A Review of One-Pass Key Establishment Model and Protocols for Wireless Roaming.

Umakanth Vellanki, Dr Syed Umar, Venkat Purnesh Gaddam

Department of ECM, KL University, A.P., INDIA.

***Abstract*— Two novel mutual authentication and key exchangeprotocols with anonymity are proposed for different roamingscenarios in the global mobility network. The new features inthe proposed protocols include identity anonymity and one-timesession key renewal. Identity anonymity protects mobile usersprivacy in the roaming network environment. One-time sessionkey progression frequently renews the session key for mobileuser's and reduces the risk of using a compromised session keyto communicate with visited networks. It has demonstrated thatthe computation complexity of the proposed protocols is similarto the existing ones, while the security has been significantlyimproved.**

Keywords—**Authentication, key exchange, roaming service, Anonymity, secret-splitting, self-certified.**

I. INTRODUCTION

GLOBAL mobility network (GLOMONET) [1], such asGSM and CDMA networks etc., offers effective globalroaming service for a legitimate user between the homenetwork and the visited network. However, it also increasesthe possibility of illegal access from malicious intruders. Fig. 1shows a general architecture of GLOMONET. The home networkhas a network prefix matching that of the mobile station'shome address. The visited foreign network (*V*) and the homenetwork have a roaming agreement and share a secret key.When a mobile station (*M*) roams to *V*, it performs authenticationand updates its registration information with its homeagent (*H*) in the home network, either directly or indirectly. Asession key is setup to encrypt further communications in thesession between the parties if the authentication is successful.In order to provide wireless access and especially roamingservice in foreign network, strong authentication measures arerequired for all involved parties: the mobile device, the visitedforeign network and its home network, to prevent privacycompromise and service abuse, etc. Several authenticationManuscript received February 3, 2005; revised May 17, 2005; acceptedSeptember 3, 2005. The associate editor coordinating the review of thispaper and approving it for publication was Y.-B. Lin. This relative workhas been supported in part by the National Natural Science Foundation ofChina under contracts No.60573144, 60218003, 60429202, and 90412012 protocols for global roaming service have been developedfor the GLOMONET [2]. A challenge/response interactiveauthentication mechanism with a symmetric cryptosystem toconstruct their authentication protocol is introduced in [1].However, there are several potential attacks to the protocol[3]. A legitimate, but malicious user may be able to obtain theauthentication key *Kauth*. The intruder then can impersonatethe roaming user or the visited network. The protocol mayallow the intruder to feed the roaming user with acompromisedand old authentication key, and thus to masqueradeas the visited network. The home network may obtain theauthentication key *Kauth*, which was originally designed tobe kept confidential between the roaming user and the visitednetwork only. In [4], a simpler and more efficient protocolbased on self-encryption for roaming services is proposed. Thehome network *H* maintains a long-term secret key *KMH* =*f*(*IDM*) for its user by using a secret one-way hash function *f*, where *IDM* denotes the identity of the mobile device (orthe user). However, since the protocol cannot provide identityanonymity, an intruder can obtain *IDM* by intercepting theexchanged messages. If the function *f* is spied (which is notquite difficult by reverse-engineering on the mobile device),the intruder may compute *KMH* of all mobile devices in suchcryptosystem and the advantage of self-encryption would becounteracted. The disclosure of a user identity may also allowunauthorized entities to track his moving history and current location. Any illegal access to information related to the user'slocation without his attention can be a serious violation of hisprivacy. The identity anonymity is an important property forroaming services.

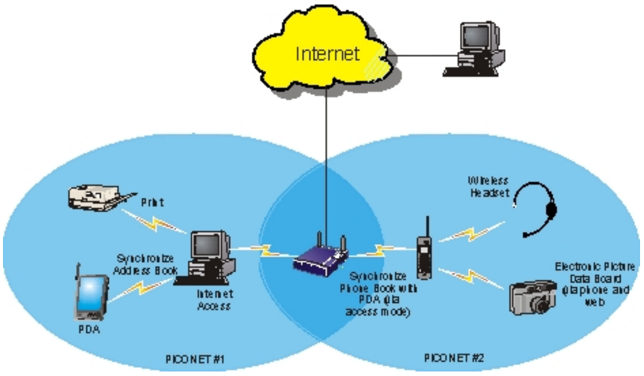

Fig 1

On the other hand, a secure protocol design for roamingservices requires: 1) Prevention of fraud by ensuring that themobile user and network entity are authentic, that is, thereare a mutual authentication mechanism between a networkentity and a mobile user; 2) Assuring mutualagreementand freshness of the session key; 3) Prevention of replayingattack, so that intruders are not able to obtain sensitive databy relaying a previously intercepted message; 4) Privacy ofmobile user's location information during the communicationso that it is requisite to provide the identity anonymity mechanism[5]. Since the protocols are implemented on the mobiledevices in wireless environment, there are other two factorsto be considered: 1) The low computational power of mobiledevices should be a concern, which means a security protocolrequiring heavy computation on the mobile is not feasible [6],[7], [8]; 2) Since the bandwidth is lower and the channel erroris higher in wireless networks than that in wired networks, thesecurity protocols should be designed to minimize the messagesize and the number of message exchanges.In this paper, aiming at providing the identity anonymity andsimplifying the existing authentication protocols for secureroaming service in GLOMONET environment, we proposetwo sets of mutual authentication and key exchange protocolswith anonymity property for roaming service, by using use thesecret-splitting principle and self-certified scheme [9], [10],[11], known as a public key authentication cryptosystem,respectively. The two protocols can be deployed dependingon whether the home network and the mobile user share afixed long-term secret key. The mutual authentication withanonymity property prevents the disclosure of mobile user's real identities and protects their privacy in the roaming networkenvironment. The proposed authentication protocols usethe temporary identity (*TID*) for a mobile user instead of hisreal one. *TID* is prearranged and distributed by the homenetwork H in advance or temporarily generated by encryptingthe real identity [12], [13], [14], [15], [16]. The key exchangerenews a mobile user's session key for each session, andtherefore, reduces the risk of using a compromised session keyto communicate with visited networks. The proposed protocolscan improve security features significantly, while requiringsimilar computation power as the existing protocols.The rest of this paper is organized as follows. Two newauthentication and key exchange protocols with anonymity forsecure roaming service are proposed in Sections 2 and 4, eachof which is followed by the security analysis in Section 3and 5, respectively. The performance comparisons between theprotocol in [4] and the proposed two protocols are presentedin Section 6, and conclusion is given in Section 7.

II. PROTOCOL I BASED ON SECRET-SPLITTING PRINCIPLE

Secret splitting [17] is a type of information-hidden techniquethat divides a message into pieces. Each piece byitself has no meaning, but when these pieces are put together,the original message can be restored. Using the *secretsplitting* principle, we propose a simple authentication andkey exchange protocol with anonymity property for roamingservices. The protocol includes two phases. In phase I, thevisited network V authenticates a roaming user M through hishome network H. After a successful validation, an authenticationkey isestablished between M and V. In the subsequentcommunication sessions, V can directly authenticate M byusing the authentication key rather than doing it again through$H$. In phase II, a novel mechanism called "one-time sessionkey Renewal" is introduced to assure the mutualauthenticationand freshness of the session key. User M establishes or renewsa session key with V, and M can get the service from Vdirectly.

A. Phase I: Mutual Authentication Protocol (MAP)

Firstly, we introduce the concept of pseudonym identity$PIDM$ for user M. Let H generate a secret m-bits randomnumber NM for each user and records the mapping relationof ith user's $PIDi$and Ni ($PIDi \leftrightarrow Ni$). To prevent theexclusive search attack, m should be sufficiently large, e.g.256 bits. When a user M registers with his home network H,he submits his identity IDM to H. Then, H computes $PIDM$for user M as:

$$PIDM = h(NM\ \_\ IDH) \oplus IDM \oplus IDH, \quad (1)$$

where $\oplus$ denotes bitwise XOR operation and h is a publicstrong one-way hash function. (1) is constructed so that both$M$ and H's identity information is associated to $PIDM$.Subsequently, H delivers $PIDM$ to M through a securechannel, such as issuing a smart card for user M. By thissecret-splitting mechanism, we can conceal the real identityIDM in $PIDM$ and provide identity anonymity for M withoutincreasing the computation complexity.

Message 1. $M \rightarrow V : IDH, P\ IDM, EKMH(rM\_KMH)$
Message 2. $V \rightarrow H : PIDM, EKVH(rV\ \_tV\ \_EKMH(rM\_KMH))$
Message 3. $V \leftarrow H : EKVH(rV\ \_rM\_h(IDM)), EKMH(rM\_rV\_IDV\ )$
Message 4. $M \leftarrow V : EKMH(rM\_rV\ \_IDV\ )$

Messag 5. $M \rightarrow V : EKauth(Kauth)$

Fig. 2. Authentication Protocol I for Roaming Services

The goal of MAP is to provide a mutual authenticationmechanism for users M and V. Our proposed protocol for theroaming services (Phase I) is described as in Fig. 2. Two newfeatures are introduced. A simple secret splitting mechanism isutilized to provide the identity anonymity, which prevents thatunauthorized entities from tracing the mobile users roaminghistory and his current location. The generation mechanism of authentication key $Kauth$is also improved such that:

$$Kauth = rM \oplus rV, \quad (2)$$

where$rM$and $rV$are sufficiently large random numbergenerated by M and V, respectively. $Kauth$is computed withthe random numbers chosen by both parties, while $Kauth$in[4] was only determined by V, i.e. $Kauth = rV$. The modifiedmechanism makes the protocol fairer and more secure withoutincreasing the computation complexity since the XOR is avery simple operation.

In the following, we describe the proposed MAP protocolaccording to the order of message exchange and discuss thesecurity goals that can be achieved during the execution ofeach protocol message.

1) When a mobile user M enters a new visited network$V$, he initiates a registration authentication process with$V$ in order to identify himself to be a legal subscriberof his home network H. M generates a secret randomnumber rM, computes the long-term secret key $KMH = f(IDM)$, where f is a public one way function, andsends $EKMH(rM\ \_\ KMH)$, $PIDM$, and IDH to thevisited network V, respectively.

2) On receiving message 1 from M, V forwards $PIDM$ andsends $EKMH(rV \_ tV \_ EKMH(rM \_ KMH))$ to H foridentity authentication, where KVH is the shared secretkey between V and H, $rV$is a secret random numbergenerated by V, and $tV$is a time stamp.

3) After receiving the message from V, H first decrypts$EKMH(rV _ tV _ EKMH(rM _ KMH))$ by using KVH.Then H determines whether the time stamp is withinsome allowable range compared with its current time. If$tV$is not within the range, H terminates the execution.Otherwise, H gets M's real identity by computing:

$IDM = PIDM \oplus h(NM \_ IDH) \oplus IDH$ (3)

Afterwards, H calculates the long-term key KMH by$KMH = f(IDM)$ and uses it to decrypt $EKMH(rM \_KMH)$. If the decrypted secret key, KMH, is equal to$f(IDM)$, the authenticity of user M is authenticated. Italso provides the implicit identity authentication of V.Subsequently, H sends $EKVH(rV \_ rM \_ h(IDM)$ and$EKMH(rM _ rV _ IDV)$ to V.

4) Messages 4 and 5 show the process of the mutualauthentication and key negotiation between M and V.On receiving the message from H, V first decrypts$EKVH(rV _ rM _ h(IDM))$. If the decrypted rVin $EKVH(rV \_ rM \_ h(IDM))$ is the same as itsoriginal rV, then V believes that M is an authorized user.Subsequently, V does the following:

1) Saving the value$h(IDM)$ for identifying the identity of user M in PhaseII;
2) Setting $Kauth= rM \oplus rV$as the authentication key$Kauth$;
3) Forwarding message $EKMH(rM \_ rV \_IDV)$ to M.
5) M decrypts $EKMH(rM \_ rV \_ IDV)$ using KMH. Ifthe decrypted $r*$

M is equal to its original value rM, then$M$ can compute the authentication key as $Kauth= rM \oplus rV$. Afterwards, M sends to V to verify the key $Kauth$.

6) If $E{-}1Kauth(EKauth(Kauth)) = Kauth$, V records the authentication key $Kauth$for user M. V has finishedthe authentication process with M and established anauthentication key $Kauth$.

Message 1. $M \rightarrow H{:}IDH,P\ IDM,EKMH(rM\_KMH)$
Message 2. $M \leftarrow H{:}EKMH(rM\_rH\_IDH)$
Message 3. $M \rightarrow H{:}EKauth(Kauth)$

Fig. 3. Authentication Protocol I for Local Services

As a special case, consider the authentication protocol whenuser M is located in his home network. The correspondingauthentication protocol for local services is shown in Fig. 3.Note that the difference between Fig. 2 and Fig. 3 is that theauthentication protocol for local services ignores the originalMessages 2 and 3 in Fig. 2.In the protocol, the self-encryptionproperty of the protocolin [4] is maintained, that is, the home network also maintainsa long-term secret key $Kauth$for its user M by using a onewayfunction. By extracting the real identity IDM of user $M$from $PIDM$, the shared key KMH can be generated, whichis used to encrypt the corresponding text.

B. Phase II: One-time session key Renewal Protocol (SKRP)

The goal of SKRP protocol is to establish or renew a sessionkey between M and V. In this phase, a novel mechanismcalled "One-time session key renewal" is introduced, whichallows mobile user M to renew his session key frequently andreduces the risk that he uses a compromised session key tocommunicate with V.

Message 1. $M \rightarrow V{:}IDV,P\ IDM,i,EKi{-}1\ (rM,i\_Ki{-}1)$
Message 2. $M \leftarrow V{:}EKi{-}1\ (rM,i\_rV,i\_IDH)$
Message 3. $M \rightarrow V{:}EKi(Ki)$

Fig. 4. One-time Session Key Renewal Protocol I

Suppose that M need to renew his session key $Ki{-}1$ with $V$for the ith time, he can obtain the new session Ki according tothe steps shown in Fig. 4. The new session key Ki is calculatedas

$Ki = rM,i \oplus rV,i,\ i= 1, 2, 3, ..., n,$ (4)

and$K0$ is set as the authentication key $Kauth$(Phase I), thatis, $K0 = Kauth$. The pseudonym identity $PIDM,i$for M iscomputed as

$PIDM,i= h(IDM) \oplus rM,i.$ (5)

Clearly, $PIDM,i$will vary in each session key negotiationbecause of rM,i.As shown in Fig. 4, on receiving the message 1 from M, Vcan obtain the original rM,ias

$rM,i= PIDM,i \oplus h(IDM)= (h(IDM) \oplus rM,i) \oplus h(IDM).$ (6)

Then, V uses the previous session key $Ki{-}1$ to decrypt$EKi{-}1\ (rM,i _ Ki{-}1)$ and checks whether $rM,i$and $Ki{-}1$in $EKi{-}1\ (rM,i \_ Ki{-}1)$ are the same as that in (6) andthe previous key $Ki{-}1$ kept by V, respectively. If it is not,V terminates the execution. Otherwise, $PIDM,i$of M isauthenticated. Subsequently, V does the following:

1) Generatinga random number rV,i; 2) Setting as the next sessionkey $Ki = rM,i \oplus rV,i$and keeping it secretly; 3) Sending$EKi{-}1\ (rM,i _ rV,i _ IDV)$ to M.

Since $rM,i$and $rV,i$are generated by M and V, respectively, $Ki = rM,i \oplus rV,i$plays a role of one-time key when Maccesses V. We call this new mechanism "One-time sessionkey renewal".

In addition, comparing with Fig. 2, 3 and 4, it can beseen that the mechanism in the mobile device for session keyrenewal is the same as that for roaming services except theintroduction of different parameters according to the specificenvironment. Hence, though there are redundant fields inSKRP protocol (e.g., IDV in Message 1, we preserve theconsistency of protocol architecture and decrease the complexityof implementation. In other words, the complexity ofthe mobile device can be further simplified.

III. SECURITY ANALYSIS FOR PROTOCOL I

In this section, we analyze the security of the proposed protocolI to verify whether the security requirements introducedin Section I have been satisfied.

A. Identity Anonymity and Intractability Analysis

Our scheme provides identity anonymity in all proceduresby replacing the real identity with a pseudonym identity.

1) In MAP, the real identity IDM of M is replaced withhis pseudonym identity $PIDM$, which is computed as$PIDM = h(NM _ IDH) \oplus IDM \oplus IDH$. Since onlyhome network H knows the secret, nobody except$H$ can obtain the real identity IDM from $PIDM$ by$IDM = PIDM \oplus h(NM _ IDH) \oplus IDH$. Therefore, atracker cannot obtain the secret $h(NM \_ IDH) \oplus IDH$,and it is impossible for him to extract the real identityIDM from the transmitted messages and then trace thelocation of a mobile target user. Since each mobile user$j$'s $PIDj$is computed using unique Nj, the legitimatemobile user j cannot compute another mobile user k's$IDk$by intercepting $PIDk$and impersonate user k.

2) In SKRP, the identity anonymity is guaranteed bythe similar mechanism. In other words, M substituteshis real identity IDM with the pseudonym identity$PIDM,i$, where $PIDM,i$is computed as $PIDM,i=h(IDM) \oplus rM,i$.

The identity intractability is assured by two measures:

1) When M roams in a visited network, the pseudonym identity $PIDM,i= h(IDM) \oplus rM,i$will vary in each session key renewal because of the variance of rM,i;
2) Once M roams into a different visited network, the pseudonym identity $PID_ M,I$also varies due to $r\_ M,i$, which guarantees the freshness of the pseudonym identity PID_M,iin different roaming domains.

Finally, we analyze the *cooperation* attacks in identityanonymity. Assume that there are separate domains betweenvisited networks. When a user enters a new visited network,hewill send a new different pseudonym identity $PIDM,i$to thenew visited network. Moreover, the session key Ki changeswith the variation of $rM,i$and rV,i. So even though there is acooperation between visited networks, a new visited networkstill cannot recognize the user's real identity.

B. Prevention of Fraud

To prevent fraud, the mobile user, the visited network, andhome network should authenticate each other, which requiresthat our scheme provide mutual authentication mechanismbetween any two of them. The proposed MAP protocol canefficiently prevent impersonation attacks from an intruder byconsidering the following scenarios:

1) An intruder cannot impersonate H to cheat V, since hedoes not possess the long-term secret key KVH. Henceit is impossible for an intruder to generate the validresponse $EKVH(rV \_ rM \_ h(IDM))$ to V.

2) V cannot impersonate H to cheat M. Since the sharedkey KMH is unknown to V, and V cannot send user $M$the valid response $EKMH(rM \_ rV \_ IDV)$ which isgenerated by H.

3) An intruder cannot impersonate M either since he cannotknow the real identity of M. If the intruder uses a phonyidentity ID_M, the corresponding spurious pseudonymidentity PID_M can be identified by home network,because H cannot obtain the ID_M by computing$ID_M = PID_M \oplus h(N_M_ IDH) \oplus IDH$Given that the real identity is kept anonymity in ourscheme, only the user himself and his home network Hcan know his real identity.

Similarly, in SKRP Protocol, the identities of M and V are alsocompulsorily authenticated with each other. We consider thefollowing impersonation attack scenarios in SKPP protocol.

1) An intruder cannot impersonate V to cheat M, since hedoes not possess the previous session key $Ki-1$. Henceit is impossible for an intruder to send the authenticmessage $EKi-1(rM,i \_ Ki-1)$ to M.

2) An intruder cannot impersonate M to cheat V. Sincethe previous shared session key $Ki-1 = rM,i-1 \oplus rV,i-1$ is unknown to anyone except only M and$V$, the intruder cannot send the authentic message$PIDM,i,EKi-1\ (rM,i _ Ki - 1)$to V, where $PIDM,i=h(IDM) \oplus rM,i$. Actually, $PIDM,i$also provides animplicit signature $rM,i$for with the shared key $Ki-1$.Moreover, M is required to send back the message$EKi(Ki)$ to V for mutual implicit key authentication.Therefore, due to the mandatory mutual authentication between$M$ and V, our SKRP protocol is efficiently refrainedfrom fraudulent attacks.

C. Mutual Agreement and the Freshness of Session Key

Consider the mutual key exchange mechanism in MAPprotocol. According to (2), $Kauth= rM \oplus rV$. It can beshown that the authentication key $Kauth$is determined by tworandom numbers $rM$and rV, which are chosen by M and V,respectively.Similarly, in SKRP, it can be seen that the session key Kican be also obtained from the mutual agreement mechanism,since the key Ki is derived as $Ki = rM,i \oplus rV,i,\ (i=1,\ 2,\ \ldots,\ n)$, where the two random numbers $rM,i$and rV,iarerespectively determined by M and V independently (4).

In addition, in our scheme the freshness of session keyis guaranteed by executing SKRP protocol. The exchangedMessages 1 and 2 in SKRP protocol provide two fresh random Numbers$rM,i$and rV,i, respectively. Due to $Ki = rM,i \oplus rV,i$,the freshness of $rM,i$and rV,iguarantees the freshness of thesession key Ki in each session key renewal (Fig. 2).

IV. PROTOCOL II BASED ON SELF-CERTIFIED SCHEME

The proposed protocol II is based on the Self-certified scheme [9], [10], [11]. In the protocol, home network H isconsidered as a temporary Trusted Third Party (TTP) forroaming services. When user M visits the visited network V,both of them initialize a registration procedure with H (V actsas an access agent for M). If M and V successfully registerwith H, they will obtain a witness from H, respectively, andthe trust relations between M and V can be established. Mcan then directly negotiate the session key with V withoutaccessing his home network.

A. Self-Certified Scheme

The self-certified scheme combines the advantages ofcertificated-based and identity-based public keycryptosystems[18], [19], and it can also provide a mechanism for authenticatinga user's public key. In this scheme (contrary to identitybasedschemes), each user (mobile device) chooses his secretkey and computes his public key. Then, instead of signing thepair of public key and identity string (contrary to certificatebasedschemes), the authority creates a certificate from thatpair in such a way that it cannot be computed without theknowledge of some trapdoor, known only to the authority,which is H, in this case.For simplicity, we only describe a simple self-certifiedscheme. In the setup phase, the TTP chooses a modulus$n = p \cdot q$, as the product of two random safe primes p and$q$ ($p - 1 = 2p\_$, and $q - 1 = 2q\_$, where $p\_$ and $q\_$ are alsoprimes), generates a base element $g\_ = 1$ of order $r = p\_ \cdot q\_$($g\_ = 1 \bmod(n)$), and picks a large integer $u < r$. Let $t \in Z{*}u$be an element $Z{*}u$ of of order u. A one-way function f willoutput positive integers less than $p\_$ and $q\_$. The TTP makes g,u, f and n public and keeps r secret. $p$and q are discarded.Any user Uithen can register with TTP by performing thefollowing steps.

1) User Uichooses a random number $xi \in \{2, 3, ..., u - 1\}$ as his secret key, computes $yi= gxi \bmod(n)$ as hispublic key and sends y to the TTP.
2) The TTP prepares a string Ii associated with the personalinformation (Name, Address, etc.) of Uiandcomputes $wi= yf(Ii) - 1i$as a witness for user Uiandsends message $\{Ii, wi\}$ to Ui.
3) User Uiverifies Ii and witness $wi$by checking whetherthe equation $yi= wf(Ii)i \bmod(n)$ holds.

Regarding to the security strength of self-certified scheme, itis shown in [8] that forging a valid witness $wi$for user Uiisequivalent to break an instance of RSA cryptosystem.Based on the self-certified scheme, we propose the ProtocolII for secure roaming services. Similar to Protocol I, itcomposes of two phases: 1) the mutual authentication protocol(Phase I); 2) Session key renewal protocol (Phase II).*B. Phase I: Mutual Authentication Protocol (Registration)*Suppose $yM= grM \bmod(n)$ and $yV= grV \bmod(n)$, where$rM$and $rV$are generated by user M and V, respectively.Let IM and IV be two strings associated with the personalinformation (Name, Address, etc.) of M and V, respectively.In addition, let$wM$and wVbe the witness of M and V, whichare issued and calculated by H as follows:$wM= ((yM \oplus IM)f(IM) - 1) \bmod(n)$ (7)$wV= ((yV \oplus IV)f(IV) - 1) \bmod(n)$ (8)

Then the new authentication protocol for roaming servicescan be described in Fig. 5. The shared key KMH is computedas $KMH = (PKH)rM$, where $rM$is generated by M and thepublic key $PKH = gSKH$of H is already delivered to user Mthrough a secure channel in advance. The real identity $IDM$of user M is hidden in the temporary identity $TIDM$, whichis computed as $TIDM = EKMH(grM \oplus IDM)$.Message 1. $M \rightarrow V$:$yM,IDH,T\ IDM$Message 2. $V \rightarrow H$:$yM,yV ,EKVH(yV\_IDV\_TIDM\_TV)$

Message 3. $V \leftarrow H$:$EKVH(wV\_IV),EKMH(wM\_IM\_IDV)$
Message 4. $M \leftarrow V$:$EKMH(wM\_IM\_IDV)$

Fig. 5. Authentication Protocol II for Roaming Services

We explain our proposed protocol II in detail according tothe order of message exchanges as follows.

1) M generates a random number $rM \in Z * u \backslash \{1\}$, computes$yM= grM$and $KMH = (PKH)rM$. M then computes$TIDM = EKMH(yM \oplus IDM)$, and sends IDM and $yM$to V.
2) V chooses a random number $rV \in Z * u \backslash \{1\}$ to compute$yV= grV$, and sends $\{yM, yV ,EKVH(yV\_IDV\_TIDV\_TV)\}$ to H.
3) H decrypts $EKVH(yV\_IDV\_TIDV\_TV)$ byusing shared key KVH. If the time stamp TV is withina reasonable threshold and the decrypted value, $y{*}V$ isequal to clear-text yV, H computes the shared key $KMH$by $KMH = (grM)SKH$ and then decrypts $TIDM =EKMH(grM \oplus IDM)$ with KMH. Then H can get thereal identity of M by computing

$$IDM = E-1KMH(EKMH(grM \oplus IDM)) \oplus grM. \quad (9)$$

If it is legal, H does the following:

1) Prepare twostrings IM and IV associated with the personal information(Name, Address, etc.) of M and V, respectively;
2) Compute the witness $wM$and $wV$for M and Vaccording to (7) and (8).
3) H sends $EKVH(wV_IV)$and $EKMH(wM\_IM\_IDV)$ to$V$.
4) V decrypts $EKVH(wV\_IV)$ and verifies witness andby checking whether (10) holds.

$$yV= ((wv)f(IV) \bmod(n)) \oplus IV. \quad (10)$$

If it is true, V successfully registers with H, and believesthat M is an authorized user. Subsequently, V forwards$EKMH(wM_IM_IDV)$ to M.

5) Similarly, M decrypts $EKMH(wM\_IM\_IDV)$ andverifies IM and $wM$by checking

$$yM= ((wM)f(IM) \bmod(n)) \oplus IM. \quad (11)$$

If it is true, M successfully registers with H, and believesthat the trust relations between M and V are alsoestablished with the help of H.In addition, when M is located in his home network, theauthentication protocol can be described in Fig. 6.

Message 1. $M \rightarrow H$:$yM,IDH,T\ IDM$
Message 2. $M \leftarrow H$:$EKMH(wM\_IM\_IDH)$

Fig. 6. Mutual Authentication Protocol II for Local Services

C. Phase II: Session Key Renewal Protocol

In phase II, we also use one-time session key renewalmechanism.Being different from previous protocols, the mechanismfor this protocol renews the session key by utilizing amodified self-certified scheme and Diffie-Hellman mechanism(Fig. 7).

Message 1. $M \rightarrow V$:wM,IM,gtM
Message 2. $M \leftarrow V$:wV ,IV ,gtV

Fig. 7. Session Key Renewal Protocol II

In Fig. 7, $tM, tV \in Z{*}u$ denotes two different elements of$Z{*}u$ of order u. And the session key KMV can be calculatedrespectively by users M and V as follows.For mobile user M, the session key can be computed as

$$yV= ((wv)f(IV) \bmod(n)) \oplus IV, \quad (12)$$
$$KM = ytMV$$
$$\cdot (gtV)rM= grVtM+rMtV \bmod(n), \quad (13)$$
$$KMV = h(KM). \quad (14)$$

For V, the session key can be computed similarly as follows:

$$yM= ((wM)f(IM) \bmod(n)) \oplus IM, \quad (15)$$
$$KV = ytVM$$
$$\cdot (gtM)rV= grVtM+rMtV \bmod(n), \quad (16)$$

$KMV = h(KV)$. (17)

Clearly, the session key calculated by M and V, respectively,is equal since

$KMV = h(KM) = h(grVtM+rMtV\bmod(n)) = h(KV)$, (18)

where$h$ is a collision-resistant hash function. Key confirmationis done implicitly during the session. Moreover, thisprotocol can yield a different key for each session renewal.The security of the key exchange is greatly improved bythis approach, since each session key is renewed for eachsession. Moreover, compared with our Protocol I, the numberof message exchanges is reduced to two, while the one-timesession key renewal mechanism is preserved.

V. SECURITY ANALYSIS FOR PROPOSED PROTOCOL II

Similar to the analysis in Section III, we analyze the securityof protocol II to verify the security requirements.

A. Identity Anonymity and Intractability Analysis

As shown in Fig. 5, the real identity IDM of M is replacedwith his temporary identity $TIDM$, which is computed as

$TIDM = EKMH(grM \oplus IDM)$, where $KMH = (PKH)rM$.

Since only home network H knows its own secret key SKH,nobody except H can calculate the shared key KMH as$KMH = (grM)SKH$. Hence, only H can decrypt the temporalidentity $TIDM$ with key KMH and obtain the real identityIDM by computing$IDM = E-1KMH(TIDM) = E-1KMH$

$(EKMH(grM \oplus IDM)) \oplus grM$. (19)

Since an illegal tracker cannot obtain the shared key KMH, hecannot extract the real identity IDM from $TIDM$ and tracethe location of a targeted mobile user.The identity intractability is assured by two measures:

1)When user M roams in different visited networks, $TIDM$is different in each session because of different rM;

2) Theshared key $KMH = (PKH)rM$is *one-time-use* so that there isno direct relationship between these shared keys. The changeof rMguarantees the freshness of $TIDM$ and the shared keyin different roaming domains.

B. Prevention of Fraud

Firstly, our MAP scheme can efficiently prevent an intruderfrom impersonating attacks, since the scheme provides securemutual authentication mechanisms between mobile users $M$and V, M and H, or V and H. Consider the followingimpersonation attack scenarios in MAP scheme (Fig. 5):

1) An intruder cannot impersonate H to cheat V, sincehe does not possess the long-term secret key KVH.Hence an intruder cannot to generate the respondingconfirmation $EKVH(wV \_ IV \_ grM)$ to V.

2) V cannot impersonate H to cheat user M. Since theshared key KMH is unknown to V, and V cannotgenerate $EKMH(wM \_ IM \_ IDV \_ grM \_ grV)$ wherewMcontains yMgenerated by M.

3) An intruder also cannot impersonate M since he cannotknow the real identity and/or the password ofuser M. If the intruder uses a phony identity ID_M,the corresponding spurious temporal identity PID_Mcan be identified by home network, since H can obtainID_M by computing $ID\_M = E - 1K\_MH(TID\_M) = E - 1K\_MH(EK\_MH(grM \oplus ID\_M)) \oplus grM$, and then H candetect the spurious identity ID_M. Moreover, the realidentity is kept anonymity in our scheme. Hence nobodyexcept the user himself and his home network H knowhis real identity. If the real identity is shared by otherapplication, the authenticity is further protected by thepassword of user M.

Similarly, we also consider the impersonation attack scenariosin SKRP Phase (Fig. 7) as follows.

1) An adversary is not able to impersonate M to cheat$V$. Since it is impossible for an adversary to obtainthe secret rMunless he can resolve the problem ofcomputing discrete logarithm modulo a large composite.Hence, the adversary can not pretend to act as user$M$ to share or obtain the same session key KMV withthe visited network V, even though any adversary caneasily compute an authenticated pair (wM, IM) for user$M$ satisfying the equation $yM = grM = (wf(IM)M \oplus IM)\bmod(n)$.

2) Similarly, an adversary also cannot impersonate V tocheat M.Comparing with the basic self-certified scheme, we use $wM=((yM \oplus IM)f(IM)-1)\bmod(n)$ as the witness in stead of the original$wM = yf(IM)-1$

$M \bmod(n)$. The improvement is to prevent acheating user from having a chance to get forged self-certifiedwitness, by requiring only one more XOR operation.

C. Mutual Agreement and the Freshness of Session Key

Consider the mutual key exchange mechanism in SKRPprotocol. The new session key is obtained with the mutualagreement mechanism since according to (18) we can derivekey KMV as follows

$KMV = h(grVtM+rMtV\bmod(n))$, (20)

where the two random numbers $rM$and $rV$are respectivelydetermined by M and V independently. In addition, the twonumbers, $tM$and tV, are also randomly selected by M and V,respectively.The freshness of session key is evidently assured, since theexchanged Messages 1 and 2 in SKRP protocol safeguard thefreshness of the two numbers $tM$and tV, which are randomlyselected by M and V, respectively.

D. Prevention of Replay Attack

Finally, we analyze the *replay attack* in session key renewalprotocol (Fig. 7). Consider the case that an adversary pretendsto act as M and tries to exchange a secret key with Vsuch that V intends to share the secret key with M. Theadversary can randomly choose an integer $\alpha \in Z*u$; then hesets $r*M = \alpha \cdot f(IM)$ as a fake secret key for M and replace M'soriginal public key $yM$with $y*M = gr*M\bmod(n)$. However, theadversary cannot compute a valid witness $w*M$ for M, becausethe original witness $wM = ((yM \oplus IM)f(IM)-1)\bmod(n)$ foruser M is self-certified. Therefore, although the adversary canintercept the message $\{wM, IM, gtM\}$, he still cannot forge thecorrect message $\{wM, IM, gtM\}$ which satisfies the followingrelation: $w*M = ((y*M \oplus IM)f(IM) - 1)\bmod(n)$, unless he cancompute discrete logarithm modulo alarge composite. So theproposed protocol is able to resistsuch replay attack, i.e., theadversary and V cannot obtain the same secret key. Similarly,an adversary that impersonates V cannot obtain the same secretkey with M either.

VI. PERFORMANCE ANALYSIS

The performance comparisons, specifically the number of hash operation, symmetric encryption/decryption, exponentialoperation, and the number of message exchanges, between theproposed two protocols and the protocol in [4] are given inTable I and Table II. Note that the rows in bold font show thecomparisons related to mobile user M. It can be generallyconcluded that though the identity anonymity mechanismis introduced into our protocols for roaming service, thecomplexity of the proposed protocols is equivalent to or lessthan the protocol in [4] and the computation requirement formobile device is quite low.The proposed protocol II increases the exponentiation operations,however it reduces the number of symmetric encryption/decryption operations. Though the exponentiation is arelatively time consuming operation, some exponentiation operationcan be pre-computed, e.g. grM, gtM, grV, and gtV. Asa result of these improvements, the real exponentiation computationload is not remarkable. The protocol also provides:

1)identity anonymity;
2) the mutual authentication between thetwo entities withoutpre-setup shared secret key; 3) the sessionkeys renewal for each session. All the features are especiallyfavorable and safer in the roaming environment. Moreover, thereasonable increase of computational load resulting from theidentity anonymity and one-time session key renewal providethe improved security strength that are not considered in [4].Note that the exponential operations required for M are in(11) (Phase I) and (13) (Phase II), respectively. If we onlyconsider the exponential operations except those pre-computedexponential operations, the average computation complexityis 32 _log n2 _ · $M(n)$, where $M(n)$ denotes the computationcomplexities of modular modulo n. In fact, according to thebinary algorithm for fast exponentiation [20], computing gxwill take 2 _log x_ multipliers in the worst case and 32_log x_on the average. So the complexity of computing (11) and (13)can be approximately considered as 32 _log n2 _ on the average.In (13), the exponential operation for $ytMV$ can be pre-computedwhile $(gtV)rM$mod(n) cannot be computed in advance sincethe random variable $tV$is only determined by V and varies inevery session key renewal phase.

VII. CONCLUSION

Two novel mutual authentication and key exchange protocolswith identity anonymity and one-way session key progressionhave been proposed for GLOMONET. The protocolsare suitable for distributed security management, since thetemporary security manager in the visited network performsthe same as that of the original security manager in the homenetwork for subsequent communication. For each protocol, theidentity anonymity has been achieved by hiding the real useridentity in prearranged *PID*s based on the secret-splitting principle or by encrypting the real identity with the sharedkey, respectively. The proposed protocols can protect a mobileusers privacy in the roaming network environment by hidingthe real identity and reduces the risk that a mobile useruses a compromised session key to communicate with visitednetworks by refreshing the session key frequently. The twoprotocols can be applied depending on the availability of thelong-term shared secret key shared by the home network andits mobile users. The performance comparisons have shownthat significant security improvement can be achieved whilethe complexity of our protocols is similar to [4].

REFERENCES

[1] S. Suzukiz and K. Nakada, "An authentication technique based ondistributed security management for the global mobility network," *IEEEJ. Sel. Areas in Commun.*, vol. 15, no. 8, pp. 1606-1617, Oct. 1997.

[2] Z.-J. Tzeng and W.-G. Tzeng, "Authentication of mobile users in thirdgeneration mobile system," *Wireless Personal Commun.*, vol. 16, no. 1,pp. 35-50, Jan. 2001.

[3] L. Buttyan, C. Gbaguidi, and et al., "Extensions to an authenticationtechnique proposed for the global mobility network," *IEEE Trans.Commun.*, vol. 48, no. 3, pp. 373-376, Mar. 2000.

[4] K.-F. Hwang and C.-C. Chang, "A self-encryption mechanism forauthentication of roaming and teleconference services," *IEEE Trans. Wireless Commun.*, vol. 2, no.2 pp. 400-407, Mar. 2003.

[5] S. Patel, "Weakness of north American wireless authentication protocol,"*IEEE Pers. Commun.*, vol. 4, no. 3, pp. 40-44, June 1997.

[6] D. S. Wong and A. H. Chan, "Mutual authentication and key exchangefor low power wireless communications," in *Proc. IEEE Military CommunConf. 2001*, pp. 39-43.

[7] K. Shim, "Cryptanalysis of mutual authentication and key exchange forlow power wireless communications," *IEEE Commun. Lett.*, vol. 7, no.5, pp. 248-250, May 2003.

[8] S. L. Ng and C. Mitchell, "Comments on mutual authentication andkey exchange protocols for low power wireless communications," *IEEECommun. Lett.*, vol. 8, no. 4, pp. 262-263, Apr. 2004.

[9] S. Saeednia, "Identity-based and Self-certified Key Exchange Protocols,"in *Proc. Second Australian Conf. on Info. Security and Privacy 1997*,pp. 303-313.

[10] S. Saeednia, "A note on Girault's self-certifiedmodel," *Info. ProcessingLetters, Elsiver*, vol. 86, no. 6, pp. 323-327, June 2003.