International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:9, 2007

Comparative Analysis of Mobility Support in Mobile IP and SIP

Hasanul Ferdaus, Sazzadur Rahman, and Kamrul Islam

***Abstract*—**With the rapid usage of portable devices mobility in IP networks becomes more important issue in the recent years. IETF standardized Mobile IP that works in Network Layer, which involves tunneling of IP packets from HA to Foreign Agent. Mobile IP suffers many problems of Triangular Routing, conflict with private addressing scheme, increase in load in HA, need of permanent home IP address, tunneling itself, and so on. In this paper, we proposed mobility management in Application Layer protocol SIP and show some comparative analysis between Mobile IP and SIP in context of mobility.

***Keywords*—**Mobility, mobile IP, SIP, tunneling.

I. Introduction

WITH the recent advances of portable devices and wireless networks, mobile computing is increasing day by day. Many users of the Internet have portable computers and want to stay connected to the Internet when they are away from their home network boundary. The original Internet Protocol (IP) versions do not support host mobility because of its addressing scheme. To support a mobile host with current methods, reconfiguration is necessary any time a mobile host moves. This is an unacceptable solution as it is time consuming and error prone.

The mobility itself can be largely divided into three types: Roaming, Macro-mobility, and Micro-mobility. Roaming is the movement of the user in absence of the Internet connectivity. This roaming is usually triggered when a MH initiates the Internet connectivity. Macro-mobility and Micro-mobility are the change of point of attachment with ongoing Internet connections and thus normally accompany the handoff. The Macro-mobility is related to the movement of the user from one administrative domain to another.

Hasanul Ferdaus is a student of Computer Science and Engineering Department, Bangladesh University of Engineering and Technology, Dhaka-1000, Bangladesh (e-mail: hasanul_ferdaus @yahoo.com).

Sazzadur Rahman is a student of Computer Science and Engineering Department, Bangladesh University of Engineering and Technology, Dhaka-1000, Bangladesh (e-mail: sazzad1009@yahoo.com).

Kamrul Islam is a student of Computer Science and Engineering Department, Bangladesh University of Engineering and Technology, Dhaka-1000, Bangladesh (e-mail: kamrul34@yahoo.com).

In such a case, the relevant domains must collaborate to ensure seamless connectivity to the moving user. Micro-mobility concerns the user's movement inside a given domain, which involves intradomain (subnet-level) handoff. A well-defined mobility management framework or scheme should deal with all three types of mobility, especially seeking to reduce disruption in handoff.

To solve this problem of mobility the IETF has standardized IP mobility support [1] known as Mobile IP (MIP), which provides for transparent mobility in that it hides the change of IP address when the mobile host is moving between IP subnets. Mobile IP is an Internet Protocol designed to support host mobility. Its goal is to provide the ability of a host to stay connected to the Internet regardless of their location. MIP is able to track a mobile host without needing to change the mobile host's long-term IP address. MIP can be seen as the least common mobility denominator - providing seamless Macro-mobility solutions among the diversity of accesses.

However, MIP is struggling with the problem of Triangular Routing, i.e., a packet to a Mobile Host (MH) travels via the HA (HA), whereas a packet from the MH is routed directly to the destination. The Route Optimization [2] solves this by sending binding updates to inform the sending host about the actual location of the MH. This solution also has several problems, as will be discussed in later sections. For real-time traffic such as voice or video over IP, it is more common to use the Real-Time Transport Protocol (RTP) [3] over UDP, and important issues are fast handoff, low latency, and especially for wireless networks - high bandwidth utilization. Therefore, we see a need to introduce mobility awareness on a higher layer, where we can utilize knowledge about the traffic to make decisions on how to handle mobility in different situations. There are two main approaches to application layer mobility support - the augmentations of the well-known H.323 and Session Initiation Protocol (SIP) [4]. Telecom-based H.323 is much complicated to evolve in practice. Whereas, SIP already supports personal mobility and the changes needed to support device mobility are minor. In this paper, our main theme is to compare the IP layer mobility solution (MIP) with the application layer solution (SIP) and show how SIP can improve the performance for real time services in wireless networks.

II. Mobility Support using MIP

A. Basic MIP Architecture

Mobile IP introduces two new functional entities within IP networks. Those are the Foreign Agent (FA) and the HA (HA). These two new entities together with enhancements in

the Mobile Host (MH) are the basic building blocks for a MIP enabled network. The last entity for providing a full reference for a basic Mobile IP enabled network is the Correspondent Host (CH) that communicates with the MH. Each area (LAN or Wireless Cell) of MIP enabled network has one or more FA which are processes that keep tract of all MH visiting the area. Each area has a HA, which keeps track of hosts whose home is in the area, but who are currently visiting another area.

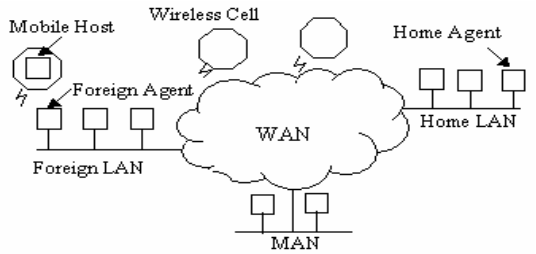

Fig. 1 WAN with MH, FA, HA

B. MIP Registration

When a new host enters an area, either by connecting to it through LAN or wandering into the wireless cell, it must register itself with the FA there. Mobility agents (HA/FA) advertise their presence on a network using special messages called Agent Advertisements. These messages are broadcast or multicast at regular intervals. From the agent advertisement, the MH can determine if it is on the home or a foreign network. When a MH moves to a foreign network it acquires a Care-of-Address (CoA) in one of two ways. The CoA may be obtained from a particular field of the agent advertisement and is known as a 'foreign agent CoA'. This is actually the address of the FA that the MH is registered with and not the MH itself. This way more than one MH can share the same CoA, as data from the HA is only tunneled as far as the FA who then determines which MH the data is destined for and sends it to this host. Alternatively the CoA can be assigned directly to the MH using some external means, such as the Dynamic Host Configuration Protocol (DHCP). This type is known as a 'co-located CoA'. This address is uniquely addressable so data can be forwarded directly to the MH. Once a CoA has been assigned, the MH must then register this address with the HA. This is done by sending a Registration Request message to the HA who then replies with a Registration Reply (accepting or denying) the request. Once the MH has been registered, communication between the CH and the MH can occur.

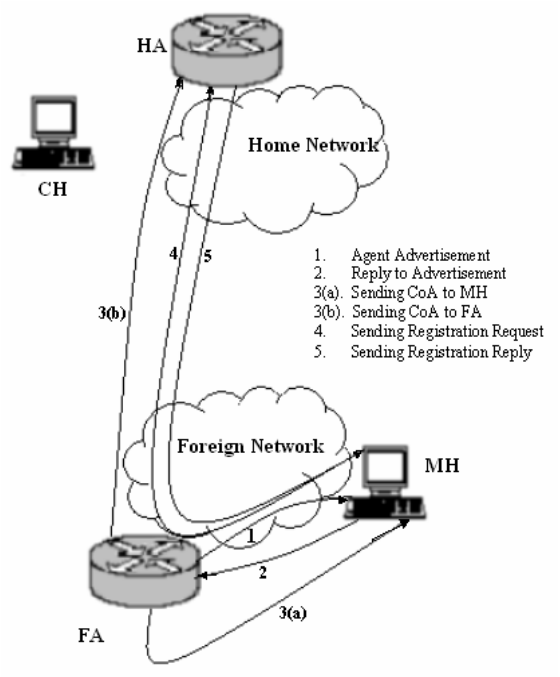

Fig. 2 MIP Basic Registration process

C. MIP Operation

MIP works by allowing each MH to be associated with two IP addresses - a home address and a CoA. The home address is fixed for that MH but the CoA changes as the MH moves from site to site. The home address is the address where the MH seems to be the reachable by other CHs. When CN sends a packet to a mobile host, it is routed to the host's home LAN as the CN knows only MH's home address, and the HA there intercepts the packets. If the MH is not attached to a foreign network, the HA simply delivers the packet to the MH's point of attachment in the home network. When the MH is attached to a foreign network, the HA modifies the packet so that the CoA appears as the destination IP address and routes i.e. redirects that packet to the FA. This process of IP encapsulation is called Tunneling.

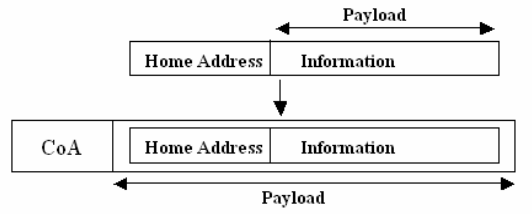

Fig. 3 IP encapsulation

When the packet arrives at the FA, the new "routing" header is removed and the original packet is sent to the HM. Tunneling between the agents can be done using IP encapsulation within IP (RFC2003 [5]) or GRE, Generic Routing Encapsulation (RF2784 [6]).

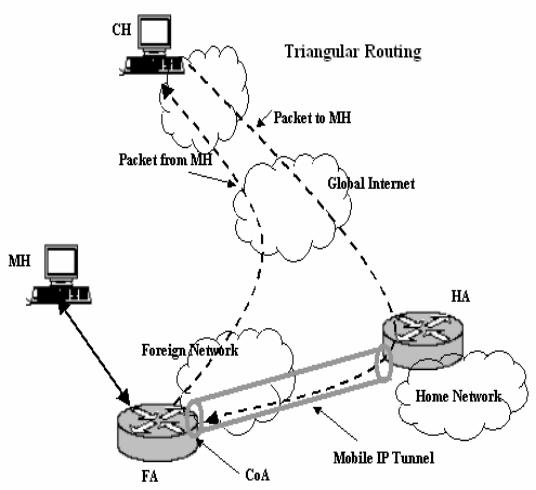

Fig. 4 Basic MIP Operation.

D. Problems of Basic MIP

Basic MIP suffers from a problem called "Triangular Routing". Packets from a CN to a MH in a visited network are routed from the CN to the HA. The HA encapsulates the packets in a MIP tunnel. The tunnel is terminated in the FA and the FA then forwards the packet within a layer two technology to the MH. But from the MH to the CN packets are sent from the MH (in a layer two technology) to the FA. Since the CN (in a basic scenario) is supposed to have a public IP address, it is possible for the FA to directly forward the packet to the CN. Triangular Routing inherits some problem.

- It increases the traffic on the network especially the load on the HA as the packets are first routed to the HA.
- It cannot support private addressing in a good way since the solution requires unique IP addresses on every interface.

Also Ingress Filtering [7] involves routers dropping packets that do not have a source IP address consistent with the network address of the network it is being sent from. As in MIP, MH attached to a foreign network sends packets using its home address as the packet source; hence the packet source will have a different network prefix to the foreign network address. Routers in the foreign network that employ ingress filtering will drop this packet.

E. Solution approach using Route Optimization

The recommended solution for Triangular Routing problem is termed route optimization [2]. Initially CN will send packets to the MH's home address. The HA will then tunnel these packets to the MH as is normal in MIP. However, by receiving a tunneled packet the MH can reason that the CN is unaware of its changed location. In this case the MH sends a binding update to the correspondent node. A binding contains the MH's home address along with the CoA it is currently using and is stored in a binding cache. The update informs the CN of the MH's CoA so it can now send packets directly to the MH without tunneling through the HA. Also to perform smooth Handoff [8], when the MH obtains a new CoA due to handoff the Old FA and the new FA can exchange the Binding Update message.

However, route optimization has some problems

- Route optimization requires changes in the IP stack of the CH, since it must be able to encapsulate IP packets, and store CoA of the FA or MH.
- Only the HA may send binding updates to CH. This means that there will be an extra delay before the CH finds out where to send the packets, during which the old FA must forward the packets to the correct location.
- The MH needs to rely on the old FA forwarding packets to its new FA until the correspondent host has got the binding update. There is no requirement saying that the FA must do so.
- The binding warnings and updates are not compulsory, and should be used sparingly, since it can be expected that many hosts will not support the binding update function.

III. Mobility Support using SIP

A. SIP Overview

The Session Initiation Protocol (SIP) [4] is an application-layer protocol used for establishing and tearing down multimedia sessions, both unicast and multicast. It has been standardized within the Internet Engineering Task Force for the invitation to multicast conferences and Internet telephone calls [10]. Entities in SIP are user agents, proxy servers and redirect servers. A user is addressed using an email-like address "user@host", where "user" is a user name or phone number and "host" is a domain name or numerical address. SIP defines a number of methods, listed in Table 1. Responses to methods indicate success or failure, distinguished by status codes, 1xx (100 to 199) for progress updates, 2xx for success, 3xx for redirection, and higher numbers for failure. Each new SIP transaction has a unique call identifier, which identifies the session. If the session needs to be modified, e.g. for adding another media, the same call identifier is used as in the initial request, in order to indicate that this is a modification of an existing session.

The SIP user agent has two basic functions: Listening for incoming SIP messages, and sending SIP messages upon user actions or incoming messages. The SIP user agent typically also starts appropriate applications according to the session that has been established. The SIP proxy server relays SIP messages, so that it is possible to use a domain name to find a user, rather than knowing the IP address or name of the host. A SIP proxy can thereby also be used to hide the location of the user. A redirect server returns the location of the host rather than relaying the SIP message. This makes it possible to build highly scalable servers, since it only has to send back a response with the correct location, instead of participating in the whole transaction, which is the case for the SIP proxy. Both the redirect and proxy server accepts registrations from users, in which the current location of the user is given. The location can be stored either locally at the SIP server, or in a dedicated location server (more about the location server further below). Deployment of SIP servers enables personal mobility, since a user can register with the server independently of location, and thus be found even if the user is changing location or communication device. SIP requests and

responses are generally sent using UDP, although TCP is also supported.

TABLE I
SIP REQUESTS

Message Name	Function
INVITE	Invite user(s) to a session. The session description is contained in the body of the message, e.g. using the Session Description Protocol (SDP) [10]. The session description contains the address where the host wants to receive media streams.
ACK	Acknowledgment of an INVITE request
BYE	Sent when a call is to be released.
OPTIONS	Query user agents about capabilities.
CANCEL	Cancel a pending request.
REGISTER	Register with a SIP server.

The SIP user agent has two basic functions: Listening for incoming SIP messages, and sending SIP messages upon user actions or incoming messages. The SIP user agent typically also starts appropriate applications according to the session that has been established. The SIP proxy server relays SIP messages, so that it is possible to use a domain name to find a user, rather than knowing the IP address or name of the host. A SIP proxy can thereby also be used to hide the location of the user. A redirect server returns the location of the host rather than relaying the SIP message. This makes it possible to build highly scalable servers, since it only has to send back a response with the correct location, instead of participating in the whole transaction, which is the case for the SIP proxy. Both the redirect and proxy server accepts registrations from users, in which the current location of the user is given. The location can be stored either locally at the SIP server, or in a dedicated location server (more about the location server further below). Deployment of SIP servers enables personal mobility, since a user can register with the server independently of location, and thus be found even if the user is changing location or communication device. SIP requests and responses are generally sent using UDP, although TCP is also supported.

The INVITE message contains a session description expressed in SDP, and is received by a redirect server, which consults a location server to find out where to redirect the invitation. The function of the location server is not specified, but can be anything that can return a next hop address in the chain of finding the callee (which could be an address to another redirect server or a proxy). In many cases, the location server can simply be a table handled by the SIP server, containing the users' locations as they register with the SIP server. From now on, only redirect servers will be discussed, but this does not mean that a proxy server cannot be used instead. However, the load on a redirect server can be expected to be lower since it only needs to send an answer with the user's location, instead of participating in the whole signaling transaction. The SIP redirect server has properties resembling those of the HA in mobile IP with route optimization, in that it tells the caller where to send the invitation. In addition, it can store preferences for the user regarding how to treat incoming requests depending on where the user is located, time of day, or the identity of the caller.

B. Mobility Support in SIP

Registration: SIP registration is same as MIP registration. By default, registrations are sent to the "home" registrar. Thus, any location change causes a SIP REGISTER request and response to be sent. Within SIP, registrations can be proxied just like other requests, as shown in Fig. 5. In the figure, Alice, with a home in New York, visits California. Each time she moves, she sends a REGISTER request towards her home registrar, through the outbound proxy in California. For the first REGISTER, originating in San Francisco, the outbound proxy makes a note of the registration and then forwards the request to the normal home registrar, after modifying the Contact in the registration to point to it rather than Alice's mobile host. After Alice travels to Los Angeles, the REGISTER update hits the same registrar (CA). It recognizes that Alice is already in California and does not forward the request. A call from anywhere first reaches the NY proxy server, which forwards the request to the CA proxy server, which in turn forwards it to Alice's MH.

The mechanism described here works whether the ISP in California is the same has Alice home ISP or not. While only a single level of indirection is shown, the ISP in California could nest this as deeply as desired, with a hierarchy of "outbound proxies".

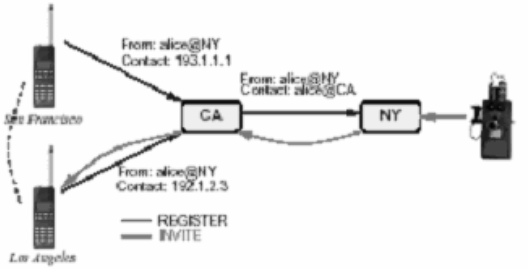

Fig. 5 Registration in SIP

Session Establishment: Mobility impacts SIP at three stages, pre-call, mid-call and to recover from network partitions, as described below.

Pre-Call Mobility: The easiest part of SIP mobility is the pre-call mobility, where the mobile host (MH) acquires a new address prior to receiving or making a call. The MH simply re-registers with its "home" registrar each time it obtains a new IP address.

When the correspondent host sends an INVITE to the mobile host, the redirect server having the current information of the mobile host's location returns redirect INVITE response. For this, it generates a SIP response with 302 status

code and "Moved Temporarily" reason phrase containing the new location address in Contact header field.

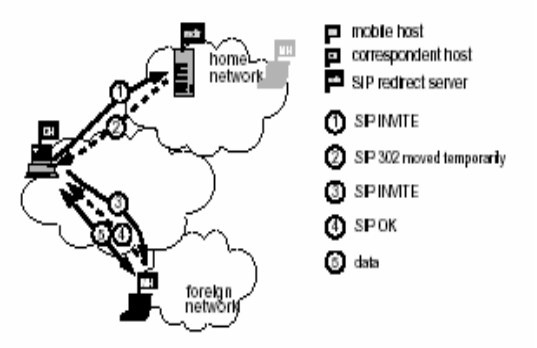

Fig. 6 SIP based pre-call location

Mid-Call Mobility: For mid-call mobility, the moving MH sends another INVITE request to the correspondent host (CH), without going through any intermediate SIP proxies. (A SIP proxy will be traversed if, during the initial call setup, it has requested to be part of future signaling messages by inserting a Record-Route header.) This is called Re-Invite, which maintains the same sip dialog established on the initial Invite. This INVITE request contains an updated session description with the new IP address. Thus, the location update takes one one-way delay after the application in the MH recognizes that it has acquired a new IP address.

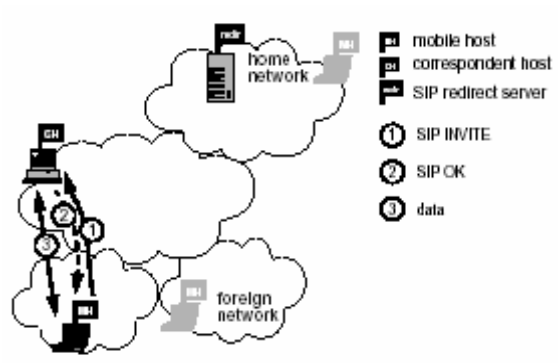

Fig. 7 SIP based hand-off in Mid-Call

Network Partitions: If the network partition lasts less than about thirty seconds, SIP will recover without further mechanisms, as it retransmits the request if there is no answer. If the network partition lasts longer, updates may be lost and the other host may also have moved. In that case, to rendezvous again, each side should address the SIP INVITE request to the canonical address, the home proxy of the other side. Recovery from such partitions can be done automatically if the user agents implement the SIP session timer mechanism [11] that automatically causes a refresh of the session at user-configurable intervals.

IV. Comparison between MIP and SIP

A. Performance Comparison

It is not trivial to compare the performance of mobile IP vs. SIP mobility, because it very much depends on the distance between the mobile host, correspondent host, and the mobile host's home network.

End-to-End Delay: It is obvious that the end-to-end delay will be lower if packets are sent directly to the mobile host without being routed via the home network and/or being encapsulated. The extra latency introduced by mobile IP is basically proportional to the distance to the home network and the correspondent host. The delay introduced by the HA and FA are relatively small unless a congestion occurs and packets are buffered.

Handoff Delay: The handoff delay depends on the delays of several different operations:

- Both mobile IP and SIP-based mobility need to discover that they are in a new network. This depends on the wireless technology and the operating system interface of, say, a wireless LAN card.
- Then, a host needs to acquire an IP address via DHCP, which, depending on implementation [12] can be a major part of the overall handoff delay. A mobile-IP host needs to instead discover its new FA. The number of messages exchanged is roughly similar for either DHCP or FA discovery.
- A mobile IP host then has to register with the foreign and/or HA (which in turn notifies the CH if route optimization is used), while a SIP-speaker needs to send an INVITE to the correspondent host, thus incurring misdirected packets for the one-way delay from MH to CH. Generally, the path from MH to HA to CH is going to be longer, possibly significantly so, than the direct path between CH and MH. This is a particular problem if the paths between MH and HA or HA and CH suffer from high packet loss, since that would significantly delay the binding update. The magnitude of this effect clearly depends on the relative location of the CH, MH and HA and thus can't be quantified with any generality. As long as end-to-end delays of a round-trip time are acceptable, application-layer mobility as described here should be able to provide transparent mobility, even without lower-layer assistance (such as soft hand-offs).

In addition, for SIP mobility, the mobile host must register with the SIP server on the home network, although this does not factor into the handoff delay. In summary, we see that the difference in handoff delay is the same difference as mobile IP has for data packets between the current version and the use of route optimization.

Handling mobility at the application layer does introduce slight additional delays since an operating system context switch in the end host is required, but in modern OS, these are generally below one millisecond.

B. Context Comparison

TABLE II
CONTEXT COMPARISON - MIP VS SIP

Context	IP	SIP
Constant	IP address	SIP url user@home.com
Update	Binding upd.	Re-INVITE
Security	Via HA	Call-ID, crypto
Impl.	OS	app.
Reg.	HA & FA	Proxy

V. CONCLUSION

In this paper, we have proposed the use and advantage of SIP, an application layer protocol over network layer protocol Mobile IP especially in the context of real-time communications. Mobile IP uses the technique of tunneling of packet and this introduced some difficulties in smooth communication. SIP, being implemented in application layer supports the mobility intensively and efficiently. SIP can be installed easily, eliminates the difference between personal mobility and device mobility.

It is also very much attractive for mobile communication (i.e. voice). . Also SIP mobility is possible without change in the IP stack of the MH.

REFERENCES

[1] C. Perkins, "IP mobility support," IETF RFC 2002, 1996.
[2] C. Perkins and D. Johnson, "Route optimization in mobile IP," Internet Draft, Internet Engineering Task Force, Feb. 1999. Work in progress.
[3] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: a transport protocol for real-time applications," Request for Comments (Proposed Standard) 1889, Internet Engineering Task Force, Jan. 1996.
[4] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: session initiation protocol," Request for Comments (Proposed Standard) 3261, Internet Engineering Task Force, June, 2002.
[5] IP encapsulation within IP, C. Perkins, RFC 2003, http://www.ietf.org/rfc/rfc2003.txt, October 1996.
[6] Generic Routing Encapsulation (GRE), D. Farinacci et al., RFC 2784, http://www.ietf.org/rfc/rfc2784.txt, March 2000.
[7] Ferguson, P. & Senie, D., 2000, 'Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing', IETF RFC 2827.
[8] C. Perkins and Kuang-Yeh Wang, "Optimized Smooth Handoffs in Mobile IP," Int'l. Symp. Comp. Commun, 1999.
[9] H. Schulzrinne and J. Rosenberg, "The session initiation protocol: Providing advanced telephony services across the internet," Bell Labs Technical Journal, vol. 3, pp. 144–160, October-December 1998.
[10] M. Handley and V. Jacobson, "SDP: session description protocol," Request for Comments (Proposed Standard) 2327, Internet Engineering Task Force, Apr. 1998.
[11] S. Donovan and J. Rosenberg, "SIP session timer," Internet Draft, Internet Engineering Task Force, July 2000.Work in progress.
[12] J.-O. Vatn and G. Q. M. Jr., "The effect of using co-located care-of addresses onmacro handover latency," in Proc. of 14th Nordic Tele-traffic Seminar, (Technical University of Denmark, Lyngby, Denmark), Aug. 1998.
[13] Henning Schulzrinne & Elin Wedlund, "Application-Layer Mobility Using SIP".