User Authentication Scheme Based on Self-Certified Public-Key for Next Generation Wireless Network

Dake He, Jianbo Wang, Yu Zheng

School of Computer Sciences and Technologies, Southwest Jiaotong Univ., Chengdu 610031, Sichuan, China
E-mail: yuzheng@hotmail.com, dkhe@home.swjtu.edu.cn

***Abstract* – The developing next generation (4G) mobile communication system will offer us great convenience and huge opportunities of service creation with numerous security threats. As a critical security mechanism, user authentication and key agreement (AKA) schemes have received considerable attentions in recent years. In this paper, a AKA scheme (SPAKA) based on self-certified public-key is proposed for the coming 4G system to reduce the storage, computation and communicational load of existing public-key based user authentication schemes while improving the security of 3G AKA scheme. Three authentication protocols including first-time authentication, re-authentication and handoff authentication are designed respectively for different authentication scenarios. According to the performance analysis, our approach has outperformed related schemes by providing better flexibility and scalability while maintain the expected security and efficiency. Consequently, it is more appropriate for 4G wireless system.**

***Index Terms* – Security of Wireless network, Authentication, Self-certified public-key, 4G wireless network.**

I. INTRODUCTION

The coming 4G wireless systems [1][2][3] focus on seamlessly integrating the existing wireless technologies and providing fast and pervasive access and service for mobile user. The combination of mobility and networking has led to the development of a whole new class of very interesting applications, but has also led to a whole new set of technical problems. Security is considered as one of the most challenging problems introduced by mobile networking. User mobility increases the risk of illegal users masquerading as legal users and radio channels have become more vulnerable to eavesdroppers. What's more the resource-constrained mobile device has also presented more requirements on the efficiency of security scheme.

In the scenario of 4G system, firstly, users are empowered to roam among different wireless networks while the heterogeneous wireless networks have their own security domains, mechanisms and security architectures separately. It requires the designed security schemes having more flexibility and scalability. Secondly, there are several wireless network operators in the 4G system, which will raise more risks of cheating on charge and repudiation of the service. Finally, since the wireless networks are no longer isolated respectively, the security of the wired link among the network entities should also be taken into account.

As a critical security mechanism to identify the user's remote logon and control user's access to wireless service, the user authentication and key agreement (AKA) protocol has received considerable research interest in the past years. However, the secret-key based 2G AKA [4] and 3G AKA [5] can not be introduced to 4G systems for the following weaknesses [2][3][6]. (1) Since heterogeneous wireless networks will be connected via IP based bone networks, the unprotected link among the wired parties in 4G systems will suffer from many existing attacks from Internet. (2) In some cases, the system will leak user's international mobile subscriber identity (IMSI) in clear text over air interface. It will cause user suffering from illegal trace. (3) They do not provide any mutual authentication mechanisms between wired parties, e.g. between VLR (visited location register) and HLR (home location register). (4) Compared with public key-based authentication scheme, they have poor scalability and are not suitable for supporting global mobility. (5) They can not provide non-repudiation proof. It will bring trouble in solving the conflict of interest among different network operators.

In this paper a self-certified public-key based AKA (SPAKA) scheme is proposed for the coming 4G system to offer fast access, flexibility, scalability and non-repudiation proof. Our work has the following contributions.

(1) According to the features of mobile network and user mobility, we divided the authentication scenarios of future wireless networks into two categories, referred to as registration authentication and call authentication. We design authentication schemes for them separately, and investigate their transfer relationship. It benefits to support user's mobility and enhance the feasibility of the designed authentication scheme while maintaining security.

(2) A public-key broadcast protocol (PKBP) based on the probabilistic method is proposed for ME to identify the genuine access point (AP) or base station (BS). The PKBP reduces the complexity of the validation on AN's certificate while helping ME resist the possible attack launched by the fake or forged AP/BS.

(3) We introduce self-certified public-key, which need not be accompanied with a separate digital certificate, into the wireless network. Thus, it is unnecessary for the ME to send AN its public-key certificate over the air interface. Our approach contributes to greatly reducing the storage, computation and communicational load of user authentication.

(4) Three protocols, user's first-time authentication, re-authentication and handover authentication, employing different security policies and mechanisms have been designed

1-4244-2427-6/08/$20.00 ©2008 IEEE

to for different authentication scenarios. They will improve the efficiency of authentication and support user's global mobility without sacrificing convenience.

The rest of this paper is organized as follows. In section II, we survey the related work. In Section III, all authentication scenarios in wireless network have been investigated and classified into two categories. Three kinds of authentication protocols, which should be employed in different authentication scenarios of wireless system, are proposed as well. In section IV, PKBP is presented while three kinds of SPAKA are designed for different authentication scenarios separately in Section V. In section VI, our scheme is evaluated and compared with some related authentication schemes. Finally, the conclusion is given in Section VII.

II. RELATED WORK

With the advancing computational capability and increasing storage, the mobile equipment (ME) becomes more powerful to undertake more complex operations. Thus, more and more attentions have been paid on the public-key based authentication schemes recently. In [7][8][9][10], several public-key based AKA schemes including MSR+DH, Siemens, KPN, Boyd-Park and BCY have been proposed and analyzed for wireless networks. However, we argue that all of them have the following security defects:

(1) Both ME and wireless access network (AN) have to exchange their public certificate over the air interface. The transmission increases the communication loads.

(2) Before the authentication ME has to check the validity of AN's certificate, which increases the computational loads on the resource-constrained ME. What's more, it is hard for the ME to verify the AN's certificate when ME enters into an alien wireless network located in the different security domain. Consequently, attackers have the chance to masquerade as a genuine AN to cheat the access of a ME and launch possible attacks.

(3) In some special occasions, e.g. when ME handovers intra or inter the wireless networks, the current public-key based AKA schemes are not efficient enough to support user's mobility since almost all of them require ME computing many heavy operations, such as the digital signature and public-key decryption.

(4) The ME's HE (home environment) does not participate the authentication which is not benefit to providing non-repudiation proof for accounting and charging.

(5) They do not offer different security policies and protocols for user's first time logon, re-logon and handover since the features of user's mobility in wireless network are not taken into account thoroughly.

In [6][11], the secure socket layer/transportation layer security (SSL/TLS) is employed in wireless network to provide strong end-to-end security and flexible user authentication. However, from the viewpoint of ME, the SSL-AKA is still a public-key based authentication and also has the first 3 weaknesses mentioned above.

Some AKA schemes associating the public-key with the secret-key have been presented in [12][13][14] to enhance the security of the secret-key based authentication protocols and improve the efficiency of public-key based methods. However, they just build the trusted relationship among the wired parties such as VLR and HLR etc. in wireless network via public-key mechanism while ME still shares a secret-key with its HE. Hence, it is still hard to provide the trusted non-repudiation proof and will remain many conflicts of interests in the coming 4G systems.

Recently, the EAP (extensible authentication protocol)-SIM [15], EAP-AKA [16], EAP-SSL [17] has been introduced to the wireless networks to solve the security issues of WLAN-2G or WLAN-3G inter-working. In fact, they just encapsulate the authentication message within the EAP [18] protocol, which is a general protocol for point-to-point protocol (PPP) authentication and can support multi authentication mechanism, to achieve communication between the 2G/3G and WLAN. Thus, from the perspective of the cryptographic mechanism and the viewpoint of ME, there is little or no difference between them and the original 2G-AKA [4], 3G-AKA [5], TLS-AKA [11] respectively. Therefore, a secure, flexible, scalable and efficient authentication mechanism is especially needed for the 4G mobile communication systems which should also provide non-repudiation service and offer protection on the wired link intra and inter the wireless networks.

Furthermore, before we design the authentication scheme for wireless network, it is essential to investigate the authentication scenarios in wireless network as well as the relationship between the authentication protocols and the scenarios, which were ignored in many related research works. Unlike the wired network, mobile user may register or launch a call inside or outside his HE, roam to different wireless networks and handoff between diverse systems. The feature of wireless communication and user mobility promote new requirements on the authentication scheme for 4G system. If ME always accesses mobile network via same authentication protocol, e.g. first-time registration protocol, system resources of both network and ME are wasted and wireless service, for instance, handover call, may be blocked because of the long time consumed by the authentication. What's more mobile user may complaint the long time spent on authentication every time he accesses and lose the interest on wireless service. Consequently, we should employ reasonable security policies and mechanisms in different wireless scenarios to improve the performance and security while keeping the advantages of wireless network and user's convenience.

III. Authentication Scenarios in Wireless Network

As shown in table I we roughly divide the authentication scenarios of mobile communication system into two categories, registration authentication and call authentication.

The first scenario, which is implemented when user powers his ME up inside or outside his HE, includes first-time registration and re-registration. Meanwhile, the 2nd scenario composed of the new call and handoff call is employed when user launches a call. The registration authentication is always performed before the call authentication so as to identify user and establish trust relationship between the mobile user and the visited wireless network for the following authentication in advance. On the other hand, the call authentication is implemented to control user's access before the channel allocation, which is usually more efficient than the registration authentication by leveraging the prebuilt trust relationship, e.g. temporary user ID and shared session key.

TABLE I AUTHENTICATION SCENARIOS AND CORRESPONDING PROTOCOLS

<table>
<tr><td colspan="3" rowspan="2">Authentication scenarios</td><td colspan="2">Authentication protocols</td></tr>
<tr><td>1st choice</td><td>2nd Choice</td></tr>
<tr><td rowspan="5">Registration authentication</td><td rowspan="3">First-time registration</td><td>In HE</td><td colspan="2">First-time auth. protocol</td></tr>
<tr><td rowspan="2">Outside HE</td><td>Handoff auth. protocol</td><td rowspan="6">First-time auth. protocol</td></tr>
<tr><td colspan="2">Re-registration</td><td>Re-auth. protocol</td></tr>
<tr><td rowspan="4">Call authentication</td><td colspan="2">New call</td><td>Re-auth. protocol</td></tr>
<tr><td rowspan="3">Handoff call</td><td>Intra sub-networks</td><td>Re-auth. protocol</td></tr>
<tr><td>Inter sub-networks</td><td rowspan="2">Handoff auth. protocol</td></tr>
<tr><td>Inter networks</td></tr>
</table>

On the other side we just need to design three authentication protocols presented in the second column of table I, which includes (1) first-time authentication protocol, (2) re-authentication protocol and (3) handoff authentication protocol, to satisfy the requirement of different authentication scenarios. All the authentication scenarios except for first-time registration inside HE have two protocols to choose. The first choice, which is fitter for the corresponding scenario, will be substituted by the 2nd choice if it fails in performing.

In Figure 1 the logical data flow of different authentication protocols designed for different authentication scenarios are presented briefly. Here we do not specify a certain wireless network but rather discuss the authentication in a universal wireless environment. The wireless network in Fig.1 may be UMTS (Universal Mobile Telecommunication System), GPRS (General Packet Radio Service) or WLAN system etc. and the AP/BS may be a base station in GPRS system, a node-B in UMTS or an access point in WLAN.

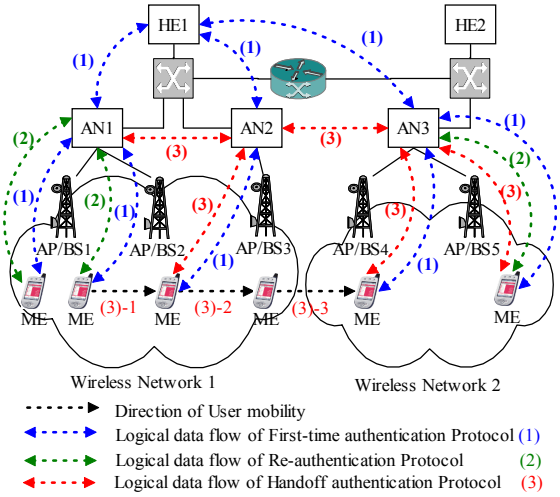

Figure 1. Authentication scenarios and corresponding protocols employed in wireless network

For instance a mobile user belongs to HE1 should perform the first-time authentication protocol when he register with AN1 for the first time since AN1 also belongs to HE1. While the re-authentication protocol should be implemented when he access AN1 again, e.g. re-register after re-powers ME up or launch a call. When the ME moves forward to AP/BS2 from AP/BS1 during the conversation a handoff call will be launched. Since both AN1 and AN2 belong to the same HE1 the re-authentication protocol should be performed as the first choice to improve the efficiency of the access. However, if the ME roams from AP/BS2 to AP/BS3 or handoff between AP/BS3 and AP/BS4 the handoff authentication should be implemented as the first choice. Only when the handoff authentication fails in implementation, the possible reason may be the temporary user ID or shared key is expired or the failure on retrieving user ID from the temporary one, the first-time authentication protocol will be performed.

IV. Public-key Broadcast Protocol (PKBP)

Recently, the public key infrastructure (PKI) has been gradually introducing in wireless network to provide enhanced scalability and advanced security for mobile user. Projects like ASPeCT [19], USECA [20] and Third Generation Partnership Project (3GPP) discussion documents [21,22] anticipate that evolution and the advanced protocols such as the MExE (Mobile Execution Environment) [23] and WAP (Wireless application protocol) [24] have moved forward to employ the public-key methods as well.

It is well known that in the public-key based authentication the authenticator and the authenticatee must exchange their digital certificate and validate other side's certificate before the further negotiation. Unfortunately, in current wireless PKI architectures more attention has been paid on how to manage and verify the user's digital certificate as well as identify user's access via public-key mechanism. On the contrary from the perspective of ME few security

mechanisms have been offered for the mobile user, which are used to validate the wireless network's certificate and support wireless roaming without sacrificing user convenience and security. In [6], given that the change on CA's certificate is rare, a trusted CAs list with corresponding public-key are pre-stored in the USIM card so that user can verify the received certificate from the wireless network. We name it after *pre-store method* in the following description for convenience. However, in the scenario of the future mobile communication system it is really hard to pre-store all the CA's public-key in user's USIM card in view of the randomness of user mobility and the diversity of trusted domains. What's more, this method can only verify the integrity but not the time-validity of the wireless network's certificate since the CAs list and corresponding public-key in the USIM (Universal Subscriber Identity Module) card can not be updated in time and easily. I.e. the mobile user is vulnerable to be cheated by fake AP/BS and suffers from the possible attacks when he roams into another security domains.

The second method we can figure out is that user only stores the certificate of CA he belongs to and pre-downloads the adjacent CA's certificate real-timely from his own wireless network after passing the authentication procedure. Thus user can perform authentication with the AP/BS when entering the adjacent wireless network. Subsequently, the ME can keep on downloading the adjacent CA's certificate so as to perform the authentication in the following roam. We name it after *pre-download method* hereafter. This method is effective when user moves continuously from one wireless network to another adjacent one but fail in the scenario of user's jump-move, for instance we fly to a new area by airplane and the ME is turned off during the move. Consequently the ME cannot pre-download the certificate successively in this case.

The third method maybe performed in the wireless PKI is that ME's HE validate the visited AN's certificate on behalf of ME in advance. On receiving ME's request the visited AN sending its certificate to the ME's HE and gain a returned validation result, which includes the HE's signature on the sent certificate. Then the visited AN transfers its certificate with the validation result to ME. Since trusting its own HE and holding HE's certificate ME can validate visited AN's certificate according to the HE's signature on the certificate. We name it after *online-validation method*. However, the validation procedure will consume lots of time cost on computation and communication especially when the visited AN is far away from ME's HE, which will scarify the efficiency and convenience of user's access and may increase the possible block probability of communication system.

Consequently, we do need to provide a verification mechanism for the mobile user to validate the AN's certificate which can support user's mobility, convenience and security simultaneously. As shown in Fig.2, every AP/BS co-broadcasts its own public key (PK_{AP}), identity (ID_{AP}), and modulus (N_{AP}) as well as those parameters of its neighbors from public broadcasting channel (BCH). Optionally, the IPv6 address (IP_{AP}) can also be included in the parameter to support IP-based mobile network. I.e., AP/BS2 broadcasts its public parameters (PK_{AP2}, ID_{AP2}, N_{AP2}, IP_{AP2}) together with AP/BS1's (PK_{AP1}, ID_{AP1}, N_{AP1}, IP_{AP1}) and AP/BS3's (PK_{AP3}, ID_{AP3}, N_{AP3}, IP_{AP3}). Just like AP/BS2, AP/BS1 broadcasts its own parameters and that of AP/BS2 and AP/BS3 and so on. Thus a pervasive broadcast will be formed based on 4G network's seamless coverage. In fact the number of fake/forged AP/BS established by attackers is much smaller than genuine AP/BS in the real world in view of the expensive cost for an AP/BS. I.e. even if attackers publish its parameters via fake/forged AP/BS, the number of parameters broadcasted by genuine AP/BS is greater than that issued by the forged/fake one.

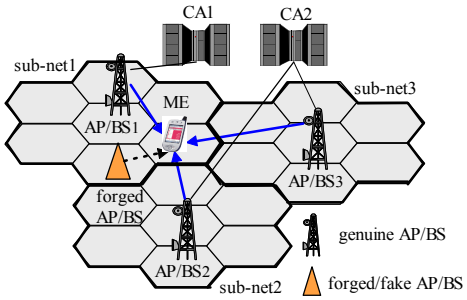

Figure 2. An example of PKBP in a wireless network

When entering sub-network1, ME will receive parameters issued by the forged AP/BS and that co-broadcasted by genuine (AP/BS1, AP/BS2, AP/BS3) respectively. As shown in Fig.3, a small FIFO (First In First Out) buffer should be hold in ME, the main role of which is to store received public-key parameters and corresponding signal power (SP). As a result, the number of (PK_{AP1}, ID_{AP1}, N_{AP1}, IP_{AP1}) in the FIFO is much more than (PK_{AP}', ID_{AP}', N_{AP}', IP_{AP}') issued by the forged AP/BS. Then according to SP_{AP1}, which is greater than SP_{AP2} and SP_{AP3}, ME will access AP/BS1 despite of the most powerful signal SP_{AP}'. In this way, according to the number of received public-key parameters and corresponding signal power, ME can resist attack launched by fake/forged AP/BS and reduce the complexity on validating AP/BS's certificate.

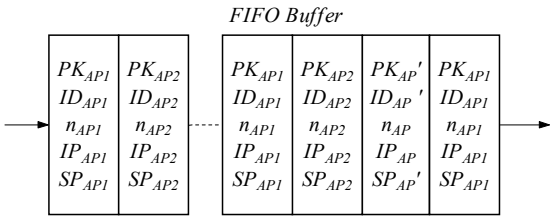

Figure 3. Judge the valid parameters via PKBP

V. SELF-CERTIFIED PUBLIC-KEY BASED AUTHENTICATION

The following notations will be used in the description of our authentication scheme: ID_X, SK_X, PK_X, $Cert_X$ and Sig_X

denote the entity X's identity, private-key, public-key, digital certificate and signature separately. $H(x)$ is a secure hash function and $\{x\}_k$ represents encrypting content x with key k. $\|$ and $\oplus$ represent the symbol of concatenation and bit-wise XOR separately. $|x|$ denotes the length of x and N_X is a nonce generated by the entity X.

A. Architecture of our user authentication scheme

In our scheme, a certificate authority (CA) is employed in each wireless network and issues public-key certificate to the network entities, e.g. VLR, HLR and access point (AP), located in its security domain. The CAs distributed in different security domain can build the trusted relationship via different trusted model of PKI, which is not the topic of this paper. Each CA generates a RSA key pair (e, d) and a large integer n, a product of two prime factors p and q, for itself respectively. The integer e co-prime to p-1 and q-1 and the converse d of e modulo (p-1)(q-1). Then CA computes an integer g of the maximal order in the multiplicative group Z_n^*. The CA publishes the e, n and g, and keeps the d, p and q secret. According to equation (1) CA generates the self-certified public-key (I_U) for each mobile user in its domain.

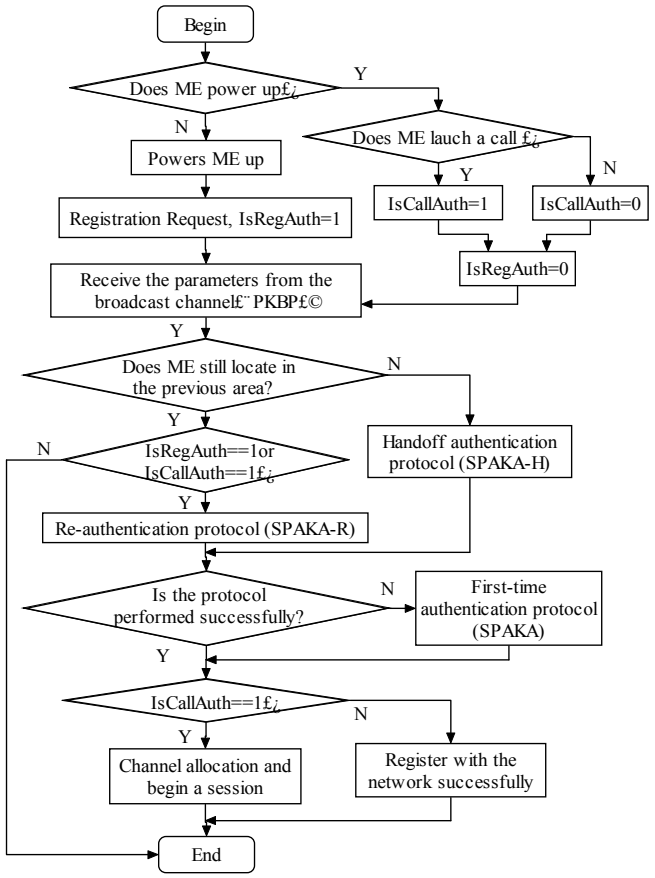

Figure 4. Flowchart describing how to select the reasonable protocol

$$I_U = (g^{-S_U} - ID_{User} - ID_{HE})^{1/e} \bmod n . \qquad (1)$$

In equation (1) S_u is a more than 160-bit private-key selected by the user. CA issues every user a USIM card, which stores the S_u, ID_{HE}, ID_{User}, g and n. Subsequently, CA saves g, I_U and ID_{User} in HE's database and destroys the p, q and S_u. All the users can share the same g, which does not reduce the security of our scheme.

Based on user's mobility and the requirements of authentication scenarios, different security policies and mechanisms are employed in our scheme to provide first-time authentication protocol (SPAKA), re-authentication protocol (SPAKA-R) and handover authentication protocol (SPAKA-H). How to select the reasonable protocol in terms of situation is depicted in Fig.4 where TID_{User} is a temporary ID issued by the previously visited AN.

B. First-time authentication protocol of SPAKA

The first-time authentication procedure of our SPAKA is depicted in Fig.5, which is based on user's permanent identity and should be used when TID_{User} is not available or expired. In the following description the A, B, S are three integers satisfying $|B| \geq 32$, $|S| \geq 160$ and $|A| \geq |S| + |B| + 80$.

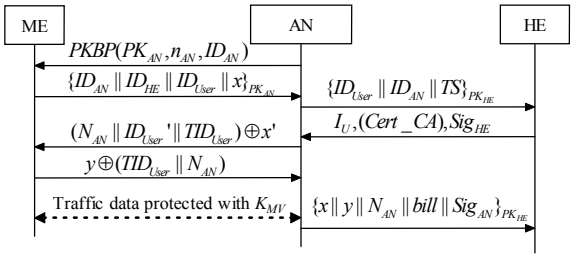

Figure 5. The first-time authentication protocol of our SPAKA

(1) ME keeps on receiving the public-key parameters from the broadcasting channel and judges the valid AP/BS as well as the corresponding parameters via PKBP protocol.

(2) ME selects a nonce $N_U \in [0, A]$ and computes x as follows.

$$x = H(g^{N_U} \bmod n) . \qquad (2)$$

Then ME encrypts the (x, ID_{AN}, ID_{HE}, ID_{User}) with AN's public-key (PK_{AN}) and sends them to AN.

(3) AN decrypts the message (2) and checks the correctness of the received ID_{AN}. Then AN sends $\{ID_{User} \| ID_{AN} \| TS\}_{PK_{HE}}$ to the user's HE according to the received ID_{HE} to request user's self-certified public-key. The TS shown in this message is a timestamp to against replay attack.

(4) If checking the received message is valid, user's HE responds user's I_U with its signature Sig_{HE} computed as equation (3) to the AN. Optionally, the $Cert_{CA}$ can also be included in this message if AN does not hold the certificate of the CA which issues I_U for the user.

$$Sig_{HE} = \{H(I_U \| Cert_{CA} \| TS)\}_{SK_{HE}} . \qquad (3)$$

(5) After checking the validity of the Sig_{HE}, AN generates a nonce $N_{AN} \in [0, B]$ and a temporary identity (TID_{User}) for

the user. Then AN protects (ID_{User}, N_{AN}, TID_{User}) with the least significant 128-bit of the x (x') and sends encrypted message to ME.

(6) With its own x, ME recovers (N_{AN}, ID_{User}, TID_{User}) from the received message (5). If checking the ID_{User} is identical to the sent one in message (2), ME authenticates the AN and saves the TID_{User} for future authentication. Subsequently, ME computes y as equation (4) and delivers AN the y encrypted by (N_{AN}, TID_{User}).

$$y = N_U + N_{AN} \times S_U . \quad (4)$$

(7) AN retrieves the y and checks whether equation 5 and 6 hold. If both equations hold, the user is identified by the AN. Both ME and AN use the least significant 128-bit of y as the shared session key (K_{MA}) for future communication. Otherwise, the authentication is terminated.

$$H[g^y (I_U{}^e + ID_{User} + ID_{HE})^{N_{AN}} \bmod n] \stackrel{?}{=} x . \quad (5)$$

$$y \stackrel{?}{\in} [0, A + (B-1)(S-1)] . \quad (6)$$

Hereafter, AN stores (ID_{User}, TID_{User}, I_U , K_{MA}) for future re-authentication. After offering the service to the user, AN can send ($x||y||N_{AN}||bill||Sig_{AN}$) as charging proof to the user's HE. Where *bill* includes the detail information about the provided service and Sig_{AN} is AN's signature on the full message.

C. Re-authentication protocol of SPAKA (SPAKA-R)

As shown in Fig.6, when user re-logon the AN he accessed previously, e.g. user launches a new call or repowers up his mobile phone, the re-authentication procedure of SPAKA (SPAKA-R) is called. Firstly, ME generates x as equation (2) and sends it with TID_{User} to AN. Then AN retrieves the (ID_{User}, I_U , K_{MA}) from its database according to the TID_{User}, and issues a nonce N_{AN} and new temporary identity (TID_{User}') for the user. Subsequently, AN responds ME the (N_{AN}, TID_{User}', TID_{User}) encrypted with K_{MA}. After checking the received TID_{User} is identical to the sent one, ME computes y as equation (4) and sends it to AN. If equation (5) and (6) are both verified correctly, the user is authenticated and AN can utilize the ($x||y||N_{AN}||bill||Sig_{AN}$) as the non-repudiation proof to charge from user's HE. Meanwhile both ME and AN update the TID_{User} with TID_{User}' and substitute K_{MA} with the least significant 128-bit of the present y separately.

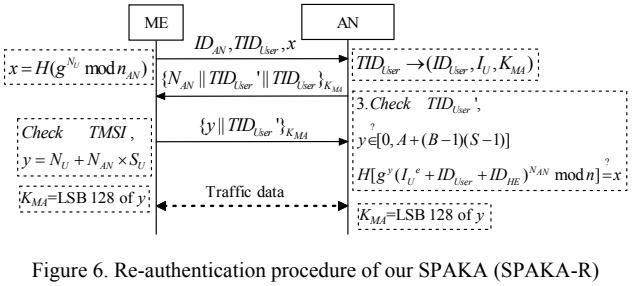

Figure 6. Re-authentication procedure of our SPAKA (SPAKA-R)

D. Handover authentication protocol (SPAKA-H)

As shown in Figure 7, when user roams into a new AN or handover between two ANs during a conversation, the SPAKA-H is called to support user mobility. Here we name the AN previously accessed by the ME after old AN while name the presently visited AN is called new AN.

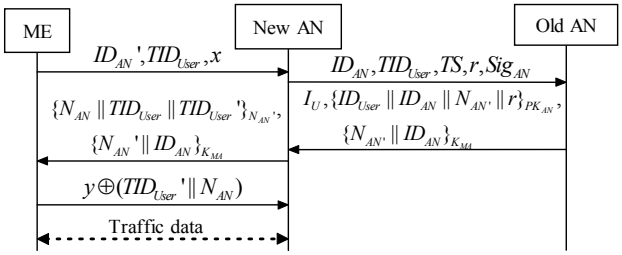

Figure 7. Handover authentication procedure of SPAKA (SPAKA-H)

(1) ME generates x as equation (2) and sends x, TID_{User} and old AN's identity (ID_{AN}') to the new AN.

(2) If the received ID_{AN}' is not its identity, the new AN generates a nonce r and delivers its identity ID_{AN}, timestamp TS and the received TID_{User} to the corresponding old AN according to the ID_{AN}'. Meanwhile the new AN signs the message with its private-key and attaches the signature Sig_{AN} in the message.

(3) If checking the received message is valid, the old AN generates a nonce N_{AN}' and sends the new AN I_U, $\{ID_{User} \| ID_{AN} \| N_{AN'} \| r\}_{PK_{AN}}$ and $\{N_{AN'} \| ID_{AN}\}_{K_{MA}}$.

(4) The new AN decrypts $\{ID_{User} \| ID_{AN} \| N_{AN'} \| r\}_{PK_{AN}}$ with its private-key and checks whether the included ID_{AN} and r are both correct. If the condition holds, the new AN issues a new TID_{User}' for the user and encrypts the (N_{AN}, TID_{User}, TID_{User}') with N_{AN}'. Then it is sent to ME with the received $\{N_{AN'} \| ID_{AN}\}_{K_{MA}}$.

(5) After ME decrypts $\{N_{AN'} \| ID_{AN}\}_{K_{MA}}$ with K_{MA} and checks the ID_{AN} is correct, ME retrieves the (N_{AN}', TID_{User}, TID_{User}') with N_{AN}' and verifies the TID_{User} is identical to the user's present temporary identity. Then ME sends y to the new AN, which is computed as equation (4) and protected by TID_{User}' and N_{AN}.

(6) If the new AN verifies both equation (5) and (6) hold, the user is identified. Otherwise, user's access is resisted.

VI. Performance Analysis

A. Performance analysis on PKBP

As shown in table II, our PKBP is compared with the current *pre-stored method*, possible *pre-download method* and *online validation method*, which indicate our scheme is more efficient and scalable to support user mobility and convenience. Where the more symbol '+' a scheme owns in one item the better its corresponding feature is. Since our PKBP is a probability-based scheme, it is possible to gain an error judge-result when the density of fake AP/BS is higher than that of genuine AP/BS in a local area. But the

attacker must cost a lot, may even more valuable than the information they attempt to capture, to perform the attack on our PKBP. In view of the seamless coverage of the 4G system our PKBP will develop its practical functionality in the real communication system. How to select the length of the FIFO buffer and determine the relationship between the density of fake AP/BS and the credibility of the judge-result is our undergoing future work.

TABLE II COMPARISON OF CERTIFICATE VALIDATION SCHEME FOR ME

Scheme	Mobility	Efficiency	Scalability	Credibility	
				Integrity	Time-validity
Pre-stored	+	++	+	++	+
Pre-download	++	++	++	+++	+++
Online validation	+++	+	+++	+++	+++
PKBP	+++	+++	+++	++	++

B. Security analysis on SPAKA

As shown in table III our scheme is compared with the major user authentication scheme proposed for wireless network. Where the symbol '/' denotes the security feature does not pertain to the corresponding scheme.

TABLE III COMPARISON OF SECURITY AMONG AUTHENTICATIONS SCHEMES

Security features	GPS [19]	Ours	3G AKA [5]	SSL AKA [6,11]	PK AKA [7,8,9]	Hybrid AKA [12,13]
Mutual authentication between ME and AN	No	Yes	Yes	Yes	Yes	Yes
Auth. among wired parties	/	Yes	No	Yes	/	Yes
Resist replay attack	Yes	Yes	Yes	Yes	Yes	Yes
Resist man-in-middle attack	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality of user's identity	/	Yes	No	Yes	Yes	Yes
Fairness of the key agreement	/	Yes	No	Yes	Yes	Yes
Non-repudiation	Yes	Yes	No	Yes	Yes	No
Protection on the wired link	/	Yes	No	No	/	Yes
Resist fake AP's attack	/	Yes	No	No	No	No
Transfer cert. over air interface	No	No	No	Yes	Yes	Yes
Scalability	Yes	Yes	No	Yes	Yes	Yes
Support temporary identity	No	Yes	Yes	Yes	No	Yes
Support handoff	No	Yes	Yes	Yes	No	Yes
Efficiency	High	High	High	Low	Low	Middle

The security of our scheme is based on the GPS [25] identification scheme, which was proposed by Girault and proven secure by Poupard and Stern [26]. The security analysis shows that if an attacker is able to forge valid signatures for a non-negligible fraction of the possible public keys then he is able to compute discrete logs mod N and therefore to factor N. On the other hand if an attacker is only able to forge signatures for a fixed key then he must be able to compute the discrete log of this key or to solve the so-called strong RSA problem as it was noticed by Camenisch and Michels in [27].

However, with the following advantages our SPAKA is more secure, efficient and qualified to support user mobility as compared to the original GPS identification scheme. (1) We introduce temporary identity mechanism into GPS, which improves the efficiency of original GPS scheme and protects user privacy. (2) We associate public-key with secret-key to offer different security policies for different authentication scenarios. (3) The x and y, which are public in GPS scheme, are also kept secret and the mutual authentication between the user and the AN has been achieved in the SPAKA. Consequently our scheme enhances the security of the original GPS scheme. (4) With the help of our PKBP, ME can judge the validity of the received public-key parameters and access the valid AN flexibly and efficiently.

C. Efficiency analysis on SPAKA

As shown in table IV, from the viewpoint of ME, our scheme is compared with some existing user authentication protocol in the aspect of computation. The pre-exponential operation (Pre-Ex), exponential operation, public-key encryption (PKE), signature generation, signature verification (Ver), Pre-hash operation (Pre-H), online Hash operation, Xor and secret-key encryption/decryption are listed from the 2nd column to the 9th column separately.

TABLE IV CRYPTOGRAPHIC OPERATION OF DIFFERENT AUTHENTICATION SCHEMES IN ME

Protocol	Pre-EX	EX	PKE	Sig	Ver	Pre-H	H	Xor	EK
Siemens	1	1	0	1	1	0	2	0	1
Boyd-Park	0	0	1	1	0	0	2	0	1
BCY	0	1	1	0	1	0	1	0	1
IBCY1	0	1	1	0	1	0	1	1	1
SPAKA	1	0	1	0	0	1	0	2	0
SPAKA-R	1	0	0	0	0	1	0	0	2
SPAKA-H	1	0	0	0	0	1	0	1	2
3G AKA	0	0	0	0	0	0	0	1	2
SSL AKA	0	0	2	1	1	0	3	0	0

II. CONCLUSION

In this paper, we designed three categories of authentication scenarios for the coming 4G system. An efficient user authentication scheme, called SPAKA, based on self-certified public-key has been proposed for future wireless network. The proposed SPAKA is evaluated via performance analysis. As a result, SPAKA reduces the storage, computation and communicational load of the user authentication while maintaining security and user mobility. Con-

sequently, it is qualified to satisfy the requirements of the future mobile network.

In the future, on one hand, we are going to build a mathematic model to determine the PKBP's probability of successfully identifying a valid AP/BS in the real world. Then, constructing an experimental wireless network via WLAN or bluetooth system to validate the PKBP is a potential work.

REFERENCES

[1] Y.H Suk., H.Y. Kai. Challenges in the migration to 4G mobile systems. IEEE Communications Magazine, 2003, 41(3): 54-59.

[2] Y. Zheng, D. He, X. Tang, H. Wang. Trusted Computing-Based Security Architecture For 4G Mobile Networks. In: Proc. of Int. conf. on PDCAT, Dalian, China. 2005.12, IEEE Computer Society: 251-255

[3] Y. Zheng, D. He, X. Tang. AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform, In: Proc. of Int. conf. on ICICS05, Bangkok Thailand. 12, 2005, IEEE Press: 976-980

[4] ETSI GSM 02.09. Digital cellular telecommunications system (Phase 2+) (GSM); Security aspects. ETSI GSM

[5] 3GPP TS 33.102: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; 3G Security Architecture. 3GPP, 1999.

[6] G. Kambourakis, A. Rouskas. Performance evaluation of public key-based Authentication in future mobile communication systems. EURASIP Journal on Wireless Comm. and Networking. 2004, 1(1): 184-197.

[7] M. J. Beller, L. F. Chang, Y. Yacobi. Privacy and authentication on a portable communications system. IEEE Journal on Selected Areas in Communications. 1993, 11(6): 821-829.

[8] N. El-Fishway, A.Tadros, On the design of authentication protocols for third generation mobile communication systems. In: proc. of conf. on the 20th National Radio Science, Cairo Egypt, 2003: C24_1-C24_10.

[9] T. Newe, T. Coffey. Security protocols for 2G and 3G wireless communications, In Proc. of the 1st Int. symposium on Information and communication technologies, 23-26, 2003. Dublin, Ireland. Sep. ACM International Conference Proceeding Series; Vol. 49, 2003. pp. 335-340

[10] S. Putz, R. Schmitz, and F. Tonsing, Authentication schemes for third generation mobile radio systems, In: Proc. of the 9th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. 1998, 1(1): 126-130.

[11] G. Kambourakis, A. Rouskas, and S. Gritzalis, Using SSL/TLS in authentication and key agreement procedures of future mobile networks. In: Proc. of 4th Int. Workshop on Mobile and Wireless Comm. Network. September 9-11, 2002, Stockholm, Sweden. IEEE press, pp.191-195.

[12] J. M. Jeong, G. Y. Lee, Y. Lee. Mutual authentication protocols for the virtual home environment in 3G mobile network. GLOBECOM '02. Nov. 17-21, 2002, Taipei, Taiwan, IEEE press, Vol. 2: 1658-1662.

[13] J. M. Jeong, G. Y. Lee, Yong Lee. Design and analysis of extended mutual authentication scheme for the virtual home environment in 3G mobile network. In: proc. Student Conference on of Research and Development, July 16-17, 2002, pp.245-248.

[14] S. M. CHENG, S.Y. SHIEH, W. H. YANG, Designing Authentication Protocols for Third Generation Mobile Communication Systems [J]. Journal of information science and engineering, 2005, 21(2): 361-378.

[15] H. Haverinen,J. Salowey. "EAP SIM Authentication". Internet Draft: draft-haverinen-pppext-eap-sim-11.txt. June 2003, work in progress.

[16] EAP-AKA, 3GPP TS 23.234

[17] G. Kambourakis, A. Rouskas, G. Kormentzas, S. Gritzalis. Advanced SSL/TLS-based authentication for secure WLAN-3G interworking, IEE Proceedings 2004, Vol.151, PP.501-506.

[18] RFC 2284 - PPP Extensible Authentication Protocol (EAP)

[19] ASPeCT Project, *Securing the future of mobile communications*, 1999, http://www.esat.kuleuven.ac.be/cosic/aspect.

[20] USECA Project, "UMTS security architecture: Intermediate report on a PKI architecture for UMTS," Public Report, July 1999.

[21] 3GPP TSG, "Using PKI to provide network domain security," Discussion Document S3- 010622 SA WG3 Security–S3# 15bis, November 2000.

[22] 3GPP TSG, "Architecture proposal to support subscriber certificates," Discussion and Approval document, Tdoc S2-022854, October 2002.

[23] 3G TS 23.057, Mobile Station Application Execution Environment (MExE); *Functional description; Stage 2;* Version 1.3.0, August 1999.

[24] "Wireless Application Protocol Public Key Infrastructure Definition", WAP Forum Draft, version 24-April-2001.

[25] C. Poupard, J. Stern. On the fly signatures based on factoring . In: Proc. of ACM Conf. on Computer and Communications Security, Singapore, ACM press, 1999:37-45

[26] G. Poupard, J. Stern, Security analysis of a practical on the fly Authentication and Signature Generation. In: Proc. Eurocrypt'1998, Espoo Finland, LNCS, 1998: 422-436.

[27] J. Camenisch and M. Michels. A Group Signature Scheme with Improved Efficiency. In Asiacrypt'98, 1998, LNCS, Springer Verlag.