Predictive Mobility Support with Secure Context Management for Vehicular Users*

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

1 School of Electrical and Electronics Engineering,
Chung-Ang University, 221, Heukseok-dong, Dongjak-gu, Seoul, 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@etri.re.kr

Abstract. This paper presents a predictive mobility management framework with the secure context management in mobile networks. We devised the authentication method for seamless handovers that exploit the knowledge of the mobility prediction. Previous Access Router (AR) forwards the pre-established context information to the new AR in the predicted target wireless cell where MN might move in the near future. Therefore the context for autonomous services is available in the right place at right time.

1 Introduction

In the vision of 4G networks the demand for telematics applications in smart vehicles will rise steeply over the next few years with navigation services, emergency call, real-time multimedia services, and becoming increasingly popular choices among motorists [1]. Seamless security, mobility and QoS management are therefore required for mobile users in vehicles, often equipped with several wireless network technologies, for example, wireless local area networks (WLANs), 3G cellular networks and wireless metropolitan area networks (WMANs).

The ability to provide seamless security QoS is the key to the success of autonomous services in 4G networks and ubiquitous computing. There has been a considerable amount of QoS research recently. However, the main part of this research has been in the context of individual architectural components, and much

* 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

less progress has been made in addressing the issue of an overall QoS architecture for the mobile Internet [2].

Another major challenge for seamless mobility is the creation of a secure vertical handover protocol: a secure handover protocol for users that move between different types of networks [3].

The seamless communication environments require a variety of context such as user identity, time of day, date or season, current physical location, mobility patterns and whether the user is driving or walking. However, the context information is difficult to manage, because the amount of the context information can be enormous and location dependent.

When the handover occurs in the most of mobile networks, the Mobile Node (MN) and the access router (AR) need to exchange security information. This process is time-consuming and creates a significant amount of signaling. To minimize the conversation over the wireless link, context transfer mechanism could be one solution [4, 5, 6, 7, 8].

This paper presents a secure context management scheme minimizing the signaling overhead. Previous AR forwards the pre-established AAA information to the new AR in the predicted target wireless cell where MN might move in the near future. Therefore the context for autonomous services is available in the right place at right time. We also designed the detailed context transfer procedure for secure telematics applications.

The rest of this paper is organized as follow. Section 2 describes the fast handover with the predictive mobility support in mobile networks. Section 3 suggests our secure context management framework for vehicular users in mobile networks. Section 4 describes the performance analysis of our framework through a closed queuing network model. Section 5 concludes this paper.

2 Mobility-aware Fast Handover with Context Transfer in Mobile Networks

Primary motivation of context transfer protocol with mobility prediction is to quickly re-establish context transfer candidate services without requiring the MN to explicitly perform all protocol flows for seamless security services.

However, context transfer may not always be the best solution for re-establishing services on a new subnet. There are some issues as following:

* Router compatibility: Context transfer between two routers is possible only if the receiving router supports the same context transfer-candidate services as the sending router. This does not mean that the two nodes are identical in their implementation, nor does it even imply that they must have identical capabilities.

* Requirement to re-initialize a service from scratch: There may be situations where either the device or the access network would prefer to reestablish or re-negotiate the level of service.

* Suitability for the particular service: Context transfer assumes that it is faster to establish the service by context transfer rather than from scratch.

These limitations should be taken into account in the design considerations of seamless mobility solutions.

As the predictive mobility support for vehicular users we designed Location Predictor (LP). LP performs mobility prediction both for micro movement in a cell and for macro movement between cells (Figure 1). LP request current time, destination information and movement patterns of the user from the Location History DB. For the micro movement prediction, LP performs the local prediction using location history of the user and the current user mobility. As the macro movement prediction, LP sets cell sequence and the next context transfer zones using road segments, road sequence and handover segments.

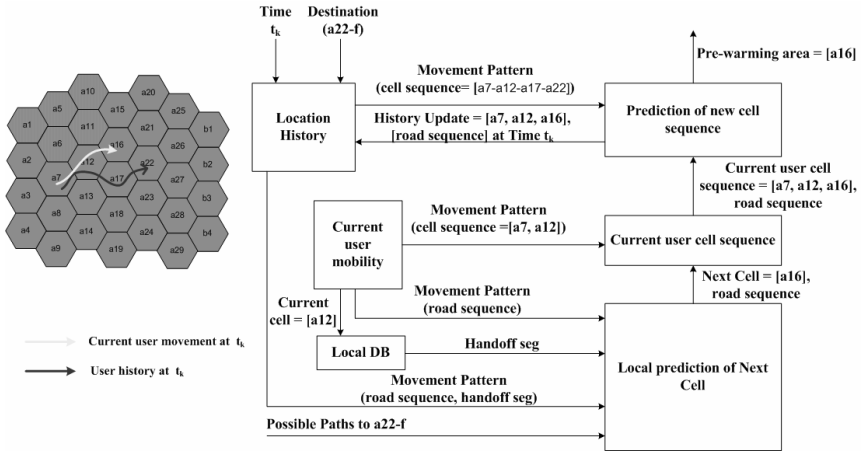

Fig. 1. Mobility Prediction using User Movement Patterns

3 Mobility-aware Security Context Management Framework for Autonomous Services

Figure 2 shows our predictive mobility management with secure context management for vehicular users. MN performs full authentication for initial login in core network (CN) where stores registration data for users after network selection procedure.

At this time, mobile user may configure user specific information such as destination, user applications and downloaded telematics services. After that, AAA context including cipher key is installed in current AR and MN gets GPS-based real-time location information and receives handover road segments and its coordination periodically from Location Manager. Mobile user who moves by car predicts next cell(s) through Mobile Manager inside the vehicle or within the mobile terminal, and transmits the next Context Transfer Zones Indication (CTZI) to Location Manager at appropriate time.

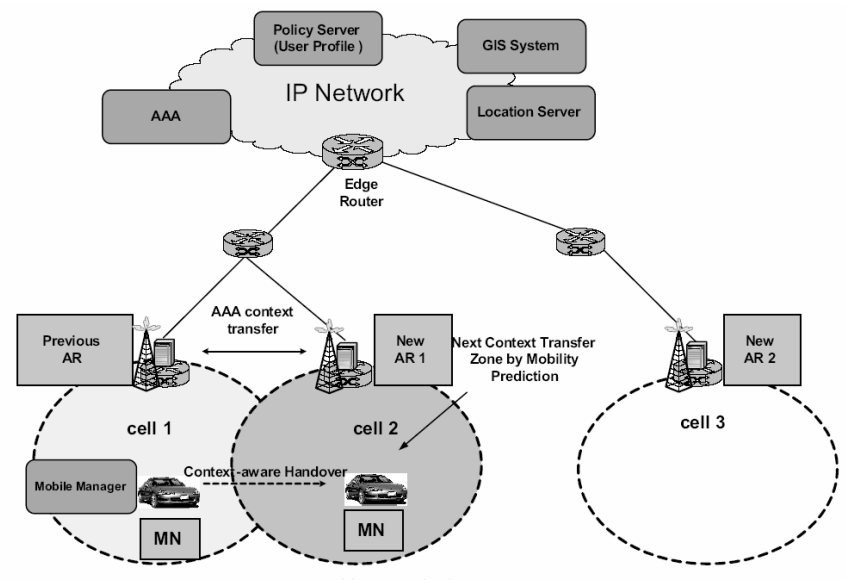

Fig. 2. Predictive Mobility Support for Vehicular Users

Location Manager which received CTZI from MN sends a Context Transfer Activate Request (CTAR) message as a context transfer triggering that causes the current AR to transfer AAA context. New AR installs AAA context and waits for the MN's CTAR message within time bound. If the MN transfers CTAR message to new AR with authorization token during handover, New AR sends success message to the MN if token verification is successful.

Mobile Manager may be built inside a vehicle typically. It predicts next cell(s) using real-time location data and mobility prediction application, and determines the next context transfer zones at appropriate time. Location Manager plays a role of context transfer trigger in the proposed architecture. It also monitors all MN's movements and maintains handover road segments and their coordination in its local DB. While a Location Manager interoperates all MNs in an administrative domain, it mediates AAA context transfer among ARs.

If the mobility prediction is correct, MN performs secure context-aware handover procedure. However, if it is failure, the MN can complete the handover using general context transfer.

4 Performance Analysis

We analyzed the performance of our context-aware handover scheme in the simulation environment as shown in Figure 3. We assumed that each router guarantees router compatibilities for context transfer and context transfer between

two routers is possible only if the receiving router supports the same context transfer-candidate services as the sending router.

In the scenario of Figure 3, the context-aware handover procedure has three job classes; the context transfer zone setup step and two main steps according as it is successful or failure. If mobility prediction is successful, MN performs context-aware handover procedure. However, if the mobility prediction is failure, it is possible to use general context transfer protocol. We have modeled and tried to solve our architecture as a closed queuing system for the proposed protocol as in Figure 3 and Table 1.

We analyzed of approximate Mean Value Analysis (MVA) as described in [9, 10]. $r_{im,jn}$ means the probability that a class m job moves to class n at node j after completing service at node i. p represents a probability of the mobility prediction accuracy.

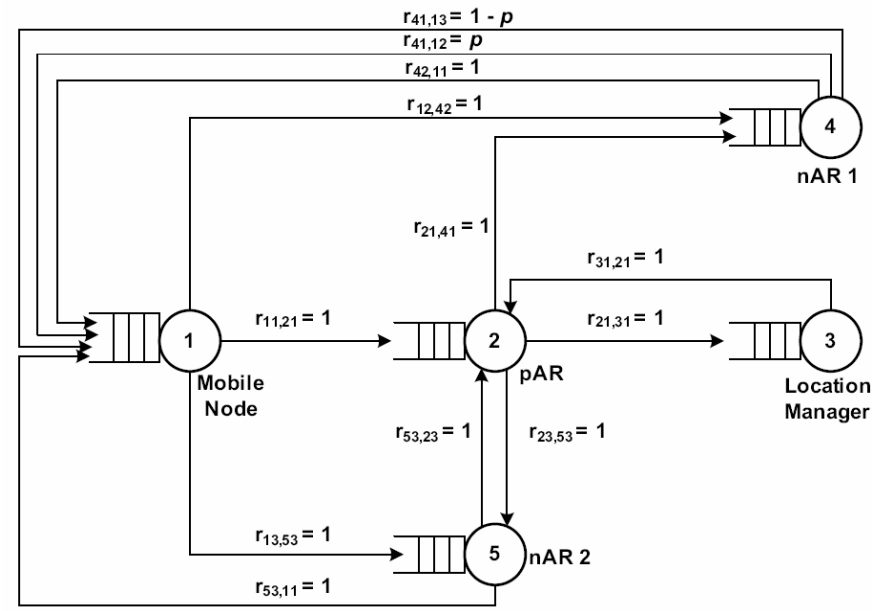

Fig. 3. The Testbed of the Predictive Mobility Support Scenario

Table 2 summarizes the basic parameter settings underlying the performance experiments. Location Manager and ARs used Solaris 8 machine with Pentium III 933 MHz, 512 MB RAM. MN used Pentium III 800 MHz, 256MB RAM, Windows XP operating system with Lucent Orinoco IEEE 802.11b wireless LAN card. The cryptographic library was OpenSSL 0.9.7c [11], and data size was 1KB in token verification and 10 KB in context transfer.

Table 1. The number of operations at each queue and class

Class	Pre-warming step (class 1)	Location-aware step (class 2)	Context-transfer step (class 3)
Mobile node (node 1)	1 location prediction indication	1 CTAR	1 CTAR
pAR (node 2)	2 forwarding (indication, context)	0	1 token verification 1 forwarding (context)
Location Manager (node 3)	1 forwarding (CT Trigger)	0	0
nAR 1 (node 4)	1 install context	1 token verification	0
nAR 2 (node 5)	0	0	1 CT-Req forwarding 1 install context

Table 2. Basic parameters for setting the queuing network model

Entity	Operation in scenario	Performance
Mobile Node	Context Transfer Indication with authorization token	30.34 ms
Location Manager	Context transfer trigger with authorization token	27.4 ms
pAR	Context transfer with token parameter	30 ms
Mobile Node	CTAR with authorization token	30 ms
nAR 2	CT-Req with authorization token	27.4 ms
pAR	Context transfer	30 ms

Figure 4 describes the authentication latency for each case after the handover events at layer 2. Our method sets up AAA context in advance before the handover events and only performs token verification if the mobility prediction is successful. Therefore, MN experiences low latency relatively when it uses our secure context-aware handover protocol with high mobility prediction accuracy.

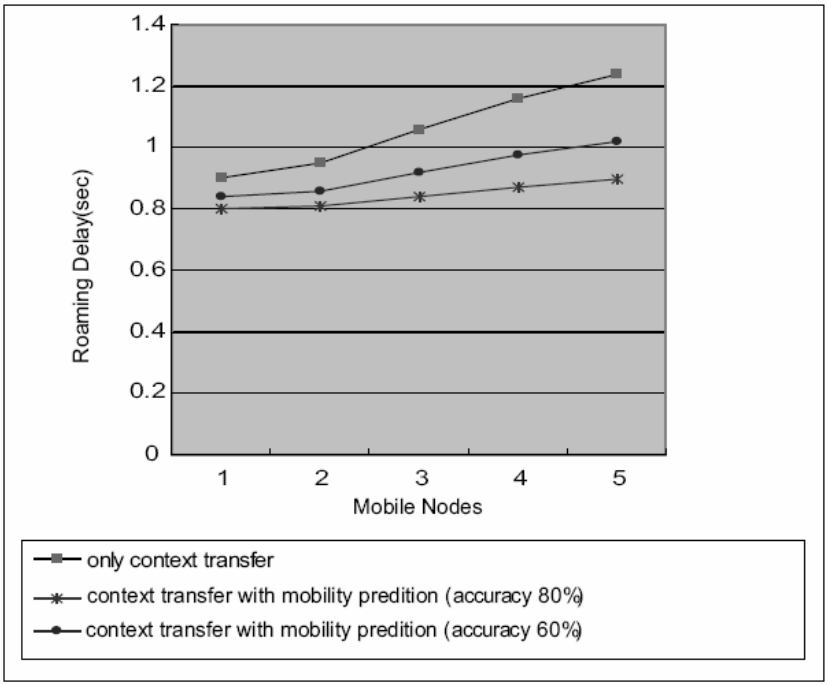

Fig. 4. Authentication delay of context-aware handover

5 Conclusions

In this paper, we proposed a mobility-aware handover scheme to minimize the signaling overhead during the handover procedure in the future mobile networks. We designed a Mobile Manager to effectively provide the seamless mobile services with the context transfer and the mobility prediction for fast re-authentication. To minimize the signaling overhead after the handover events at layer 2, we propose an efficient context transfer mechanism between Mobile Managers, providing the context is available in the right place at right time. Previous AR forwards the AAA pre-established information to the new AR of the predicted wireless cell where MN might move in the near future. Simulations of our context-aware handover performance gave a good insight into the current excitation. The proposed mobility-aware mechanism is being integrated with secure Web Services infrastructure [12] and the new interworking systems [13, 14].

References

[1] Leelaratne, R., Langley, R.: Multiband PIFA vehicle telematics antennas. Vehicular Technology,IEEE Transactions on, vol. 54, issue 2, March 2005 pp.477-485.

[2] Xio Gao, GangWu, Miki, T.: End-to-end QoS provisioning in mobile heterogeneous networks. IEEE Wireless Communications, vol. 11, issue 3, June 2004 pp.24-34.

[3] McNair, J., Fang Zhu: Vertical handovers in fourth-generation multinetwork environments. IEEE Wireless Communications, vol. 11, issue 3, June 2004 pp:8-15.

[4] J. Loughney: Context Transfer Protocol. Seamoby Working Group, Internet Engineering Task Force, draft-ietf-seamoby-ctp-11.txt

[5] Christos Politis, Kar Ann Chew, Nadeem Akhtar, Michael Georgiades and Rahim Tafazolli: Hybrid Multilayer mobility management with AAA context transfer capabilities for All-IP networks. IEEE Wireless Communications, Aug 2004

[6] J.Kempf: Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network. RFC 3374, Internet Engineering Task Force.

[7] Tim Ruckforth, Jan Linder: AAA Context Transfer for Fast Authenticated Interdomain Handover. Swisscom SA, Mar 2004

[8] Juan M. Oyoqui, J. Antonio Garcia-Macias: Context transfer for seamless micromobility. IEEE ENC' 03, 2003

[9] Boudewijn R. Haverkort John: Performance of Computer Communication Systems : A Model-Based Approach' , Wiley & Sons, October 1999.

[10] Gunter Bolch, Stefan Greiner, Kishor Trevedi: A Generalized Analysis technique for queueing networks with mixed priority strategy and class switching. Technical Report TR-I4-95-08, Oct. 1995.

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

[12] 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.

[13] Minsoo Lee, Jintaek Kim, Sehyun Park, Ohyoung Song and Sungik Jun, A Location-Aware Secure Interworking Architecture Between 3GPP and WLAN Systems, Lecture Notes in Computer Science, vol. 3506, May 2005, pp. 394-406.

[14] Minsoo Lee, Gwanyeon Kim, and Sehyun Park: Seamless and Secure Mobility Management with Location Aware Service (LAS) Broker for Future Mobile Interworking Networks, JOURNAL of COMMUNICATIONS and NETWORKS, vol. 7, no. 2, JUNE 2005, pp. 207-221.