keywords—roaming authentication; anonymous; chaotic maps; key agreement

I. INTRODUCTION

High-speed development of mobile internet has a profound influence on people's daily life. The mobile user wishes to share something or get some resources via mobile devices anytime anywhere and it should not be an issue when he or she locates in the range of the home network provider. However, when a mobile user moves to the region of a foreign network, how does he or she access the foreign network. Undoubtedly, as shown in Fig. 1., the ubiquitous networks should be equipped with authentication and session key establishment before it permits the user to access the Internet provided by itself.

Many authentication and key establishment protocols for mobile networks [1-7] have been proposed in recent years. In 2009 Chang et al. [1] proposed an efficient authentication protocol for mobile devices, which uses one-way hash functions and exclusive-or operation to reduce computation, and they claimed that their scheme can achieve perfect forward secrecy. However, their protocol cannot protect user's privacy since plaintext of real identities are used during the authentication. Later, Chang et al. [2] proposed another enhanced authentication scheme, which uses a random number and one-way hash functions to protect the user's identity, while the scheme cannot prevent insider attack as a malicious inner user can get the real identity at ease. Li et al. [8] proposed an efficient mobile networks authentication scheme, which can protect mobile users' privacy, while it is vulnerable to the man-in-the-middle attacks. Shin et al. [9] and Wen et al.[10] proposed anonymous authentication schemes for mobile networks respectively, while Shin et al.'s [9] scheme cannot resist to the man-in-the-middle attacks, and Wen et al.'s [10] scheme will reveal the user's real identity. In 2014, Xie et al. [11] proposed a mobile roaming authentication protocol and claimed this scheme can protect users' privacy; however, its efficiency is not desirable. Mao et al. [12] proposed an anonymous authentication for global mobility networks in the same year. Recently, Farash et al. [13] proposed a light weight authentication scheme for roaming ubiquitous networks, while it is vulnerable to the replay attacks.

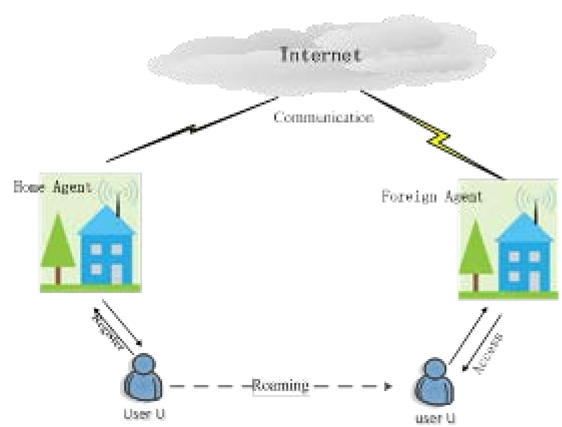

Fig. 1. The scenario of roaming authentication

To improve the security issues, some protocols [14-16] use smart card to authenticate and establish session key. In 2010, Li et al. [15] proposed an efficient authentication protocol using smart card to make user be anonymous, which enhances the security with untraceablility property. Recently, much work on Chebyshev chaotic map based authentication with smart card [17-21] have been done. Juang et al. [22] proposed an authenticated key agreement using smart card, which is privacy-preserving and time-synchronization free. However, in 2009, Sun et al. [23] pointed out that Juang et al.'s [22] scheme suffers inability of the password-changing operation and the session-key problem, hence they proposed an improved authentication protocol using smart card. In 2013, Guo et al. [21] proposed a password-authenticated using smart card. In 2015, Lin et al. [24] proposed an improved chaotic maps based authentication protocol using smart card.

As the popularity of mobile network-enabled devices, people are fond of dealing all work on those devices. However, the private information, for example user identification, may be illegally intercepted and then tracked by the potential attackers. However, the existing schemes either fail to provide privacy preserving or incur huge key management, since traditional symmetric or asymmetric encryption is employed for the handshake message. To address mobile users' privacy effectively, a privacy preserving roaming authentication and key agreement (PPRAS) is proposed in this paper. In PPRAS, the smart card together with chaotic maps is employed to improve efficiency and simplify the session key agreement and key management. In the proposed scheme, the foreign agent can authenticate the mobile user without knowing the user's real identity, then they can agree the shared session key and the temporary identification.

The rest of the article is organized as follows, some related basics are briefly reviewed in section II. The concrete construction of PPRAS is illustrated in section III. Analysis and comparison are presented in section IV. The paper is concluded in the last section.

II. PREMILARIES

A brief introduction of the Chebyshev maps and some related basics are given in this section.

A. Chebyshev Chaotic Maps

Definition 1: Let n be an integer, $x \in [-1,1]$, an n-order Chebyshev polynomial map $T_n(x):[-1,1] \to [-1,1]$ is defined as follows:

$$T_n(x) = \cos(n * \cos(x))$$

According the definition, the recursive form of Chebyshev polynomial map can be produced as follows

$$T_n(x) = 2 * x * T_{n-2}(x) - T_{n-2}(x) \quad , n \geq 2 ,$$

where $T_0(x) = 1$, $T_2(x) = x$, $n \geq 2$.

The Chebyshev polynomial map follows the following two properties

1) Semi-group property

$$T_r(T_s(x)) = \cos(r * \cos^{-1}(s * \cos^{-1}(x)))$$
$$= \cos(r * s * \cos^{-1}(x))$$
$$= T_{sr}(x) = T_s(T_r(x))$$

where r, s are two integers, $x \in [-1,1]$.

2) Chaos property

When n>1 , a n-degree Chebyshev polynomial map $T_n(x):[-1,1] \to [-1,1]$ has the constant measure $f^*(x) = 1/(p\sqrt{1-x^2})$ and positive Lyapunov exponent $\lambda = \ln n > 0$.

B. The Extended Chebyshev Chaotic Maps

According to the periodicity of $y = \cos(x)$, there exist multiple x associated with the same y to make the equation hold. Zhang [25] proved that the Chebyshev polynomial map still keeps the semi-group property over the interval $(-\infty,\infty)$, and proposed the concept of the extended Chebyshev chaotic maps as follows.

$$T_n(x) = (2xT_{n-1}(x)) - T_{n-2}(x)) \bmod P ,$$

where $n \geq 2$, $x \in [-1,1]$, and P is a big prime number. Furthermore, the following equation holds as well:

$$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)) \bmod P$$

Definition 2: Discrete Logarithm Problem (DL)

Given any two big integer x, y, find an integer s to satisfy the equation $T_s(x) \equiv y$.

Definition 3: Decisional Diffie-Hellman Problem (DDH)

Given $T_r(x)$, $T_s(x)$, $T_u(x)$, where r, s, u are unknown, determine the equation $T_{sr}(x) = T_u(x) \bmod P$ holds or not.

III. CONSTRUCTION OF PPRAS

In this section, the detailed construction of PPRAS is presented. For convenience, the descriptions of some symbols to be used are listed in TABLE I.

In PPRS, there exist three entities: the mobile user MU, the home agent HA and the foreign agent FA. When MU moves to FA's network, FA needs to authenticate MU before giving him the permission to access the network. To finish the authentication, FA needs the assistance of HA to verify whether MU is an authorized user or not. If not, the authentication process will be terminated. The proposed scheme consists four stages: registration phase, authentication phase including session key establishment, session key update and login password update phase.

During the initialization, FA shares a session key with HA, which is securely stored locally. The authentication is launched by MU, and then proceeds as the following interactive steps.

TABLE I. DESCRIPTION OF SYMBOLS

Symbol	Description
ID_i	identification of communication entity *i*
SID	temporary identification of mobile user(MU)
$T_n(x)$	Chebyshev polynomial with degree *n*
T_s	$T_s(x)$
T_{MU}, T_{FA}	$T_{r_{MU}}(x), T_{r_{FA}}(x)$
x	the initial value of chaotic map
s	private key of the home agent
P	a big prime number
x_i, r_i	random numbers chosen by users
K_{MU}	session key shared between *MU*,*FA* and *HA*
k_{HF}	the shared key between *FA* and *HA*
$E(.) / D(.)$	symmetric encryption/decryption algorithm
t_{MU}, t_{FA}	timestamp
ΔT	threshold of interval
$H(.)$	a secure one-way hash function
$\oplus$	XOR operation
PW_{MU}	password of mobile user
T_H	running time for hash operation
T_E	running time for encryption operation
T_D	running time for decryption operation
T_C	running time for chaotic map operation
T_M	running time for modular exponential operation

A. Registration Phase

A mobile user MU registers himself in his or her home agent HA using the following steps,

1) HA chooses two random numbers x , s and a big prime number P , then computes $T_s = T_s(x) \bmod P$, and publishes (x , T_s , P).

2) MU chooses his PW_{MU} and a random number λ , then computes $H = h(PW_{MU}, \lambda)$, then sends $\{ID_{MU}, H\}$ to HA via a secure channel.

3) HA checks the validity of ID_{MU} and $H(PW_{MU}, \lambda)$ using $H(H(PW_{MU}, \lambda) \| ID_{MU})$. If yes, computes the message $IM = h(ID_{MU} \| s \| t_{reg})$ which respect the identity of MU, with his secret key s and the timestamp t_{reg} , then store the parameters{ ID_{MU} , H , IM , x , T_s , ID_{HA} , $H(.)$, $E(.)$, $T_n(.)$, P } into a smart card and send it to MU , where $T_n(.)$ is a Chebyshev polynomial with degree n among them. Otherwise, MU fails to register in the system.

B. Authentication and Key Establishment Phase

MU and FA can complete the authentication and establishment by following the steps shown in Fig. 2.

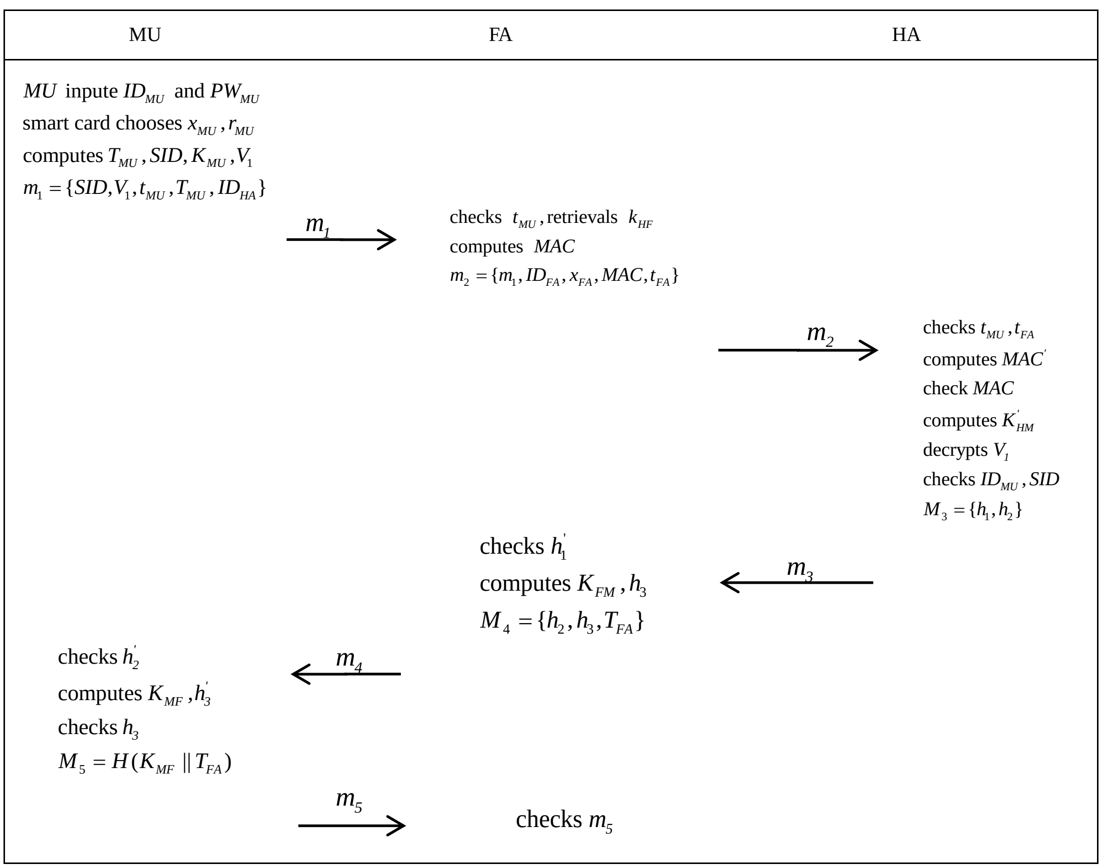

Fig. 2. The process of authenticating and key establishing

- $MU \rightarrow FA$: $m_1=\{SID,V_1,T_{MU},t_{MU},ID_{HA}\}$

MU first inputs his real identity ID_{MU} and password PW_{MU} into the smart card, then the smart card (SC) make the decision that allowing MU to login or not by computing $H^{'}=h(PW_{MU},\lambda)$ and checking validity of ID_{MU} and $H^{'}?=H$. If yes, SC chooses two random numbers: x_{MU}, r_{MU}, then computes $T_{MU}=T_{r_{MU}}(x) \bmod P$, $K_{MH}=T_{r_{MU}}(T_s) \bmod P$ and $SID=ID_{MU}\oplus H(x_{MU})$, where SID denotes the temporary identification of MU, and K_{MH} denotes the shared session key between MU and HA. After that, SC encrypts ID_{MU}, ID_{HA}, IM, x_{MU} and the current timestamp t_{MU} using K_{MH}, that is $V_1=E_{K_{MH}}(ID_{MU}\|ID_{HA}\|IM\|x_{MU}\|t_{MU})$. Next, MU sends $m_1=\{SID,V_1,T_{MU},t_{MU},ID_{HA}\}$ to FA.

- $FA \rightarrow HA$: $m_2=\{m_1,ID_{FA},x_{FA},MAC,t_{FA}\}$

Upon receiving m_1 from MU, FA firstly checks $|t_{FA}\text{-}t_{MU}|<\Delta T$ holds or not, where t_{FA} is the current time of FA, ΔT denotes the permissible threshold of time interval. If yes, stores SID temporarily firstly, and then searches the shared session key k_{HF} between FA and HA using ID_{HA}. Next, computes the message authentication code MAC:

$MAC=h(ID_{FA}\|V_1\|x_{FA}\|t_{FA}\|k_{HF})$, where x_{FA} is a random number chosen by FA temporarily. At last, sends the message $m_2=\{m_1,ID_{FA},x_{FA},MAC,t_{FA}\}$ to HA.

- $HA \rightarrow FA$: $m_3=\{h_1,h_2\}$

After receiving m_2 from FA, HA firstly checks $|T\text{-}t_{FA}|<\Delta T$, $|T\text{-}t_{MU}|<\Delta T$ holds or not, where T denotes the timestamp of HA, ΔT denotes the permissible threshold of time interval.

If these two equation hold, HA confirms ID_{FA} and SID as follows:

Step 1. Uses ID_{FA} retrievals the shared session key k_{HF} between HA and FA, then computes $MAC^{'}=h(ID_{FA}\|V_1\|x_{FA}\|t_{FA}\|k_{HF})$ and checks whether $MAC^{'}=MAC$ holds or not.

Step 2. If yes, HA confirms the identity ID_{FA} from FA, then computes $K_{HM}=T_s(T_{MU}) \bmod P$ to decrypt V_1, and checks whether t_{MU}, ID_{HA} in V_1 are all equal to the plaintext t_{MU}, ID_{HA} in message m_1. if yes, uses the decrypted ID_{MU} to retrieval his database to check whether $t_{MU}>t_{reg}$. If holds, computes $IM^{'}=h(ID_{MU}\|s\|t_{reg})$ and $SID^{'}=ID_{MU}\oplus H(x_{MU})$, then checks if $IM?=IM^{'}$ and $SID?=SID^{'}$. If they all hold, confirms the anonymous identity SID is valid.

Step 3. Computes the message $m_3=\{h_1=h(SID\|x_{FA}\|k_{HF}\|h_2),h_2=h(IM\|x_{MU}\|k_{HM})\}$, then sends it to FA.

- $FA \rightarrow MU$: $m_4=\{h_2,h_3,T_{FA}\}$

After receiving m_3 from HA, FA firstly computes $h_1^{'}=h(SID\|x_{FA}\|k_{HF}\|h_2)$, then checks if $h_1^{'}=h_1$. If yes, confirms the temporary identification SID of MU is valid. After that, FA chooses a random number r_{FA}, then computes $T_{FA}=T_{r_{FA}}(x) \bmod P$, $K_{FM}=T_{FA}(T_{MU}) \bmod P$ and $h_3=h(SID\|k_{FM}\|h_2\|T_{FA})$, where K_{FM} is the session key between FA and MU, then sends $m_4=\{h_2,h_3,T_{FA}\}$ to MU.

- $MU \rightarrow FA$: $m_5=h(K_{MF}\|T_{FA})$

After receiving m_4 from FA, MU firstly computes $h_2^{'}=h(IM\|x_{MU}\|K_{HM})$, checks whether $h_2=h_2^{'}$ holds or not. If yes, MU confirms FA is authenticated, then computes the following values: $K_{MF}=T_{MU}(T_{FA}(x)) \bmod P$ and $h_3^{'}=h(SID\|k_{MF}\|h_2^{'}\|T_{FA})$, where K_{MF} is the session key between MU and FA, then checks if $h_3^{'}?=h_3$. If yes, establishes the session key K_{MF}, then MU computes the message $m_5=h(k_{MF}\|T_{FA})$ and sends it to FA.

- Upon receiving m_5 from MU, FA firstly computes $m_5^{'}=h(k_{FM}\|T_{FA})$, then check if $M_5^{'}?=M_5$. If holds, completes establishing the session key.

C. Session Key Update Phase

In order to ensure the security, it is necessary for MU to periodically update the session key established previously between himself and FA. MU follows the following steps to update his or her session key in the i^{th} time:

Step 1. MU firstly chooses a number t_i randomly, computes $T_{vMU}=T_{t_i}(x) \bmod P$ and $m_i=\{E_{K_{MF_i}}(SID,T_{vMU},t_{vMU},Ch),SID,t_{vMU}\}$, then sends the message m_i to FA, where SID is the anonymous identity of MU when he establishes the session key k_{MF_i} between himself and FA at the previous time, t_{vMU} is current timestamp, Ch is the flag to denotes update query.

Step 2. Upon receiving the message m_1 from MU, firstly checks $|T_i\text{-}t_{vMU}|<\Delta T$ holds or not, where T_i is the current time of FA, ΔT denotes the permissible threshold of time interval. If yes, FA uses SID to get the i^{th} session key K_{FM_i} to decrypt m_i and check whether SID is equal to the plaintext SID.

If yes, FA chooses a random number r_{i+1}, and computes $T_{FA_{i+1}} = T_{r_{i+1}}(x) \bmod P$, $k_{FM_{i+1}} = T_{FA_{i+1}}(T_{vMU}(x)) \bmod P$, where $k_{FM_{i+1}}$ is the current session key. Then FA sends the message $m_{i+1} = \{E_{K_{FM_i}}(h(K_{FM_{i+1}} \| K_{FM_i}), T_{FA_{i+1}}, ID_{FA}), ID_{FA}\}$ to MU

Step 3. After receiving m_{i+1} from FA, MU firstly uses the previous session key k_{MF_i} to decrypt m_2, computes the new session key $k_{MF_{i+1}} = T_{vMU}(T_{FA_{i+1}}(x)) \bmod P$ and $h'(K_{FM_{i+1}} \| K_{FM_i})$, then checks if $h'(K_{FM_{i+1}} \| K_{FM_i}) = h(K_{FM_{i+1}} \| K_{FM_i})$ holds or not. If yes, completes session key update.

D. Login Password Update Phase

It is necessary for MU to update his or her login password dynamically to prevent someone else who knows his or her password from doing some impersonation attacks. The update of login password can be finished as follows:

Step 1. MU puts his or her smart card into the reader, then inputs his or her real identity ID_{MU} and the password PW_{MU}, then the smart card can make the decision that allowing MU to login or not by computing $H' = h(PW_{MU}, \lambda)$ and checking validity of ID_{MU} and $H' ?= H$. If yes, MU sends update request.

Step 2. When the smart card receives the request, it asks MU to input the new password PW'_{MU}, and a random number t' if necessary, then the smart card computes $H' = h(PW'_{MU}, t')$ and updates it.

IV. Analysis of PPRAS

A. Correctness Analysis

The Burrows–Abadi–Needham (i.e. BAN) logic [27] is useful to identify some possible weakness in the security protocols, especially for the authentication protocol, so the BAN logic is used to analyze the correctness of PPRAS. Some notations are listed in TABLE II.

TABLE II. Notations for BAN Logic

Notation	Description
$A \mid\equiv X$	A trusts X, or A believes X
$A \triangleleft X$	A sees X, or A holds X
$A \mid\sim X$	A has said X
$A \mid\Rightarrow X$	A completely controls over X
$\frac{\text{Rule 1}}{\text{Rule 2}}$	Rule 2 comes from Rule 1
$A \xleftrightarrow{x} B$	x is a secret key or information between A and B
$\{X\}_K$	X is encrypted by the key K

1) Idealization

According to the rules of the BAN logic, the first step is to idealize the authentication phases of PPRAS as follows:

a) $MU \rightarrow FA$:
$$m_1 = \{SID, \{ID_{MU} \| ID_{HA} \| IM \| x_{MU} \| t_{MU}\}_{MU \xleftrightarrow{K_{MH}} HA}, T_{MU}, t_{MU}\}$$

b) $FA \rightarrow HA$:
$$m_2 = \{m_1, h(ID_{FA} \| V_1 \| x_{FA} \| t_{FA} \| FA \xleftrightarrow{K_{FH}} HA), t_{FA}\}$$

c) $HA \rightarrow FA$:
$$m_3 = \{h_1 = h(SID \| x_{FA} \| HA \xleftrightarrow{k_{HF}} FA \| h_2), h_2 = h(IM \| x_{MU} \| HA \xleftrightarrow{k_{HM}} MU)\}$$

d) $FA \rightarrow MU$:
$$m_4 = \{h_2, h_3 = h(SID \| FA \xleftrightarrow{k_{FM}} MU \| h_2 \| T_{FA}), T_{FA}\}$$

e) $MU \rightarrow FA$: $m_5 = h(MU \xleftrightarrow{k_{MF}} FA \| T_{FA})$

2) Assumptions

In PPRAS, there exist three entities: the mobile user (*MU*), the foreign agent (*FA*) and the home agent (*HA*). Each entity has his or her possessions and abilities. The initial assumptions are descripted as follows:

For *MU*:

A1. $MU \triangleleft ID_{MU}$

A2. $MU \mid\equiv SID$

A3. $MU \mid\equiv ID_{HA}$

A4. $MU \mid\equiv r_{MU}$

A5. $MU \mid\equiv MU \xleftrightarrow{K_{MH}} HA$

A1: *MU* believes his or her own identity.

A2: *MU* believes his or her own pseudonym SID.

A3: As MU registers himself in his home agent *HA* to be a legitimate user, so he believes *HA*'s identity ID_{HA}.

A4: *MU* believes the number x_{MU} chosen by himself.

A5: *MU* believes the session key K_{MH} between himself and HA, because K_{MH} is computed using the Chebyshev polynomials with *HA*'s public parameter T_{HA} and T_{MU}.

For *HA*:

A6: $HA \triangleleft ID_{HA}$

A7: $HA \mid\equiv \#(t_{MU})$

A8: $HA \mid\equiv \#(t_{FA})$

A9: $HA \mid\Rightarrow s$

A10: $HA \mid\equiv HA \xleftrightarrow{k_{HF}} FA$

A6: *HA* holds his own identity.

A7: *HA* believes t_{MU} is fresh, and has never received it before so that he can authenticate *MU*.

A8: *HA* believes t_{FA} is fresh, and has never received it before so that he can authenticate *FA*.

A9: As s is *HA*'s secret key, so *HA* completely controls over his secret key s.

A10: *HA* believes the key shared between *HA* and *FA* before authenticating.

For *FA*:

A11: $FA \lhd ID_{FA}$

A12: $FA \lhd ID_{HA}$

A13: $FA \mid\equiv \#(t_{MU})$

A14: $FA \mid\equiv FA \xleftrightarrow{k_{HF}} HA$

A15: $FA \mid\equiv r_{FA}$

A11: *FA* holds his own identity.

A12: *FA* needs to authenticate *MU* with the help of *HA*, so he needs to hold *HA*'s identity ID_{HA}.

A13: *FA* believes t_{MU} is fresh so that he will be able to finish the next operation.

A14: *FA* believes the session key K_{FH} between himself and *HA*, because K_{FH} is computed using Chebyshev polynomials with *HA*'s public parameter T_{HA} and the value T_{FA} computed by *FA* himself.

3) Goals

According to the proposed scheme, *MU* and *FA* want to establish a session key with the help of *HA*, so our proposed scheme needs to achieve the following goals:

G1: $HA \mid\equiv SID$

G2: $HA \mid\equiv ID_{FA}$

G3: $FA \mid\equiv HA \mid\equiv SID$

G4: $MU \mid\equiv HA \mid\equiv ID_{FA}$

G5: $MU \mid\equiv MU \xleftrightarrow{K_{MF}} FA$

G6: $FA \mid\equiv FA \xleftrightarrow{K_{FM}} MU$

G1: *HA* believes the anonymous identity of *MU*.

G2: *HA* believes *FA*'s identity.

G3: *FA* believes that *HA* has verified *MU*'s anonymous identity *SID*.G4: *MU* believes that *HA* believes *FA* is a legitimate agent.

G5: *MU* believes the session key between himself and *FA*, that is *MU* has already successfully generated the session key with *FA*.

G6: *FA* believes the session key between himself and *MU*, that is *FA* has already successfully generated the session key with *MU*.

MU wants to establish a session key with *FA* without leaking his identify, he needs an anonymous identify which used to be authenticated by *HA*, and *HA* must believe *FA*'s identify to enable *MU* to communicate with *FA*. After they finish the process of generating the session key, *FA* and *MU* must believe the authenticated peer holds the common session key.

4) Verification

In this section, the BAN logic is employed to check whether PPRAS is correct or not. The primary steps are shown as follows:

Theorem 1. *HA* believes the anonymous identity of *MU* and the identity of *FA*.

Proof :

V1:
$$\cfrac{\cfrac{\cfrac{HA \lhd m_2}{HA \lhd h(ID_{FA} \| V_1 \| x_{FA} \| t_{FA} \| k),\ HA \mid\equiv HA \xleftrightarrow{k_{HF}} FA}}{HA \mid\equiv FA \mid\sim ID_{FA},\ HA \mid\equiv \#(h(ID_{FA} \| V_1 \| x_{FA} \| t_{FA} \| k_{HF}))}}{HA \mid\equiv FA \mid\equiv ID_{FA}}$$

V2:
$$\cfrac{\cfrac{\cfrac{\cfrac{HA \lhd k_{HM}}{HA \lhd (ID_{MU}, IM, x_{MU})}}{HA \lhd IM,\ HA \mid\Rightarrow s}}{HA \mid\equiv ID_{MU},\ HA \lhd SID}}{HA \mid\equiv SID}$$

According to the assumption A7 and A8, *HA* believes the message m_1 and m_2 are fresh, and he has never received them before, applying the seeing rule:

$$\frac{A \lhd (x, y)}{A \lhd x},$$

HA holds $h(ID_{FA} \| V_1 \| x_{FA} \| t_{FA} \| k_{HF})$, with the assumption A10, applying the message-mean rule: $\frac{P \mid\equiv P \xleftrightarrow{k} Q,\ P \lhd \{x\}_k}{P \mid\equiv Q \mid\sim x}$,

HA believes that *FA* has said ID_{FA}, applying fresh rule: $\frac{A \mid\equiv \#(x, y)}{A \mid\equiv \# x}$,

HA believes $h(ID_{FA} \| V_1 \| x_{FA} \| t_{FA} \| k_{HF})$ is fresh, applying nonce-verification rule:

$$\frac{P \mid\equiv \#(x),\ P \mid\equiv Q \mid\sim x}{P \mid\equiv Q \mid\equiv x},$$

HA believes that *FA* believes ID_{FA}, so *HA* believes ID_{FA}.

After verifying the correction of *MAC*, *HA* believes the session key k_{HF}, so he believes the identity of *FA*, and also believes the message m_1 has not been tampered. Then *HA* computes K_{HM} to decrypt V_1 in message m_1, applying the seen rule:

$$\frac{A \lhd (x, y)}{A \lhd x},$$

HA can get ID_{MU}, *IM* and x_{MU}. According to the assumption A9, *HA* believes the real identify of *MU*, then *HA* can verify the anonymous identity of *MU* with the received value *SID* in message m_1.

With the proof above, it can be found that *HA* believes the anonymous identity (SID) of *MU* and the identity (ID_{FA}) of *FA*.

Theorem 2. *FA* believes that *HA* has verified *MU*'s anonymous identity *SID*.

Proof:

V3: $$\frac{\dfrac{FA \lhd m_3}{FA \lhd h_1, FA \mid\equiv FA \xleftrightarrow{k_{HF}} HA}}{FA \mid\equiv HA \mid\equiv SID}$$

After *FA* receives the message m_3 from *HA*, applying the seen rules:

$$\frac{A \lhd (x,y)}{A \lhd x},$$

FA receives the value h_1 in message m_3. According to the assumption A14, we know that *HA* has verify the anonymous identity *SID*, so *FA* believes that *HA* believes the anonymous identity *SID* of *MU* after he verify the message h_1 in the received message m_3.

Above all, *FA* believes that *HA* has verified *MU*'s anonymous identity *SID*.

Theorem 3. *MU* believes that *HA* believes *FA* is a legitimate agent.

Proof：

V4 : $$\frac{\dfrac{\dfrac{\mathrm{MU} \lhd m_4}{MU \lhd h_2, MU \mid\equiv MU \xleftrightarrow{k_{HM}} HA}}{MU \mid\equiv \mathrm{h}_2, MU \mid\equiv r_{MU}}}{MU \mid\equiv HA \mid\equiv ID_{FA}}$$

After *MU* receives the message m_4 from *FA*, applying the seeing rules:

$$\frac{A \lhd (x,y)}{A \lhd x},$$

MU receives the value h_2 in message m_4. According to the assumption A5, *MU* believes the value h_2, and also believes *MU* believes that *HA* believes FA's identity after he or she verifies h_2 under the assumption A4. So *MU* believes that *HA* believes *FA* is a legitimate agent.

Theorem 4. *MU* believes the session key between himself and *FA*, that is *MU* has already generated the session key with *FA*.

Proof:

V5: $$\frac{\dfrac{\dfrac{MU \lhd m_4}{MU \lhd h_3, MU \mid\equiv (SID, h_2)}}{MU \mid\equiv h_3, MU \lhd K_{MF}}}{MU \mid\equiv MU \xleftrightarrow{K_{MF}} FA}$$

After *MU* receives the message m_4 from *FA*, applying the seeing rules:

$$\frac{A \lhd (x,y)}{A \lhd x},$$

MU receives the value h_3 in message m_4. According to the assumption A2 and the theorem 3, *MU* believes h_3.

After *MU* verifies h_2, he or she computes the session key K_{MF} between *MU* and *FA*, so *MU* holds K_{MF}, according to the proof above that MU believes h_3, *MU* can verify the key K_{MF} is right with h_3, that is *MU* believes the session key between himself and *FA*.

Theorem 5. *FA* believes the session key between himself and *MU*, that is *FA* has already generated the session key with MU.

Proof:

V6: $$\frac{\dfrac{FA \mid\equiv r_{FA}}{FA \mid\equiv T_{FM},\ FA \lhd m_5}}{FA \mid\equiv FA \xleftrightarrow{K_{FM}} MU}$$

After *FA* receives the message m_5 from *MU*, according to the assumption A15, applying the belief rules:

$$\frac{A \mid\equiv x}{A \mid\equiv (x,y)},$$

FA believes T_{FM}, as *FA* holds the message m_5, so *FA* believes the session key K_{FM} between *FA* and *MU*.

B. Performance Analysis

The performance evaluation of the existing protocols [9-13] and PPRAS will be discussed in this section. The overall resultes are listed in TABLE III.

TABLE III. COMPARISON ON PERFORMANCE

	Client	Server
Farash et.al.'s[13]	$6T_H$	$6T_H + 2T_E + 2T_D$
Mao et al.'s[12]	$8T_H + 2T_E$	$4T_H + 2T_E + 4T_D$
Xue et al.'s[11]	$4T_H + T_E + T_D$	$3T_H + 2T_E + 3T_D$
Shin et al.'s[9]	$4T_H$	$7T_H + 2T_E + 2T_D$
Wen et al.'s[10]	$4T_H + T_M$	$10T_H + 3T_M$
PPRAS	$4T_H + T_E + 2T_C$	$9T_H + T_D + 2T_C$

Since the authentication is a series of synchronized processes, the total computational cost of the client and server during the authentication and key agreement should be investigated. As the cost of XOR operation and module addition are rather cheap, these two operations are not included in the comparison, and only symmetric encryption/decryption operation, chaotic map operation, hash operation and modular exponential operation are evaluated. As shown in TABLE III, the computational cost of client in [9,10,13] is much cheap than PPRAS, however, as discussed previously, the scheme in

[9,12] cannot resist to the man-in-the-middle attacks, and the scheme in [10] cannot preserve the user's privacy. However, the efficiency of [11] is not desirable. The scheme in [13] is vulnerable to the replay attacks. Furthermore, the schemes in [9-13] will inevitably incur huge key management for the symmetric and public key encryption. Although no explicit advantage of performance for PPRAS cannot be found in TABLE III, the underlying featured chaotic map based encryption for handshake message would save much more computation and storage cost.

C. Security Analysis

In this section, the security analysis and performance comparison are illustrated.

1) User Anonymity: The user who wants to authenticate others should provide its real identifies to the trusted three party in the 3PAKE [26] protocol. If the user transfers authentication messages including his identity in plaintext via an insecure channel, an attacker can identify the user by intercepting and analyzing the message, this is not a a desirable scheme for authentication. In PPRAS, the real identity of mobile user is encrypted with the session key computed using Chebyshev polynomial. Even if the adversary got the ciphertext, he or she still faces the difficulty of solving DL hard problem if he or she want to compute the decryption key. Since the temporary identification of MU is generated with the XOR operation on the random number and real identity, it is infeasible in polyninomial time to guess the right identity since the space of identity is big enough. Therefore, FA can get nothing about the user's real identity and the privacy of the useris preserved well.

2) Resistance to The Man-in-The-Middle Attack: Suppose there exists an active attacker over the communication channel, who attempts to intercept and tamper the messages transferred via this channel to carry out the man-in-the-middle attack. If the attacker wants to tamper m_1, he or she needs to tamper V_1 in message m_1 produced by symmetric encryption with the session key, which is computed with the Chebyshev polynomials. However the attacker will face the difficulty of solving the DL problem. As for the messages m_2, m_3, m_4, m_5 generated with the secure one-way hash functions, if the attacker wants to tamper them, he or she will face the difficulty of breaking the secure one-way hash functions according to the definition of the protocol. Above all, PPRAS is secure enough to counter the man-in-the-middle attack.

3) Forward Secrecy: In PPRAS, the forward secrecy means that even if an adversary has obtained the current session key and the password of MU, he or she cannot deduce the previous used session key. The agreement of the session key K_{MF} (or K_{FM}) between MU and FA is based on the random number x_{MU} and x_{FA}, and even MU does not know x_{MU} which is chosen dynamically by the smart card, so the adversary can get nothing about K_{MF} (or K_{FM}), that is , the proposed scheme achieves forward secrecy.

4) Backward Secrecy: The backward secrecy of PPRAS refers to the adversary cannot successfully fulfil authentication and session key agreement with the password of MU and all previous used session key together with the current session key. However, all the messages are produced by the smart card and transferred in anonymous way, thus he or she cannot generate a valid message without possesing this smart card according to the protocol, even if he or she is given PW_{MU}. So PPRAS achieves the backward secrecy.

5) Resistance to Password Guessing Attack: This attack means that an attacker attemps to deduce the password of the user with interception and analysis over the transferred messages. In PPRAS, however, there does not exist user's password in all these messages, and the attacker can get nothing about user's passwordThus, the proposed scheme can resist to password guessing attack.

6) Resistance to The Replay Attack: According to the construction of the presented protocol， all the transffered messages among MU , FA and HA combine the timestamp t_{FA} , t_{MU} to provide freshness. What's more, the paramters（ x_{MU} , r_{MU} ） and（ x_{FA} , r_{FA} ） are chosen randomly to ensure freshness at the beginning of every authentication session. So the adversary can not replay those messages.

Finally, the overall security comparison of PPRAS and the existing similar schemes are listed in TABLE IV. As shown in the table, only PPRAS can achieve all the security features.

TABLE IV. COMPARISON ON SECURITY

Security Features	Farash et.al.'s[13]	Mao et al.'s[12]	Li et al.'s[8]	Shin et al.'s.[9]	Wen et al.'s[10]	PPRAS
Forward Secrecy	√	√	√	´	√	√
Backward Secrecy	√	√	√	√	´	√
Anti-replay attack	´	√	√	√	√	√
Anti-MIM attack	´	´	´	´	√	√
User Anonymity	√	√	√	´	√	√
Anti-guessing attack	√	´	´	´	´	√

V. CONCLUSIONS

Roaming authentication is essential to the ubiquitous networks, and a lot of efforts have been done to better the security and performance in authentication. However, the existing authentication protocols cannot avoid the huge burden of key agreement and management for authentication which comes from the encryption and poses a barrier to apply it to the multi-user situations. Thus a novel roaming authentication scheme based on Chebyshev chaotic map with user anonymity is proposed in this paper. With the advantage of semi-group property of Chebyshev polynomial, the entities involved in the authentication can agree the session key at low cost, and no additional key management is needed. Meanwhile, the foreign agent can authenticate the user without knowing his real identity, which achieves privacy preserving for the user.

ACKNOWLEDGEMENT

This work was jointly supported by the National Social Science Foundation of China (no. 14CTQ026), the National Natural Science Foundation of China (no. 61472464), the

Chongqing Research Program of Application Foundation and Advanced Technology (no. cstc-2014jcyjA40028, no. cstc-2013jcyjA40017), the Natural Science Foundation of Shandong Province, China (no. ZR2015FL024).

REFERENCES

[1] C. C. Chang, S. Y. Lin, J. H.Yang,“ Efficient user authentication and key establishment protocols with perfect forward secrecy for mobile devices,” Computer and Information Technology, Ninth IEEE International Conference on. IEEE,Xiamenpp.131-135, 2009.

[2] C. C.Chang, C. Y. Lee, Y. C. Chiu, “ Enhanced authentication scheme with anonymity for roaming service in global mobility networks,” Computer Communications, vo.32, no.4, pp.611-618, 2009.

[3] D. He, S. Chan, “A secure and light weight user authentication scheme with anonymity for the global mobility network,” Network-Based Information Systems (NBiS), 2010 13th International Conference on. IEEE, Takayama, Gifu, pp.305-312, 2010.

[4] C. Chen, D. He, S. Chan, et al, “Light weight and provably secure user authentication with anonymity for the global mobility network,” International Journal of Communication Systems, vol.24, no.3, pp.347-362, 2011.

[5] T. Zhou, J. Xu, “Provable secure authentication protocol with anonymity for roaming service in global mobility networks,” Computer Networks, vol.55, no.1, pp.205-213, 2011.

[6] J. Xu,W. T. Zhu, D. G. Feng, “An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks,” Computer Communications, vol.34, no.3, pp.319-325, 2011.

[7] J. Lu, J. Zhou, “On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks,” IACR Cryptology ePrint Archive, pp.126, 2010.

[8] H. Li,Y. Yang, L. Pang, “An efficient authentication protocol with user anonymity for mobile networks,” Wireless Communications and Networking Conference (WCNC), 2013 IEEE, Shanghai, pp.1842-1847.

[9] S. Shin, H. Yeh, K. Kim, “An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks,” Peer-to-Peer Networking and Applications, pp.1-10, 2013.

[10] F. Wen, W. Susilo, G. Yang, “A secure and effective anonymous user authentication scheme for roaming service in global mobility networks,” Wireless personal communications, 2013, pp.993-1004.

[11] Q. Xie, D. Hong, M. Bao, N. Dong and D. S. Wong,., “Privacy-Preserving Mobile Roaming Authentication with Security Proof in Global Mobility Networks,” International Journal of Distributed Sensor Networks, 2014.

[12] K. Mao, J. Chen, J. Liu and D. Tong, “An anonymous roaming authentication scheme in global mobility networks,” Communications Security Conference (CSC 2014), IET, Beijing, pp.1-4, 2014.

[13] M.S.Farash, S.A.Chaudhry, M.Heydari,et al, “A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security,” International Journal of Communication Systems, 2015.

[14] D. He, M. Ma, Y. Zhang, C. Chen and J. Bu “A strong user authentication scheme with smart cards for wireless communications,” Computer Communications, vol.34, no.3, pp.367-374, 2011.

[15] X. Li, W. Qiu, D. Zheng, K. Chen and J. Li, “Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards,” Industrial Electronics, IEEE Transactions on, vol.57, no.2, pp.793-800, 2010.

[16] D. Wang, P. Wang, J. Liu, “Improved privacy-preserving authentication scheme for roaming service in mobile networks,”Wireless Communications and Networking Conference (WCNC), 2014 IEEE Istanbul, pp.3136-3141, 2014.

[17] C. C. Lee, “A simple key agreement scheme based on chaotic maps for VSAT satellite communications,” International Journal of Satellite Communications and Networking, vol.31, no.4, pp.177-186, 2013.

[18] K. Chain, W. C. Kuo, “A new digital signature scheme based on chaotic maps,” Nonlinear Dynamics, vol.74, no.4, pp.1003-1012, 2013.

[19] M. S. Hwang, S. K. Chong, T. Y. Chen, “DoS-resistant ID-based password authentication scheme using smart cards,” Journal of Systems and Software, vol.83, no.1, pp.163-172, 2010.

[20] R. Song, “Advanced smart card based password authentication protocol,” Computer Standards & Interfaces, vol.32, no.5, pp.321-325, 2010.

[21] C. Guo, C. C. Chang, “Chaotic maps-based password-authenticated key agreement using smart cards,” Communications in Nonlinear Science and Numerical Simulation, vol.18, no.6, pp.1433-1440, 2013.

[22] W.S.Juang, S.T.Chen, H.T. Liaw, “Robust and efficient password-authenticated key agreement using smart card,” IEEE Trans Ind Electron vol.55, no.6, pp.2551–2556, 2008.

[23] D. Z. Sun, J. P. Huai, J. Z. Sun, et al, “Improvements of Juang's password-authenticated key agreement scheme using smart cards,” Industrial Electronics, IEEE Transactions on, vol.56, no.6, pp.2284-2291, 2009.

[24] H.Y. Lin, “Improved chaotic maps-based password-authenticated key agreement using smart cards,” Communications in Nonlinear Science and Numerical Simulation, vol.20, no.2, pp. 482-488, 2015.

[25] L. Zhang, “Cryptanalysis of the public key encryption based on multiple chaotic systems,” Chaos, Solitons & Fractals, vol.37, no.3, pp.669-674, 2008.

[26] C. T. Li, C. W. Lee, J. J.Shen, “A secure three-party authenticated key exchange protocol based on extended chaotic maps in cloud storage service,” Information Networking (ICOIN), 2015 International Conference on. IEEE, Cambodia, pp.31-36, 2015.

[27] M. Burrows, M. Abadi, R. Needham, “A logic of authentication,” ACM Trans Comput Syst , vol.426, no.1871, pp.18–36, 1989.