This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2005 proceedings.

Fast and Secure Universal Roaming Service for Mobile Internet

Yeali S. Sun [1] , Yu-Chun Pan [2] , Meng Chang Chen [3]

Dept. of Information Management[1] National Taiwan University Taipei, Taiwan sunny@im.ntu.edu.tw

Dept. of Information Management [2] National Taiwan University Taipei, Taiwan ycpan@ntu.edu.tw

Institute of Information Science[3] Academia Sinica Taipei, Taiwan mcc@iis.sinica.edu.tw

***Abstract*—Rapid deployment of IEEE 802.11 based wireless access networks in hot spots and the integration of the networks to the existing wide-area communication infrastructure have become a major driving force to speed up the design and development of necessary security and quality of service (QoS)-guaranteed mechanisms with roaming capacity to mobile users. Three issues are raised in such a communication environment: a) service users would like to have IP-based roaming capability as they move rather than being constrained to a single spot or being forced to disconnect because his/her service provider does not have entire coverage of the city/region; b) the need on security and accounting management for mobile Internet; and c) the execution of AAA however would incur extra delay to handoff latency. For applications like VoIP, video streaming and TCP connections, it may disrupt the on-going communications if such latency becomes too large. In this paper, we propose an AAA-enabled roaming alliance architecture that provides *fast* and *secure universal roaming service* across *multiple* service domains. The associated protocols and the supporting security mechanisms are also proposed. Our design provides continuing communications service to mobile user belonging to different service operators to quickly and securely access service when roaming across multiple service domains. Mobile users only need to carry a *U-Mobile Token* to receive the service. The schemes proposed only incur minimal latency in security check. This is particularly important to the support of real-time mobile applications.**

I. INTRODUCTION

The motivation for this work comes from an observation of rapid deployment of IEEE 802.11 based hot spot wireless access networks and the integration of these networks to the existing wide-area communication infrastructures, both wired and wireless. It has become one of the major driving forces to speed up the development and deployment of new services (e.g., VoIP and multimedia content delivery) and new multi-network attachment equipment (e.g., dual-mode wi-fi and GPRS/3G handset).

Our vision of the future wireless networks will have the following characteristics: *a*) different, possibly overlapping, radio access networks serving the same area; *b*) each provides different services in terms of coverage range, bandwidth or delay; and *c*) users carry small light-weight, pocket-size multi-mode terminal devices (e.g., a 3G/wi-fi terminal device). Users may access multimedia services through multi-mode mobile devices, across possibly integrated heterogeneous networks, anytime, anywhere they move from one cell/network to another. Network provider must develop services and applications that are able to attract customers and to produce profitable business. To make the business model of such vision successful, services must be rich and varied, catering to various subscribers' needs and tastes.

We have identified several important features for these emerging Internet services. First is the *mobility* – service users would like to have IP-based roaming capability as they move rather than being constrained to a single spot or being forced to disconnect because his/her service provider does not have entire coverage of the city/region. Hence, seamless IP roaming across different service domains is an essential service to assure users good service usage experience as well as to make the service business successful. Here, a service domain is an independently administered service network. This service enables mobile users belonging to different service operators to access needed resources provided by foreign network domains. We refer to such service as the *universal roaming service*.

The importance of providing universal roaming service is easy to understand by looking at the advantage (or the success) of the current cellular phone service over the fixed-line phone service. This service model is indeed a win-win to both service providers and service users. Service providers can profit from additional use of their networks/services from the customers of other service operators. Moreover, individual operator has no need to spend enormous investment on building infrastructure that covers the entire area. All operators' investments are not overlapped and wasted due to redundancy. Resources will be better utilized. From the service user's perspective, they can enjoy convenience access to more resources whenever they go and on-going communications are guaranteed to continue. The administration issues such as service authentication, authorization and accounting should be well designed and equipped to make them transparent to service users. We believe providing universal IP roaming service is fundamental and key to the success of mobile business and mobile commerce.

In this paper, we propose a service architecture to support fast and secure universal roaming service across multiple service domains. The associated protocols and the supporting security mechanisms are also presented. The goals are *a*) to provide continuing communications service when mobile user belonging to different service operators roam across multiple service domains; *b*) mobile users only need to carry one single identification or service token to receive the same service on any service networks; and *c*) to minimize the handoff latency in secure (AAA-enabled) roaming service specifically to support real-time applications.

This paper is organized as follows. In Section II, we briefly summarize the operations of AAA-enabled mobile IP architecture and point out the performance issue raised in the support of fast handoff in secure universal roaming service. In Section III, we present the AAA-enabled roaming alliance architecture and the membership management protocol. The proposed model is aligned with IETF Mobile IP[1]and AAA

frameworks[5][6][15]. In Section IV, we describe the goals and the design of U-Mobile Token which is used to enable mobile users to fast securely roam across different service domains belonging to the same AAA roaming alliance. In Section V, we present the two-stage roaming authentication procedure to achieve fast and secure handoff. Finally, the conclusion is given in Section VI.

II. AAA-ENABLED MOBILE IP ARCHITECTURE

A. *Mobile IP and AAA*

The goal of the basic Mobile IP architecture [1] is to enable a mobile node with a registered home address in a home domain to roam across different network segments of a service domain. In the simple triangle routing model, the home agent (HA) will redirect packets destined to the mobile node to the network indicated by the mobile node's care-of-address by using IP-in-IP tunneling technique. A more efficient communication paradigm called route optimization is to let mobile node or home agent send binding update to the correspondent node (CN).

In response to the growing demands on security and accounting management for mobile Internet, IETF has defined the AAA Framework [5][6] to assure only authenticated mobile users can get access to the resources in a foreign network. As shown in Figure 1, each network domain has at least one AAA server. A mobile node (MN) must have a home AAA and establishes a service subscription relationship with its home AAA. To receive services at a foreign domain, a MN must follow the AAA protocol for identity authentication, service level authorization and accounting for billing purpose. This AAA framework requires two security relationships established in advance: a security association (SA) between MN and its home AAA, and an SA between the foreign AAA and the MN's home AAA.

In AAA-enabled mobile IP, there are two basic scenarios. First is that user must complete the AAA check from the service provider's AAA server before performing Mobile IP (MIP) operations, e.g., sending the MIP registration message. The other scenario is to explore the possibility of parallelizing and/or pipelining the exchange of these message to reduce the latency. This is important when handoff across different service domains. Figure 2 shows a simple protocol of the second approach (similar to the pull sequence in [5]). When a mobile node moves to a foreign domain, a mobile node sends a message containing both the Mobile IP registration request and the AAA request to the foreign agent (FA). The FA extracts the AAA request from the received message, forwards it to the local AAA server (i.e. AAAF) and waits for approval. To authenticate the foreign visitor, AAAF can either establish a security association with the mobile node's home AAA server (i.e. AAAH) or indirectly via an AAA broker. Once authenticated, the service access is enabled and FA forwards the Mobile IP registration request to HA. Note that the execution of AAA incurs extra delay to the handoff latency. For applications like VoIP [14], video streaming and TCP connections, it may disrupt the on-going communications if such latency becomes too large.

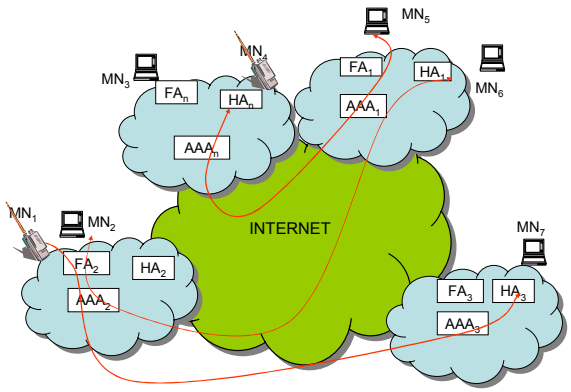

Figure 1. The Mobile-IP AAA Trust Model.

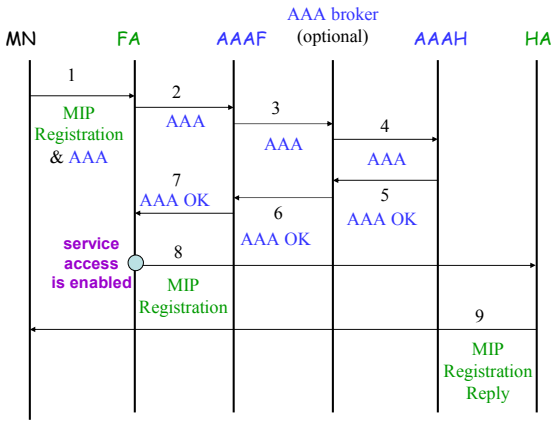

Figure 2. A simple AAA+Mobile IP protocol.

Although there are a number of researches on how to minimize handoff latency (such as [2][3][4]). Very few papers addressed the fast handoff problem in secure universal roaming service. In [7], a quasi-registration method is proposed which suggests a MN's AAAH to send service authorization message to not only the requesting AAAF also some candidate neighbors of AAAF to minimize the AAA-enabled handoff latency if MN roams to these neighbor domains. However, this paper did not describe any security mechanisms or details about how to avoid forgery users to access the service in these neighbor domains. Neither the paper describes how AAAH would know the identities or information about AAAF's neighbors and how rigorous the authentication and authorization process is conducted between them and MN. In [8], they consider AAA with QoS requirement. They do not address roaming across multiple administrative domains.

III. FORMING AN AAA-ENABLED ROAMING ALLIANCE

In this section, we present the architecture and the protocols to form an *AAA-enabled roaming alliance* to support *fast* and *secure universal roaming service.* An AAA-enabled roaming alliance is an association of service domains (or service operators) that agree to cooperate with one another to expedite AAA authentication/authorization to ensure non-interrupt service to mobile users. Each alliance member supports the

architecture as shown in Figure 1. They all support IP technology although individual physical networks may employ different networking technologies such as IEEE 802.11, GPRS, 3G and WiMAX. It is assumed that the AAA and mobile IP entities operating in a service domain are pre-configured to share administratively created security associations. Namely, HA and FA have established security relationships with their local AAA servers as part of the trust model in the AAA-enabled mobile IP architecture. The AAAF will dynamically establish security relationships with external authorities to check the credentials of mobile visitors and their authorized service level. The establishment of security association may use techniques such as IKE[9] and IPSec[10][11].

A roaming alliance is assumed to have a *master* domain, for example the creator of the alliance. The master domain is responsible for alliance membership management and the key management for the secure universal roaming service.

A. Join

Member domains join the alliance by invitation from the master domain. The join process consists of two phases. In phase one, the authorities (e.g. AAA servers) of the master domain and the invited service domain authenticate each other and agree upon the keys to be used to protect the alliance service-related key distribution between them. A simple three-way handshake protocol is used (as shown in Figure 3) by exchanging the RoamAllianceInvite(), RoamAllianceAccept() and RoamAllianceAck() messages. Then they determine the four keys: transmit and receive pairs of the keys for authentication and encryption between the two AAA authorities. Here we assume the Diffie-Hellman [16] key exchange algorithm is used. If the invited domain rejects the invitation, it will reply a RoamAllianceReject() message to the master domain.

In phase two, master domain distributes the *fast roaming authentication package* and the *alliance membership package* to the newly allied domain. The former is for the new domain AAA server to distribute it to its home service users to generate U-Mobile Token. The latter is to be used by the domain AAA server to authenticate mobile users from the other allied service domains.

B. Leave

When wishing to leave the alliance, a member domain sends a RoamAllianceLeave() message to the master domain which will confirm the request by replying a RoamAllianceLeaveConfirm() message.

IV. U-MOBILE TOKEN

In this section, we present the design of U-Mobile Token which is dynamically generated by mobile service users to receive secure universal roaming service. The benefits of the use of U-Mobile Token are two folds. First, a MN can conveniently access the subscribed service at areas or networks not owned and administered by its home domain. Second, the token is designed to enable rapid AAA check especially when roaming across multiple service domains to minimize the secure handoff latency so to avoid undesirable disruption to any on-going communications.

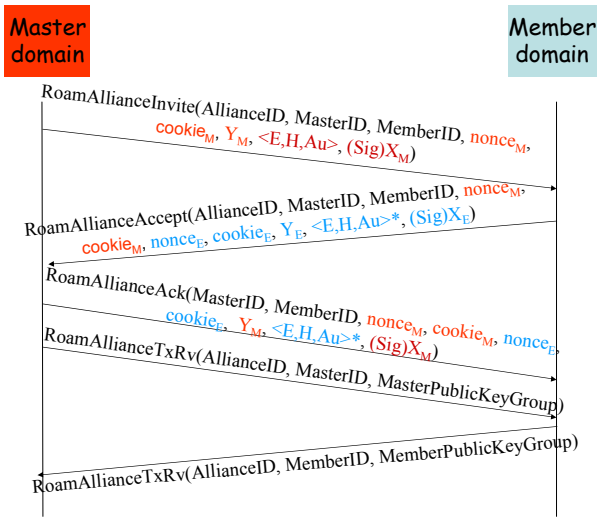

Figure 3 The three-way handshake protocol in phase one member join process

A. Design Goals

A MN subscribes the universal roaming service from a home service domain. At the subscription time, the MN will receive a fast roaming authentication package from its home AAA for the generation and management of *U-Mobile Token*. Since a wireless network is basically an open communication channel, strong authentication of mobile nodes is necessary. Under the AAA roaming architecture, a MN wishing to attach to a foreign network sends a U-Mobile Token to AAAF. For AAAF, the inspection of the U-Mobile Token should include the following three tasks:

- *authentication of the issuing party* - AAAF must check whether the received U-Mobile Token is genuine and issued by the claimed home domain.
- *authentication of whether the token holder is truly the claimed user* so that when AAAF issues a billing statement to the user (or user's AAAH), user cannot deny the use of the service;
- *integrity check* - The content of the U-Mobile Token is not modified en route.

In the meantime, the U-Mobile token shall also serve the purpose of, from the mobile node's perspective, authenticating the AAAF as a legitimate alliance member to further inspect the content of the U-Mobile Token and charge the service usage at the foreign network accordingly. These checks are necessary and important between mutually un-trusted sender (mobile user), receiver (foreign AAA) and token issuer (home domain and alliance master domain) in mobile-commerce for the purpose of service charging and billing. The service record must be undeniable and of no repudiation.

To achieve these goals, two security mechanisms are proposed: *alliance key pair* and *alliance service key*.

B. Alliance Key Pair

The alliance key pair consists of a public key and a private key denoted as $Y_{alliance}$ and $X_{alliance}$. Upon joining the alliance, a member domain will receive a *membership authentication*

package from the alliance master which contains an alliance public key $Y_{alliance}$ and two Diffie-Hellman algorithm parameters: q (a very large prime number) and α (a primitive root of q). The *alliance private key* $X_{alliance}$ is held by mobile service user. When a mobile user roams to a service domain (home or foreign), the AAA server and mobile node will follow a *distributed alliance service key generation protocol* to dynamically generate an *alliance service key* - a shared secret key based on the Diffie-Hellman algorithm for U-Mobile Token encryption.

The master domain is responsible for the generation of the alliance key pair according to the following equation:

$$Y_{alliance} = \alpha^{X_{alliance}} \quad (1)$$

It is also responsible for rekeying after member join and leave. Each member AAAH will periodically receive a new alliance key pair for each service period. The methods such as periodic batch rekeying method[12] can be used for alliance key pair management.

C. *Alliance Service Key*

Each mobile service user will be given a fast roaming authentication package upon service subscription time. The package contains an alliance private key $X_{Alliance}$ and the two Diffie-Hellman algorithm parameters: q and α the same as those in the alliance membership package. To secure the exchange of U-Mobile Token and for timeliness control, a *shared alliance service key* is devised *between MN and AAA server (AAAF* and *AAAH)*. Alliance service key is dynamically generated by the two parties according to the following *distributed key generation protocol*. Per universal roaming service period, AAA server determines a random integer X_{AAA} as its private key and sends its public key denoted as Y_{AAA} in the route advertisement message. It then computes the alliance service key for the current service period as follows:

$$K_{allianceSvcKey} = (Y_{alliance})^{X_{AAA}} \bmod q \quad (2)$$

When received the route advertisement message, a MN computes the *current* alliance service key according to the following equation:

$$K_{allianceSvcKey} = (Y_{AAA})^{X_{alliance}} \bmod q \quad (3)$$

In this method, the shared alliance service key is never transported on the network for security. The advantages include the alliance service keys are updated and generated periodically by local AAA servers and mobile nodes (no master domain is involved); and there is no need to store alliance service keys for a long period of time for timeliness to prevent replay attack. Moreover, each service domain (even individual network segment of a service domain) may use different alliance service keys for better security control.

D. *Content Design*

To achieve the goals of "fast" and "secure" roaming authentication across multiple service domains of an alliance, the information necessary to carry in the U-Mobile Token is designed as follows:

U-Mobile Token = (roamAllianceID, Y_{AAA}, homeDomainID, nounce, {userID, serviceClass, homeDomainID, $\{userID\}_{homeDomainKey}$, {serviceClass, serviceLifeTime, alliancePrivateKey, allianceSvcIndex$\}_{usrPrivateKey}\}_{allianceSvcKey}$)

The roamAllianceID is the identifier of the universal roaming service alliance with which the MN's home domain has a membership. The public key (Y_{AAA}) sent by FA/HA in the route advertisement message is repeated here for timeliness control. The homeDomainID is the identifier of the MN's AAAH. The rest of the data is encrypted by the *alliance service key* generated according to the protocol in Section III.C. The purposes are three-fold. First, if AAAF/AAAH can decrypt and read the content, it simultaneously authenticates AAAF/AAAH and mobile node as a legitimate member domain and a legitimate service user. Second, the information encrypted in this data block is secure because non-allied members cannot read the content. Last, both AAAF/AAAH and MN are synchronized in terms of having the keys of the same current alliance key pair. In the case that the AAAF's (AAAH's) decryption of U-Mobile Token fails, the AAA server will forward the token to AAAH requesting for alliance private key update. The updated information from AAAH will be relayed back to the MN which can then re-compute shared alliance service key and re-issue the U-Mobile Token.

In this encrypted block, it contains *three* sets of data (*info4AAA, info4AAAH* and *info4Update)* related to the service. The first three fields are for AAA server's authentication of the user's access to the service (referred to as *info4AAAF*). The requested service class can be such as the gold, silver and bronze as defined in the DiffServ or detailed QoS requirements of the service user. The protected home domain id is for AAAF to forward the AAA messages. The second set of data (referred to as *info4AAAH*) is intended to forward to AAAH for token holder's identity validation, thus encrypted by AAAH's homeDomainKey. The third set of data (referred to as *info4Update*) contains four important service parameters which are intended to be forwarded to AAAH as well for information update. It is encrypted by using mobile node's private key. We assume a home AAA has access to the public keys of its service users. The allianceSvcIndex and alliancePrivateKey are the current service period index and the key used when the U-Mobile Token was sent.

V. FAST ROAMING AUTHENTICATION

The service provision to and security check of a mobile user under the proposed fast and secure universal roaming service are conducted in two stages. Decrypting a received U-Mobile Token constitutes the stage-one security check. If passed, AAA server will temporarily grant MN the requested service to keep minimal handoff latency to assure on-going communication sessions are not disrupted in handoff. While the service has started, the AAA server will continue to perform stage-two security check by sending a *service authorization request* message to MN's AAAH according to *info4AAAF*. If the authorization request is confirmed by AAAH, the service to MN will continue. Otherwise, the service will be terminated immediately. Figure 4 shows the time step diagram of the proposed scheme. The timer intervals denoted as T_a and T_b refer to the stage-one and stage-two authentication. While the

former achieves faster security check, the latter keeps up rigorous security check.

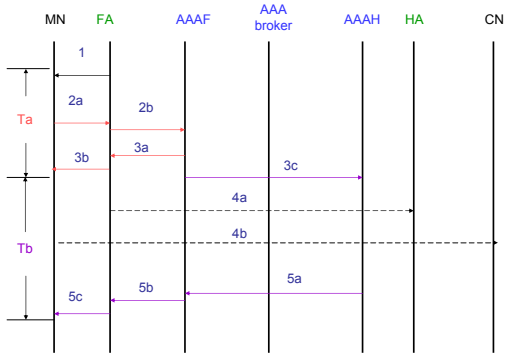

Figure 4. The protocol of the proposed fast and secure AAA-enabled Mobile IP procedure when a mobile user roams to a foreign service domain.

Message 1: FA sends a route advertisement message including Y_{AAA}.
Message 2a: MN sends a message including Mobile IP registration and U-Mobile token which is encrypted by alliance service key.
Message 2b: FA forwards U-Mobile Token and forwarded it to sends the U-Mobile token to AAAF.
Message 3a: AAAF sends stage-one service authorization confirmation to FA to granting mobile user temporary service access.
Message 3b: FA replies MN a temporary service authorization.
Message 3c: AAAF sends service authorization request message to AAAH.
Message 4a: FA forwards MN's Mobile IP registration to HA.
Message 4b: MN sends a Binding Update message to CN.
Message 5a: AAAH replies a service authorization confirmation/failure message to AAAF.
Message 5b: Depending on the service authorization result, AAAF notifies FA to either continue or terminate the service to the MN.
Message 5c: AAAF forwards the service authorization result including the information update from AAAH to MN.

A. *Service Data Record (SDR)*

In the *service authorization request message* to AAAH, in addition to the *info4AAAH* and *info4Update* excerpted from the U-Mobile Token, AAAF also includes its own identity and information such as a service instance identifier for complete authentication of the mobile user and authorization of the requested service. If authorization is granted, a *service authorization confirmation message* is sent back to AAAF. The AAAF will then notify its service equipment to continue the provisioning of the service to MN. Otherwise, a *service authorization failure message* is returned and the service will be terminated immediately.

The purpose of having AAAH-encrypted *info4AAH* and MN-encrypted *info4Update* are to be used as a secure proof of the service instance by MN at AAAF's service domain. Because throughput the entire course of the authentication and authorization of universal roaming service, these data are secure. No one except the home domain and the mobile node can produce, decrypt and modify the contents. As a result, the authorization confirmation will be used by both AAAF and AAAH as the *service data record* (SDR) for the service charging and billing of the home domain/mobile user.

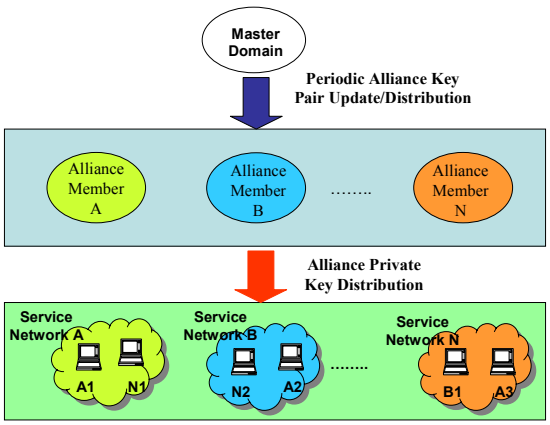

Figure 5. The alliance key pair update and distribution structure.

B. *Universal Roaming Service Management*

Info4AAAH and *infor4Update* are stored in the MN's fast roaming authentication package which were originally initialized by the home AAA server at the MN's service subscription time. When received a service authorization request message, AAAH will first decrypt *Info4AAAH* to obtain user id and checks if MN is still a valid service user. If so, it then uses MN's public key to decrypt *Info4Update* and updates the content of *Info4Update* with the current alliance private key, the associated service period index and the MN's service life time and service class. Here we assume when a service user subscribes the service, the value of ServieLifeTime is set to a very large number (equivalent to infinite). In the case that between two service confirmation instances the user's service subscription has been terminated, AAAH will set the ServieLifeTime to zero.

The updated *info4Update* is re-encrypted by using the MN's public key and included in the reply message (confirmation or failure) to return to MN. When received the update data, if serviceLifeTime is set to zero, the fast roaming authentication package of MN will destroy itself so that the service user will no longer be able to use the service. Otherwise, the package will update the local parameters accordingly.

C. *Distribution of Alliance Private Key to Mobile Nodes*

Besides the above mentioned update scenario when a mobile user issues a U-Mobile Token for service access, we still need a method to update mobile users (possibly a very large population dispersed in a very large geographic area) the new alliance private key periodically? The issues raised are not only scalability of user population, also how to locate them. There are possibilities that some users may turn off their service equipment while the home AAA is conducting the update process. The others may be in the middle of the AAA service. In the design of alliance key pair management, it is important to make sure there is no blind service period during the rekeying distribution process over a distributed environment.

The alliance key pair management is similar to group key management in terms of sharing keys among a group of users[12][13] but with higher complexity. In the universal roaming service model, three parties are involved: the master domain, member domains and mobile users. Figure 5 shows the

relationship between them. The update or rekeying interval of the alliance key pair is a design parameter between the key update/distribution overheads and the degree of forward access control vulnerability. The forward access control refers to after a member leaves, it will not be able to access future communications. Here we assume the rekeying interval is the same as the service period.

In a distributed environment, it is very difficult to achieve exact synchronization of information distribution. Here, three methods are taken to synchronize the alliance key pair used by AAA server and mobile node in generating shared alliance service key. First, when a mobile user makes a first-attempt to associate to an allied network (either home or foreign) (e.g., power on the mobile equipment, "log-in" the service on a laptop, etc.), it will use the local values to generate U-Mobile Token. As described in the stage-one authentication procedure, if the MN's alliance private key is out of date, AAAF will not be able to decrypt the token. Instead, it will forward the token to MN's AAAH for update. After receiving the updated information, MN can re-submit the U-Mobile Token. Second, after "logging-in" the service, the MN's fast roaming authentication package will periodically send an alliance private key update request to AAAH at the time interval aligned with the service period. Such update can be done some time right before the expiration of the service period (e.g., 1/3 of service period). Third, considering that a handoff may take place right during the period across two service periods, we introduce the notion of validation window. An AAA server will keep a window of the valid alliance key pair. We assume the window size is two. An AAAF will honor the U-Mobile Token encrypted by using either the current or the previous alliance key. It is assumed that the package residing in the MN's equipment is secure such that the mobile user has no access to the fast roaming authentication key, thus it cannot modify the content of the U-Mobile Token such as forging a user or home domain ID.

VI. CONCLUSIONS

In this paper, we first propose a service model called *universal roaming service* in which mobile users belonging to different service operators can fast and securely access needed resources provided by foreign service domains as they move without being constrained to a single spot or being forced to disconnect because his/her service provider does not have entire coverage of the city/region. We then propose the architecture and the protocols to form an AAA-enabled roaming alliance to allow different service operators to cooperate with one another to expedite AAA authentication/authorization to ensure non-interrupt service to mobile users. The supporting security protocols and algorithms including the generation and management of the alliance key pair and the alliance service key for U-Mobile Token are described. Our design of U-Mobile Token successfully achieves the authentication of the issuing party and the holder as well as the integrity of U-Mobile Token by AAA servers (AAAF and AAAH), and the authentication of AAA server as a legitimate service authority by mobile node. The schemes support undeniable and of no repudiation service data records for service charging and billing. This is necessary and important between mutually un-trusted mobile user, foreign AAA and token issuer (home domain and alliance master domain) in mobile-commerce. Moreover, the U-Mobile Token is so designed to facilitate two-stage security check for not only rapid service provision to mobile user with minimal handoff latency, also with strong, rigorous service authentication and authorization.

Our design of the fast and secure universal roaming capability to mobile users which we believe is an essential feature both to provide users good service usage experience and to make the service successfully. This is fundamental and key to the success of mobile business and mobile commerce.

REFERENCES

[1] C. Perkins, "IP Mobility Support", RFC 2002, 1996.
[2] R. Ramjee, T. L. Porta. S. Thuel, and K. Varadhan, "IP micro-mobility support using HAWAII," Draft-ramjee-micro-mobility-hawaii-00.txt, Feb. 1999.
[3] Valko, A. Campbell, and J. Comez., "Cellular IP". Draft-valko-cellularip-00.txt, Nov. 1998
[4] Charles E. Perkins and Kuang-Yeh Wang. "Optimized Smooth Handoffs in Mobile IP," Proceedings of the Fourth IEEE Symposium on Computers and Communications, July 1999.
[5] RFC 2904 ,"AAA Authorization Framework," 2000.
[6] RFC 2905, "AAA Authorization Application Example," 2000.
[7] Ted "Takeyoung" Kwon, Mario Gerla. An IP-level Mobility Management Based on Quasi-Registration in Wireless Technologies Convergence, World Wireless Congress 2002
[8] Torsten Braun, Li Ru ,Funther Stattenberger, "An AAA Architecture Extension for Providing Differentiated Services to Mobile IP Users," ISCC 2001
[9] Internet Key Exchange, RFC 2409,1998
[10] IP Encapsulated Security Payload (ESP),RFC 2406,1998
[11] IP Authentication Header (AH), RFC 2402,1998
[12] Y. Richard Yang, X. Steve Li, X. Brian Zhang and Simon S. Lam, "Reliable Group Rekeying: A Performance Analysis," ACM SIGCOMM, pp. 27-38, 2001.
[13] Yan Sun and K.J. Ray Liu, Scalable Hierarchical Access Control in Secure Group Communications, IEEE INFOCOM 2004
[14] Thomas J. Kostas, et al," Real-Time Voice Over Packet-Switched Networks," IEEE Network Magazine Jan/Feb 1998
[15] B. Aboba, J. Wood.,"Authentication, Authorization and Accounting (AAA) Transport Profile." RFC3539, 2003
[16] W. Diffie and M.E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory* **22** (1976)," 644-654.