52. IWK

Internationales Wissenschaftliches Kolloquium

International Scientific Colloquium

PROCCEDINGS | 10 - 13 September 2007

FACULTY OF COMPUTER SCIENCE AND AUTOMATION

COMPUTER SCIENCE MEETS AUTOMATION

VOLUME II

Session 6 - Environmental Systems: Management and Optimisation

Session 7 - New Methods and Technologies for Medicine and Biology

Session 8 - Embedded System Design and Application

Session 9 - Image Processing, Image Analysis and Computer Vision

Session 10 - Mobile Communications

Session 11 - Education in Computer Science and Automation

TECHNISCHE UNIVERSITÄT ILMENAU

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der deutschen Nationalbiografie; detaillierte bibliografische Daten sind im Internet über **http://dnb.ddb.de** abrufbar.

ISBN 978-3-939473-17-6

Impressum

Herausgeber:	Der Rektor der Technischen Universität Ilmenau Univ.-Prof. Dr. rer. nat. habil. Peter Scharff
Redaktion:	Referat Marketing und Studentische Angelegenheiten Kongressorganisation Andrea Schneider Tel.: +49 3677 69-2520 Fax: +49 3677 69-1743 e-mail: kongressorganisation@tu-ilmenau.de
Redaktionsschluss:	Juli 2007
Verlag:	Technische Universität Ilmenau/Universitätsbibliothek Universitätsverlag Ilmenau Postfach 10 05 65 98684 Ilmenau www.tu-ilmenau.de/universitaetsverlag
Herstellung und Auslieferung:	Verlagshaus Monsenstein und Vannerdat OHG Am Hawerkamp 31 48155 Münster www.mv-verlag.de
Layout Cover:	www.cey-x.de
Bezugsmöglichkeiten:	Universitätsbibliothek der TU Ilmenau Tel.: +49 3677 69-4615 Fax: +49 3677 69-4602

Preface

Dear Participants,

Confronted with the ever-increasing complexity of technical processes and the growing demands on their efficiency, security and flexibility, the scientific world needs to establish new methods of engineering design and new methods of systems operation. The factors likely to affect the design of the smart systems of the future will doubtless include the following:

- As computational costs decrease, it will be possible to apply more complex algorithms, even in real time. These algorithms will take into account system nonlinearities or provide online optimisation of the system's performance.
- New fields of application will be addressed. Interest is now being expressed, beyond that in "classical" technical systems and processes, in environmental systems or medical and bioengineering applications.
- The boundaries between software and hardware design are being eroded. New design methods will include co-design of software and hardware and even of sensor and actuator components.
- Automation will not only replace human operators but will assist, support and supervise humans so that their work is safe and even more effective.
- Networked systems or swarms will be crucial, requiring improvement of the communication within them and study of how their behaviour can be made globally consistent.
- The issues of security and safety, not only during the operation of systems but also in the course of their design, will continue to increase in importance.

The title "Computer Science meets Automation", borne by the 52nd International Scientific Colloquium (IWK) at the Technische Universität Ilmenau, Germany, expresses the desire of scientists and engineers to rise to these challenges, cooperating closely on innovative methods in the two disciplines of computer science and automation.

The IWK has a long tradition going back as far as 1953. In the years before 1989, a major function of the colloquium was to bring together scientists from both sides of the Iron Curtain. Naturally, bonds were also deepened between the countries from the East. Today, the objective of the colloquium is still to bring researchers together. They come from the eastern and western member states of the European Union, and, indeed, from all over the world. All who wish to share their ideas on the points where "Computer Science meets Automation" are addressed by this colloquium at the Technische Universität Ilmenau.

All the University's Faculties have joined forces to ensure that nothing is left out. Control engineering, information science, cybernetics, communication technology and systems engineering – for all of these and their applications (ranging from biological systems to heavy engineering), the issues are being covered.

Together with all the organizers I should like to thank you for your contributions to the conference, ensuring, as they do, a most interesting colloquium programme of an interdisciplinary nature.
I am looking forward to an inspiring colloquium. It promises to be a fine platform for you to present your research, to address new concepts and to meet colleagues in Ilmenau.

Professor Peter Scharff
Rector, TU Ilmenau

Professor Christoph Ament
Head of Organisation

Table of Contents

C O N T E N T S

10 Mobile Communications

11 Education in Computer Science and Automation

52nd Internationales Wissenschaftliches Kolloquium
Technische Universität Ilmenau
10 – 13 September 2007

A. Diab / A. Mitschele-Thiel

MIFAv6: A Fast and Smooth Mobility Protocol for IPv6

ABSTRACT

In this paper we present Mobile IP Fast Authentication protocol for IPv6 (MIFAv6). MIFAv6 is developed to support a fast and smooth mobility in IPv6 networks. The Mobile Node (MN) needs to update its binding only at the new Access Router (AR) to be able to resume sending and receiving of data packets. The latency between the current AR and the Home Agent (HA) / Corresponding Node (CN) is hidden from the application and does not affect the performance. A main advantage of MIFAv6 is that it does not make any restrictions on the network topology.

I- INTRODUCTION

The growing demand for high-speed wireless access to the Internet anywhere and anytime are the driving forces resulting in the current trend to develop All-IP wireless networks. A common IP core is used to connect all wireless radio access networks and technologies. The radio gateways and MNs use IP protocol for signaling and data transport. However, an All-IP wireless network requires efficient and flexible mobility solutions, which can satisfy the requirements of delay sensitive applications.
Mobile IP version 4 (MIPv4) [1] and version 6 (MIPv6) [2] present the well known IETF standards used to support mobility in IP based networks. With MIP, the MN has to be registered and authenticated by the HA every time it moves from one subnet to another. This introduces communication latency when the MN is moving. This latency makes MIP only suitable for the management of global mobility, referred to as macro mobility too. Therefore, it is important to develop a new mobility solution able to overcome the shortcomings of MIP and to satisfy the real-time requirements.
The rest of this paper is organized as follows: The related work is presented in section (II). After that, we describe MIFAv6 in section (III). In section (IV) we conclude with the main results.

II- RELATED WORK

In order to avoid MIP drawback, several approaches have been proposed to support local, termed as micro, mobility. These approaches can be classified into two main groups [3], Proxy Agent Architectures (PAA) and Localized Enhanced Routing Schemes (LERS). PAA solutions try to extend MIP principle by using a hierarchical network architecture with intermediate agents to process the movements of MNs inside a certain domain locally. Regional Registration for MIPv4 [4] and Hierarchical Mobile IPv6 [5] are examples of this group. LERS solutions introduce a new dynamic layer3 routing protocol inside a certain localized area. A special path set-up protocol is used to implement per host soft-stat forwarding entries used to forward the packets towards the MNs. Cellular IP [6] and Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [7] are examples of this group.

In order to accelerate the layer3 handoff in macro or micro mobility solutions, some approaches propose the use of layer2 information to trigger the handoff on layer3. This information is called layer2 triggers. These triggers force the MNs to perform a layer3 handoff in advance and so the layer3 handoff latency can be minimized or even eliminated. The well known protocols that employ this principle are Fast MIPv6 [8], pre- and post-registration methods [9] and seamless MIP [10].

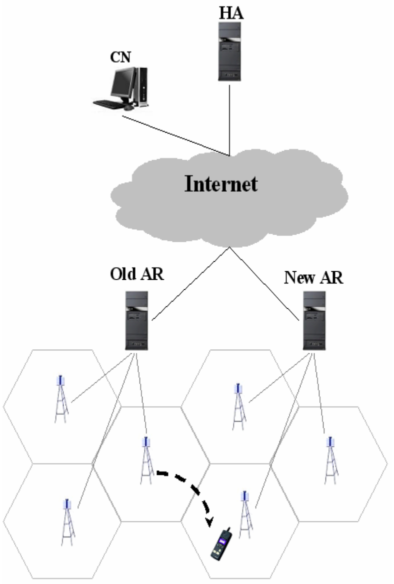
Another trend in developing mobility management solutions is currently obtaining a big interest. The researchers are trying now to realize network-based mobility management frameworks. In these frameworks the MN has a minimal support of mobility or even no support. The network should perform all the tasks related to the mobility on behalf of the MN. The well known example of these approaches is Proxy MIP [11]

III- MIFAV6: MOBILE IP FAST AUTHENTICATION PROROCOL FOR IP VERSION 6

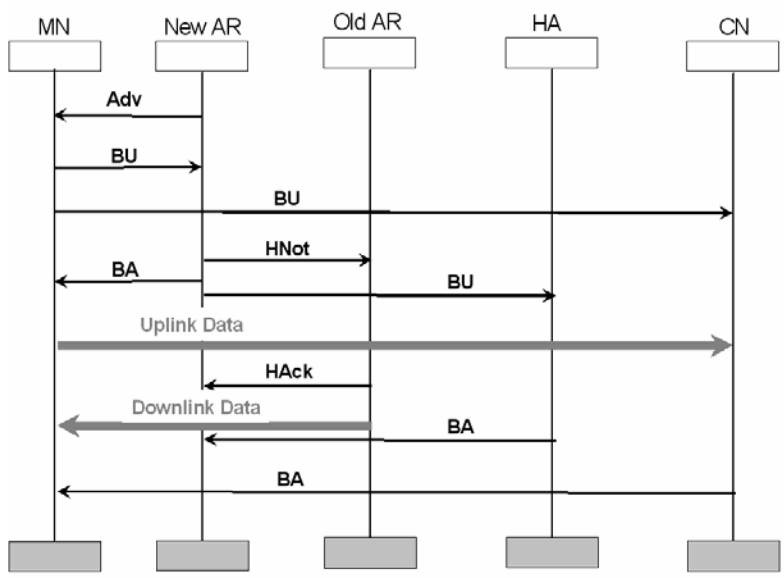
a) Basic idea

In order to avoid the problems of MIPv6 without introducing any new entities and without making restrictions on the network topology, Mobile IP Fast authentication protocol for IPv6 (MIFAv6) is proposed. The new protocol is a continuous development of MIFA [12], which is developed mainly for IPv4. The network topology of MIFAv6 is the same as by

MIPv6 with the exception that the ARs should support mobility. The topology and the handoff procedure of MIFAv6 are plotted in figure1.



(a)



(b)

Figure 1: Network topology and handoff procedure of MIFAv6

In reality, the MN moves always to a neighbor AR, which has normally a short distance to the old AR with respect to the number of hops. By utilizing this fact, the HA can delegate the authentication to the ARs. As a result, the MN requires only contacting the new AR to resume the communication on uplink. On downlink, the new AR relies on the old AR to obtain the packets of the MN until the HA or the CN is informed about the new MN's binding.

Each AR builds a Layer 3 Frequent Handoff Region (L3-FHR), which is composed of a set of neighboring ARs to which the MN is likely to move [12]. L3-FHRs can be built statically by means of a certain algorithm such as neighboring graph [13]. L3-FHRs can be built dynamically too using neighbor discovery protocol of IPv6 [14] or by tracking the MNs movements.

We suppose here, that there are Security Associations (SA) between the ARs in one L3-FHR. These SAs can be established using AAA infrastructure [15], IKE [16], or any other key distributing mechanism [17].

b) Protocol operation

When the MN attaches to the network, it uses the same procedures of MIPv6. Firstly, the MN performs a return routability procedure with the CN and obtains a binding management key (kbm) to authenticate the control messages exchanged with the CN.

Afterwards, Binding Updates (BU) are sent to the CN and to the HA. The MN informs the AR and the HA that it wants to use MIFAv6 in the next registrations. This is achieved by setting one of the reserved bits in BU message, *referred to as MI flag*. Of course, the AR advertises its support of MIFAv6 by setting one of the reserved bits in the Router Advertisement message (RA), *referred to as MI flag too*. The BU sent to the CN is built according to MIPv6 specifications. The HA responds to the BU by building two SAs. One is between the HA itself and the AR ($K1_{HA,AR}$). The second is between the MN and the AR ($K1_{MN,AR}$). These two SAs are sent with the Binding Acknowledgement (BA) message to the AR, which extracts the SAs, generates two random variables *R1*, *R2*, generates another key ($K2_{MN,AR}$) between the MN and the ARs in the current L3-FHR. $K2_{MN,AR}$ is encrypted with $K1_{MN,AR}$ and sent to the MN with *R1* and *R2* in suitable extensions to the BA message. The security between the AR and the MN should be granted through the using of ESP [18] in transport mode. As said above, the SAs can be built through AAA infrastructure or any other key distribution method.

After the MN has been registered and authenticated, Movement Probability Notification (MPN) and Movement Probability Acknowledgement (MPAck) messages are exchanged between the current AR and the HA. MPN contains the random variables *R1*, *R2* and a SA, $K2_{HA,AR}$, between the HA and the new AR, to which the MN will move in the future. $K2_{HA,AR}$ is encrypted using $K1_{HA,AR}$. MPAck contains all the information required to authenticate the MN during the registration with the new AR. The HA computes two authentication values using *R1* and *R2*, the first value (*auth1*) present the authentication value the MN should generate, while the other (*auth2*) expresses the value the HA should generate as a response to *auth1*. These two values are sent encrypted to the current AR. For security consideration, it is highly recommended that the messages exchanged between the AR and the HA are authenticated and authorized using ESP in transport mode too.

After the current AR obtains all data required to authenticate the MN, it distributes this data to all ARs locating in the current L3-FHR. This is done by sending another MPN message to each neighbor AR. This data is recorded in soft state and will be used by one AR in the future and deleted from the others. The MPN messages sent to the neighbor ARs should be authenticated and authorized using the existing SA established between the ARs in the L3-FHR.

After the MN moves to another AR, it waits for a RA message. When receiving this message, it sends a BU message to the new AR and a BU message to the CN. The BU message sent to the CN is sent according to MIPv6 specifications, while the *MI* flag is set in the BU sent to the new AR. This BU contains *auth1* too and authenticated using $K2_{MN,AR}$. After the new AR authenticates the MN, it compares the *auth1* generated by the MN with the value of *auth1* generated by the HA and checks if the HA can satisfy the MN's requirements. This is achieved by checking the data distributed from the old AR with the MPN message. If the check is successful, the new AR sends a Handoff Notification (HNot) message to the old AR and a BA to the MN. The BA contains two new random variables and a new key $K3_{MN,AR}$ for the next registration with the next new AR, to which the MN will move in the next registration. Additionally, the value of *auth2*, generated by the HA, is sent with BA message to the MN, which in turns should generate this value using *R1* and *R2* and compare the generated value with the value, which has received from the new AR.

In addition, the new AR sends another BU message to the HA to inform it about the new binding. The new generated random variables and a new key ($K3_{HA,AR}$), as a SA between the HA and the next new AR, are sent with this BU message. The HA responds by sending a BA message to the new AR and starts forwarding the packets to the new Care of Address (CoA) if the triangular routing is used. This BA message contains the information required to authenticate the MN in the next registration. Upon the new AR receives this BA message it distribute this data to the ARs in the current L3-FHR with MPN messages.

When the old AR receives the HNot message, it responds by sending a Handoff Acknowledgement (HAck) message to the new AR and starts forwarding the MN's packets to the new CoA.

The BU sent to the CN follows the same procedures as by MIPv6. This is motivated from the fact that any update in the CNs should be avoided to make MIFAv6 applicable.

As known from MIPv6, the MNs configure their CoAs in stateful or stateless mode. In case of stateless mode, after the MN configures its CoA, a Duplicated Address Detection procedure (DAD) should be performed to ensure that the address is not used by another MN. Configuration of CoA and DAD procedure slow up the handoff. This is avoided by MIFAv6 because it configures the CoA and executes the DAD procedure in advance. Pre-configuration of the new CoA depends on the used mode. In stateless mode, the MN generates a random value *"host-id"*. Host-id can be the MAC address of the MN. This value is sent to the new AR with the BU message. After the new AR obtains the authentication information required to authenticate the MN during the next registration, it distributes this information with the host-id to the ARs of the current L3-FHR. Each neighbor AR combines the CoA, *net-prefix+host-id*, and executes DAD in advance in each AR in this L3-FHR. In stateful mode, the MN does not generate any host-id. Upon the ARs of the current L3-FHR are informed about the MN, they can configure the CoA in advance.

IV- CONCLUSION AND FUTURE WORK

In this paper we have proposed a new mobility protocol for IPv6. From the discussion above we see that MIFAv6 presents a good mobility framework to support fast and smooth handoff in IPv6 backbone. The MN needs to update its binding only at the new AR to be able to resume sending and receiving of packets, It does not have to wait for update the binding at the HA or the CN. The latency between the current AR and the HA / CN is hidden from the application and does not affect the performance. MIFAv6 does not require any intermediate nodes or hierarchical topology. It is a protocol to support macro and micro mobility management. A main advantage of MIFAv6 that the updating is only restricted to the MNs, the ARs and the HA

References:

[1] C. Perkins, Ed, " IP Mobility Support for IPv4 ", RFC: 3344, 2002.
[2] D. Johnson, C. Perkins, J. Arkko, " Mobility Support in IPv6 ", < draft-ietf-mobileip-ipv6-23.txt >, 2003.
[3] P. Eardley, A. Mihailovic, T. Suihko, " A framework for the evaluation of IP mobility protocols ", 11th PIMRC, 2000.
[4] D E. Gustafsson, A. Jonsson, C. E. Perkins, " Mobile IPv4 Regional Registration ", < draft-ietf-mobileip-reg-tunnel-08.txt >, 2003.
[5] H. Soliman, et.al, " Hierarchical Mobile IPv6 mobility management (HMIPv6)", < draft-ietf-mobileip-hmipv6-08.txt >, 2003.
[6] A. Campbell, et.al, " Cellular IP ", < draft-ietf-mobileip-cellularip-00.txt > 2000.
[7] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, " IP micro-mobility support using HAWAII ", < draft-ietf-mobileip-hawaii-00 >, 1999.
[8] R. Koodli, " Fast Handovers for Mobile IPv6 ", RFC 4068, 2005.
[9] K. El Malki, et al. " Low Latency Handoffs in Mobile IPv4 ", <draft-ietf-mobileip-lowlatency-handoffs-v4-04.txt>, 2002
[10] R. Hsieh, Z.G, Zhou, A. Seneviratne, " S-MIP: A Seamless Handoff Architecture for Mobile IP ", INFOCOM, 2003.
[11] S. Gundavelli, et.al., "Proxy Mobile IPv6", Internet draft <draft-ietf-netlmm-proxymip6-00.txt>, 2007.
[12] A. Diab, A. Mitschele-Thiel, J. Xu, " Perfomance Analysis of the Mobile IP Fast Authentication Protocol ", MSWIM04, 2004.
[13] S.K. Sen, et al., " A Selective Location Update Strategy for PCS Users ", ACM/Baltzer J. Wireless Networks, 1999.
[14] T. Narten, E. Nordmark, W. Simpson, " Neighbor Discovery for IP Version 6 (IPv6) ", RFC2461, 1998.
[15] C. Laat, G. Gross, et al., " Generic AAA Architecture ", RFC 2903, 2000.
[16] D. Harkins, D. Carrel, " The Internet Key Exchange (IKE) ", RFC2409, 1998
[17] D. B. Johnson, N. Asokan, " Registration Keys for Route Optimization ", < draft-ietf- mobileip-regkey-03.txt >. 2000.
[18] S. Kent, R. Atkinson, " IP Encapsulating Security Payload (ESP) ", RFC2406, 1998.

Authors:

Dipl.-Ing Ali Diab
Prof. Dr.-Ing. habil. Andreas Mitschele-Thiel
TU - Ilmenau, Faculty for Informatics und Automation, Gustav-Kirchhoff-Str. 1, P.O.B. 10 0565
98693, Ilmenau
Phone: +49 3677 69 2819
Fax: +49 3677 69 1220
E-mail: {ali.diab|mitsch}@tu-ilmenau.de