Efficient 3G/WLAN Interworking Techniques for Seamless Roaming Services with Location-aware Authentication *

Minsoo Lee[1], Gwanyeon Kim[1], Sehyun Park[1] **, Sungik Jun[2], Jaehoon Nah[2], and Ohyoung Song[1]

[1] School of Electrical and Electronics Engineering, Chung-Ang University, 221, Heukseok-dong, Dongjak-gu, Seoul 156-756, Korea
{lemins, cityhero}@wm.cau.ac.kr,{shpark, song}@cau.ac.kr
[2] Electronics and Telecommunications Research Institute 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{sijun, jhnah}@etri.re.kr

Abstract. This paper proposes novel concepts and architectures for location-aware seamless authentication and roaming in the new interworking system between third-generation (3G) mobile networks and wireless local area networks (WLANs) where local mobility movements (micro-mobility) are handled together with global movements (macro-mobility). We introduce location as a key context in secure roaming mechanism for context-aware interworking. The fast secure roaming with location-aware authentication is implemented at an entity called *LBS Broker* that utilizes the concepts of direction of user and *pre-warming zone*. We present the interworking techniques with *LBS Broker* for seamless secure WLAN/3G integration enabling to meet the requirements of the future location-aware service scenarios. Performance evaluation is also presented to demonstrate the effectiveness of the proposed scheme for fast location-aware secure roaming.

Keywords: ubiquitous computing, location-aware, 3G, 4G, WLAN, interworking, security

1 Introduction

In the fourth-generation (4G) mobile networks which are expected to be very complex systems interconnecting various technologies and architectures, new intelligent services will need to be aware of *location* that can determine which types of devices are available and how communication should be conducted. *Location-aware computing* may soon become a part of everyday life with Location-based

* 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).

** The corresponding author

services (LBS) like asset tracking, environmental resource discovery and control, and electronic tourist guides [1].

Location-aware computing is made possible by the convergence of three distinct technical capabilities: location sensing, wireless communication, and mobile computing systems. As multiple access technologies are becoming part of a common wireless infrastructure, mobility management is more complicated in the integrated networks of wireless LANs (WLANs) with third-generation (3G) mobile networks such as Global System for Mobile Communications/General Packet Radio Service (GSM/GPRS), Universal Mobile Telecommunications System (UMTS) and CDMA2000.

Recently, complementary features between WLANs with high data rates and 3G mobile networks with wide coverage have spurred the demand for 3G/WLAN interworking systems. In these interconnected wireless networks we need smart techniques for determining the current location of a mobile node (MN). Apart from technical difficulties in providing accurate location information, there is also a lack of a clearly defined framework to create innovative security services with location information. There are few safeguards on location privacy and security as in our previous work [2].

On the 3G/WLAN interworking, a feasibility study [3] 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 the next generation wireless networks. Based on [4,5,6], 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 allows a customer to change access between 3G and WLAN networks during a service session. Scenario 3 features should be essential for the first stage deployment.

In our paper we focus mainly on scenarios 3 and 4, and 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 [6, 7] we suggest location-aware authentication introducing *location* as a new element in a user authentication mechanism. In particular, we propose and discuss efficient mobility management schemes with *LBS Broker* that can support consistent secure LBS provisioning. LBS Broker includes location-aware authenticator for fast secure roaming using the concepts of the direction of the user and pre-warming zone. We further explain how the proposed approach can be applied to seamless secure interworking between 3G and WLAN with the evaluation of our testbed.

The rest of this paper is organized as follow. Section 2 gives related works about location-aware computing in 4G mobile networks. Section 3 identifies the problems and requirements of location-aware security in 3G/WLAN interworking. In Section 4 we propose LBS Broker with location-aware authentication and pre-warming for fast secure roaming. Section 5 suggests our location-aware secu-

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 MN	- 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 Based Service (LBS) via 3G and WLAN	- User data traffic management with Packet Data Gateway (PDG) and Wireless Access Gateway(WAG) - LBS platform with LBS Broker to enforce Location-aware Services
4 (Tight Coupling)	Access to 3G PS-based services with service continuity	- Service continuity for transitions between 3GPP Systems and WLANs. - Changes of QoS - To allow transition of multiple sessions and services	- Location-aware Vertical handover - Location-aware Resource Management - Policy-based location management to enforce location privacy - LBS using Web Services through Internet - LBS 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 - LBS QoS guarantees - Secure LBS Platform with LBS 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 - LBS QoS guarantees - Secure LBS Platform for heterogeneous networks

rity architecture for 3G/WLAN interworking systems. In Section 6, we discuss experimental result and we conclude in Section 7.

2 Related Works

4G mobile networks are expected to be very complex systems interconnecting various technologies and architectures. On these complex systems new intelligent services will need to be aware of *location* that can determine which types of devices are available and how communication should be conducted in order to maintain QoS guarantees. Location information will be available from various types of network including sensor networks, WLANs, 3G including UMTS and CDMA 2000[8]. According to development of WLANs, 3G and 4G networks and increase of the accuracy of the positioning technology, many LBSs with efficiency and reliability will appear.

Toward seamless security of the interconnected 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 [18] and an integrated management that combines the strengths of

Mobile IP Location Registers (MIP-LR) and Session Initiation Protocol (SIP) [19]. As solutions for integrating 3G and WLAN services some of the recent studies have focused on a gateway [4], interworking techniques and architectures [5], a roaming and authentication service framework [24].

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 indispensible in 4G networks, there are challenging issues with regard to location-aware seamless secure roaming.

3 Motivations and Requirements

In the vision of 4G mobile networks MN should be able to connect the best wireless networks among ad-hoc, personal, wired and wireless LANs and 3G mobile networks [8, 23]. 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 [9]. Even with future mobile devices are likely equipped with reasonably accurate positioning capability, location-aware computing also includes many issues related to location privacy, consistent QoS guarantee, seamless vertical handover, common authentication, and so on. The following requirements should be considered to fulfill the promising services of the 3G/WLAN interworking.

- *Privacy and Security*: 3G/WLAN interworking shall not be compromised. It is required that authentication and key distribution should be based on the UMTS authentication and key agreement (AKA) procedure and EAP-AKA or EAP-SIM for WLAN [15,16]. The interworking system should eliminate the invasion of privacy by unwanted disclosure and commercial use of location information [2,20,21,22].
- *Global Secure Roaming*: MNs should be seamlessly served from foreign domain without any pre-established user authentication or authorization.
- *QoS guarantees*: The effectiveness of location-aware services depends not only on the user population but also on QoS guarantee. - Reduction of signaling overheads and latency of service delivery - Maintain QoS guarantees in different mobile systems.
- *Handover Management*: Handover latency is especially disruptive to continuous location tracking, even if most of the reauthentication during the handover in different networks are not lost but delayed.

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 security for seamless interworking of the new 3G/WLAN system by means of the efficient location-aware schemes.

4 Location-aware Services with LBS Broker

In this section, we discuss how security can be improved through a new form of authentication based on location-aware mechanisms with LBS Broker. The location of the mobile device can be added as an additional authentication parameter for 3G/WLAN integration. Carefully managed location information could be used as authentication information. In order to provide location-aware seamless services at any time and anywhere, mobility is the key element in 3G/WLAN interworking systems. We have identified parameters for location-aware handover in consideration for vertical handover [10] as in Figure 1.

One of the difficulties in providing seamless roaming service is how to promptly and securely exchange security context during handover. The exchange of authentication information in advance by tracking and predicting users direction, so called *pre-warming* may helpful to simplify the authentication process during the handover to support seamless roaming service [11, 12]. For example, if the MN A in Figure 2 is on the subway, it will obviously handover from AP1 to AP2. Therefore, the authentication information of the mobile station needs to be delivered from AP1 to AP2 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. A prediction of pre-warming zones is especially possible in track bounded wireless networks. 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 Bob in Figure 2, its path may be effectively predicted by the history based location algorithms 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 [12].

For seamless roaming service, we propose a LBS Broker including a location-aware authenticator that maintains a dynamic trust. Once LBS Broker predicts a users direction in heterogeneous networks, it forms a pre-warming zone to pre-establish trust relationships with AAA for fast handover. During the handover

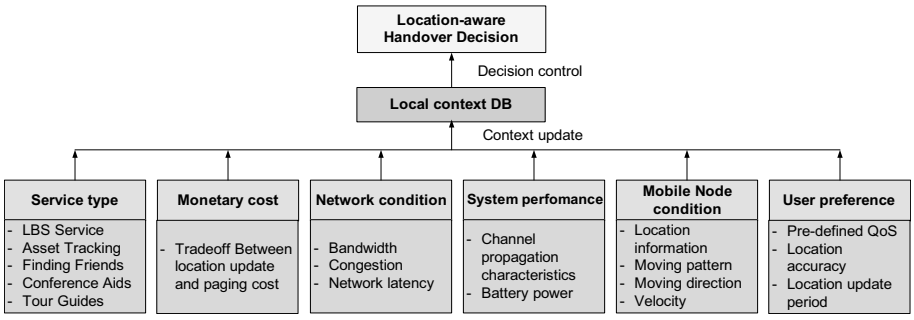


Fig. 1. The Proposed Location-aware handover decision criteria

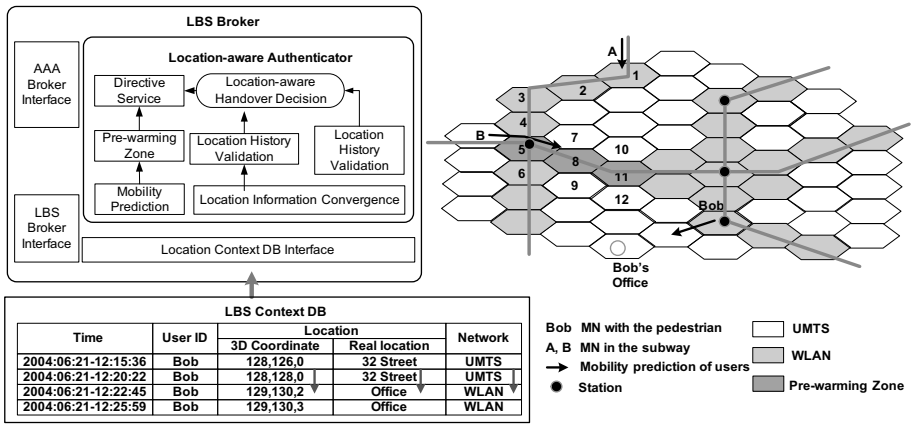


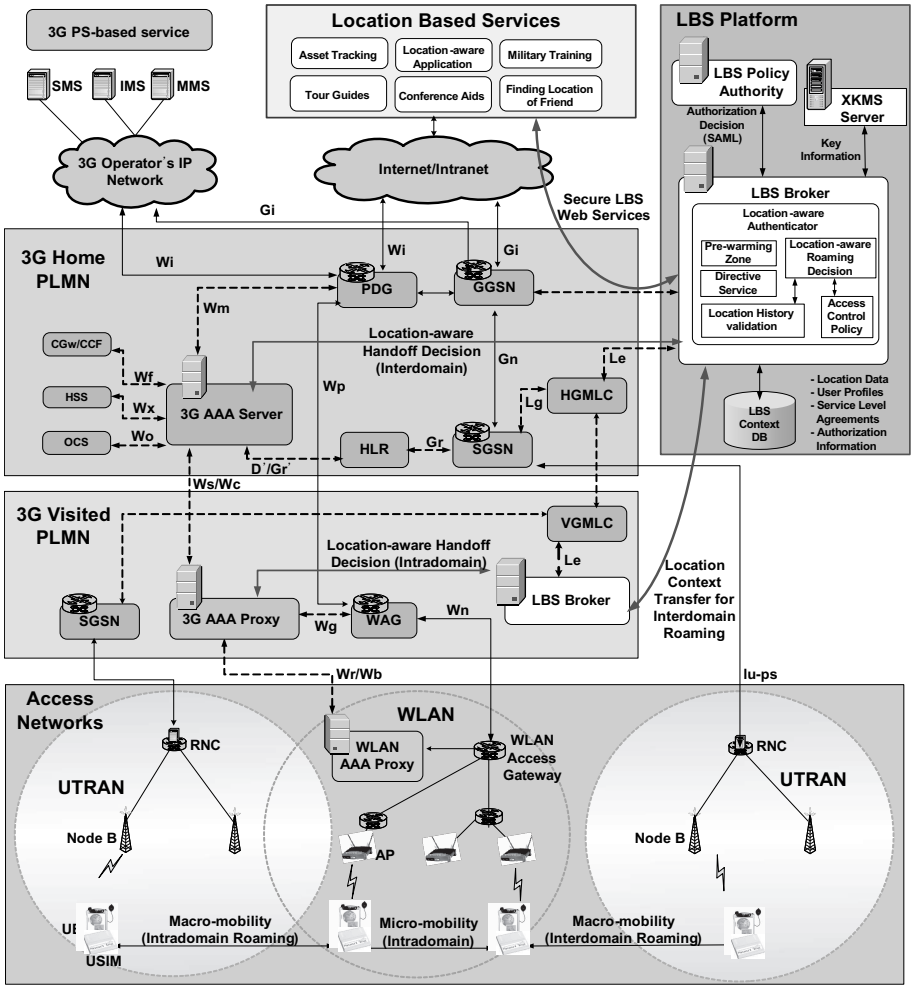
Fig. 2. LBS Broker with Location-aware Authentication and Pre-warming

location history of the user in 3G networks could enforce the location-aware authentication. In the case of the roaming from UMTS to WLAN, LBS 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 not necessary to process full reauthentication, handover latency can be greatly decreased by performing only association and 4-way handshake (if necessary). If the MN B in Figure 2 is on the subway, LBS Broker decides APs within its pre-warming zone (5→ 8→11) and performs pre-authentication in advance for fast handover.

5 The 3G/WLAN Interworking System for Seamless Roaming Services with Location-aware Authentication

5.1 3G/WLAN Interworking System with Location Services

We designed the location-aware security architecture for 3G/WLAN interworking to meet the location-aware computing requirements in section 3. Figure 3 shows the proposed interworking architecture. For satisfying the key requirements of 3G/WLAN interworking scenario 3 in Section 1, the user data traffic in WLANs is routed to the 3G home Public Land Mobile Network or visited PLMN through a component called a packet data gateway (PDG) or a wireless access gateway (WAG), which in the case of roaming is located in the preferred 3G visited PLMN. For several interfaces, Wn, Wm, Wi, Wg, and Wp, we also adopt the notation and functionality specified in [13]. Location services (LCS) is logically implemented on the network structure through the addition of one network node, the Gateway Mobile Location Center (GMLC) or Mobile Location Center (MLC)[14]. LBS Broker may get location information directly from Gateway Mobile Location Center (GMLC).



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. 3. The 3G/WLAN Interworking System for Seamless Roaming Services with Location-aware Authentication(dashed lines: signaling; solid lines: data and signaling)

5.2 Location-aware Authentication and Secure Roaming Services

We present LBS Broker to securely provide the functionalities of location authority that gives a space of possible locations and can respond to queries on distances, routes, and proximity. LBS Broker plays key roles not only in

location-aware authentication for fast roaming and but also in protecting users privacy.The agent model of LBS Broker could separate the security system from the location-based application. Supporting abstraction has a number of advantages. Firstly, it allows security unaware applications to be secured. This means that applications do not need to know much about the security features, because location security and privacy policies are enforced by LBS Broker. As an abstraction for location-aware computing, LBS Broker supports Web Services for interoperability of LBS. It also provides Web Services Security Specification like XML Signature, XML Encryption and Security Assertion Markup Language (SAML). LBS Broker act as a Policy Enforcement Point (PEP) that checks permission with the LBS policy authority, the Policy Decision Point (PDP) by requesting SAML assertion before making decisions and releasing the secured location data to the LBS service providers.

Intradomain (micro-mobility) authentication, authorization, and accounting (AAA) are handled together with LBS Broker and AAA server. When a user moves into a foreign network for interdomain roaming (macro-mobility), LBS Broker, AAA proxy and AAA server take charge of reauthentication process. LBS Broker enforce fast vertical handover by validation location history of MN using concepts of direction of user and pre-warming zone for 3G/WLAN interworking. Between AAA proxy in visited PLMN and AAA server in home PLMN, AAA context transfer protocol is used. Location context are exchanged between LBS Brokers. In the absence of context transfer, there may be large delays because of the network signaling required to re-establish QoS flows, re-authenticate the mobile user [10].

5.3 AAA Signaling for Location-aware Authentication and Roaming

One of the challenging problems in the 3G/WLAN interworking systems is the interdomain roaming, which requires additional efforts to establish security relationships from the previous to the new access router in the different types of networks. To enforce the authenticity of MNs the location-aware authentication and secure roaming should be associated with AAA procedures.

The proposed location-aware secure roaming procedure from UMTS to WLAN is depicted in Figure 4. Based on the network advertisement data, a MN selects a preferred 3G visited PLMN and forms a second Network Address Identifier (NAI) corresponding to this PLMN [5]. 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. If the 3G AAA Server uses Location-aware authentication, it sends a location authentication request to LBS Broker. LBS Broker authenticates to the user and it sends a Location authentication response to the 3G AAA server. If the 3G AAA authenticates to the MN successfully, it sends EAP-Success message with keying material and some filter rules.

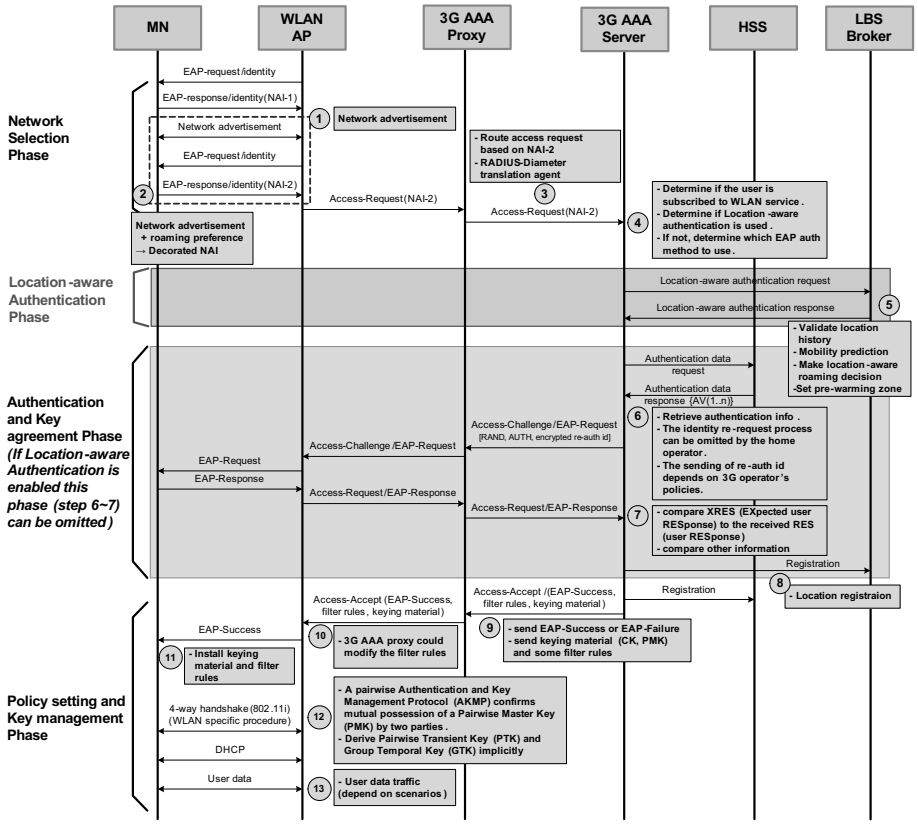


Fig. 4. Location-aware Secure Roaming procedure from UMTS to WLAN

6 Experimental Results

In order to test our location-aware secure roaming in 4G networks, we created the testbed shown in Figure 5. We consider UMTS AKA and EAP-AKA for 3G/WLAN interworking. We also consider WLANs authenticate a MN according to the IEEE 802.1x and IEEE 802.11i standards which use EAP-TLS and EAP-TTLS. Table 2 summarizes the base parameters underlying the performance experiments. LBS Broker and LBS 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 with Linux O/S and the modified FreeRADIUS library for RADIUS functionality. The cryptographic library is OpenSSL 0.9.7a and SAML Library is OpenSAML 0.9.1.

Figure 6 and 7 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. The solid curves represent the measurements without our location-aware scheme and the dotted curves repre-

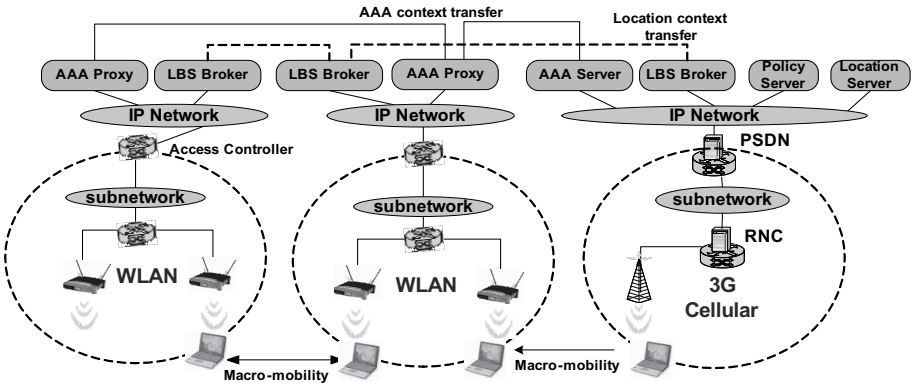


Fig. 5. Testbed of the Location-aware Security Architecture for UMTS/WLAN interworking

Table 2. Simulation Parameters of the Testbed of Location-aware Secure Roaming

Entity	Operation	Description	Performance
MN-AAA	802.1X full authentication (EAP-TLS)	Average delay	1,600ms
LBS Broker	Location history request to Location Server	Request location history of MN	50ms
LBS Broker	Location-aware authentication	Validation of location history of MN	80ms
LBS Broker	SAML Authorization Request	XML Parsing & RSA 1024 signature	27.4 ms
LBS Policy Authority	SAML Authorization Response	XML Parsing & RSA SHA-1 1024 bit key signature verify	20.4 ms
LBS Policy Authority	SAML Authentication Token generation and response to MN	3DES Symmetric key encryption	7.702 MB/s
LBS Broker	Response with Location information	RSA encrypt on 512 bit keys	31.201 KB/s
MN-AP	802.11 scan (active)	Average latency	40 300ms
MN-AP	802.11 reassociation with IAPP	Average latency	40ms
MN-AP	Fast Handover(4-way handshake only)	Average delay	60ms
802.11/CDMA	TCP parameter adjustment	Average delay	5000ms
802.11/GPRS	TCP parameter adjustment	Average delay	20000ms
UMTS/802.11	Intradomain UMTS to WLAN Handover with EAP-SIM authentication	Average delay	9,300ms

sent our location-aware case. We notice an important difference between the existing authentication case and the location-aware secure 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 authentication methods. In the roaming case of Figure 6, the location-aware scheme with EAP-TTLS CHAP shows almost the same performance with roaming of EAP-TLS without location-aware scheme. The overhead of our location-aware scheme in UMTS-to-WLAN roaming is 9.54% in Figure 7. We should consider trade-off among QoS of location-aware services 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 trade-off between two extremes is one fundamental challenge in security design for location-aware computing.

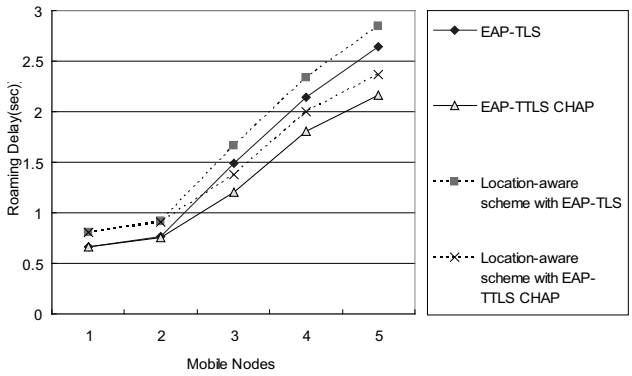


Fig. 6. Delay performance of Location-aware Secure Roaming from WLAN to WLAN

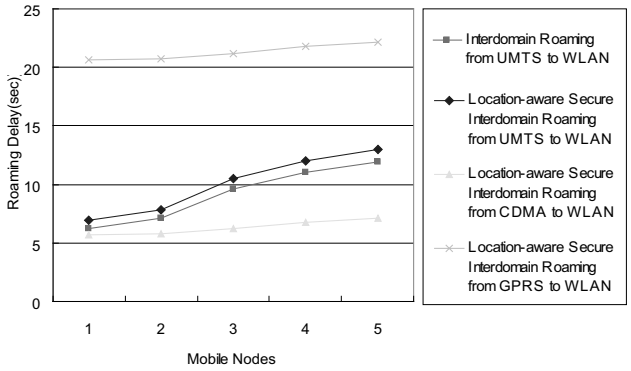


Fig. 7. Delay performance of Location-aware Secure Roaming from 3G to WLAN

7 Conclusions

We analyze mobility, interworking and security issues in location-aware computing and give our view on the future prospects for 3G/WLAN interworking. We introduce concepts of location-aware security and propose solution with several existing and new systems. The 3G/WLAN interworking system can be enhanced by new functionalities such as more advanced LBS service support by enabling efficient support of location-aware secure fast roaming with LBS Broker and location privacy policy control functions with LBS Policy Authority. This integrated scheme could provide the desired security features and requirements for survivable heterogeneous wireless networks. A testbed has been developed and experimental results of the secure handover have been presented. The proposed location-aware handover mechanism is currently being integrated with our secure Web Services infrastructure and 3GPP/WLAN interworking systems [2, 17].

References

1. Mike Hazas, et. al: Location-Aware Computing Comes of Age. IEEE Computer, Feb. 2004.
2. Minsoo Lee, Jintaek Kim, Sehyun Park, Jaeil Lee and Seoklae Lee: A Secure Web Services for Location Based Services in Wireless Networks. Lecture Notes in Computer Science, vol. 3042. May, 2004, pp. 332-344.
3. 3GPP TR 22.934: Feasibility Study on 3GPP System to WLAN Interworking,R6.
4. Feng, V. W.-S., et. al: WGSN: WLAN-based GPRS Environment Support Node with Push Mechanism. The Computer Journal, vol. 47, 2004. pp. 405-417.
5. A. K. Salkintzis:Interworking Techniques and Architectures for WLAN/3G Integration toward 4G Mobile Data Networks.IEEE Wireless Communications,June 2004.
6. D. E. Denning and P. D. MacDoran: Location-Based Authentication: Grounding Cyberspace for Better Security. Computer Fraud and Security, February 1996.
7. Jakob E. Bardram, et. al: Context-Aware User Authentication-Supporting Proximity-Based Login in Pervasive Computing. UbiComp'03, 2003.
8. Petri Mähönen, et. al: Hop-by-Hop Toward Future Mobile Broadband IP. IEEE Communications Magazine, March 2004.
9. Akyildiz, I.F., et. al.: A survey of mobility management in next-generation all-IP-based wireless systems. IEEE Wireless Communications, Aug. 2004.
10. McNair, J. Fang Zhu: Vertical handoffs in fourth-generation multinetwork environments. IEEE Wireless Communications, June 2004.
11. Christian Prehofer, et. al: Active Networks for 4G Mobile Communication: Motivation, Architecture and Application Scenarios. LNCS, vol. 2546. 2004.
12. R. Chellappa-Doss, A. Jennings and N. Shenoy: User Mobility Prediction in Hybrid and Ad Hoc Wireless Networks. ATNAC, Dec. 2003.
13. 3GPP TS 23.234 v6.0.0:3G System to WLAN Interworking;System Description,R6.
14. 3GPP TS 23.271:Functional stage 2 description of Location Services(LCS)",R6.
15. 3G TS 33.234 v050: 3G Security;Wireless Local Area Network(WLAN) Interworking Security.R6.
16. Koien, G.M.; Haslestad, T: Security aspects of 3G-WLAN interworking. IEEE Communications, November 2003.
17. Minsoo Lee, Jintaek Kim, Sehyun Park, Ohyoung Song and Sungik Jun: A Location-Aware Secure Interworking Architecture Between 3GPP and WLAN Systems, accepted for publication in Lecture Notes in Computer Science, Proc. ICISC 2004, Dec 2004.
18. Nicolas Montavont, et al:Handover Management for Mobile Nodes in IPv6 Networks.IEEE Communications, August 2002.
19. K. Daniel Wong, et. al: Mobility Management Scheme for Auto-configured Wireless IP Networks. IEEE Wireless Communications, October 2003.
20. Qi He, et. al: The Quest for Personal Control Over Mobile Location Privacy. IEEE Communications, May 2004.
21. MARCO GRUTESER et. al: Protecting Privacy in Continuous Location-Tracking Applications. IEEE SECURITY & PRIVACY, March-April 2004.
22. Alastair R. Beresford and Frank Stajano: Location Privacy in Pervasive Computing. IEEE PERVASIVE computing, Jan-Mar 2003.
23. Marques, V. et. al: An IP-based QoS architecture for 4G operator scenarios. IEEE Wireless Communications, June 2003.
24. Minghui Shi, et al: IEEE 802.11 roaming and authentication in wireless LAN/cellular mobile networks. IEEE Wireless Communications, Aug 2004.