Dynamic Fast Authentication and Authorization during Inter-domain Mobility

Zhikui Chen
School of Software, Dalian University of Technology
Dalian, Liaoning, China
zkchen@dlut.edu.cn

Xiaodi Huang
School of Business and Information Technology, Charles Sturt University
Albury, NSW 2640, Australia
xhuang@csu.edu.au

***Abstract*—Mobile technologies made their headway by offering more flexibility to end-users and improve the productivities. Many businesses have quickly adopted them so as to gain and sustain a competitive edge, especially in global roaming. Within the application of ubiquitous access and pervasive communication, security, privacy and QoS becomes a critical issue during global mobility, particularly in getting smooth and seamless mobile services by decreasing handover latency. Based on single sign on and the context transfer protocol, this paper proposes a dynamic fast authentication and authorization scenario during inter-domain mobility, that can save one trip communication time consummation between administrative domains.**

Keywords- inter-domain mobility, authentication, authorization, single sign on, VID

I. INTRODUCTION

In today's fast expanding and dynamic marketplace, the emergence of mobility technologies has revolutionized our global village. The benefits of mobility are of many folds. Mobile technologies made their headway by offering more flexibility to end-users and improve the productivity. Many businesses have quickly adopted them so as to gain and sustain a competitive edge. While mobility technologies and applications are clearly becoming an essential part of our daily life and business strategies, it is of utmost importance for professionals to stay relevant and equipped with up-to-date technical competencies, in order to meet the competitiveness of the global economy successfully.

Generally, there are several types of mobility as described below:

a) User mobility, a user can access the network from multiple devices, in which the user actually is able to connect and act in a seamless way from all communication mobile terminals.

b) Device mobility, a device can change its attachment point to the network, which handles mobility of network access sessions between different access networks. When re-authentication is necessary, the change from one network access session to another would also be considered as terminal mobility (but may not be considered seamless and may break running sessions).

c) Interface mobility, a session can be moved from one interface to another in the same device. Network access session mobility would be a change of the network access session from one network interface to another or to move the network access session to another device. This can be supported by the network access provider through multihoming support.

d) Service mobility, the provider of a service can be moved during the provision of that service.

e) Session mobility, an on-going session can be moved between devices. This last characteristic is especially flexible if the session uses SIP as the signaling protocol, which can be related to mobility of application sessions and pervasive sessions with associated streams and network connections. Since application and pervasive sessions are composed of sub-sessions and services that use multiple network access sessions, session mobility has many aspects, and may cover several above-mentioned mobility types: 1) partial session mobility: either signaling/control or contained connections/streams move; 2) multihoming: part of a session moves from one to another network interface;3) multi-device: part of a session moves from one device to another device: 4) full session mobility: the whole session moves from one device to another including signaling; 5) Service mobility: part of a composed service moves from one to another network interface of a device (could be 3rd-party service or service on terminal); part of a composed service moves from one device to another device (could be 3rd-party service or service on terminal) and when moving to another domain a similar service is used in that domain or when the user, personalization, or context indicates a service can be replaced by another with similar. Parts of this mobility features require specific signaling protocols to operate, such as SIP, or distributed support from the Pervasive Platform.

All of these mobility interactions among network inter/intra-domains require the securely and credibly exchange of terminal, session and some personal data. In other words, during mobility, the terminal, session and user should be authenticated and authorized in the new domain. The required authentication and authorization are normally based on an identity management. This paper describes a fast authentication and authorization during inter-domain mobility, based on a virtual digital identity concept (VID), which was proposed in a European 6th framework project—Daidalos [1].

Generally, a Digital Identity Management Infrastructure

978-1-4244-2108-4/08/$25.00

provides management of miscellaneous digital identifiers including both users/persons and devices/entities in the telecommunications network. This is analogous to the identity card system in the real world, which is the infrastructure for public security applying to all people in a country regardless of their occupations sex, ages, social roles, and business roles etc. On the other hand, using digital identifiers for tracing back to a network attacker may be useful for information and network security in the cyber world.

The crucial requirement of the mobile communication in the ubiquitous environment is how to dynamically protect user personal privacy information securely in a mobility environment. It is obvious that such systems will have access to confidential personal information in order to adapt according to the user's personal situation. For achieving privacy, users must be aware of how and where personal data are processed and used during roaming among different administrative domain. Furthermore, users must be confident that they are interacting with genuine providers. In such a dynamic pervasive system, how to ensure continuity of the conversation during handover between different network operators must be efficiently resolved, which two operators locate in the different continent, maybe far remote physically. Therefore, key challenges towards the development of a more consistent approach are to tackle the conflicting requirements of privacy, identification and security for the opened, distributed pervasive service[6].

In one word, future networks pose new challenges to service operators, service provisioning platform operators and access network operators by introducing multiple administrative domains and federations, as well as by introducing users having multiple identities and maintaining multiple sessions on different devices, here a federation seems a roaming agreement, more details, see [12].

The goal of this paper is to introduce a fast and securely scenario of authentication and authorization for mobile terminal mobility among different domains. Section 2 describes some inter-domain issues and its related fast handover technology. A fast dynamic authentication and authorization is introduced in section 3. Section 4 summarizes the paper.

II. RELEVANT INTER-DOMAIN MOBILITY ISSUES

Mobility is a critical aspect of the next generation mobile communication, namely 4G. There are three main issues regarding mobility management in 4G networks [13]:

The first issue deals with optimal choice of access technology, or how to be best connected. Given that a user may be offered connectivity from more than one technology at any one time, one has to consider how the terminal and an overlay network choose the radio access technology suitable for services the user is accessing. A handover algorithm should both determine which network to connect to as well as when to perform a handover between the different networks. Ideally, the handover algorithm would assure that the best overall wireless link is chosen. The network selection strategy should take into consideration the type of applications being run by the user at the time of handover. This ensures stability as well as optimal bandwidth for interactive and background services.

The second issue is about the design of a mobility enabled IP networking architecture, which contains the functionality to deal with mobility between access technologies. This includes fast, seamless vertical (between heterogeneous technologies) handovers (IP micro-mobility), quality of service (QoS), security and accounting.

The third issue concerns the adaptation of multimedia transmission across 4G networks. Indeed multimedia will be a main service feature of 4G networks, and changing radio access networks may in particular result in drastic changes in the network condition. Thus the framework for multimedia transmission must be adaptive.

A basic requirement of handover in different domains must satisfy the following three conditions: the handover is secure without disclosing privacy and breaking integrity of user's data; the handover is enough fast without packet loss; and the QoS with different federation classes in different domains, as shown in Fig. 1.

This paper focuses on a part of the second case, which is fast and secure mobility during interdomain handover. As

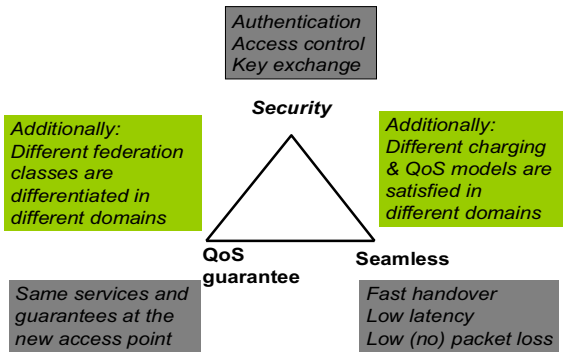

Fig. 1, Handover requirement in pervasive environment

secure mobility service is becoming a critical issue in the ubiquitous environment, the Mobile IP Working Group in IETF is preceding the research about it. If it provides weak security features to the mobile service, then the Mobile IPv6 will not be trusted. Although the IPSec (Internet Protocol Security) and RR (Return Routability) was selected to provide security supports and related work have been obligated, these approaches have drawbacks in that the hand-held devices such as cellular phones and PDAs are battery-powered so that the security processing is a big burden and security feature is not relatively abundant. Based on Daidalos, this paper attempts to find one of such desired fast and securely authenticate and authorization solutions in a ubiquitous environment using VID during inter-domain mobility, which includes network mobility and terminal mobility.

III. PROPOSED SCENARIO

In the Daidalos project, device mobility is impacted by the Virtual Identity concept, as mentioned above. Following the VID framework specifications, mobility should be regarded not anymore as a pure device mobility issue, rather as a mean of providing mobility to identities for a network access session. In this sense VID-specific network access sessions become mobile. This would be called the traditional host mobility when it is related to changing network access on one interface. Using the VID concept, the proposed fast handover scheme at access router is based on RFC4068, which proposed fast handover for Mobile IPv6 [4]. RFC describes the protocol operations for a mobile node by which to maintain connectivity to the Internet, during its handover from one access router to another. These operations involve movement detection, IP address configuration, and location update, as shown in Fig.2.

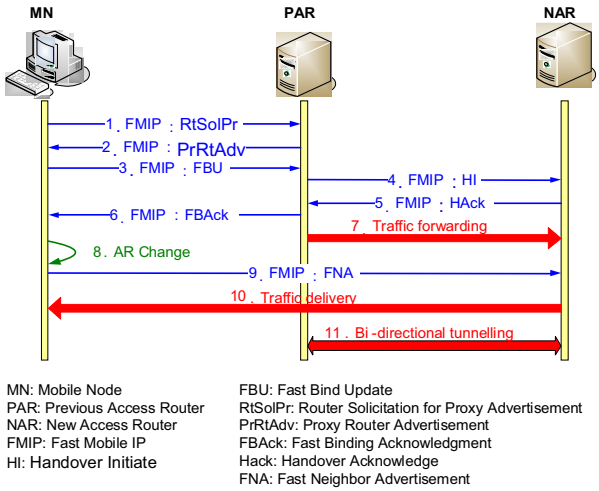

Fig. 2 Fast handover for Mobile IPv6

The introduced fast dynamic authentication and authorization scenario is implemented after the handover decision is made. When the handover decision is made by mobile terminal (namely terminal initiated handover) or access network (namely network initiated handover) according to the received signal strength, for example, the mobile terminal or old access router provides some credentials, which will be transferred to the new inter-domain access router using handover context transfer protocol—RFC4067[2]. The new AR delivers them to the new inter-domain A4C server, which forwards them to the home A4C server using Diameter protocol—RFC3588 [3]. The home A4C checks them, and sends the result back to the new inter-domain A4C and then to the attendant (mobile terminal or access router). Based on single sign on (SSO) and SAML protocol, if all credentials are successfully verified, the service will continue; otherwise the service will be denied and re-authentication and re-authorization are needed. But this process may cause some latency due to signaling communication between different inter-domains. This single thread handoff process will consume much time. Figure 2 shows this authentication and authorization process.

To reduce the signaling transport latency, we propose a multiple-threads approach to signaling transport scenario, using SSO and SAML technology. During a conversation, a mobile node or the user's authenticated and authorized data is stored in the user's home domain, such as QoS agreement and VID credential. During handover this scenario uses the federation concept [12], in which handover between two foreign domains are federated. When a handoff decision is made, one thread transfers context information from the old access router to the new access router. Another thread is in current foreign domain which asks VID credential (ID Token) from user's home domain to the new foreign domain. Finally, the third thread contacts the QoS broker to verify the QoS level under federation class. The process is illustrated in Fig.

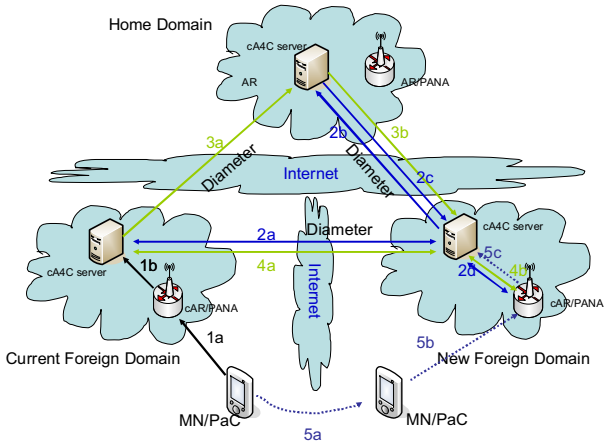

Fig. 3, Proposed fast Handover scenario

3, where QoS signaling is not described in the figure. The details of this approach are described below.

The basic idea is as follows: when L2 triggers handover and new foreign domain is found, the old AR will send a message to Home domain via current foreign A4C domain in order to request the VID information with a timestamp. This information will be sent to the new foreign domain (this process depends on federation classes). Then the VID credential will be verified locally in order to reduce the handover latency. When handover failed within a given time, which is specified in timestamp, the VID credential will be automatically destroyed. If handover is successful, the VID credential will be destroyed immediately. The terminal VID information will be transferred to the new domain using CXTP. For example, you are a subscriber of DT (Deutsch TeleKom), such a handover between different domains could be faster than that using the current method when you are in USA or Asia. The transferred VID information of MN (Mobile Node) will be delivered from the new foreign domain to Home domain for verification. During this process, such a long distance routing may consume many milliseconds.

It is obvious in Fig.3 that a handover has four communications among different domains. Using the traditional method, the path should be 2a-2b-2c-2a (here we only consider the communications among A4C servers). The proposed scheme, however, has only three communications among different domains, because communication 3a and first 4a are parallel. This can save one trip communication time. Fig.4 describes its signaling chart, in which the diameter protocol is used for communication between different

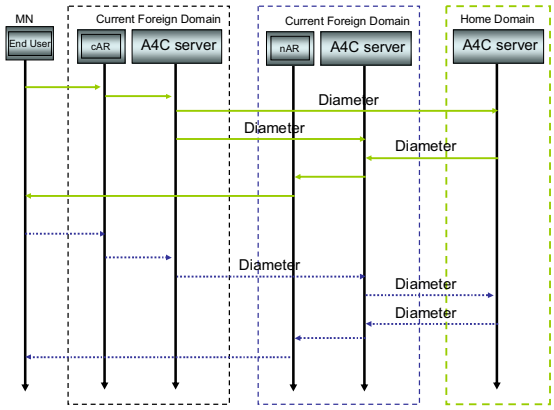

Fig. 4, Signalling chart of proposed scenario

domains.

The proposed mobility scheme considers the splitting of the architecture in local and global domains - each one associated to administrative domains. Global domains are typically identified with the home operator domain, retaining most of the information related to users' profiles. Implementations of such global domains should provide global reachability by means of protocols such as Mobile IPv6 or HIP (Host Identity Protocol). Obviously, the proposed multiple-threads method is much suitable for global mobility.

Local domains are associated in the Daidalos architecture with Internet Service Provider (ISP) or Network Access Provider (NAP). ISP or NAP provides network access and mobility services independently of the global domain, and interconnected to them (through at least one router, called LMA). This concept allows ISPs and NAPs to implement their preferred local mobility scheme in a manner that is reasonably independent of the global mobility management scheme and completely transparent to the end users.

The proposed scenario is different from pre-authentication. The author of [14] describes an extension to the PANA protocol used for proactively executing EAP authentication and for establishing a PANA SA (Security Association) between a PaC (PANA Client or mobile node) in an access network and a PAA in another access network to which the PaC may move. If the PaC is a mobile device and is capable of moving one access network to another while running its applications, it is critical for the PaC to perform a handover seamlessly without degrading the performance of the applications during the handover period. When the handover requires the PaC to establish a PANA session with the PAA in the new access network, the signaling to establish the PANA session should be completed as fast as possible.

The proposed scenario is similar to the context transfer scheme, but it is faster than the context transfer technology.

IV. RESULTS

This paper has described a fast handover scenario based on the context transfer protocol, which moves the VID credential verification from home domain to new foreign domain. In other words, the VID credential's verification is done in the new foreign domain, rather than in user's home domain. In this way, the time consummation of one trip could be saved, so that the time of authentication and authorization during inter-domain mobility is shortened.

In order to quantify the saved time, our future work will simulate the proposed scenario using some simulation tools such as OMNET++ and NS-2.

ACKNOWLEDGMENT

The work presented in this paper was partially funded by Dalian University of Technology.

REFERENCES

[1] European FP6 IST project Daidalos (Nov.2003-Dec.2008): http://www.ist-daidalos.org.

[2] J. Loughney, Ed., Context Transfer Protocol (CXTP), RFC4067, July 2005.

[3] P. Calhoun, etc., Diameter Base Protocol, RFC3588, Sept. 2003.

[4] R. Koodli, Ed., Fast Handovers for Mobile IPv6, July, 2005.

[5] R.L. Aguiar,; J. Jaehnert,; A.F. Gomez Skarmeta,; C., Hauser, "Identity Management in Federated Telecommunications Systems". Proceedings of the Workshop on Standards for Privacy in User-Centric Identity Management 2006, Zurich, 2006.

[6] B. Weyl, P. Brandao, A. F. Gomez Skarmeta, R. M. Lopez, P. Mishra, C. Hauser, H. Ziemek, "Protecting Privacy of Identities in Federated Operator Environments", IST- 14th Wireless Mobile Summit 2005.

[7] Z. Chen, "A Scenario for Identity Management in Daidalos," Proceedings of IEEE CNSR2007, May 2007.

[8] R. M. Bahat, M. A. Bauer, E. M. Vieira and O.K. Baek, "Using Policies to Drive Autonomic Management", In Proceedings of the 2006 international Symposium on World of Wireless, Mobile and Multimedia Networks, International Workshop on Wireless Mobile Multimedia. IEEE Computer Society, Washington, DC, 475-479, June 2006.

[9] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry and S. Waldbusser, "Terminology for Policy-Based Management", RFC 3198

[10] E. Lupu, M. Sloman, N. Dulay and N. Damianou, "Ponder: Realising Enterprise Viewpoint Concepts", Fourth International Enterprise Distributed Object Computing Conference (EDOC'00), 2000.

[11] J. O. Kephart and W. E. Walsh, "An Artificial Intelligence Perspective on Autonomic Computing Policies", Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04), 2004.

[12] Z. Chen "Federated Dynamic Authentication and Authorization in Daidalos," Proceedings of IEEE NTMS2007, May 2007.

[13] Frederic Paint, Paal Engelstad, Erik Vanem, Thomas Haslestad, Anne Mari Nordvik, Kjell Myksvoll, Stein Svaet, "Mobility aspects in 4G Networks- White Paper

[14] Yoshihiro Ohba, "Pre-authentication Support for PANA", http://www.ietf.org/internet-drafts/draft-ietf-pana-preauth-02.txt, Nov. 2007.