Seamless and Secure Mobility Management with Location-Aware Service (LAS) Broker for Future Mobile Interworking Networks

Minsoo Lee, Gwanyeon Kim, and Sehyun Park

Abstract: **The proliferation of wireless local area networks (WLANs) offering high data rate in hot spot area have spurred the demand for possible WLANs and third-generation (3G) cellular network integration solutions as the initiative step towards 4G systems. This paper provides a novel architecture for seamless location-aware integration of WLANs into 3G cellular networks and also an analysis for the efficient handover techniques. We introduce location as a key context in secure roaming mechanism for context-aware interworking in 4G systems. The fast secure roaming with location-aware authentication is implemented at an entity called *location-aware service (LAS) broker* that utilizes the concepts of direction of user and *pre-warming zone*. The location-aware interworking architecture supports seamless roaming services among heterogeneous wireless networks including WLANs, wireless metropolitan area networks (WMANs), and 3G cellular networks. This paper also includes a description of procedures needed to implement efficient mobility and location management. We show how the LAS broker with pre-warming and context transfer can obtain significant lower latency in the vertical handover.**

Index Terms: **4G, interworking, location-awareness, mobility management, security, ubiquitous computing.**

I. INTRODUCTION

Context-aware computing refers to the special capability of an information system to sense and react to dynamic environments and activities. Perhaps the most critical aspects of context are location and identity. With numerous factors driving deployments of sensing and networking technologies, *location-aware computing* may soon become a part of everyday life with location-based services (LBS) like asset tracking, environmental resource discovery and control, and electronic tourist guides [1], [2]. Location-aware computing is made possible by the location sensing, wireless communication, and mobile computing systems. In order to provide the location-aware service (LAS) anywhere, anytime, these technologies in third-generation (3G) systems should be improved considerably toward beyond 3G (B3G) and fourth-generation (4G) systems.

4G systems are expected to converge into a heterogeneous, all-IP based system, which includes different wireless access networks such as wireless personal area networks (WPANs), wireless local area networks (WLANs), and 3G mobile networks like universal mobile telecommunications system (UMTS) and CDMA2000. As the first step toward to 4G systems, complementary features between 3G mobile networks with wide coverage and WLANs with high data rates have spurred the demand for 3G/WLAN interworking systems.

Coping with the ever-increasing demand from high-speed data applications at least in hot spot and indoor environments, this initiative is becoming so attractive that many people believe that it will ultimately result in 4G. systems. At the same time, such integration will ultimately reduce the cost and provide service affordability to mobile data users.

However, integrating multiple subsystems into 4G systems brings about many challenges. In the 3G/WLAN interworking, the problem of location-aware efficient resource management has not been considered adequately in respect of reducing secure handover signaling as well as satisfying the QoS guarantees. In order to provide intelligent services, we need smart techniques for location management of a mobile node (MN).

There is also a lack of a clearly defined framework to create innovative security services with location information. Many previous works on context-aware support for mobility have not emphasized heavily on security, which is very crucial since we are dealing with the interworking and roaming between heterogeneous networks. There are few safeguards on location privacy and security as in our previous work [3]. In fact, the demand for improved public safety is pushing regulation in the opposite direction [4]. Without these core functionalities such as mobility management, security, user authentication, and QoS guarantee, a seamless interworking between the two systems would not be feasible.

A study on the 3G/WLAN interworking [5] with six scenarios was conducted by the 3rd generation partnership project (3GPP). However, the study does not deal with efficient mobility and security management techniques that are indispensable features for 4G system. Based on [5]–[7], we identified location-aware security service requirements and functionalities in 3G/WLAN interworking in Table 1.

Scenario 3 allows a customer to access 3G packet-switched (PS) services over WLAN. Scenario 4 is an extension of scenario 3 with more enhanced mobility management. Scenario 4 allows a customer to change access between 3G and WLAN networks during a service session. QoS is a critical issue for service continuity.

Scenario 3 features should be essential for the first stage de-

Manuscript received February 15, 2005.

A preliminary version of this paper was appeared in part in Proceedings of Networking 2005, May 2005.

The authors are with the School of Electrical and Electronics Engineering, Chung-Ang University, 156-756, Seoul, Korea, email: {lemins, cityhero}@wm.cau.ac.kr, shpark@cau.ac.kr.

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the Chung-Ang University HNRC (Home Network Research Center)-ITRC support program supervised by the IITA (Institute of Information Technology Assessment).

Table 1. 3G/WLAN interworking requirements with location-aware services.

Scenarios	Characteristics	Requirements	Related functions
1 (Loose coupling)	Common billing and customer care	- Common billing	- Network discovery and selection - Common billing functions
2 (Loose coupling)	3G-based access control 3G-based access charging	- AAA for 3G subscribers in a WLAN - IP connectivity via WLAN for 3G subscribers - Multimode 3G/WLAN UE	- Network selection with network address identifier (NAI) - AAA proxy - RADIUS-diameter interworking function - Authentication with EAP-AKA and EAP-SIM
3 (Loose coupling)	Access to 3G PS-based services	- User data traffic needs to be routed to the 3G home or visited PLMN - Location-aware service (LAS) via 3G and WLAN	- User data traffic management with packet data gateway (PDG) and wireless access gateway (WAG) - Short messaging service (SMS), IP multimedia (core network) subsystem (IMS), multimedia message service (MMS) - LAS platform and LAS broker to enforce location-aware authentication and roaming
4 (Tight coupling)	Access to 3G PS-based services with service continuity	- Service continuity for transitions between 3GPP systems and WLANs (do not include those that may be internal to the WLANs) - Changes of QoS - To allow transition of multiple sessions and services	- Session continuity - Location-aware vertical handover - Location-aware resource management - Policy-based location management to enforce location privacy with LAS policy authority - LAS using web services through Internet - LAS service continuity
5 (Very tight coupling)	Access to 3G PS-based services with seamless service continuity	- Seamless changes of service - Service change shall not be noticeable to the user	- Service continuity with fast vertical handover - QoS guarantees for LAS - Secure LAS platform with LAS broker
6 (Very tight coupling)	Access to 3G CS-based services with seamless mobility	- Seamless roaming for 3G PS-based service - CS-based service with WLAN	- Seamless service continuity - Transparent roaming - Seamless QoS guarantees for LAS - Secure LAS platform for heterogeneous networks

ployment and the Scenario 4 features may or may not be deployed in the long term commercial operation. In our paper, we focus on the Scenario 3 and 4 in order to have an overview of the real interworking possibilities over 3G and WLANs.

We propose location-aware secure interworking techniques and architectures that could meet their respective requirements. We discuss how security can be substantially improved through a new form of authentication based on the location-aware security architecture. In line with Denning [8], [9], we suggest location-aware authentication introducing *'location'* as a new element in a user authentication mechanism. Our design is based on supplementing well-known user authentication mechanisms with the knowledge about the context and location of the user.

Our location-aware authentication is a strong authentication method that can verify location of a MN when the MN pops up in a new cell and claims to be somebody who was located in a neighboring cell.

In particular, we propose and discuss efficient mobility management schemes with an agent called *location-aware service (LAS) broker* that can support consistent secure LAS provisioning. As an abstraction of location-aware security model, LAS broker includes location-aware authenticator for fast secure roaming using the concepts of the direction of the user and pre-warming zone. Performance evaluation is also presented to demonstrate the effectiveness of the proposed scheme minimizing the processing overhead in vertical handover.

The rest of this paper is organized as follow. Section II gives related works about location-aware computing in future wireless networks. Section III identifies the problems and requirements of location-aware security in 3G/WLAN interworking. In Section IV we propose location-aware authentication for fast roaming with LAS broker. Section V suggests our location-aware security architecture for 3G/WLAN interworking systems. In Section VI, we discuss evaluation of our location-aware secure roaming. Finally, we conclude in Section VII.

II. RELATED WORKS

Toward seamless secure services in the future mobile interworking networks, fundamental features such as smooth roaming and interworking techniques, QoS guarantee, data security, user authentication, and authorization are required. For smooth roaming, several studies have been made on a fast handover management in IPv6 networks [10] and an integrated management that combines the strengths of mobile IP location registers (MIP-LR) and session initiation protocol (SIP) [11]. As solutions for integrating 3G and WLAN services, some of the recent studies have focused on a gateway [6], interworking techniques and architectures [7], or a roaming and authentication service framework [12].

For adaptive QoS management, the location information will play a vital role in defining context-awareness. Intuitively, it is clear that successful location prediction can lead to fully automated activation of handovers. The mobile motion prediction (MMP) algorithm [13] makes use of the user's movement history. The hierarchical position prediction (HPP) algorithm [14] makes use of location history in addition to the instantaneous measurements of surrounding cells. The profile based next-cell prediction algorithm [15] predicts based on a location classification and a user movement history. Recently, the road topology based mobility predictions [16] and our directive service with the pre-warming scheme [17] can achieve dynamic resource reservation for cellular networks.

In the vision of 4G systems, location information will be available from various types of network [18]. Therefore, the enhancement of these location-based schemes will enable further advances towards location-aware computing and the pursuit of perfect context awareness for the future 4G systems. The main evolutions are the migration of legacy LBS toward LAS, the introduction of the location-awareness in applications. LAS makes adaptively and autonomously modifying the services in heterogeneous wireless networks. According to the development of the networking technologies and the increase of the accuracy of the positioning technologies [19], many LAS with efficiency and reliability will appear.

Furthermore, as the future mobile devices are likely equipped with more accurate positioning capability, location privacy is going to become increasingly important in a world where LBS are available over larger geographical areas [20]–[23]. For location security and privacy, there were frameworks with a cryptographic approach of an authorized-anonymous-ID-based scheme [20] and algorithms for location discloser-control [21] and based on frequently changing pseudonyms [22].

However, in the 3G/WLAN interworking the problem of location-aware efficient resource management has not been considered adequately in respect of reducing secure handover signaling as well as satisfying the QoS guarantees.

As reconfigurable and adaptable features are needed in the B3G and 4G systems there are challenging issues with regard to location-aware seamless secure roaming. This paper concentrates mainly on the location-aware schemes with LAS broker and context transfer technologies to enforce security for seamless interworking in 4G systems.

III. MOTIVATIONS AND REQUIREMENTS

A. *Requirements for Future Mobile Interworking Networks*

In the vision of 4G mobile networks a MN should be able to connect the best wireless networks among ad-hoc, personal, wireless LANs, and 3G mobile networks in respect of location of the MN[18], [24].

However, the integration of these different networks generates new research challenges because of the heterogeneities of access technologies, network architectures, protocols, and various service demands of mobile users [25]. The following requirements should be considered to fulfill the promising services of the 3G/WLAN interworking.

* *Privacy and security*: 3G/WLAN interworking should not compromise the UMTS security architecture. Therefore, it is required that authentication and key distribution should be based on the UMTS authentication and key agreement (AKA) procedure and extensible authentication protocol (EAP)-AKA or EAP-SIM for WLAN [26], [27]. The interworking system should eliminate the invasion of privacy by unwanted disclosure and commercial use of location information [3], [4].
* *Global secure roaming*: MNs should be seamlessly served from foreign domain without any security leakage of user information from the interworking systems.
* *QoS guarantees*: The effectiveness of location-aware services depends not only on the user population but also on QoS guarantee in vertical handovers and roaming services.
  - Reduction of signaling overheads and latency of service delivery.
  - Maintain QoS guarantees in different mobile systems.
* *Handover management*: Handover latency is especially disruptive to real time applications, even if most of the reauthentication during the handover in different networks is not lost but delayed. In addition to the latency of handover at the physical and link layers, secure roaming could add significant latency.

To overcome the heterogeneities and to meet the requirements, a new common architecture with enhanced security, privacy and mobility management is indispensable to interconnect multiple access networks. The focus of this paper is trying to enforcing the location security with context-aware support for efficient mobility management in the seamless interworking among heterogeneous wireless networks.

B. *Location-Awareness for Seamless and Secure Services in Future Mobile Interworking Networks*

In the secure handover with the existing security mechanisms like AAA mechanisms with EAP based protocols (e.g., EAP-AKA [26] in UMTS, EAP-transport layer security (EAP-TLS) [28] in WLANs), the most of the authentication and key management procedures take place after the handover. When the user roams from one cell to another, he should gain or request authentication from the 3G AAA home server. This means that authentication efficiency should be significantly considered, since it is mainly involved in the latency quality of the intersystem handover procedure [29]. A large number of MNs would substantially increase the handover delay.

To minimize the signaling overhead, pre-authentication mechanisms that provide the exchange of authentication information in advance could be the one of possible solutions. As the security standard for WLAN, IEEE 802.11i [30] supports the pre-authentication.

However, the pre-authentication in 802.11i, which is carried out on layer 2, is sufficient only in the scenario of an intra-domain handover (horizontal handover). As the pre-authentication is carried out over the EAP over LAN (EAPOL) protocol, it can not be routed to another subnet. 802.11i pre-authentication does not define a solution for an inter-domain handover (vertical handover).

There is another critical issue about how to choose the best AP or cell for the next handover. Pre-authentication mechanisms for all neighboring APs or cells are undesirable in the view point of efficient resource management.

In order to provide the seamless vertical handovers, the location information can play a key role for the seamless services with mobility, security and QoS support. The location prediction enables the directive security services for consistent QoS guarantee throughout the interworking networks. We described the advantages of the location-awareness as shown Table 2 from the analysis of the challenges in 4G systems [31].

The main objective behind the scheme is simple: The location-aware mechanism reduces the expensive handover signaling to the minimal number of messages required by the existing security mechanisms as well as provides same level of security as full authentication.

To compensate the limitation of the existing AAA mechanisms, we designed LAS broker that acts as a "*location security proxy*" server. It expands local security capabilities to support the context transfer with pre-authentication so called pre-warming. Pre-warming means the exchange of authentication information in advance by tracking and predicting user's direc-

Table 2. Location-awareness for future mobile interworking networks.

Issues	Key challenges	Location-aware management with LAS broker
Service	- To provide seamless personal mobility to users without modifying the existing mobile systems. - Most of services use pre-defined due to the limited usage of dynamic context.	- Not pre-defined services but adaptive services and dynamic services according to change of the location of a MN. - Intelligent seamless services by knowledge of location information (direction, location prediction, track, map).
Resource management and QoS support.	- Resource management is limited to current network. - Mostly static, flat QoS support by user profile, network preferences. - Limited QoS guarantee in vertical handovers.	- Efficient resource reservation and QoS provisioning through heterogeneous networks by pre-warming. - By utilizing the integrated and interoperable location context through LAS brokers, location unaware applications (e.g., multimedia applications) can adaptively change the services with enhanced location-aware QoS guarantee (e.g., elastic buffering for a high speed MN).
Security and privacy	- The heterogeneity of wireless networks complicates the security issue. - Dynamic reconfigurable, adaptive, and lightweight security mechanisms should be developed.	- Carefully managed location information as an additional strong authentication as location-aware authentication. - Pre-established trust relationship between an old AP/BS and a new AP/BS before handover by accurate and fast AAA context transfer.
Interworking	- A lock of knowledge of different communication patterns, network coverage. - Limited scope of interworking management between homogeneous networks.	- Seamless interworking by pre-warming that predicts the best wireless networks for the next handovers. - Wide scope of interworking management among heterogeneous networks in consideration of differences in network coverage, location and moving directions of MNs.
Scalability	- When the user roams, he should gain or request authentication from the 3G AAA home server. - Authentication efficiency should be significantly considered. A large number of MNs would substantially increase the handover delay.	- More scalable by network of LAS brokers supporting load balancing of AAA servers. - LAS broker that acts as a location security proxy that expands local security capabilities supporting the more accurate and fast AAA context transfer with pre-warming.
Handover management	- New AP/BS for the next handover is decided by signal strength (reactive handover).	- Proactive handover to optimal new AP by location context. - Location-aware fast handover by pre-warming and context transfer.

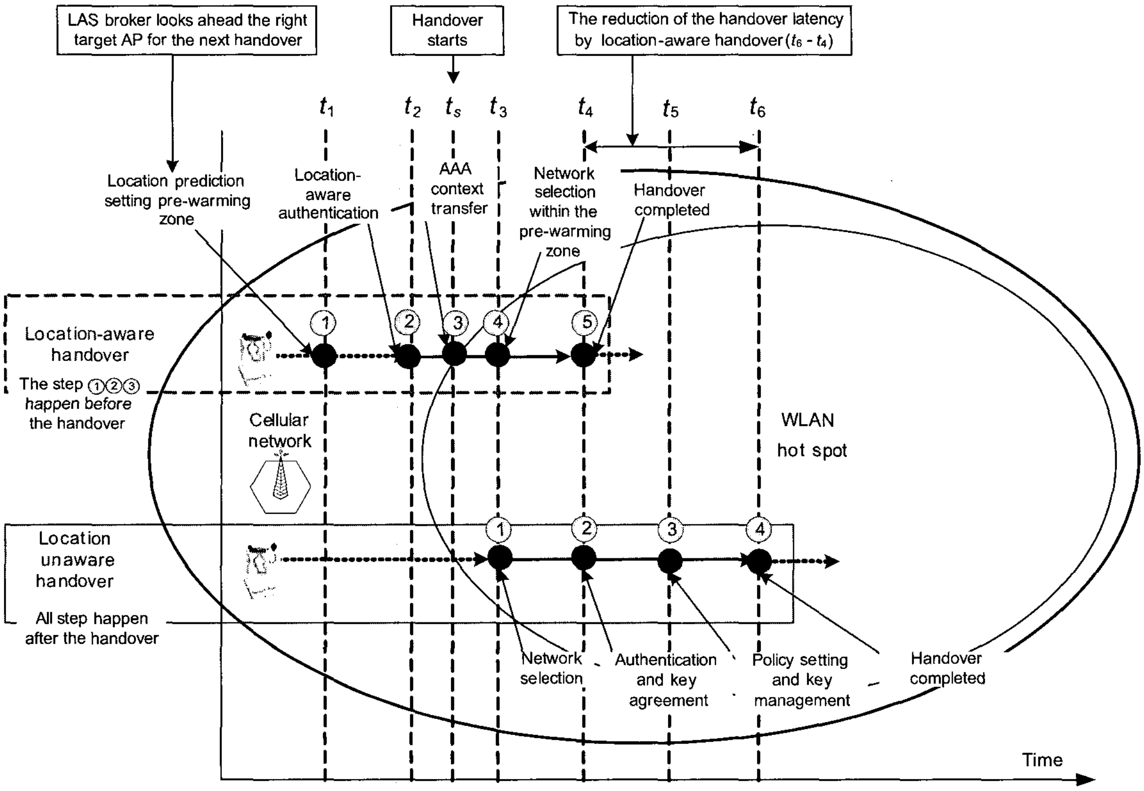

LAS broker looks ahead the right target AP for the next handover
Handover starts
The reduction of the handover latency by location-aware handover (t_6 - t_4)
t_1
t_2
t_s
t_3
t_4
t_5
t_6
Location prediction setting pre-warming zone
Location-aware authentication
AAA context transfer
Network selection within the pre-warming zone
Handover completed
Location-aware handover
The step ①②③ happen before the handover
①
②
③
④
⑤
Cellular network
WLAN hot spot
Location unaware handover
All step happen after the handover
①
②
③
④
Network selection
Authentication and key agreement
Policy setting and key management
Handover completed
Time

Fig. 1. Location-aware handover processing in mobile interworking networks.

tion. Pre-warming serves to determine possible new target cells to which the MN is likely to handover in the very near future. These mechanisms are also devised to maximize the probability of targeting the AP/BS to connect the best wireless networks (e.g., a network of higher data rates or wider bandwidth). Therefore, the right AP/BS for the next handover has the authentication information of the users. As the users don't have to gain each authentication from the 3G AAA servers for further handovers, these mechanisms avoid the additional reauthentication delay, thus improve handover performance and reduce the traffic load on the wireless backbone.

Fig. 1 describes the reduction of the signaling overhead in the vertical handover by pre-warming. In the case of the location-aware secure handover from UMTS to WLAN, LAS broker validates the location history of the user then sends authentication and key information like pairwise master key (PMK) to APs in the pre-warming zone in WLANs. Since there is no necessity to process full reauthentication, handover latency can be greatly

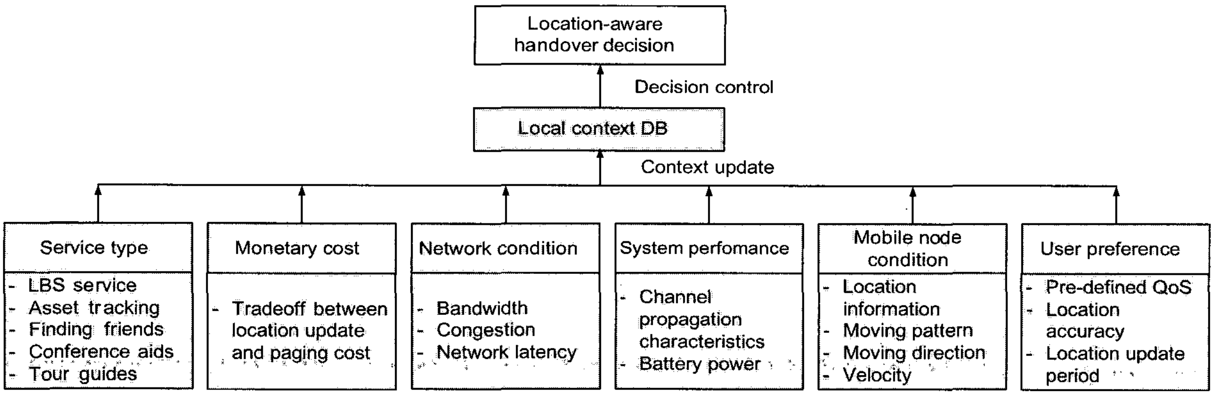


Fig. 2. The proposed context model for the location-aware handover decision.

decreased by performing only association and 4-way handshake (if necessary).

IV. LOCATION-AWARE SEAMLESS SECURE ROAMING WITH LAS BROKER

In this section, we discuss how mobility and security can be improved through new location-aware mechanisms with LAS broker for the future interworking networks.

A. *Location-Aware Handover with Pre-Warming Zone*

In order to provide location-aware seamless services at any time and anywhere, the terminal mobility is the key element in 3G/WLAN interworking systems. The terminal mobility allows a MN to roam across geographic boundaries of wireless networks. There are two main issues in terminal mobility: Location management and handover management.

We have identified contexts for location-aware handover in the consideration for the vertical handover [32] as in Fig. 2.

One of the difficulties in providing seamless roaming service is how to promptly and securely exchange security context during handover. Pre-warming may be helpful to simplify the authentication process during the handover to support seamless roaming service [33], [34]. For example, if the MN A in Fig. 3 is on the subway, it will obviously handover from AP1 to AP3. Therefore, the authentication information of the mobile station needs to be delivered from AP1 to AP3 correctly in advance for seamless roaming before the handover procedure.

Reasonably accurate prediction of the user movements during the handover can help to solve the problem of the seamless secure interworking. In case of the handover between WLANs, location prediction can decrease the total handover processing time with one RTT between the old and new APs.

A prediction of pre-warming zones is especially possible in track bounded wireless networks. Most of the cellular systems and LBS platforms have the interfaces for geographic information systems (GIS) providing tracking services. We designed LAS broker that has the interface for GIS to use the local map. In the case of the MN B, its pre-warming zones will include the areas around the subway station with areas along the track. In the case of the pedestrian C in Fig. 3, its path may be effectively predicted by the location history based algorithms [14] that has a record of the previous user movements and take into account the respective probability of movements together with factors such as the direction and the speed [35].

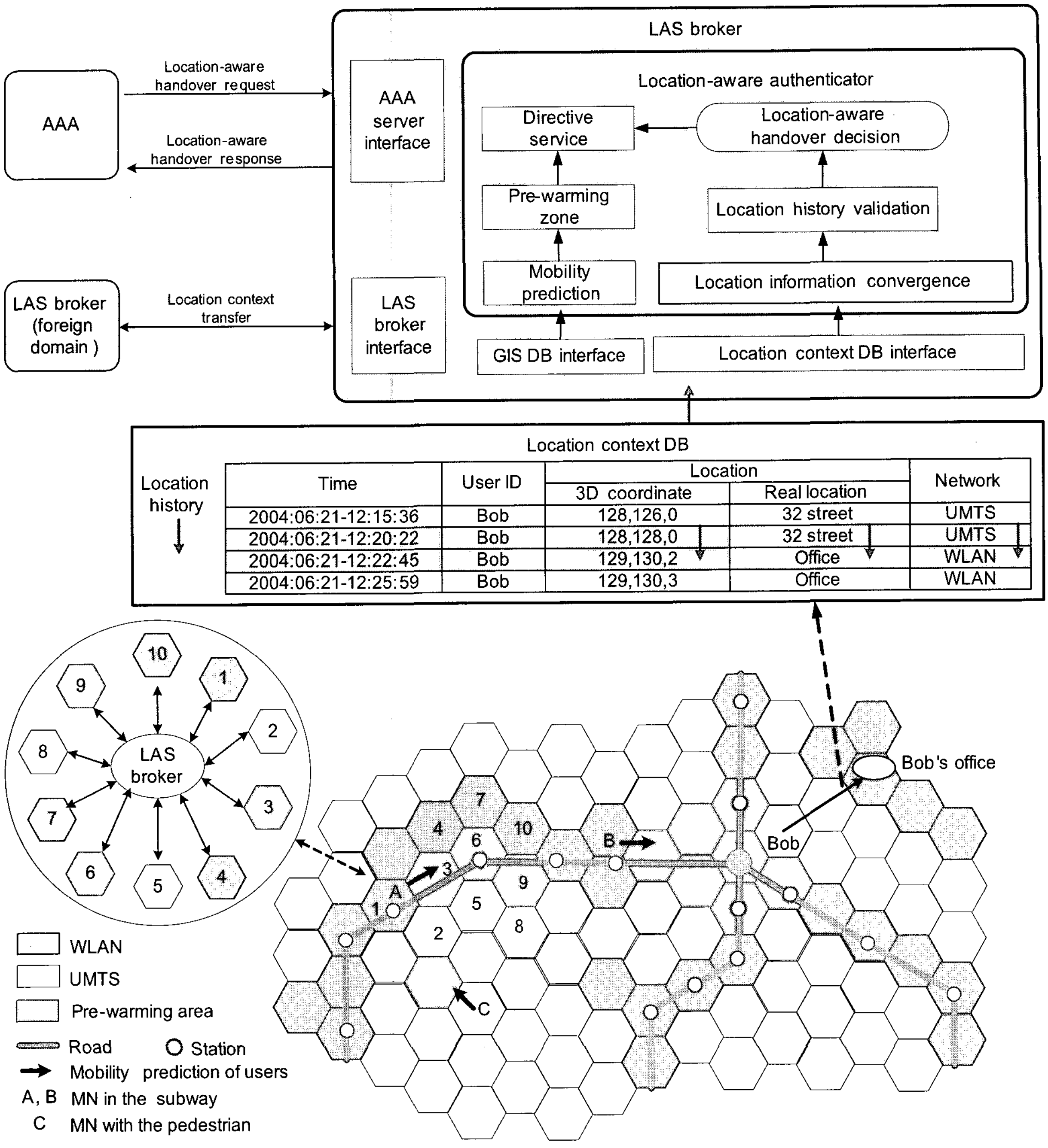
The concept of pre-warming zone can enhance the efficiency of roaming from gathering location data only in the paging areas. The pre-warming zones adaptively vary as the mobility of the MN changes.

B. *LAS Broker for Directive Security Service and Fast Handover*

For seamless roaming services, LAS broker includes a location-aware authenticator that verifies location history and maintains pre-warming zones. In our location-aware authentication, LAS broker verifies the location history of a MN when the MN pops up in a new cell and claims to be somebody who was located in a neighboring cell. Then, LAS broker predicts a user's direction in heterogeneous networks and it forms a pre-warming zone to pre-establish trust relationships with AAA for fast handover. During the handover location history of the user in 3G networks could enforce the location-aware authentication. If the MN A in Fig. 3 is on the subway, LAS broker decides APs within its pre-warming zone (3→ 6→9) and performs pre-authentication in advance for fast handover.

V. THE PROPOSED LOCATION-AWARE SECURE INTERWORKING ARCHITECTURE FOR 4G SYSTEMS

We designed the location-aware security architecture for 4G systems to meet the location-aware computing requirements in Section III. Fig. 4 shows the proposed interworking architecture. For location-aware fast vertical handover we deploy the LAS brokers with context transfer schemes in each network domain. LAS brokers AAA proxies and AAA servers play key role in enforcing location-aware security in the interworking system. LAS policy authority takes charge of location privacy policies for QoS guarantees. We will describe the basic functionalities of the components and we will show some practical scenarios in which location-aware fast roaming are provided while preserving user's location security and privacy.


LAS broker
AAA
Location-aware handover request
Location-aware handover response
AAA server interface
Location-aware authenticator
Directive service
Location-aware handover decision
Pre-warming zone
Location history validation
Mobility prediction
Location information convergence
LAS broker (foreign domain)
Location context transfer
LAS broker interface
GIS DB interface
Location context DB interface
Location context DB
Location history
10
9
1
2
8
LAS broker
3
7
6
5
4
Bob's office
Bob
B
A
C
WLAN
UMTS
Pre-warming area
Road
Station
Mobility prediction of users
A, B MN in the subway
C MN with the pedestrian

Time	User ID	Location		Network
		3D coordinate	Real location	
2004:06:21-12:15:36	Bob	128,126,0	32 street	UMTS
2004:06:21-12:20:22	Bob	128,128,0	32 street	UMTS
2004:06:21-12:22:45	Bob	129,130,2	Office	WLAN
2004:06:21-12:25:59	Bob	129,130,3	Office	WLAN

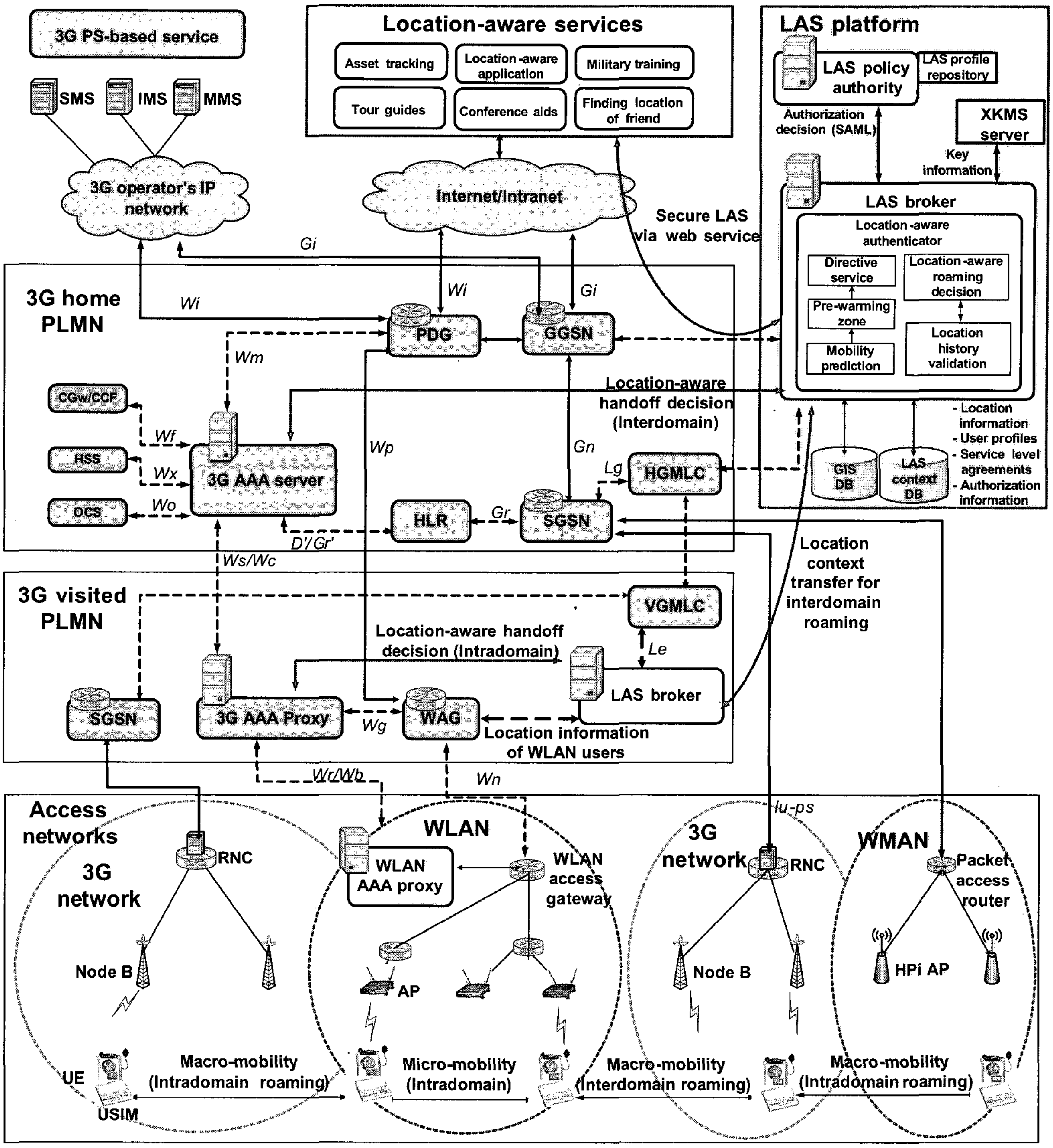
Fig. 3. Directive secure roaming services with LAS broker for future mobile interworking networks.

A. The Proposed Interworking System for Location-Aware Services over the Current Networks

Our architecture supports context-aware vertical handovers by the cooperation of various components. LAS broker performs the location-aware authentication with pre-warming. LAS policy authority gathers and manages profiles and policies as the result of service level agreement (SLA). AAA proxies are responsible for secure AAA information exchanges in executing handovers. Fig. 5 depicts a functional overview of these entities from the point of view of the location-aware architecture.

For satisfying the key requirements of 3G/WLAN interworking scenario 3 in Section I, the user data traffic in WLANs is routed to the 3G home public land mobile network (PLMN) or visited PLMN through a component called a packet data gateway (PDG) or a wireless access gateway (WAG), which is located in the preferred 3G visited PLMN. For several interfaces, *Wn*, *Wm*, *Wi*, *Wg*, and *Wp*, we adopt the notation and functionality specified in [36]. We have also considered the interworking of the wireless metropolitan area networks (WMANs) with IEEE 802.16 [37] and HPi (high-speed portable Internet).

In the 3G cellular networks, location services (LCS) is logically implemented on the gateway mobile location center (GMLC) or mobile location center (MLC) [38]. Location information may be communicated between GMLCs via the *Lr*



Wr/Wb: This interface carries AAA signaling between the WLAN and the 3G visited or home PLMN in a secure manner.
Ws/Wc: This interface provides the same functionality as Wr/Wb but runs between a 3G AAA proxy and a 3G AAA server.
Wn: This interface is used for transporting tunneled user data between the WLAN and the WAG.
Wx: This reference point provides communication between AAA infrastructure and HSS.
Wg: An AAA interface between the 3GPP AAA proxy and the WAG for provisioning of routing enforcement functions for authorized users.
Wo: This is used by a 3GPP AAA server to communicate with the online charging system (OCS) for charging information.
Wf: The interface between 3GPP AAA server and charging gateway function (CGF)/charging collection function (CCF) for charging.
Wi: Reference point between the packet data gateway and a packet data network (external public or private).
D'/Gr': This optional interface is used for exchanging subscription information between the 3G AAA server and the HLR.

Fig. 4. The proposed location-aware secure interworking architecture over the current networks for 4G systems (dashed lines: Signaling; solid lines: Data and signaling).

interface. LAS broker gets location history from the GMLC via *Le* interface. When MNs are using WLANs, location information is gathered via the additional dedicated interface between the WAG and the LAS broker. In the location-aware authentication procedure, LAS broker gets the location information from GMLC and WAG. Then, it validates the location history of a MN. Finally, it generates the location authentication response to an AAA server.

For business model agreements in 3G/WLAN interworking we assume that 3G operators set up dedicated roaming agree-

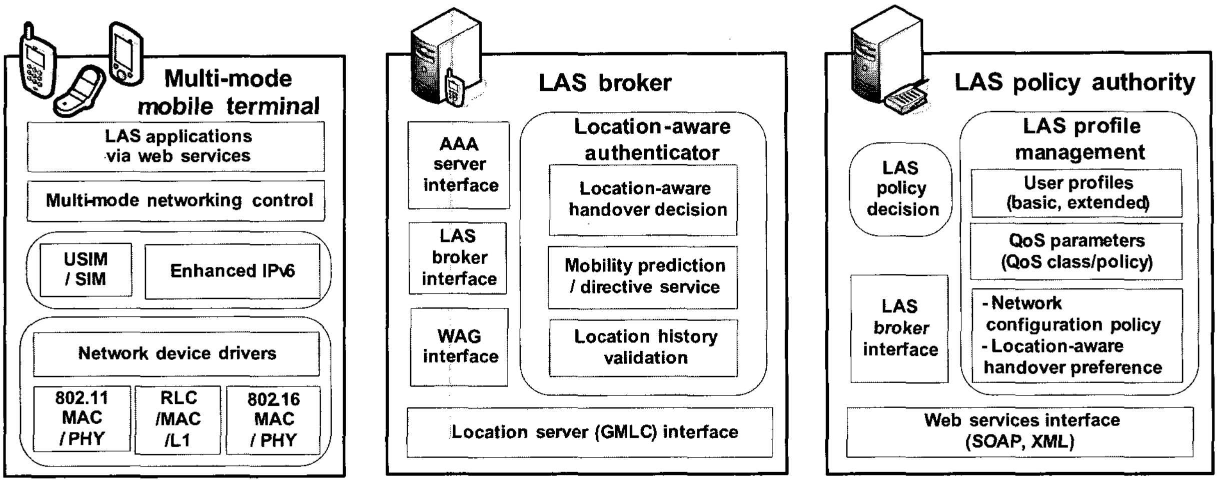

Multi-mode mobile terminal
LAS applications via web services
Multi-mode networking control
USIM / SIM
Enhanced IPv6
Network device drivers
802.11 MAC / PHY
RLC /MAC /L1
802.16 MAC / PHY
LAS broker
AAA server interface
LAS broker interface
WAG interface
Location-aware authenticator
Location-aware handover decision
Mobility prediction / directive service
Location history validation
Location server (GMLC) interface
LAS policy authority
LAS policy decision
LAS broker interface
LAS profile management
User profiles (basic, extended)
QoS parameters (QoS class/policy)
- Network configuration policy
- Location-aware handover preference
Web services interface (SOAP, XML)

Fig. 5. Components of the location-aware interworking architecture: The mobile terminal, LAS broker, and LAS policy authority.

ments with WLAN operators beforehand and UMTS operators allow WLANs to interwork.

The ownership of proposed LAS broker could be important since it allows location-aware authentication and fast roaming. As it is also responsible for hiding user location information to non-secure applications or services, the LAS broker must be an entity of particular trust. Acting as PDP with respect to the LAS broker (as PEP), the ownership and operation of LAS policy authority is also important.

We assume that home 3G operator takes the charge of owning and running the LAS broker. However, at the same time, this puts lots of power in the operator's hand. Third party service providers that would like to offer LBS to the end user might be blocked by operators that own the LAS broker. By such, monopolies (that already exist today) will be kept making it difficult for new players to enter the market.

According to the careful consideration with Korea Telecom Freetel (KTF) (the one of the most representative mobile communication companies in Korea), such ownership of LAS broker and LAS policy authority may be common in the initiative interworking systems. As the market grows, it may be desirable to establish the licensed location authority like the licensed certification authority (CA) in public key infrastructure (PKI). If LAS broker acts as a location authority, it would be easier for new services providers to enter the market.

B. LAS Broker as an Abstraction Model for Location-Aware Computing

As an abstraction for location-aware computing, we devise LAS broker with web services functionalities. LAS broker allows applications and users to be aware of their mobility. LAS broker can respond to queries on directions, distances, routes, and proximity. The existing LBS and other applications for wireless networks can exploit LAS broker for customizing their functionality with location-awareness. Due to possible separation of location-aware security with LBS, the LAS broker could act as a location security Proxy.

LAS broker also provides web services security specification like XML signature, XML encryption, and security assertion markup language (SAML) [39]. LAS policy authority creates SAML assertions as the service level agreements (SLAs) with a user. These assertions also include the location-aware handover preference which means the priority settings by the user for targeting the next handover in consideration of network bandwidth, data rates, velocity of the user, and other parameters in Fig. 2.

LAS broker plays key roles not only in location-aware authentication for fast roaming and but also in protecting user's privacy. LAS broker act as a policy enforcement point (PEP) that checks permission with the LAS policy authority, the policy decision point (PDP) by requesting SAML assertions before making decisions and releasing the secured location data to the LBS providers. LAS broker could provide users with the greatest amount of control over their personal information, since the users are in control to choose whether their location is transmitted to the LBS providers.

For scalable management of location-aware secure interworking architecture, implementation of LAS broker may be done centrally and in a distributed manner by cooperation of LAS brokers. Intradomain (micro-mobility) authentication, authorization, and accounting (AAA) are handled together with LAS broker and AAA server. When a MN moves into a foreign network for interdomain roaming (macro-mobility), LAS brokers, AAA proxies, and AAA servers take charge of reauthentication process.

To minimize the signaling overhead, AAA context transfer protocol is used for the fast secure roaming between the AAA proxy in visited PLMN and the AAA server in home PLMN. Location context is also exchanged between LAS brokers. In the absence of context transfer, there may be large delays because of the network signaling required to re-establish QoS flows to re-authenticate the mobile user [32]. The detailed protocols are discussed later (Section V-C).

C. AAA Context Transfer Signaling for Location-Aware Authentication and Roaming

To enforce the authenticity of MNs the location-aware authentication and secure roaming should be associated with AAA procedures [27]. The proposed location-aware secure roaming

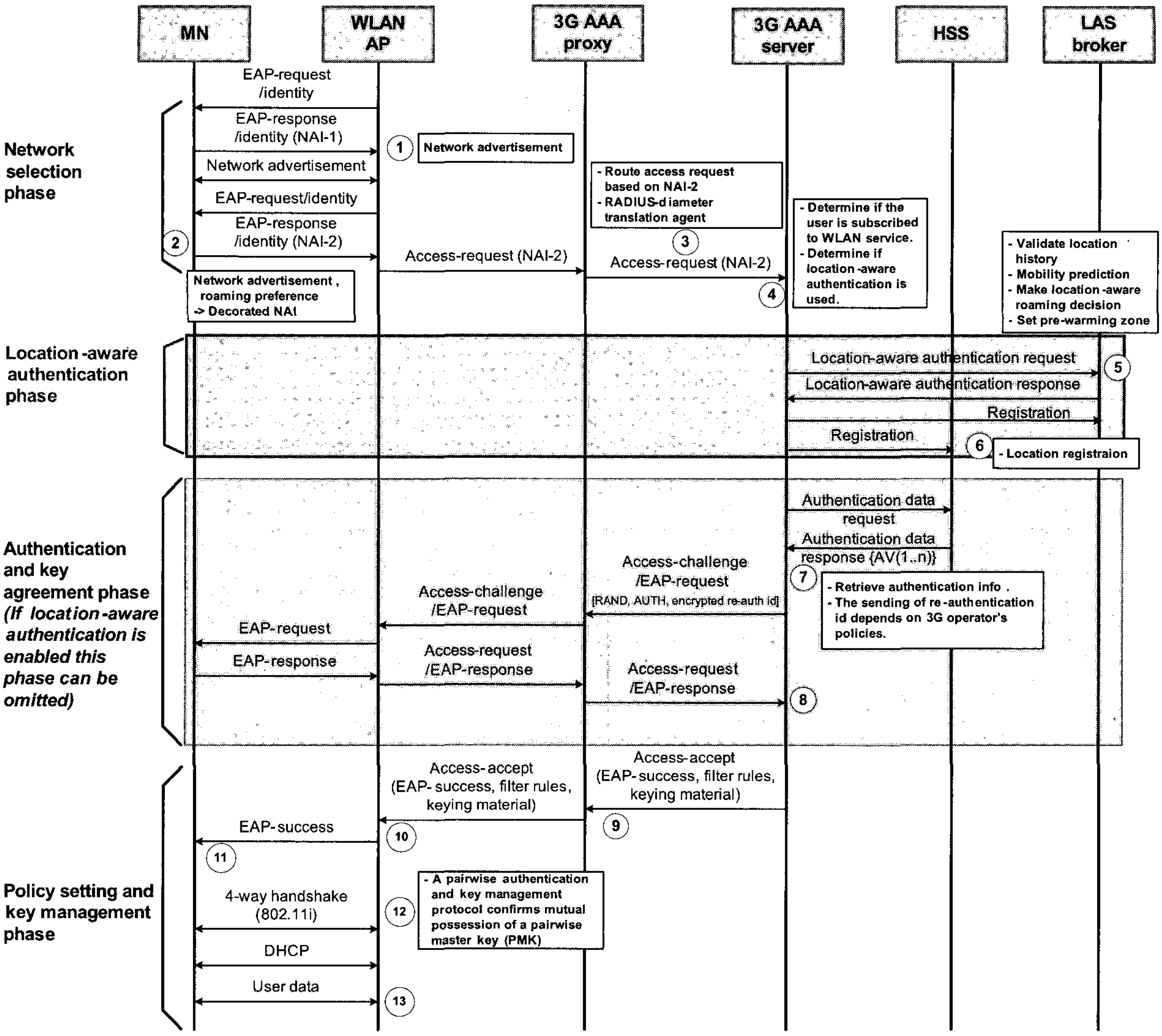

MN
WLAN AP
3G AAA proxy
3G AAA server
HSS
LAS broker
Network selection phase
EAP-request /identity
EAP-response /identity (NAI-1)
Network advertisement
EAP-request/identity
EAP-response /identity (NAI-2)
① Network advertisement
② Network advertisement, roaming preference -> Decorated NAI
Access-request (NAI-2)
- Route access request based on NAI-2
- RADIUS-diameter translation agent
③ Access-request (NAI-2)
④ - Determine if the user is subscribed to WLAN service.
- Determine if location-aware authentication is used.
- Validate location history
- Mobility prediction
- Make location-aware roaming decision
- Set pre-warming zone
Location-aware authentication phase
Location-aware authentication request ⑤
Location-aware authentication response
Registration
Registration
⑥ - Location registraion
Authentication and key agreement phase (If location-aware authentication is enabled this phase can be omitted)
Authentication data request
Authentication data response {AV(1..n)}
⑦ - Retrieve authentication info .
- The sending of re-authentication id depends on 3G operator's policies.
Access-challenge /EAP-request [RAND, AUTH, encrypted re-auth id]
Access-challenge /EAP-request
EAP-request
EAP-response
Access-request /EAP-response
Access-request /EAP-response ⑧
Policy setting and key management phase
Access-accept (EAP-success, filter rules, keying material)
Access-accept (EAP-success, filter rules, keying material)
⑨
EAP-success ⑩
⑪
4-way handshake (802.11i)
⑫ - A pairwise authentication and key management protocol confirms mutual possession of a pairwise master key (PMK)
DHCP
User data ⑬

Fig. 6. Location-aware secure roaming procedure from UMTS to WLAN.

procedure from UMTS to WLAN is depicted in Fig. 6. We employ the UMTS authentication and key agreement (AKA) procedure and EAP-AKA for WLANs.

Initially, a MN selects a 3G visited PLMN based on the network advertisement data and forms a second network address identifier (NAI-2) corresponding to this PLMN [7] (Step ①, ②). For business model agreements in 3G/WLAN interworking, we assume that UMTS operators and WLAN operators set up dedicated roaming agreements beforehand and UMTS operators allow WLANs to interwork.

The WLAN routes the AAA message to the 3G AAA server or 3G AAA proxy based on the NAI and the access authentication is performed (Step ③). In the case of the 3G, AAA server uses location-aware authentication during the handover, it sends a location authentication request to LAS broker (Step ④). When the LAS broker authenticates to the user successfully, it sends a location authentication response to the 3G AAA server (Step ⑤) and it registers the location of the user (Step ⑥). If the 3G AAA server doesn't use the location-aware authentication method, it will perform authentication and key agreement phase based on EAP-AKA again (Steps ⑦ and ⑧). As the 3G AAA authenticates to the UE successfully, it sends EAP-success message with keying material and some filter rules (Steps ⑨–⑫). Finally, the user data traffic is routed based on the routing policy of the WLAN and policed by the filter rules defined by the 3G home and visited PLMNs (Step ⑬).

Other open research issues for 4G systems include a framework for reducing the intersystem signaling and authentication. To reduce the large delays in the roaming we designed the context transfer protocol with location-aware authentication and Fig. 7 shows the procedure.

As the MN moves from its previous access router to the new access router, the location-aware authentication and AAA information about each of the MN is forwarded between the LAS brokers and AAA servers, respectively. We devised the reactive context transfer in which a new access router explicitly requests the MN's context information as the part of the location-aware secure handover. *Location-aware authentication phase* starts before the *network selection phase*. LAS broker generates the location authentication response before handover. Therefore

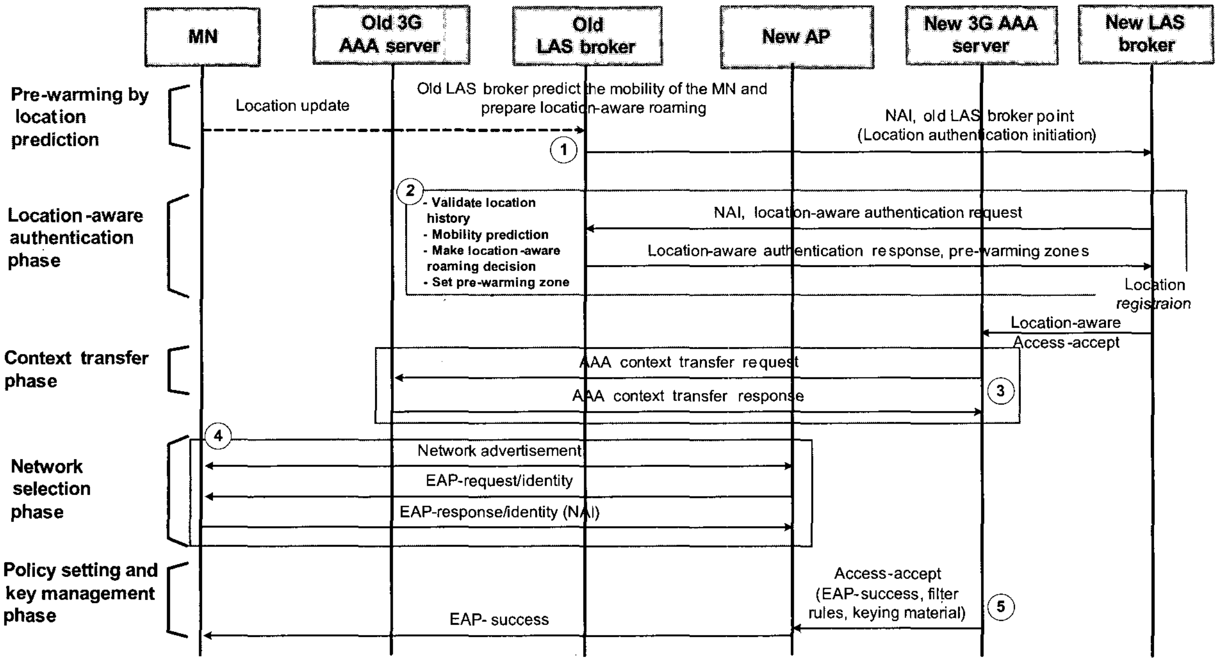

MN
Old 3G AAA server
Old LAS broker
New AP
New 3G AAA server
New LAS broker
Pre-warming by location prediction
Location-aware authentication phase
Context transfer phase
Network selection phase
Policy setting and key management phase
Location update
Old LAS broker predict the mobility of the MN and prepare location-aware roaming
1
NAI, old LAS broker point (Location authentication initiation)
2
- Validate location history
- Mobility prediction
- Make location-aware roaming decision
- Set pre-warming zone
NAI, location-aware authentication request
Location-aware authentication response, pre-warming zones
Location registraion
Location-aware Access-accept
AAA context transfer request
AAA context transfer response
3
4
Network advertisement
EAP-request/identity
EAP-response/identity (NAI)
Access-accept (EAP-success, filter rules, keying material)
5
EAP- success

Fig. 7. Location-aware secure roaming procedure from UMTS to WLAN with context transfer.

the handover process is not slowed down due to location-aware authentication.

Initially, the old LAS broker extracted possible new LAS broker based on the location prediction in advance (Step ①). To begin a context transfer for location-aware secure roaming, the authentication request message is sent from the new LAS broker to old LAS broker (Step ②). After the old LAS broker computes the pre-warming zones and validates the location history of the MN, the new LAS broker permits the location-aware roaming and sends the accept message to new AAA server. Then, the AAA context transfer request message is sent from the new AAA server to old AAA server to begin AAA context transfer (Step ③). Note that in the *networks selection phase* and *policy setting and key management phase* the signaling flow is the same as that shown in Fig. 6.

VI. EVALUATION OF LOCATION-AWARE SECURE ROAMING

A. Testbed Setup

In order to test our location-aware secure roaming for LAS in 4G networks, we created the testbed shown in Fig. 8. We employ four different wireless networks in our testbed: WLANs, GPRS, CDMA, and UMTS.

Table 3 summarizes the base parameters underlying the performance experiments. The parameters of the cellular systems are based on the Korea Telecom Freetel (KTF) cellular systems with the core network components such as Node B, RNC, SGSN, and GGSN developed by LG Electronics Inc. We setup a radio environment that emulates the radio transmission [40] of the KTF 3G cellular systems.

LAS broker and LAS policy authority are running on server machines of Pentium III 933 MHz CPUs with Solaris 8 operating system (O/S). AAA server is running on a server of Pentium III 800 MHz (Linux O/S) and the modified FreeRADIUS [41] library for RADIUS functionality. APs are working on a Pentium III 500 MHz machines (Linux O/S) with Lucent Orinoco 802.11b WLANs cards. MNs are running on Pentium III 500 MHz machines (WindowsXP O/S) with the same WLAN cards. The cryptographic library is OpenSSL 0.9.7a [42], and SAML library is OpenSAML 0.9.1 [43]. Data size is 1 KB in digital signature.

B. Location-Aware Authentication

We evaluate our location-aware secure roaming scheme in three cases. In the fist case, we evaluate our location-aware secure roaming scheme between WLANs for micro-mobility as shown in Figs. 9 and 10. Then, we evaluate our scheme between UMTS and WLAN for macro-mobility as shown in Figs. 11 and 12. Finally, to demonstrate the effectiveness of our location-aware context-transfer and pre-warming we present the performance evaluation as shown in Figs. 13 and 14. Note that the previous two cases from Figs. 9 to 12 did not include our location-aware context-transfer and pre-warming schemes.

Fig. 9 shows the averages of our measurements in full authentication for initial secure association. The solid curves represent the measurements without our location-aware scheme and the dotted curves represent our location-aware case. Figs. 10–12 show the delay performances for the proposed location-aware secure roaming for micro-mobility between WLANs and for macro-mobility among CDMA, GPRS, UMTS, and WLAN, respectively. We notice an important difference between the full authentication case and the roaming case. When the moving MNs are increasing, our location-aware scheme does not create much burden on roaming as to selection of 802.1X [44] authentication methods.

Table 3. Base parameters of the testbed.

Entity	Operation	Description	Performance
MN-AAA	802.1X full authentication (EAP-TLS)	Average delay	1, 600 ms
LAS broker	Location history request to location server	Request location history of MN	50 ms
LAS broker	Location-aware authentication	Validation of location history of MN	80 ms
LAS broker	SAML authorization request	XML parsing and RSA 1024 signature	27.4 ms
LAS policy authority	SAML authorization response	XML parsing and RSA SHA-1 1024 bit key signature verify	20.4 ms
LAS policy authority	SAML authentication token generation and response to MN	3DES symmetric key encryption	7.702 MB/s
LAS broker	Token response with location information	RSA encrypt on 512 bit keys	31.201 KB/s
MN-AP	802.11 scan (active)	Average latency	40 ~ 300 ms
MN-AP	802.11 reassociation with IAPP	Average latency	40 ms
MN-AP	Fast handover (4-way handshake only)	Average delay	60 ms
CDMA	Full authentication and association	Average delay[a]	4, 300 ms
802.11/CDMA	TCP parameter adjustment	Average delay[a]	5, 000 ms
802.11/GPRS	TCP parameter adjustment	Average delay[a]	20, 000 ms
UMTS/802.11	Intradomain UMTS to WLAN handover with EAP-SIM authentication	Average delay[a]	9, 300 ms
AAA proxy-AAA server	AAA context transfer response	Average delay	25 ms

[a] The parameters are based on the KTF cellular systems with the core network components (node B, RNC, GGSN, and SGSN) of LG Electronics.

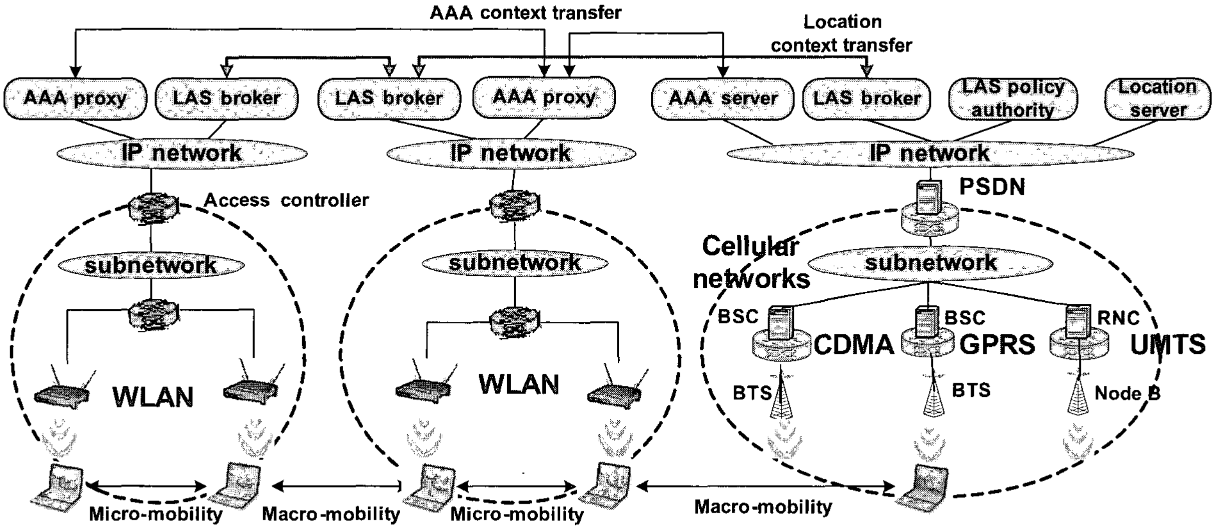


Fig. 8. Testbed of the location-aware secure roaming with 3G/WLAN interworking context transfer for 4G mobile networks.

In full authentication of Fig. 9, compared to EAP-TLS scheme, the latency increase of the location-aware scheme with EAP-TLS is about 7.61%. But in the roaming case of Fig. 10, location-aware scheme with EAP-TTLS CHAP [45] shows almost the same performance with roaming of EAP-TLS without location-aware scheme. In Fig. 11, the roaming delay between wireless LANs and 2G cellular systems including CDMA and GPRS are increased due to the large delay of parameter adjustment. The overhead of our location-aware scheme in UMTS-to-WLAN roaming is 9.54% in Fig. 12.

We should consider trade-off among QoS of LAS including location update period and location precision, security, and privacy. In fact, both dimensions of security strength and network performance are equally important, and achieving a good tradeoff between two extremes is one fundamental challenge in security design for location-aware computing. The strength of the location-aware authentication scheme by LAS broker is given its improved security which is achieved at the expense of increasing delays.

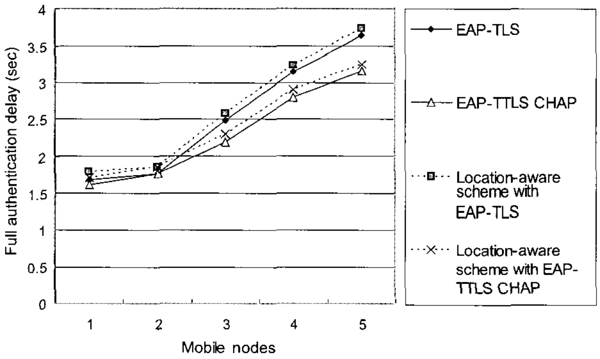


Fig. 9. Full authentication latencies in WLAN.

C. *Location-Aware Authentication with Pre-warming and AAA Context Transfer for Fast Handover*

To minimize the additional delay of location-aware authentication, we developed and tested the pre-warming by LAS bro-

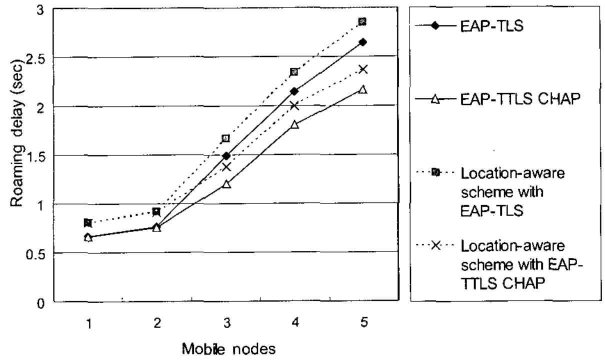


Fig. 10. Delay performance of the location-aware secure roaming from WLAN to WLAN.

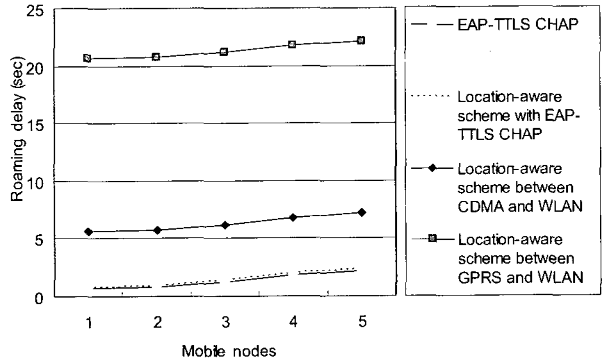


Fig. 11. Delay performance of the location-aware secure roaming among wireless LAN, CDMA, and GPRS.

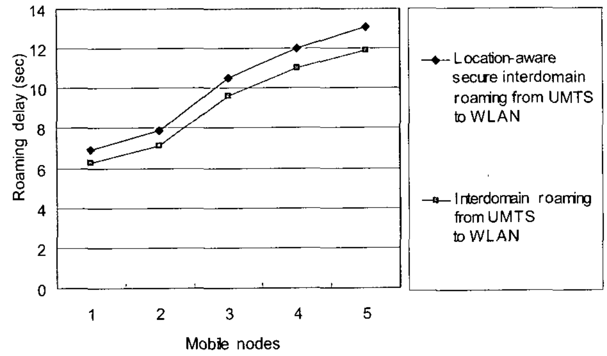


Fig. 12. Delay performance of the location-aware secure roaming from UMTS to WLAN.

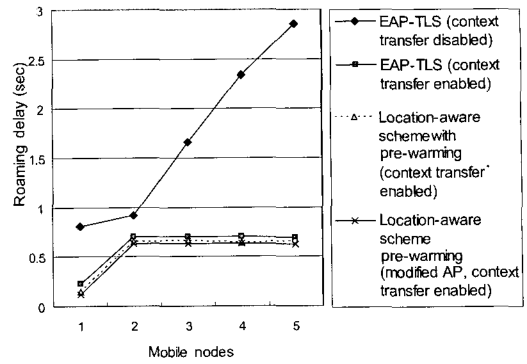


Fig. 13. Delay performance of the location-aware secure roaming from WLAN-to-WLAN with context transfer and pre-warming.

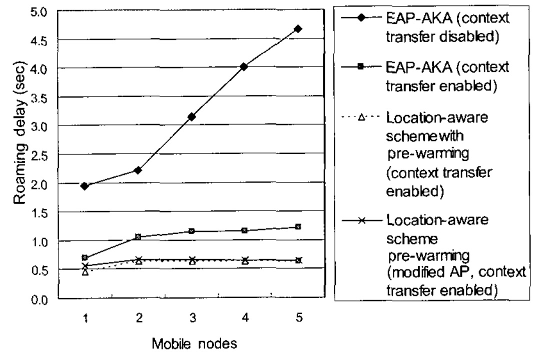


Fig. 14. Delay performance of the location-aware secure roaming from UMTS-to-WLAN with context transfer and pre-warming.

ker and context transfer between AAA servers and LAS brokers. The main objective behind the scheme is to reduce the conversations to the minimal number of messages required by the existing security mechanisms and provide the same security level of the full authentication.

Figs. 13 and 14 demonstrate the effectiveness of the location-aware authentication with the context transfer and pre-warming zone.

Table 4 shows the packets captured during our location-aware secure roaming from UMTS-to-WLANs. Fig. 13 shows that the interdomain handover from WLAN-to-WLAN introduces an average delay of 1.986 s, while for handover with context transfer the average delay is 0.704 s. Fig. 14 show that the interdomain handover from UMTS-to-WLAN introduces an average delay of 3.313 s, while for handover with context transfer the average delay is 1.153 s.

Our location-aware scheme with pre-warming and context transfer show more enhanced performances and the average delay is 0.656 s by avoiding the additional delay of 0.881 s introduced by AAA context transfer and installing the key material. The modified APs represent that we enhanced the state machine of APs to support context caching in AAA context transfer. It is important to note that the improvement of location-aware handover with pre-warming and context transfer is almost 5 times.

In our location-aware case, AAA context transfer actually takes place between an AAA proxy and an AAA server before handover by setting the pre-warming zone with a LAS broker. The right AP/BS in the pre-warming zone for the next handover has the authentication information of users. As the users don't have to gain each authentication from the 3G AAA servers for further handovers, our mechanisms avoid the additional reauthentication delay. Autonomous location-prediction by LAS brokers should be used in order to keep the location-aware authentication fresh and dynamic. Pre-warming has no effect on the performance of the vertical handover. Therefore, a larger number of MNs did not put too much burden on the

Table 4. Signaling exchanges of EAP-AKA and our location-aware secure roaming from UMTS-to-WLANs.

Message	Information	Source	Destination	Time (s)
	1. EAP-AKA without context transfer			
1	Authenticate request	MN	AP	3.923
2	Authenticate response	AP	MN	3.923
3	Association request	MN	AP	4.223
4	Association response	AP	MN	4.523
5	EAPOL- START	MN	AP	4.544
6	Request identity	AP	MN	4.545
7	Identity	MN	AP	4.580
8	Identity	AP	AAA proxy	4.581
9	Identity	AAA proxy	Home AAA	4.606
10	Authentication data request	Home AAA	HSS	4.631
11	Authentication data response	HSS	Home AAA	5.531
12	Access-challenge/EAP-request	Home AAA	AAA proxy	5.556
13	Access-challenge/EAP-request	AAA proxy	AP	5.590
14	EAP-request	AP	MN	5.590
15	EAP-response	MN	AP	5.659
16	Access-request/EAP-response	AP	AAA proxy	5.684
17	Access-request/EAP-response	AAA proxy	Home AAA	5.710
18	Registration	Home AAA	HSS	5.710
19	Access-accept/EAP-success, key material, filter rules	Home AAA	AAA proxy	5.735
20	Access-accept/EAP-success, key material, filter rules	AAA proxy	AP	5.766
21	EAP-success	AP	MN	5.767
	Handover delay $= 5.767 - 3.923 = 1.844$ s			
	2. EAP-AKA with context transfer			
1	Authenticate request	MN	New AP	6.670
2	Authenticate response	New AP	MN	6.671
3	Association request	MN	New AP	6.971
4	Association response	New AP	MN	7.271
5	EAPOL- START	MN	New AP	7.281
6	Request identity	New AP	MN	7.282
7	Identity, old AAA server	MN	New AP	7.310
8	Identity, old AAA server	New AP	New AAA	7.311
9	AAA context transfer request	New AAA	Old AAA	7.336
10	AAA context transfer response	Old AAA	New AAA	7.351
11	Access accept (EAP-success, keying material)	New AAA	New AP	7.358
12	EAP-success	New AP	MN	7.359
	Handover delay $= 7.359 - 6.670 = 0.688$ s			
	3. Location-aware authentication with context transfer, pre-warming			
	Before handover			
	Pre-warming zone indication	Old LAS broker	New LAS broker	0.025
	Location-aware access accept	New LAS broker	New AAA	0.007
	AAA context transfer request	New AAA	Old AAA	0.025
	AAA context transfer response	Old AAA	New AAA	0.025
	Handover start			
1	Authenticate request	MN	New AP	12.357
2	Authenticate response	New AP	MN	12.387
3	Association request	MN	New AP	12.557
4	Association response	New AP	MN	12.857
5	EAPOL- START	MN	New AP	12.878
6	Request identity	New AP	MN	12.878
7	Identity	MN	New AP	12.911
8	Identity	New AP	New AAA	12.912
9	Access accept (EAP-success, keying material)	New AAA	New AP	12.916
10	EAP-success	New AP	MN	12.916
	Handover delay $= 12.916 - 12.357 = 0.559$ s			
	4. Location-aware authentication with context transfer, pre-warming, modified APs			
	Before handover			
	Pre-warming zones	Old LAS broker	New LAS broker	0.025
	Location-aware access accept	New LAS broker	New AAA	0.007
	AAA context transfer request	New AAA	Old AAA	0.025
	AAA context transfer response	Old AAA	New AAA	0.025
	Access accept (EAP-success, keying material)	New AAA	New AP	0.007
	Handover start			
1	Authenticate request	MN	New AP	7.080
2	Authenticate response	New AP	MN	7.091
3	Association request	MN	New AP	7.181
4	Association response	New AP	MN	7.481
5	EAPOL-START	MN	New AP	7.501
6	Request identity	New AP	MN	7.502
7	Identity	MN	New AP	7.532
8	EAP-success	New AP	MN	7.533
	Handover delay $= 7.533 - 7.080 = 0.453$ s			

handover process and the roaming delay isn't substantially increased. We have repeated this test and it has been observed that although the actual times vary, our location-aware scheme with context transfer is much faster than that without context transfer.

VII. CONCLUSIONS AND FUTURE WORKS

In this paper, we have reviewed the advantages provided by the adoption of location-awareness with LAS broker in support of seamless secure roaming for future mobile networks. We analyze interworking and security issues in location-aware computing and give our view on the future prospects for the interworking system to support variety of access technologies such as WLANs, WMANs, and UMTS.

Our architecture integrates location-aware authentication scheme for macro and micro mobility with directive services by the cooperation of LAS brokers and AAA servers. Our interworking system can be enhanced by new functionalities such as more advanced LAS by enabling efficient support of location-aware secure fast roaming with LAS broker and location privacy policy controls with LAS policy authority. This integrated scheme could provide the desired security features and requirements for survivable heterogeneous wireless networks.

A testbed has been developed and simulation results demonstrate how the location-aware mechanism enhances the overall vertical handover performance (up to 80% latency reduction) as well as provides the advanced seamless secure mobility management for the 4G mobile systems. Based on these results, we believe our fast secure roaming scheme with LAS broker could potentially lead to an efficient method of managing a large-scale cooperative wireless networks. The proposed location-aware mechanism is being integrated with secure web services infrastructure [3] and the new interworking systems [17].

This paper leaves open the issue of how to handle the location-aware secure roaming process when the verification of location-aware authentication (location history data) fails. Fallback to full authentication procedure might be a problem for time critical services. High level location prediction algorithms and intelligent message handling algorithms tied to the mobile systems may be important areas for future research.

ACKNOWLEDGMENTS

The authors would like to thank Jungman Park of KTF for helping with the experiments on our testbed.

REFERENCES

[1] M. Hazas *et al.*, "Location-aware computing comes of age," *IEEE Computer*, vol. 37, pp. 95–97, Feb. 2004.

[2] G. D. Abowd *et al.*, "Cyberguide: A mobile context-aware tour guide," *ACM/Baltzer Wireless Networks*, vol. 3, no. 5, pp. 421–433, Oct. 1997.

[3] M. Lee *et al.*, "A secure web services for location based services in wireless networks," *Lecture Notes in Computer Science*, vol. 3042, pp. 332–344, May 2004.

[4] B. Schilit *et al.*, "Wireless location privacy protection," *IEEE Computer*, vol. 36, pp. 135–137, Dec. 2003.

[5] 3GPP TR 22.934 v6.2.0, "Feasibility study on 3GPP system to WLAN interworking (Release 6)," Sept. 2002.

[6] V. W.-S. Feng *et al*, "WGSN: WLAN-based GPRS environment support node with push mechanism," *Computer J.*, vol. 47, no. 4, pp. 405–417, July 2004.

[7] A. K. Salkintzis, "Interworking techniques and architectures for WLAN/3G integration toward 4G mobile data networks," *IEEE Wireless Commun.*, vol. 11, pp. 50–61, June 2004.

[8] D. E. Denning and P. D. MacDoran. "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud and Security*, Feb. 1996.

[9] J. E. Bardram *et al.*, "Context-aware user authentication - supporting proximity-based login in pervasive computing," in *Proc. UbiComp 2003*, Oct. 2003.

[10] N. Montavont *et al.*, "Handover management for mobile nodes in IPv6 networks," *IEEE Commun. Mag.*, vol. 40, pp. 38–43, Aug. 2002.

[11] K. D. Wong *et al.*, "Mobility management scheme for auto-configured wireless IP networks," *IEEE Wireless Commun.*, vol. 10, pp. 62–69, Oct. 2003.

[12] M. Shi *et al.*, "IEEE 802.11 roaming and authentication in wireless LAN/cellular mobile networks," *IEEE Wireless Commun.*, pp. 66–75, Aug. 2004.

[13] G. Liu and G. Maguire Jr., "A class of mobile motion prediction algorithms for wireless mobile computing and communicatons," *ACM/Baltzer MONET*, vol. 1, no. 2, pp. 113–121, Oct. 1996.

[14] T. Liu, P. Bahl, and I. Chlamtac, "Mobility modeling, location tracking, and trajectory prediction in wireless ATM networks," *IEEE J. Select. Areas Commun.*, vol. 16, no. 16, pp. 922–936, Aug. 1998.

[15] V. Bhargavan and M. Jayanth, "Profile-based next-cell prediction in indoor wireless LAN," in *Proc. IEEE SICON'97*, Apr. 1997.

[16] W.-S. Soh and H. S. Kim, "Dynamic bandwidth reservation in cellular networks using road topology based mobility predictions," in *Proc. IEEE INFOCOM 2004*, Mar. 2004.

[17] M. Lee *et al.*, "A location-aware secure interworking architecture between 3GPP and WLAN systems," *Lecture Notes in Computer Science*, vol. 3506, pp. 400–412, May 2005.

[18] P. Mähönen *et al.*, "Hop-by-hop toward future mobile broadband IP," *IEEE Commun. Mag.*, vol. 42, pp. 138–146, Mar. 2004.

[19] M. Vossiek, "Wireless local positioning," *IEEE Microwave*, vol. 4, pp. 77–86, Dec. 2003.

[20] Q. He *et al.*, "The auest for personal control over mobile location privacy," *IEEE Commun. Mag.*, vol. 42, pp. 130–136, May 2004.

[21] M. Gruteser *et al.*, "Protecting privacy in continuous location-tracking applications," *IEEE SECURITY & PRIVACY*, vol. 2, pp. 28–34, Mar.–Apr. 2004.

[22] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, pp. 46–55, Jan-Mar. 2003.

[23] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proc. PerSec 2004*, Mar. 2004, pp. 127–131.

[24] V. Marques *et al.*, "An IP-based QoS architecture for 4G operator scenarios," *IEEE Wireless Commun.*, vol. 10, pp. 54–62, June 2003.

[25] I. F. Akyildiz *et al.*, "A survey of mobility management in next-generation all-IP-based wireless systems," *IEEE Wireless Commun.*, vol. 11, pp. 16–28, Aug. 2004.

[26] 3GPP TS 33.234 v050, "3G Security; wireless local area network (WLAN) interworking security," Release 6, work in progress.

[27] G. M. Koien and T. Haslestad, "Security aspects of 3G-WLAN interworking," *IEEE Commun. Mag.*, vol. 41, pp. 82–88, Nov. 2003.

[28] IETF RFC 2716, "PPP EAP-TLS authentication protocol," Oct. 1999.

[29] G. Kambourakis *et al.*, "Advanced SSL/TLS-based authentication for secure WLAN-3G interworking," *IEE Proc. Commun.*, vol. 151, no. 5, Oct. 2004.

[30] IEEE Standard 802.11i, July 2003.

[31] S. Y. Hui and K. H. Yeung, "Challenges in the migration to 4G mobile systems," *IEEE Commun. Mag.*, pp. 54–59, Dec. 2003.

[32] J. McNair and Z. Fang, "Vertical handoffs in fourth-generation multinetwork environments," *IEEE Wireless Commun.*, vol. 11, pp. 8–15, June 2004.

[33] C. Prehofer and Q. Wei, "Active networks for 4G mobile communication: Motivation, architecture, and application scenarios," in *Proc. IWAN 2002*, Dec. 2002.

[34] N. Shenoy *et al.*, "Performance of a framework for seamless integration of cellular and WLANs," in *Proc. OPNETWORK 2004*, Sept. 2004.

[35] R. Chellappa-Doss, A. Jennings, and N. Shenoy, "User mobility prediction in hybrid and ad hoc wireless networks," in *Proc. ATNAC 2003*, Dec. 2003.

[36] 3GPP TS 23.234 v6.1.0, "3GPP system to wireless local area network (WLAN) interworking: System description," Release 6, June 2004.

[37] IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks, part 16, "Air interface for fixed broadband wireless access systems," IEEE Press, 2001.

[38] 3GPP TS 23.271 v6.9.0, "3GPPF functional stage 2 description of location services (LCS)," Release 6, Sept. 2004.

[39] OASIS Security Services TC, Security Assertion Markup Language (SAML) v1.1, Aug. 2003.

[40] S. Dixit and R. Prasad, *Wireless IP and Building the Mobile Internet*, Artech House, 2003.

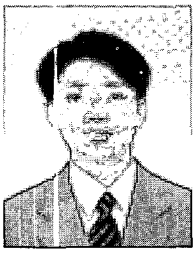
[41] FreeRADIUS, http://www.freeradius.org/.

[42] OpenSSL, http://www.openssl.org/.

[43] OpenSAML, http://www.opensaml.org/.

[44] IEEE 802.1X, "Port-based network access control," 2001.
[45] IETF Internet Draft, "EAP tunneled TLS authentication protocol," Apr. 2004.

Minsoo Lee received the B.S. and M.S. degrees in the School of Electrical and Electronics Engineering from the Chung-Ang University, Seoul, Korea in 2001 and 2003, respectively. He is currently a Ph.D. candidate in the School of Electrical and Electronics Engineering at the Chung-Ang University. He is pursuing the Ph.D. degree under the advice of Professor Sehyun Park. He is also a senior research staff at Chung-Ang University HNRC (Home Network Research Center)-ITRC (Information Technology Research Center) supported by the MIC (Ministry of Information and Communication), Korea. His major research interests are in location-aware computing, location security and privacy, ubiquitous computing, home networks, and mobile network security.



Gwanyeon Kim received the B.S. and M.S. degrees in the School of Electrical and Electronics Engineering from the Chung-Ang University, Seoul, Korea in 2001 and 2003, respectively. He is currently a Ph.D. candidate in the School of Electrical and Electronics Engineering at the Chung-Ang University. He is pursuing the Ph.D. degree under the advice of Professor Sehyun Park. He is also a senior research staff at Chung-Ang University HNRC (Home Network Research Center)-ITRC (Information Technology Research Center) supported by the MIC (Ministry of Information and Communication), Korea. His major research interests are in home networks, ubiquitous computing, mobile networks, and network security.

Sehyun Park received the B.S. and M.S. degrees in electronics engineering from the Chung-Ang University, Seoul, Korea in 1986 and 1988, respectively, and the Ph.D. from University of Massachusetts, Amherst in 1998. From 1988 to 1999, he was a senior research staff at ETRI, Korea. He is currently an Associate Professor of School of Electrical and Electronics Engineering at the Chung-Ang University, where he has established the Ubiquitous Computing and Cipher Internet Laboratory. He is the head of Chung-Ang University HNRC (Home Network Research Center)-ITRC (Information Technology Research Center) supported by the MIC (Ministry of Information and Communication), Korea. His major research interests include home networks, ubiquitous computing, and network security.