

# Multilayered Mobility Management for Survivable Network

Ashutosh Dutta, James Burns, K. Daniel Wong, Ravi Jain, Ken Young  
Telcordia Technologies, 445 South Street, Morristown, NJ 07960

Henning Schulzrinne

Computer Science Department, Columbia University, New York, NY 10027

*Abstract—*

A variety of mobility management scheme have been developed for commercial networks ranging from Mobile IP (network layer support), to the Session Initiation Protocol (SIP) based on application layer components such as DNS and SMTP, and Micro-Mobility approaches like Cellular IP, HAWAII. There are significant challenges, however, with regard to the robustness, management overhead requirements and latency in each of these approaches, especially in military environments where the network is very dynamic. It is desirable to provide continuous connectivity between the nodes for real-time and non-real-time traffic.

We propose to dramatically improve mobility management of the terrestrial networks to provide support for dynamic military networks by developing an integrated mobility management approach that both meets the needs of end-user applications and deals with the harsh networking environment. This approach is based on the concept of dynamic servers, provided on the airborne nodes, that enhance the mobility of nodes on the ground. Unlike in the fixed Internet, where such servers are always present, our approach requires the development of robust mechanisms that allow the servers to advertise their existence to terrestrial nodes and to synchronize with each other and with their terrestrial peers to ensure coherency.

Proposed approach provides a multi-layered mobility management solution. It provides personal and terminal mobility for real-time traffic such as voice-over-IP or video streaming through deployment of dynamic SIP and DNS servers in a distributed manner. It provides network layer support through the use of Mobile IP with Location Registers (MIP-LR) for non-real-time applications. Local mobility management is achieved through the use of micro-mobility management protocol (MMP) that reduces the need to update the SIP, DNS and MIP-LR servers when end nodes move locally within a domain.

## I. INTRODUCTION

In a military environment nodes are highly mobile under dynamic network conditions. Thus in this environment mobility management is needed to ensure that nodes can be located quickly and packet delivery operates properly in the presence of mobility of nodes, networks and multimedia session does not get affected.

There are many mobility management scheme defined to support real-time and non-real-time application in the terrestrial Internet, both for inter-domain and intra-domain mobility [1], [4], [5] while providing support for personal, terminal and session mobility. There are significant challenges however with regard to the robustness, management overhead requirements and latency of some of these existing approaches and hence none of these traditional mobility management scheme alone can provide adequate support with respect to survivability, robustness, redundancy for adhoc type network in a military environment. Triangular routing and encapsulation asso-

ciated with traditional Mobile IP scheme do not make it suitable in wireless scenario since it adds to network delay and wastage of bandwidth. Although there are other approaches such like Mobile IP with Route Optimization to take care of triangular routing problem, it still needs to have a modified version of kernel's TCP/IP stack. SIP based mobility management [3], [8] although suitable for real-time application it alone cannot take care of non-real-time application in its current form, however there are extensions proposed [9], although a new transport protocol called SCTP [11], can be used with SIP to take care of traffic due to mobility when IP address changes.

Thus military environment requires a new comprehensive and integrated mobility management scheme which would take care of precise handoff delay, latency and bandwidth requirement while providing the needs for a survivable network. This approach consists of mobility management at several layers, such as application layer based on SIP, network layer approach based on Mobile IP with location register, and local mobility management protocol for Intradomain mobility.

This paper is organized as follows. Section II touches upon the individual mobility component of the integrated approach involved here and their performance with respect to Mobile IP. Section III briefly describes the mobility management architecture for a typical military environment and how these mobility protocols fit in together. Section IV cites some related work, and section V concludes the paper with some open issues.

Figure 1 shows the protocol stack where each of the mobility management component fits in.

## II. MOBILITY COMPONENTS

The sections below would provide some analytical and simulation results for each of these approaches while providing background on each of the mobility components. Each of these mobility management protocols would provide better performance in terms of delay and throughput compared to the traditional Mobile IP approach.

### A. Application Layer Component - SIP based approach

Application layer mobility management is based on Session Initiation Protocol which has been proposed standard as

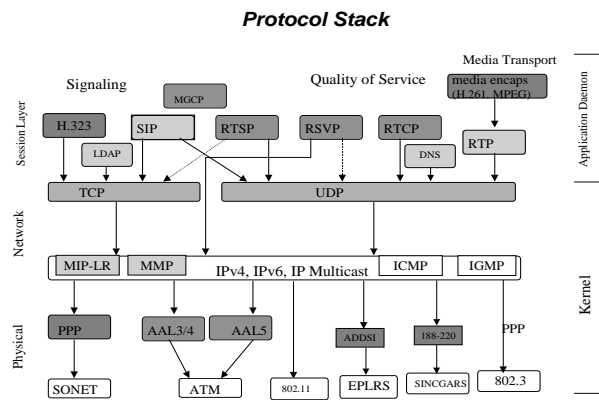


Fig. 1. Mobility Management Protocol Stack

an RFC 2543 in IETF [13]. [3] provide a good background about the application layer mobility management using SIP. Following paragraph provides an overview of SIP based mobility management which can be applied to a military environment.

SIP provides application layer mobility solution in three different ways: pre-session mobility often known as personal mobility, mid-session mobility often known as terminal mobility, session mobility where it keeps the same service while mobile [16] and irrespective of the network attached. Since most of the networks currently do not support mobile IP, besides Mobile IP has triangular routing and other overhead problems, and basic kernel stack has to be modified on the end-points, it is not suitable for deployment in a typical military environment which is so much delay sensitive. On the other hand SIP is gaining momentum as the signaling protocol for real-time multimedia calls. So it is proposed to use SIP to take care of mobility management because of its server based approach. Both personal mobility and terminal mobility can be achieved by SIP for real-time communication. Real-time traffic is mostly RTP/UDP based, and thus higher layer error recovery can be taken advantage of if we use SIP as the signaling entity. Mobile host registers with a SIP server in the home domain, although it can be better optimized if the mobile host registers with the SIP register in the visited domain [14]. When the correspondent host sends an INVITE to the mobile host, the redirect server has the current information about the mobile host's location and re-directs the INVITE to the new location. Thus personal mobility can be achieved by using unique URI scheme. If the mobile host moves during a session it sends a new INVITE to the correspondent host using the same call identifier as in the original call setup and puts the new IP address in the "contact" field of the SIP message's SDP parameters. At the same time it should also make a new registration at the SIP server with its unique URI for the new incoming calls. It would need to update the DNS if the terminal is a mobile server, so that DNS database gets updated dynamically. There can be two scenarios in one case CH is static and there are cases when both CH and MH move,

Re-invite is sent through the SIP server, since the SIP server would keep track of CH's current location, thus it is quite likely to send the Re-INVITE through SIP server. SIP's application layer approach along with its interaction with DNS servers and LDAP database makes it a good alternative for managing the real-time traffic. There have also been many ways of propagating the registration information using some techniques mentioned in [14]. Multiple SIP servers can be provisioned during the boot time and by using DNS's "SRV" record, SIP proxy servers for a particular domain can be discovered. Thus in case of a failure one SIP server, a secondary SIP server can be used. SIP's session timer feature can be used to choose between alternate servers. Figure 2 shows use of SIP mobility in a distributed environment where some of the nodes may be airborne.

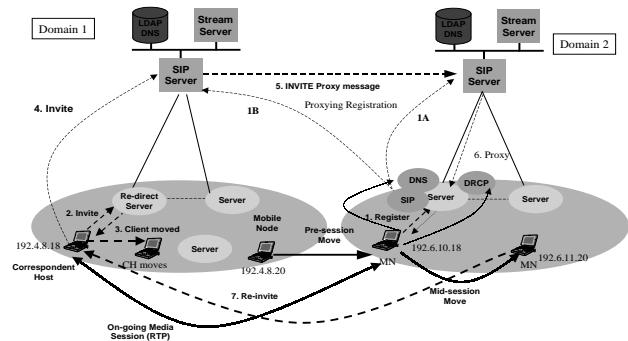


Fig. 2. SIP Mobility for a Survivable Network

## B. SIP performance

Using SIP to provide mobility management for real-time traffic would provide better throughput and performance compared to standard mobile IP. By using SIP instead of Mobile IP without route optimization one can expect to have 50 percentage latency improvement in real-time (RTP/UDP) traffic (reduction in latency from baseline of 27 ms to 16 ms for large packets) and 35 percentage utilization increase (60 bytes packet size compared with baseline of 80 bytes packet size with IP-in-IP encapsulation in Mobile IP). The curves in figure 3 and figure 4 show the relative performance difference between SIP and Mobile IP under different network conditions. These results were obtained from analysis and simulation. Experiments were also carried out in the laboratory comparing both the approaches using controlled traffic. Some of the analysis tools such as netperf, tcpdump and rtpdump were used to measure the performance details. Comparison was made for SIP based mobility with Stanford's MosquitoNet mobile IP.

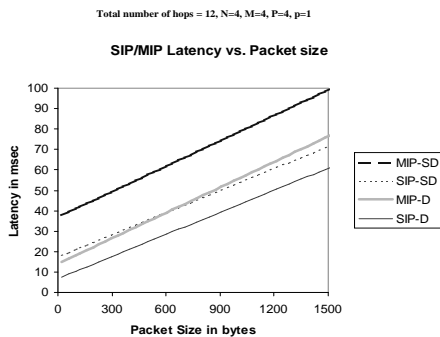


Fig. 3. Signaling and Transport Overhead

### C. Network Layer component- MIP-LR approach

MIP-LR (Mobile IP with Location Register) [2] provides a network layer mobility solution but with placement of additional location registers.

MIP-LR addresses the following four limitations of basic MIP:

1. Home Agent Location: The mobile's Home Agent must be located in its home network.
2. Home Agent Vulnerability: There is no scheme to allow multiple, geographically distributed Home Agents located outside the Home Network to serve the user.
3. Triangle Routing: All packets destined to the mobile host must traverse its home network.
4. Tunneling: Packets destined to the mobile must be tunneled (typically by being encapsulated inside another IP packet) enroute.

MIP-LR provides an efficient approach compared to MIP by taking care of forwarding, profile replication, local anchoring, hierarchical organization. The first two limitations inhibit survivability, particularly in a military scenario where the mobile's home network may be in a vulnerable forward area. The second two limitations imply a performance penalty and also inhibit interoperability with other protocols like RSVP which rely on inspecting the original IP packet header. In MIP-LR we eliminate the tunneling function. In addition, the database mapping the mobile host's IP address to its COA is maintained by an entity called the Home Location Register (HLR), by analogy with cellular systems, since it is queried in a manner analogous to how the HLR is queried in cellular systems to determine the mobile host's location. Unlike the Home Agent, it need not necessarily be located in the home network. In keeping with the cellular analogy, the Foreign Agent is renamed the Visitor Location Register (VLR). MIP-LR uses a set of databases, called Location Registers, to maintain the current Care-Of Address (COA) of the mobile host. When a mobile host moves from one subnet to another, it registers its current COA with a database called a Home Location Register (HLR). When a correspondent host has a packet to send,

it first queries the HLR to obtain the mobile host's COA, and then sends packets directly to the mobile host. The mapping from the mobile host's permanent IP address to its COA is done by the IP layer at the correspondent host and is transparent to higher-layer protocols; the reverse mapping is done at the mobile. The correspondent host caches the mobile host's COA to avoid querying the HLR for every subsequent packet destined for the mobile host. The mobile host maintains a list of correspondent hosts with which it is in active communication and informs them if it moves to a different subnet (as is done in Mobile IP for IPv6). MIP-LR is especially suited to military environment as compared to Mobile IP as it provides Better performance, less delay and network load on ground and elsewhere. It provides better survivability by allowing multiple replicated LRs along the battlefield, and LRs placed outside the vulnerable area within the domain. Figure 5 shows the use of MIP-LR in a military environment where some of the nodes may not be in the ground.

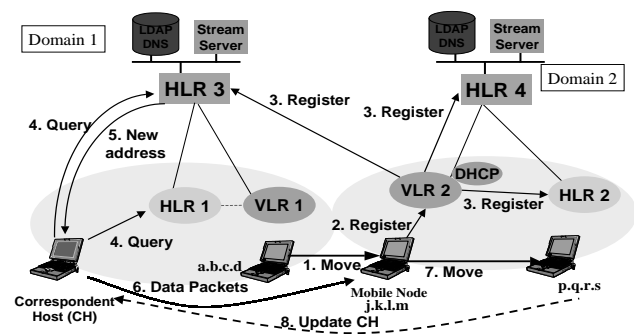


Fig. 4. MIP-LR for a Survivable Network

### D. MIP-LR performance

While MIP-LR provides survivability and redundancy, it also offers better performance compared to traditional Mobile IP. Using MIP-LR instead of Mobile IP one can expect to achieve a goal of 50 percentage reduction in management overhead (latency of 10.5 ms vs. baseline of 18.5 ms in MIP case for a packet size of 1Kbyte in a small campus environment). Figure 6 provides an analytical comparison between MIP and MIP-LR.

Experimental results for MIP-LR and MIP taken in a testbed show similar results.

### E. Micro Mobility Management Component - MMP

MMP is a derivative of the Cellular IP/HAWAII family of micro-mobility schemes [5], [4]. Cellular IP is one of the first micro-mobility schemes proposed. It was proposed as a response to perceived short-comings of Mobile IP (RFC 2002) for handling mobility in some cases. In particular, Mobile IP is designed such that a new registration is required to be

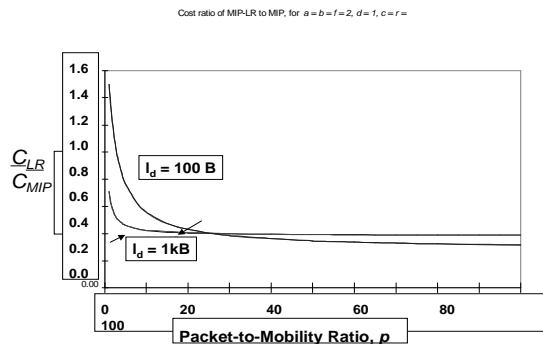


Fig. 5. Cost comparison MIP vs. MIP-LR

sent to the Home Agent, with a new care-of-address, every time a mobile node moves to a new subnet. The registration process may introduce unnecessary latency, which is alright in the original scenarios for which it was designed - where the rate of movement between subnets is low. In addition, if there are lots of idle mobile nodes, these will all be performing Mobile IP registrations whenever they move, causing a lot of signaling overhead. This signaling overhead is not localized, but goes over the global Internet.

MMP is designed as a micro-mobility protocol to handle intra-domain mobility. Domain in this case does not have to be DNS domain but consists of few subnetworks. MMP is designed to work with SIP and MIP-LR, where SIP and MIP-LR handle macro-mobility. MMP shares certain benefits of forwarding-cache-based local/micro-mobility schemes like Cellular IP and HAWAII, exploiting hierarchical structures of military networks, etc. The extended MMP uses multiple paths, and possibly multiple gateways, for robustness and reliability.

In basic MMP, gateway beacon messages are sent down by the gateway periodically so the MMP nodes can refresh their cache mappings of the uplink interface. It can be used, with modifications, for topology discovery, e.g. when network mobility occurs. This is not exploited by the basic MMP. In particular, the gateway beacon message interval is not optimized. Extended MMP will relate the message rate to mobility parameters. The hierarchical nature of forwarding-cached based protocols like MMP makes a good fit for military networks like the Tactical Internet.

Figure 6 shows an abstraction of MMP, in particular, of two MMP domains (each with a gateway).

The gateway is the dividing point between macro-mobility and micro-mobility. Below it is one MMP domain. The nodes in the tree beneath it are MMP nodes which may be routers or even “layer-2 switches” since they do host based routing and do not need IP routing protocols like RIP, OSPF etc. Micro-mobility is handled by special host-based routing. This host-based routing is integrated with location management as described below.

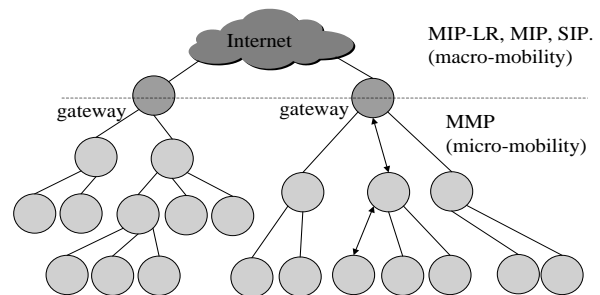


Fig. 6. An abstraction of MMP

Uplink (base stations to gateway) routing: Gateway sends beacons downlink so MMP nodes can route uplink. The interface through which the first copy of a particular beacon (beacons may use sequence numbers) arrives, is recorded, and is used as the next-hop for routing of any packet to the gateway.

Advertisement for network detection is passed along from access points (base stations), with gateway’s address. When a node first arrives in an MMP domain, it performs autoconfiguration and obtains a COA. The registration message is a paging update from mobile node to gateway, moves hop-by-hop up to gateway, updating routing caches; the entry for a particular mobile node will point to the interface through which the registration packet arrived from the mobile node, allowing downlink routing; gateway takes care of Mobile IP registration, if necessary (acts as FA). Routing to mobile node is done by tunneling data to gateway from HA, decapsulated, and forwarded to mobile node by routing caches. Routing from mobile node is forwarded to gateway and then into Internet.

Paging caches have usually longer expiry than routing caches and are used only when no valid routing cache entry exists.

Figure 7 shows the simulation results from relative throughput performance of MMP with respect to Mobile IP as network latency varies. Figure 8 shows actual experimental results obtained from the testbed.

### III. INTEGRATED MOBILITY MANAGEMENT ARCHITECTURE

Main objective of this architecture is to provide mobility support for both real-time and non-real-time applications while providing survivability and redundancy features in a military network. This is achieved by means of distributed servers, location registers and proxies which provide fall back features, and forward caching technique within a domain.

Proposed mobility management architecture is mostly based on server based approach. Figure 9 shows the mobility architecture where all three mobility management approaches are taken into account. This mobility architecture

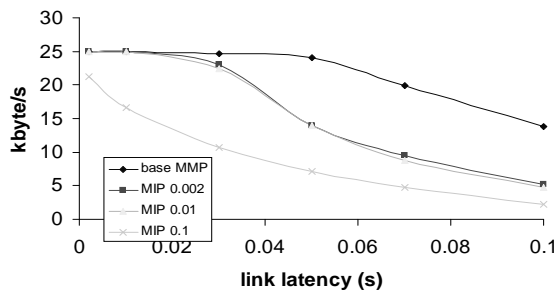


Fig. 7. Throughput with varying latency

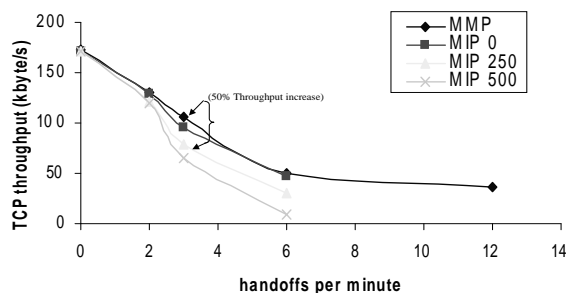


Fig. 8. Experimental Result

assumes that the end hosts are smart and IP addressable, and the routers can also provide application layer signaling functionality. Some of the intermediary and gateway nodes can act like routers and can have the server functionality such as DNS, HTTP, and location register functionality, thus providing redundancy support in case of router/server failure on the ground. In this particular figure, each footprint may belong to a different MMP domain, although each footprint may be an autonomous system belonging to the same domain.

As described in the earlier sections these three mobility management can work together to provide a reliable operation. Each mobility management approach would become active depending on if the client is communicating via real-time traffic (RTP/UDP), non-real-time traffic (TCP/IP) and whether the client is moving between domains or within a domain.

MMP is used for intra-domain mobility; SIP based mobility scheme and MIP-LR are used for inter-domain mobility based on the type of application being supported by the end user terminal (i.e, Real-time or Non-real-time respectively). SIP based personal mobility feature would provide a means

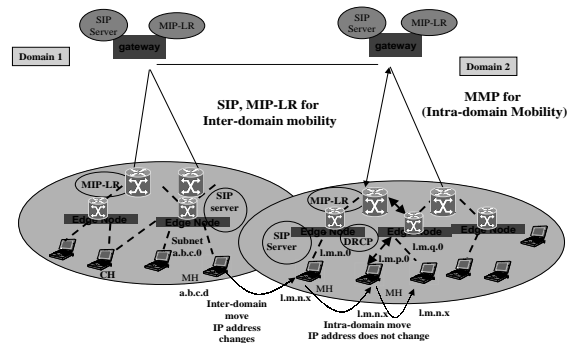


Fig. 9. Integrated Mobility Management

for pre-session mobility.

In this case Mobile Node obtains a new IP address once it moves to a new domain, and it does not obtain any new IP address as long as it remains within this domain, mobility is taken care of by MMP scheme within this domain. When MN moves to a new domain for the first time, it obtains a new IP address, registers with the SIP server or ground VLR which gets propagated to other SIP servers or HLRs spread across the network. Thus CH becomes aware of the new URI or new IP address from the Re-direct server or HLRs. In case of real-time communication if the MH moves between the domains, then a Re-INVITE is sent to the CH to keep the session active, similarly UPDATE message is sent to CH in case of MIP-LR. But any subsequent move within the new domain Re-INVITE or update messages are not sent, since MMP takes care of routing the packets properly within that domain. As shown in figure 9 as the mobile node moves between the domains it would use SIP or MIP-LR depending upon the type of application being supported. But while roaming within a domain mobility management is taken care of by MMP, where the gateway would act like a FA in case of a MIP-LR and would provide the new contact address in case of SIP based mobility management.

#### IV. RELATED WORK

There have been some related work to support mobility in military environment [15]. Most of these approaches are limited to intra-domain case, and does not offer an application specific integrated mobility management approach for a military type environment. This integrated approach provides survivability solution while saving the extra overhead and added delay because of triangular routing and take care of both real-time (e.g., audio, video streaming traffic and non-real-time traffic (e.g., ftp, telnet).

#### V. CONCLUSION AND OPEN ISSUES

This paper illustrates a novel mobility management architecture suitable for a mobile military environment, discussion

of each of the mobility component of the architecture, some performance results of each method and how these can work together in a military environment. There are many open issues as to how these mobility management scheme can work with auto-configuration and self managed virtual networks are being studied currently.

## VI. ACKNOWLEDGEMENT

Authors would like to acknowledge Tony Mcauley and Subir Das for several useful discussion on mobility management protocols and its integrated approach.

## REFERENCES

- [1] C. Perkins, "IP mobility support for IPV4, revised", draft-ietf-mobileip-rfc2002-bis-02.txt, July 2000, Work in Progress.
- [2] Ravi Jain, Thomas Raleigh et. al "Enhancing Survivability of Mobile Internet Access using Mobile IP with Location Registers" IEEE Infocom 1999.
- [3] E. Wedlund and H. Schulzrinne, "Mobility support using SIP", *Proc. The Second ACM International Workshop on Wireless Mobile Multimedia*, ACM/IEEE, August 1999, pp76-82.
- [4] R. Ramjee, T. La Porta, S. Thuel and K. Varadhan, "IP micro-mobility support using HAWAII", draft-ietf-mobileip-hawaii-01.txt, IETF, July 2000, Work in Progress.
- [5] A. Campbell, J. Gomez, C-Y. Wan, S. Kim, Z. Turanyi and A. Valko, "Cellular IP", Draft draft-valko-cellularip-00.txt, IETF, July 2000, Work in Progress.
- [6] E. Gustafsson, A. Jonsson and C. Perkins, "Mobile IP regional registration", draft-ietf-mobileip-reg-tunnel-03.txt, IETF, July 2000, Work in Progress.
- [7] M. Handley, H. Schulzrinne, E. Schooler and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, IETF, March 1999.
- [8] F. Vakil, A. Dutta, J. C. Chen, S. Baba and Y. Shobatake, H. Schulzrinne "Mobility Management in a SIP environment, requirements and functions", draft-itsumo-sip-mobility-req-02.txt, IETF, December 2000 Work in Progress.
- [9] F. Vakil, A. Dutta, J. C. Chen, S. Baba and Y. Shobatake, H. Schulzrinne et al. " Supporting Mobility for TCP with SIP ", draft-itsumo-sip-mobility-tcp-00.txt, IETF, December 2000 Work in Progress.
- [10] R. Droms, "Dynamic Host Configuration Protocol (DHCP)", RFC 2131, IETF, March 1997.
- [11] Stream Control Transport Protocol, <http://www.ietf.org/rfc/rfc2960.txt>
- [12] A. Misra, S. Das, A. Mcauley, A. Dutta, and S. K. Das, "Supporting fast intra-domain handoffs with TeleMIP in cellular environments", submitted 3G Wireless 2001.
- [13] M. Handley, Eve Schooler, H. Schulzrinne, Jonathan Rosenberg " Session Initiation Protocol" RFC 2543.
- [14] H. Schulzrinne " SIP registration draft" draft-schulzrinne-sip-register-00.txt, IETF work in progress.
- [15] Subir Das, Archan Misra, Anthony Mcauley "A Comparison of Mobility protocols for Quasi-Dynamic networks" submitted for ATIRP conference
- [16] Ashutosh Dutta, Faramak Vakil, Henning Schulzrinne et al. "Application Layer Mobility Management Scheme for Mobile Wireless Internet"